PORTARIA TRT 18ª GP/SGGOVE Nº 1094/2020

PODER JUDICIÁRIO DA UNIÃO
TRIBUNAL REGIONAL DO TRABALHO DA 18ª REGIÃO

** Texto compilado até as alterações promovidas pela Portaria SGP/CSIN nº 721/2024*

Institui norma para a realização de cópias de segurança (*backup*), restauração e testes de restauração de dados em meio digital, no âmbito do Tribunal Regional do Trabalho da 18ª Região.

O DESEMBARGADOR-PRESIDENTE DO TRIBUNAL REGIONAL DO TRABALHO DA 18ª REGIÃO, no uso de suas atribuições legais e regimentais, tendo em vista o que consta do Processo Administrativo nº 8297/2015,

CONSIDERANDO a Resolução Administrativa TRT 18ª nº 145/2019, que Institui a Política de Segurança da Informação do Tribunal Regional do Trabalho da 18ª Região;

CONSIDERANDO o objetivo de controle "12.3 Cópias de segurança" da norma ABNT ISO/IEC 27002:2013 (código de prática para controles de segurança da Informação),

RESOLVE:

CAPÍTULO I
DAS DISPOSIÇÕES GERAIS

Art. 1º Esta Portaria institui normas para a realização de cópias de segurança (*backup*), restauração e testes de restauração de dados.

§ 1º Aplica-se o disposto nesta Portaria aos dados armazenados em meio digital produzidos ou manipulados no exercício das atividades do Tribunal Regional do Trabalho da 18ª Região e aos agentes responsáveis por esta produção ou manipulação. ***(Parágrafo único transformado em § 1º pela Portaria SGP/CSIN nº 721/2024)***

§ 2º No contexto desta Portaria, considera-se o termo "dados" no sentido de dados e sistemas (softwares aplicativos, sistemas operacionais, imagens

de servidores e demais artefatos de software necessários ao tratamento de dados). ***(Parágrafo incluído pela Portaria SGP/CSIN nº 721/2024)***

Art. 2º Para os fins desta Portaria, consideram-se as definições constantes do art. 2º da Resolução Administrativa TRT18 nº 145/2019 e as seguintes:

I – administrador de *backup*: pessoa ou grupo responsável por atividades de planejamento e operação das atividades de *backup*, de acordo com a categoria de *backup* que administre;

II – *backup*: cópia de segurança de arquivos e dados;

III – categoria de *backup*: nome atribuído a um procedimento que uniformiza a cópia dos dados associados a um determinado grupo de ativos de informação (e-mail, servidores de arquivos, bancos de dados Oracle, bancos de dados PostgreSQL, computadores de usuários etc);

IV – equipe de backup: equipe composta pelo gerente e administradores de backup;

V – gerente de *backup*: pessoa responsável pela coordenação das atividades de *backup* executadas e planejadas em conjunto com os administradores de *backup*;

VI – local de armazenamento: espaço de armazenamento lógico na mídia em que os dados serão gravados;

VII – mídia: dispositivo de armazenamento de dados, podendo ser disco, fita, ou outro meio de armazenamento;

VIII – período de retenção: período de tempo em que os dados gravados não podem ser apagados;

IX – repositório: local de guarda das mídias, podendo ser o cofre ou outro local apropriado;

X – restauração: procedimento por meio do qual as informações contidas no *backup* são recuperadas e disponibilizadas para uso;

XI – teste de restauração: procedimento que visa a testar a efetividade das cópias de segurança.

Art. 3º Deverão ser definidos procedimentos de *backup*, restauração e testes de restauração de dados. ***(Artigo incluído pela Portaria SGP/CSIN nº***

721/2024)

Art. 4º Os procedimentos de *backup* devem definir requisitos específicos de segurança da informação para as cópias realizadas, a exemplo de controles de acesso lógico, uso de criptografia, armazenamento em local seguro e/ou em local remoto diferente do local de origem. ***(Artigo incluído pela Portaria SGP/CSIN nº 721/2024)***

Art. 5º Os procedimentos de *backup* devem definir o tipo (exemplo: incremental, diferencial ou *full*) e a abrangência/escopo das cópias de segurança de dados, ou seja, o que deve ser copiado, incluindo indicações de datas/períodos. ***(Artigo incluído pela Portaria SGP/CSIN nº 721/2024)***

Art. 6º Em cada procedimento de backup deve-se definir a frequência (diária, semanal, mensal etc.) de realização das cópias de segurança. ***(Artigo incluído pela Portaria SGP/CSIN nº 721/2024)***

Art. 7º Devem ser definidos, em cada procedimento de backup, o tempo de retenção das cópias de segurança, seja este baseado em requisitos de negócio ou em requisitos legais. ***(Artigo incluído pela Portaria SGP/CSIN nº 721/2024)***

CAPÍTULO II
DAS COMPETÊNCIAS

Art. 8º Compete à Administração disponibilizar à equipe de *backup* os recursos humanos, físicos e computacionais adequados para garantir a efetividade desta Portaria.

Art. 9º Compete aos usuários dos sistemas de informação manter os dados em locais de armazenamento compatíveis com sua categorização, de forma que tenham o tratamento devido.

Art. 10. Compete ao gerente de *backup*:

I – coordenar as atividades de planejamento, operação e testes do *backup*, atuando como ponto de convergência dos administradores de *backup*;

II – garantir a elaboração e a atualização dos procedimentos de *backup* e restauração de dados, bem como da documentação mencionada no art. 12;

III – aprovar os procedimentos pertinentes à operacionalização do *backup*;

IV – solicitar recursos para as operações de *backup*;

V - solicitar informações a instâncias superiores e a gestores de ativos, de modo a viabilizar a elaboração da documentação indicada no art. 12.

Art. 11. Compete aos administradores de *backup*, no que concerne às categorias de *backup* que administrem:

I – planejar e operacionalizar o *backup* de dados;

II – elaborar e manter a documentação de *backup* atualizada e em conformidade com os normativos pertinentes;

III – efetuar e registrar testes de restauração;

IV – atender e registrar os chamados técnicos de restauração.

CAPÍTULO III
DA DOCUMENTAÇÃO

Art. 12. A unidade de Tecnologia da Informação e Comunicação deve elaborar, bem como manter atualizada e em local padronizado a documentação referente aos seguintes aspectos do *backup*:

I – procedimentos de cópia, restauração e testes de restauração de dados referentes a cada categoria de *backup*, levando em consideração os seguintes aspectos:

a) as informações elegíveis a *backup*;

b) o tipo, a abrangência/escopo, a frequência da geração das cópias, a periodicidade de realização e a abrangência dos testes de restauração devem refletir os requisitos de negócio da organização (por exemplo, período de retenção dos dados), além dos requisitos de segurança da informação envolvidos e a criticidade da informação para a continuidade da operação da organização; ***(Alínea alterada pela Portaria SGP/CSIN nº 721/2024)***

II – identificação, guarda, transporte e controle da vida útil das mídias;

III – solicitações de inclusão de novos sistemas ou dados no planejamento do *backup*;

IV - fluxos do processo de *backup*, testes e restauração de dados a serem deliberados pela Comissão de Gestão de TIC como norma de cumprimento

obrigatório.

Parágrafo único. As solicitações referidas no inciso III deste artigo serão recebidas em processo administrativo para deliberação por parte da Comissão de Gestão de TIC e, na escassez de recursos que viabilizem o pleito, pelo Comitê de Governança e Gestão Participativa, e devem conter ao menos o volume de dados a ser guardado, o período de retenção pretendido e uma estimativa percentual de crescimento anual dos dados a serem copiados.

Art. 13. Deverão ser mantidos registros das operações de *backup*, restauração de dados e testes de restauração de dados, com detalhamento suficiente para evidenciar tais operações e por tempo compatível com o período de retenção atribuída aos dados.

CAPÍTULO IV
DO MONITORAMENTO E DA MEDIÇÃO

Art. 14. O processo de realização das cópias de segurança deve garantir que registros completos e exatos da operação sejam gerados e mantidos em base de dados para fins de monitoramento e medição de eficácia.

Art. 15. A documentação de que trata o art. 12 deverá apontar, em seção específica, indicadores que serão acompanhados periodicamente, incluindo inicialmente a porcentagem de operações de *backup* realizadas com sucesso e a porcentagem de testes de restauração realizados com sucesso.

CAPÍTULO V
DO ARMAZENAMENTO E DA SEGURANÇA

Art. 16. As cópias de segurança devem ser armazenadas em uma localidade remota, a uma distância suficiente para escapar dos danos de um desastre ocorrido no local principal, sendo admissível o armazenamento em nuvem. ***(Artigo alterado pela Portaria SGP/CSIN nº 721/2024)***

Art. 17. As cópias de segurança devem possuir um nível apropriado de proteção física, lógica e ambiental, consistentes com as normas aplicadas na instalação principal.

CAPÍTULO VI
DOS TESTES DE RESTAURAÇÃO DOS DADOS

Art. 18. A unidade de Tecnologia da Informação e Comunicação deve

realizar testes de restauração e manter registros desses testes.

Art. 19. Os testes de restauração devem ser realizados em ambiente reservado para essa finalidade, não sobrepondo o conteúdo existente no local original de armazenamento.

Art. 20. Caso ocorra falha no teste, o administrador de *backup* deverá tomar as medidas necessárias à correção do problema.

CAPÍTULO VII
DAS DISPOSIÇÕES FINAIS

Art. 21. O gerente e os administradores de *backup* serão designados pelo gestor da unidade de Tecnologia da Informação e Comunicação.

Art. 22. Esta Portaria entra em vigor na data de sua publicação, revogando-se a Portaria GP/NGTIC n° 014/2015.

Publique-se no Diário Eletrônico da Justiça do Trabalho.

(assinado eletronicamente)
PAULO PIMENTA
Desembargador-Presidente
TRT da 18ª Região