Processo nº 08650.003513/2022-43 SEI nº 42964203

Boletim de Serviço Eletrônico em 09/08/2022

MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA
POLÍCIA RODOVIÁRIA FEDERAL
DIREÇÃO-GERAL

INSTRUÇÃO NORMATIVA PRF Nº 92, DE 08 DE AGOSTO DE 2022

Institui a Política de **backup** das informações eletrônicas, no âmbito da Polícia Rodoviária Federal (PRF).

O DIRETOR-GERAL DA POLÍCIA RODOVIÁRIA FEDERAL, no uso das atribuições que lhe foram conferidas pelo Decreto nº 9.662, de 1º de janeiro de 2019, tendo em vista o disposto no Decreto nº 9.637, de 26 de dezembro de 2018, no Decreto nº 10.222, de 5 de fevereiro de 2020, na Instrução Normativa PRF nº 45, de 2021, bem como o contido nos autos dos processos SEI nº 08650.003513/2022-43 e 08001.003748/2020-18, resolve:

Objeto e âmbito de aplicação

Art. 1º Instituir a Política de **Backup** das informações eletrônicas, no âmbito da Polícia Rodoviária Federal (PRF).

Parágrafo único. A Política de **Backup** tem por objetivo estabelecer diretrizes para o processo de cópia e armazenamento dos dados sob gestão da Diretoria de Tecnologia da Informação e Comunicação (DTIC), visando garantir segurança, integridade e disponibilidade, em conformidade com a Política de Segurança da Informação da PRF (POSIN/PRF).

Art. 2º Para fins desta Instrução Normativa (IN), considera-se:

I - **Backup**: cópia de segurança de dados de um dispositivo de armazenamentos ou sistema para outro ambiente no qual os dados possam ser restaurados em caso de incidente que gere sua indisponibilidade;

II - Restauração (**Restore**): ação de recuperar os dados armazenados em determinado dispositivo durante a rotina de backup, garantindo que todas as informações gravadas estejam intactas;

III - **Backup** Completo (**full**): modalidade de **backup** na qual os dados são copiados em sua totalidade;

IV - **Backup** Diferencial: modalidade de **backup** na qual somente os dados/arquivos novos ou modificados, desde o último backup completo, são copiados;

V - **Backup** Incremental: modalidade de **backup** na qual somente os dados/arquivos novos ou modificados desde o último backup - seja ele completo, diferencial ou incremental - são copiados;

VI - Cliente de **backup**: todo equipamento servidor no qual é instalado o agente de backup;

VII - **Disaster Recovery**: estratégia de recuperação de dados motivada por sinistros de grave amplitude física ou lógica;

VIII - Mídia: meio físico ou virtual no qual efetivamente armazenam-se os dados de um **backup**;

IX - Retenção: período de tempo em que o conteúdo da mídia de **backup** deve ser preservado;

X - Objeto: qualquer dado passível de **backup** e restauração;

XI - Tarefa de **Backup**: procedimento executado sob demanda e/ou de acordo com um agendamento que vincula um ou mais objetos a uma modalidade de **backup** e um período de retenção; e

XII - **Network Operations Center** (NOC): estrutura responsável pelo monitoramento da rede de computadores da PRF.

Papeis e Responsabilidades

Art. 3º Para avaliar e monitorar a qualidade do serviço de backup de dados será designado servidor público para atuar no papel de Dono do Serviço de **Backup**, o qual será responsável por:

I - assegurar que o serviço de **backup** seja gerenciado com foco nas diretrizes estabelecidas nesta norma;

II - prestar contas à Autoridade Máxima de Tecnologia da Informação e Comunicação (TIC) da PRF, no que se refere às entregas do serviço de **backup**;

III - reportar interrupções ou falhas que afetem as entregas contínuas do serviço de **backup**;

IV - representar o serviço de **backup** nas reuniões do Comitê Consultivo de Mudança (CCM) e do Comitê Consultivo de Mudança Emergencial (CCME);

V - identificar e patrocinar a melhoria contínua do serviço; e

VI - gerir, com foco negocial, os ativos que suportam o serviço de backup, sejam físicos ou lógicos.

Art. 4º Para gerir recursos e dados passíveis de **backup**, será designado servidor público para atuar no papel de Administrador de Recurso, o qual será responsável por:

I - conceder permissão ao Administrador de **Backup** para configurar e modificar a ferramenta cliente de **backup**, nos recursos de TIC sob sua gestão, bem como nas modificações necessárias para a correta execução do serviço de **backup**;

II - avaliar o resultado dos procedimentos de restauração executados nos recursos de TIC sob sua gestão;

III - informar ao Administrador do **Backup** as necessidades de alteração nas políticas de uso dos recursos de TIC sob sua gestão; e

IV - solicitar formalmente a inclusão de itens nas políticas de **backup,** na ferramenta de Gestão de Serviços de TIC da PRF (https://suporteadm.prf.gov.br).

Art. 5º Para administrar as atividades de configuração, execução, monitoramento e testes dos procedimentos de **backup** e restauração será designado agente público para atuar no papel de Administrador de **Backup**, o qual será responsável por:

I - propor modificações visando o aperfeiçoamento da política de **backup**;

II - criar e manter as tarefas de **backup**;

III - configurar a ferramenta de **backup** e os clientes;

IV - criar e manter as mídias;

V - testar o **backup** e a restauração;

VI - criar notificações e relatórios;

VII - verificar periodicamente os relatórios gerados pela ferramenta de **backup**;

VIII - restaurar os **backups** em caso de necessidade;

IX - gerenciar mensagens e **logs** diários dos **backups**, fazendo o tratamento dos erros, de forma que o procedimento de **backup** tenha sequência e os erros na sua execução sejam eliminados;

X - realizar manutenções periódicas dos dispositivos (físicos e lógicos) de **backup**;

XI - realizar o carregamento das mídias necessárias para os **backups** programados;

XII - comunicar ao Administrador do Recurso os erros e/ou intercorrências nos procedimentos de **backup**; e

XIII - realizar o armazenamento das mídias de **backup** no recipiente apropriado.

Escopo do Backup e sua Formalização

Art. 6º Todo e qualquer ativo de TIC que armazene dados e que esteja sob responsabilidade da DTIC deverá ser considerado para avaliação de sua inclusão no processo de **backup**.

§ 1º O Administrador do Recurso deverá definir quais diretórios e arquivos serão incluídos no **backup**, tendo como prioridade:

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

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

III - informações e configurações de banco de dados;

IV - conteúdo de repositórios de dados associados a sistemas;

V - arquivos institucionais de usuários (documentos e **e-mails**), exceto quando contratados como serviço do tipo **SaaS**; e

VI - arquivos de aplicações desenvolvidas pela PRF ou de quaisquer outras cuja perda de informações gere prejuízo à PRF.

§ 2º O Administrador de Recurso que pleiteia a inclusão de um cliente de **backup** deverá definir quais diretórios e arquivos não serão incluídos na rotina, tendo como referência:

I - arquivos do sistema operacional ou de aplicações que podem ser colocados por meio de uma nova instalação; e

II - arquivos temporários.

§ 3º Para as aplicações e/ou bancos de dados, devem ser seguidas as recomendações sugeridas pelo desenvolvedor e/ou fabricante, em alinhamento com o requerido pelo Administrador de Recurso.

§ 4º Em nenhuma hipótese será considerado válido o **backup** de réplicas de ativos dos ambientes da PRF.

Art. 7º Os procedimentos de **backup** deverão ser atualizados quando houver:

I - novas aplicações desenvolvidas;

II - novos locais de armazenamento de dados ou arquivos;

III - novas instalações de bancos de dados;

IV - novas aplicações instaladas; e

V - outras informações que necessitem de proteção, as quais deverão ser informadas ao Administrador de **Backup**, pelo Administrador de Recurso.

Art. 8º. As solicitações de criação, alteração ou exclusão de recursos na política e nos procedimentos de **backup** devem ser registradas formalmente na Ferramenta de Gestão de Serviços de TIC (https://suporte.prf.gov.br), devendo constar no mínimo as informações relativas:

I - ao serviço de negócio ou sistema a ser protegido;

II - à identificação da máquina (servidor de aplicação); e

III - aos dados a serem incluídos, tendo por base o disposto no art. 6º.

Parágrafo único. Os procedimentos de **backup** deverão ser configurados na ferramenta, de acordo com as orientações da solicitação.

Retenção dos Dados de Backup

Art. 9º A retenção de **backups** deve observar o ativo de informação a ser protegido, conforme os prazos estabelecidos no Anexo.

§ 1º Expirado o prazo de retenção dos dados armazenados, a mídia poderá ser reutilizada ou destruída, observando sempre seu estado de utilização e número de leitura/gravação.

§ 2º A mídia não deverá ultrapassar 30 anos de armazenamento, devendo, atingido esse prazo, ser copiada para outra mídia, com destruição de forma segura e descarte apropriado, em obediência às leis ambientais.

Art. 10. Sempre que necessário, deverá ser realizada a atualização das mídias de **backup** com a finalidade de preservar o acesso aos dados nelas contidas.

Procedimentos de Backup

Art. 11. A criação e operacionalização dos **backups** deverá obedecer às seguintes regras:

I - criação de **backups**:

a) o **backup** deverá ser programado para execução automática em horários de menor utilização dos sistemas;

b) o **backup** será realizado, preferencialmente, por meio de rede específica para esse fim.

II - operação de **backups**:

a) todo procedimento de **backup** deverá ser monitorado pelo NOC da Central Nacional de Serviços de Tecnologia da Informação e Comunicação (CNST), devendo tais atividades constarem no relatório diário;

b) todos os **backups** realizados devem gerar e enviar extratos automatizados ao Administrador de **Backup**, devendo o envio se dar por e-mail e/ou aplicativos de mensagens instantâneas;

c) no caso de falha nos **backups,** o Operador do NOC deverá abrir chamado na ferramenta de Gestão de Serviços de TIC da PRF, citando o(s) cliente(s) de **backup** e se foi adotada ação corretiva, ficando a cargo do Administrador de **Backup** tratar as falhas remanescentes.

Art. 12. Os **backups** serão realizados preferencialmente:

I - **backups** diários: de segunda à sexta-feira, entre 00h e 06h do dia posterior, em modo incremental;

II - **backups** semanais: nos finais de semana, iniciando aos sábados, em modo incremental; e

III - **backups** mensais: nos finais de semana, iniciando aos sábados, sendo dispensada a realização de backups semanais quando coincidentes.

Art. 13. Todo sistema/serviço a ser descontinuado deverá ser submetido a um **backup full** e sua retenção deverá ser de, no mínimo, um ano.

Parágrafo único. O Administrador do Recurso poderá solicitar ampliação do prazo de retenção previsto no **caput**, ficando a cargo do Comitê de Governança Digital aprovar o pedido.

Armazenamento e Descarte das Mídias

Art. 14. Todas as cópias de segurança devem ser guardadas em local seguro, cujos acessos (físicos e lógicos) devem ser restritos ao Dono do Serviço de **Backup** e ao Administrador de **Backup**.

Art. 15. O armazenamento das mídias de **backups** deve ser protegido contra agentes nocivos naturais (poeira, calor, umidade), devendo ainda ter proteção contra incêndio e manutenção das condições de temperatura, umidade e pressão recomendadas pelo fabricante.

Art. 16. O armazenamento dos **backups** poderá ser feito em fitas, discos ou na plataforma de nuvem contratada pela PRF.

Art. 17. As mídias devem ser etiquetadas, contendo o código de identificação e outras informações relacionadas ao ativo, como data e hora do **backup** e tipo de **backup** efetuado.

Art. 18. As mídias de **backup** a serem descartadas devem ser eliminadas de forma segura e protegida, por meio de incineração, trituração, quebra, execução de procedimentos de sobrescrita de dados remanescentes (disco rígido) ou outro procedimento que impossibilite a recuperação dos dados.

Teste e Prevenção do Processo de Restauração

Art. 19. O Administrador de **Backup** coordenará as atividades de restauração de dados, podendo envolver os demais atores necessários à realização de testes periódicos e averiguar o alcance dos objetivos do processo para identificar e propor melhorias.

§ 1º As políticas de **backup** devem ser testadas, ao menos, anualmente para garantir sua confiabilidade.

§ 2º Para sistemas/serviços críticos, os testes referentes às suas respectivas políticas de **backup** deverão ser realizados trimestralmente.

§ 3º Os testes de **restore** devem ser adequadamente documentados, informando no mínimo o tipo de sistema/serviço que teve o seu restabelecimento testado, a data da realização do teste, o tempo gasto para o retorno do **backup** e se o procedimento foi concluído com sucesso.

§ 4º Os **backups** devem ser restaurados em ambientes de teste distintos dos de produção, visando sua validação.

§ 5º Um **backup** será considerado válido quando o ambiente original puder ser recriado de forma consistente.

§ 6º Sempre que determinado procedimento de **backup** for alterado, deve ser feito o teste de **restore**.

§ 7º Em caso de falha na restauração, o Administrador de **Backup** deverá informar

à Coordenação de Infraestrutura e Aplicações para que sejam tomadas providências para a correção da falha.

§ 8º Para cada teste realizado deve ser gerado um relatório a ser enviado ao Diretor de Tecnologia da Informação e Comunicação quando de sua finalização.

Disposições Finais

Art. 20. Mediante solicitação da Diretoria de Tecnologia da Informação ou da gestão negocial, poderão ser definidos pelo Comitê Gestor de Segurança da Informação (CGSI) períodos de retenção de dados diferentes do padrão estabelecido por esta IN, para sistema ou serviço específico.

Art. 21. Deverão ser precedidos da realização do **backup** dos dados quaisquer procedimentos programados para equipamentos servidores e dispositivos de armazenamento que impliquem em riscos no seu funcionamento.

Art. 22. Esta Instrução Normativa entra em vigor em 1º de setembro de 2022.

SILVINEI VASQUES

PRF

Documento assinado eletronicamente por **SILVINEI VASQUES**, **Diretor-Geral**, em 08/08/2022, às 18:42, horário oficial de Brasília, com fundamento no art. 10, § 2º, da Medida Provisória nº 2.200-2, de 24 de agosto de 2001, no art. 4º, § 3º, do Decreto nº 10.543, de 13 de novembro de 2020, e no art. 42 da Instrução Normativa nº 116/DG/PRF, de 16 de fevereiro de 2018.

A autenticidade deste documento pode ser conferida no site https://sei.prf.gov.br/verificar, informando o código verificador **42964203** e o código CRC **A13E514D**.

ANEXO DA INSTRUÇÃO NORMATIVA PRF Nº 92, DE 08 DE AGOSTO DE 2022
PRAZOS DE RENTENÇÃO DOS DADOS DE BACKUP

Ativo de Informação: **Banco de Dados**			
Ambiente	**Estratégia de Backup**	**Retenção**	**Tipo de Backup**
Produção	Backup completo: semanal; Backup incremental: diário.	Backup Completo: 20 (vinte) dias em disco e 6 meses em fita (ou outro meio de armazenamento compatível) Backup incremental: 10 (dez) dias em disco	Estrutura lógica e dados
Homologação	Backup completo: semanal; Backup incremental: diário.	Backup Completo: 10 (dez) dias em disco e 1 (um) mês em fita (ou outro meio de armazenamento compatível) Backup incremental: 1 (uma) semana em disco.	Estrutura lógica e dados
Desenvolvimento	Backup completo: semanal. Backup incremental: diário.	Backup Completo: 10 (dez) dias em disco e 01 (um) mês em fita (ou outro meio de armazenamento compatível) Backup incremental: 01 (uma) semana em disco	Estrutura lógica

Ativo de Informação: **Servidor de Arquivos**			
Ambiente	**Estratégia de Backup**	**Retenção**	**Tipo de Backup**
Produção	Backup Completo: Semanal e Mensal Backup diferencial: diário	Backup Completo semanal: 2 (duas) semanas em disco e 2 (dois) meses em fita (ou outro meio de armazenamento compatível). Backup Completo mensal: 2 (duas) semanas em disco e 1 (um) ano em fita. Backup diferencial: 1 (uma) semana em disco.	Sistema de Arquivos

Ativo de Informação: **Máquinas Virtuais**			
Ambiente	**Estratégia de Backup**	**Retenção**	**Tipo de Backup**
Produção	Backup Completo: Semanal; Backup diferencial: diário.	Backup Completo: 03 (três) meses em disco; Backup diferencial: 01 mês em disco	Imagem das máquinas virtuais
Homologação	Backup Completo: Semanal; Backup diferencial: diário.	Backup Completo: 03 (três) meses em disco; Backup diferencial 01 mês em disco	Imagem das máquinas virtuais
Desenvolvimento	Backup Completo: Semanal; Backup diferencial: diário.	Backup completo: 01 (um) mês em disco; Backup diferencial 01 mês em disco.	Imagem das máquinas virtuais

Criado por rafael.duclou, versão 3 por rafael.duclou em 08/08/2022 09:50:15.