



Modelo de Norma de *Backup*



MINISTÉRIO DA
GESTÃO E DA
INOVAÇÃO EM
SERVIÇOS PÚBLICOS

Programa de Privacidade e
Segurança da Informação
PPSI 2.0

Versão 1.0

Brasília, 13 de maio de 2026



MODELO DE NORMA DE BACKUP**MINISTÉRIO DA GESTÃO E DA INOVAÇÃO EM SERVIÇOS PÚBLICOS**

Esther Dweck

Ministra

SECRETARIA DE GOVERNO DIGITAL

Rogério Souza Mascarenhas

Secretário de Governo Digital

DIRETORIA DE PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO

Leonardo Rodrigo Ferreira

Diretor de Privacidade e Segurança da Informação

COORDENAÇÃO-GERAL DE PRIVACIDADE

Marta Juvina de Medeiros

Coordenadora-Geral de Privacidade

COORDENAÇÃO-GERAL DE SEGURANÇA DA INFORMAÇÃO

Loriza Andrade Vaz de Melo

Coordenadora-Geral de Segurança da Informação

EQUIPE TÉCNICA DE ELABORAÇÃO

Adriano de Andrade Moura

Anderson Souza de Araújo

Leonard Keyzo Yamaoka Batista

Raphael Cesar Estevão

Ricardo Borges Almeida

Thainan Cardoso Rezende

EQUIPE DE REVISÃO

Marta Juvina de Medeiros



Histórico de versões

Data	Versão	Descrição	Autor
13/05/2026	1.0	Elaboração do Modelo de Norma de Backup (PPSI 2.0)	Equipe Técnica de Elaboração

Orientações

Esta seção consigna informações básicas para a elaboração da Norma de Backup do órgão ou entidade:

1. este modelo, assim como todos os modelos disponibilizados pela Diretoria de Privacidade e Segurança da Informação (DEPSI) no âmbito do Programa de Privacidade e Segurança da Informação (PPSI) – instituído pela Portaria SGD/MGI nº 9.511, de 28 de outubro de 2025 –, serve como referência para órgãos e entidades do SISP. Seu uso exige análise e adaptação (com inclusão ou exclusão de diretrizes) para atender às particularidades locais, alinhando-se à realidade específica e às boas práticas;
2. o presente documento apoia diretamente a implementação do Controle 11 do *framework* do PPSI 2.0, incluindo diretrizes relacionadas às medidas 11.1, 11.2, 11.3, 11.4 e 11.5;
3. as informações [destacadas em amarelo] neste modelo devem ser substituídas conforme o caso concreto. As [dispostas em vermelho], por sua vez, devem ser removidas. Também devem ser removidas, antes da publicação da norma, a capa, esta página e a página final.

Licença Creative Commons

Esta obra está licenciada sob a Licença *Creative Commons* Atribuição-NãoComercial-SemDerivações 4.0 Internacional¹.

Você está autorizado a copiar e redistribuir o conteúdo deste modelo para uso interno e externo à sua organização, somente para fins não comerciais, desde que (i) o devido crédito seja dado à Secretaria de Governo Digital do Ministério da Gestão e da Inovação em Serviços Públicos (SGD/MGI), e (ii) um *link* para a licença seja fornecido. Além disso, não é permitida a distribuição de obras derivadas, remixadas, transformadas ou desenvolvidas a partir deste modelo ou respectivo *framework*.

¹ Disponível em: <https://creativecommons.org/licenses/by-nc-nd/4.0/legalcode>.



[ATO NORMATIVO Nº XX, DE XX DE XXXXXXXXX DE 20XX)

Dispõe sobre a Norma de *Backup* no âmbito do [órgão ou entidade].

O [representante do órgão ou entidade], no uso da atribuição que lhe confere o [dispositivo legal], e tendo em vista o disposto na Lei nº 13.709, de 14 de agosto de 2018, no Decreto nº 11.856, de 26 de dezembro de 2023, e no Decreto nº 12.572, de 4 de agosto de 2025, resolve:

CAPÍTULO I
DISPOSIÇÕES PRELIMINARES

Art. 1º Fica instituída a Norma de *Backup* do [órgão ou entidade], em complemento à Política de *Backup*.

Art. 2º Esta Norma constitui um dos instrumentos de implementação do Programa de Privacidade e Segurança da Informação (PPSI) disposto na Portaria SGD/MGI nº 9.511, de 28 de outubro de 2025.

[listar outras diretrizes que julgar necessário]

CAPÍTULO II
DOS CONCEITOS E DEFINIÇÕES

Art. 3º Os termos e definições desta Norma observam o disposto na Lei nº 13.709, de 14 de agosto de 2018 (LGPD), e no Glossário de Segurança da Informação do Gabinete de Segurança Institucional da Presidência da República, aprovado pela Portaria GSI/PR nº 93, de 18 de outubro de 2021, além de:

I - *backup* completo: tipo de *backup* que contém a cópia integral de todos os dados definidos no escopo do *backup*;

II - *backup* incremental: tipo de *backup* que contém a cópia apenas dos dados que foram alterados desde a última execução de *backup*, seja ela completa ou incremental;

III - *backup* diferencial: tipo de *backup* que contém a cópia dos dados modificados desde a última execução de *backup* completo;

IV - proprietário do ativo: agente público que assume autoridade e responsabilidade pelas decisões relacionadas à classificação, proteção, uso e ciclo de vida de um ativo ou grupo de ativos de informação;

V - *Recovery Point Objective* (RPO): intervalo máximo admissível de perda de dados, medido em tempo, que a organização está disposta a aceitar em caso de incidente; e

VI - *Recovery Time Objective* (RTO): intervalo máximo admissível para a restauração de um ativo de informação ou serviço após a ocorrência de um incidente.

[acrescentar demais conceitos e definições empregados neste documento]

CAPÍTULO III DA FINALIDADE

Art. 4º Esta Norma tem por finalidade estabelecer os critérios operacionais e requisitos necessários à implementação das diretrizes previstas na Política de *Backup*.

[listar outros objetivos que julgar necessário]

CAPÍTULO IV DOS REQUISITOS GERAIS

Art. 5º Os parâmetros de *backup* devem ser formalizados em um plano de *backup*, utilizando como referência a tabela de critérios disposta no Anexo I.

Parágrafo único. Especificidades técnicas ou operacionais dos ativos de informação podem demandar frequências e tempos de retenção diferenciados, devidamente justificados e formalmente aprovados.

Art. 6º Os parâmetros de *backup* incluem, no mínimo:

I - frequência de execução;

II - tipo de *backup* adotado;

III - tempo de retenção;

IV - objetivos de recuperação (RPO e RTO) definidos nos instrumentos de continuidade de negócios;
e

V - local de armazenamento.

Art. 7º A definição do tipo de *backup* (completo, incremental ou diferencial) deve considerar a eficiência operacional, o volume de dados e os requisitos de recuperação.

Art. 8º A definição da janela de execução das rotinas de *backup* deve considerar os potenciais impactos no desempenho dos ativos de informação, de modo a minimizar a degradação dos serviços e assegurar a continuidade das operações.

Art. 9º Técnicas de compressão de dados podem ser aplicadas na realização do *backup*, desde que sejam considerados o impacto no tempo de restauração e a janela de execução.

[listar outras diretrizes que julgar necessário]

CAPÍTULO V DOS CONTROLES TÉCNICOS E ADMINISTRATIVOS GERAIS

Art. 10. A segregação do ambiente de *backup* deve observar, sempre que possível:

I - separação lógica e, sempre que possível, física, da infraestrutura de produção;

II - restrição de acesso administrativo; e

III - isolamento contra comprometimento do ambiente principal.

Art. 11. Os *backups* devem ser protegidos por mecanismos de controle de acesso e registro de atividades.

Art. 12. As operações de armazenamento, movimentação e descarte de mídias de *backup* devem ser registradas de forma a assegurar rastreabilidade e controle.

Art. 13. Os *backups* de ativos de informação com criticidade [severa] para a organização ou com dados pessoais sensíveis devem ser criptografados.

[listar outras diretrizes que julgar necessário]

CAPÍTULO VI DO ARMAZENAMENTO

Art. 14. Os *backups* de ativos com criticidade [acima de alta] devem possuir cópia armazenada em local adicional, distinto do ambiente principal.

Art. 15. Deve haver ao menos um repositório para armazenamento dos *backups* com mecanismos que assegurem a imutabilidade dos dados.

Art. 16. A aplicação de imutabilidade deve considerar, no mínimo, os ativos de informação com [criticidade alta].

Art. 17. Os mecanismos de imutabilidade podem incluir, entre outros:

I - bloqueio por retenção (*retention lock*);

II - armazenamento WORM (*Write Once Read Many*); e

III - controles equivalentes implementados por solução tecnológica.

Art. 18. A aplicação de imutabilidade deve considerar, no mínimo, os ativos de informação com [criticidade alta].

Art. 19. As unidades e mídias de *backup* devem ser selecionadas considerando as seguintes características:

I - a criticidade dos ativos de informação contemplados pelo *backup*;

II - o tempo de retenção dos dados;

III - os requisitos de confidencialidade, integridade e disponibilidade;

IV - a probabilidade de necessidade de restauração;

V - o tempo estimado para restauração;

VI - o custo de aquisição e manutenção;

VII - as restrições de acesso físico ao local de armazenamento das mídias de *backup*; e

VIII - a vida útil e a confiabilidade das unidades de armazenamento utilizadas.

Art. 20. As mídias de *backup* devem ser claramente identificadas.

Art. 21. Os ativos de informação que suportam o armazenamento dos *backups* devem ser mantidos em locais adequados, com controle de fatores ambientais, tais como temperatura, umidade e poeira, observadas as especificações técnicas dos fabricantes.

[listar outras diretrizes que julgar necessário]

CAPÍTULO VII DO MONITORAMENTO

Art. 22. As rotinas de *backup* devem ser monitoradas continuamente, incluindo verificação de falhas, integridade e desempenho.

Art. 23. A infraestrutura de *backup* deve considerar o crescimento projetado dos dados, de modo a assegurar a continuidade e a eficiência das rotinas.

[listar outras diretrizes que julgar necessário]

CAPÍTULO VIII DA VERIFICAÇÃO

Art. 24. Testes de restauração devem ser executados por amostragem, em equipamentos distintos daqueles utilizados em ambiente de produção, observando-se os recursos humanos e tecnológicos disponíveis.

Art. 25. Os testes de restauração devem confirmar o atendimento aos níveis de serviço pactuados, incluindo o RTO e o RPO, quando aplicável.

Art. 26. Os registros dos testes de restauração devem conter, no mínimo:

I - a identificação do ativo de informação testado;

II - a data de realização do teste;

III - o tempo total gasto para a restauração; e

IV - o resultado obtido, indicando se o procedimento foi concluído com sucesso.

[listar outras diretrizes que julgar necessário]

CAPÍTULO IX DA RESTAURAÇÃO

Art. 27. A restauração de *backup* depende de solicitação formal do proprietário do ativo.

Art. 28. A restauração deve observar os parâmetros de RTO, RPO e criticidade dos ativos.

[listar outras diretrizes que julgar necessário]

CAPÍTULO X DO DESCARTE

Art. 29. Devem ser implementados métodos seguros para descarte das mídias de *backup*, incluindo destruição física ou lógica, conforme aplicável.

§ 1º Antes do descarte, deve ser realizado procedimento formal de verificação e registro da inutilização, por meio de laudo, termo de destruição ou outro documento comprobatório, assegurando a irreversibilidade do processo.

§ 2º Quando aplicável, a destruição lógica (por sobrescrita segura ou “*wipe*”) deve preceder a destruição física, conforme boas práticas de segurança da informação.

§ 3º O descarte de mídias de *backup* deve observar métodos ambientalmente adequados e a legislação vigente sobre descarte sustentável.

[listar outras diretrizes que julgar necessário]

CAPÍTULO XI

DISPOSIÇÕES FINAIS

Art. 30. Esta Norma deve ser revisada e atualizada periodicamente a cada [2 (dois)] anos ou quando eventos ou mudanças significativas assim o exigirem.

Art. 31. O descumprimento das disposições desta Norma sujeitará o infrator às sanções administrativas, disciplinares, contratuais ou legais cabíveis, aplicadas conforme a legislação vigente.

Art. 32. Quaisquer exceções a esta Norma devem ser integralmente documentadas e submetidas à aprovação do [comitê de segurança da informação ou estrutura equivalente], com justificativa técnica e prazo de correção definido.

Art. 33. Esta Norma entra em vigor na data de sua publicação.

[listar outras disposições finais que julgar necessário]

ANEXO I – Modelo de tabela contendo critérios para o plano de *backup***Tabela 1:** critérios para o plano de *backup*

Criticidade do ativo	Frequência mínima	Retenção mínima	RPO máximo	RTO máximo	Armazenamento	Imutabilidade obrigatória
Severa	Semanal completa; Diária incremental	3 anos	4 horas	2 horas	Local + ambiente remoto; Criptografado	Sim
Alta	Mensal completa; Semanal diferencial	2 anos	24 horas	4 horas	Local + ambiente remoto	Sim
Média	Mensal completa	1 ano	1 semana	24 horas	Local apenas	Não
Baixa	Mensal completa	6 meses	1 mês	1 semana	Local apenas	Não



Dúvida?

Entre em contato
conosco

Acesse o site do PPSI 2.0:

[PPSI 2.0 - Governo Digital](#)