ATO TRT13 SGP N.º 067, DE 18 DE ABRIL DE 2023

Dispõe sobre normas e procedimentos para a realização de cópias de segurança de dados (backup) no âmbito do Tribunal Regional do Trabalho da 13ª Região.

O DESEMBARGADOR PRESIDENTE DO TRIBUNAL REGIONAL DO TRABALHO DA DÉCIMA TERCEIRA REGIÃO, no uso de suas atribuições legais e regimentais, e nos termos do PROAD n.º 2971/2023,

CONSIDERANDO a necessidade de atualizar normas e procedimentos relacionados à realização de cópias de segurança de dados na instituição;

CONSIDERANDO a necessidade de promover a integridade e disponibilidade das informações no âmbito deste Tribunal;

CONSIDERANDO que a perda de informações computacionais pode significar prejuízo à prestação jurisdicional por meio da paralisação de atividades essenciais do Tribunal;

CONSIDERANDO que a realização de cópias de segurança é fundamental para a continuidade da prestação jurisdicional em caso de perda de dados ou desastres;

RESOLVE:

Art. 1º Regulamentar a realização de cópias de segurança de dados no âmbito do Tribunal Regional do Trabalho da 13ª Região.

Art. 2º Este Ato integra a estrutura normativa da Segurança da Informação deste Tribunal.

Art. 3º Para efeitos deste Ato, aplicam-se as definições da Política de Segurança da Informação e Comunicações e da Política de Proteção de Dados Pessoais, além das seguintes:

I - backup: cópia de segurança de dados armazenados em recursos de TIC; e

II - mídia de backup: meio físico no qual é armazenado um backup.

Art. 4º As disposições deste Ato aplicam-se a todos os usuários internos e externos do Tribunal Regional do Trabalho da 13ª Região, conforme disposto na Política de Segurança da Informação e Comunicações da instituição, devendo ser rigorosamente observadas, sob pena de responsabilidade.

Art. 5º A frequência, o tipo e o tempo de retenção dos backups gerados serão definidos pela unidade gestora de TIC em conjunto com a área negocial, considerando os requisitos legais e a criticidade dos dados envolvidos em relação às atividades da instituição e à disponibilidade de recursos de infraestrutura de TIC.

Art. 6º As mídias de backup devem ser armazenadas em um local seguro, que possua um nível apropriado de proteção física, lógica e ambiental.

§1º As mídias de cópia de segurança devem ser mantidas em uma localidade remota, que possua um nível apropriado de proteção física, lógica e ambiental, além de uma distância suficiente do local principal de armazenamento.

§2º As cópias de segurança que possuem dados sensíveis devem ser protegidas por criptografia ou controle de acesso físico e lógico restritos.

Art. 7º O transporte e o descarte de mídias de backup devem ser realizados de forma segura para evitar a obtenção de dados por pessoas não autorizadas.

Art. 8º Os procedimentos de recuperação de backups devem ser verificados regularmente, de forma a garantir que estes são efetivos e que podem ser concluídos dentro dos prazos definidos nos procedimentos operacionais de recuperação.

Parágrafo Único. Os testes de recuperação do backup completo das bases de dados dos sistemas considerados críticos devem ser realizados ao menos uma vez por ano, e os resultados divulgados.

Art. 9º Para sistemas críticos, os procedimentos de backup devem abranger todas as aplicações, dados, configurações e informações essenciais para a completa recuperação do sistema em caso de necessidade.

Art. 10. Para serviços em nuvem, devem ser realizados backups de informações, aplicações e sistemas da instituição no ambiente de serviços em nuvem, sendo avaliado se os requisitos desta norma são atendidos pelo serviço de backup fornecido como parte do serviço em nuvem.

Art. 11. Sempre que possível, os procedimentos de backup devem ser automatizados, minimizando erros e facilitando o processo de geração e recuperação das cópias.

Art. 12. Somente serão realizados backups de dados de usuários armazenados nos locais/serviços divulgados pela unidade gestora de TIC do Tribunal.

Parágrafo Único. Não serão realizados backups de dados armazenados em estações de trabalho (computadores, notebooks, smartphones, tablets, etc), assim como em dispositivos de armazenamento portáteis (pen drives, discos externos, etc) e em equipamentos não registrados como patrimônio do Tribunal.

Art. 13. Compete à unidade gestora de TIC do Tribunal:

I - documentar, implementar e executar a política e os planos/procedimentos /roteiros de backup;

II - supervisionar o armazenamento, transporte e descarte das mídias de backup;

III - implementar e gerenciar os recursos de tecnologia da informação relacionados à realização de backups;

IV - implementar os requisitos específicos de segurança da informação paras as cópias de segurança realizadas;

V - realizar testes periódicos de recuperação de backups, visando garantir que as cópias geradas são confiáveis para uso em caso de necessidade; e

VI - buscar a otimização das rotinas, recursos e janelas de backup.

Art. 14. Solicitações para realização ou recuperação de backups deverão ser encaminhadas, via chamado eletrônico, à unidade gestora de TIC do Tribunal pelo gestor da unidade do usuário solicitante.

Art. 15. A unidade gestora de TIC do Tribunal deverá comunicar qualquer irregularidade ao Comitê Gestor de Segurança da Informação, a fim de que sejam tomadas as providências cabíveis.

Art. 16. Compete à chefia imediata do usuário verificar a observância das disposições deste Ato no âmbito de sua unidade, comunicando ao Comitê Gestor de Segurança da Informação as irregularidades.

Art. 17. Os casos omissos ou que suscitam dúvidas serão dirimidos pelo Comitê Gestor de Segurança da Informação.

Art. 18. Revoga-se o ATO TRT SGP Nº 073/2020.

Art. 19. O presente Ato entra em vigor a partir da data de sua publicação.

Cientifique-se.
Publique-se no DEJT-Adm.

THIAGO DE OLIVEIRA ANDRADE
Desembargador Presidente