# ATOS DA PRESIDÊNCIA

## INSTRUÇÕES NORMATIVAS

### INSTRUÇÃO NORMATIVA TRE-RS P N. 98/2022.

DISPÕE SOBRE AS REGRAS E OS PROCEDIMENTOS PARA GERENCIAMENTO DE *BACKUP* E RESTAURAÇÃO DE DADOS NO ÂMBITO DA REDE CORPORATIVA DE DADOS DO TRIBUNAL REGIONAL ELEITORAL DO RIO GRANDE DO SUL.

O PRESIDENTE DO TRIBUNAL REGIONAL ELEITORAL DO RIO GRANDE DO SUL, no uso de suas atribuições legais e regimentais,

CONSIDERANDO a Resolução CNJ n. 396/2021, que institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ);

CONSIDERANDO a Resolução TSE n. 23.644/2021, que institui a Política de Segurança da Informação (PSI) no âmbito da Justiça Eleitoral;
CONSIDERANDO a Resolução TRE-RS n. 370/2021, que adota, no âmbito do Tribunal Regional Eleitoral do Rio Grande do Sul, a Resolução TSE n. 23.644/2021;
CONSIDERANDO a Portaria DG/TSE n. 444/2021, que dispõe sobre a instituição da norma de termos e definições relativas à Política de Segurança da Informação do Tribunal Superior Eleitoral;
CONSIDERANDO as boas práticas em segurança da informação, previstas nas normas ABNT ISO /IEC 27001 e ABNT NBR ISO/IEC 27002;
CONSIDERANDO as boas práticas em segurança da informação, previstas no modelo CIS Controls V.8;
CONSIDERANDO a Instrução Normativa TRE-RS P n. 88/2022, que dispõe sobre a instituição do Controle de Acesso Físico e Lógico aos ativos de informação no âmbito do Tribunal Regional Eleitoral do Rio Grande do Sul;
CONSIDERANDO que a segurança da informação e a proteção de dados pessoais são condições essenciais para a prestação dos serviços jurisdicionais e administrativos do Tribunal Regional Eleitoral do Rio Grande do Sul.
RESOLVE:
CAPÍTULO I
DISPOSIÇÕES PRELIMINARES
Art. 1º Instituir a norma complementar da Política de Segurança da Informação para gerenciamento das cópias de segurança (*backup*) e restauração de dados.
Art. 2º Esta norma tem por objetivo instituir diretrizes, responsabilidades e competências que visam garantir a segurança, integridade e disponibilidade dos dados custodiados pelo Tribunal Regional Eleitoral do Rio Grande do Sul (TRE-RS).
Art. 3º Os dados custodiados pelo TRE-RS, incluindo informações pessoais, dados biográficos, biométricos e corporativos, devem ser protegidos por meio de rotinas sistemáticas de *backup*.
Art. 4º Não estão cobertos por esta norma os dados armazenados localmente em microcomputadores, *notebooks*, dispositivos móveis ou outros dispositivos de uso individual.
Art. 5º A cópia de segurança e a recuperação dos dados de sistemas de informação custodiados por outras entidades, públicas ou privadas, utilizados pelo TRE-RS, deverão estar estabelecidas em cláusulas contratuais.
CAPÍTULO II
DAS DEFINIÇÕES
Art. 6º Para efeitos desta norma consideram-se os termos e definições previstos na Portaria DG /TSE n. 444/2021, além dos seguintes:
I - *backup* ou cópia de segurança: conjunto de procedimentos que permitem salvaguardar os dados de um sistema computacional, garantindo guarda, proteção e recuperação;
II - *backup* completo (ou total): modalidade de *backup* em que todos os dados a serem salvaguardados são copiados integralmente (cópia de segurança completa) para uma unidade de armazenamento, independentemente de terem sido ou não alterados desde o último *backup*;
III - *backup* diferencial: modalidade de *backup* em que são salvaguardados apenas dados novos ou modificados desde o último *backup* completo efetuado;
IV - *backup* incremental: modalidade de *backup* em que são salvaguardados apenas os dados novos ou modificados desde o último *backup* de qualquer modalidade efetuado;
V - criticidade: grau de importância dos dados para a continuidade das atividades e serviços da organização;
VI - descarte: eliminação correta dos dados, unidades de armazenamento e acervos digitais;

VII - janela de *backup*: período durante o qual, cópias de segurança sob execução agendada ou manual poderão ser executadas;
VIII - Plano de Gerenciamento de *Backup* e Restauração de Dados: documento formal onde são definidos os responsáveis pela cópia dos dados, o que será armazenado, a periodicidade de execução da cópia e a retenção, de acordo com as orientações da norma complementar da Política de Segurança da Informação para gerenciamento de *backup* e restauração de dados;
IX - restauração: processo de recuperação e disponibilização de dados salvaguardados em determinada imagem de *backup*;
X - retenção: período pelo qual os dados devem ser salvaguardados e estar aptos à restauração;
XI - rotina de *backup*: procedimento utilizado para se realizar um *backup*;
XII - unidade de armazenamento (ou mídia de *backup*): dispositivo para armazenamento de dados em suporte digital com características específicas para retenção de cópia de segurança de dados digitais.

CAPÍTULO III

DOS PADRÕES OPERACIONAIS

Seção I

Dos princípios gerais

Art. 7º As rotinas de *backup* devem ser orientadas para a restauração dos dados no menor tempo possível, principalmente quando um incidente ocasionar indisponibilidade de serviços de Tecnologia da Informação (TI).
Art. 8º As rotinas de *backup* devem possuir requisitos mínimos, diferenciados de acordo com o tipo de serviço de TI ou dado salvaguardado, dando prioridade aos serviços de TI críticos da organização.
Art. 9º As tecnologias utilizadas para a realização do *backup* devem cumprir os requisitos necessários para preservar a integridade, a confidencialidade, a disponibilidade e a irretratabilidade das informações.
Art. 10. Os dados abarcados por esta norma deverão ser definidos em um Plano de Gerenciamento de *Backup* e Restauração de Dados, a ser definido pela área técnica responsável, refletindo os requisitos de negócio da organização, bem como os requisitos de segurança da informação envolvidos.
Parágrafo único. O Plano de Gerenciamento de *Backup* e Restauração de Dados deve ser aprovado pela Comitê de Segurança da Informação e Proteção de Dados Pessoais (CSI).
Art. 11. A solicitação e validação de salvaguarda dos dados referentes aos serviços de TI deve ser realizada por seus responsáveis técnicos.
Art. 12. A infraestrutura de *backup* não pode utilizar os mesmos controladores de domínio do restante da infraestrutura e nem os dos usuários comuns, devendo ainda, ficar em rede totalmente apartada e protegida por equipamento de segurança de perímetros.
Art. 13. O Plano de Gerenciamento de *Backup* e Restauração de Dados deve explicitar, no mínimo, os seguintes requisitos técnicos:
I - escopo (dados a serem salvaguardados/restaurados);
II - modalidade de *backup* (*backup* completo, *backup* incremental e *backup* diferencial);
III - frequência (diária, semanal, mensal e anual);
IV - retenção;
V - unidade de armazenamento;
VI - janela de *backup*;
VII - local de guarda da unidade de armazenamento;
VIII - periodicidade de teste de restauração do *backup*.

Art. 14. A documentação do Plano de Gerenciamento de Backup e Restauração de Dados e das suas rotinas inerentes devem ser armazenadas em local seguro e com acesso restrito à área responsável pelo seu gerenciamento.

Art. 15. Os *backup*s devem estar em conformidade com a legislação vigente, em especial ao que compete à Lei Geral de Proteção de Dados (LGPD).

Art. 16. Os *backup*s devem ser armazenados de forma criptografada, considerando as melhores práticas de mercado e normas vigentes.

Parágrafo único. Deverão ser implementados controles criptográficos nos arquivos que trafegam na rede da organização ou na internet.

Art. 17. Deverão ser utilizadas soluções de *backup* e restauração de dados adequadas e especializadas, preferencialmente capazes de atuar de maneira automatizada.

Parágrafo único. Identificada a viabilidade de utilização de diferentes tecnologias na realização dos *backup*s, poderá ser escolhida a melhor solução para cada caso.

Art. 18. Poderão ser estabelecidos tipo, frequência e retenção diferenciados para cada serviço e/ou sistema de informação, de acordo com o seu nível de criticidade, desde que respeitados os padrões mínimos estabelecidos no Plano de Gerenciamento de *Backup* e Restauração de Dados.

Parágrafo único. Poderão ser utilizadas técnicas de compressão de dados, contanto que o acréscimo no tempo de recuperação dos dados seja considerado aceitável.

Art. 19. Expirado o prazo de retenção dos dados armazenados, a unidade de armazenamento poderá ser reutilizada.

Seção II

Do uso da rede

Art. 20. Deverá ser considerado, para a execução das rotinas de *backup*, o seu impacto sobre o desempenho da rede computacional, garantindo que o tráfego necessário para tal não cause indisponibilidade dos demais sistemas e serviços de TI.

Parágrafo único. O *backup* das informações armazenadas nos servidores da rede corporativa deve ser realizado em período de baixa utilização de seus recursos computacionais, preferencialmente fora do horário de expediente ordinário das unidades administrativas do Tribunal.

Seção III

Das unidades de armazenamento de *backup*s

Art. 21. A escolha das unidades de armazenamento utilizadas na salvaguarda dos dados deverá observar os custos de aquisição e de vida útil, bem como atender às seguintes características dos dados resguardados:

I - criticidade;

II - retenção;

III - probabilidade de necessidade de restauração;

IV - tempo esperado para restauração.

Art. 22. O *backup*, de acordo com sua criticidade, deve ser provido em 2 (duas) unidades de armazenamento distintas, com conteúdo idêntico, observado o seguinte:

I - uma cópia de segurança deve ser mantida em um local que permita sua rápida localização e recuperação;

II - outra cópia deve ser armazenada em local externo à sede do Tribunal;

III - ao menos uma cópia deve ser armazenada em local que não seja endereçável de forma contínua por meio de chamadas do sistema operacional.

Art. 23. Os locais de armazenamento das unidades devem, sempre que possível, ter mecanismos de segurança, considerando, minimamente, os seguintes elementos:

I - acesso restrito e monitorado;

II - acesso registrado em *logs*, contendo minimamente a identificação do usuário e informações de data e hora de entrada e saída;
III - possuir controles de prevenção, detecção e combate a incêndio;
IV - possuir proteção contra interferências eletromagnéticas.
§1º Os locais de armazenamento externos devem possuir requisitos de segurança adequados e separados do ambiente de armazenagem da cópia principal, de forma que não permaneçam expostos aos mesmos riscos de desastres.
§2º A cópia de segurança referida no inciso II do art. 22 pode ser armazenada em serviços de nuvem, desde que sejam criptografados e gerenciados pela mesma solução de *backup*, sendo observados, ainda, os cuidados de gerenciamento de acessos privilegiados e de bloqueio de redes de acesso.
Seção IV
Do descarte e da substituição da cópia de segurança
Art. 24. O descarte e a substituição da unidade de armazenamento utilizada para geração da cópia de segurança devem respeitar o disposto na norma complementar específica da Política de Segurança da Informação que trata do Controle de Acesso Físico e Lógico aos Ativos de Informação.
Art. 25. Nos casos de substituição da solução de *backup* (*hardware* ou *software*), as informações contidas nas unidades da antiga solução devem ser transferidas, em sua totalidade, para unidades compatíveis com a nova solução.
Art. 26. Quando da necessidade de descarte de unidades de armazenamento de *backup*s, tais recursos devem ser fisicamente destruídos de forma a inutilizá-los, atentando-se ao descarte sustentável e ambientalmente correto.
Parágrafo único. A solução de *backup* obsoleta somente poderá ser desativada após a certificação de que todas as informações foram transferidas para a nova solução implementada.
Seção V
Dos testes de restauração dos *backup*s
Art. 27. A restauração dos *backup*s deve ser testada periodicamente com o objetivo de garantir a sua confiabilidade e a integridade e disponibilidade dos dados salvaguardados.
Art. 28. Os testes de restauração dos *backup*s devem ser realizados em equipamentos servidores diferentes dos equipamentos que atendem os ambientes de produção, observados os recursos humanos e tecnológicos disponíveis.
Art. 29. A periodicidade, a abrangência, os procedimentos e as rotinas inerentes aos testes de restauração de *backup* devem ser devidamente registradas no Plano de Gerenciamento de *Backup* e Restauração de Dados.
CAPÍTULO IV
DAS RESPONSABILIDADES
Art. 30. São atribuições dos responsáveis pela execução e gestão das rotinas de *backup* e restauração:
I - planejar os recursos necessários para implantar os requisitos desta norma e do Plano de Gerenciamento de *Backup* e Restauração de Dados;
II - elaborar o Plano de Gerenciamento de *Backup* e Restauração de Dados específico;
III - propor soluções de *backup* das informações produzidas ou custodiadas pelo Tribunal;
IV - providenciar a criação e manutenção dos *backup*s;
V - configurar as soluções de *backup*;
VI - manter as unidades de armazenamento de *backup*s funcionais, preservadas e seguras;

VII - verificar periodicamente os eventos gerados pela solução de *backup*, tomando as providências necessárias para remediação de eventuais falhas;
VIII - gerenciar mensagens e registros de auditoria (*logs*) dos *backup*s;
IX - tomar medidas preventivas para evitar falhas;
X - reportar imediatamente os incidentes ou erros que causem indisponibilidade ou que impossibilitem a restauração dos *backup*s;
XI - providenciar a execução dos testes de restauração;
XII - restaurar ou recuperar os *backup*s em caso de necessidade.
CAPÍTULO V
DAS DISPOSIÇÕES FINAIS
Art. 31. Os casos omissos serão dirimidos pela Diretoria-Geral, ouvida a Comissão de Segurança da Informação e Proteção de Dados Pessoais deste Tribunal.
Art. 32. Fica revogada a Portaria P TRE-RS n. 204/2019.
Art. 33. Esta Instrução Normativa entrará em vigor na data de sua publicação.
DESEMBARGADOR FRANCISCO JOSÉ MOESCH,
PRESIDENTE.

# PORTARIAS

## PORTARIA TRE-RS P N. 1550, DE 13 DE DEZEMBRO DE 2022.

O DESEMBARGADOR FRANCISCO JOSÉ MOESCH, PRESIDENTE DO TRIBUNAL REGIONAL ELEITORAL DO RIO GRANDE DO SUL, NO USO DE SUAS ATRIBUIÇÕES LEGAIS, COM FUNDAMENTO NA RESOLUÇÃO TSE N. 23.448/2015,
RESOLVE,
Art. 1.º Designar o servidor Marcos Roberto Zerbin, Técnico Judiciário, Área Administrativa, do Quadro de Pessoal deste Tribunal, para a Função Comissionada de Assistente I (FC-1) da 017ª Zona Eleitoral de Cruz Alta/RS, a partir de 12-12-2022.
Art. 2.º Esta Portaria entra em vigor na data de sua publicação.
DESEMBARGADOR FRANCISCO JOSÉ MOESCH,
PRESIDENTE.

## PORTARIA TRE-RS P N. 1552, DE 13 DE DEZEMBRO DE 2022.

O DESEMBARGADOR FRANCISCO JOSÉ MOESCH, PRESIDENTE DO TRIBUNAL REGIONAL ELEITORAL DO RIO GRANDE DO SUL, NO USO DE SUAS ATRIBUIÇÕES LEGAIS, COM FUNDAMENTO NA RESOLUÇÃO TSE N. 23.448/2015,
RESOLVE,
Art. 1.º Dispensar o servidor Marco Antônio Randazzo, Analista Judiciário, Área administrativa, do Quadro de Pessoal deste Tribunal, da Função Comissionada de Assistente I (FC-1) da 039ª Zona Eleitoral de Rosário do Sul/RS, e designá-lo para a Função Comissionada de Chefe de Cartório (FC-6) da 039ª Zona Eleitoral de Rosário do Sul/RS, a partir de 19-12-2022.
Art. 2.º Designar o servidor Patrick Birkan Beria, Técnico Judiciário, Área Administrativa, do Quadro de Pessoal deste Tribunal, para a Função Comissionada de Assistente I (FC-1) da 039ª Zona Eleitoral de Rosário do Sul/RS, a partir de 19-12-2022.
Art. 3.º Esta Portaria entra em vigor na data de sua publicação.
DESEMBARGADOR FRANCISCO JOSÉ MOESCH,
PRESIDENTE.

# APOSTILAS