P O D E R J U D I C I Á R I O
JUSTIÇA DO TRABALHO
TRIBUNAL REGIONAL DO TRABALHO DA 8ª REGIÃO

PORTARIA PRESI Nº 147, DE 15 DE FEVEREIRO DE 2017

Estabelece a Política de Backup de dados a ser utilizada pela Secretaria de Tecnologia da Informação do Tribunal Regional do Trabalho da 8ª Região.

A DESEMBARGADORA PRESIDENTE DO TRIBUNAL REGIONAL DO TRABALHO DA OITAVA REGIÃO, no uso de suas atribuições legais e regimentais; e

CONSIDERANDO a dependência crescente dos sistemas de informação nas atividades judiciais e administrativas da Justiça do Trabalho no Pará e Amapá;

CONSIDERANDO a necessidade de garantir a segurança das informações armazenadas nos servidores do Tribunal Regional do Trabalho da 8ª Região;

CONSIDERANDO a necessidade de regulamentar o procedimento de cópia de segurança dos dados armazenados nos servidores do Tribunal Regional do Trabalho da 8ª Região;

CONSIDERANDO a necessidade de gerenciar os dados a fim de manter a completude, a precisão, a disponibilidade e a proteção das informações;

CONSIDERANDO a necessidade de assegurar o acesso e a proteção das informações eletrônicas deste Tribunal, por meio de uma política de backup que observe criteriosamente o modo e a periodicidade de cópia dos dados armazenados pelos sistemas computacionais;

CONSIDERANDO que a perda de informações eletrônicas podem significar graves dificuldades administrativas e de prestação jurisdicional ocasionando a paralisação de atividades essenciais do Tribunal;

CONSIDERANDO o item 12.3 da norma ABNT-NBR 27.002/2013, que estabelece diretrizes para definição de política de backup (cópias de segurança), com o intuito de proteger o negócio contra perda de dados.

R E S O L V E:

Art. 1º Regulamentar a política de backup das informações eletrônicas, no âmbito do Tribunal Regional do Trabalho da 8ª Região,

com o objetivo de estabelecer diretrizes para o processo de cópia e armazenamento dos dados sob a guarda da Secretaria de Tecnologia da Informação, visando garantir a sua integridade e disponibilidade.

CAPÍTULO I
DAS DISPOSIÇÕES GERAIS

Art. 2º Para o disposto nesse ato, considera-se:

I - Administrador de backup: servidor responsável pelos procedimentos de configuração, execução, monitoramento e testes dos procedimentos de backup e restore;

II - Ambiente de produção: computador instalado, configurado e mantido pela Secretaria de Tecnologia da Informação cuja finalidade é dar sustentação a execução de sistemas e de serviços de tecnologia da informação do Tribunal;

III - Backup: é o processo de criação de cópias de segurança de dados que assegura a existência das informações para que possam ser recuperadas quando necessário;

IV - Backup completo: modalidade de backup na qual todos os dados são copiados;

V - Backup incremental: modalidade de backup na qual somente os arquivos modificados desde o último backup completo ou incremental são copiados;

VI - Computador Desktop: Computador pessoal ou estação de trabalho;

VII - Confidencialidade: Garantia de que o acesso à informação seja obtido apenas por pessoas autorizadas;

VIII - Data Center: É um ambiente projetado para abrigar e concentrar os equipamentos de processamento e armazenamento de dados de uma organização;

IX - Disco Rígido: É o componente físico do computador onde são armazenados os dados, funciona como uma memória não volátil impedindo que a informações sejam perdidas quando o computador é desligado;

X - Disponibilidade: Garantia de que os usuários autorizados obtenham acesso à informação e aos recursos correspondentes sempre que necessário;

XI - Estratégia de backup: grupo de informações e procedimentos para a execução de backups;

XII - Fita magnética: é uma mídia de armazenamento não-volátil que consiste em uma fita plástica coberta de material magnetizável;

XIII - Integridade: Salvaguarda de exatidão e completeza da informação e dos métodos de processamento;

XIV - Log: histórico de avisos, erros e mensagens de aplicativos e sistemas;

XV - Mídia: meio físico no qual efetivamente é armazenado o backup;

XVI - Nuvem: São recursos computacionais que podem ser utilizados de forma automatizada, dinâmica e sob demanda, disponibilizados através de grandes servidores compartilhados e interligados por meio da Internet, possibilitando o acesso de qualquer lugar e a qualquer hora.

XVII - Periodicidade: frequência com que a cópia é executada;

XVIII - Programa-fonte: é o código escrito em linguagem de programação que contém as instruções que fazem um sistema computacional funcionar;

XIX - Retenção: período de tempo em que o conteúdo da mídia de backup deve ser preservado;

XX - RPO (Recovery Point Objetive): o quanto é necessário voltar no tempo para encontrar um backup dos dados, ou seja, o tempo máximo de perda de dados;

XXI - RTO (Recovery Time Objetive): tempo estimado para restaurar os dados ou para tornar os sistemas operacionais novamente;

XXII – SGBD: Sistema Gerenciador de Banco de Dados;

XXIII - Script: É um conjunto de instruções em código que executa diversas funções no interior de um programa de computador. Utilizado para instalação, configuração e controle de um determinado aplicativo;

XXIV - Servidor: É um computador com alto poder de processamento, desenvolvido para lidar com cargas de trabalho mais

pesadas, transmitir informações e fornecer produtos e serviços de software a outros computadores que estiverem conectados a ele por uma rede;

XXV - Servidor de Backup: É o equipamento capaz de geranciar os backups realizados;

XXVI - Storages: são dispositivos projetados especificamente para prover uma alta capacidade de armazenamento de dados, permitindo o trabalho de diversos discos em conjunto através de uma rede exclusiva.

CAPÍTULO II
DO PROCESSO DE BACKUP

Art. 3º O processo de backup deve ser dividido em três macro etapas: planejamento, execução e controle.

§ 1º A etapa de planejamento objetiva a identificação dos repositórios de dados e a elaboração de estratégia de cópia eficiente para a recuperação das informações.

§ 2º A etapa de execução deve ser automatizada e consiste na geração dos arquivos de cópia de segurança de cada repositório. Os arquivos resultantes podem ser únicos, em formato reconhecido pela própria solução automatizada, podendo ou não ser compactados e/ou criptografados.

§ 3º A etapa de controle visa garantir a efetividade das cópias, tanto no aspecto de assegurar o cumprimento da estratégia de backup (periodicidade, tipo de cópia, retenção e local de armazenamento), quanto na certificação de integridade dos arquivos de cópias resultantes da fase de execução. Esta etapa deve também diagnosticar impropriedades da rotina de backup. Caso estas impropriedades comprometam definitivamente a eficiência de recuperação dos arquivos, a falha deverá ser notificada ao Secretário de Tecnologia da Informação.

CAPÍTULO III
DA ESPECIFICAÇÃO DO BACKUP

Art. 4º As cópias de segurança devem ser geradas, transportadas e armazenadas de forma segura, com controles físicos e lógicos compatíveis com os requisitos de confidencialidade, integridade e disponibilidade das informações respectivas.

§ 1º O backup de determinado sistema ou serviço deve contemplar todos os arquivos e dados necessários à sua plena restauração.

§ 2º As cópias de segurança devem permitir a recuperação dos servidores, contemplando os dados históricos e as versões dos programas fontes anteriores.

§ 3º O serviço de backup deve ser estruturado visando a restauração das informações no menor tempo possível, principalmente quando houver indisponibilidade de outros serviços que dependam da operação de restauração.

Art. 5º Somente devem ser geradas cópias de segurança dos dados armazenados em discos de servidores e storages mantidos pela Secretaria de Tecnologia da Informação e em seus anexos.

§ 1º As cópias de segurança devem ser baseadas no seguinte conteúdo:

I - arquivos de documentos corporativos;

II - sistemas e códigos fonte;

III - bancos de dados;

IV - todos os dados dos servidores e registros de sistema operacional.

§ 2º Não deve ser realizado backup de arquivos armazenados em estações de trabalho, não sendo garantida a recuperação em caso de erro físico do disco rígido local ou instabilidade no sistema operacional instalado, salvo solicitação expressa da área requisitante devidamente aprovada pelo Diretor de Tecnologia da Informação.

CAPÍTULO IV
DAS MÍDIAS DE BACKUP

Art. 6º Os backups podem ser armazenados em:

I - disco rígido;

II - fitas magnéticas;

III - nuvem.

PORTARIA PRESI Nº 147, DE 15 DE FEVEREIRO DE 2017

Art. 7º Os dados estruturados devem ser periodicamente copiados para um dispositivo de disco distinto daquele no qual se encontrem, de tal forma que possam ser recuperados e restaurados, em caso de corrompimento, indisponibilidade ou perda dos dados de produção.

Art. 8º De acordo com a criticidade, as cópias de segurança armazenadas em disco também devem ser copiadas para fitas magnéticas que são apropriadas para esse fim.

Art. 9º As fitas magnéticas devem ser armazenadas em cofres especiais (cofres-data) que garantam a proteção em caso de incêndio, enchentes e vazamentos de gases.

Parágrafo único. Os cofres-data devem ser mantidos trancados para garantir a hermeticidade das mídias armazenadas.

Art. 10. A cópia de segurança pode ser guardada de modo diferente do armazenamento padrão, de acordo com necessidades especiais, peculiaridades das aplicações, motivos judiciais e/ou legais.

Art.11. Expirado o prazo de retenção dos dados armazenados, a mídia pode ser reutilizada.

Art. 12. As mídias de backup inservíveis ou inutilizáveis devem ser descartadas, sendo encaminhadas para picotamento, incineração, procedimentos de sobrescrita de dados remanescentes ou outro procedimento que impossibilite a recuperação dos dados por pessoas não autorizadas.

CAPÍTULO V
DO BACKUP DE ARQUIVOS E MÁQUINAS VIRTUAIS

Art. 13. Os procedimentos de backup realizados pela Seção de Infraestrutura e Redes da SETIN devem ser executados de forma automática e abrangem, os dados gravados nos diretórios de rede privativos de cada unidade organizacional do TRT 8, os dados nos diretórios destinados à gravação de arquivos pessoais dos usuários, além das máquinas virtuais e sistemas nelas contidas.

Art. 14. O backup dos dados das unidades organizacionais fora da sede deve ser realizado a partir de cada repositório disponível em cada localidade após sincronização direta com o servidor de backup.

Art. 15. Os dados, objeto de backup, devem ser armazenados inicialmente em storages-pools, com volume alocado no Storage para essa tarefa. Ao ser completado 40% de ocupação, deve ser efetuada uma cópia no conjunto de fitas primárias disponíveis para restaurações e outra cópia no conjunto de fitas secundárias.

Art. 16. A cópia de segurança deve ser realizada, preferencialmente, fora do horário de expediente do Tribunal.

Parágrafo único. Na ocorrência de falha no backup ou se o mesmo estiver incompleto, novo backup deve ser executado com vistas ao seu armazenamento. Neste caso, o administrador de backup deve criar um relatório de acompanhamento de backup, no qual deve constar a data, os horários de início e término deste, os objetos e os clientes de backup, a causa da falha, a ação corretiva adotada e qual parte do backup ficou comprometida.

Art. 17. Nos casos de impossibilidade de execução da ferramenta automatizada de backup, o administrador de backup deverá adotar as providências no sentido de salvaguardar as informações através de outra solução, como por exemplo a cópia dos dados para outro servidor ou mesmo execução do backup em horário de produção.

Art. 18. Caso seja detectada a realização de backup de arquivo impróprio, a Coordenadoria de Infraestrutura deve excluí-lo com posterior comunicação ao Diretor de Tecnologia da Informação e ao responsável pelo arquivo.

Art. 19. A SETIN deve contar com uma solução de espelhamento de storages, de forma que o storage principal deve estar localizado na Sala Cofre do Tribunal, sendo espelhado sincronicamente com o storage secundário localizado no Site Backup.

Art. 20. Devem ser adotadas estratégias específicas e diferenciadas de backup, de acordo com os dados a serem armazenados:

§ 1º Os arquivos armazenados no Servidor de Arquivos devem ter backup incremental, com frequência diária, período de retenção de 12 (doze) meses, retendo até 7 (sete) versões do arquivo armazenado, possuindo RPO e RTO de 24 (vinte e quatro) horas.

§ 2º Os arquivos armazenados no Servidor de Arquivos da sede devem ter backup completo, com frequência anual, período de retenção de 5 (cinco) anos, possuindo RPO de 12 (doze) meses do último backup anual e RTO de 24 (vinte e quatro) horas.

§ 3º Os arquivos de configuração dos ativos da rede

corporativa de dados do TRT8 devem ter backup incremental, com frequência semanal, período de retenção de 12 (doze) meses, possuindo RPO de 7 (sete) dias e RTO de 1 (uma) hora.

§ 4º Os arquivos de configuração dos Sistemas e Aplicações críticas devem ter backup completo, com frequência semanal, período de retenção de 30 (trinta) dias, possuindo RPO de 7 (sete) dias e RTO de 1 (uma) hora.

§ 5º Os arquivos de gravação de audiências devem ter backup incremental, com frequência diária, período de retenção de 12 (doze) meses, possuindo RPO de 24 (vinte e quatro) horas e RTO de 1 (uma) hora.

§ 6º As Máquinas Virtuais devem ter backup completo, com frequência mensal, período de retenção de 30 (trinta) dias, possuindo RPO de 30 (trinta) dias e RTO de 15 (quinze) horas.

Art. 21. O Backup deve ser realizado em mídias do tipo cartucho de fita, sendo armazenadas no cofre de segurança do Tribunal, conforme os seguintes requisitos:

§ 1º Os backups devem ser copiados de forma duplicada em fitas distintas.

§ 2º As fitas devem ser identificadas por etiquetas autoadesivas constando o conteúdo da cópia, o tipo de periodicidade, a data e a hora.

§ 3º O administrador de Backup deverá efetuar cópia dos dispositivos que armazenam os backups, sempre que estiverem próximos de esgotar a sua vida útil.

Art. 22. Os backups devem ser enviados para fita através do agendamento da tarefa, de forma que o envio para fita seja iniciado automaticamente com a periodicidade especificada. Nesse cenário, a responsabilidade pelo agendamento, acompanhamento e notificação do resultado da execução será da Seção de Infraestrutura e Redes da SETIN.

CAPÍTULO VI
DO BACKUP DE BANCO DE DADOS

Art. 23. Os dados estruturados, armazenados nos bancos de dados do Tribunal, devem ser periodicamente copiados para um dispositivo de disco distinto daquele no qual se encontram atualmente,

de tal forma que possam ser recuperados e restaurados, em caso de corrompimento, indisponibilidade ou perda dos dados de produção.

Art. 24. O backup em disco deve permitir a restauração íntegra de um banco de dados até o momento imediatamente anterior ao evento que causou a corrupção, indisponibilidade ou perda dos dados.

Art. 25. O procedimento de backup de banco de dados deve ser realizado preferencialmente fora do horário de expediente do Tribunal, não devendo indisponibilizar o banco de dados do qual esteja sendo extraído.

Art. 26. Como medida adicional de segurança, os backups dos dados de produção também devem ser copiados para fita.

Art. 27. Devem ser adotadas estratégias específicas e diferenciadas de backup para os dados de produção armazenados em cada um desses ambientes em virtude de critérios como: tamanho das bases de dados gerenciadas, criticidade da informação para o Tribunal e mecanismos de backup disponibilizados pelo ambiente.

§ 1º Para os bancos de dados do SGBD PostgreSQL deve existir:

I - Replicação constante dos dados do banco principal para outro, o qual deve ser armazenado em dispositivo de disco próprio. Esse banco de dados replicado funciona como backup online, sendo inclusive acessível para leitura e, por ser gerenciado por um servidor próprio, pode ser imediatamente promovido e utilizado pela aplicação, em caso de queda do banco principal;

II - 1(um) Backup físico completo, realizado diariamente, retido em disco por vinte e quatro horas, e enviado para fita logo após o seu término;

III - 1(um) Backup dos dos logs das transações, arquivados em dois dispositivos de disco distintos e retidos em ambos até a realização do próximo backup físico completo. De hora em hora, esses logs devem ser enviados para fita;

IV - 1(um) Backup lógico, apenas das bases não binárias, realizado diariamente, retido em disco por vinte e quatro horas, e não copiado para fita.

§ 2º Para os bancos de dados do SGBD Oracle deve existir:

I - Replicação constante dos bancos de produção para cópias passivas (não acessíveis sequer para leitura), armazenadas em

dispositivo de disco distinto. Essas réplicas funcionam com um backup online, podendo ser promovidas em caso de indisponibilidade dos bancos principais;

II - 1(um) Backup físico completo, realizado semanalmente, retido em disco por sete dias, e copiado para fita logo após o seu término;

III - 1(um) Backup físico incremental, realizado diariamente, retido em disco até a realização do próximo backup físico completo, e copiado para fita logo após o seu término;

IV - 1(um) Backup dos logs das transações, retidos em disco até a realização do próximo backup físico completo, e copiados para fita de hora em hora;

V - 1(um) Backup lógico, com exceção das tabelas de documentos e arquivos, realizado diariamente, retido em disco por vinte e quatro horas, e não copiado para fita;

VI - Dados históricos das últimas vinte e quatro horas, disponíveis para consulta.

§ 3º Para os bancos de dados do SGBD Caché deve existir:

I - 1(um) Backup físico completo, realizado diariamente, retido em disco por vinte e quatro horas, e copiado para fita logo após o seu término;

II - 1(um) Backup dos logs das transações, arquivados em dois dispositivos de disco distintos e retidos em ambos por quarenta e oito horas. De hora em hora, esses logs devem ser enviados para fita.

§ 4º Para os bancos de dados do SGBD MySQL deve existir:

I - Replicação constante dos bancos de produção para cópias ativas (acessíveis para leitura), armazenadas em dispositivo de disco distinto. Essas réplicas funcionam com um backup online, podendo ser promovidas em caso de indisponibilidade dos bancos principais;

II - 1(um) Backup físico completo, realizado semanalmente todo domingo, retido em disco por sete dias, e copiado para fita logo após o seu término;

III - 1(um) Backup físico incremental, realizado diariamente de segunda a sábado, retido em disco até a realização do próximo backup físico completo, e copiado para fita logo após o seu

término;

IV - 1(um) Backup dos logs das transações, arquivados em dois dispositivos de disco distintos e retidos em ambos, até a realização do próximo backup físico completo. De hora em hora, esses logs são enviados para fita;

V - 1(um) Backup lógico, realizado diariamente, retido em disco por sete dias, e copiado para fita logo após o seu término.

§ 5º Para os bancos de dados do SGBD SQL Server deve existir:

I - Replicação constante dos bancos de produção para cópias passivas (não acessíveis sequer para leitura), armazenadas em dispositivo de disco distinto. Essas réplicas funcionam com um backup online, podendo ser promovidas em caso de indisponibilidade dos bancos principais;

II - 1(um) Backup físico completo, realizado semanalmente, retido em disco por sete dias, e copiado para fita logo após o seu término;

III - 1(um) Backup físico incremental, realizado diariamente, retido em disco até a realização do próximo backup físico completo, e copiado para fita logo após o seu término;

IV - 1(um) Backup dos logs das transações, retidos em disco até a realização do próximo backup físico completo, e copiados para fita de hora em hora;

Art. 28. Os backups dos objetos de banco de dados devem ser gerados em dispositivo de disco e, como medida adicional de segurança, enviados para fita.

Art. 29. Os backups podem ser enviados para fita de duas formas:

I - Através do agendamento da tarefa, de forma que o envio para fita seja iniciado automaticamente no horário e com a periodicidade especificados. Nesse cenário, a responsabilidade pelo agendamento, acompanhamento e notificação do resultado da execução será da Seção de Infraestrutura e Redes da SETIN;

II - Através da inclusão nos scripts de backup da referência explícita ao aplicativo responsável pelo envio para fita. Nesse cenário, a responsabilidade pelo acompanhamento e notificação do resultado da execução será da Seção de Banco de Dados.

Art. 30. Em virtude da criticidade para o Tribunal dos dados estruturados, armazenados em diversos bancos de dados existentes, deve ser disponibilizado um canal dedicado para o envio dos backups desses dados para fita, que não concorra com o envio dos demais objetos, sendo que os backups devem ser copiados de forma duplicada em fitas distintas.

Art. 31. Os backups físicos completos e backups lógicos deverão ser enviados para fita de forma completa.

Art. 32. Os backups físicos incrementais e logs de transações deverão ser enviados para fita de forma incremental.

Art. 33.Com relação ao período de retenção dos dados, os backups enviados para fita de forma:

I - Incremental: devem ser retidos durante cinco anos;

II - Completa e diária: devem ser retidos por uma semana;

III - Completa e semanal: devem ser retidos por um mês;

IV - Completa e mensal: devem ser retidos por um ano;

V - Completa e anual: devem ser retidos por cinco anos.

CAPÍTULO VII
DO TESTE DE RECUPERAÇÃO DE DADOS

Art. 34. Os backups armazenados em disco e em fita, devem ser testados de forma amostral a cada 6 (seis) meses para assegurar que a confiabilidade das mídias de backup, a integridade dos dados e o tempo de restauração das cópias estejam aderentes aos requisitos de continuidade de negócio definidos pelo Tribunal.

§ 1º Anualmente, pelo menos um teste deve ser realizado nos backups de cada um dos ambientes de dados do Tribunal. Este teste deve ser preferencialmente aplicado em backups físicos armazenados em fita.

§ 2º Os testes devem incluir um procedimento de restauração dos dados para comprovar a eficácia do backup.

§ 3º Os backups devem ser restaurados em ambientes de teste

distintos dos de produção, como forma de validação.

§ 4º Um backup será considerado válido quando, o ambiente original puder ser recriado em um estado consistente.

§ 5º Sempre que determinado procedimento de backup for alterado, o backup resultante deve ser testado.

§ 6º Em caso de falha na restauração, o administrador de backup deverá informar a Coordenadoria de Infraestrutura para que as medidas necessárias à correção do problema sejam tomadas.

§ 7º Para cada teste realizado deve ser gerado um relatório, sendo este apresentado ao Diretor de Tecnologia da Informação.

CAPÍTULO VIII
DAS RESPONSABILIDADES

Art. 35. A administração do backup de banco de dados é de responsabilidade da Seção de Banco de Dados da SETIN. Neste caso o papel de administrador de backup deve ser desempenhado por servidor lotado nesta Seção.

Art. 36. A administração do backup de arquivos e máquinas virtuais é de responsabilidade da Seção de Infraestrutura e Redes da SETIN. Neste caso o papel de administrador de backup deve ser desempenhado por servidor lotado nesta Seção.

Art. 37.São atribuições do administrador de backup:

I - propor modificações visando o aperfeiçoamento da política de backup;

II - criar e manter os backups;

III - configurar a ferramenta de backup e os clientes;

IV - criar e testar scripts;

VI - testar o restore;

VII - criar notificações e relatórios;

VIII - verificar periodicamente os relatórios gerados pela

ferramenta de backup;

IX - restaurar backup;

X - gerenciar mensagens e logs diários dos backups, fazendo o tratamento dos erros de forma que o procedimento de backup tenha sequência e os erros na sua execução sejam eliminados;

XI - fazer manutenções periódicas dos dispositivos de backup;

XII - fazer o carregamento das mídias necessárias para os backups programados;

XIII - comunicar ao administrador do recurso os erros e ocorrências nos backups;

XIV - guardar e manter as mídias de backup em cofre próprio;

XV - documentar a geração, teste, armazenamento e recuperação das cópias de segurança corporativa;

XVI - Manter documentação pertinente ao backup, incluindo planos de backup (nível operacional), planos de testes, registros (logs) de execução e monitoramento;

XVII - realizar e controlar o inventário de mídias.

Art. 38. Para o desempenho das atividades de recuperação de dados, o administrador de backup lotado na Seção de de Infraestrutura e Redes da SETIN pode demandar apoio à Coordenadoria de Sistemas da SETIN, em caso de necessidade de auxílio na validação dos dados restaurados.

Art. 39. Para o desempenho das atividades de recuperação de dados, o administrador de backup lotado na Seção de Banco de Dados pode demandar apoio à:

I - Seção de de Infraestrutura e Redes da SETIN, em caso de necessidade de recuperação a partir de fita e disponibilização temporária de recursos;

II - Seção de Sistemas Corporativos da SETIN, em caso de necessidade de auxílio na validação dos dados restaurados.

Art. 40. Em caso de falha no backup ou se o mesmo estiver incompleto, o administrador de backup deverá adotar as providências

necessárias no sentido de salvaguardar as informações através da execução de um novo backup, com vistas ao seu armazenamento.

Art. 41. O controle operacional e os procedimentos de administração de backup não podem ser de domínio exclusivo de uma única pessoa a fim de garantir a continuidade do negócio.

Art. 42. Compete ao Diretor da Secretaria de Tecnologia da Informação:

I - garantir o armazenamento dos registros de maneira segura para prevenir alterações, bem como para fins de auditoria e gestão de mudança.

II - solicitar anualmente a inserção da previsão de aquisição das fitas no plano de trabalho anual.

Art. 43. Compete ao Tribunal Regional da 8ª Região garantir a disponibilização de estrutura e recursos adequados para a realização dos procedimentos de backup.

CAPÍTULO IX
DAS DISPOSIÇÕES FINAIS

Art. 44. Períodos de retenção de dados, diferentes do padrão estabelecido por esta política, poderão ser definidos pelo Comitê de Segurança da Informação para sistema ou serviço específico, mediante solicitação da Secretaria de Tecnologia da Informação ou do gestor do sistema.

Art. 45. Quaisquer procedimentos programados nos equipamentos servidores e que impliquem riscos de funcionamento ou em quaisquer dispositivos de armazenamento do Tribunal, somente deverão ser executados após a realização do backup dos seus dados.

Art. 46. Esta Portaria entra em vigor na data de sua publicação no Diário Eletrônico da Justiça do Trabalho.

Publique-se, dê-se ciência e cumpra-se.

SUZY ELIZABETH CAVALCANTE KOURY
Desembargadora Presidente