MINISTÉRIO DO TRABALHO E EMPREGO
Secretaria-Executiva
Diretoria de Tecnologia da Informação

PORTARIA DTI/SE/MTE Nº 2385, DE 04 DE JULHO DE 2023

Dispõe sobre as diretrizes e os procedimentos para a realização de cópia de segurança e restauração de dados no âmbito do Ministério do Trabalho e Emprego.

O DIRETOR DE TECNOLOGIA DA INFORMAÇÃO, no uso das atribuições que lhe conferem os incisos VII e VIII do art. 17, do Decreto nº 11.359, de 1º de janeiro de 2023, e tendo em vista o disposto no Decreto nº 9.637, de 26 de dezembro de 2018, e na Instrução Normativa GSI/PR nº 3, de 28 de maio de 2021, **RESOLVE:**

CAPÍTULO I
DAS DISPOSIÇÕES GERAIS

Art. 1º Estabelecer as diretrizes e os procedimentos para cópia de segurança e restauração de dados no âmbito do Ministério do Trabalho e Emprego.

Art. 2º Esta Portaria se aplica aos procedimentos de cópias de segurança, armazenamento, testes e recuperação de dados sob a guarda da Diretoria de Tecnologia da Informação, visando garantir a segurança, disponibilidade, integridade, confiabilidade e autenticidade, em conformidade com a Política de Segurança da Informação.

Art. 3º Tal instrumento aplica-se a todos os sistemas, bases de dados e repositórios de arquivos institucionais, em formato digital, em uso e de propriedade do Ministério, no âmbito de todos os órgãos de assistência direta e imediata ao Ministro de Estado, aos órgãos específicos singulares e às unidades descentralizadas.

Art. 4º Deverá ser elaborado um Plano de Backup, conforme requisitos presentes nesta Portaria, para todos os sistemas, bases de dados, servidores físicos ou virtuais e repositórios de arquivos institucionais do Ministério que serão objeto de cópias de segurança, refletindo 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

Art. 5º Não serão salvaguardados nem recuperados dados armazenados localmente, nos microcomputadores dos usuários ou em quaisquer outros dispositivos fora dos centros de processamento de dados mantidos pelo Ministério ou que não façam parte de um plano de backup formalmente definido, cabendo ao administrador de backup a prerrogativa de negar solicitações neste sentido.

Art. 6º A salvaguarda dos dados em formato digital pertencentes ao Ministério, mas custodiados por outras entidades, públicas ou privadas, como nos casos de serviços em nuvem, devem estar garantidos nos acordos ou contratos que formalizam a relação entre os envolvidos.

Art. 7º Para os efeitos desta Portaria, aplicam-se os termos do Glossário de Segurança da

Informação, aprovado pela Portaria GSI/PR nº 93, de 18 de outubro de 2021, e, em complemento, os seguintes termos:

I - administrador de backup: pessoa responsável pelos procedimentos de configuração, execução, monitoramento, elaboração de padrões, atendimentos avançados, resolução de incidentes, testes dos procedimentos de backup e restauração. Deve ser designado entre os empregados ou servidores públicos da Coordenação-Geral de Infraestrutura da Diretoria de Tecnologia da Informação, com formação ou capacitação técnica compatível às suas atribuições;

II - backup completo (full): 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;

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

IV - backup incremental: modalidade de backup na qual somente os arquivos novos ou modificados desde o último backup – seja ele completo, diferencial ou incremental – são salvaguardados;

V - código fonte: é o conjunto de palavras ou símbolos escritos de forma ordenada, contendo instruções em uma das linguagens de programação existentes, de maneira lógica;

VI - criticidade: grau de importância da informação para a continuidade das atividades e serviços;

VII - dado: informação preparada para ser processada, operada e transmitida por um sistema ou programa de computador;

VIII - gestor da informação: agente público formalmente responsável pela administração do serviço de TI/sistema e pelas informações produzidas em seu processo de trabalho. Preferencialmente, deve ser um gestor da área negocial;

IX - janela de backup: intervalo de tempo durante o qual as cópias de segurança sob execução agendada ou manual poderão ser executadas;

X - nuvem: uma vasta rede de servidores remotos ao redor do globo que são conectados e operam como um único ecossistema. Estes servidores são responsáveis por armazenar e gerenciar dados, executar aplicativos ou fornecer serviços ou conteúdos, que podem ser acessados de qualquer dispositivo com acesso à Internet;

XI - plano de backup: Documento formal onde são definidos os responsáveis pela cópia dos dados, o que será armazenado, periodicidade de execução da cópia e tempo de retenção, de acordo com as orientações da Política de Backup;

XII - repositório de arquivo: Conjunto de documentos ou lugar onde os documentos são guardados;

XIII - retenção: intervalo de tempo pelo qual os dados devem ser salvaguardados e estar aptos à restauração; e

XIV - rotina de backup: procedimentos de realização de cópias de segurança.

CAPÍTULO II
DAS RESPONSABILIDADES

Art. 8º São atribuições do administrador de backup:

I – propor soluções de cópia de segurança das informações digitais corporativas produzidas ou custodiadas pelo Ministério;

II – providenciar a criação e manutenção dos backups;

III – providenciar a configuração das soluções de backup;

IV – manter as unidades de armazenamento de backups preservadas, funcionais e seguras;

V – definir os procedimentos de restauração e neles auxiliar;

VI – verificar os eventos gerados pela solução de backup, tomando as providências necessárias para remediação de eventuais falhas;

VII – tomar medidas preventivas para evitar falhas;

VIII – reportar imediatamente à chefia imediata os incidentes ou erros que causem indisponibilidade ou impossibilitem a execução ou restauração de backups;

IX – gerenciar mensagens e registros de auditoria (LOGs) de execução dos backups;

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

XI – solicitar restaurações de dados, com anuência do gestor da informação;

XII – propor modificações visando ao aperfeiçoamento desta Portaria; e

XIII – providenciar a execução dos testes de restauração.

Parágrafo único. O administrador de backup poderá contar com auxílio de equipe técnica especializada, composta por servidores ou terceirizados, para execução de suas atribuições.

Art. 9º São atribuições dos gestores da informação:

I – solicitar, formalmente, a salvaguarda das informações geridas e dar anuência à solicitação feita pelo administrador de backup 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.

CAPÍTULO III
DOS PROCEDIMENTOS

Seção I
Da Solicitação

Art. 10. As solicitações para análise de viabilidade de backup devem ser realizadas pelo gestor da informação, por meio de abertura de chamado em ferramenta institucional, e enviadas ao administrador de backup.

Art. 11. O administrador de backup analisará a solicitação de viabilidade de backup.

§1º Não sendo viável o atendimento da solicitação, o administrador de backup encaminhará, por meio de resposta ao chamado em análise, resposta ao gestor da informação.

§2º Sendo viável o atendimento, o administrador de backup deverá elaborar o Plano de Backup em conjunto com o gestor da informação, de modo a atender as necessidades específicas de negócio.

§3º O Plano de Backup deverá ser assinado pelo gestor da informação e pelo administrador do backup e inserido no chamado em análise.

§4º Após a inclusão do Plano de Backup devidamente assinado, o chamado poderá ser encerrado.

Art. 12. O administrador de backup, caso identifique a necessidade de guarda de informação, pode entrar em contato com o gestor da informação para a elaboração, em conjunto, do Plano de Backup.

Art. 13. O Plano de Backup deverá conter, no mínimo, as seguintes informações:

I – escopo: dados digitais a serem salvaguardados, com apontamento do local, tais como:

a) código fonte;

b) banco de dados;

c) repositório de arquivos;

d) arquivos de configuração de servidores e ativos de rede; e

e) máquinas virtuais.

II – tipo de backup: completo, incremental, diferencial, podendo ser uma associação destes;

III – frequência temporal de realização do backup: diária, semanal, mensal, anual, podendo ser uma associação destes;

IV – retenção: período em que o dado copiado no backup ficará retido e disponível para uso numa eventual recuperação antes de ser substituído por uma versão mais nova. Deverá ser definido com base na criticidade, frequência da atualização dos dados e características específicas de cada sistema;

V – unidade de armazenamento: indicação da unidade de armazenamento a ser utilizada, podendo ser storage, fita ou outras unidades em uso no Ministério;

VI – local de armazenamento: indicação da localização de armazenamento do backup, incluindo se o backup é acessível por meio da rede, se não é acessível pela rede ou se a unidade de armazenamento se encontra em outra localidade remota, sendo em serviço de nuvem ou em edifício distinto do Ministério;

VII – testes previstos: devem ser previstos a periodicidade, a abrangência e os procedimentos relativos aos testes que serão realizados;

VIII – procedimento de recuperação: documentar o procedimento para recuperar o backup quando necessário;

IX – logs: previsão de criação e armazenamento de registros sobre a execução dos testes e das recuperações realizadas, a fim de detectar eventuais falhas e assegurar que houve a realização integral do backup;

X – RPO (Recovery Point Objective): indicador que mensura o prazo máximo de perda de dados em caso de incidentes; e

XI – RTO (Recovery Time Objective): indicador que mensura o tempo máximo em que um sistema ou uma informação pode ficar indisponível após um incidente.

Art. 14. Os backups devem ter, no mínimo, duas cópias realizadas em unidades de armazenamento distintos, sendo um online e outro offline ou disposto em outra localidade .

Art. 15. 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.

Seção II

Das Rotinas de Backup

Art. 16. As rotinas de backup, devem ser orientadas para a restauração dos dados no menor tempo possível, principalmente quando um incidente ocasionar indisponibilidade de serviços de TI.

Art. 17. As rotinas de backup devem possuir requisitos mínimos diferenciados de acordo com o tipo de serviço de TI ou dado salvaguardado, dando prioridade aos serviços de TI críticos da organização, conforme Plano de Backup.

Art. 18. Os backups devem estar em conformidade com a legislação vigente, em especial no que compete à Lei Geral de Proteção de Dados Pessoais.

Art. 19. Os backups devem ser realizados conforme previsto no Plano de Backup, preferencialmente criptografados, considerando as melhores práticas de mercado e normas vigentes.

Art. 20. As rotinas de backup devem utilizar soluções próprias e especializadas para este fim, preferencialmente de forma automatizada.

Art. 21. Os ativos envolvidos no processo de backup são considerados ativos críticos para a

organização.

Art. 22. O administrador de backup deve considerar o impacto da execução das rotinas de backup sobre o desempenho da rede de dados do Ministério, garantindo que o tráfego necessário às suas atividades não ocasione problemas aos demais serviços de TI.

Art. 23. A execução do backup deve se concentrar, preferencialmente, no período de janela de backup, a ser definido pela Diretoria de Tecnologia da Informação.

Art. 24. 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.

Seção III

Do Armazenamento de Backup

Art. 25. 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; e

VI – a vida útil da unidade de armazenamento de backup.

Art. 26. 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. 27. Todos os ativos relacionados ao armazenamento dos backups devem ser acondicionados 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. 28. Quando da necessidade de descarte de unidades de armazenamento de backups, tais recursos devem ser fisicamente destruídos de forma a inutilizá-los, atentando-se ao descarte sustentável e ambientalmente correto.

Seção IV

Dos Testes de Backup

Art. 29. Os backups devem ser testados periodicamente, com o objetivo de garantir a sua confiabilidade, a integridade dos dados salvaguardados e atestar seu funcionamento em caso de necessidade.

Art. 30. 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. 31. A periodicidade, a abrangência, os procedimentos e as rotinas inerentes aos testes de backup devem ser devidamente registradas no plano de backup.

Seção V

Da Restauração de Backup

Art. 32. A solicitação de restauração de dados que tenham sido salvaguardados deve ser realizada por meio por meio de abertura de chamado em ferramenta institucional e depende de prévia e formal autorização do respectivo gestor da informação.

Art. 33. Caso o administrador de backup detecte a necessidade de restauração, deve entrar em contato com o gestor da informação e obter a anuência para a realização do procedimento.

Art. 34. Deverá ser mantido registro de todos os procedimentos adotados para a restauração do backup, juntamente com as informações do solicitante.

CAPÍTULO IV

DISPOSIÇÕES FINAIS

Art. 35. Os planos de backup deverão ser atualizados sempre que necessário e revisados no mínimo a cada 12 meses.

Art. 36. A não observância do disposto nesta Portaria sujeita o infrator à aplicação de sanções administrativas conforme a legislação vigente, sem prejuízo das responsabilidades penal e civil, assegurados sempre aos envolvidos o contraditório e a ampla defesa.

Art. 37. Esta Portaria entra em vigor na data de sua publicação.

HEBER FIALHO MAIA JUNIOR
Diretor de Tecnologia da Informação

Documento assinado eletronicamente por **Heber Fialho Maia junior**, **Diretor(a)**, em 07/07/2023, às 16:56, 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 deste documento pode ser conferida no site https://sei.economia.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **35408657** e o código CRC **A17CD3B7**.

Referência: Processo nº 19958.101571/2023-84. SEI nº 35408657