CONTROLADORIA-GERAL DA UNIÃO

MINUTA DE PORTARIA NORMATIVA SE/CGU, DE 14 DE AGOSTO DE 2024

Institui a Política de Gestão de *Backup* de Dados Digitais da Controladoria-Geral da União.

A SECRETÁRIA-EXECUTIVA DA CONTROLADORIA-GERAL DA UNIÃO , no exercício das atribuições previstas no art. 35 do Anexo I do Decreto nº 11.330, de 1º de janeiro de 2023, e no art. 6º, inciso II, da Portaria CGU nº 1.973, de 31 de agosto de 2021, e considerando o disposto no Decreto nº 10.332, de 28 de abril de 2020, na Portaria SE/CGU nº 587, de 10 de março de 2021, e na Instrução Normativa GSI/PR nº 3, de 28 de maio de 2021, bem como com base no Processo Administrativo nº 00190.105052/2024-67, resolve:

CAPÍTULO I

DISPOSIÇÕES PRELIMINARES

Art. 1º Esta Portaria Normativa institui a Política de Gestão de *Backup* de Dados Digitais e estabelece princípios, diretrizes e responsabilidades relacionadas à realização de cópias de segurança e recuperação de dados digitais da Controladoria-Geral da União.

Art. 2º Para os efeitos desta Portaria Normativa, considera-se:

I - administrador de *backup*: pessoa responsável pela implantação de configurações e atendimento avançado de resolução de incidentes e problemas;

II - *archiving*: procedimento de execução única, com armazenamento de dados que não são utilizados diariamente e que geralmente correspondem a dados armazenados em arquivo permanente, tendo, como objetivo principal, armazenar dados por longas retenções para atender conformidades legais ou regulamentos pertinentes às unidades organizacionais;

III - arquivo corrente: conjunto de documentos, em tramitação ou não, que, pelo seu valor primário, é objeto de consultas frequentes pela entidade que o produziu, a quem compete a sua administração;

IV - arquivo intermediário: conjunto de documentos originários de arquivos correntes com uso pouco frequente e que aguarda sua respectiva destinação;

V - arquivo permanente: conjunto de documentos preservados em caráter definitivo em função de seu valor;

VI - *backup*:

a) conjunto de procedimentos, executados em frequência pré-definida, que permitem salvaguardar os dados de um sistema computacional, garantindo guarda, proteção e recuperação em caso de incidentes, sejam eles causados por ataques cibernéticos, erros humanos ou desastres naturais; ou

b) termo de identificação da mídia em que a cópia de salvaguarda é realizada;

VII - cópia *off-line*: cópia de segurança imutável, na qual nem a conta administrativa tem permissão para apagá-la antes do prazo definido;

VIII - custodiante da informação: indivíduo responsável pela unidade gestora que tenha responsabilidade formal sobre as informações;

IX - dados ativos: dados que estão disponíveis para acesso imediato do usuário por meio de sistemas de informação ou arquivos em pastas de rede, de modo que geralmente correspondem a dados armazenados em arquivos corrente ou intermediário;

X - dados inativos: dados guardados em *backup* ou *archiving*, que somente podem ser acessados pelo usuário mediante solicitação de restauração;

XI - dados processados: dados submetidos a qualquer operação ou tratamento, por meio de processamento eletrônico ou automatizado com o emprego de tecnologia da informação;

XII - janela de *backup*: período durante o qual cópias de segurança sob execução agendada ou manual poderão ser executadas;

XIII - mídia: mecanismos em que dados podem ser armazenados, incluindo discos ópticos e magnéticos, CDs, fitas, papel, entre outros;

XIV - operador de *backup*: pessoa responsável por procedimentos de atendimento de primeiro nível, acompanhamento de execução de rotinas de *backup*, realização de restaurações de arquivos de usuários, manutenção de troca de mídias e gerenciamento de estoque de mídias locais;

XV - *recovery point objective* – RPO: ponto no tempo em que os dados dos serviços de tecnologia da informação – 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;

XVI - *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;

XVII - retenção: período durante o qual as informações estarão disponíveis na solução de *backup* para restauração e que, após transcorrido, serão descartadas, sem possibilidade de sua restauração; e

XVIII - serviços de TI: provimento de serviços de desenvolvimento, de implantação, de manutenção, de armazenamento e de recuperação de dados e de operação de sistemas de informação, projeto de infraestrutura de redes de comunicação de dados, modelagem de processos e assessoramento técnico necessários à gestão da informação.

Parágrafo único. Na aplicação desta Portaria Normativa, deverão ser observados, no que couber, os conceitos constantes do Glossário de Segurança da Informação aprovado pela Portaria GSI/PR nº 93, de 18 de outubro de 2021.

Objetivos

Art. 3º São objetivos da Política de Gestão de *Backup* de Dados Digitais:

I - instituir diretrizes, responsabilidades e competências que visam à segurança, proteção e disponibilidade dos dados digitais custodiados pela Diretoria de Tecnologia da Informação e formalmente definidos como de necessária salvaguarda na Controladoria-Geral da União para manter-se a continuidade do negócio;

II - estabelecer mecanismos que permitam a guarda dos dados de *backup* e sua eventual restauração em casos de indisponibilidades ou perdas por erro humano, ataques, catástrofes naturais ou outras ameaças;

III - estabelecer o modo e a periodicidade de *backup* dos dados armazenados pelos sistemas computacionais; e

IV - estabelecer mecanismos de *archiving* que permitam a guarda de dados por longas retenções e sua eventual restauração para atender conformidades legais ou regulamentos pertinentes às unidades organizacionais.

Abrangência

Art. 4º As disposições desta Portaria Normativa e da regulamentação correlata aplicam-se:

I - a todos os dados processados e armazenados no âmbito da Controladoria-Geral da União, incluindo dados da organização armazenados em ambiente de computação em nuvem; e

II - aos agentes públicos que podem ser criadores ou usuários dos dados mencionados no inciso I do *caput*, bem como a terceiros que acessam e usam sistemas e equipamentos de TI na Controladoria-Geral da União ou que criam, processam ou armazenam dados de propriedade da Controladoria-Geral da União.

Art. 5º Não serão salvaguardados nem recuperados:

I - dados armazenados localmente, nas estações de trabalho dos usuários ou em quaisquer outros dispositivos fora dos centros de processamento de dados mantidos pelas unidades de TI, ficando sob a responsabilidade do indivíduo que usa o(s) dispositivo(s);

II - dados relativos a ambientes de desenvolvimento, laboratório e testes; e

III - dados armazenados nas pastas públicas no compartilhamento “CORPORATIVO” do sistema de arquivos da Controladoria-Geral da União.

Exceções

Art. 6º As exceções às definições padrões, referentes à gestão de *backup* dos dados em formato digital, solicitadas por meio de Acordo de Nível de Serviço, deverão ser previamente autorizadas pelo Coordenador-Geral de Infraestrutura Tecnológica da Diretoria de Tecnologia da Informação.

Parágrafo único. A Diretoria de Tecnologia da Informação é a unidade responsável por definir o processo e a guarda dos Acordos de Nível de Serviço.

CAPÍTULO II

DOS PRINCÍPIOS GERAIS

Art. 7º A Política de Gestão de *Backup* de Dados Digitais de que trata esta Portaria Normativa deve estar alinhada à Política de Segurança da Informação da Controladoria-Geral da União.

Art. 8º Devem ser realizadas cópias de segurança das informações essenciais para a Controladoria-Geral da União.

§ 1º O preenchimento de Acordo de Nível de Serviço com definições de *backup* e *archiving* é obrigatório para sistemas críticos.

§ 2º Para sistemas não críticos, a Coordenação-Geral de Infraestrutura Tecnológica da Diretoria de Tecnologia da Informação poderá, a qualquer tempo, avaliar a relevância do sistema

ou serviço e definir a necessidade do preenchimento de Acordo de Nível de Serviço pelo custodiante da informação.

§ 3º Para sistemas que necessitem de Acordo de Nível de Serviço, o custodiante da informação, com apoio da Diretoria de Tecnologia da Informação, definirá quais informações são consideradas essenciais e devem ter cópia de segurança realizada, bem como as definições de *backup* e *archiving* que deverão ser aplicadas.

§ 4º As definições de que trata o § 3º deverão ser armazenadas em repositório definido pela Diretoria de Tecnologia da Informação.

§ 5º A fase de planejamento de novas soluções de TI, ou de alterações em soluções existentes, deve contemplar requisitos de *backup*, *archiving* e restauração.

§ 6º As cópias de segurança e os testes de restauração serão realizados de acordo com a disponibilidade orçamentária ou de recursos, físicos e lógicos, de infraestrutura, com prioridade para sistemas críticos.

Art. 9º O *backup* de sistemas críticos deve atender aos seguintes critérios:

I - possuir, no mínimo, três diferentes cópias do dado, sendo uma delas o dado original;

II - armazenar uma cópia em *datacenter* distinto da infraestrutura do dado original – *off-site*; e

III - possuir uma cópia *off-line*.

§ 1º Para sistemas não críticos, os critérios mencionados no *caput* devem ser adotados de acordo com a disponibilidade orçamentária ou de recursos, físicos e lógicos, de infraestrutura.

§ 2º Para serviços na modalidade de Software como Serviço – SaaS ou Plataforma como Serviço – PaaS, devem ser observadas as melhores práticas recomendadas pelo fabricante.

Art. 10. As rotinas de *backup* devem:

I - utilizar soluções próprias e especializadas para este fim, preferencialmente de forma automatizada; e

II - possuir requisitos mínimos diferenciados de acordo com o tipo de serviço de TI ou dado salvaguardado, dando prioridade aos sistemas de TI críticos da organização.

Art. 11. As mídias físicas que guardam os dados de *backup* serão armazenadas de forma centralizada, em ambiente que proporcione segurança adequada, com controles de acesso e prevenção a incêndios.

Parágrafo único. No caso de necessidade de movimentação das mídias entre ambientes *on-premises* da Controladoria-Geral da União, o transporte deve ser supervisionado por servidor ou colaborador designado pela Diretoria de Tecnologia da Informação.

Art. 12. Nas situações em que a confidencialidade seja necessária, as cópias de segurança devem ser protegidas por meio de encriptação.

CAPÍTULO III

DAS RESPONSABILIDADES

Art. 13. A Coordenação-Geral de Infraestrutura Tecnológica da Diretoria de Tecnologia da

Informação é a unidade responsável pela administração e pelos procedimentos relativos à solução de *backup*, bem como pela guarda e proteção das mídias de *backup*.

Parágrafo único. Como responsável pela solução de *backup*, a Coordenação-Geral de Infraestrutura Tecnológica deve:

I - propor soluções de cópia de segurança das informações digitais corporativas produzidas ou custodiadas pela Controladoria-Geral da União;

II - propor modificações visando ao aperfeiçoamento da Política de Gestão de *Backup* de Dados Digitais, prevista nesta Portaria Normativa;

III - realizar o planejamento das cópias de segurança quando da solicitação de criação de *backup* ou *archiving*;

IV - planejar, bianualmente, os testes de restauração e providenciar, trimestralmente, a sua execução; e

V - identificar a viabilidade de utilização de diferentes tecnologias na realização das cópias de segurança, propondo a melhor solução para cada caso.

Art. 14. O administrador de *backup* e o operador de *backup* devem ser capacitados nas tecnologias, nos procedimentos e nas soluções utilizadas nas rotinas de *backup* e *archiving*.

Art. 15. São responsabilidades relacionadas à administração da solução de *backup*:

I - implantar, configurar e manter a solução de *backup*;

II - criar, testar e manter rotinas de *backup*, de *archiving* e de manutenção;

III - gerar e acompanhar os relatórios relacionados ao funcionamento da solução de *backup*, atuando tempestivamente na correção de falhas e problemas;

IV - executar operações de restauração de *backups* quando necessário;

V - gerenciar as mídias de armazenamentos de *backups*, garantindo a guarda, substituição e descarte seguros;

VI - reportar imediatamente ao setor a que está subordinado os incidentes ou erros que causem indisponibilidade ou impossibilitem a execução ou restauração de *backups*; e

VII - monitorar os recursos de armazenamento de *backup*, de forma a subsidiar as decisões referentes à gestão de capacidade do serviço.

Art. 16. São atribuições dos custodiantes da informação:

I - avaliar a necessidade do preenchimento de Acordo de Nível de Serviço, considerando os requisitos legais e de negócio e a criticidade da informação para a continuidade da operação; e

II - validar negocialmente o resultado das restaurações de dados.

CAPÍTULO IV

DA FREQUÊNCIA E RETENÇÃO DOS DADOS DE *BACKUP*

Art. 17. Os *backups* dos serviços de TI do ambiente de produção da Controladoria-Geral da União devem observar a retenção padrão de quatro meses, resguardados conforme a distribuição das retenções estabelecidas a seguir:

I - diária: trinta dias;

II - semanal: dezessete semanas;

III - mensal: quatro meses; e

IV - anual: não se aplica.

Art. 18. Os backups dos dados armazenados nas pastas “GRUPOS”, no compartilhamento “CORPORATIVO” do sistema de arquivos da CGU, devem observar a retenção padrão de um ano, resguardados conforme a distribuição das retenções estabelecidas a seguir:

I - diária: cento e oitenta dias;

II - semanal: cinquenta e três semanas;

III - mensal: doze meses; e

IV - anual: não se aplica.

Art. 19. O *backup* da solução de centralização de *logs* de segurança deve observar a retenção padrão de dois anos.

Art. 20. Os backups dos serviços de TI que estão no ambiente de homologação e treinamento da Controladoria-Geral da União devem observar a retenção padrão de quatro semanas, resguardados conforme a distribuição das retenções estabelecidas a seguir:

I - diária: quinze dias;

II - semanal: quatro semanas;

III - mensal: não se aplica; e

IV - anual: não se aplica.

Art. 21. As distribuições estabelecidas nos arts. 17, 18 e 20 podem ser alteradas por solicitação do custodiante da informação, sem necessidade da autorização prevista no art. 6º, desde que sejam respeitados os respectivos períodos de retenção padrão.

Art. 22. Os *backups* dos serviços de *OneDrive*, *Sharepoint* e *Teams* devem observar um prazo de retenção mínima de três anos.

Parágrafo único. Em caso de desligamento permanente do usuário, formulários do *Microsoft Forms* que estejam associados a esse perfil e que não foram movidos para um grupo do *Microsoft Teams* terão seus dados mantidos somente por trinta dias, a partir da desativação da conta.

Art. 23. Os *backups* do serviço de correio eletrônico devem observar um prazo de retenção mínima de cinco anos.

Art. 24. O RPO padrão é de vinte e quatro horas.

Art. 25. A execução das rotinas de *backup* deve concentrar-se, preferencialmente, na janela de *backup* a ser definida no seu processo de gestão.

Art. 26. Dados tratados em ambiente de nuvem em *data centers* fora do território nacional devem possuir cópia de segurança atualizada armazenada em *data centers* localizados em território brasileiro, conforme estabelecido pela Portaria SGD/MGI nº 5.950, de 26 de outubro de 2023.

CAPÍTULO V

DAS LONGAS RETENÇÕES DE DADOS DIGITAIS

Art. 27. Dados digitais que necessitam ser armazenados por períodos de longa retenção devem:

I - permanecer como dados ativos, armazenados no respectivo sistema de informação ou arquivo em pasta de rede; ou

II - ser armazenados como dados inativos por meio de *archiving*, em que o custodiante da informação definirá o prazo de retenção.

Parágrafo único. Solicitações de *archiving* serão tratadas conforme art. 6° desta Portaria Normativa.

CAPÍTULO VI

DAS FASES DA GESTÃO DE *BACKUP*

Do planejamento

Art. 28. Para sistemas críticos e demais sistemas ou serviços que a Coordenação-Geral de Infraestrutura Tecnológica da Diretoria de Tecnologia da Informação definiu como relevantes, deve-se realizar solicitação do *backup* ou *archiving* por meio do preenchimento de Acordo de Nível de Serviço pelos custodiantes das informações.

Art. 29. O Acordo de Nível de Serviço de *backup* padrão contemplará os seguintes parâmetros:

I - RPO e prazo de retenção conforme disposto no Capítulo IV; e

II - RTO de setenta e duas horas para sistemas em ambientes de produção.

Parágrafo único. Os ambientes que não são de produção serão restaurados após restauração de sistemas que possuem RTO definido.

Art. 30. O planejamento do *backup* deve ser realizado considerando a arquitetura do sistema de informação e o Acordo de Nível de Serviço.

Parágrafo único. O planejamento deverá produzir como artefato o plano de *backup*.

Art. 31. Solicitações de criação de *backup* identificadas como exceção às definições padrões serão tratadas conforme art. 6° desta Portaria Normativa.

Da configuração

Art. 32. A configuração das rotinas de *backup* será implementada considerando o plano de *backup*.

Parágrafo único. O plano de restauração será elaborado após a configuração do *backup*.

Do monitoramento

Art. 33. As rotinas de *backup* deverão ser monitoradas diariamente.

Parágrafo único. Na detecção de falhas na execução das rotinas, o administrador de *backup* deverá atuar tempestivamente, corrigindo as falhas e os problemas detectados.

Art. 34. O administrador de *backup* deve identificar o momento de realização do descarte dos *backups* ou *archiving*.

Do descarte

Art. 35. Quando da necessidade de descarte de dados de *backup*, tais recursos devem ser logicamente e fisicamente apagados de forma a não permitir a sua recuperação.

Parágrafo único. A inutilização das mídias físicas de *backup* deve ser realizada de forma sustentável e ambientalmente correta.

Da restauração

Art. 36. Em respeito à privacidade e ao sigilo da informação, a solicitação de restauração de dados depende de prévia e formal autorização dos respectivos custodiantes das informações ou de seus superiores hierárquicos.

§ 1º O conteúdo restaurado deve ser disponibilizado apenas ao solicitante da restauração.

§ 2º Excetuam-se do disposto no *caput*:

I - apuração de incidente de segurança cibernética;

II - necessidade da Diretoria de Tecnologia da Informação para restauração da disponibilidade do sistema ou serviço;

III - instrução de procedimentos e processos investigativos e acusatórios correcionais conduzidos pela Corregedoria-Geral da União;

IV - cumprimento de determinação judicial; e

V - compartilhamento de informações solicitadas por órgãos de persecução criminal, civil ou administrativa, para instrução de processos instaurados no órgão ou entidade solicitante.

§ 3º A apuração de incidente de segurança cibernética ficará a cargo da Equipe de Tratamento e Resposta a Incidentes Cibernéticos no âmbito da Controladoria-Geral da União – ETIR-CGU.

Art. 37. A restauração de dados somente será possível nos casos em que estes tenham sido alcançados pelos prazos e requisitos da estratégia de gestão de *backup*.

Dos testes de restauração

Art. 38. As cópias de segurança devem ser verificadas periodicamente, preferencialmente de forma automatizada, com o objetivo de garantir a sua confiabilidade e a integridade dos dados salvaguardados.

Art. 39. Os testes de restauração devem ser realizados trimestralmente, de acordo com o

plano bianual de testes.

§ 1º Os testes devem ser priorizados para os sistemas de TI críticos da organização.

§ 2º O atendimento dos níveis de serviço pactuados deve ser verificado nos testes.

§ 3º Os testes devem ser adequadamente documentados informando, minimamente, o tipo de serviço de TI que teve o seu reestabelecimento testado, a data dos dados de *backup* restaurados, o tempo gasto para o retorno do *backup* e se o procedimento foi concluído com sucesso.

CAPÍTULO VII

DISPOSIÇÕES FINAIS

Art. 40. Os prazos de retenção definidos no Capítulo IV deverão ser praticados a partir da data de publicação desta Portaria Normativa.

Parágrafo único. Os Acordos de Nível de Serviço anteriormente firmados serão mantidos pela Diretoria de Tecnologia da Informação.

Art. 41. A revisão desta Portaria Normativa deve ser realizada a cada dois anos ou sempre que se fizer necessário.

Art. 42. Fica revogada a Norma Operacional DTI/SE/CGU nº 6, de 09 de julho de 2018.

Art. 43. Esta Portaria Normativa entra em vigor na data de sua publicação.

EVELINE MARTINS BRITO

Documento assinado eletronicamente por **EVELINE MARTINS BRITO**, **Secretária-Executiva**, em 15/08/2024, às 20:16, 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://super.cgu.gov.br/conferir informando o código verificador 3323144 e o código CRC 2CAC6534

Referência: Processo nº 00190.105052/2024-67 SEI nº 3323144