Boletim Eletrônico em 09/11/2022

00094.002189/2022-97

PRESIDÊNCIA DA REPÚBLICA

COMITÊ DE GOVERNANÇA DIGITAL E SEGURANÇA DA INFORMAÇÃO

# RESOLUÇÃO Nº 36, DE 07 DE NOVEMBRO DE 2022

Institui a Política de *Backup* e Recuperação de Dados da Presid

**O COMITÊ DE GOVERNANÇA DIGITAL E SEGURANÇA DA INFORMAÇÃO DA PRESIDÊNCIA DA REPÚBLICA**, no uso das atribuições que lhe confere o inciso I do art. 2º do Decreto nº 10.433 de 21 de julho de 2020, e **considerando**:

a) o disposto na Resolução nº 4 do Comitê de Governança Digital e Segurança da Informação da Presidência da República, de 5 de junho de 2020, que institui a Política de Segurança da Informação em Meios Tecnológicos da Presidência da República;

b) a Instrução Normativa GSI/PR nº 1, de 27 de maio de 2020, do Gabinete de Segurança Institucional da Presidência da República, que dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da Administração Pública Federal;

c) a Instrução Normativa GSI/PR nº 3, de 28 de maio de 2021, que dispõe sobre os processos relacionados à gestão de segurança da informação nos órgãos e nas entidades da Administração Pública Federal; e

d) a recomendação do Tribunal de Contas da União contida no Acórdão 1.109/2021, item 9.1, ao Gabinete de Segurança Institucional da Presidência da República, que edite normativos para orientar e regulamentar a obrigatoriedade de que as entidades e órgãos públicos aprovem formalmente e mantenham atualizadas políticas gerais e planos específicos de *backup*.

**RESOLVE**:

Art. 1º Instituir a **Política de Backup e Recuperação de Dados da Presidência da República**.

## CAPÍTULO I

## DAS DISPOSIÇÕES PRELIMINARES

Art. 2º A **Política de Backup e Recuperação de Dados da Presidência da República**, vinculada à Política de Segurança da Informação da Presidência da República, objetiva estabelecer os princípios, as diretrizes, as competências e responsabilidades, os procedimentos e os mecanismos que visam à salvaguarda dos dados de propriedade ou custodiados pelos órgãos da Presidência da República e pela Vice-Presidência da República.

Art. 3º Esta política abrange a salvaguarda e recuperação dos dados dos órgãos da Presidência da República e da Vice-Presidência da República, custodiados pela Diretoria de Tecnologia da Secretaria Especial de Administração da Secretaria-Geral da Presidência da República ou por terceiros.

§1º Não serão salvaguardados nem recuperados dados em formato digital armazenados localmente nas estações dos usuários, ou em quaisquer outros dispositivos fora do Centro de Dados da Presidência da República mantido pela Diretoria de Tecnologia.

§2º A salvaguarda dos dados em formato digital pertencentes aos órgãos da Presidência da República e à Vice-Presidência da República, 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, conforme os requisitos estabelecidos nesta Política, bem como na Resolução nº 24, de 10 de junho de 2022, que estabelece as diretrizes e os procedimentos para o uso seguro de computação em nuvem no âmbito da Presidência da República e da Vice-Presidência da República, na Instrução Normativa nº 5, de 30 de agosto de 2021, do Gabinete de Segurança Institucional da Presidência da República, e demais legislações vigentes que tratem sobre o tema.

## CAPÍTULO II

## DOS CONCEITOS E DEFINIÇÕES

Art. 4º Para fins desta Resolução, consideram-se os conceitos a seguir, adicionalmente aos constantes do Glossário de Segurança da Informação do Gabinete de Segurança Institucional e na Política de Segurança da Informação em Meios Tecnológicos da Presidência da República.

I - Administrador de **Backup**: unidade ou agente responsável pelo planejamento, definição de padrões e procedimentos de configuração, execução, monitoramento e testes de **backup** e restauração de dados;

II - Ativo Crítico: ativos de informação que possuem elevada importância para a continuidade das atividades e serviços e concretização dos objetivos institucionais;

III - **Backup** Completo: modalidade de backup em que todos os dados são copiados integralmente, independentemente de terem sido ou não alterados desde o último backup;

IV - **Backup** Incremental: modalidade de **backup** em que são salvaguardados apenas os dados novos ou modificados desde o último b**ackup**;

V - Gestor da Informação: agente público, proprietário ou custodiante da informação, responsável pela administração das informações tratadas em seu processo de trabalho;

VI - Janela de **Backup**: período de tempo durante o qual cópias de segurança sob execução agendada ou manual poderão ser executadas;

VII - Restauração: processo de recuperação e disponibilização de dados salvaguardados em determinada imagem de **backup**;

VIII - Retenção: período de tempo pelo qual os dados devem ser salvaguardados e estar aptos à restauração;

IX - Ponto de Recuperação Objetivo (RPO - **Recovery Point Objective**): ponto para o qual a informação usada por uma atividade é restaurada para permitir que a atividade de operação seja retomada. Também pode ser referido como "perda máxima de dados";

X - Tempo de Recuperação Objetivo (RTO - **Recovery Time Objective**): período de tempo após um incidente dentro do qual um produto e serviço ou uma atividade é retomada, ou os recursos estão recuperados. Para produtos, serviços e atividades, o RTO é menor do que o tempo que levaria para os impactos adversos que surgiriam como resultado do não fornecimento de um produto/serviço ou realização de uma atividade tornar-se inaceitável;

XI - Rotina de **Backup**: procedimento utilizado para se realizar um **backup**; e

XII - Unidade de Armazenamento: local para armazenamento de dados.

## CAPÍTULO III

## DOS PRINCÍPIOS, DIRETRIZES E OBJETIVOS

Art. 5º A **Política de Backup e Recuperação de Dados da Presidência da República** tem como princípios:

I - observância das diretrizes previstas na Política de Segurança da Informação da Presidência da República, bem como da legislação vigente sobre o tema;

II - garantia da disponibilidade e integridade das informações institucionais;

III - alinhamento às estratégias de gestão de continuidade de negócios e de gestão de riscos em segurança da informação, em nível organizacional; e

IV - foco na continuidade dos ativos críticos da organização.

Art. 6º Os procedimentos de *backup* e recuperação de dados deverão observar as seguintes diretrizes:

I - ser periódicos e orientados para a restauração dos dados no menor tempo possível;

II - utilizar soluções especializadas para este fim, preferencialmente de forma automatizada;

III - realizar verificação periódica de integridade dos dados armazenados;

IV - possuir requisitos mínimos diferenciados de acordo com o tipo do ativo de informação e sua criticidade quanto ao nível de disponibilidade requerido;

V - observar os requisitos de controle de acesso estabelecidos na Política de Controle de Acesso da Presidência da República e da Vice-Presidência da República; e

VI - buscar a melhoria contínua de acordo com as melhores práticas vigentes.

Art. 7º São os objetivos da **Política de Backup e Recuperação de Dados da Presidência da República**:

I - garantir a continuidade das atividades críticas da organização;

II - minimizar os riscos de perdas e danos em caso de desastre;

III - viabilizar a recuperação dos dados institucionais;

IV - definir regras, procedimentos e periodicidade para salvaguarda, tratamento e recuperação dos dados institucionais; e

V - definir os requisitos específicos de segurança de informação para as cópias de segurança realizadas.

## CAPÍTULO IV

## DOS PADRÕES OPERACIONAIS

### Seção I

### Das Regras Gerais

Art. 8º O procedimento de *backup* deve ser utilizado somente para a recuperação de desastres, perda de dados originais por apagamentos acidentais ou corrupção de dados, não podendo ser utilizado como uma estratégia de guarda ou preservação de longo prazo.

Art. 9º Os arquivos de dados armazenados nas estações de trabalho são de responsabilidade exclusiva do usuário, sendo o mesmo responsável por realizar o seu *backup*.

Art. 10. A inclusão de um ativo no processo de *backup* será realizada por meio de solicitação de salvaguarda das informações enviada pelos responsáveis técnicos do serviço, com a anuência prévia e formal dos gestores das informações, considerando:

I - os requisitos de negócio da organização;

II - os requisitos de segurança da informação envolvidos;

III - a criticidade da informação para a continuidade da operação da organização; e

IV - o impacto da perda da informação para a organização.

Art. 11. As solicitações de que trata o art. 10 devem explicitar, no mínimo, os seguintes requisitos técnicos:

I - escopo (dados digitais a serem salvaguardados);

II - tipo de *backup* (completo, incremental);

III - frequência temporal de realização do *backup*;

IV - retenção;

V - RPO; e

VI - RTO.

Parágrafo único. As solicitações de salvaguarda deverão ser alteradas sempre que houver mudança de escopo, frequências ou tempos de retenção, devendo ser enviada pelos responsáveis técnicos do serviço, com a anuência prévia e formal dos gestores das informações.

Art. 12. Poderá ser solicitada salvaguarda de dados para os seguintes tipos de ativos de informação:

I - arquivos de configurações de sistemas operacionais e aplicativos instalados em servidores;

II - arquivos de *log* dos aplicativos, inclusive *log* da ferramenta de *backup* e restauração;

III - informações e configurações de banco de dados;

IV - conteúdo de repositórios de dados associados a sistemas; e

V - arquivos institucionais.

Art. 13. Quaisquer procedimentos programados nos equipamentos “servidores” ou em quaisquer dispositivos de armazenamento dos órgãos da Presidência da República e da Vice-Presidência da República, e que impliquem riscos de funcionamento, somente deverão ser executados após a realização do *backup* dos seus dados.

Art. 14. Em situações em que a confidencialidade do ativo de informação for importante, as cópias de segurança deverão ser protegidas através de encriptação, por solicitação do responsável técnico pelo serviço ou do gestor da informação.

Art. 15. Os locais de gravação dos *backups* deverão possuir identificação suficiente para permitir, direta ou indiretamente, a localização e extração dos dados neles armazenadas.

Seção II

Da Infraestrutura de *Backup*

Art. 16. A infraestrutura de *backup* deve ser apartada, lógica e fisicamente, dos sistemas críticos da organização.

Art. 17. O administrador de *backup* deverá manter reserva de recursos, físicos e lógicos, de infraestrutura para a realização de teste de restauração de *backup*.

Parágrafo Único. Os testes de restauração poderão ser feitos por amostragem, quando não houver infraestrutura suficiente para realizar restaurações completas.

Art. 18. Os ativos envolvidos no processo de *backup* são considerados ativos críticos para a organização.

Seção III

Da Frequência e Retenção de Dados

Art. 19. Os procedimentos de *backup* serão realizados utilizando-se as seguintes frequências temporais:

I - Diário;

II - Semanal;

III - Mensal; e

IV - Anual.

Art. 20. Para os serviços considerados críticos, as solicitações de que trata o art. 10 devem observar a correlação frequência/retenção de dados estabelecida a seguir:

I - Diário: até 30 dias;

II - Semanal: até 12 semanas;

III - Mensal: até 12 meses; e

IV - Anual: até 5 anos.

Art. 21. Para os demais serviços, procedimentos de *backup* deverão observar a correlação frequência/retenção de dados estabelecida a seguir:

I - Diária: até 7 dias;

II - Semanal: até 4 semanas;

III - Mensal: até 6 meses; e

IV - Anual: até 1 ano.

Art. 22. Expirado o prazo de retenção os *backups* serão eliminados.

§1º Especificidades dos serviços críticos ou em casos especiais, justificados, podem demandar frequência e tempo de retenção diferenciados.

§2º Expirado o prazo de retenção dos dados armazenados, os mesmos serão apagados.

§3º A execução de quaisquer procedimentos que impliquem riscos de funcionamento nos serviços ou sistemas deverá ser precedida da realização de *backup*.

Seção IV

Do Uso da Rede

Art. 23. O Administrador de *backup* deve considerar o impacto da execução de suas rotinas sobre o desempenho da rede de dados, garantindo que o tráfego necessário as suas atividades não ocasione indisponibilidade dos demais serviços.

Art. 24. A execução do *backup* deve concentrar-se, preferencialmente, no período de janela de *backup*, determinado pelo Administrador de *backup* em conjunto com a área técnica responsável pela administração da rede de dados.

Seção V

Do Transporte e Armazenamento

Art. 25. As unidades de armazenamento devem ser acondicionadas em locais apropriados, com controle de fatores ambientais sensíveis, como umidade e temperatura, e com acesso (físico e lógico) restrito a pessoas autorizadas pelo Administrador de *backup* e/ou pelo Gestor da informação.

Art. 26. As unidades de armazenamento utilizadas na salvaguarda dos dados devem considerar as seguintes características dos dados resguardados:

I - a criticidade do dado;

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*; e

VI - a vida útil da unidade de armazenamento de *backup*.

Art. 27. 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. 28. Podem ser utilizadas técnicas de compressão de dados, contanto que o acréscimo no tempo de recuperação dos dados seja considerado aceitável pelos gestores das informações.

Art. 29. Quando da necessidade de descarte de unidades de armazenamento de *backups*, tais recursos devem ser lógica e fisicamente destruídos de modo seguro, de forma a impossibilitar a recuperação dos dados, atentando-se ao descarte sustentável e ambientalmente correto.

Seção VI

Dos Testes de *Backup*

Art. 30. Os *backups* devem ser testados periodicamente, com o objetivo de garantir a sua confiabilidade e a integridade dos dados salvaguardados, bem como verificar o atendimento dos níveis de serviços pactuados.

Art. 31. Os testes devem ser realizados em todos os *backups* produzidos independente do ambiente.

Art. 32. Os testes de restauração dos *backups* devem ser realizados em equipamentos servidores diferentes dos equipamentos que atendem os ambientes de produção, observados os recursos humanos e tecnológicos disponíveis.

Art. 33. A periodicidade, os procedimentos e as rotinas inerentes aos testes de *backup* serão definidos pela Diretoria de Tecnologia da Secretaria Especial de Administração, em conjunto com os gestores das informações, conforme a criticidade do ativo.

Art. 34. A Diretoria de Tecnologia da Secretaria Especial de Administração manterá registros de *backups* e testes de restauração para assegurar a conformidade com esta política.

Parágrafo único. Os registros deverão conter, no mínimo, o tipo de 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.

Seção VI

Dos Procedimentos de Restauração de *Backups*

Art. 35. A recuperação de *backups* deverá obedecer às seguintes orientações:

I - as solicitações de restauração de sistemas/arquivos deverão ser abertas formalmente, com autorização do gestor da informação; e

II - A restauração de objetos somente será possível nos casos em que estes tenham sido atingidos pela estratégia de *backup*.

Art. 36. A recuperação de dados não será viabilizada em caso de perdas anteriores à conclusão da cópia de segurança.

CAPÍTULO V

DAS COMPETÊNCIAS E RESPONSABILIDADES

Art. 37. A Diretoria de Tecnologia da Secretaria Especial de Administração será o Administrador de *backup*, ficando responsável por definir os procedimentos e as orientações complementares necessárias à aplicação das disposições estabelecidas nesta política.

Art. 38. São atribuições do Administrador de *backup*:

I - propor soluções de cópia de segurança das informações corporativas produzidas ou custodiadas pelos órgãos da Presidência da República e pela Vice-Presidência da República;

II - definir, em conjunto com os gestores de informação, os requisitos mínimos para os procedimentos de *backup* e recuperação de dados de cada ativo de informação, de acordo com o seu tipo e sua criticidade;

III - providenciar a criação e a manutenção dos *backups*;

IV - manter as soluções de *backup*;

V - manter as unidades de armazenamento de *backups* preservadas, funcionais e seguras;

VI - definir, documentar e executar os procedimentos de *backup* e restauração;

VII - comunicar ao gestor da informação os incidentes ou erros que causem indisponibilidade ou impossibilitem a execução ou restauração de *backups*;

VIII - gerenciar mensagens e registros de auditoria dos *backups*;

IX - elaborar relatórios periódicos de *backup* e restauração;

X - disponibilizar informações que subsidiem as decisões referentes à gestão de capacidade relacionada aos *backups*;

XI - propor modificações visando ao aperfeiçoamento desta Política; e

XII - gerenciar a realização de testes periódicos de restauração.

Art. 39. São atribuições das áreas técnicas:

I - solicitar a salvaguarda e restaurações de dados, com anuência do gestor da informação;

II - sanar dúvidas técnicas do Administrador de *backup* acerca dos dados salvaguardados;

III - validar, tecnicamente, o resultado das restaurações eventualmente solicitadas; e

IV - validar, tecnicamente, o resultado dos testes de restauração dos *backups*.

Art. 40. São atribuições dos gestores da informação:

I - solicitar a salvaguarda dos dados geridos e dar anuência à solicitação feita pela área técnica para recuperação de dados;

II - validar, negocialmente, o resultado das restaurações eventualmente solicitadas; e

III - validar, negocialmente, o resultado dos testes de restauração dos *backups*.

Art. 41. Os servidores responsáveis pela operacionalização das rotinas de *backup* e restauração de dados deverão ser capacitados para as tecnologias, procedimentos e soluções utilizadas.

CAPÍTULO VI

DAS DISPOSIÇÕES FINAIS

Art. 42. Esta Política poderá ser revisada a qualquer tempo, para fins de eventual atualização, quando identificada a necessidade de alteração em qualquer de seus dispositivos.

Art. 43. A Diretoria de Tecnologia da Secretaria Especial de Administração e os gestores das informações tomarão as providências necessárias para a adequação das rotinas e dos procedimentos de *backups* definidos nesta Política.

Parágrafo único. Casos omissos serão decididos pelo Comitê de Governança Digital e Segurança da Informação, com análise do Subcomitê de Segurança da Informação da Presidência da República, da Diretoria de Tecnologia da Secretaria Especial de Administração e, se necessário, dos gestores da informação.

Art. 44. Em caso de violação desta Política poderão ser aplicadas sanções previstas na Lei 8.112/1990 e outras legislações cabíveis.

Art. 45. Esta Política entra em vigor em 1º de dezembro de 2022.

**MARIO FERNANDES**

**Presidente do Comitê de Governança Digital e Segurança da Informação**

Documento assinado eletronicamente por **Mario Fernandes**, **Presidente do Comitê de Governança Digital e Segurança da Informação da Presidência da República**, em 08/11/2022, às 16:02, 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 do documento pode ser conferida informando o código verificador **3731805** e o código CRC **0C290859** no site: https://super.presidencia.gov.br/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0

**Referência:** Processo nº 00094.002189/2022-97 SUPER nº 3731805