MINISTÉRIO DA INFRAESTRUTURA

DEPARTAMENTO NACIONAL DE INFRAESTRUTURA DE TRANSPORTES

INSTRUÇÃO NORMATIVA Nº 1/DNIT SEDE, DE 27 DE JANEIRO DE 2022

Institui a Política de **Backup** e Recuperação de Dados Digitais do Departamento Nacional de Infraestrutura de Transportes.

O DIRETOR-GERAL DO DEPARTAMENTO NACIONAL DE INFRAESTRUTURA DE TRANSPORTES – DNIT, no uso das atribuições que lhe conferem o artigo 173, do Regimento Interno aprovado pela Resolução nº 39 de 17/11/2020, publicado no DOU de 19/11/2020, o Relato nº 9/2022/DAF/DNIT SEDE, o qual foi incluído na Ata da 4ª Reunião Ordinária da Diretoria Colegiada, realizada em 24/01/2022, e o constante no processo administrativo nº 50600.023746/2021-33, resolve:

Art. 1º INSTITUIR a Política de **Backup** e Recuperação de Dados Digitais do Departamento Nacional de Infraestrutura de Transportes - DNIT.

CAPÍTULO I
DAS DISPOSIÇÕES PRELIMINARES

Art. 2º A Política de **Backup** e Recuperação de Dados Digitais objetiva instituir diretrizes, responsabilidades e competências que visam à segurança, proteção e disponibilidade dos dados digitais custodiados na infraestrutura de tecnologia da informação da Autarquia e formalmente definidos como de necessária salvaguarda (**backup**) pelo Proprietário da Informação no Departamento Nacional de Infraestrutura de Transportes.

Art. 3º A Política de que trata esta Instrução Normativa aplica-se a todas as unidades do DNIT que tenham sob sua custódia dados em suporte digital.

Art. 4º A salvaguarda e recuperação dos dados digitais do DNIT abrange exclusivamente dados digitais custodiados na infraestrutura de tecnologia da informação da Autarquia, cuja responsabilidade da Coordenação-Geral de Tecnologia da Informação - CGTI.

Parágrafo único. Não serão salvaguardados nem recuperados dados armazenados localmente, nos microcomputadores dos usuários ou em quaisquer outros dispositivos ou ambientes fora infraestrutura de tecnologia da informação da Autarquia, cuja responsabilidade é da Coordenação-Geral de Tecnologia da Informação - CGTI.

Art. 5º Todos os contratos, convênios, acordos e instrumentos congêneres cujo o cumprimento do objeto produza ou manuseie dados digitais, devem conter cláusulas que estabeleçam a obrigatoriedade de observância desta Política de **Backup**.

§ 1º. A salvaguarda (**backup**) dos dados em formato digital relacionados a ativos de informação do DNIT, 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.

§ 2º. Excepcionalmente, a CGTI poderá optar pela realização do **backup** de dados dispostos em nuvem nos **appliances on premises,** quando devidamente justificado, considerando o princípio da economicidade e a garantia da continuidade dos negócios.

CAPÍTULO II
DOS CONCEITOS E DEFINIÇÕES

Art. 6º Para os fins desta Instrução Normativa, considera-se:

I - administrador de **backup**: unidade responsável pelo planejamento de soluções de **backup**, definição de padrões, configurações e atendimento avançado de resolução de incidentes e problemas referentes a **backups**. No âmbito do DNIT, a Coordenação de Infraestrutura de Tecnologia de Informação - COINF;

II - área técnica: unidade responsável (CGTI) pela operação técnica dos ativos e serviços de TI;

III - ativos de informação: os meios de armazenamento, transmissão e processamento da informação, os equipamentos necessários a isso, os sistemas utilizados para tal, os locais onde se encontram esses meios, e também os recursos humanos que a eles têm acesso;

IV - **backup** ou cópia de segurança: conjunto de procedimentos que permitem salvaguardar os dados de um sistema computacional, garantindo guarda, proteção e recuperação;

V - **backup** completo: modalidade de **backup** em que todos os dados a serem salvaguardados são copiados integralmente (cópia de segurança completa) para uma unidade de armazenamento, independentemente de terem sido ou não alterados desde o último **backup**;

VI - **backup** incremental: modalidade de **backup** em que são salvaguardados apenas os dados novos ou modificados desde o último **backup** de qualquer modalidade efetuado;

VII - **backup** diferencial: modalidade de **backup** em que são salvaguardados apenas dados novos ou modificados desde o último **backup** completo efetuado;

VIII - COSIC: acrônimo para Comitê de Segurança da Informação;

IX - criticidade: grau de importância dos dados para a continuidade das atividades e serviços da organização;

X - descarte: eliminação correta de informações, documentos, mídias e acervos digitais;

XI - disponibilidade: propriedade pela qual se assegura que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade devidamente autorizados;

XII - imagem de **backup**: arquivo gerado pela solução de **backup**, não necessariamente no formato original dos arquivos que contêm os dados salvaguardados;

XIII - infraestrutura de tecnologia da informação: consiste nos componentes e serviços que fornecem a base para sustentar todos os sistemas de informação de uma organização;

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

XV - plano de **backup** – planejamento que detalha a execução da Política de **Backup**, no qual são anexadas as rotina/roteiro de **backup** de cada dado ou informação a ser salvaguardado;

XVI - plano de continuidade de negócios (PCN): documentação dos procedimentos e informações necessárias para que o órgão mantenha seus ativos de informação críticos e a continuidade de suas atividades críticas em local alternativo em um nível previamente definido, em casos de incidentes;

XVII - proprietário da informação: área interessada do órgão ou indivíduo legalmente instituído por sua posição ou cargo, que é responsável primário pela viabilidade e sobrevivência da informação;

XVIII - **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;

XIX - **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;

XX - restauração: processo de recuperação e disponibilização de dados salvaguardados em determinada imagem de **backup**;

XXI - retenção: período pelo qual os dados devem ser salvaguardados e estar aptos à restauração;

XXII - rotina/roteiro de **backup**: procedimento utilizado para se realizar um **backup**;

XXIII - serviço 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;

XXIV - unidade de armazenamento: dispositivo para armazenamento de dados em suporte digital; e

XXV - unidade de armazenamento de **backup**: unidade de armazenamento com características específicas para retenção de cópia de segurança de dados digitais.

CAPÍTULO III
DOS PADRÕES OPERACIONAIS

Seção I
Dos princípios gerais

Art. 7º A Política de **Backup** e Recuperação de Dados Digitais deve estar alinhada com uma gestão de continuidade de negócios em nível organizacional.

Art. 8º O Plano de **Backup** deve conter as rotinas de backup para cada serviço ou recurso que armazene dado digital, cumprindo as diretrizes da Política, definindo requisitos específicos de segurança da informação paras as cópias de segurança realizadas (ex.: controles de acesso lógico, uso de criptografia, armazenamento em local seguro, armazenamento em local remoto seguro diferente do local original etc.).

Art. 9º O Plano de **Backup** deve atender ao **checklist** disposto no Anexo II.

Parágrafo único. Os pontos do **checklist** que não sejam atendidos ou não se aplicarem, devem ser devidamente justificados, considerando o princípio da economicidade e a garantia da continuidade dos negócios.

Art. 10. As rotinas de **backup** devem ser orientadas para a restauração dos dados no menor tempo possível, principalmente quando da indisponibilidade de serviços ou recurso.

Art. 11. As rotinas de **backup** devem possuir requisitos mínimos diferenciados de acordo com o tipo de serviço, recurso ou dado salvaguardado, dando prioridade aos serviços ou recursos críticos da organização.

Art. 12. Os serviços ou recursos críticos do DNIT devem ser formalmente elencados pelo Comitê Gestor de Tecnologia da Informação do DNIT na elaboração do Plano de Continuidade dos

negócios.

Art. 13. O **backup** de serviços ou recursos não críticos devem ser formalmente solicitados ao Administrador de **Backup** pelo Proprietário da Informação.

Art. 14. As rotinas de **backup** dos dados referentes aos serviços e recursos críticos e não críticos devem refletir os requisitos de negócio da organização, bem como os requisitos de segurança da informação envolvidos e a criticidade da informação para a continuidade da operação da organização, e devem 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;

VII - requisitos de segurança da informação (criptografia, acessos, etc.); e

VIII - requisitos legais e normativos.

Art. 15. Os incisos I, III, IV, VII e VIII do Art. anterior são vinculados à segurança e criticidade da informação para a continuidade da operação da organização, razão pela qual devem ser definidos pelo Proprietário da Informação, com o apoio técnico do Administrador de **backup**.

.

Seção II
Das ferramentas de backup

Art. 16. As rotinas de **backup** devem utilizar soluções próprias e especializadas para este fim, preferencialmente de forma automatizada.

Art. 17. Os ativos envolvidos no processo de **backup** são considerados ativos críticos para a organização.

Parágrafo único. Compete à CGTI solicitar, a Administração, com as justificativas pertinentes, os equipamentos necessários para manter o parque de ativos sempre atualizado e em quantidade necessária ao atendimento da demanda da Autarquia.

Seção III
Da frequência e retenção dos dados

Art. 18. Os **backups** dos serviços ou recursos críticos do DNIT devem ser realizados utilizando-se as seguintes frequências temporais:

I - diária;

II - semanal;

III - mensal; e

IV - anual.

Parágrafo único. Deverá ser avaliado a necessidade de realização de **backups** com frequência menor que a diária, conforme a criticidade do serviço ou recurso.

Art. 19. Os serviços ou recursos críticos do DNIT devem ser resguardados sob um padrão mínimo, o qual deve observar a correlação frequência/retenção de dados estabelecida a seguir:

I - diária: semanal;

II - semanal: mensal;

III - mensal: 1 ano;

IV - anual: 5 anos.

Art. 20. Os serviços e recursos não críticos do DNIT devem ser resguardados observando-se o padrão mínimo de correlação frequência/retenção de dados estabelecida a seguir:

I - diária: semanal;

II - semanal: mensal;

III - mensal: 6 meses;

IV - anual: 1 anos.

Art. 21. Especificidades dos serviços ou recursos críticos e não críticos podem demandar frequência e tempo de retenção diferenciados, cabendo a devida justificativa na respectiva rotina de **backup**, acordadas entre o Proprietário da Informação e o Administrador de **Backup**.

Art. 22. A recuperação de dados não será viabilizada em caso de perdas anteriores à conclusão da cópia de segurança. Dados criados ou modificados entre execuções de cópias de segurança subsequentes não serão protegidos por soluções de **backup**.

Art. 23. A alteração das frequências e tempos de retenção definidos nesta seção deve ser precedida de solicitação e justificativa formais encaminhadas ao Administrador de **Backup** e acordadas junto ao Proprietário da Informação.

Seção IV
Do uso da rede

Art. 24. O administrador de **backup** deve considerar o impacto da execução das rotinas de **backup** sobre o desempenho da rede de dados do DNIT, garantindo que o tráfego necessário às suas atividades não ocasione indisponibilidade dos demais serviços e recursos de Tecnologia da Informação do DNIT.

Art. 25. A execução do **backup** deve concentrar-se, preferencialmente, no período de janela de **backup**.

Art. 26. O período de janela de **backup** deve ser determinado pelo administrador de **backup** em conjunto com o Proprietário da Informação.

Seção V
Das unidades de armazenamento de backups

Art. 27. 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**.

Art. 28. 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. 29. Podem ser utilizadas técnicas de compressão de dados, contanto que o acréscimo no tempo de recuperação dos dados seja considerado aceitável pelo Proprietário da Informação.

Art. 30. As unidades de armazenamento dos **backups** devem ser acondicionadas em locais apropriados, com controle de fatores ambientais sensíveis, como umidade e temperatura, e com acesso restrito a pessoas autorizadas pelo administrador de **backup**.

Art. 31. Os **backups** podem ser classificados como **on-line, off-line** ou **off-site**, a depender da forma de acesso ao **backup** realizado:

I - **On-line** - uma vez realizado, o **backup** é acessível dentro da rede de dados do DNIT;

II - **Off-line** - uma vez realizado, o **backup** não é acessível em rede, sendo armazenado em mídias físicas removíveis; e

III - **Off-site** - uma vez realizado, o **backup** é armazenado em outro data center, geograficamente separado, ou em serviço de **backup** em nuvem.

Art. 32. Os **backups** devem ter no mínimo duas cópias, realizadas em formatos de mídia distintos, sendo um **on-line** e outro **off-line** ou **off-site.**

Parágrafo único. Os dados considerados críticos devem ser armazenados no mínimo, de forma redundante, ***off-line*** e ***off-site*.**

Art. 33. **Backups** armazenados em nuvem estão sujeitos à Instrução Normativa nº 5, de 30 de agosto de 2021 e suas atualizações, e à Lei nº 13.709/2018 - Lei Geral de Proteção de Dados Pessoais.

Art. 34. **Backups** com dados sensíveis e que requeiram tratamento específico quanto à segurança da informação devem ser criptografados e ter seus acessos devidamente controlados.

Art. 35. Quando da necessidade de descarte de unidades de armazenamento de **backups**, tais recursos devem ser fisicamente destruídos de forma a inutilizá-los, garantindo a sanitização dos dados, atentando-se ao descarte sustentável e ambientalmente correto.

Seção VI
Dos testes de backup

Art. 36. Os **backups** devem ser testados periodicamente, com o objetivo de garantir a sua confiabilidade e a integridade dos dados salvaguardados.

§ 1º O administrador de **backup** deverá elaborar cronograma de testagem priorizando os **backups** mais importantes para a continuidade das rotinas de trabalho por nível de criticidade (ou relevância) dos dados, aplicações e sistemas, do qual o Proprietário da Informação deve estar ciente e de acordo.

§ 2º A metodologia a ser utilizada para testes será o teste de ***restore***.

§ 3º Realizado o **restore** com sucesso, o Proprietário da Informação deve providenciar os testes de validação da integridade dos dados.

§ 4º Os resultados dos testes sejam adequadamente documentados.

Art. 37. Os testes de restauração dos **backups** devem ser realizados, por amostragem, em equipamentos servidores diferentes dos equipamentos que atendem os ambientes de produção, observados os recursos humanos e tecnológicos disponíveis no DNIT.

Art. 38. A periodicidade, a abrangência, os procedimentos e as rotinas inerentes aos testes de **backup** serão definidos em Plano de **Backup**.

§ 1º A alteração das frequências da realização de testes de **backup** deve ser precedida de solicitação e justificativa formais encaminhadas ao Administrador de **Backup** e acordadas junto ao Proprietário da Informação.

§ 2º Recomenda-se que os testes de restauração (***restore***) dos **backups** dos dados críticos sejam realizados ao menos mensalmente e dos dados não críticos, ao menos semestralmente, haja vista que uma periodicidade superior a essa (realização menos frequente do que uma vez por mês) aumenta o risco para a organização.

CAPÍTULO IV
DAS RESPONSABILIDADES

Art. 39. São atribuições do **administrador de backup**:

I - propor soluções de cópia de segurança das informações digitais corporativas produzidas ou custodiadas no DNIT;

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

III - providenciar a configuração das soluções de **backup**;

IV - providenciar a manutenção das unidades de armazenamento de **backups** preservadas, funcionais e seguras;

V - providenciar a definição dos procedimentos de restauração;

VI - providenciar as medidas preventivas para evitar falhas;

VII - reportar imediatamente a Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos - ETIR os incidentes ou erros que causem indisponibilidade ou impossibilitem a execução ou restauração de **backups**;

VIII - providenciar a disponibilização das informações que subsidiem as decisões referentes à gestão de capacidade relacionada aos **backups**;

IX - propor modificações visando ao aperfeiçoamento da Política de **Backup** e Recuperação de Dados Digitais, objeto desta Instrução Normativa;

X - providenciar a execução dos testes de restauração;

XI - providenciar a elaboração dos procedimentos operacionais;

XII - providenciar a restauração ou recuperação dos **backups** em caso de necessidade, com anuência do Proprietário da Informação;

XIII - providenciar a operação e manuseio das unidades de armazenamento de **backups**;

XIV - providenciar o gerenciamento das mensagens e registros de auditoria (LOGs) diários dos **backups**;

XV - providenciar a verificação diária dos eventos gerados pela solução de **backup**, tomando as providências necessárias para remediação de eventuais falhas;

XVI - sanar dúvidas técnicas do Proprietário da Informação acerca das informações salvaguardadas;

XVII - providenciar a validação, tecnicamente, do resultado das restaurações eventualmente solicitadas; e

XVIII - providenciar a validação, tecnicamente, do resultado dos testes de restauração dos **backups**.

Art. 40. São atribuições dos **Proprietários da Informação**:

I - solicitar, formalmente, a salvaguarda das informações geridas;

II - providenciar a validação, negocialmente, do resultado das restaurações eventualmente solicitadas;

III - providenciar a validação, negocialmente, do resultado dos testes de restauração dos **backups**; e

IV - informar qual o escopo de dados, recursos e ou serviços serão incluídos na rotina de **backup**.

Art. 41. A solicitação de administrador 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.

CAPÍTULO V
DAS DISPOSIÇÕES FINAIS

Art. 42. Esta Instrução Normativa 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 CGTI, as unidades de TI (nas superintendências regionais) e os proprietários das informações tomarão as providências necessárias para a adequação das rotinas e dos procedimentos de **backups** às diretrizes definidas nesta Instrução Normativa.

Parágrafo único. Casos excepcionais não previstos nesta Instrução Normativa serão apresentados pelo administrador de **backup** ao COSIC, que deliberará sobre a questão.

Art. 44. Esta Instrução Normativa entra em vigor no dia 1º de março de 2022.

ANTÔNIO LEITE DOS SANTOS FILHO
Diretor-Geral

ANEXO I

REFERÊNCIAS NORMATIVAS

1. Dispositivos legais e normas técnicas aplicáveis à Política de **Backup**:

I - Portaria nº 1745, de 29 de março de 2021, que institui a Política de Segurança da Informação e Comunicações – POSIC e estabelece as diretrizes para a segurança do manuseio, tratamento e controle e para a proteção dos dados, informações e conhecimentos produzidos, armazenados ou transmitidos, por qualquer meio, pelos sistemas de informação a serem, obrigatoriamente, observadas na definição de regras operacionais e procedimentos no âmbito do Departamento Nacional de Infraestrutura de Transportes - DNIT;

II - Instrução Normativa GSI/PR Nº 1, de 27 de maio de 2020 e suas alterações e Normas Complementares, do Gabinete de Segurança Institucional da Presidência da República, que disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, e dá outras providências;

III - Portaria GSI/PR Nº 93, de 26 de setembro de 2019, que aprova o Glossário de Segurança da Informação;

IV - Acórdão 1.109/2021-TCU-Plenário, pelo qual foram tecidas análises do Tribunal de Contas da União, que objetivam o constante melhoramento de plano de continuidade de negócio e criação e implantação de política de geração de cópias de segurança dos dados cautelados por esta Autarquia (**backup** e restauração);

V - Norma Técnica ABNT NBR ISO/IEC 27001:2013, que especifica os requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão da segurança da informação dentro da organização;

VI - Norma Técnica ABNT NBR ISO/IEC 27002:2013, que detalha Técnicas de segurança e código de prática para a gestão da segurança da informação; e

VII - Lei nº 13.709/2018 - Lei Geral de Proteção de Dados Pessoais;

VIII - Instrução Normativa nº 22/DNIT SEDE, de 12 de maio de 2021, que dispõe sobre a Estrutura de Gestão da Segurança da Informação no âmbito do Departamento

Nacional de Infraestrutura de Transportes – DNIT; e

IX - Instrução Normativa/GSI/PR nº 5, de 30 de agosto de 2021 e suas atualizações, que dispõe sobre os requisitos mínimos de segurança da informação para utilização de soluções de computação em nuvem pelos órgãos e pelas entidades da administração pública federal.

ANEXO II

CHECKLIST PARA VERIFICAÇÃO DE PLANO (OU PROCEDIMENTO/ROTEIRO) DE BACKUP ESPECÍFICO

#	VERIFICAR SE	Sim/Não/ Não se aplica	Observações/ Evidências
1	O plano foi publicado/comunicado para as partes interessadas (titulares dos dados, usuários e gestores dos sistemas etc.)		
2	O plano foi aprovado pelas partes interessadas		
3	O plano registra/define de modo completo e exato a abrangência/escopo das cópias de segurança (ou seja, aquilo que deve ser copiado, incluindo indicações de datas/períodos) Ex.: quais arquivos de dados ou de sistema, quais bases de dados, quais tabelas, quais pastas/folders etc.		
4	O plano estabelece que seja monitorada e documentada a execução do procedimento de geração das cópias de segurança, por meio de registros (logs) relativos a todos os itens copiados, a fim de detectar eventuais falhas e assegurar que houve a realização integral das cópias de segurança		
5	O plano documenta os procedimentos para realizar a recuperação/restauração (*restore*) das cópias de segurança quando necessário (ou seja, o "como" recuperar os **backups**)		
6	O plano define a frequência de realização das cópias de segurança (ex.: diária, semanal, mensal, anual etc.)		
7	O plano define os tipos de cópias a serem realizadas (completa, incremental ou diferencial)		
8	O plano define o tempo de retenção das cópias de segurança		
9	O plano define requisitos específicos de segurança da informação* (ex.: controles de acesso lógico, uso de criptografia etc.) *Requisitos relativos à confidencialidade, à integridade e à disponibilidade das informações		
10	O plano define a necessidade de armazenamento das cópias de		

	segurança em local seguro e em local remoto seguro diferente do local original		
11	O plano define procedimentos regulares de teste de recuperação/restauração (*restore*) das cópias de segurança, a fim de detectar tempestivamente eventuais falhas lógicas e físicas (nas mídias de armazenamento)		
12	O plano estabelece que a execução dos procedimentos de teste de recuperação/restauração (*restore*) das cópias de segurança seja documentada por meio de registros (logs) relativos a todos os itens restaurados, a fim de detectar eventuais falhas e assegurar que houve a recuperação integral das informações		

Documento assinado eletronicamente por **Antônio Leite dos Santos Filho**, **Diretor-Geral**, em 28/01/2022, às 13:23, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site https://sei.dnit.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **10366972** e o código CRC **4772B646**.

Referência: Processo nº 50600.023746/2021-33 SEI nº 10366972

Setor de Autarquias Norte | Quadra 3 | Lote A
CEP 70040-902
Brasília/DF | (061) 3315-4201

DIREÇÃO SUPERIOR

ATOS DA DIRETORIA-GERAL

INSTRUÇÃO NORMATIVA Nº 1/DNIT SEDE, DE 27 DE JANEIRO DE 2022 (*)

Institui a Política de **Backup** e Recuperação de Dados Digitais do Departamento Nacional de Infraestrutura de Transportes.

O DIRETOR-GERAL DO DEPARTAMENTO NACIONAL DE INFRAESTRUTURA DE TRANSPORTES – DNIT, no uso das atribuições que lhe conferem o artigo 173, do Regimento Interno aprovado pela Resolução nº 39 de 17/11/2020, publicado no DOU de 19/11/2020, o Relato nº 9/2022/DAF/DNIT SEDE, o qual foi incluído na Ata da 4ª Reunião Ordinária da Diretoria Colegiada, realizada em 24/01/2022, e o constante no processo administrativo nº 50600.023746/2021-33, resolve:

Art. 1º INSTITUIR a Política de **Backup** e Recuperação de Dados Digitais do Departamento Nacional de Infraestrutura de Transportes - DNIT.

CAPÍTULO I
DAS DISPOSIÇÕES PRELIMINARES

Art. 2º A Política de **Backup** e Recuperação de Dados Digitais objetiva instituir diretrizes, responsabilidades e competências que visam à segurança, proteção e disponibilidade dos dados digitais custodiados na infraestrutura de tecnologia da informação da Autarquia e formalmente definidos como de necessária salvaguarda (**backup**) pelo Proprietário da Informação no Departamento Nacional de Infraestrutura de Transportes.

Art. 3º A Política de que trata esta Instrução Normativa aplica-se a todas as unidades do DNIT que tenham sob sua custódia dados em suporte digital.

Art. 4º A salvaguarda e recuperação dos dados digitais do DNIT abrange exclusivamente dados digitais custodiados na infraestrutura de tecnologia da informação da Autarquia, cuja responsabilidade da Coordenação-Geral de Tecnologia da Informação - CGTI.

Parágrafo único. Não serão salvaguardados nem recuperados dados armazenados localmente, nos microcomputadores dos usuários ou em quaisquer outros dispositivos ou ambientes fora infraestrutura de tecnologia da informação da Autarquia, cuja responsabilidade é da Coordenação-Geral de Tecnologia da Informação - CGTI.

Art. 5º Todos os contratos, convênios, acordos e instrumentos congêneres cujo o cumprimento do objeto produza ou manuseie dados digitais, devem conter cláusulas que estabeleçam a obrigatoriedade de observância desta Política de **Backup**.

§ 1º. A salvaguarda (**backup**) dos dados em formato digital relacionados a ativos de informação do DNIT, 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.

§ 2º. Excepcionalmente, a CGTI poderá optar pela realização do **backup** de dados dispostos em nuvem nos **appliances on premises,** quando devidamente justificado, considerando o princípio da economicidade e a garantia da continuidade dos negócios.

CAPÍTULO II
DOS CONCEITOS E DEFINIÇÕES

Art. 6º Para os fins desta Instrução Normativa, considera-se:

I - administrador de **backup**: unidade responsável pelo planejamento de soluções de **backup**, definição de padrões, configurações e atendimento avançado de resolução de incidentes e problemas referentes a **backups**. No âmbito do DNIT, a Coordenação de Infraestrutura de Tecnologia de Informação - COINF;

II - área técnica: unidade responsável (CGTI) pela operação técnica dos ativos e serviços de TI;

III - ativos de informação: os meios de armazenamento, transmissão e processamento da informação, os equipamentos necessários a isso, os sistemas utilizados para tal, os locais onde se encontram esses meios, e também os recursos humanos que a eles têm acesso;

IV - **backup** ou cópia de segurança: conjunto de procedimentos que permitem salvaguardar os dados de um sistema computacional, garantindo guarda, proteção e recuperação;

V - **backup** completo: modalidade de **backup** em que todos os dados a serem salvaguardados são copiados integralmente (cópia de segurança completa) para uma unidade de armazenamento, independentemente de terem sido ou não alterados desde o último **backup**;

VI - **backup** incremental: modalidade de **backup** em que são salvaguardados apenas os dados novos ou modificados desde o último **backup** de qualquer modalidade efetuado;

VII - **backup** diferencial: modalidade de **backup** em que são salvaguardados apenas dados novos ou modificados desde o último **backup** completo efetuado;

VIII - COSIC: acrônimo para Comitê de Segurança da Informação;

IX - criticidade: grau de importância dos dados para a continuidade das atividades e serviços da organização;

X - descarte: eliminação correta de informações, documentos, mídias e acervos digitais;

XI - disponibilidade: propriedade pela qual se assegura que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade devidamente autorizados;

XII - imagem de **backup**: arquivo gerado pela solução de **backup**, não necessariamente no formato original dos arquivos que contêm os dados salvaguardados;

XIII - infraestrutura de tecnologia da informação: consiste nos componentes e serviços que fornecem a base para sustentar todos os sistemas de informação de uma organização;

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

XV - plano de **backup** – planejamento que detalha a execução da Política de **Backup**, no qual são anexadas as rotina/roteiro de **backup** de cada dado ou informação a ser salvaguardado;

XVI - plano de continuidade de negócios (PCN): documentação dos procedimentos e informações necessárias para que o órgão mantenha seus ativos de informação críticos e a continuidade de suas atividades críticas em local alternativo em um nível previamente definido, em casos de incidentes;

XVII - proprietário da informação: área interessada do órgão ou indivíduo legalmente instituído por sua posição ou cargo, que é responsável primário pela viabilidade e sobrevivência da informação;

XVIII - **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;

XIX - **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;

XX - restauração: processo de recuperação e disponibilização de dados salvaguardados em determinada imagem de **backup**;

XXI - retenção: período pelo qual os dados devem ser salvaguardados e estar aptos à restauração;

XXII - rotina/roteiro de **backup**: procedimento utilizado para se realizar um **backup**;

XXIII - serviço 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;

XXIV - unidade de armazenamento: dispositivo para armazenamento de dados em suporte digital; e

XXV - unidade de armazenamento de **backup**: unidade de armazenamento com características específicas para retenção de cópia de segurança de dados digitais.

CAPÍTULO III
DOS PADRÕES OPERACIONAIS

Seção I
Dos princípios gerais

Art. 7º A Política de **Backup** e Recuperação de Dados Digitais deve estar alinhada com uma gestão de continuidade de negócios em nível organizacional.

Art. 8º O Plano de **Backup** deve conter as rotinas de backup para cada serviço ou recurso que armazene dado digital, cumprindo as diretrizes da Política, definindo requisitos específicos de segurança da informação paras as cópias de segurança realizadas (ex.: controles de acesso lógico, uso de criptografia, armazenamento em local seguro, armazenamento em local remoto seguro diferente do local original etc.).

Art. 9º O Plano de **Backup** deve atender ao **checklist** disposto no Anexo II.

Parágrafo único. Os pontos do **checklist** que não sejam atendidos ou não se aplicarem, devem ser devidamente justificados, considerando o princípio da economicidade e a garantia da continuidade dos negócios.

Art. 10. As rotinas de **backup** devem ser orientadas para a restauração dos dados no menor tempo possível, principalmente quando da indisponibilidade de serviços ou recurso.

Art. 11. As rotinas de **backup** devem possuir requisitos mínimos diferenciados de acordo com o tipo de serviço, recurso ou dado salvaguardado, dando prioridade aos serviços ou recursos críticos da organização.

Art. 12. Os serviços ou recursos críticos do DNIT devem ser formalmente elencados pelo Comitê Gestor de Tecnologia da Informação do DNIT na elaboração do Plano de Continuidade dos negócios.

Art. 13. O **backup** de serviços ou recursos não críticos devem ser formalmente solicitados ao Administrador de **Backup** pelo Proprietário da Informação.

Art. 14. As rotinas de **backup** dos dados referentes aos serviços e recursos críticos e não críticos devem refletir os requisitos de negócio da organização, bem como os requisitos de segurança da informação envolvidos e a criticidade da informação para a continuidade da operação da organização, e devem 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;
VII - requisitos de segurança da informação (criptografia, acessos, etc.); e
VIII - requisitos legais e normativos.

Art. 15. Os incisos I, III, IV, VII e VIII do Art. anterior são vinculados à segurança e criticidade da informação para a continuidade da operação da organização, razão pela qual devem ser definidos pelo Proprietário da Informação, com o apoio técnico do Administrador de **backup**.

.

Seção II
Das ferramentas de backup

Art. 16. As rotinas de **backup** devem utilizar soluções próprias e especializadas para este fim, preferencialmente de forma automatizada.

Art. 17. Os ativos envolvidos no processo de **backup** são considerados ativos críticos para a organização.

Parágrafo único. Compete à CGTI solicitar, a Administração, com as justificativas pertinentes, os equipamentos necessários para manter o parque de ativos sempre atualizado e em quantidade necessária ao atendimento da demanda da Autarquia.

Seção III
Da frequência e retenção dos dados

Art. 18. Os **backups** dos serviços ou recursos críticos do DNIT devem ser realizados utilizando-se as seguintes frequências temporais:

I - diária;
II - semanal;
III - mensal; e
IV - anual.

Parágrafo único. Deverá ser avaliado a necessidade de realização de **backups** com frequência menor que a diária, conforme a criticidade do serviço ou recurso.

Art. 19. Os serviços ou recursos críticos do DNIT devem ser resguardados sob um padrão mínimo, o qual deve observar a correlação frequência/retenção de dados estabelecida a seguir:

I - diária: semanal;
II - semanal: mensal;
III - mensal: 1 ano;
IV - anual: 5 anos.

Art. 20. Os serviços e recursos não críticos do DNIT devem ser resguardados observando-se o padrão mínimo de correlação frequência/retenção de dados estabelecida a seguir:

I - diária: semanal;
II - semanal: mensal;
III - mensal: 6 meses;
IV - anual: 1 anos.

Art. 21. Especificidades dos serviços ou recursos críticos e não críticos podem demandar frequência e tempo de retenção diferenciados, cabendo a devida justificativa na respectiva rotina de **backup**, acordadas entre o Proprietário da Informação e o Administrador de **Backup**.

Art. 22. A recuperação de dados não será viabilizada em caso de perdas anteriores à conclusão da cópia de segurança. Dados criados ou modificados entre execuções de cópias de segurança subsequentes não serão protegidos por soluções de **backup**.

Art. 23. A alteração das frequências e tempos de retenção definidos nesta seção deve ser precedida de solicitação e justificativa formais encaminhadas ao Administrador de **Backup** e acordadas junto ao Proprietário da Informação.

Seção IV
Do uso da rede

Art. 24. O administrador de **backup** deve considerar o impacto da execução das rotinas de **backup** sobre o desempenho da rede de dados do DNIT, garantindo que o tráfego necessário às suas atividades não ocasione indisponibilidade dos demais serviços e recursos de Tecnologia da Informação do DNIT.

Art. 25. A execução do **backup** deve concentrar-se, preferencialmente, no período de janela de **backup**.

Art. 26. O período de janela de **backup** deve ser determinado pelo administrador de **backup** em conjunto com o Proprietário da Informação.

Seção V
Das unidades de armazenamento de backups

Art. 27. 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**.

Art. 28. 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. 29. Podem ser utilizadas técnicas de compressão de dados, contanto que o acréscimo no tempo de recuperação dos dados seja considerado aceitável pelo Proprietário da Informação.

Art. 30. As unidades de armazenamento dos **backups** devem ser acondicionadas em locais apropriados, com controle de fatores ambientais sensíveis, como umidade e temperatura, e com acesso restrito a pessoas autorizadas pelo administrador de **backup**.

Art. 31. Os **backups** podem ser classificados como **on-line, off-line** ou **off-site**, a depender da forma de acesso ao **backup** realizado:

I - **On-line** - uma vez realizado, o **backup** é acessível dentro da rede de dados do DNIT;
II - **Off-line** - uma vez realizado, o **backup** não é acessível em rede, sendo armazenado em mídias físicas removíveis; e
III - **Off-site** - uma vez realizado, o **backup** é armazenado em outro data center, geograficamente separado, ou em serviço de **backup** em nuvem.

Art. 32. Os **backups** devem ter no mínimo duas cópias, realizadas em formatos de mídia distintos, sendo um **on-line** e outro **off-line** ou **off-site.**

Parágrafo único. Os dados considerados críticos devem ser armazenados no mínimo, de forma redundante, ***off-line*** e ***off-site*****.**

Art. 33. **Backups** armazenados em nuvem estão sujeitos à Instrução Normativa nº 5, de 30 de agosto de 2021 e suas atualizações, e à Lei nº 13.709/2018 - Lei Geral de Proteção de Dados Pessoais.

Art. 34. **Backups** com dados sensíveis e que requeiram tratamento específico quanto à segurança da informação devem ser criptografados e ter seus acessos devidamente controlados.

Art. 35. Quando da necessidade de descarte de unidades de armazenamento de **backups**, tais recursos devem ser fisicamente destruídos de forma a inutilizá-los, garantindo a sanitização dos dados, atentando-se ao descarte sustentável e ambientalmente correto.

Seção VI
Dos testes de backup

Art. 36. Os **backups** devem ser testados periodicamente, com o objetivo de garantir a sua confiabilidade e a integridade dos dados salvaguardados.

§ 1º O administrador de **backup** deverá elaborar cronograma de testagem priorizando os **backups** mais importantes para a continuidade das rotinas de trabalho por nível de criticidade (ou relevância) dos dados, aplicações e sistemas, do qual o Proprietário da Informação deve estar ciente e de acordo.

§ 2º A metodologia a ser utilizada para testes será o teste de ***restore***.

§ 3º Realizado o **restore** com sucesso, o Proprietário da Informação deve providenciar os testes de validação da integridade dos dados.

§ 4º Os resultados dos testes sejam adequadamente documentados.

Art. 37. Os testes de restauração dos **backups** devem ser realizados, por amostragem, em equipamentos servidores diferentes dos equipamentos que atendem os ambientes de produção, observados os recursos humanos e tecnológicos disponíveis no DNIT.

Art. 38. A periodicidade, a abrangência, os procedimentos e as rotinas inerentes aos testes de **backup** serão definidos em Plano de **Backup**.

§ 1º A alteração das frequências da realização de testes de **backup** deve ser precedida de solicitação e justificativa formais encaminhadas ao Administrador de **Backup** e acordadas junto ao Proprietário da Informação.

§ 2º Recomenda-se que os testes de restauração (***restore***) dos **backups** dos dados críticos sejam realizados ao menos mensalmente e dos dados não críticos, ao menos semestralmente, haja vista que uma periodicidade superior a essa (realização menos frequente do que uma vez por mês) aumenta o risco para a organização.

CAPÍTULO IV
DAS RESPONSABILIDADES

Art. 39. São atribuições do **administrador de backup**:

I - propor soluções de cópia de segurança das informações digitais corporativas produzidas ou custodiadas no DNIT;

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

III - providenciar a configuração das soluções de **backup**;

IV - providenciar a manutenção das unidades de armazenamento de **backups** preservadas, funcionais e seguras;

V - providenciar a definição dos procedimentos de restauração;

VI - providenciar as medidas preventivas para evitar falhas;

VII - reportar imediatamente a Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos - ETIR os incidentes ou erros que causem indisponibilidade ou impossibilitem a execução ou restauração de **backups**;

VIII - providenciar a disponibilização das informações que subsidiem as decisões referentes à gestão de capacidade relacionada aos **backups**;

IX - propor modificações visando ao aperfeiçoamento da Política de **Backup** e Recuperação de Dados Digitais, objeto desta Instrução Normativa;

X - providenciar a execução dos testes de restauração;

XI - providenciar a elaboração dos procedimentos operacionais;

XII - providenciar a restauração ou recuperação dos **backups** em caso de necessidade, com anuência do Proprietário da Informação;

XIII - providenciar a operação e manuseio das unidades de armazenamento de **backups**;

XIV - providenciar o gerenciamento das mensagens e registros de auditoria (LOGs) diários dos **backups**;

XV - providenciar a verificação diária dos eventos gerados pela solução de **backup**, tomando as providências necessárias para remediação de eventuais falhas;

XVI - sanar dúvidas técnicas do Proprietário da Informação acerca das informações salvaguardadas;

XVII - providenciar a validação, tecnicamente, do resultado das restaurações eventualmente solicitadas; e

XVIII - providenciar a validação, tecnicamente, do resultado dos testes de restauração dos **backups**.

Art. 40. São atribuições dos **Proprietários da Informação**:

I - solicitar, formalmente, a salvaguarda das informações geridas;

II - providenciar a validação, negocialmente, do resultado das restaurações eventualmente solicitadas;

III - providenciar a validação, negocialmente, do resultado dos testes de restauração dos **backups**; e

IV - informar qual o escopo de dados, recursos e ou serviços serão incluídos na rotina de **backup**.

Art. 41. A solicitação de administrador 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.

CAPÍTULO V
DAS DISPOSIÇÕES FINAIS

Art. 42. Esta Instrução Normativa 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 CGTI, as unidades de TI (nas superintendências regionais) e os proprietários das informações tomarão as providências necessárias para a adequação das rotinas e dos procedimentos de **backups** às diretrizes definidas nesta Instrução Normativa.

Parágrafo único. Casos excepcionais não previstos nesta Instrução Normativa serão apresentados pelo administrador de **backup** ao COSIC, que deliberará sobre a questão.

Art. 44. Esta Instrução Normativa entra em vigor no dia 1º de março de 2022.

ANTÔNIO LEITE DOS SANTOS FILHO
Diretor-Geral

ANEXO I
REFERÊNCIAS NORMATIVAS

1. Dispositivos legais e normas técnicas aplicáveis à Política de **Backup**:

I. Portaria nº 1745, de 29 de março de 2021, que institui a Política de Segurança da Informação e Comunicações – POSIC e estabelece as diretrizes para a segurança do manuseio, tratamento e controle e para a proteção dos dados, informações e conhecimentos produzidos, armazenados ou transmitidos, por qualquer meio, pelos

sistemas de informação a serem, obrigatoriamente, observadas na definição de regras operacionais e procedimentos no âmbito do Departamento Nacional de Infraestrutura de Transportes - DNIT;

II. Instrução Normativa GSI/PR Nº 1, de 27 de maio de 2020 e suas alterações e Normas Complementares, do Gabinete de Segurança Institucional da Presidência da República, que disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, e dá outras providências;

III. Portaria GSI/PR Nº 93, de 26 de setembro de 2019, que aprova o Glossário de Segurança da Informação;

IV. Acórdão 1.109/2021-TCU-Plenário, pelo qual foram tecidas análises do Tribunal de Contas da União, que objetivam o constante melhoramento de plano de continuidade de negócio e criação e implantação de política de geração de cópias de segurança dos dados cautelados por esta Autarquia (**backup** e restauração);

V. Norma Técnica ABNT NBR ISO/IEC 27001:2013, que especifica os requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão da segurança da informação dentro da organização;

VI. Norma Técnica ABNT NBR ISO/IEC 27002:2013, que detalha Técnicas de segurança e código de prática para a gestão da segurança da informação; e

VII. Lei nº 13.709/2018 - Lei Geral de Proteção de Dados Pessoais;

VIII. Instrução Normativa nº 22/DNIT SEDE, de 12 de maio de 2021, que dispõe sobre a Estrutura de Gestão da Segurança da Informação no âmbito do Departamento Nacional de Infraestrutura de Transportes – DNIT; e

IX. Instrução Normativa/GSI/PR nº 5, de 30 de agosto de 2021 e suas atualizações, que dispõe sobre os requisitos mínimos de segurança da informação para utilização de soluções de computação em nuvem pelos órgãos e pelas entidades da administração pública federal.

ANEXO II
CHECKLIST PARA VERIFICAÇÃO DE PLANO (OU PROCEDIMENTO/ROTEIRO) DE BACKUP ESPECÍFICO

#	VERIFICAR SE	Sim/Não/ Não se aplica	Observações/ Evidências
1	O plano foi publicado/comunicado para as partes interessadas (titulares dos dados, usuários e gestores dos sistemas etc.)		
2	O plano foi aprovado pelas partes interessadas		
3	O plano registra/define de modo completo e exato a abrangência/escopo das cópias de segurança (ou seja, aquilo que deve ser copiado, incluindo indicações de datas/períodos) Ex.: quais arquivos de dados ou de sistema, quais bases de dados, quais tabelas, quais pastas/folders etc.		
4	O plano estabelece que seja monitorada e documentada a execução do procedimento de geração das cópias de segurança, por meio de registros (logs) relativos a todos		

#	VERIFICAR SE	Sim/Não/ Não se aplica	Observações/ Evidências
	os itens copiados, a fim de detectar eventuais falhas e assegurar que houve a realização integral das cópias de segurança		
5	O plano documenta os procedimentos para realizar a recuperação/restauração (*restore*) das cópias de segurança quando necessário (ou seja, o "como" recuperar os **backups**)		
6	O plano define a frequência de realização das cópias de segurança (ex.: diária, semanal, mensal, anual etc.)		
7	O plano define os tipos de cópias a serem realizadas (completa, incremental ou diferencial)		
8	O plano define o tempo de retenção das cópias de segurança		
9	O plano define requisitos específicos de segurança da informação* (ex.: controles de acesso lógico, uso de criptografia etc.) *Requisitos relativos à confidencialidade, à integridade e à disponibilidade das informações		
10	O plano define a necessidade de armazenamento das cópias de segurança em local seguro e em local remoto seguro diferente do local original		
11	O plano define procedimentos regulares de teste de recuperação/restauração (*restore*) das cópias de segurança, a fim de detectar tempestivamente eventuais falhas lógicas e físicas (nas mídias de armazenamento)		
12	O plano estabelece que a execução dos procedimentos de teste de recuperação/restauração (*restore*) das cópias de segurança seja documentada por meio de registros (logs) relativos a todos os itens restaurados, a fim de detectar eventuais falhas e assegurar que houve a recuperação integral das informações		

(*) Republicado por ter saído com incorreção no Boletim Administrativo nº 021, de 31 de janeiro de 2022.

ATOS DA CORREGEDORIA

PORTARIA Nº 482, DE 28 DE JANEIRO DE 2022

O CORREGEDOR SUBSTITUTO DO DEPARTAMENTO NACIONAL DE INFRA-ESTRUTURA DE TRANSPORTES – DNIT, no uso das atribuições que lhe confere o art. 15, inciso IV, da Estrutura Regimental aprovada pelo Decreto nº 8.489, de 10 de julho de 2015, publicado no Diário Oficial da União nº131, de 13 de julho de 2015; o art. 35, incisos III e IV, do Regimento