POLÍTICA Nº 14, DE 15 DE SETEMBRO DE 2017.

*Institui a **Política de Backup e Retenção de Dados** no âmbito do Tribunal Regional do Trabalho da 9ª Região.*

O DIRETOR DA SECRETARIA DE TECNOLOGIA DA INFORMAÇÃO DO TRIBUNAL REGIONAL DO TRABALHO DA 9ª REGIÃO, no uso de suas atribuições legais e regimentais,

CONSIDERANDO:

- a Política de Segurança da Informação (PSI) do Tribunal Regional do Trabalho da 9ª Região;

- o disposto no Art. 12, inciso "II", alínea "a", da Resolução 211/2015 CNJ, sobre a necessidade de constituir e manter estruturas organizacionais adequadas e compatíveis com a relevância e demanda de TIC, considerando, entre outros macroprocessos, o de Segurança da Informação e seu processo de continuidade de serviços essenciais;

- o disposto no Art. 24, inciso "VII", da Resolução 211/2015 CNJ, sobre a capacidade da solução de backup ser suficiente para garantir a salvaguarda das informações digitais armazenadas, incluindo tecnologias para retenção de longo prazo e cópia dos backups mais recentes, em local distinto do local primário do órgão, de modo a prover redundância e atender à continuidade do negócio em caso de desastre;

- o item 12.3 da norma ISO 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;

- a necessidade de atender a todos os pilares da Segurança da Informação, a saber, Confidencialidade, Integridade e Disponibilidade;

- a instituição, por meio do Ato 140/2017, do Sistema de Apoio à Governança de TIC (SAGG);

- o Ato 190/2017 da Presidência, que normatiza a Instituição de Políticas de TIC;

- a instituição, por meio da Política nº 10/2017, da Política de Gerenciamento de Processos de trabalho no âmbito do Tribunal;

RESOLVE:

CAPÍTULO I
DAS DISPOSIÇÕES INICIAIS

Art. 1° Instituir a POLÍTICA DE BACKUP E RETENÇÃO DE DADOS, no âmbito deste Tribunal.

Art. 2º Esta política integra a Política de Segurança da Informação (PSI) do Tribunal Regional do Trabalho da 9ª Região e tem como objetivo assegurar a correta elaboração, aprovação, execução e auditoria dos planos de backup e dos relatórios de backup e restauração de dados, prevenindo a perda e a indisponibilidade de sistemas e informações produzidos e/ou armazenados nos ativos de Tecnologia de Informação e Comunicação (TIC) do Tribunal.

CAPÍTULO II
DOS CONCEITOS E DEFINIÇÕES

Art. 3° Para os efeitos desta Política, aplicam-se as seguintes definições e conceitos:

I - AMBIENTE PRIMÁRIO DE BACKUP: local onde é feito a primeira cópia dos arquivos originais;

II - AUDITOR DE BACKUP: unidade ou agente responsável pela verificação da conformidade da execução do processo de Backup com a política e com os planos de backup previamente estabelecidos.

III - BACKUP: cópia de segurança de informação para prevenir perda de disponibilidade em caso de perda da informação principal;

IV - CÓPIA DE SEGURANÇA *OFFSITE*: cópia de backup em mídia armazenada fora do ambiente primário de dados de backup;

V - CUSTODIANTE DOS ATIVOS DE INFORMAÇÃO: unidade, setor ou agente responsável pela guarda e proteção das informações a ele confiadas pelo proprietário da informação, de acordo com os requisitos de segurança definidos pelo dono da informação. É responsável pelos procedimentos de planejamento, configuração, execução, monitoramento e testes dos procedimentos de backup e restauração;

VI - DONO DA INFORMAÇÃO: proprietário da informação, (alta administração, gestores e utilizadores do equipamento, serviço ou sistema), responsável pela definição dos requisitos de segurança para o tratamento das informações do negócio, no que concerne à confidencialidade, à integridade e à disponibilidade de suas informações corporativas;

VII - JANELA DE BACKUP: período de tempo compreendido entre o início e o fim de uma operação de backup, sendo um fator importante de avaliação de desempenho da solução de backup instalada;

IX - RESTAURAÇÃO: processo realizado para colocar disponível uma cópia de segurança de informação anteriormente preservada;

X - RETENÇÃO DOS DADOS: período de tempo pelo qual os dados copiados são preservados no ambiente de backup.

Parágrafo único. Outros conceitos e definições específicos encontram-se definidos no GLOSSÁRIO ELETRÔNICO, disponível em sítio na Intranet ou Internet mantidos por este Tribunal.

CAPÍTULO III
DAS DIRETRIZES GERAIS

Art. 4º As cópias de backup das informações, softwares e sistemas devem ser realizadas e testadas regularmente, de acordo com esta política.

§ 1º O backup de determinado sistema ou serviço deve contemplar todos os arquivos e dados necessários à sua plena restauração, incluindo executáveis, definições de estrutura de banco de dados, entre outros.

§ 2º O backup de sistemas, aplicativos e documentos protegidos por direitos autorais deve observar às restrições de cópia previstas em suas respectivas licenças de uso e sua legislação vigente.

§ 3º 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 respectivas informações.

§ 4º As mídias de cópia de segurança *offsite* devem ser mantidas em uma localidade distanciada do ambiente primário de backup, se possível em outra sede, a uma distância suficiente para prevenir eventuais danos ocasionados por um desastre ocorrido no local primário.

§ 5º As informações que possuem dados sigilosos devem ter seus backups protegidos por criptografia ou controle de acesso físico e lógico restritos.

CAPÍTULO IV
DOS PAPEIS E RESPONSABILIDADES

Art. 5º São atribuições do **Custodiante dos ativos de informação**:

I - criar o Plano de Backup, detalhado no **Art. 7º,** levando em consideração os requisitos de segurança da informação a serem resguardados e a Política de Classificação de Informações vigente, seguindo os parâmetros de Tabelas de Temporalidade, Guia ou Política de Gestão Documental vigente;

II - preencher o Relatório de Backup e o Relatório de Restauração de Backup;

III - efetuar a verificação periódica e o acompanhamento das rotinas de backup, de acordo com o que foi definido no Plano de Backup;

IV - buscar a otimização das rotinas, recursos e janelas de backup;

V - efetuar testes de restauração periódicos;

VI - realizar a operação de restauração de backup, caso necessário;

VII - reavaliar periodicamente o Plano de Backup.

Art. 6º São atribuições do Auditor de Backup:

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

II - validar o Plano de Backup;

III - realizar auditorias periódicas nos backups e restaurações executadas, bem como nas configurações implementadas;

IV - acompanhar e fiscalizar a execução desta política.

Parágrafo único. O papel de Auditor de Backup não deve ser atribuído ao custodiante direto dos dados contemplados na auditoria.

CAPÍTULO V
DOS PLANOS E RELATÓRIOS

Art. 7º O Plano de Backup, a ser elaborado pelo Custodiante dos ativos de informação, deve conter, no mínimo:

I - identificação e descrição dos recursos e das informações que serão resguardados;

II - lista de estruturas de dados que serão copiados, quando for o caso;

III - periodicidade do backup;

IV - horário preferencial da execução do backup;

V - previsão do volume de dados a ser armazenado;

VI - procedimentos preparatórios a serem realizados para a execução do backup;

VII - estratégia de utilização dos dispositivos de retenção para os dados de backups (ex. discos, fitas, etc.);

VIII - estratégia de classificação e retenção dos backups;

IX - periodicidade dos Relatórios de Backup e de Restauração;

X - estratégia de recuperação de dados críticos no processo de continuidade do negócio;

XI - definição da necessidade de manutenção de segunda cópia *offsite*.

Parágrafo único. O Plano de Backup deve ser submetido à validação do Auditor de Backup antes de sua efetiva implementação.

Art. 8º A definição do período retenção dos dados em backup deve observar os prazos acordados entre o Dono e o Custodiante da Informação, do que deve ser

feito registro no Catálogo de Serviços, sendo validada pelo Auditor de Backup, levando-se em consideração os requisitos tecnológicos e de infraestrutura e, consequentemente, os custos para implementação.

§1º Os períodos de retenção dos dados devem contemplar, conforme o caso, os seguintes tipos de backup:

I - backup diário;

II - backup mensal;

III - backup anual (conhecido também como arquivamento de dados de longa retenção - *archive*).

§2º O(s) período(s) de retenção acordados entre Dono e Custodiante da informação deve(m) constar do catálogo de serviços e integrar o Plano de Backup para o ativo relacionado, e qualquer alteração prática deve estar refletida no documento tão logo seja implantada no ambiente.

Art. 9º O Relatório de Backup deverá conter, no mínimo:

I - identificação do recurso copiado;

II - identificação do ambiente e do software gerenciador de backup;

III - classificação do backup (incremental, diferencial, *full*, etc.);

IV - data e horário de início e término da rotina;

VI - resultado do backup;

VII - eventuais ações corretivas que foram tomadas com o intuito de assegurar a execução do processo de backup.

Art. 10. O Relatório de Restauração de Backup deve conter, no mínimo:

I - identificação do recurso restaurado;

II - identificação do ambiente e do software gerenciador de backup;

III - identificação do escopo da amostra de restauração;

IV - tempo da restauração completa da amostra;

V - resultado do teste de restauração;

VI - eventuais ações corretivas que foram tomadas com o intuito de assegurar a execução do processo de restauração.

CAPÍTULO VI
DAS DIRETRIZES ESPECÍFICAS

Art. 11. A criação e a operação dos backups devem observar as seguintes orientações:

I - CRIAÇÃO DE BACKUPS: o backup deverá ser programado, preferencialmente, para execução automática, em horários de menor ou nenhuma utilização dos sistemas e da rede, observando os requisitos do Plano de Backup;

II - OPERAÇÃO DE BACKUPS: o backup deverá ser monitorado pelo Custodiante da Informação. Um relatório (preferencialmente automatizado) deverá ser

gerado para as execuções de backup, contendo informações dos registros dos resultados do processo.

Art. 12. Na restauração de dados, por conta de solicitação específica, deve ser mantido o registro da informação restaurada, juntamente com as informações relativas à solicitação (número do chamado técnico, solicitação de serviço ou ticket de abertura de chamado, quando houver), para fins de auditoria.

CAPÍTULO VII
DA PRESTAÇÃO DE CONTAS

Art. 13. A STI deve apresentar aos membros da Comissão de Segurança da Informação (CSI) ou aos demais órgãos Colegiados de TIC informações acerca do cumprimento da presente política:

I- detalhadamente, quanto por eles requerido;
II- resumidamente, juntamente com o relatório periódico de gestão.

CAPÍTULO VIII
DAS DISPOSIÇÕES FINAIS E TRANSITÓRIAS

Art. 14. Cabe à STI estabelecer os critérios técnicos relacionados aos procedimentos e às configurações de backup e de restauração para cada sistema ou base de dados, em harmonia com os acordos firmados entre o Dono e o Custodiante da Informação.

Art. 15. Compete ao Dono do Processo analisar sobre os casos omissos ou que suscitem dúvidas quanto ao disposto nesta política, encaminhando o tema às partes interessadas ou à Alta Administração para deliberação.

Art. 16. Os Processos de Trabalho necessários ao cumprimento dessa política, bem como os demais documentos elencados no **Art. 14** deste normativo serão catalogados no módulo próprio do Sistema de Apoio à Governança e à Gestão vigente, pela STI.

Art. 17. Em consonância com a Política nº 10, o dono do Processo de Backup e Retenção de Dados é o(a) Diretor(a) da STI.

Parágrafo único. O(s) gerente(s) Processo de Backup e Retenção de Dados será(ão) designado(s) pelo Dono do Processo.

Art. 18. Esta Política entra em vigor a partir da data de sua publicação.

EDUARDO SILVEIRA ROCHA
Diretor da Secretaria de Tecnologia da Informação