PODER JUDICIÁRIO FEDERAL
Tribunal Regional do Trabalho da 2ª Região

ATO GP nº 07/2015

Institui a Política de Armazenamento de Dados no âmbito do Tribunal Regional do Trabalho da 2ª Região.

A PRESIDENTE DO TRIBUNAL REGIONAL DO TRABALHO DA 2ª REGIÃO, no uso de suas atribuições legais e regimentais,

CONSIDERANDO a necessidade de estabelecer padrões que sirvam como princípios básicos aplicáveis à criação de procedimentos de cópia de segurança e restauração das informações armazenadas nos equipamentos deste Tribunal;

CONSIDERANDO a necessidade de definir parâmetros para que as informações armazenadas nos equipamentos deste TRT sejam salvaguardadas de forma consistente e que propicie, em um evento de desastre que os afete de forma total ou parcial, a possibilidade de retorno dos dados a fim de restaurar a funcionalidade deste Tribunal;

CONSIDERANDO que a perda de informações pode incorrer em dificuldades administrativas e até na interrupção de atividades essenciais deste Regional,

RESOLVE:

Art. 1º. Instituir a Política de Armazenamento de Dados no âmbito do Tribunal Regional do Trabalho da 2ª Região, com o objetivo de estabelecer diretrizes para os processos de cópia de segurança e armazenamento dos dados sob a guarda da Secretaria de Tecnologia da Informação, visando preservar sua integridade, confidencialidade e disponibilidade.

Art. 2º. Para os efeitos deste Ato, aplicam-se as seguintes definições:

I. Administrador de Backup: funcionário responsável pelos procedimentos de configuração, execução, monitoramento e testes dos procedimentos de backup e restore;
II. Administrador do Recurso: funcionário responsável pela administração de serviços ou equipamentos de TI;
III. Backup: Cópia dos dados de um dispositivo de armazenamento para outro, para que possam ser restaurados em caso de perda dos dados originais;
IV. Mídia: meio físico, magnético ou óptico, no qual se armazena dados ou backup de dados;
V. Retenção: período de tempo em que o conteúdo da mídia de backup deve ser preservado;
VI. Restore: ação de recuperar dados previamente armazenados em uma mídia de backup;
VII. Administrador de Banco de Dados: funcionário responsável por gerenciar, instalar, configurar, atualizar e monitorar um banco de dados ou sistemas de bancos de dados. É também responsável pela geração dos arquivos de banco de dados que são objeto dos procedimentos de backup;
VIII. Administrador de Rede: funcionário responsável pelo gerenciamento da rede local, manutenção e configuração dos recursos computacionais inseridos no contexto da infraestrutura de rede, tais como servidores de arquivos, aplicações e serviços;
IX. Dados sob Custódia da Secretaria de Tecnologia da Informação: dados armazenados em servidores de arquivo, aplicações e serviços, excluindo-se os dados armazenados localmente em microcomputadores, notebooks e mídias removíveis (CD, DVD, pen drive, HD externo);
X. Datacenter: instalação projetada para abrigar e proteger os principais recursos computacionais responsáveis pelo armazenamento e processamento de informações, bem como sua infraestrutura de apoio (equipamentos de telecomunicação e de fornecimento de energia).

Escopo

Art. 3º. As disposições deste Ato aplicam-se a todos os administradores dos recursos e demais funcionários envolvidos na guarda e manuseio dos dados sob custódia da Secretaria de Tecnologia da Informação.

Papeis e responsabilidades

Art. 4º. Ao titular da Seção de Operação incumbirá a função de administrador do backup.

§ 1º. As atribuições do administrador de backup poderão ser delegadas a funcionário que atue na Seção de Operação, exceto a de monitoramento dos processos, que deve ser mantida sob responsabilidade do titular.

§ 2º. São atribuições do administrador de backup:

I. Criar e aperfeiçoar os procedimentos de backup;
II. Monitorar e aprimorar os processos relacionados a backup;
III. Configurar as ferramentas de backup;
IV. Criar e manter os backups;
V. Administrar as mídias de backup;
VI. Fazer o carregamento das mídias necessárias para os backups programados;
VII. Efetuar testes de backup e restore;
VIII. Criar controles e relatórios que permitam acompanhar a eficácia dos procedimentos;
IX. Verificar periodicamente os relatórios gerados pela ferramenta de backup;
X. Restaurar backup quando necessário;
XI. Gerenciar mensagens e registros dos backups eliminando as eventuais falhas detectadas;
XII. Promover as manutenções periódicas dos dispositivos de backup;
XIII. Comunicar ao administrador do recurso os erros e ocorrências nos backups;

XIV. Armazenar as mídias de backup em local seguro e com condições ambientais apropriadas garantindo sua integridade e confidencialidade.

Art. 5º. Compete ao administrador do recurso fornecer ao administrador de backup todas informações necessárias para configuração e execução do backup.

Parágrafo único. O Administrador de Banco de Dados e o Administrador de Redes, assim como os demais administradores de recursos, devem contribuir efetivamente para a confecção e homologação dos procedimentos de backup e restore.

Art. 6º. A Seção de Segurança em Tecnologia da Informação, sempre que solicitada, proverá o apoio necessário à elaboração dos procedimentos relativos ao armazenamento de dados pelas áreas envolvidas, atuando de forma coordenada nos assuntos relativos à Segurança da Informação.

Do procedimento de backup

Art. 7º. Todo e qualquer dispositivo que armazene dados poderá ser considerado para inclusão no backup.

Parágrafo único. O administrador de backup deverá, em conjunto com o administrador do recurso, estabelecer procedimentos de rotina para implementar as políticas e estratégias para a geração de cópias de segurança e possibilitar a geração dessas cópias e sua recuperação em um tempo aceitável.

Art. 8º. Para a especificação de um backup, o administrador do recurso deverá preencher um documento de solicitação de backup contendo as informações necessárias, tais como informações do equipamento, dados a serem incluídos na rotina de backup, periodicidade e prazo para retenção.

§ 1º. O administrador de backup deverá desenvolver documento padronizado para solicitação de backup.

§ 2º. O backup deverá ser executado seguindo as orientações do documento de solicitação de backup.

§ 3º. Todos os backups criados deverão ser testados antes da aplicação da programação solicitada.

§ 4º. O teste de backup citado no parágrafo anterior deverá contemplar o respectivo procedimento de restore para comprovar seu correto funcionamento, sendo em seguida, aprovado pelo administrador do recurso através de atestado.

Art. 9º. O Tribunal disponibilizará os recursos necessários à geração de cópias de segurança, de forma a garantir que toda informação e softwares essenciais possam ser recuperados na ocorrência de falha de uma mídia ou mediante necessidade específica de recuperação.

Art. 10. O período de retenção para informações essenciais ao negócio deve ser determinado levando em conta os parâmetros apontados pela política de Gestão Documental referente à Operação de Sistemas de Informática a ser definida institucionalmente, bem como requisitos estatutários, contratuais ou regulamentares, o que se mostrar mais abrangente, de forma a apoiar as atividades essenciais do negócio.

Art. 11. Para a geração de cópias de segurança o administrador de backup deve considerar os seguintes itens:

a. clara identificação das informações referentes ao backup, afixadas na mídia, quando aplicável;
b. produção de registros completos e exatos de cópias de segurança;

c. documentação apropriada sobre os procedimentos de restauração das informações;
d. a modalidade e a frequência da geração de cópias de segurança, de acordo com os requisitos de negócio e a criticidade da informação, para a continuidade da operação;
e. um nível apropriado de proteção física para as cópias de segurança, consistente com as especificações requeridas pelo fabricante da mídia e com as normas aplicadas no datacenter;
f. armazenamento de cópias de segurança em localidade remota, a uma distância de, no mínimo, duas quadras ou quarteirões, para livrar dos danos causados por um desastre ocorrido no local principal;
g. testes regulares em mídias de backup a fim de garantir sua confiabilidade em uso emergencial;
h. garantir a efetividade dos procedimentos de recuperação por meio de testes e verificações regulares, assegurando que possam ser concluídos nos prazos estipulados, descritos no procedimento;
i. proteger as cópias de segurança por meio de encriptação em casos onde a confidencialidade seja importante.

Parágrafo único. Para sistemas críticos, definidos por este Tribunal, convém que os mecanismos de geração de cópias de segurança abranjam todos os dados necessários para a completa recuperação do sistema, quando necessário.

MÍDIAS REMOVÍVEIS

Do gerenciamento das mídias

Art. 12. O administrador de backup deverá estabelecer procedimentos operacionais apropriados para o gerenciamento de mídias removíveis, visando controlar e proteger as mídias contra acesso não autorizado, modificação, remoção e destruição.

§ 1º. As seguintes diretrizes deverão ser consideradas para o manuseio de mídias removíveis:

a. deverá ser mantido registro de mídias removíveis para limitar a oportunidade de perda de dados;
b. toda mídia deverá ser guardada de forma segura e protegida, de acordo com as especificações do fabricante;
c. quando necessária a remoção de qualquer mídia da organização, deverá ser providenciado e mantido o registro dessa remoção como trilha de auditoria;
d. quando não for mais necessário, o conteúdo de qualquer mídia reutilizável deverá ser destruído, antes de ser descartado pela organização.

§ 2º. Todos os procedimentos e os níveis de autorização devem ser explicitamente documentados.

Do transporte das mídias

Art. 13. As mídias e informações nelas contidas deverão ser protegidas contra acesso não autorizado, modificação, remoção e danos durante o transporte externo aos limites físicos da organização.

Parágrafo único. Deverão ser consideradas as seguintes diretrizes para o transporte de mídias:

a. deverão ser adotados meios de transporte designados por este Tribunal;
b. deverá ser definida uma relação de portadores autorizados;
c. deverão ser estabelecidos procedimentos para a verificação da identificação dos transportadores;
d. a embalagem deverá ser suficiente para proteger o conteúdo contra dano físico e fatores ambientais que possam reduzir a possibilidade de restauração dos dados, como a exposição ao calor, umidade ou campos eletromagnéticos;

e. deverão ser adotados controles para evitar o acesso não autorizado ao conteúdo da mídia, como utilização de recipientes lacrados e lacre explícito de pacotes que revele qualquer tentativa de acesso.

Do descarte das mídias

Art. 14. O administrador de backup deverá providenciar o descarte das mídias que não forem mais necessárias à organização, através de procedimentos apontados na Política de Descarte Seguro de Mídias.

Art. 15. O presente Ato entra em vigor a partir da data de sua publicação, revogadas as disposições em contrário.

Parágrafo único. Recursos implementados antes da publicação deste Ato, e que estejam em desacordo com esta norma, devem ser regularizados em até 1 (um) ano.

Publique-se e cumpra-se.
São Paulo, 23 de março de 2015.

SILVIA REGINA PONDÉ GALVÃO DEVONALD
Desembargadora do Trabalho Presidente do Tribunal