Esta Política foi aprovada pela DIREXE em sua 1389ª Reunião Ordinária, realizada no dia 31/05/2022, e pelo Conselho de Administração da CDP na 536ª reunião realizada em 25/10/2022 por meio de Deliberação CONSAD 80/2022.

CAPÍTULO I – OBJETIVO E DISPOSIÇÕES INICIAIS

Artigo 1º O objetivo deste documento é divulgar toda a estratégia, incluindo diretrizes, responsabilidades e competências, para a realização de cópia de segurança (*backup*) de dados sensíveis ao negócio no ambiente corporativo da Companhia Docas do Pará (CDP).

Artigo 2º Este documento deverá ficar disponível em uma área na intranet, com acesso de leitura para todas as áreas de negócio responsáveis pelos processos de backup na CDP.

Artigo 3º A salvaguarda e recuperação dos dados digitais da CDP abrange exclusivamente repositórios institucionais custodiados pela unidade administrativa de TI, armazenados nos centros de processamento de dados da empresa.

Artigo 4º Não serão salvaguardados nem recuperados dados armazenados localmente, isto é, armazenados nos microcomputadores utilizados pelos usuários de TI ou em quaisquer outros dispositivos fora dos centros de processamento de dados mantidos pela unidade de TI.

Artigo 5º A salvaguarda dos dados em formato digital pertencentes a serviços de TI da CDP, mas custodiados por outras entidades, públicas ou privadas, como nos casos de serviços em nuvem, deve estar garantida nos acordos ou contratos que formalizam a relação entre os envolvidos.

Artigo 6º Os serviços de armazenamento de dados e/ou backup fornecidos pela CDP será para uso exclusivo de dados corporativos, sendo passíveis de auditoria.

Parágrafo único. Dados pessoais poderão ser excluídos sem aviso prévio e

não poderão ser recuperados.

CAPÍTULO II - CONCEITOS E DEFINIÇÕES

Artigo 7º Para os fins desta política, considera-se:

I. **Administrador de *backup*:** agente ou unidade responsável pelo planejamento de soluções de *backup*, definição de padrões, configurações e atendimento avançado de resolução de incidentes e problemas.

II. **Área técnica:** unidade responsável pela operação técnica dos ativos e serviços de TI.

III. **Ativo crítico:** equipamento físico, unidade de armazenamento e dados que possuem elevada importância para a continuidade das atividades e serviços e concretização dos objetivos da organização.

IV. ***Backup*:** cópia de segurança de dados computacionais, que pode ser utilizada ou consultada após sua restauração, em caso de indisponibilidade, perda ou alteração dos dados originais.

V. ***Backup* completo:** modalidade de *backup* em que todos os dados a serem salvaguardados são copiados integralmente (cópia de segurança completa) para uma unidade de armazenamento, independentemente de terem sido ou não alterados desde o último *backup*.

VI. ***Backup* incremental:** modalidade de *backup* em que são salvaguardados apenas os dados novos ou modificados desde o último *backup* de qualquer modalidade efetuado.

VII. ***Backup* diferencial**: modalidade de *backup* em que são salvaguardados apenas dados novos ou modificados desde o último *backup* completo efetuado;

VIII. **Criticidade:** grau de importância dos dados para a continuidade das atividades e serviços da organização.

IX. **Descarte:** eliminação correta de dados, documentos, unidades de armazenamento e acervos digitais;

X. **Disponibilidade:** garantia de que o dado esteja acessível e utilizável sob demanda de pessoa física ou determinado serviço de TI, órgão ou entidade devidamente autorizados;

XI. **Gestor da informação:** agente público formalmente responsável pela administração de serviço de TI e pelas informações produzidas em seu processo de trabalho.

XII. **Imagem de *backup*:** arquivo gerado pela solução de *backup*, não necessariamente no formato original dos arquivos que contêm os dados salvaguardados.

XIII. **Janela de *backup*:** período de tempo durante o qual cópias de segurança sob execução agendada ou manual poderão ser executadas.

XIV. **Operador de *backup*:** profissional responsável por procedimentos de atendimento de primeiro nível, acompanhamento de execução de rotinas de *backup*, realização de restaurações de arquivos de usuários e manutenção nos sistemas de *backup* e recuperação.

XV. **Plano de continuidade de negócios (PCN):** plano que define as etapas necessárias para recuperação dos processos de negócio logo após uma interrupção, identificando também os gatilhos para invocação, as pessoas a serem envolvidas, as comunicações, etc.

XVI. **Restauração:** processo de recuperação e disponibilização de dados salvaguardados em determinada imagem de *backup*.

XVII. **Retenção:** período de tempo pelo qual os dados devem ser salvaguardados e estar aptos à restauração.

XVIII. ***Recovery point objective* (RPO):** ponto no tempo em que os dados dos serviços de TI devem ser recuperados após uma situação de parada ou perda, correspondendo ao prazo máximo em que se admite perder dados no caso de um incidente.

XIX. ***Recovery time objective* (RTO):** tempo estimado para restaurar os dados e tornar os serviços de TI novamente operacionais; correspondendo ao prazo máximo em que se admite manter os serviços de TI inoperantes até a restauração de seus dados, após um incidente.

XX. **Rotina de *backup*:** procedimento utilizado para se realizar um *backup*.

XXI. **Serviço de TI:** sistema de informação ou qualquer solução de tecnologia da informação que armazene informações em formato digital.

XXII. **Unidade de armazenamento:** dispositivo para armazenamento de dados em suporte digital.

XXIII. **Unidade de armazenamento de *backup*:** unidade de armazenamento com características específicas para retenção de cópia de segurança de dados digitais.

CAPÍTULO 3 - PADRÕES OPERACIONAIS

SEÇÃO I - PRINCÍPIOS GERAIS

Artigo 8º A Política de *Backup* e Recuperação de Dados Digitais deve estar alinhada com uma gestão de continuidade de negócios em nível organizacional.

Artigo 9º As rotinas de *backup* devem ser orientadas para a restauração dos dados no menor tempo possível, principalmente quando da indisponibilidade de serviços de TI.

Artigo 10 As rotinas de *backup* devem possuir requisitos mínimos diferenciados de acordo com o tipo de serviço de TI ou dado salvaguardado, dando prioridade aos serviços de TI críticos da organização.

Artigo 11 Os serviços e ativos de TIC críticos da CDP devem ser formalmente elencados pelo Comitê de Gestão de Tecnologia da Informação (CGTI) da empresa.

Artigo 12 Já ficam previamente estabelecidas as seguintes soluções e suas bases de dados na CDP: Sistema de Gestão Portuária, ERP Gestão de Pessoal e Gestão Empresarial, Portal de Internet e Servidor de Arquivos (*Active Directory*).

Parágrafo Único. Os fornecedores e desenvolvedores de sistemas devem documentar as melhores práticas de backup para seus respectivos sistemas.

SEÇÃO II - FERRAMENTAS DE *BACKUP*

Artigo 13 As rotinas de *backup* devem utilizar soluções próprias e especializadas para este fim, preferencialmente de forma automatizada.

Artigo 14 Os ativos envolvidos no processo de *backup* são considerados ativos críticos para a organização.

Artigo 15 Compete à Gerência de TI solicitar, à Diretoria da CDP, com as justificativas pertinentes, os equipamentos e softwares necessários para manter o parque de ativos computacionais sempre atualizado e em quantidade necessária ao atendimento da demanda de *backup* da CDP.

SEÇÃO III - FREQUÊNCIA E RETENÇÃO DOS DADOS

Artigo 16 Os *backups* dos serviços de TI críticos da CDP devem ser realizados utilizando-se as seguintes frequências temporais:

I. Diária;
II. Semanal;
III. Mensal;
IV. Anual.

Artigo 17 A retenção dos *backups* críticos e não críticos da CDP devem ser resguardados sob um padrão mínimo, o qual deve observar a correlação frequência/retenção de dados estabelecida a seguir:

I. Diária: 1 semana;
II. Semanal: 1 mês;
III. Mensal: 12 meses;
IV. Anual: 2 anos.

Artigo 18 O *backup* de serviços de TI não críticos deve ser formalmente solicitado ao administrador de *backup* pelo responsável técnico do serviço de TI.

Artigo 19 Especificidades dos serviços de TI críticos e dos serviços de TI não críticos podem demandar frequência e tempo de retenção diferenciados ao citado no Artigo 16.

Artigo 20 As especificidades que demandam frequência e retenção diferenciadas deverão constar em documentos normativos complementares da CDP.

Artigo 21 A solicitação de salvaguarda dos dados referentes aos serviços de TI críticos e aos serviços de TI não críticos deve ser realizada pelos responsáveis técnicos dos serviços de TI, com a anuência prévia e formal dos gestores das informações, refletindo os requisitos de negócio da organização, bem como os requisitos de segurança da informação envolvidos e a criticidade da informação para a continuidade da operação da organização, e deve explicitar, no mínimo, os seguintes requisitos técnicos:

I. Escopo ou abrangência (dados digitais a serem salvaguardados);
II. Tipo de *backup* (completo, incremental, diferencial);
III. Frequência temporal de realização do *backup* (diária, semanal, mensal, anual);
IV. Retenção;
V. RPO;
VI. RTO.

Artigo 22 A recuperação de dados não será viabilizada em caso de perdas anteriores à conclusão da cópia de segurança. Dados criados ou modificados entre execuções de cópias de segurança subsequentes não serão protegidos por soluções de *backup*.

Artigo 23 A alteração das frequências e tempos de retenção definidos nesta seção deve ser precedida de solicitação e justificativa formais encaminhadas ao administrador de *backup*. A aprovação para execução da alteração depende da anuência do gestor da informação e de prévia apreciação pelo CGTI.

Artigo 24 O administrador de *backup* deve considerar o impacto da execução das rotinas de *backup* sobre o desempenho da rede de dados da CDP,

garantindo que o tráfego necessário às suas atividades não ocasione indisponibilidade dos demais serviços de TI da organização.

Artigo 25 A execução do *backup* deve concentrar-se, preferencialmente, no período de janela de *backup*.

Artigo 26 O período de janela de *backup* deve ser determinado pelo administrador de *backup* em conjunto com a área técnica responsável pela administração da rede de dados da CDP.

CAPÍTULO 4 – UNIDADES DE ARMAZENAMENTO DE *BACKUPS*

Artigo 27 As unidades de armazenamento utilizadas na salvaguarda dos dados digitais devem considerar as seguintes características dos dados resguardados:

I. A criticidade do dado salvaguardado;
II. O requisito de segurança da informação;
III. O tempo de retenção do dado;
IV. A probabilidade de necessidade de restauração;
V. O tempo esperado para restauração;
VI. O custo de aquisição da unidade de armazenamento de *backup*;
VII. A vida útil da unidade de armazenamento de *backup*.

Artigo 28 O administrador de *backup* deve identificar a viabilidade de utilização de diferentes tecnologias na realização das cópias de segurança, propondo a melhor solução para cada caso.

Artigo 29 Podem ser utilizadas técnicas de compressão de dados, contanto que o acréscimo no tempo de recuperação dos dados seja considerado aceitável pelos gestores das informações.

Artigo 30 As unidades de armazenamento dos *backups* devem ser acondicionadas em locais apropriados, com controle de fatores ambientais sensíveis, como umidade e temperatura, uso de criptografia e com acesso restrito a pessoas autorizadas pelo administrador de *backup***.**

Artigo 31 Quando da necessidade de descarte de unidades de armazenamento de *backups*, tais recursos devem ser fisicamente destruídos de forma a inutilizá-los, atentando-se ao descarte sustentável e ambientalmente correto**.**

Artigo 32 Os *backups* devem ser testados periodicamente, com o objetivo de garantir a sua confiabilidade e a integridade dos dados salvaguardados.

Artigo 33 Os testes de restauração dos *backups* devem ser realizados, por amostragem, em equipamentos servidores diferentes dos equipamentos que atendem os ambientes de produção, observados os recursos humanos e tecnológicos disponíveis em cada unidade da CDP.

Artigo 34 A periodicidade, a abrangência, os procedimentos e as rotinas inerentes aos testes de *backup* serão definidos em norma específica a ser elaborada pela Gerência de Tecnologia da Informação (GETINF) em conjunto com os gestores das informações**.**

CAPÍTULO 5 – RESPONSABILIDADES

Artigo 35 O administrador de *backup* e o operador de *backup* devem ser capacitados para as tecnologias, procedimentos e soluções utilizadas nas rotinas de *backup*.

Artigo 36 O administrador e o operador de *backup* da CDP serão indicados pelo CGTI e nomeados Diretor Presidente, entre os empregados de carreira lotados no setor de TI da organização.

Artigo 37 Caso não seja possível a indicação de empregados distintos, o mesmo empregado poderá exercer os papéis de administrador e operador de *backup* desde que não conflite com outras funções do funcionário.

Artigo 38 São atribuições do **administrador de *backup***:

I. Propor soluções de cópia de segurança das informações digitais corporativas produzidas ou custodiadas pela CDP;
II. Providenciar a criação e manutenção dos *backups*;
III. Configurar as soluções de *backup*;

IV. Manter as unidades de armazenamento de *backups* preservadas, funcionais e seguras;
V. Definir os procedimentos de restauração e neles auxiliar;
VI. Verificar diariamente os eventos gerados pela solução de *backup*, tomando as providências necessárias para remediação de eventuais falhas;
VII. Tomar medidas preventivas para evitar falhas;
VIII. Reportar imediatamente ao setor a que está subordinado os incidentes ou erros que causem indisponibilidade ou impossibilitem a execução ou restauração de *backups*;
IX. Gerenciar mensagens e registros de auditoria (logs) diários dos *backups*;
X. Disponibilizar informações que subsidiem as decisões referentes à gestão de capacidade relacionada aos *backups*;
XI. Propor modificações visando ao aperfeiçoamento desta Política de *Backup* e Recuperação de Dados Digitais;
XII. Providenciar a execução dos testes de restauração.

Artigo 39 São atribuições do **operador de *backup***:

I. Restaurar ou recuperar os *backups* em caso de necessidade;
II. Operar e manusear as unidades de armazenamento de *backups*;
III. Informar ao administrador de *backup* qualquer problema que impossibilite a restauração de um *backup*.

Artigo 40 São atribuições das **áreas técnicas**:

I. Solicitar restaurações de dados, com anuência do gestor da informação;
II. Sanar dúvidas técnicas do administrador de *backup* acerca das informações salvaguardadas;
III. Validar, tecnicamente, o resultado das restaurações eventualmente solicitadas;
IV. Validar, tecnicamente, o resultado dos testes de restauração dos *backups*.

Artigo 41 São atribuições dos **gestores da informação**:

I. Solicitar, formalmente, a salvaguarda das informações geridas e dar anuência à solicitação feita pela área técnica para recuperação de dados;
II. Validar, negocialmente, o resultado das restaurações eventualmente solicitadas;
III. Validar, negocialmente, o resultado dos testes de restauração dos *backups*;
IV. A solicitação de restauração de dados que tenham sido salvaguardados depende de prévia e formal autorização dos respectivos gestores das informações;
V. O operador de *backup* terá a prerrogativa de negar a restauração de dados cujo conteúdo não seja condizente com a atividade institucional, cabendo recurso da negativa ao gestor da unidade do demandante.

CAPÍTULO 6 - REFERENCIAL NORMATIVO

Artigo 42 A Instrução Normativa GSI/PR 1, de 13 de junho de 2008, do Gabinete de Segurança Institucional da Presidência da República, que disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, e dá outras providências;

Artigo 43 As determinações do Tribunal de Contas da União contidas no Acórdão 2732/2017, item 9.6.1, para que se formule e se apresente ao TCU plano de ação para a criação de plano de continuidade de negócio e criação e implantação de política de geração de cópias de segurança dos dados cautelados pelo Tribunal (*backup* e restauração);

Artigo 44 A Norma Técnica ABNT NBR ISO/IEC 27001:2013, que especifica os requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão da segurança da informação dentro da organização;

Artigo 45 A Deliberação CGTI Nº 13/2021, que institui no âmbito desta

Companhia Docas do Pará - CDP, Comissão Política de *Backup* - CDP, com o objetivo de elaborar um Plano de Ação com cronograma de trabalho, com vista à introdução de uma Política de *Backup* na CDP, para vias de sanar e/ou mitigar as fragilidades do Armazenamento de dados da Companhia.

CAPÍTULO 7 - DISPOSIÇÕES FINAIS

Artigo 46 Esta Política deverá ser amplamente divulgada na CDP, fazendo-se ainda constar, em destaque, na área de tecnologia da informação da intranet da CDP, o link de sua publicação.

Artigo 47 Esta Política deverá ser revisada anualmente. Contudo, quando identificada a necessidade de alteração em qualquer de seus dispositivos, poderá ser atualizada a qualquer tempo.

Artigo 48 A Gerência de Tecnologia da Informação, as unidades de TI e os gestores das informações digitais tomarão as providências necessárias para a adequação das rotinas e dos procedimentos de *backups* definidos nesta Política.

Artigo 49 Poderão fazer parte desta Política, como anexos, dispositivos operacionais e auxiliares da estratégia de *backup*, tais como planos detalhados, normas, fluxos de processos, etc.

Artigo 50 Casos excepcionais não abordados neste documento serão decididos pelo CGTI, com análise da Gerência de Tecnologia da Informação, e sendo necessário, pelas demais unidades de TI (supervisão/coordenação) ou pelos gestores das informações digitais.