PODER JUDICIÁRIO FEDERAL
TRIBUNAL REGIONAL DO TRABALHO DA 7ª REGIÃO

ATO TRT7.GP Nº 88/2020

Aprova a Norma Complementar de Cópia de Segurança e de Restauração de Sistemas, Aplicativos, Dados e de Documentos no âmbito do Tribunal Regional do Trabalho da 7ª Região.

O PRESIDENTE DO TRIBUNAL REGIONAL DO TRABALHO DA 7ª REGIÃO, no uso de suas atribuições legais e regimentais,

CONSIDERANDO as boas práticas de Governança de TI que visam garantir a disponibilidade e integridade de sistemas, aplicativos, dados e de documentos digitais do TRT da 7ª Região;

CONSIDERANDO a Norma Complementar sobre os procedimentos de cópia de segurança e de restauração de sistemas, aplicativos, dados e de documentos digitais do Tribunal Regional do Trabalho da 7ª Região, aprovada pelo Ato TRT7 nº 02/2017;

CONSIDERANDO a solicitação de alteração da Norma Complementar nº 01/NC/STI/SESTI, requerida pelo Secretário de Tecnologia da Informação e Comunicação, mediante Ofício TRT7 SETIC Nº 003/2020 (Proad 6846/2019),

RESOLVE:

Art. 1º Aprovar a Norma Complementar nº 01/NC/SETIC, Revisão 02, da Secretaria de Tecnologia da Informação, que dispõe sobre procedimentos de cópia de segurança e de restauração de sistemas, aplicativos, dados e de documentos digitais do Tribunal Regional do Trabalho da 7ª Região, na forma do anexo, para observância e aplicação em todo o Regional.

Art. 2º Fica revogado o Ato nº 227, de 29 de maio de 2013

Art. 3º Este ato entra em vigor na data de sua publicação.

PUBLIQUE-SE. REGISTRE-SE. CUMPRA-SE.

Fortaleza, 04 de agosto de 2020.
PLAUTO CARNEIRO PORTO
Presidente do Tribunal

Secretaria de Tecnologia da Informação e Comunicação

Norma Complementar de Cópia de Segurança e Restauração de Sistemas, Aplicativos, Dados e Documentos Eletrônicos	Número	Revisão
	01/NC/SETIC	02

1 - Objetivo

Definir as diretrizes para cópia de segurança (backup) e restauração de sistemas, aplicativos, dados e documentos digitais a serem adotados pelo Tribunal Regional do Trabalho da 7ª Região a fim de zelar pela disponibilidade e integridade da informação.

2 - Fundamento Legal da Norma Complementar

2.1 - Cobit 5.1, DSS 04.07 - Gerenciar mecanismos de backup - “Manter a disponibilidade de informações críticas de negócios.”

2.2 - ABNT NBR ISO/IEC 27002:2013, Código de prática para a gestão de segurança de informação;

2.3 - O Ato TRT7 nº 2/2017 que define as diretrizes para a continuidade de TIC;

3 - Conceitos e Definições

Para os efeitos desta Norma Complementar são estabelecidos os seguintes conceitos e definições:

3.1 - **Dados** - Referem-se a uma escolha de informações organizadas, normalmente o resultado da experiência ou observação de outras informações dentro de um sistema de computador, ou um conjunto de instalações;

3.2 - **Bancos de Dados** - é o conjunto de dados de um ou mais sistemas de informação mantidos por um sistema gerenciador de banco de dados (software SGBD), como por exemplo a base de dados (conjunto) do sistema PJe de 1º Grau mantido pelo SGBD Postgres.

3.3 - **Cópia de Segurança (backup)** - É a cópia de um conjunto de dados de um dispositivo de armazenamento a outro para que possam ser restaurados em caso da perda dos dados originais, o que pode envolver apagamentos acidentais ou corrupção de dados;

Fonte: Diário Eletrônico da Justiça do Trabalho, Brasília, DF, n.3031, 05 ago. 2020. Caderno Administrativo do Tribunal Regional do Trabalho da 7ª Região, p. 1.

4 - Competência e Responsabilidades

4.1 - **Da Competência da Divisão de Infraestrutura de TIC**
4.1.1 - Compete à Divisão de Infraestrutura de TIC a programação, execução, monitoramento, recuperação, teste, documentação e guarda das cópias de segurança dos sistemas, aplicativos, dados e documentos digitais pertencentes ao Tribunal Regional do Trabalho da 7ª Região.

4.1.2 - Documentar, em repositório centralizado e com acesso restrito à SETIC, os procedimentos operacionais de backup, arquivamento e recuperação, contendo, no mínimo, a identificação dos equipamentos (nome, endereço IP), do conjunto de dados, do cronograma (dias e horários de execução), da política de cópia e retenção associadas.

4.1.3 - Administrar os componentes de hardware e softwares responsáveis pela realização das cópias de segurança e restauração.

4.1.4 - Realizar testes periódicos a fim de se evitar falhas críticas durante a realização de um backup ou restauração.

4.2 - O Diretor da Secretaria de Tecnologia da Informação através de Portaria indicará servidores para as funções de Gerência, Administração e Operação da Solução de Backup.

4.2.1 - O papel de gerência preferencialmente não deve ser exercido pelo mesmo servidor indicado para administração ou operação.

4.3 - Cabe ao Gerente de Backup:

- garantir que todos os sistemas informatizados em produção cuja necessidade de backup foi definida pelo comitê gestor de TIC possuam cópias de segurança;

- consultar as instâncias superiores e definir a periodicidade das cópias a serem realizadas;
- consultar as instâncias superiores e definir a criticidade e o tempo de retorno da informação.

4.4 - Cabe ao Administrador da Solução de Backup:

- configurar a frequência e o tipo de cópia de segurança a serem realizados;
- configurar o dispositivo de armazenamento de acordo com a criticidade da informação;
- definir procedimentos para a recuperação de dados;
- realizar testes periódicos de acordo com as especificações contidas nesse documento.

4.5 - Cabe ao Operador da Solução de Backup:

- verificar problemas na execução diária das cópias de segurança;
- gerenciar as possíveis falhas na realização da cópia de dados;
- enviar as fitas de Disaster Recovery para o cofre;
- trazer do cofre as fitas limpas a serem utilizadas em novas cópias de segurança;
- realizar operações de recuperação de dados.;
- auxiliar o administrador na realização dos testes periódicos.

5 - Dos Tipos de Cópia de Segurança

5.1 - **BACKUP**: é a cópia de dados de um dispositivo de armazenamento a outro para que possam ser restaurados em caso da perda dos dados originais, o que pode envolver apagamentos acidentais ou corrupção de dados. A cópia do BACKUP é destinada primordialmente a recuperação de dados para continuidade das operações. Desejável, conforme a criticidade do conjunto de dados para o negócio, que a cópia disponível para restauração do ambiente seja a mais recente possível, ou seja, deve atender o limite de tolerância da perda de dados definido na política de continuidade

de TIC do TRT7. Geralmente, são cópias diárias ou em intervalos menores, com retenção de curto prazo.

5.2 - **ARQUIVAMENTO**: é a cópia de dados de um dispositivo de armazenamento a outro, destinados principalmente, mas não unicamente, à recuperação de dados em momentos específicos do tempo, destinado a auditorias, análises ou recuperação de informação alterada. Geralmente são cópias semanais, mensais e anuais com retenção de longo prazo.

5.3 - **OFFSITE**: cópias de todos os dados referentes às políticas para armazenamento em cofre de mídia externo ao ambiente de produção.

5.4 - **ARQUIVOS DURÁVEIS**: alguns serviços baseados em nuvem não tem cópia de segurança que possibilite sua recuperação quando excluídos consciente e definitivamente pelo usuários, contudo são duráveis e com alta disponibilidade, características essas garantidas em contrato.

6 - Dos Tipos de Dados alvos da cópia de segurança

6.1 - Todas as informações pertinentes às atividades do Tribunal Regional do Trabalho devem entrar no planejamento das atividades de cópia de segurança, levando em consideração o tipo de cópia mais adequado para cada tipo de dado. Os tipos de dados incluem:

a) arquivos de usuários armazenados na rede, tais como documentos de texto e planilhas eletrônicas (MS-Office, OpenOffice);
b) dump dos bancos de dados das aplicações corporativas, tais como Oracle (PROAD, SPT1, SPT2, SIGEP, etc), PostgreSQL (PJe etc) e MySQL (Intranet, Site, etc);
c) arquivos de usuários armazenados em nuvem contratada, tais como documentos de texto, planilhas eletrônicas e arquivos pdf´s;
d) e-mails armazenados na solução de correio eletrônico*;*
e) arquivos de instalação e configuração, responsáveis pela disponibilização de serviços ou aplicações de TIC;
f) servidores virtuais, responsáveis pela disponibilização de serviços ou aplicações de TIC;

g) registros de operações (arquivos de logs) dos computadores servidores e ativos de rede.

7 - Das Estruturas de Hardware e Software

7.1 - Software de Backup: é o programa de computador para executar e gerenciar as operações de backup, arquivamento e recuperação;

7.2 - Cofre de Mídia: Estrutura resistente que armazena, protege e isola as mídias de dados de interferências externas degradantes;

7.3 - Subsistema automatizado de backup (robô): Unidade robótica que cataloga e controla o acionamento e a utilização de forma automática das fitas de armazenamento utilizadas para a realização das cópias.

8 - Das Políticas de Cópias de Segurança

8.1 - A execução das cópias deve, quando possível, ser definida para os horários de menor fluxo atividades na instituição.

8.2 - **Arquivos de usuários armazenados na rede corporativa - SEDE e INTERIOR**

Arquivos de usuários armazenados na rede corporativa - SEDE e INTERIOR			
Tipo de Cópia de Segurança	**Periodicidade**	**Retenção**	**Frequência de testes de restauração de dados**

Backup	Diário	Enquanto o arquivo existir, as 5 (cinco) últimas versões do arquivo serão armazenadas, sendo as versões antigas mantidas pelo prazo de 120 dias. No caso de arquivos deletados, a última versão será mantida pelo prazo de 365 dias.	Anual
Backup	Semanal	N/A	
Arquivamento	Diário	N/A	
Arquivamento	Mensal	N/A	
Arquivamento	Anual	Retenção de 5(cinco) anos	Sem teste, apenas monitoramento do log de execução
OFFSITE	Diariamente, em dias úteis		Anual, auditoria nos volumes por amostragem

8.3 - **Dump dos bancos de dados ORACLE (PROAD, SIGEP, etc)**

Dump dos bancos de dados ORACLE (PROAD, SIGEP, etc)			
Tipo de Cópia de Segurança	**Periodicidade**	**Retenção**	**Frequência de testes de restauração de dados**

Backup	Diário	Enquanto o banco existir, as 7 (sete) últimas versões do banco serão armazenadas, sendo as versões antigas mantidas pelo prazo de 30 dias. No caso de banco excluídos, a última versão será mantida pelo prazo de 30 dias.	Anual
Backup	Semanal	N/A	
Arquivamento	Diário	N/A	
Arquivamento	Mensal	1 ano	Anual
Arquivamento	Anual	5 anos	Sem teste, apenas monitoramento do log de execução
OFFSITE	Diariamente, em dias úteis		Anual, auditoria nos volumes por amostragem

8.4 - **Dump dos bancos de dados POSTGRESQL - PJe**

Dump dos bancos de dados POSTGRESQL - PJe			
Tipo de Cópia de Segurança	**Periodicidade**	**Retenção**	**Frequência de testes de restauração de dados**

Backup	Diário	Enquanto o banco existir, as 7 (sete) últimas versões do banco serão armazenadas, sendo as versões antigas mantidas pelo prazo de 30 dias. No caso de banco excluídos, a última versão será mantida pelo prazo de 30 dias.	Semestral
Backup	Semanal	N/A	
Arquivamento	Diário	N/A	
Arquivamento	Semanal	N/A	
Arquivamento	Mensal	1 ano	Anual
Arquivamento	Anual	5 anos	Sem teste, apenas monitoramento do log de execução
OFFSITE	Diariamente, em dias úteis		Anual, auditoria nos volumes por amostragem

8.5 - **Dump dos bancos de dados MYSQL e OUTROS**

Dump dos bancos de dados MYSQL e OUTROS			
Tipo de Cópia de Segurança	**Periodicidade**	**Retenção**	**Frequência de testes de restauração de dados**

Backup	Diário	Enquanto o banco existir, as 7 (sete) últimas versões do banco serão armazenadas, sendo as versões antigas mantidas pelo prazo de 30 dias. No caso de banco excluídos, a última versão será mantida pelo prazo de 30 dias.	Anual
Backup	Semanal	N/A	
Arquivamento	Diário	N/A	
Arquivamento	Mensal	1 ano	Anual
Arquivamento	Anual	5 anos	Sem teste, apenas monitoramento do log de execução
OFFSITE	Diariamente, em dias úteis		Anual, auditoria nos volumes por amostragem

8.6 - **Arquivos de usuários armazenados em nuvem contratada, tais como documentos de texto, planilhas eletrônicas e arquivos pdf´s;**

Tipo de Cópia de Segurança	Periodicidade	Retenção	Frequência de testes de restauração de dados

Backup	Diário	Última versão do arquivo, enquanto o arquivo existir. No caso de arquivos deletados, a última versão será mantida pelo prazo de 30 dias.	por demanda, pelo próprio usuário
Backup	Semanal	N/A	
Arquivamento	Diário	N/A	
Arquivamento	Mensal	N/A	
Arquivamento	Anual	N/A	
OFFSITE	N/A		

8.6.1 - As medidas de resiliência devem ser executadas automaticamente pela contratada, garantindo a durabilidade e disponibilidade mínimas definidas nas diretrizes de continuidade dos serviços de TIC do TRT7.

8.7 - **E-mails armazenados na solução de correio eletrônico**

Tipo de Cópia de Segurança	Periodicidade	Retenção	Frequência de testes de restauração de dados

Backup	Diário	No caso de mensagens deletadas, será mantida pelo prazo de 30 dias.	por demanda, pelo próprio usuário
Backup	Semanal	N/A	
Arquivamento	Diário	N/A	
Arquivamento	Mensal	N/A	
Arquivamento	Anual	N/A	
OFFSITE	N/A		

8.7.1 - Não haverá cópia de segurança para mensagens que tenham sido baixadas para a máquina do usuário por qualquer espécie de programa.

8.7.2 - Caso seja adotado o modelo de serviço em nuvem (SaaS) as medidas de resiliência devem ser executadas automaticamente pela contratada, garantindo a durabilidade e disponibilidade mínimas definidas nas diretrizes de continuidade dos serviços de TIC do TRT7.

8.8 - **Arquivos de instalação e configuração (binários, executáveis, bibliotecas, outros) responsáveis pela disponibilização de serviços ou aplicações de TIC**

Tipo de Cópia de Segurança	Periodicidade	Retenção	Frequência de testes de restauração de dados
Backup	Diário	Enquanto o arquivo existir, as 5 (cinco) últimas versões do arquivo serão armazenadas, sendo as versões antigas mantidas pelo prazo de 120 dias. No caso de arquivos deletados, a última versão será mantida pelo prazo de 365 dias.	Anual, por amostragem
Backup	Semanal	N/A	-
Arquivamento	Diário	N/A	
Arquivamento	Mensal	N/A	
Arquivamento	Anual	N/A	
OFFSITE	Diariamente, em dias úteis		Anual, auditoria nos volumes por amostragem

8.9 - **Máquinas Virtuais responsáveis pela disponibilização de serviços ou aplicações de TIC essenciais**

Tipo de Cópia de Segurança	Periodicidade	Retenção	Frequência de testes de restauração de dados
Backup	Diário (apenas máquinas essenciais com mudanças frequentes)	Última versão do arquivo.	Anual, por amostragem
Backup	Semanal	Última versão do arquivo.	Anual, por amostragem
Arquivamento	Diário	N/A	
Arquivamento	Mensal	N/A	
Arquivamento	Anual	N/A	
OFFSITE	Diariamente, em dias úteis		Anual, auditoria nos volumes por amostragem

8.10 - **Registro de operações (LOGS) dos computadores servidores e ativos de rede.**

Tipo de Cópia de Segurança	Periodicidade	Retenção	Frequência de testes de restauração de dados

Backup	Diário	O registro deverá ser mantido pelo prazo de 120 dias.	Anual
Backup	Semanal	N/A	-
Arquivamento	Diário	N/A	
Arquivamento	Mensal	N/A	
Arquivamento	Anual	5 anos	Sem teste, apenas monitoramento do log de execução
OFFSITE	Diariamente, em dias úteis		Anual, auditoria nos volumes por amostragem

9 - Da Rotina de Restauração de Cópia de Segurança

9.1 - As cópias de segurança serão restauradas mediante solicitação justificada pelos usuários.

9.2 - Considerando o sigilo das informações e os privilégios de acesso concedidos por força das atividades exercidas, o usuário não poderá solicitar a recuperação das informações fora da sua área de atuação, salvo situações específicas autorizadas pela Administração.

9.3 - Para requerer a recuperação de dados, o usuário deverá abrir uma solicitação através da Central de Serviços de TIC.

10 - Do Armazenamento das Cópias de Segurança

10.1 - As cópias de segurança tipo Offsite deverão ficar acondicionadas no cofre de mídia para preservar sua integridade física.

10.2 - As mídias de armazenamento que tenham o seu prazo de retenção expirado, mas que ainda sejam compatíveis com tecnologia empregada nos serviços de cópia de segurança, deverão ser reaproveitadas.

10.3 - As mídias de armazenamento defeituosas ou inservíveis deverão ser destruídas impossibilitando a recuperação por terceiros dos dados armazenados.

11 - Do Teste das Cópias de Segurança

11.1 - As cópias de segurança deverão ser testadas periodicamente, conforme estipulado nesta norma.

11.2 - O teste das cópias de segurança poderá envolver outras unidades, além da Divisão de Infraestrutura de TIC, para validação das informações recuperadas.

11.3 - O procedimento deverá garantir que o respectivo conteúdo seja recuperado em sua totalidade e de maneira íntegra.

11.4 - A validação das informações recuperadas deverão garantir que as mesmas estejam consistentes e em conformidade para eventuais processos de recuperação.

11.5 - A validação dos testes de recuperação será realizada pela DITIC e, sempre que possível, acompanhada pelo dono do serviço definido no catálogo de serviço de TIC, publicado na intranet.

11.6 - A validação dos dados Offsite será realizada através de uma auditoria dos volumes que armazenam essas informações, por amostragem não inferior à 10% do total.

12 - Do Registro e Documentação das Cópias de Segurança

12.1 - Deverá ser mantido registro eletrônico das operações de cópia de segurança atualizado para fins de auditoria.

13 - Vigência

13.1 - Esta Norma Complementar entra em vigor na data de sua publicação.