Poder Judiciário
Justiça do Trabalho
Tribunal Regional do Trabalho da 13ª Região

ATO TRT SGP N.º 73, DE 18 DE JUNHO DE 2020

Institui norma 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, regimentais e considerando o protocolo 000-4699/2020,

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 essências 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;

R E S O L V E

Art. 1º Estabelecer norma para 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, além das seguintes:

I - backup: cópia de segurança de dados armazenados em recursos de TIC;
II - mídia de backup: meio físico no qual é armazenado um backup.

Art. 4º As disposições deste Ato aplicam-se a todos os usuários de recursos de tecnologia da informação 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, tipo e tempo de retenção dos backups gerados serão definidos considerando os requisitos legais e a criticidade dos dados envolvidos com relação às atividades da instituição.

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

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

Parágrafo Único. As mídias a serem descartadas deverão ser destruídas de forma a impedir sua reutilização ou acesso aos 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.

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

Art. 11. Somente serão realizados backups de dados armazenados na rede local nos locais 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. 12. Compete à unidade gestora de TIC do Tribunal:

I - documentar, implementar e executar a política e os procedimentos 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 - realizar testes periódicos de recuperação de backups, visando garantir que as cópias geradas são confiáveis para uso em caso de necessidade.

Art. 13. 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. 14. 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. 15. 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. 16. Os casos omissos ou que suscitem dúvidas serão dirimidos pelo Comitê Gestor de Segurança da Informação.

Art. 17. O presente Ato entra em vigor a partir da data de sua publicação.

Art. 18. Revogam-se as disposições em contrário, especialmente o ATO TRT GP Nº 248/2017.

Dê-se ciência.
Publique-se no DA_e.

WOLNEY DE MACEDO CORDEIRO:103147770

Assinado de forma digital por WOLNEY DE MACEDO CORDEIRO:103147770
Dados: 2020.06.18 15:57:57 -03'00'

WOLNEY DE MACEDO CORDEIRO
Desembargador Presidente

Tribunal Regional do Trabalho
13ª Região | Paraíba