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		

#	VERIFICAR SE	Sim/Não/ Não se aplica	Observações/ Evidências
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		