MINISTÉRIO DA INTEGRAÇÃO E DO DESENVOLVIMENTO REGIONAL
DEPARTAMENTO NACIONAL DE OBRAS CONTRA AS SECAS
PORTARIA Nº 135 DG, DE 22 DE MARÇO DE 2024

Ministério da Integração e do Desenvolvimento Regional - MDR
Departamento Nacional de Obras Contra as Secas – DNOCS
Comitê de Governança Digital - CGD

Institui a Política de Backup e Restauração de Dados Digitais – DNOCS.

O DIRETOR-GERAL O DEPARTAMENTO NACIONAL DE OBRAS CONTRA AS SECAS – DNOCS, no uso das atribuições legais que lhe confere o disposto no Art. 68 e respectivo inciso XII da Portaria DNOCS/DG/GAB nº 43, de 31 de janeiro de 2017, em atendimento à Estratégia de Governo Digital e à Instrução Normativa GSI/PR nº 1, de 27 de maio de 2020;

R E S O L V E:

Art. 1º Aprovar a Política de Backup e Restauração de Dados Digitais do Departamento Nacional de Obras Contra as Secas – DNOCS, na forma do Anexo I desta Portaria, de observância obrigatória no âmbito dessa Autarquia Federal.

Art. 2º Esta Portaria entra em vigor em 1º de Abril de 2024.

Fernando Marcondes de Araújo Leão
Diretor-Geral do DNOCS

ANEXO I

POLÍTICA DE BACKUP E RESTAURAÇÃO DE DADOS DIGITAIS

CAPÍTULO I
PROPÓSITO

Art. 1º A Política de Backup e Restauração de Dados Digitais objetiva instituir diretrizes, responsabilidades e competências que visam à segurança, proteção e disponibilidade dos dados digitais custodiados pelo Serviço de Tecnologia da Informação e formalmente definidos como de necessária salvaguarda no DNOCS, para se manter a continuidade do negócio.

Art. 2º No sentido de assegurar sua missão é fundamental estabelecer mecanismos que permitam a guarda dos dados e sua eventual restauração em casos de indisponibilidades ou perdas por erro humano, ataques, catástrofes naturais ou outras ameaças.

Art. 3º O presente documento apresenta a Política de Backup e Restauração de Dados Digitais, onde se estabelece o modo e a periodicidade de cópia dos dados armazenados pelos sistemas computacionais.

CAPÍTULO II
ESCOPO

Art. 4º Esta política se aplica a todos os dados no âmbito do DNOCS, incluindo dados fora do DNOCS armazenados em um serviço de nuvem Pública ou Privada. “Dados críticos”, neste contexto, incluem base de dados de sistemas em produção, correio eletrônico, Sistema eletrônico de Informações(SEI) e o ambiente Apoena. A definição de dados críticos e o escopo desta política de backup serão revisados anualmente;

Art. 5º Já ficam previamente estabelecidos os serviços relacionados aos processos de Monitoramento e Segurança de Barragens, Estudos e Implantação de Infraestruturas Hídricas e Execução de Projetos e Planos de Irrigação como serviços críticos do *DNOCS*.

Art. 6º Esta política se aplica a agentes públicos que podem ser criadores e/ou usuários de tais dados. A política também se aplica a terceiros que acessam e usam no DNOCS sistemas e equipamentos de TI ou que criam, processam ou armazenam dados de propriedade do DNOCS.

Art. 7º Não serão salvaguardados nem recuperados dados armazenados localmente, nos microcomputadores dos usuários ou em quaisquer outros dispositivos fora dos centros de processamento de dados mantidos pelas unidades de TI, ficando sobre a responsabilidade do indivíduo que usa o(s) dispositivo(s).

Art. 8º A salvaguarda dos dados em formato digital pertencentes a serviços de TI do DNOCS 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.

CAPÍTULO III
TERMOS E DEFINIÇÕES

Art. 9º Abaixo definições de termos chaves, siglas ou conceitos que serão utilizados na política

I. BACKUP OU CÓPIA DE SEGURANÇA - Conjunto de procedimentos que permitem salvaguardar os dados de um sistema computacional, garantindo guarda, proteção e recuperação. Tem a fidelidade ao original assegurada. Esse termo também é utilizado para identificar a mídia em que a cópia é realizada;

II. CUSTODIANTE DA INFORMAÇÃO - Qualquer indivíduo ou estrutura de órgão ou entidade da Administração Pública Federal, direta e indireta, que tenha responsabilidade formal de proteger a informação e aplicar os níveis de controles de segurança em conformidade com as exigências de Segurança da Informação comunicadas pelo proprietário da informação;

III. ELIMINAÇÃO - Exclusão de dado ou conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado;DESCARTE - eliminação correta de

informações, documentos, mídias e acervos digitais.

IV. MÍDIA - Mecanismos em que dados podem ser armazenados. Além da forma e da tecnologia utilizada para a comunicação - inclui discos ópticos, magnéticos, CDs, fitas e papel, entre outros. Um recurso multimídia combina sons, imagens e vídeos;

V. INFRAESTRUTURA CRÍTICA – instalações, serviços, bens e sistemas, virtuais ou físicos, que se forem incapacitados, destruídos ou tiverem desempenho extremamente degradado, provocarão sério impacto social, econômico, político, internacional ou à segurança;

VI. EVENTO DE SEGURANÇA - Qualquer ocorrência identificada em um sistema, serviço ou rede, que indique uma possível falha da política de segurança, falha das salvaguardas ou mesmo uma situação até então desconhecida, que possa se tornar relevante em termos de segurança.

VII. 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;

VIII. 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;

CAPÍTULO IV
REFERÊNCIA LEGAL E DE BOAS PRÁTICAS

Art. 10 Abaixo lista de leis, regulamentos e guias de boas práticas que regem a política em sua conformidade e cumprimento.

Orientação	**Seção**
Acórdão 1.109/2021-TCU-Plenário	Em sua íntegra
Decreto 10.332/2020 - Estratégia de Governo Digital 2020-2022	Em sua íntegra
Decreto Nº 10.046/2019 - Governança no Compartilhamento de Dados (GCD)	Art. 2, XXIII
Decreto Nº 10.222/2020 - Estratégia Nacional de Segurança Cibernética (E-CIBER)	Anexo, Item 2.3.4 e 2.3.5
Decreto Nº 9.573/2018 - Política Nacional de Segurança de Infraestruturas Críticas (PNSIC)	Anexo, art.3, Inciso I, II e V
Decreto Nº 9.637/2018 - Política Nacional de Segurança da Informação (PNSI)	CAPÍTULO I - Art.2, Incisos III e IV CAPÍTULO II - Art.3, Inciso III, IV, VIII XI CAPÍTULO VI - Seção IV – Art.15
Framework Control Objectives for Information and Related Technology – Cobit, conjunto de boas práticas a serem aplicadas à governança da TI;	v4.1: DS11: Gerenciar Dados v5: DSS01.01, DSS04.08; DSS06.04, DSS04.08, DSS05.06; DSS06.05-06, DSS04.08, DSS001.01; DSS05.02-05; DSS06.03; DSS06.06
Guia do Framework de Privacidade e Segurança da Informação	Controle 11
Framework Information Technology Infrastructure Library – ITIL, v. 4, conjunto de boas práticas a serem aplicadas na infraestrutura, operação e gerenciamento de serviços de TI;	Gestão da Segurança da Informação

Instrução Normativa 01/GSI/PR	Art.12, Inciso IV, alínea g, h
Instrução Normativa Nº 03/GSI/PR, de 28 de maio de 2021	Capítulo IV
Lei Nº 13.709/2018 – Lei Geral de Proteção de Dados	CAPÍTULO VII - Seção I – Art. 46, Seção II Art. 50
Lei Nº 12.527/2011 – Lei de Acesso à Informação (LAI)	Em sua íntegra
Norma ABNT NBR ISO/IEC 27001:2013 Tecnologia da informação - Técnicas de segurança - Sistemas de gestão de segurança da informação - Requisitos;	A.12.3 Cópias de segurança
Norma ABNT NBR ISO/IEC 27002:2013 Tecnologia da informação - Técnicas de segurança - Código de prática para a gestão da segurança da informação;	12.3 Cópias de segurança
Portaria GSI/PR nº 93, de 18 de outubro de 2021	Em sua íntegra

CAPÍTULO V
DECLARAÇÕES DA POLÍTICA

Art. 11 Dos princípios gerais:

I. A Política de Backup e Restauração de Dados deve estar alinhada com à Política de Segurança da Informação do DNOCS.

II. A Política de Backup e Restauração de Dados deve estar alinhada com uma gestão de continuidade de negócios em nível organizacional.

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

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

V. 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.

VI. O armazenamento de backup, se possível, deve ser realizado em um local distinto da infraestrutura crítica. É desejável que se tenha um sítio de backup em um local remoto ao da sede da organização para armazenar cópias extras dos principais backups, a exemplo dos backups de dados de serviços críticos.

VII. A infraestrutura de rede de backup deve ser apartada, lógica e fisicamente, dos sistemas críticos da organização.

VIII. Manter reserva de recursos (físicos e lógicos) de infraestrutura para realização de teste de restauração de backup.

IX. Em situações em que a confidencialidade é importante, convém que cópias de segurança sejam protegidas através de encriptação.

Art. 12 **Da frequência e retenção dos dados:**

I. Os backups dos serviços de TI críticos do DNOCSdevem ser realizados utilizando-se as seguintes frequências temporais:

   a. Diária;

   b. Semanal;

   c. Mensal;

   d. Anual.

II. Os serviços de TI críticos do DNOCS devem ser resguardados sob um padrão mínimo, o qual deve observar a correlação frequência/retenção de dados estabelecida a seguir:

a. Diária: 2 meses;

b. Semanal: 4 meses;

c. Mensal: 1 ano;

d. Anual: 5 anos.

III. Os serviços de TI NÃO críticos do DNOCS devem ser resguardados sob um padrão mínimo, o qual deve observar a correlação frequência/retenção de dados estabelecida a seguir:

1. Diária: 1 meses;

2. Semanal: 2 meses;

3. Mensal: 6 meses;

4. Anual: 2 anos.

IV. Especificidades dos serviços de TI críticos e dos serviços de TI não críticos podem demandar frequência e tempo de retenção diferenciados.

V. Os ativos envolvidos no processo de backup são considerados ativos críticos para a organização.

VI. A solicitação de salvaguarda dos dados referentes aos serviços de TI críticos e aos serviços de TI não críticos deve ser realizada pela unidade de TIC, com a anuência prévia e formal do Comitê de Governança Digital, refletindo os requisitos de negócio da organização, bem como os requisitos de segurança da informação e proteção de dados envolvidos e a criticidade da informação para a continuidade da operação da organização, e deve explicitar, no mínimo, os seguintes requisitos técnicos:

a. Escopo (dados digitais a serem salvaguardados);

b. Tipo de *backup* (completo, incremental, diferencial);

c. Frequência temporal de realização do backup (diária, semanal, mensal, anual);

d. Retenção;

e. RPO;

f. RTO.

VII. A alteração das frequências e tempos de retenção definidos nesta seção deve ser precedida de solicitação e justificativa formais encaminhadas à unidade de TIC. A aprovação para execução da alteração depende da anuência do responsável pela unidade de TIC.

VIII. Os responsáveis pelos dados deverão ter ciência dos tempos de retenção estabelecidos para cada tipo de informação e os administradores de backup deverão zelar pelo cumprimento das diretrizes estabelecidas.

IX. **Tipo de backup**

I – Completo (*full*);

II – Incremental;

III – Diferencial.

Backup incremental diário (segunda a sábado), armazenado no local.

X. Backup completo semanal (sábado a domingo), armazenado externamente. Sempre que possível, os backups devem ser iniciados às 12h da manhã de sábado para permitir mais tempo durante o fim de semana para realizar o backup e tempo suficiente para lidar com quaisquer problemas que possam surgir durante o processo de backup.

XI. **Tipo de backup**

I – Completo (*full*);

II – Incremental;

XII. Salvo indicação em contrário, o backup dos dados do sistema será feito de acordo com a seguinte programação padrão:

XIII. Backup incremental diário (segunda a sábado), armazenado no local.

XIV. Backup completo semanal (sábado a domingo), armazenado externamente. Sempre que possível, os backups devem ser iniciados às 12h da manhã de sábado para permitir mais tempo durante o fim de semana para realizar o backup e tempo suficiente para lidar com quaisquer problemas que possam surgir durante o processo de backup.

Art. 13 **Do uso da rede**

I. O administrador de backup deve considerar o impacto da execução das rotinas de backup sobre o desempenho da rede de dados do DNOCS, garantindo que o tráfego necessário às suas atividades não ocasione indisponibilidade dos demais serviços de TI do DNOCS.

II. A execução do backup deve concentrar-se, preferencialmente, no período de janela de backup.

III. 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 do DNOCS.

Art. 14 **Do transporte e armazenamento**

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

   a. A criticidade do dado salvaguardado;

   b. O tempo de retenção do dado;

   c. A probabilidade de necessidade de restauração;

   d. O tempo esperado para restauração;

   e. O custo de aquisição da unidade de armazenamento de backup;

   f. A vida útil da unidade de armazenamento de backup.

II. 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.

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

IV. A execução das rotinas de backup deve envolver a previsão de ampliação da capacidade dos dispositivos envolvidos no armazenamento.

V. No caso de desligamento do usuário (de forma permanente ou temporária), o backup de seus arquivos em nuvem deverá ser mantido por, no mínimo, 3 meses. Após esse período os arquivos poderão ser excluídos a qualquer tempo.

VI. As unidades de armazenamento dos backups devem ser acondicionadas em locais apropriados, com controle de fatores ambientais sensíveis, como umidade, temperatura, poeira e pressão, e com acesso restrito a pessoas autorizadas pelo administrador de backup. Além disso, as condições de temperatura, umidade e pressão devem ser aquelas descritas pelo fabricante das unidades de armazenamento.

VII. 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.

VIII. A mídia será claramente identificada e armazenada em uma área segura acessível apenas para fornecedor contratado para operação da infraestrutura de tic, servidores da unidade de tic e da unidade de documentação.

IX. A mídia não será deixada sem supervisão durante o transporte.

X. Backups completos mensais dos dados arquivados serão mantidos por até 3 meses. Depois deste período, as fitas serão devolvidas à unidade TIC e serão reutilizadas ou destruídas.

XI. Backups completos anuais dos dados arquivados serão mantidos por 10 anos. Após esse período, as fitas serão devolvidas à unidade de TIC e serão reutilizadas ou destruídas.

XII. Backups completos diários serão mantidos por até 3 meses em uma sala com segurança básica.

Art. 15 **Dos testes de backup:**

I. Os backups serão verificados periodicamente:

II. Diariamente os logs de backup serão revisados em busca de erros, durações anormais e em busca de oportunidades para melhorar o desempenho do backup.

III. Ações corretivas serão tomadas quando os problemas de backup forem identificados, a fim de reduzir os riscos associados a backups com falha.

IV. A TI manterá registros de backups e testes de restauração para demonstrar conformidade com esta política.

V. Os testes devem ser realizados em todos os backups produzidos independente do ambiente.

VI. Os testes de restauração dos backups devem ser realizados 1(uma) vez ao mês, em equipamentos servidores diferentes dos equipamentos que atendem os ambientes de produção, observados os recursos humanos de TI e tecnologias disponíveis, a fim de verificar backups bem-sucedidos.

VII. Verificar se foi atendido os níveis de serviço pactuados, tais como os Recovery Time Objective – RTOs.

VIII. Os registros deverão conter, no mínimo, o tipo de sistema/serviço que teve o seu reestabelecimento testado, a data da realização do teste, o tempo gasto para o retorno do backup e se o procedimento foi concluído com sucesso

IX. Quaisquer exceções a esta política serão totalmente documentadas e aprovadas pelo Comitê de Governança Digital.

Art. 16 Procedimento de restauração de backup

I. O atendimento de solicitações de restauração de arquivos, e-mails e demais formas de dados deverá obedecer às seguintes orientações:

   a. A solicitação de restauração de objetos deverá sempre partir do responsável pelo recurso, através de chamado técnico.

   b. A restauração de objetos somente será possível nos casos em que este tenha sido atingido pela estratégia de backup.

   c. A solicitação de restauração de dados que tenham sido salvaguardados depende de prévia e formal autorização dos respectivos gestores das informações.

d. 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.

II. O cronograma de restauração de dados:

a. O tempo de restauração é de 48h, podendo ser prorrogado por mais 48h caso o volume de dados seja superior a 100gb.

b. Backups externos serão disponibilizados em aproximadamente 3 dias de uma falha catastrófica do sistema, observando a prioridade para restauração de acordo com a criticidade de cada um;

c. Backups externos serão disponibilizados em aproximadamente 5 dias de uma falha não catastrófica do sistema, observando a prioridade para restauração de acordo com a criticidade de cada um.

III. Qualquer solicitação para recuperação de dados deverá ser registrada via ticket de suporte contendo caminho completo do(s) arquivo(s) e/ou diretório(s)

IV. Não serão aceitos pedidos de recuperação total de um compartilhamento de rede ou diretórios com mais de 50GB.

Art. 17 **Do Descarte da Mídia**

I. A mídia de backup será retirada e descartada conforme descrito neste documento:
a. A TI garantirá que a mídia não contenha mais imagens de backup ativas e que o conteúdo atual ou anterior não possa ser lido ou recuperado por terceiros não autorizados.
b. A TI garantirá a destruição física da mídia antes do descarte.

Art. 18 **Das Responsabilidades**

São atribuições do administrador de backup:

I. Propor soluções de cópia de segurança das informações digitais corporativas produzidas ou custodiadas pela organização;

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;

CAPÍTULO VI
NÃO CONFORMIDADE

Art. 19 As sanções por descumprimento podem incluir, mas não se limitam a um ou mais dos seguintes:

I. Processo Administrativo disciplinar de acordo com a legislação aplicável

II. Exoneração.

III. Ação judicial de acordo com as leis aplicáveis e acordos contratuais.

IV. Rescisão contratual ao bem do serviço público.

CAPÍTULO VIII
CONCORDÂNCIA

Art. 20 O termo de concordância em anexo firma o entendimento e o acordo para cumprir a política pelos colaboradores do DNOCS.

CAPÍTULO XVII
DISPOSIÇÕES FINAIS

Art. 21 Os casos omissos serão resolvidos pelo Comitê de Governança Digital(CGD)

ANEXO II

Termo de Concordância

Eu li e entendi a Política de Backup e Restauração de Dados Digitais do DNOCS. Entendo que se eu violar as diretrizes estabelecidas nesta Política, posso enfrentar ações legais e/ou disciplinares de acordo com as leis aplicáveis e as normas internas do DNOCS.

_____

Nome do Servidor/Empregado

_____

Assinatura do Colaborador/Data