

XXVIII - Serviços de TIC: Conjunto estruturado e organizado de recursos tecnológicos, processos operacionais e atividades de suporte essenciais para fornecer serviços de coleta, processamento, armazenamento, transmissão e proteção de informações digitais no Ministério dos Transportes.

§ 1º Além das definições contidas neste artigo, a interpretação e a aplicação desta Norma deverão considerar e respeitar os conceitos dispostos na Lei nº 12.527, de 2011 (Lei de Acesso à Informação - LAI), na Lei nº 13.709, de 2018 (Lei Geral de Proteção de Dados Pessoais - LGPD), no Glossário de Segurança da Informação (Portaria GSI/PR nº 93, de 18 de outubro de 2021) e na Política de Segurança da Informação em vigor no Ministério - POSIN (Portaria MT nº 287, de 4 de abril de 2025).

§ 2º Em caso de divergência ou omissão de conceitos técnicos, prevalecerão as definições estabelecidas na Política de Segurança da Informação do Ministério e nas normas de segurança cibernética emitidas pelo Gabinete de Segurança Institucional da Presidência da República - GSI/PR.

Seção III

Do Âmbito de Aplicação

Art. 6º A presente Norma se aplica a todos os dados digitais institucionais produzidos ou custodiados pelo Ministério dos Transportes, inclusive os armazenados em serviços de computação em nuvem formalmente contratados pela Pasta.

Parágrafo único. A obrigatoriedade de salvaguarda dos dados digitais pertencentes aos serviços de TIC do Ministério dos Transportes, mas que estejam sob a custódia, interna ou externa, de outras entidades, públicas ou privadas, como ocorre nos casos de ambientes e serviços em nuvem (cloud computing), deverá estar explicitamente garantida e detalhada nos acordos, termos de referência e instrumentos contratuais que formalizam a relação de fornecimento e responsabilidade entre as partes envolvidas, assegurando a retenção da propriedade e do controle dos dados pelo Ministério.

Art. 7º As diretrizes estabelecidas nesta Norma aplicam-se a todos os agentes que interagem com o ambiente de Tecnologias da Informação e Comunicação do Ministério dos Transportes, compreendendo:

I - os servidores efetivos, os empregados públicos, os estagiários e quaisquer colaboradores terceirizados que, em razão de sua função ou acesso autorizado, criem, manipulem ou acessem dados pertencentes formalmente ao acervo informacional do Ministério; e

II - os prestadores de serviço, as empresas contratadas e quaisquer terceiros que utilizem, ainda que de forma temporária ou eventual, os serviços de TIC sob a responsabilidade do Ministério dos Transportes, inclusive no âmbito de suas unidades descentralizadas ou de entidades a ele vinculadas que utilizem a infraestrutura central de TIC.

Art. 8º Em virtude da distribuição de competências e da necessidade de delimitar o escopo de atuação direta da área de Tecnologia da Informação do Ministério, não se submetem às rotinas padronizadas de backup e restauração de dados digitais previstas nesta Norma:

I - os dados armazenados localmente em estações de trabalho pessoais, computadores portáteis (notebooks), dispositivos de armazenamento externos, mídias removíveis ou quaisquer outros equipamentos de TI que não sejam gerenciados, monitorados e controlados diretamente pela área de Infraestrutura de Tecnologias da Informação do Ministério dos Transportes; e

II - os dados produzidos e armazenados por órgãos ou entidades federais que, embora mantenham vínculo formal ou institucional com o Ministério dos Transportes, detenham autonomia administrativa, orçamentária e tecnológica para gerir sua própria infraestrutura e política de backup.

CAPÍTULO II

DOS PRINCÍPIOS GERAIS DE BACKUP E CONTINUIDADE

Art. 9º Esta Norma regulamenta as ações relacionadas ao backup e à restauração de dados digitais no âmbito do Ministério dos Transportes, devendo observar as diretrizes e os requisitos estabelecidos na Política de Segurança da Informação - POSIN.

Art. 10. A Norma de Backup e Restauração de Dados Digitais deverá manter alinhamento à gestão de continuidade de negócios do Ministério dos Transportes.

Art. 11. O Plano de Backup e Restauração de Dados Digitais deverá estar integrado ao Plano de Resposta a Incidentes de Segurança da Informação, à Política de Segurança da Informação - POSIN e ao processo institucional de gestão de riscos de segurança da informação do Ministério dos Transportes.

Parágrafo único. As falhas relevantes na execução das rotinas de backup, bem como os resultados dos testes de restauração que indiquem vulnerabilidades, indisponibilidades ou inconsistências relevantes, deverão ser registrados e tratados como eventos de segurança da informação, constituindo insumo para o processo institucional de gestão de riscos e para o aprimoramento contínuo dos controles de segurança da informação, devendo tais ocorrências ser comunicadas à unidade responsável pela gestão de incidentes de segurança da informação no âmbito do Ministério dos Transportes.

Art. 12. As rotinas de backup devem ser projetadas, configuradas e executadas com o propósito de viabilizar a restauração integral dos dados dentro do Recovery Time Objective (RTO) estabelecido no Plano de Backup e Restauração de Dados Digitais, especialmente em situações de indisponibilidade, falha crítica dos serviços de TIC, incidentes cibernéticos ou desastres.

Art. 13. As rotinas de backup devem utilizar soluções tecnológicas próprias e especializadas, concebidas especificamente para este fim, devendo ser implementada, sempre que tecnicamente viável, a automação das rotinas de backup.

Art. 14. Deverão ser estabelecidos requisitos mínimos diferenciados de periodicidade, frequência e retenção das rotinas de backup, definidos de acordo com a classificação de criticidade do serviço de TIC, da base de dados ou do tipo de dado salvaguardado, concedendo-se prioridade máxima de planejamento e execução aos serviços de TIC formalmente classificados como críticos para o funcionamento do Ministério dos Transportes.

Art. 15. O armazenamento dos backups deverá ser realizado, sempre que tecnicamente factível e economicamente viável, em local distinto da infraestrutura de produção.

Art. 16. A infraestrutura de rede utilizada nos processos de backup deverá ser segregada dos sistemas de produção e das redes que suportam serviços críticos, ao menos de forma lógica e, quando tecnicamente viável, também de forma física, de modo a prevenir a propagação de incidentes cibernéticos entre os ambientes de produção e de backup.

Art. 17. A unidade técnica responsável pela infraestrutura de TIC do Ministério dos Transportes deverá manter reserva estratégica de recursos físicos e lógicos de infraestrutura, adequadamente segregados dos ambientes de produção, destinados à realização de testes periódicos e formais de restauração de backups, conforme previsto no Plano de Backup e Restauração de Dados Digitais, assegurando que tais testes não comprometam a disponibilidade dos ambientes produtivos.

Art. 18. O Gestor da Informação ou o responsável técnico formalmente designado pelo produto, sistema ou serviço de TIC deverá solicitar formalmente à unidade técnica responsável pela infraestrutura de TIC do Ministério dos Transportes a inclusão de seus dados no sistema regular de backup, em conformidade com o Plano de Backup e Restauração de Dados Digitais, previamente à entrada em operação efetiva da solução.

Art. 19. Em situações em que a confidencialidade da informação seja relevante, os backups deverão ser protegidos por meio de mecanismos de criptografia, sempre que tecnicamente e economicamente viável, observados o nível de criticidade da informação e os riscos associados.

CAPÍTULO III

DA FREQUÊNCIA E ESTRATÉGIA DE BACKUP

Seção I

Da Frequência e dos Métodos de Backup

Art. 20. Os backups dos serviços de TIC do Ministério dos Transportes deverão ser realizados observando, no mínimo, as seguintes frequências temporais:

I - diária;

II - semanal;

III - mensal; ou

IV - anual.

Art. 21. As especificidades operacionais dos serviços de TIC, sejam eles classificados como críticos ou não críticos, poderão demandar a adoção de frequência, método e tempo de retenção distintos das frequências mínimas estabelecidas nos incisos do art. 20, desde que tais exceções estejam devidamente justificadas e formalmente aprovadas no Plano de Backup e Restauração de Dados Digitais.

Art. 22. Todos os ativos de informação diretamente envolvidos no processo de backup são considerados, para fins desta Norma, ativos críticos e deverão receber tratamento e níveis de proteção compatíveis com essa classificação.

Art. 23. Os backups deverão ser armazenados em diferentes dispositivos e tecnologias, conforme a necessidade técnica e a disponibilidade de recursos previstas no Plano de Backup e Restauração de Dados Digitais, podendo ser utilizados, entre outros meios:

I - fitas magnéticas;

II - discos rígidos ou de estado sólido em sistemas de armazenamento dedicados; ou

III - serviços de armazenamento em nuvem formalmente contratados pelo Ministério dos Transportes e que atendam aos requisitos de segurança da informação.

Art. 24. A realização dos backups poderá utilizar os métodos Completo, Diferencial ou Incremental.

Parágrafo único. A utilização e a periodicidade dos métodos Diferencial e Incremental poderão ser ajustadas pelo Administrador de Backup, mediante justificativa técnica formal, em razão de limitações de espaço de armazenamento ou da necessidade de otimização do uso dos recursos computacionais.

Art. 25. Os backups deverão possuir, no mínimo, duas cópias armazenadas em meios distintos, sendo uma mantida em ambiente online e outra em ambiente offline ou offsite.

Art. 26. Os sistemas, bases de dados ou repositórios de arquivos classificados como críticos deverão contar com backups armazenados em dispositivos offline, preferencialmente em mídias físicas.

Art. 27. A restauração de dados limita-se ao último ponto de recuperação disponível, correspondente à última execução bem-sucedida do backup, não sendo tecnicamente possível recuperar dados criados ou modificados após esse ponto.

Art. 28. Nos casos em que os serviços de TIC forem contratados para operar em ambiente de nuvem (cloud computing), as soluções e rotinas de backup poderão estar integradas ao serviço contratado, desde que o instrumento contratual assegure, de forma expressa e inequívoca:

I - a integridade dos dados armazenados;

II - a possibilidade de pronta restauração;

III - o atendimento ao Recovery Point Objective (RPO) estabelecido pelo Ministério dos Transportes; e

IV - o atendimento ao Recovery Time Objective (RTO) estabelecido pelo Ministério dos Transportes.

Seção II

Da Estrutura e do Escopo do Plano de Backup e Restauração de Dados Digitais

Art. 29. O Plano de Backup e Restauração de Dados Digitais deverá constituir documento dinâmico e suficientemente abrangente, refletindo com precisão os requisitos de negócio do Ministério dos Transportes, bem como os requisitos de segurança da informação e de proteção de dados.

§ 1º O Plano de Backup e Restauração de Dados Digitais deverá explicitar, como requisitos técnicos mínimos obrigatórios, para cada sistema ou conjunto de dados, no mínimo:

I - o escopo detalhado dos dados digitais a serem salvaguardados;

II - o tipo de backup a ser utilizado;

III - a frequência de execução das rotinas de backup;

IV - o período de retenção dos dados armazenados;

V - o Recovery Point Objective (RPO); e

VI - o Recovery Time Objective (RTO).

Art. 30. Somente serão incluídos nas rotinas regulares de backup os ativos de informação formalmente armazenados em servidores e demais infraestruturas físicas ou lógicas, inclusive ambientes locais (on-premises) ou em serviços de computação em nuvem, desde que:

I - estejam sob gestão direta da Subsecretaria de Gestão Estratégica, Tecnologia e Inovação (SGETI); e

II - sejam necessários à continuidade do negócio do Ministério dos Transportes ou formalmente classificados como estratégicos ou imprescindíveis.

§ 1º As naturezas dos dados e ativos de informação passíveis de backup incluem, mas não se limitam, às seguintes categorias:

I - arquivos de sistemas corporativos;

II - arquivos de sistemas operacionais;

III - bases de dados;

IV - arquivos armazenados em servidores de arquivos ou em serviços corporativos de armazenamento em nuvem;

V - repositórios de código-fonte de aplicações institucionais e documentação técnica associada;

VI - serviços de correio eletrônico corporativo;

VII - máquinas virtuais e ambientes containerizados;

VIII - diretórios de autenticação e serviços de identidade;

IX - arquivos de configuração de sistemas e equipamentos de rede; e

X - arquivos de log e registros de auditoria.

§ 2º O rol previsto no § 1º poderá ser ampliado a qualquer tempo pela SGETI, em razão da adoção de novas tecnologias, dispositivos ou contextos operacionais que demandem salvaguarda.

§ 3º A classificação de dados e ativos de informação como estratégicos ou imprescindíveis será realizada formalmente pelo Comitê de Governança Digital e Segurança da Informação (CGDSI), que poderá consultar, quando julgar pertinente, as áreas de negócio envolvidas, órgãos setoriais do Ministério dos Transportes ou entidades externas.

Art. 31. Do escopo regular das rotinas de backup estarão excluídos os dados armazenados em estações individuais de trabalho, bem como os dados de natureza pessoal de agente público do Ministério inseridos diretamente na rede ministerial, ressalvadas as seguintes hipóteses em que a salvaguarda é permitida para fins de análise e preservação probatória:

I - identificação de um incidente cibernético confirmado em algum desses ativos individuais, sendo o backup realizado para fins de mitigação de danos e análise forense; ou

II - ocorrência comprovada de infração à legislação penal ou de processo administrativo disciplinar (PAD) envolvendo dispositivo que faça parte do patrimônio do Ministério dos Transportes, sendo o backup fundamental para a cadeia de custódia da prova.

Parágrafo único. É de responsabilidade inequívoca e exclusiva do usuário o gerenciamento e o armazenamento de seus dados de trabalho no Servidor de Arquivos Corporativo, no OneDrive institucional ou no SharePoint, ambientes para os quais o Ministério já possui rotinas regulares e adequadas de backup.

CAPÍTULO IV

DA RETENÇÃO, PRESERVAÇÃO E DISPONIBILIDADE

Seção I

Da Política Geral de Retenção, Preservação e Descarte de Dados Digitais

Art. 32. A determinação do período de retenção, entendido como o prazo de armazenamento e conservação dos backups, bem como a posterior eliminação de dados, deverá observar a criticidade da informação, o tipo de serviço de TIC, a frequência de atualização dos dados, as características específicas de cada sistema e, prioritariamente, a legislação e as normas vigentes que estabeleçam os prazos mínimos e máximos de armazenamento de dados e documentos no âmbito da Administração Pública Federal.

Art. 33. Os prazos de retenção, preservação e descarte de dados digitais previstos nesta Norma deverão ser aplicados em conformidade com a legislação arquivística federal, com as normas de gestão documental da Administração Pública

