Código do documento	DDK-SI-DOC-061
Título	Declaração de Continuidade de Negócios para Clientes e Parceiros
Organização	DataDike LTDA, CNPJ 54.510.206/0001-90 (Brasil)
Versão	2.3
Data de aprovação	16/08/2026
Classificação	Público, documento destinado a clientes, clientes potenciais, distribuidores, parceiros, equipes de avaliação de fornecedores e anexação em processos licitatórios
Elaborado por	Responsável pela Segurança da Informação
Revisado por	Arquitetura, Tecnologia da Informação, DPO e CISO
Aprovado por	Country Manager
Documentos de origem	DDK-SI-PLA-045, Análise de Impacto no Negócio e Plano de Continuidade. DDK-SI-PLA-046, Plano de Testes de Continuidade
Periodicidade de revisão	Anual, após cada exercício de teste e após todo incidente que tenha exigido acionamento do plano

Sumário

Sumário 2
1. OBJETIVO 3
2. ESCOPO E APLICABILIDADE 3
2.1 O que está abrangido 3
2.2 O que não está abrangido 4
2.3 Característica determinante desta análise 4
3. DEFINIÇÕES 4
4. PAPÉIS E RESPONSABILIDADES 5
5. CONTINUIDADE DE NEGÓCIOS 6
5.1 Princípios 6
5.2 Processos essenciais e impacto da interrupção 6
5.3 Objetivos de recuperação 7
5.4 Estratégias de continuidade 7
5.5 Cópias de segurança 8
5.6 Acionamento do plano e comunicação ao cliente 9
5.7 Programa de exercícios e testes 10
5.8 Fronteira de responsabilidade 10
6. REGISTROS GERADOS 11
7. MÉTRICAS E INDICADORES 11
8. EXCEÇÕES E TRATAMENTO DE DESVIOS 11
9. REFERÊNCIAS NORMATIVAS 12
10. HISTÓRICO DE VERSÕES 12

1. OBJETIVO

Apresentar, a clientes e parceiros da DataDike, como a empresa se organiza para manter e restabelecer suas atividades diante de uma disrupção, quais processos considera essenciais, em quanto tempo se propõe a recuperá-los e como comunica o cliente enquanto a situação perdura.

Este documento é a expressão pública do plano de continuidade da DataDike. O plano completo contém a análise de impacto no negócio, o mapa de dependências da arquitetura, os cenários de teste e a avaliação de risco associada. **Esse conteúdo não é publicado em nosso website e wiki**, porque descreve em detalhe onde a empresa é vulnerável, e sua divulgação ampla trabalharia contra a própria finalidade de protegê-la.

O cliente que precisa de verificação mais profunda, em processo de homologação de fornecedor ou por exigência de auditoria própria, pode solicitar acesso ao plano completo mediante acordo de confidencialidade. A DataDike atende essa solicitação.

Posição do sistema de gestão. A DataDike implanta um Sistema de Gestão de Segurança da Informação conforme a ISO/IEC 27001:2022. A continuidade de negócios é tratada dentro desse sistema, e não como iniciativa isolada.

2. ESCOPO E APLICABILIDADE

2.1 O que está abrangido

As atividades da DataDike relacionadas ao desenvolvimento, à liberação, à distribuição e ao licenciamento dos produtos DataDike PAM, plataforma de gestão de acesso privilegiado, e DataDike SONAR, plataforma de gestão unificada de dispositivos, bem como ao atendimento ao canal de distribuição e ao recebimento de relatos de vulnerabilidade.

2.2 O que não está abrangido

Continuidade do cliente	O plano de continuidade do próprio cliente, inclusive quanto aos processos que utilizem os produtos DataDike, é elaborado e testado por ele.
Terceiros do cliente	Integrações, customizações ou serviços contratados pelo cliente junto a terceiros.

2.3 Característica determinante desta análise

Há um fato da arquitetura dos produtos DataDike que precede qualquer discussão sobre tempo de recuperação, e que convém declarar antes dos números, porque muda o que está efetivamente em jogo para o cliente.

Nenhum processo da DataDike, ao ser interrompido, afeta diretamente a disponibilidade do produto já instalado no cliente.

Os produtos operam integralmente no ambiente do cliente, sem dependência de serviço mantido pela DataDike para funcionar. A empresa não realiza acesso remoto ao ambiente onde seus produtos são executados, e os dados processados pelo produto, inclusive credenciais custodiadas, permanecem sob controle do cliente.

Disso decorre que uma disrupção na DataDike não interrompe a operação do cliente. O que ela afeta é a emissão de novas licenças, a liberação de novas versões e correções, e a capacidade de atendimento. São impactos reais, tratados neste documento, mas de natureza distinta da indisponibilidade de um serviço em nuvem do qual a operação do cliente dependa minuto a minuto.

3. DEFINIÇÕES

Termo	Definição
Disrupção	Evento que interrompe ou degrada de forma relevante a capacidade da organização de executar um ou mais de seus processos essenciais.
Processo essencial	Atividade cuja interrupção produz impacto relevante sobre o negócio, sobre compromisso assumido com cliente ou canal, ou sobre obrigação legal.
RTO	Objetivo de tempo de recuperação. Prazo máximo pretendido entre a interrupção de um processo e o seu restabelecimento.
RPO	Objetivo de ponto de recuperação. Volume máximo de informação, medido em tempo, que se admite perder em razão da interrupção.

Termo	Definição
Cópia de último recurso	Cópia de segurança mantida em provedor distinto do que hospeda os ambientes de produção, sob credencial própria e com proteção contra exclusão, destinada ao cenário de perda do ambiente principal.
Exercício de mesa	Simulação conduzida de forma discutida, sem execução técnica real, com a participação de todos os papéis envolvidos no cenário.
Teste de restauração	Restauração efetiva de informação a partir de uma cópia, em ambiente isolado, com verificação de que o conteúdo é íntegro e utilizável e com medição do tempo decorrido.
Acionamento do plano	Decisão formal de passar da operação normal para a operação sob plano de continuidade, registrada com data, hora, motivo e responsável.

4. PAPÉIS E RESPONSABILIDADES

As responsabilidades abaixo são atribuídas a funções. A designação nominal de cada função consta em registro interno da DataDike, mantido atualizado e disponível ao organismo certificador e, sob acordo de confidencialidade, ao cliente que o solicite em processo de homologação.

Função	Responsabilidade na continuidade
Direção	Ratifica os objetivos de recuperação, decide sobre o acionamento do plano e sobre os recursos necessários, e responde pelas comunicações de maior alcance.
Responsável pela Segurança da Informação	Mantém o plano, propõe os objetivos de recuperação, aciona o plano quando os critérios se verificam e conduz os exercícios.
Arquitetura e Tecnologia da Informação	Executa as cópias de segurança e os testes de restauração, coordena a recuperação técnica e mede os tempos obtidos.
Comercial e gestão do canal de distribuição	Comunica distribuidores e clientes durante a disrupção, com a periodicidade definida na seção 5.7, e registra as comunicações realizadas.
Coordenação de PSIRT	Avalia se a disrupção afeta prazos de correção de vulnerabilidade assumidos publicamente e conduz a comunicação correspondente.

Interlocutor do cliente. Durante uma disrupção, o ponto de contato do cliente e do distribuidor permanece sendo o canal comercial habitual. Não há canal distinto a memorizar. Caso o correio corporativo esteja entre os serviços afetados, a DataDike utiliza os meios alternativos indicados na seção 5.7.

5. CONTINUIDADE DE NEGÓCIOS

5.1 Princípios

a) A capacidade de recuperação é demonstrada por teste, e não apenas declarada. Cópia não testada não é considerada controle implantado.

b) Os objetivos de recuperação derivam do impacto sobre o negócio, e não da conveniência técnica. É a análise de impacto que define o investimento em infraestrutura, e não o contrário.

c) A cópia destinada ao cenário mais grave reside em provedor distinto do que hospeda a produção, sob credencial própria, de modo que o comprometimento de um não alcance o outro.

d) A recuperação dos ambientes se dá preferencialmente por reconstrução a partir do código-fonte, e não por restauração de imagem. Isso reduz a superfície de dependência e torna o ambiente reconstituível em provedor diverso e tempo hábil.

e) Toda lacuna identificada em exercício gera ação de melhoria, com responsável e prazo, acompanhada até o encerramento.

5.2 Processos essenciais e impacto da interrupção

Processo	O que se perde ao interromper	Impacto em cinco dias
Emissão de licenças	Capacidade de faturar e de o canal concluir negócios	Perda de receita, negócios postergados e desgaste com o canal
Correção e liberação de versões	Capacidade de cumprir os prazos de correção publicados	Descumprimento de compromisso público, havendo correção pendente
Atendimento ao canal e ao PSIRT	Capacidade de receber e responder relatos e demandas	Descumprimento dos prazos publicados de resposta
Desenvolvimento	Produtividade da equipe e cronograma de produto	Atraso relevante no cronograma, sem efeito externo imediato
Gestão administrativa e financeira	Obrigações fiscais, trabalhistas e pagamentos	Risco de descumprimento de obrigação com prazo

5.3 Objetivos de recuperação

Os objetivos abaixo são os prazos que a DataDike estabelece para o restabelecimento de cada processo, contados do acionamento do plano.

Processo	RTO	RPO	Fundamento
Emissão de licenças	8 horas úteis	24 horas	Sustenta o faturamento e a conclusão de negócios pelo canal
Acesso administrativo aos ambientes	8 horas úteis	24 horas	É pré-condição de todas as demais recuperações
Correção e liberação de versões	2 dias úteis	24 horas	Compatível com os prazos de correção publicados
Distribuição de artefatos	2 dias úteis	7 dias	Artefatos já entregues permanecem com o distribuidor
Atendimento ao canal e ao PSIRT	1 dia útil	Conforme o serviço	Depende de serviços em nuvem, com recuperação majoritariamente a cargo do provedor
Desenvolvimento	3 dias úteis	24 horas	Afeta produtividade, sem consequência externa imediata
Gestão administrativa	3 dias úteis	7 dias	Obrigações com prazo comportam essa janela

Os prazos são expressos em horas e dias úteis por refletirem a disponibilidade da equipe técnica. O cumprimento é verificado nos testes de restauração, e resultado superior ao objetivo enseja registro e ação de melhoria, com reavaliação do objetivo ou da infraestrutura.

Disponibilidade e continuidade (SLA):

https://wiki.datadike.com/pt/pam/deploy-operate/availability-and-sla

5.4 Estratégias de continuidade

A DataDike mantém estratégia definida para cada cenário de disrupção identificado na análise de impacto. O quadro abaixo apresenta os cenários e as respectivas estratégias em formato resumido.

Cenário	Estratégia
Perda do ambiente hospedado	Reconstrução dos ambientes em nova região ou em novo provedor, a partir do código-fonte, e restauração das bases a partir da cópia de último recurso, na ordem de prioridade definida.
Indisponibilidade do cofre de segredos	Acesso de emergência por credenciais mantidas fora do sistema que protegem, sob dupla custódia, seguido da restauração da instância.

Cenário	Estratégia
Indisponibilidade do sistema de licenças	Restauração a partir da cópia diária, com avaliação de procedimento manual de contingência para emissão pontual durante a restauração.
Perda de acesso ao repositório de código	Restauração a partir de cópia mantida fora do provedor do repositório, incluindo o histórico completo.
Cifragem maliciosa dos ambientes	Isolamento do ambiente, preservação de evidência e restauração a partir de cópia protegida contra alteração e exclusão.
Comprometimento da chave de assinatura de código	Suspensão imediata de assinaturas, revogação do certificado, comunicação ao canal e aos clientes, emissão de novo certificado e reassinatura das versões suportadas.
Ausência de pessoa com conhecimento concentrado	Suplência formalmente designada para cada função, procedimentos operacionais documentados e execução periódica pelo suplente.
Perda da sede administrativa	Operação parcialmente remota, já viável pelo regime de trabalho adotado, com reposição do equipamento afetado.

5.5 Cópias de segurança

O desenho das cópias parte de uma distinção que determina todo o restante: o que se reconstrói não precisa de cópia, e o que não se reconstrói precisa de cópia situada fora do domínio de falha que a ameaça.

Informação	Frequência	Retenção	Proteção
Base histórica de licenças emitidas	Diária	90 dias	Cifrada antes do envio, com trava que impede exclusão
Gravações de sessão de acesso privilegiado	Diária	90 dias	Cifrada antes do envio, com trava que impede exclusão
Configurações e segredos operacionais	Diária	Conforme política interna	Exportação cifrada e repartida entre custodiantes distintos
Ambientes hospedados	Diária, automática	7 dias	Cópia do provedor de infraestrutura, destinada à falha comum
Ambientes de desenvolvimento e homologação	Não se copia	Não se aplica	Reconstruídos a partir do código-fonte

A cópia de último recurso é mantida em armazenamento de objeto de provedor distinto do que hospeda os ambientes, com trava de retenção que impede exclusão e sobrescrita durante o prazo definido, inclusive por quem detenha a credencial utilizada para gravá-la. A cópia é cifrada antes do envio, com a chave custodiada fora do provedor de armazenamento: a trava impede apagar, e a cifragem impede ler.

A relação nominal dos provedores utilizados não é publicada neste documento, por constituir informação que contribui para o mapeamento da superfície de ataque da empresa. Ela é fornecida ao cliente mediante acordo de confidencialidade, em processo de homologação de fornecedor.

5.6 Acionamento do plano e comunicação ao cliente

O plano é acionado por decisão do Responsável pela Segurança da Informação, com aprovação da Direção, ou pela Direção diretamente. Não havendo possibilidade de contato com a Direção, o Responsável pela Segurança da Informação aciona e registra a decisão, comunicando assim que possível. O acionamento é registrado com data, hora, motivo e responsável.

Constituem critérios objetivos de acionamento: indisponibilidade estimada de processo essencial superior ao respectivo objetivo de tempo de recuperação; perda de acesso ao ambiente de produção interno; indício de cifragem maliciosa; e comprometimento da chave de assinatura de código.

Quanto à comunicação, a DataDike adota as seguintes regras perante o cliente e o canal:

Primeira comunicação	[PREENCHER: definir o prazo máximo para a primeira comunicação ao canal após o acionamento, sugerido 4 horas úteis]
Atualizações	[PREENCHER: definir a periodicidade das atualizações enquanto durar a disrupção, sugerido diária]
Conteúdo	O que foi afetado, o que permanece operante, a previsão de restabelecimento e o que se pede ao destinatário, quando houver.
Meio	Canal comercial habitual. Estando o correio corporativo entre os serviços afetados, a DataDike utiliza os contatos de segurança designados em contrato e os meios alternativos previstos no plano.
Encerramento	Comunicação formal de normalização, com indicação do que foi restabelecido e de eventual pendência remanescente.
Registro	Toda comunicação é registrada e integra o acervo de evidências do sistema de gestão.

O distribuidor mantém junto à DataDike um contato de segurança designado, com a obrigação contratual de comunicar sua alteração. É por esse contato que a notificação alcança o cliente final atendido pelo canal.

5.7 Programa de exercícios e testes

A verificação da capacidade de recuperação é feita por programa de exercícios com periodicidade definida, e não por avaliação pontual.

Exercício	Escopo	Periodicidade
Teste de restauração	Restauração efetiva de informação de prioridade alta, com tempo medido e verificação de integridade	Trimestral
Teste de reconstrução	Criação do servidor de emissão de licenças e do cofre de acesso privilegiado a partir do código e das configurações, cronometrada	Semestral
Teste de acesso de emergência	Abertura efetiva do acesso de emergência, com pessoas de grupos de custódia distintos	Semestral
Exercício de mesa	Cenário discutido com todos os papéis envolvidos, alternando entre os cenários da seção 5.4	Semestral
Teste de continuidade	Cenário de indisponibilidade do sistema de licenças, com recuperação efetiva e tempo comparado ao objetivo	Anual
Teste por evento	Após mudança relevante de arquitetura, de provedor ou de dependência	Por evento

Cada exercício produz ata com escopo, tempo medido, verificação realizada, resultado e responsável. Resultado superior ao objetivo definido enseja reavaliação do objetivo ou da estratégia, com registro.

5.8 Fronteira de responsabilidade

A delimitação abaixo resume, para efeito de continuidade, o que responde cada parte. Ela é coerente com a Matriz de Responsabilidade Compartilhada da DataDike, documento igualmente público.

Matéria	DataDike	Cliente
Disponibilidade do produto instalado	Não aplicável, o produto não depende de serviço da DataDike para operar	Responsável integral
Cópias de segurança do ambiente do cliente	Não executa, não acessa	Responsável integral
Emissão de novas licenças	Responsável, conforme os objetivos da seção 5.3	Solicita pelo canal
Correção de vulnerabilidade do produto	Responsável, nos prazos publicados	Aplica a correção em seu ambiente
Verificação de integridade do artefato recebido	Assina digitalmente e publica o resumo criptográfico	Verifica antes de instalar
Comunicação durante a disrupção	Comunica canal e clientes, conforme a seção 5.6	Mantém o contato designado atualizado

6. REGISTROS GERADOS

Os registros abaixo são produzidos pela gestão de continuidade e compõem o acervo de evidências do sistema de gestão. Estão disponíveis ao organismo certificador e, mediante acordo de confidencialidade, ao cliente em processo de homologação de fornecedor.

Registro	Retenção	Frequência
Ata de teste de restauração	5 anos	Trimestral
Ata de exercício de mesa	5 anos	Semestral
Ata de teste de continuidade	5 anos	Anual
Registro de acionamento do plano	5 anos	Por ocorrência
Registro de comunicações realizadas ao canal e a clientes	5 anos	Por ocorrência
Registro de ação de melhoria originada em exercício	5 anos	Por ocorrência

7. MÉTRICAS E INDICADORES

Indicador	Meta	Periodicidade
Exercícios previstos no ciclo efetivamente realizados	100%	Semestral
Testes de restauração concluídos dentro do objetivo de tempo	100%	Trimestral
Ações de melhoria originadas em exercício concluídas no prazo	100%	Semestral
Comunicações ao canal realizadas dentro do prazo durante disrupção	100%	Por ocorrência
Acionamentos do plano registrados com data, hora, motivo e responsável	100%	Por ocorrência

Os resultados são consolidados no painel de indicadores do sistema de gestão e submetidos à Análise Crítica pela Direção.

8. EXCEÇÕES E TRATAMENTO DE DESVIOS

a) Exercício não realizado na periodicidade prevista é registrado como desvio, com justificativa e nova data, e levado à Análise Crítica pela Direção.

b) Resultado de teste superior ao objetivo de recuperação declarado não é tratado como falha do teste, mas como informação que obriga à reavaliação do objetivo ou da estratégia, com registro da decisão adotada.

c) Não se admite exceção quanto ao registro do acionamento do plano, quanto à comunicação ao canal durante a disrupção e quanto à execução do teste de restauração na periodicidade definida.

d) Alteração de objetivo de recuperação publicada neste documento exige aprovação da Direção e comunicação ao canal, por constituir alteração de compromisso assumido.

9. REFERÊNCIAS NORMATIVAS

Referência	Relação com este documento
ISO/IEC 27001:2022, cláusula 8.1	Planejamento e controle operacionais
ISO/IEC 27001:2022, Anexo A, A.5.29	Segurança da informação durante disrupção
ISO/IEC 27001:2022, Anexo A, A.5.30	Prontidão de tecnologia da informação e comunicação para continuidade de negócios
ISO/IEC 27001:2022, Anexo A, A.8.13	Backup das informações
ISO/IEC 27001:2022, Anexo A, A.8.14	Redundância dos recursos de tratamento de informações
DDK-SI-PLA-045	Análise de Impacto no Negócio e Plano de Continuidade, documento de origem, de uso interno
DDK-SI-PLA-046	Plano de Testes de Continuidade, documento de origem, de uso interno
DDK-SI-POL-003	Política Geral de Segurança da Informação, de classificação pública
DDK-SI-POL-020	Política de Divulgação Responsável de Vulnerabilidades e Prazos de Correção, de classificação pública

10. HISTÓRICO DE VERSÕES

Versão	Data	Descrição da alteração	Aprovado por
1.0	13/04/2025	Emissão inicial. Versão pública derivada do DDK-SI-PLA-045 e do DDK-SI-PLA-046, destinada a clientes, clientes potenciais, distribuidores e equipes de avaliação de fornecedores.	Country Manager
2.0	09/01/2026	Revisãode escopo para acionamento do plano de continuidade	Comitê SGSI
2.1	17/06/2026	Revisãode escopo para acionamento do plano de continuidade	Comitê SGSI

Versão	Data	Descrição da alteração	Aprovado por
2.2	21/06/2026	Revisãode escopo para acionamento do plano de continuidade	Comitê SGSI
2.3	16/08/2026	Revisãode escopo para acionamento do plano de continuidade	Comitê SGSI

Este documento é de classificação pública e pode ser reproduzido e distribuído na íntegra. A reprodução parcial que altere o sentido das declarações aqui contidas, em especial quanto aos objetivos de recuperação e à fronteira de responsabilidade, não é autorizada.