

TRIBUNAL REGIONAL DO TRABALHO - 13ª REGIÃO PARAÍBA			
DOC:ATO	NUM:248	ANO:2017	DATA:25-07-2017
ATO			
PROTOCOLO: 9014		ANO:2017	Consulte Protocolo
DISPONIBILIZADO: DEJT		DATA:25-07-2017	PG:00

ATO TRT GP N. 248/2017

João Pessoa, 25 de julho de 2017.

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 e regimentais, de acordo com o Protocolo TRT n. 09014/2017 e, ainda,

CONSIDERANDO a necessidade de atualizar normas e procedimentos para a realização de cópias de segurança dos dados armazenados nos recursos de tecnologia da informação da instituição;

CONSIDERANDO (a necessidade de) manter a integridade e disponibilidade da informação e dos recursos de processamento de informação;

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 seguintes definições:

I - *backup*: cópia de segurança de dados armazenados em recursos de tecnologia da informação;

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 Compete à unidade gestora de Tecnologia da Informação e

Comunicação (TIC) do Tribunal:

I - documentar, implementar e executar a política e os procedimentos de *backup*;

II - gerenciar o armazenamento, o transporte e o 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. 6º A frequência, o tipo e o 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. 7º As mídias de *backup* devem ser armazenadas em uma localidade remota, a uma distância suficiente para evitar danos ocasionados por um eventual desastre no local principal, e que possua um nível apropriado de proteção física e ambiental.

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. Os procedimentos de *backup* devem ser automatizados, visando a facilitar 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 localmente em estações de trabalho

Art. 12. Solicitações para realização ou recuperação de *backups* deverão ser encaminhadas formalmente, via chamado eletrônico, à unidade gestora de TIC do Tribunal pelo gestor da unidade do usuário solicitante.

Art. 13. 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. 14. 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 eventuais irregularidades.

Art. 15. Os casos omissos ou que suscitem dúvidas serão dirimidos pelo

Comitê Gestor de Segurança da Informação.

Art. 16. O presente Ato entra em vigor a partir da data de sua publicação.

Art. 17. Revogam-se as disposições em contrário, especialmente o **ATO TRT GP N. 126/2009**.

Cumpra-se.

Publique-se no DEJT.

EDUARDO SERGIO DE ALMEIDA
Desembargador Presidente