Modelo de Política de Backup

PROGRAMA DE PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO (PPSI)

Versão 2.0

Brasília, março de 2023

MODELO DE POLÍTICA DE CONTROLE 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 PROTEÇÃO DE DADOS

Loriza Andrade Vaz de Melo

Coordenadora-Geral de Proteção de Dados

Equipe Técnica de Elaboração

Amaury C. da Silveira Junior

Eder Ferreira de Andrade

Francisco Magno Felix Nobre

Heráclito Ricardo Ferreira Gomes

Ivaldo Jeferson de Santana Castro

Yuri Arcanjo de Carvalho

Ramon Caldas

Guilherme Rufino Junior

Guilherme Mendonça Medeiros

Equipe Revisora

Marcus Paulo Barbosa Vasconcelos

Samuel Barichello Conceição

Sumaid Andrade de Albuquerque

Equipe Técnica de Revisão - Versão 2.0

Julierme Rodrigues da Silva

Leonard Keyzo Yamaoka Batista

Rogério Vinícius Matos Rocha

Histórico de Versões

Data	Versão	Descrição	Autor
30/03/2022	1.0	Modelo de Política de Backup	Equipe Técnica de Elaboração
05/05/2022	1.1	Modelo de Política de Backup	Equipe Técnica de Elaboração
31/03/2023	2.0	Revisão da Política de Backup Atualização para alinhamento com o Guia do Framework de Privacidade e Segurança da Informação, conforme destacado no Anexo II.	Equipe Técnica de Revisão

Sumário

Aviso Preliminar e Agradecimentos

O presente Modelo, especialmente recomendado e dirigido aos órgãos e às entidades da Administração Pública Federal - APF, visa a auxiliar na Elaboração de uma Política de Backup, em atendimento ao previsto no art. 46 da Lei nº 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados Pessoais (LGPD), que determina que a Administração Pública, ao prestar diversos serviços que tratam dados pessoais à sociedade, deve adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito dos dados que estão sob sua custódia. Adicionalmente, a Elaboração de uma Política de Backup visa a atender, além da LGPD, a outros normativos vigentes sobre o tema de privacidade e segurança da informação.

Este documento é de autoria exclusiva da Secretaria de Governo Digital (SGD) do Ministério da Gestão e da Inovação em Serviços Públicos e tem como referência fundamental o Guia do Framework de Privacidade e Segurança da Informação baseado em diversas publicações e documentos técnicos já existentes que são utilizados amplamente por profissionais da área de privacidade e segurança da informação. Destacam-se as publicações do Center for Internet Security (CIS), da International Organization for Standardization (ISO) e do National Institute of Standards and Technology (NIST). Com o objetivo de facilitar a difusão de conhecimentos sobre privacidade e segurança da informação, tais referências, quando escritas em línguas estrangeiras, foram traduzidas para o português pela equipe técnica da Diretoria de Privacidade e Segurança da Informação da Secretaria de Governo Digital.

Nesse cenário, a Secretaria de Governo Digital enfatiza que:

a) não representa, tampouco se manifesta em nome do CIS, da ISO e do NIST e vice-versa;
b) não se manifesta em nome de autoridades de privacidade e segurança da informação;
c) não é coautora das publicações internacionais abordadas;
d) não assume nenhuma responsabilidade administrativa, técnica ou jurídica por usos ou interpretações inadequadas, fragmentados ou parciais do presente modelo; e
e) caso o leitor deseje se certificar de que atende integralmente os requisitos das publicações das instituições mencionadas, deverá consultar diretamente as fontes oficiais de informação ofertadas por elas, que foram listadas na seção “Referência Legal e de Boas Práticas” deste documento.

Finalmente, um agradecimento especial deve ser registrado ao CIS, à ISO, ao NIST e aos profissionais de privacidade e segurança da informação consultados, por suas valiosas contribuições para a comunidade e para elaboração deste documento.

Este Modelo será atualizado frequentemente, de acordo com as novas diretrizes determinadas pelas autoridades em privacidade e segurança da informação ou segundo eventuais alterações que ocorram nos normativos vigentes relacionados a privacidade e segurança da informação e outras referências utilizadas neste documento.

Introdução

Este Guia tem por finalidade apresentar orientações com o intuito de auxiliar os órgãos e entidades da Administração Pública Federal, direta, autárquica e fundacional a elaborar sua Política de Backup no âmbito institucional.

O Controle 11 do Guia do Framework de Privacidade e Segurança da Informação (p. 49) estabelece que:

Controle 11: Recuperação de Dados – *Criar e manter práticas de recuperação de dados que sejam capazes de restaurar os ativos da organização para um estado pré-incidente ou o estado mais confiável possível.*

O presente documento serve como um modelo prático a ser utilizado para auxiliar na adoção do Controle 11 do Guia do Framework de Privacidade e Segurança da Informação[1] v1 e respectivas evoluções desta versão (1.1, 1.2 etc.) elaborado e publicado pela SGD. As medidas do Controle 11 que estão contempladas por este modelo são: 11.1, 11.2, 11.3, 11.4 e 11.5.

Hoje, mais do que em qualquer outro momento da história, o Governo utiliza a tecnologia para melhorar e expandir a oferta de serviços públicos para o cidadão apoiado em sistemas informatizados.

Nesse contexto, os órgãos federais, com infraestrutura própria ou contratada de terceiros, coletam, recebem, acessam, processam, modificam, produzem, extraem, validam, armazenam, distribuem e transmitem informações confidenciais e públicas para apoiar a entrega de produtos e serviços essenciais (por exemplo, fornecimento de serviços financeiros; fornecimento de serviços de emissões guias, certificados e carteiras; processamento de autorizações de segurança ou dados de saúde; fornecimento de serviços em nuvem; desenvolvendo comunicações via cabo, wireless e/ou satélites; sistemas militares de defesa). As informações federais são frequentemente fornecidas ou compartilhadas, obedecidos os requisitos legais, com entidades como governos estaduais e municipais, empresas públicas e privadas, faculdades e universidades, organizações de pesquisa independentes ou públicas e organizações do terceiro setor.

A proteção dessas informações pelo Governo enquanto agente de tratamento está designada no **art. 46 da Lei Geral de Proteção de Dados**, sancionada em 14 de agosto de 2018:

> *"Art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito."*

Importante ressaltar que adoção deste modelo não dispensa o órgão de considerar as diretrizes gerais estabelecidas para implementação da Política de Segurança da Informação, conforme prevê o art.12, Inciso IV da Instrução Normativa Nº 01/GSI/PR, bem como os Capítulos III e IV da Instrução Normativa Nº 03/GSI/PR, de 28 de maio de 2021, a qual dispõe sobre os processos relacionados à gestão de segurança da informação nos órgãos e nas entidades da administração pública federal.

[1] < https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/ppsi/guia_framework_psi.pdf >. Acesso em 03/02/2023.

Política de Backup e Restauração de Dados Digitais

IMPORTANTE: Este modelo de Política de Backup e Restauração de Dados Digitais deve ser utilizado exclusivamente como referência, devendo o órgão ou entidade considerar as particularidades técnicas específicas do seu ambiente, bem como observar a boa aderência aos processos internos, a fim de construir uma política que seja adequada a sua realidade.

Para usar este modelo, basta substituir o texto em cinza por informações personalizadas do seu órgão ou entidade. Quando estiver concluído, exclua todos os textos introdutórios ou de exemplo e converta todo o texto restante em preto antes do processo de aprovação.

Responsável	Nome da pessoa ou área responsável pela gestão desta política.
Aprovado por:	Nome da pessoa ou área responsável pela aprovação e autorização da implementação desta política.
Políticas Relacionadas	Relacione outras políticas corporativas relacionadas dentro ou externas a este modelo, por exemplo, Política de Gestão de Riscos \ Política de Retenção de Dados \ POSIN
Localização de armazenamento	Descreva a localização física ou digital das cópias desta política.
Data da Aprovação	Liste a data em que essa política entrou em vigor.
Data de revisão	Liste a data em que esta política deve passar por revisão e atualização.

Propósito [Objetivo da Política] conforme IN01 GSI/PR art.11

Levando em consideração natureza e a finalidade do órgão ou da entidade, descreva os fatores ou circunstâncias que determinam a existência da política de Backup. Além disso, afirmam os objetivos básicos da política e o que ela pretende alcançar.

Exemplo: 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 pela(s) [unidades de tecnologia da informação (TI)] e formalmente definidos como de necessária salvaguarda na [Organização], 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. 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.

Escopo [Amplitude, alcance da Política] conforme IN01 GSI/PR art.12 item I

Defina a quem e a quais sistemas esta política se aplica. Liste os agentes públicos e colaboradores necessários para cumprir ou simplesmente indique "todos" se todos devem cumprir. Também indique quaisquer exclusões ou exceções que estejam fora de escopo, ou seja, essas pessoas, elementos ou situações que não estejam cobertas por esta política ou onde uma consideração especial possa ser feita.

- Esta política se aplica a todos os dados no âmbito da [organização], incluindo dados fora da [organização] armazenados em um serviço de nuvem Pública ou Privada. “Dados críticos”, neste contexto, incluem [citar os dados considerados críticos para organização, ex.: e-mail, arquivos pessoais e compartilhados, bancos de dados e conteúdo da web específicos e sistemas operacionais]. A definição de dados críticos e o escopo desta política de backup serão revisados [informar a periodicidade, ex.: anualmente].
- Os serviços de TI críticos da [organização] devem ser formalmente elencados pelo [citar o responsável pela definição, ex.: Comitê de Gestão de Tecnologia da Informação da organização].

- Já ficam previamente estabelecidos os [citar tipo ou nome dos processos ou sistemas críticos], como serviços críticos da [organização].
- 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 ou armazenam dados de propriedade da [organização].
- 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).
- A salvaguarda dos dados em formato digital pertencentes a serviços de TI da [organização] 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.

Termos e Definições [Glossário] conforme IN01 GSI/PR art.12 item II

Defina quaisquer termos-chave, siglas ou conceitos que serão utilizados na política. [Sugere-se utilizar como referência as definições apresentadas na PORTARIA GSI/PR Nº 93, DE 18 DE OUTUBRO DE 2021 – Glossário de Segurança da Informação do Gabinete de Segurança Institucional da PRESIDÊNCIA DA REPÚBLICA].

Exemplo:

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;

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;

ELIMINAÇÃO - Exclusão de dado ou conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado;

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;

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;

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;

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;

Referência legal e de boas práticas [Documentos norteadores]

Se for aplicável, liste quaisquer leis, regulamentos ou guias de boas práticas que regem a política ou com as quais a política deve estar em conformidade ou ser cumprida. Confirme com a consultoria jurídica que a lista é completa e precisa.

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

Declarações da política [Regras aplicáveis ao caso específico]

Descreva as regras que compõem a política. Isso normalmente toma a forma de uma série de breves declarações prescritivas e proscritivas. A subdivisão desta seção em subseções pode ser necessária dependendo do comprimento ou complexidade da política.

Dos princípios gerais

1. A Política de Backup e Restauração de Dados deve estar alinhada com à Política de Segurança da Informação da [organização].
2. A Política de Backup e Restauração de Dados deve estar alinhada com uma gestão de continuidade de negócios em nível organizacional.
3. As rotinas de backup devem ser orientadas para a restauração dos dados no menor tempo possível, principalmente quando da indisponibilidade de serviços de TI.
4. As rotinas de backup devem utilizar soluções próprias e especializadas para este fim, preferencialmente de forma automatizada.
5. 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.
6. 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.
7. A infraestrutura de rede de backup deve ser apartada, lógica e fisicamente, dos sistemas críticos da organização.
8. Manter reserva de recursos (físicos e lógicos) de infraestrutura para realização de teste de restauração de backup.
9. Em situações em que a confidencialidade é importante, convém que cópias de segurança sejam protegidas através de encriptação.

Da frequência e retenção dos dados

10. Os backups dos serviços de TI críticos da [organização] devem ser realizados utilizando-se as seguintes frequências temporais:

    Exemplo:

    I – Diária;

    II – Semanal;

    III – Mensal;

    IV – Anual.

11. Os serviços de TI críticos da [organização] devem ser resguardados sob um padrão mínimo, o qual deve observar a correlação frequência/retenção de dados estabelecida a seguir:

    Exemplo:

    I – Diária: 2 meses;

    II – Semanal: 4 meses;

    III – Mensal: 1 ano;

    IV – Anual: 5 anos.

12. Os serviços de TI NÃO críticos da [organização] devem ser resguardados sob um padrão mínimo, o qual deve observar a correlação frequência/retenção de dados estabelecida a seguir:

Exemplo:

I – Diária: 1 meses;

II – Semanal: 2 meses;

III – Mensal: 6 meses;

IV – Anual: 2 anos.

13. Especificidades dos serviços de TI críticos e dos serviços de TI não críticos podem demandar frequência e tempo de retenção diferenciados.
14. Os ativos envolvidos no processo de backup são considerados ativos críticos para a organização.
15. A solicitação de salvaguarda dos dados referentes aos serviços de TI críticos e aos serviços de TI não críticos deve ser realizada [pelo(s) responsável(s)], com a anuência prévia e formal [do(s) responsável(s)], 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:

    I – Escopo (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.
16. A alteração das frequências e tempos de retenção definidos nesta seção deve ser precedida de solicitação e justificativa formais encaminhadas ao [responsável(s) pelo Backup]. A aprovação para execução da alteração depende da anuência do [responsável(s)].
17. 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.

Tipo de backup

I – Completo (*full*);

II – Incremental;

III – Diferencial.

Exemplo:

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

18. Backup incremental diário (segunda a sábado), armazenado no local.
19. 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.

Do uso da rede

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

21. A execução do backup deve concentrar-se, preferencialmente, no período de janela de backup.
22. 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 [organização].

Do transporte e armazenamento

23. 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.

24. 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.
25. 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.
26. A execução das rotinas de backup deve envolver a previsão de ampliação da capacidade dos dispositivos envolvidos no armazenamento.
27. No caso de desligamento do usuário (de forma permanente ou temporária), o backup de seus arquivos em nuvem deverá ser mantido por, no mínimo, [informar período, ex.: 30 dias]. Após esse período os arquivos poderão ser excluídos a qualquer tempo.
28. 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.
29. 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.

Exemplo: As fitas de backup serão transportadas e armazenadas conforme descrito neste documento:

- Todos os backups serão gravados para reutilizar [Mídia] com capacidade de [XX tb] e uma taxa de transferência de [XX MB/seg] (nativo).
- A mídia será claramente identificada e armazenada em uma área segura acessível apenas para [pessoa(s) autorizada(s)] ou o [fornecedor de armazenamento seguro de mídia externo contratado] usado pelo [organização].
- A mídia não será deixada sem supervisão durante o transporte.
- Backups completos diários serão mantidos por [informar período, ex.:1 semana] e armazenado no local em um cofre à prova de água ou fogo fisicamente protegido, localizado em uma sala fora do data center.
- Backups completos semanais serão mantidos por um período de [informar período, ex.: 3 semanas], e enviado a um local de armazenamento de mídia externo fisicamente protegido. Depois de [informar período, ex.: 3 semanas], as fitas serão devolvidas à TI e serão reutilizadas ou destruídas.

- Backups completos mensais dos dados arquivados serão mantidos por [informar período, ex.: 1 ano]. Depois deste período, as fitas serão devolvidas à TI e serão reutilizadas ou destruídas.
- Backups completos anuais dos dados arquivados serão mantidos por [informar período, ex.: 7 anos]. Após esse período, as fitas serão devolvidas ao TI e serão reutilizadas ou destruídas.

Dos testes de backup

30. Os backups serão verificados periodicamente:
    - [Informar período, ex.: Diariamente], os logs de backup serão revisados em busca de erros, durações anormais e em busca de oportunidades para melhorar o desempenho do backup.
    - Ações corretivas serão tomadas quando os problemas de backup forem identificados, a fim de reduzir os riscos associados a backups com falha.
    - A TI manterá registros de backups e testes de restauração para demonstrar conformidade com esta política.
    - Os testes devem ser realizados em todos os backups produzidos independente do ambiente.
31. Os testes de restauração dos backups devem ser realizados, por amostragem [informar período, ex.: uma vez por semana], 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.
32. Verificar se foi atendido os níveis de serviço pactuados, tais como os Recovery Time Objective – RTOs.
33. 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
34. Quaisquer exceções a esta política serão totalmente documentadas e aprovadas por [comitê responsável].

Procedimento de restauração de backup

35. 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 [Exemplo: 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.
36. O cronograma de restauração de dados:
    a. O tempo de restauração, preferencialmente definido em Acordo de Nível de Serviço entre as áreas de negócio e de TIC, é proporcional ao volume de dados necessários para o restore. A cada [XXGB] de dados, o tempo de restauração é de [informar o tempo ex: uma hora]. Esta estimativa é do tempo

de atendimento da [Informar a Equipe responsável], não contemplando o tempo antes ou após o pedido a equipe.

b. Backups externos serão disponibilizados em aproximadamente [X 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 [X horas] de uma falha não catastrófica do sistema, observando a prioridade para restauração de acordo com a criticidade de cada um.

37. [Acrescentar as diretrizes para restauração de dados].

Do Descarte da Mídia

38. 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.

c. [Acrescentar as diretrizes para descarte da mídia].

Das Responsabilidades

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

Exemplo:

Listar os responsáveis e suas atribuições no processo:

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;

Procedimentos Relevantes

Considere criar documentos de procedimento formal que reforcem e apoiem as declarações políticas acima. Note que é uma prática recomendada abrigar políticas e procedimentos em documentos separados para manter o conteúdo focado e reduzir o número de vezes que a política deve ser reaprovada pela alta administração.

Não conformidade

Descrever claramente as consequências (legais e/ou disciplinares) para o não cumprimento da política pelos agentes públicos ou terceiros. Pode ser pertinente descrever o processo de escalonamento para repetida não conformidade.

Em caso de violação desta política poderão ser aplicadas sanções previstas na Lei 8.112/1990 e outras legislações cabíveis.

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

Exemplo:

1. Processo Administrativo Disciplinar de acordo com a legislação aplicável

2. Exoneração.
3. Ação judicial de acordo com as leis aplicáveis e acordos contratuais.
4. Rescisão contratual ao bem do serviço público.

Concordância

Inclua uma seção que confirme o entendimento e o acordo para cumprir a política. Assinaturas e datas são necessárias. Uma declaração de amostra é fornecida abaixo.

Eu li e entendi a Política de Backup e Restauração de Dados Digitais do [órgão/empresa/fundação]. 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 da [órgão/empresa/fundação].

_____
Nome do Servidor/Empregado

_____
Assinatura do funcionário Data

ANEXO I

Mudanças da Versão 2.0

Este anexo tem a finalidade de fornecer os destaques das mudanças inseridas nesta versão do Modelo de Política de Backup.

Primeiramente, ressalta-se que as mudanças inseridas nesta versão em comparação com a anterior visam a adequação com o Guia do Framework de Privacidade e Segurança da Informação v1 elaborado e publicado pela SGD em novembro de 2022.

Foram realizadas inclusões de: seção sobre aviso preliminar e agradecimentos; referência de que controle e medidas do Framework de Privacidade e Segurança da Informação são atendidos pelo Modelo de Política de Backup; e atualização da seção “Referência legal e de boas práticas”. Foram realizadas modificações, inclusões e exclusões de textos para melhor coesão textual.