Tribunal Regional do Trabalho da 18ª Região Comissão de Segurança da Informação Núcleo de Governança Corporativa de TIC Setor de Segurança da Informação	Código: **NO07** Revisão: **0.0** Vigência: **(DATA DE PUBLICAÇÃO)** Classificação: **PÚBLICO** Ato normativo: **Portaria TRT 18ª GP/NGTIC Nº 014/2016**

BACKUP E RESTAURAÇÃO DE DADOS

1 OBJETIVO

Estabelecer requisitos para as cópias de segurança dos dados do Tribunal Regional do Trabalho da 18ª Região (TRT18) de modo que estejam íntegros e disponíveis às pessoas autorizadas.

2 APLICAÇÃO

Esta norma de segurança da informação aplica-se aos dados armazenados em meio digital produzidos ou manipulados no exercício das atividades do TRT18 e aos agentes responsáveis por esta produção ou manipulação.

3 REFERÊNCIA NORMATIVA

3.1 Portaria TRT18 GP/NGTIC 001/2016 e anexo "**PO01**", que aprova a revisão 1.1 das diretrizes da Política de Segurança da Informação e Comunicação do TRT18.

3.2 Portaria TRT18 GP/NGTIC nº 004/2016 e anexo "**NO01**", que aprova a revisão 1.1 das regras para utilização dos recursos de Tecnologia da Informação e Comunicação do TRT18.

3.3 Objetivo de Controle 12.3 da norma ABNT ISO/IEC 27002:2013 (código de prática para controles de segurança da Informação).

4 DEFINIÇÕES

4.1 **Administrador de Backup:** pessoa ou grupo responsável por atividades de planejamento e operação das atividades de *backup*, de acordo com a categoria de *backup* que administre.

4.2 ***Backup*:** cópia de segurança de arquivos e dados;

4.3 **Categoria de *backup*:** grupo de ativos de informação cujo *backup* é realizado

dentro de uma mesma rotina e seguindo um mesmo procedimento (e-mail, servidores de arquivo, bancos de dados Oracle, bancos de dados PostgreSQL, computadores de usuários, etc);

4.4 Equipe de *backup*: equipe composta pelo gerente e administradores de *backup*;

4.5 Gerente de *backup*: pessoa responsável pela coordenação das atividades de *backup* executadas e planejadas em conjunto com os administradores de *backup*.

4.6 Local de armazenamento: espaço de armazenamento lógico na mídia em que os dados serão gravados;

4.7 Repositório: local de guarda das mídias, podendo ser o cofre ou outro local apropriado;

4.8 Mídia: dispositivo de armazenamento de dados, podendo ser disco, fita, ou outro meio de armazenamento;

4.9 Período de retenção: período de tempo em que os dados gravados não podem ser apagados;

4.10 Restauração: procedimento por meio do qual as informações contidas no *backup* são recuperadas e disponibilizadas para uso;

4.11 Teste de restauração: procedimento que visa testar a efetividade das cópias de segurança;

5 RESPONSABILIDADES

5.1 É responsabilidade da administração disponibilizar à equipe de *backup* os recursos humanos, físicos e computacionais adequados para garantir a efetividade desta norma.

5.2 É responsabilidade dos usuários dos sistemas de informação manter os dados em locais de armazenamento compatíveis com sua classificação conforme regulamentação específica, de forma que tenham o tratamento devido.

5.3 Compete ao Gerente de Backup:

5.3.1 Coordenar as atividades de planejamento, operação e testes do backup, atuando como ponto de convergência dos administradores de backup;

5.3.2 Garantir a elaboração e atualização do documento de especificação de backup e demais documentos mencionados no item 6.

5.3.3 Aprovar os procedimentos pertinentes à operacionalização do *backup*.

5.3.4 Solicitar recursos para as operações de backup;

5.4 Compete ao Administrador de *backup*:

5.4.1 Planejar e operacionalizar o backup de dados referente à categoria de backup

que administre.

5.4.2 Elaborar e manter a documentação de *backup* dos dados **referente à categoria que administre, atualizada e** em conformidade com os normativos pertinentes;

5.4.3 Efetuar testes de restauração e seus registros;

5.4.4 Atender e registrar os chamados técnicos de restauração para as categorias de *backup* às quais se relaciona;

6 DOCUMENTAÇÃO

6.1 A STI deve elaborar, manter atualizada e em local padronizado a documentação referente aos seguintes aspectos do *backup*:

6.1.1 Documento de Especificação de *backup* considerando cada categoria de *backup e a classificação da informação, contemplando os seguintes aspectos:*

a) *as informações elegíveis a backup;*

b) a abrangência (por exemplo, completa ou diferencial);

c) frequência da geração das cópias;

d) período de retenção;

e) requisitos de segurança da informação envolvidos;

f) criticidade da informação para a continuidade da operação da organização;

g) transmissão das informações via rede de dados.

6.1.2 *Backup e* restauração de dados;

6.1.3 Testes de restauração;

6.1.4 Identificação, guarda, transporte e controle da vida útil das mídias;

6.1.5 Solicitações de inclusão de novos sistemas ou dados na abrangência do *backup*;

6.2 Deverão ser mantidos registros das operações de backup, restauração de dados e testes de restauração de dados.

7 MONITORAMENTO E MEDIÇÃO

7.1 O processo de geração das cópias de segurança deve garantir que registros completos e exatos da operação sejam gerados e mantidos em base de dados para fins de monitoramento e medição de eficácia.

7.2 A documentação de que trata o item 6 deverá apontar, em seção específica, indicadores que serão acompanhados periodicamente, incluindo inicialmente a porcentagem de operações de backup realizadas com sucesso e a porcentagem de testes de restauração realizados com sucesso.

8 ARMAZENAMENTO E SEGURANÇA

8.1 As cópias de segurança devem ser armazenadas em uma localidade remota, a uma distância suficiente para escapar dos danos de um desastre ocorrido no local principal.

8.2 As cópias de segurança devem possuir um nível apropriado de proteção física, lógica e ambiental, consistentes com as normas aplicadas na instalação principal.

9 TESTES DE RESTAURAÇÃO DOS DADOS

9.1 A STI deve realizar testes de restauração e manter registros destes testes.

9.2 Os testes de restauração devem ser realizados em local de armazenamento dedicado, não sobrepondo o local original;

9.3 Caso ocorra falha no teste, o gerente de backup deverá tomar as medidas necessárias à correção do problema.

10 DISPOSIÇÕES GERAIS

10.1 Os gerentes e administradores de backup deverão ser designados por meio de ato administrativo;

10.2 A primeira versão do documento de especificação do *backup* mencionado no item 6.1.1 deverá ser apresentada à Comissão de Segurança da Informação em até seis meses contados a partir da publicação deste normativo. Os demais documentos listados no item 6.1 deverão ser concluídos em seis meses a partir da publicação do documento de especificação de *backup*.