MINISTÉRIO DA ECONOMIA
Procuradoria-Geral da Fazenda Nacional

PORTARIA PGFN/ME Nº 7467, DE 18 DE AGOSTO DE 2022

Dispõe sobre a Política de Backup de Dados Digitais no âmbito da Procuradoria-Geral da Fazenda Nacional.

A PROCURADORA-GERAL DA FAZENDA NACIONAL SUBSTITUTA, no uso das atribuições que lhe conferem o art. 10, I, do Decreto-Lei nº 147, de 3 de fevereiro de 1967, e o art. 82, incisos IX, XIII e XVIII, do Regimento Interno da Procuradoria-Geral da Fazenda Nacional, aprovado pela Portaria do Ministro de Estado da Fazenda nº 36, de 24 de janeiro de 2014,

RESOLVE:

Art. 1º Instituir a Política de Backup e Restauração de Dados Digitais no âmbito da Procuradoria-Geral da Fazenda Nacional.

Art. 2º 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 e formalmente definidos como de necessária salvaguarda na PGFN, para se manter a continuidade do negócio. 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. A Política de Backup é parte integrante da Política de Segurança da Informação e Privacidade dos Dados PGFN.

CAPÍTULO I
DISPOSIÇÕES PRELIMINARES

Seção I
Do Escopo

Art. 3º Esta política se aplica a todos os dados críticos no âmbito da PGFN, incluindo dados fora da organização armazenados em um serviço de nuvem pública ou privada.

Parágrafo único. “Dados críticos”, neste contexto, incluem bases de dados de sistemas, aplicações, filesystems ou drivers de armazenamento de arquivos e sistemas operacionais de servidores.

Art. 4º Para os ambientes em que essa política seja considerada não aplicável, deve ser conduzida avaliação de risco e documentados os critérios para a escolha de não realização de backup.A documentação deve ser enviada para a Coordenação-Geral de Tecnologia da Informação PGFN (CGTI) para armazenamento.

Art. 5º Os serviços de TI críticos da PGFN devem ser formalmente elencados pelo Comitê

Estratégico de Tecnologia da Informação - CETI.

Parágrafo único. Os sistemas estruturantes, onde se implementam as atividades finalísticas e estratégias da PGFN, devem ser classificados obrigatoriamente como serviços críticos da organização.

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 na organização sistemas e equipamentos de TI ou que criam, processam e armazenam dados de propriedade da organização.

Art. 7º Não serão salvaguardados nem recuperados dados armazenados localmente, nos microcomputadores dos usuários, smartphones ou em quaisquer outros dispositivos fora dos centros de processamento de dados mantidos pela CGTI diretamente ou mediante contratos, ficando sob a responsabilidade do indivíduo que usa o(s) dispositivo(s).

Art. 8º A salvaguarda dos dados em formato digital pertencentes a serviços de TI da PGFN 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. Neste caso, a salvaguarda dos dados deve ser acompanhada mediante relatórios periódicos.

Parágrafo único. No caso de procedimentos operados por terceiros, todos os relatórios mencionados nesta política devem ser encaminhados para a CGTI juntamente dos processos de faturamento periódicos ou pelo email cgti.atendimento@pgfn.gov.br .

Seção II
Termos e Definições

Art. 9º Para os fins do disposto nesta Portaria, considera-se:

I - **Plano de Backup:** Conjunto de procedimentos que orienta a realização das cópias de segurança em nível operacional.

II - **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.

III - **Administrador de Backup:** Indivíduo ou estrutura de órgão ou entidade da Administração Pública Federal, direta ou 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. É o responsável pelos procedimentos de configuração, execução e monitoramento de backup e pela realização ou acompanhamento dos testes nos procedimentos de restore.

IV - **Eliminação:** Exclusão de dado ou conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado.

V - **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.

VI - **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.

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.

IX - **Backup full:** backup em que todos os dados são copiados integralmente (cópia de

segurança completa).

X - **Backup incremental:** backup em que somente os arquivos novos ou modificados são copiados.

XI - **Backup diferencial:** backup em que os arquivos novos ou modificados da base de dados incremental são copiados.

XII - **Clientes de backup:** todo equipamento servidor no qual é instalada a ferramenta de backup.

XIII - **Disaster recovery:** estratégia de recuperação de dados motivada por sinistros de grave amplitude física ou lógica.

XIV - **Retenção:** período de tempo em que o conteúdo da mídia de backup deve ser preservado.

XV - **Restore:** restauração dos arquivos de backup.

XVI - **Teste de backup ou teste de integridade:** teste dos arquivos de backup de forma a garantir que não estejam corrompidos.

XVII - **Teste de restore/restauração:** teste do procedimento de restauração visando garantir que os dados de fato possam ser recuperados. Não se confunde com o teste de backup/teste de integridade.

XVIII - **Catálogo de Backup:** banco de dados que contém as informações acerca dos próprios planos de backup.

XIX - **Configurações de Sistemas Operacionais:** consistem nos dados que permitem a reconstrução de uma nova máquina virtual/sistema operacional. Substituem o backup full do próprio sistema operacional.

CAPÍTULO II

DAS DIRETRIZES

Seção I

Diretrizes Gerais

Art. 10. A Política de Backup e Restauração de Dados está alinhada com a Política de Segurança da Informação e Privacidade dos Dados PGFN - PORTARIA PGFN/ME Nº 10880, DE 02 DE SETEMBRO DE 2021.

Art. 11. Todos os sistemas, plataformas, software as a service, filesystems ou outros ambientes que conterem dados da PGFN, incluindo dados fora da organização armazenados em um serviço de nuvem Pública ou Privada, devem possuir um administrador de backup. Tendo como exceção os casos já mencionados no tópico “escopo” desta política.

§ 1º Para o caso de sistemas operados pela PGFN, o administrador de backup será nomeado pela CGTI.

§ 2º Para operadores terceiros, que gerenciam sistemas mediante contrato com a PGFN, os administradores de backup devem ser nomeados em instrumentos internos do terceiro.

Art. 12. Para cada recurso ou grupo de recursos que contenham dados digitais, devem ser estabelecidos planos de backup contendo rotinas para implementar as diretrizes desta política.

Art. 13. As rotinas de backup devem ser orientadas para a restauração dos dados no menor tempo possível, principalmente quando da indisponibilidade de serviços de TI.

Parágrafo Único. No caso de sistemas operados por terceiros, os tempos de restauração devem ser acordados entre as partes e constar em contrato.

Art. 14. As rotinas de backup devem utilizar soluções próprias e especializadas para este fim, preferencialmente de forma automatizada.

Art. 15. 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.

Art. 16. 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.

Parágrafo Único. Caso haja impossibilidade de armazenamento em local distinto deve ser explicitamente informado nos relatórios de backup e enviados para a CGTI.

Art. 17. A infraestrutura de rede de backup, se possível, deve ser apartada, lógica e fisicamente, dos sistemas críticos da organização. Os ambientes físicos devem contar com controle de acesso e mecanismos adequados para armazenamento dos equipamentos e/ou mídias. Os ambientes lógicos devem ser isolados do ambiente com os dados originais com o uso de mecanismos de isolamento adequados (firewall, IPS, etc.).

Parágrafo Único. Caso haja impossibilidade de isolamento das redes deve ser explicitamente informado nos relatórios de backup e enviados para a CGTI.

Art. 18. Manter reserva de recursos (físicos e lógicos) de infraestrutura para realização de teste de restauração de backup.

Art. 19. Em situações em que a confidencialidade é importante, convém que cópias de segurança sejam protegidas através de encriptação.

Parágrafo Único. A necessidade de encriptação deve ser acordada com o gestor de negócio do sistema ou project owner do sistema.

Art. 20. Os backups devem ser retidos por tempo suficiente para atendimento às legislações relacionadas aos requisitos de negócio. O tempo de retenção deve ser estabelecido no procedimento de backup e restore de cada sistema/ambiente, respeitando os tempos mínimos estabelecidos nesta política.

Art. 21. Os backups devem ser operados e monitorados pelos administradores de backup.

Art. 22. Para cada backup realizado com sucesso, deve ser gerado relatório automatizado pela própria ferramenta de backup, confirmando a execução da operação.

Art. 23. Para os backups que apresentarem falhas, os administradores de backup deverão criar relatório de acompanhamento de backup, no qual deverá constar a data, os horários de início e término, os objetos e os clientes de backup, a causa da falha, a ação corretiva adotada e qual parte do backup ficou comprometida. Os relatórios devem ser enviados à CGTI.

Seção II

Responsabilidades

Art. 24. É atribuição dos administradores de backup, nomeados em acordo com o disposto no Art. 11 desta portaria:

I - Criar e manter atualizado os planos de backup para cada serviço sob sua administração.

II - Providenciar a criação e manutenção dos backups.

III - Configurar a ferramenta de backup.

IV - Manter as mídias preservadas, funcionais e seguras.

V - Efetuar testes de backup e auxiliar nos procedimentos de restore.

VI - Verificar diariamente os eventos gerados pela ferramenta de backup, tomando as providências necessárias para remediação de falhas.

VII - Restaurar os backups em caso de necessidade.

VIII - Gerenciar mensagens e logs diários dos backups.

IX - Realizar testes de restore.

X - Validar resultados de restore.

XI - Comunicar aos gestores e responsáveis de negócio os erros e as ocorrências nos backups.

XII - Propor modificações visando o aperfeiçoamento da política de backup.

Seção III

Dos planos de backup

Art. 25. Os planos de backup para cada recurso ou grupo de recursos devem conter, no mínimo:

I - Freqüência e tipo da geração das cópias de segurança, que devem refletir os requisitos de negócio e de criticidade dos dados, obedecendo a frequência mínima estabelecida nesta norma.

II - Procedimentos para geração de cópia de segurança.

III - Procedimentos para execução de testes de restore e frequência de teste.

IV - Responsáveis designados, reduzindo a probabilidade de que etapas ou padrões sejam esquecidos ou executados de maneira distinta da definida.

V - Lista os recursos mínimos para sua execução.

VI - Avaliação dos dados e frequência de backup de acordo com o tipo de dado e o ambiente computacional.

VII - Abrangência dos backups (por exemplo, completa ou diferencial).

VIII - Tempo de retenção.

IX - Criticidade da informação.

X - Necessidade de criptografia dos dados.

Seção IV

Do tipo de backup, frequência e tempo de retenção dos dados

Art. 26. Os critérios mínimos para sistemas não críticos e não sensíveis estão definidos no ANEXO I.

Art. 27. Os backups dos serviços de TI críticos da PGFN devem ser realizados obedecendo os critérios mínimos da tabela acima, podendo ser mais frequente ou com maior retenção a depender dos requisitos de negócio e de criticidade dos dados.

Art. 28. Especificidades dos serviços de TI críticos e dos serviços de TI não críticos podem demandar frequência e tempo de retenção diferenciados.

Art. 29. Os ativos envolvidos no processo de backup são considerados ativos críticos para a organização.

Art. 30. 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.

Seção V

Do uso da rede

Art. 31. O administrador de backup deve considerar o impacto da execução das rotinas de backup sobre o desempenho da rede de dados da PGFN, garantindo que o tráfego necessário às suas

atividades não ocasione indisponibilidade dos demais serviços de TI da organização.

Art. 32. A execução do backup deve concentrar-se, preferencialmente, no período de janela de backup.

Art. 33. 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 PGFN.

Seção VI
Do transporte e armazenamento

Art. 34. 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 tempo de retenção do dado.

III - A probabilidade de necessidade de restauração.

IV - O tempo esperado para restauração.

V - O custo de aquisição da unidade de armazenamento de backup.

VI - A vida útil da unidade de armazenamento de backup.

Art. 35. 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.

Art. 36. 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.

Art. 37. A execução das rotinas de backup deve envolver a previsão de ampliação da capacidade dos dispositivos envolvidos no armazenamento.

Art. 38. No caso de desligamento do usuário (de forma permanente ou temporária), o backup de seus arquivos em nuvem deverá ser mantido por, no mínimo, cinco anos, salvo disposto contrário previsto no plano de backup do ambiente específico. Após esse período, os arquivos poderão ser excluídos a qualquer tempo.

Parágrafo Único. Todos os dados constantes no armazenamento em nuvem do usuário serão considerados como do próprio usuário, não havendo distinção entre dados do usuário e da sua equipe.

Art. 39. 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.

Art. 40. 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.

Seção VII
Dos testes de backup e teste de Restore

Art. 41. Os backups serão verificados periodicamente por sua integridade:

I - Diariamente, os logs de backup serão revisados em busca de erros, durações anormais e em busca de oportunidades para melhorar o desempenho do backup, de forma automatizada ou manual.

II - Ações corretivas serão tomadas quando os problemas de backup forem identificados, a fim

de reduzir os riscos associados a backups com falha.

III - A CGTI manterá registros de backups e testes de restauração para demonstrar conformidade com esta política. Nos casos de backups executados por agentes externos (ex: Serpro e Dataprev), deverão ser fornecidos relatórios de segurança a fim de comprovar a conformidade com esta política.

Art. 42. Os testes de integridade dos arquivos de backup devem ser realizados em todos os backups produzidos independente do ambiente.

Art. 43. Os planos de backup/restore devem estabelecer diretrizes para a execução dos testes de recuperação de dados (Restore) periódicos, incluindo a periodicidade necessária.

Art. 44. Os planos de restore devem considerar a criticidade da informação e que os dados a qualquer tempo possam ser recuperados de forma íntegra.

Art. 45. Os planos devem abordar de forma específica os testes cujo objetivo é checar o funcionamento do próprio processo de backup e restauração dos dados.

Art. 46. Para cada teste de restore realizado com sucesso, deve ser gerado relatório, confirmando a execução da operação e integridade dos dados. Os relatórios devem ser enviados para a CGTI.

Art. 47. Os testes de restauração dos backups devem ser realizados, por amostragem de acordo com a criticidade dos dados, a ser definido em cada plano de backup, 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.

Parágrafo Único. Os testes de integridade dos backups não devem ser confundidos com testes de restore/recuperação. Enquanto o primeiro visa a mera conferência da integridade dos arquivos o segundo visa testar que os arquivos e procedimentos de restauração encontram-se válidos e permitem, ultimamente, que seja feita a restauração da informações.

Art. 48. Verificar se foi atendido os níveis de serviço pactuados, tais como os Recovery Time Objective – RTOs.

Art. 49. Os registros deverão conter, no mínimo, o tipo de sistema/serviço que teve o seu restabelecimento testado, a data da realização do teste, o tempo gasto para o retorno do backup e se o procedimento foi concluído com sucesso

Art. 50. Quaisquer exceções a esta política serão totalmente documentadas e aprovadas pelo Comitê Estratégico de Tecnologia da Informação.

Art. 51. Os planos de backup/restore devem estabelecer os procedimentos para a realização dos testes de mídias.

Art. 52. As cópias de segurança devem ser verificadas quanto à sua integridade logo após a sua geração. Adicionalmente, testes de integridade devem ser realizados periodicamente nessas mídias, por meio de ferramentas apropriadas. O resultado dos testes deve ser registrado e o tempo de vida útil das mídias deverá ser monitorado.

Art. 53. Os recursos computacionais utilizados na geração de cópias de segurança e recuperação de dados devem ser testados periodicamente.

Seção VIII
Procedimento de restauração de backup

Art. 54. O atendimento de solicitações de restauração de arquivos, e-mails e demais formas de dados deverá obedecer às seguintes orientações:

I - A solicitação de restauração de objetos deverá sempre partir do responsável pelo recurso, através de chamado técnico na central de atendimento CGTI.

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

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

IV - Caso a restauração de dados envolva dados de propriedade não exclusiva do solicitante, a restauração deve ser aprovada pelo gestor de negócios ou responsável pelos dados.

V - As demandas de recuperação ou disponibilização de arquivos de backup deverão ser registradas e armazenadas.

VI - A forma e momento de efetiva recuperação dos dados ficará à cargo do administrador de backup e gestor de negócios ou responsável pelos dados.

VII - O administrador 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.

Seção IX
Eliminação de Dados e Descarte de Mídias

Art. 55. A eliminação segura dos dados deve ser realizada por meio de sobrescrita, utilizando-se preferencialmente as ferramentas fornecidas pelos fabricantes das mídias.

Art. 56. O resultado da eliminação dos dados deve ser validado ao final do processo, assegurando que todas as áreas do mídia foram sobrescritas ou que a mídia foi destruída sem possibilidade de futura leitura.

Art. 57. Mídias contendo informações sigilosas devem ser manuseadas e descartadas de forma segura e protegida, preferencialmente com sua destruição física antes do descarte.

CAPÍTULO III
DAS DISPOSIÇÕES FINAIS

Art. 58. Esta política poderá ser revista a qualquer momento a fim de aumentar a segurança da informação no âmbito da PGFN.

Art. 59. Dentro de 180 (cento e oitenta) dias contados da data de vigência desta Portaria, os planos de backup para sistemas gerenciados diretamente pela PGFN devem ser confeccionados.

Art. 60. A partir da data de vigência desta portaria, todos os novos contratos firmados pela PGFN, que envolvam armazenamento de dados digitais, devem referenciar e constar explicitamente a necessidade de atendimento à esta portaria.

Art. 61. Esta portaria entra em vigor no primeiro dia útil do mês subsequente à data de sua publicação.

Documento assinado eletronicamente

ANELIZE LENZI RUAS DE ALMEIDA

Procuradora-Geral da Fazenda Nacional Substituta

ANEXO I

Do tipo de backup, frequência e tempo de retenção dos dados

Tipo de Ambiente	Tipo Backup	Frequência	Retenção
Catálogo de Backup	Full	Semanal	2 semanas
Catálogo de Backup	Incremental/Diferencial	Diário	2 semanas
Banco de Dados	Full	Semanal	1 mês
Banco de Dados	Incremental/Diferencial	Diário	1 mês
Aplicações	Full	Mensal	1 mês
Aplicações	Incremental/Diferencial	Diário	1 semana
Arquivos (filesystem)	Full	Mensal	1 mês
Arquivos (filesystem)	Incremental/Diferencial	Diário	1 semana
Configurações de Sistemas Operacionais	Full	Mensal	1 mês
Configurações de Sistemas Operacionais	Incremental/Diferencial	Diário	1 mês
Máquina virtual completa	Full	Mensal	1 mês
Máquina virtual completa	Incremental/Diferencial	Diário	1 mês

Documento assinado eletronicamente por **Anelize Lenzi Ruas de Almeida**, **Procurador(a)-Geral da Fazenda Nacional Substituto(a)**, em 18/08/2022, às 21:17, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

A autenticidade deste documento pode ser conferida no site https://sei.economia.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **27358187** e o código CRC **C3A171DB**.

Referência: Processo nº 10951.104949/2020-44. SEI nº 27358187