

Índice de Partes	
Índice de Processos	825

ATOS DO PRESIDENTE

PORTARIAS

PORTARIA N.º 467, DE 27 DE SETEMBRO DE 2021

O PRESIDENTE DO TRIBUNAL REGIONAL ELEITORAL DA BAHIA, no uso das atribuições que lhe são conferidas pelo art. 8º, da Resolução Administrativa TRE/BA n.º 1/2017, RESOLVE:

Art. 1º Dispensar, a pedido, SÍLVIA REBOUÇAS ROSADO DE CASTRO, servidora efetiva, da Função Comissionada de Chefe da Seção de Apoio e Assistência Jurídica - FC - 6, da Coordenadoria de Assuntos Jurídicos e Correcionais, da Secretaria da Corregedoria Regional Eleitoral, da Secretaria do Tribunal;

Art. 2º Dispensar ANABEL SOUZA AMORIM, servidora efetiva, da Função Comissionada de Assistente IV - FC - 4, da Secretaria da Corregedoria Regional Eleitoral, da Secretaria do Tribunal;

Art. 3º Designar ANABEL SOUZA AMORIM, Técnico Judiciário, Área Administrativa, NI, Classe C, Padrão 13, para exercer a Função Comissionada de Chefe da Seção de Apoio e Assistência Jurídica - FC - 6, da Coordenadoria de Assuntos Jurídicos e Correcionais, da Secretaria da Corregedoria Regional Eleitoral, da Secretaria do Tribunal;

Art. 4º Designar ALEXANDRA RODRIGUES VASQUES, Analista Judiciário, Área Judiciária, NS, Classe C, Padrão 13, para exercer a Função Comissionada de Assistente IV - FC - 4, da Secretaria da Corregedoria Regional Eleitoral, da Secretaria do Tribunal;

Art. 5º Esta Portaria entrará em vigor na data de sua publicação.

Salvador, 27 de setembro de 2021.

Desembargador ROBERTO MAYNARD FRANK

Presidente do Tribunal Regional Eleitoral da Bahia

PORTARIA Nº 433, DE 03 DE SETEMBRO/2021 PRE/SGPRE/ASSAD

Altera a Portaria n.º 356/2018, que institui Normas de Segurança da Informação (NSI) no âmbito do Tribunal Regional Eleitoral da Bahia, com alterações nos Anexos V e VII.

O PRESIDENTE DO TRIBUNAL REGIONAL ELEITORAL DA BAHIA, no uso de suas atribuições regimentais,

CONSIDERANDO a necessidade de continuamente estabelecer e revisar processos de segurança e privacidade da informação no âmbito da Justiça Eleitoral da Bahia,

CONSIDERANDO a utilização racional dos recursos de Tecnologia da Informação e Comunicação oferecidos aos usuários desta Corte,

RESOLVE:

Art. 1º Alterar a [Portaria n.º 356/2018](#), da Presidência, para promover alterações nos [Anexos V \(NSI-005 - Correio Eletrônico\) e VII \(NSI-007 - Procedimentos e Backup e Recuperação de Dados\)](#), com redações constantes no apêndice deste normativo.

Art. 2º Esta Portaria entrará em vigor na data de sua publicação.

Salvador, 03 de setembro de 2021.

Desembargador ROBERTO MAYNARD FRANK

Presidente do Tribunal Regional Eleitoral da Bahia

*Republicada em virtude de erro material.

ANEXO V

NSI-005 - Serviço de Correio Eletrônico Institucional

1. Objetivos

1. Estabelecer diretrizes e padrões para o uso do serviço de correio eletrônico no âmbito do Tribunal Regional Eleitoral da Bahia (TRE-BA).

2. Motivações

1. Alinhamento às normas, regulamentações e melhores práticas, relacionadas à matéria.

2. Proteção do ambiente tecnológico do Tribunal.

3. Correto direcionamento e dimensionamento de recursos tecnológicos para prover e controlar o serviço de correio eletrônico.

3. Referências normativas

1. Instrução Normativa GSI/PR nº 1, de 13 de junho de 2008, do Gabinete de Segurança Institucional da Presidência da República, que disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, e dá outras providências.

2. Norma Complementar 01/IN01/DSIC/GSIPR, de 15 de outubro de 2008, do Departamento de Segurança da Informação e Comunicações da Presidência da República, que estabelece critérios e procedimentos para elaboração, atualização, alteração, aprovação e publicação de normas complementares sobre a Gestão de Segurança da Informação e Comunicações, no âmbito da Administração Pública Federal, direta e indireta.

3. Norma Complementar nº 07/IN01/DSIC/GSIPR (Revisão 01), de 15 de julho de 2014, do Departamento de Segurança da Informação e Comunicações da Presidência da República, que estabelece diretrizes para a implementação de controles de acesso à Segurança da Informação e Comunicações nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta.

4. Norma Técnica ABNT NBR ISO/IEC 27001:2013, que especifica os requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão da segurança da informação dentro do contexto da organização.

5. Norma Técnica ABNT NBR ISO/IEC 27002:2013, que fornece diretrizes para práticas de gestão de segurança da informação.

4. Conceitos e definições

1. Arquivo de registro de mensagens (logs): registro de eventos relevantes, utilizados para restaurar um sistema, diagnosticar problemas ou realizar auditorias.

2. Caixa postal: conta de correio eletrônico onde são armazenadas as mensagens recebidas e/ou enviadas.

3. Caixa postal de sistema: conta de correio eletrônico de um sistema informatizado que necessite esse recurso para o seu funcionamento.

4. Caixa postal institucional pessoal: conta de correio eletrônico de uso individual.

5. Domínio: segunda parte do endereço de correio eletrônico, localizada após o símbolo arroba (@).

6. Endereço de correio eletrônico: conjunto de caracteres que individualiza e identifica o remetente e o destinatário da mensagem eletrônica. É formado por um identificador e por um domínio, separados pelo símbolo arroba (@).

7. Hoax: mensagem eletrônica encaminhada a muitos destinatários e de conteúdo geralmente alarmante e com pouca ou nenhuma veracidade, cujo objetivo é a propagação de boatos e informações distorcidas.

8. Identificador: primeira parte do endereço de correio eletrônico, localizada antes do símbolo arroba (@).

9. Lista de distribuição: agrupamento de caixas postais visando a distribuição de uma mensagem eletrônica a todos os seus integrantes.

10. Malware: programas indesejados, desenvolvidos com a finalidade de executar ações danosas e atividades maliciosas em um computador ou sistema, a exemplo de *worm*, *bot*, *spyware*, *backdoor*, cavalo de tróia, *ransomware* e *rootkit*.

11. Material criptografado: dados e/ou informações codificadas por meio de técnicas que impossibilitam o seu entendimento/leitura, cuja reversão ocorre somente com a utilização de uma senha previamente conhecida e/ou dispositivo criptográfico (ex.: *token*, *smart card*).

12. Phishing: fraude eletrônica, caracterizada pela tentativa de obtenção de dados e informações pessoais.

13. Serviço de correio eletrônico institucional: serviço de envio e recebimento de mensagens eletrônicas (e-mails) no âmbito do TRE-BA.

14. Spam: mensagem, sem valor institucional ou inútil à atividade funcional, enviada a um grande número de endereços de correio eletrônico.

15. Usuário de correio eletrônico: pessoa que possui uma caixa postal.

5. Caixas postais de correio eletrônico

1. As caixas postais são identificadas unicamente por meio de seu endereço eletrônico.

2. No âmbito do Tribunal, o domínio do endereço eletrônico é "tre-ba.jus.br".

3. A capacidade mínima de armazenamento das caixas postais é de 500 megabytes (MB).

4. Somente serão criadas caixas postais para uso institucional e por sistema informatizado.

5. As solicitações de criação, alteração e exclusão de caixas postais devem ser solicitadas por meio da Central de Serviços de TIC.

1. Caixas postais institucionais pessoais serão criadas quando da criação das contas de acesso à rede de dados.

2. As caixas postais institucionais das unidades serão automaticamente criadas utilizando-se suas siglas como identificadores.

6. No caso de alteração de endereço eletrônico, o endereço antigo será mantido como identificador alternativo.

7. Caixa postal institucional pessoal

1. Toda pessoa com conta de acesso à rede de dados do Tribunal possuirá uma caixa postal institucional pessoal.

5.7.1.1. É vedado o fornecimento de caixa postal institucional pessoal para servidores terceirizados.

2. Para pessoas sem conta de acesso à rede de dados, a solicitação de criação, alteração ou exclusão de caixa postal institucional pessoal deverá ser efetuada pela chefia imediata, no caso de requisitados e estagiários, pela Secretaria Judiciária em se tratando de membros da Corte e pelo chefe de cartório, quando for para juiz ou promotor eleitoral.

3. A identificação da caixa postal se dará por meio do número do título eleitoral, contendo 12 (doze) dígitos.

4. Cada usuário receberá, ainda, dois identificadores alternativos, sendo um formado pela primeira letra do prenome, primeira letra de sobrenome do meio e o último sobrenome, e outro composto pelo prenome, seguido do ponto (.) e do último sobrenome, no estilo prenome.sobrenome.

5. Em situações justificadas, poderá ser utilizado outro prenome ou sobrenome para a composição da identificação.

6. A adequação dos endereços de correio eletrônico que não correspondam ao padrão estabelecido nesta norma deverá ser solicitada à Central de Serviços de TIC pelo usuário.

5.7.2. A caixa postal institucional pessoal de magistrados e/ou servidores será excluída definitivamente nos casos de falecimento, exoneração, demissão, redistribuição, aposentadoria, remoção e cedência a outro órgão, ou retorno à origem.

1. Ocorridos os fatos descritos no item anterior, incumbe à Secretaria de Gestão de Pessoas comunicá-los à Secretaria de Tecnologia da Informação, no prazo de até 5 (cinco) dias úteis da publicação do Ato respectivo, exceto nos casos de demissão e exoneração, quando a comunicação deverá ocorrer de imediato à ciência do afastamento pela Secretaria de Gestão de Pessoas.

2. Nos casos de demissão e exoneração haverá suspensão imediata da caixa postal institucional, a partir da comunicação da Secretaria de Gestão de Pessoas.

1. A exclusão da caixa postal será realizada somente após comunicada pela Secretaria de Gestão de Pessoas a decisão definitiva sobre o afastamento.

3. Nos demais casos de que trata o item 5.7.2, incumbe à Secretaria de Tecnologia da Informação:

a. no prazo de 5 dias úteis, informar ao magistrado e ao servidor a data da exclusão definitiva da respectiva caixa postal;

b. no prazo de 20 dias, excluir definitivamente a caixa postal.

8. Caixa Postal de Sistema

5.8.1. A caixa postal de sistema será criada quando for necessária ao funcionamento de um sistema informatizado.

5.8.2. O gestor do sistema será o responsável pela respectiva caixa postal, competindo-lhe:

a. solicitar a criação, alteração e exclusão da caixa postal de sistema;

b. autorizar ou excluir o acesso de outros servidores.

5.8.3. O identificador do endereço de correio eletrônico será formado por denominação ou sigla que permita a identificação do respectivo sistema informatizado.

6. Lista de distribuição

1. É permitida a criação de lista de distribuição, com o objetivo de facilitar e otimizar a troca de informações sobre assuntos de interesse do Tribunal.

2. A criação de lista de distribuição poderá ser solicitada pelo gestor da unidade, núcleo, comissão ou grupo de trabalho ao qual se destina.

3. A solicitação deverá ser efetuada na Central de Serviços de TIC, acompanhada de justificativa e de informações sobre a finalidade da lista e, quando destinada a atividade temporária, do período de sua duração.

4. Cada lista de distribuição terá um gestor, a quem incumbe:

a. manter permanentemente atualizado o rol de integrantes da lista de distribuição;

b. solicitar exclusão como gestor e indicar, simultaneamente, o novo responsável pela lista de distribuição;

c. solicitar exclusão da lista de distribuição, quando esta não for mais necessária.

5. O identificador do endereço eletrônico será formado pela denominação ou sigla, que permita, de forma clara, a identificação de sua finalidade, ou do grupo de endereços eletrônicos nela reunidos.

6. No caso de alteração de endereço eletrônico, o endereço antigo será mantido como identificador alternativo.

7. Lista de distribuição de unidade

1. As unidades da estrutura organizacional do Tribunal possuirão lista de distribuição contendo as caixas postais de todos os integrantes da unidade.

1. As listas de secretarias, coordenadorias e assessorias conterão as caixas postais do titular e seus respectivos substitutos.

6.7.2. A lista de distribuição de unidade terá sua sigla como identificador do endereço de correio eletrônico.

7. Utilização dos recursos do sistema de correio eletrônico

1. As caixas postais dos usuários e as listas de distribuição do Tribunal Regional Eleitoral da Bahia destinam-se, exclusivamente, a atender à necessidade do serviço, não sendo permitido o seu uso para fins particulares.
2. A senha de acesso é pessoal e intransferível.
3. É vedada a tentativa de acesso a caixas postais às quais o usuário não tenha autorização de acesso.
4. É vedado o cadastramento de endereço de correio eletrônico institucional em qualquer tipo de *site* externo, salvo aqueles utilizados como fonte de pesquisa no desempenho das atividades funcionais.
5. O tamanho máximo da mensagem eletrônica, incluindo os anexos, não pode exceder 20 megabytes (MB).
1. Preferencialmente, os arquivos deverão ser compactados antes de anexados às mensagens de correio eletrônico.
2. Para arquivos maiores, outros meios de disponibilização deverão ser utilizados, desde que garantida a segurança dos dados.
3. Arquivos compartilhados com clientes externos (empresas e fornecedores) e que excedam o limite de 20 MB devem ser disponibilizados através de serviços externos (Google Drive, Dropbox e similares), e o link associado encaminhado ao interessado para *download*.
6. O envio de mensagem eletrônica para lista de distribuição que englobe elevado número de endereços eletrônicos somente é permitido em caráter excepcional e por aquelas unidades administrativas autorizadas pela Administração do Tribunal.
7. É de responsabilidade do usuário:
 - a. utilizar o correio eletrônico institucional de acordo com os preceitos desta Norma;
 - b. eliminar periodicamente as mensagens eletrônicas contidas na caixa postal de modo a mantê-la apta ao recebimento de novas mensagens;
 - c. não compartilhar o acesso à sua conta institucional pessoal de correio eletrônico;
 - d. realizar configurações, preferências, leitura e envio de mensagens de sua caixa postal eletrônica;
 - d) informar ao Comitê de Segurança da Informação o recebimento de mensagem que contrarie o disposto no item 7.8.
8. É vedado aos usuários o envio de qualquer mensagem eletrônica contendo:
 - a. informações privilegiadas, confidenciais e/ou de propriedade do Tribunal para destinatários não autorizados;
 - b. materiais obscenos, ilegais ou antiéticos;
 - c. materiais preconceituosos ou discriminatórios;
 - d. materiais caluniosos ou difamatórios;
 - e. propaganda com objetivo comercial;
 - f. listagem com endereços eletrônicos institucionais;
 - g. *malwares*;
 - h. material de natureza político-partidária, associativa ou sindical, que promova a eleição de candidatos para cargos eletivos;
 - i. material protegido por lei de propriedade intelectual;
 - j. entretenimentos e "correntes";
 - l. assuntos ofensivos;
 - m. músicas, vídeos ou animações que não sejam de interesse específico do trabalho;
 - n. *Spam*, *phishing* e *hoax*;
 - o. materiais criptografados.

9. Desde que previamente submetido e autorizado pela Administração do Tribunal, fica permitido o encaminhamento de mensagens com imagens vinculadas à atividade institucional, bem como campanhas de arrecadação e outras iniciativas que promovam a integração e o bem-estar do servidor do Tribunal.

8. Monitoramento e Auditoria

1. O conteúdo das caixas postais é passível de monitoramento e rastreamento por meio de ferramentas com o intuito de impedir o recebimento de *spam*, *hoax*, *phishing*, mensagens contendo vírus e outros arquivos, que coloquem em risco a segurança da infraestrutura tecnológica do Tribunal ou que contenham conteúdo impróprio.

2. As mensagens com anexos digitais poderão ser bloqueadas por mecanismo automático, sem comunicação prévia, caso seja detectado risco à segurança da rede.

8.2.1. A Secretaria de Tecnologia da Informação acompanhará a regular utilização e o desempenho do serviço de correio eletrônico institucional, comunicando ao usuário e a sua chefia imediata a ocorrência de situação não condizente com o estabelecido nesta Norma.

3. As auditorias ordinárias ou extraordinárias pela Secretaria de Tecnologia da Informação e os relatórios serão encaminhados ao Comitê de Segurança da Informação.

4. As auditorias extraordinárias deverão ser precedidas de autorização do Comitê de Segurança da Informação.

5. Os arquivos de registro de mensagens eletrônicas (*logs*) serão mantidos pelo prazo de 30 dias, exceto nos casos de auditoria ou notificação administrativa ou judicial, em que serão devidamente armazenados pelo Comitê de Segurança da Informação, a fim de salvaguardar os dados respectivos.

6. A Secretaria de Tecnologia da Informação encaminhará, até o dia 5 de dezembro de cada ano, relatório às unidades e aos respectivos gestores, com o rol das listas de distribuição e caixas postais a elas vinculadas, bem como a lista de eventuais caixas postais de estagiários lotados na respectiva unidade.

1. Caberá ao gestor responsável conferir os dados do relatório referido no item anterior e, até o dia 15 de dezembro do mesmo ano, indicar as alterações e exclusões necessárias.

7. A inobservância do quanto disposto nesta Norma ensejará a aplicação de medida disciplinar, assegurados o contraditório e a ampla defesa.

ANEXO VII

NSI-007 - Procedimentos de *Backup* e Recuperação de Dados

1. Objetivos

1.1. Estabelecer diretrizes e padrões para os procedimentos de *backup*, testes e recuperação de dados realizados pela Secretaria de Tecnologia da Informação, no âmbito do Tribunal Regional Eleitoral da Bahia.

2. Motivações

2.1. Alinhamento às normas, regulamentações e melhores práticas relacionadas à matéria.

2.2. Garantir a salvaguarda das informações de forma sistematizada e otimizada, atendendo às necessidades do Tribunal.

3. Conceitos e definições

3.1. *Backup* de dados - procedimento de transmissão de dados, por meio de cópia, de uma mídia (a principal) para outra (secundária) apartada da primeira, garantindo a salvaguarda.

3.2. *Backup* completo - são transmitidos todos os arquivos da mídia principal existentes no momento do *backup*.

3.3. *Backup* diário - procedimento realizado diariamente visando a criação de versões de *backup* menores (diárias).

3.4. *Backup* diferencial - somente os arquivos novos ou modificados desde o último *backup* são transmitidos.

3.5. *Backup* permanente - versão dos dados salvaguardados de modo permanente. No entanto, contém apenas os dados existentes no momento da cópia.

3.6. Disco rígido local - dispositivo de armazenamento de dados utilizados pelos computadores pessoais.

3.7. Equipamento servidor - computador com alta capacidade de armazenamento e processamento, destinado ao provimento de serviços e sistemas de TIC.

3.8. Especificação - conjunto e abrangência de dados especificados no Sistema de Proteção de Dados.

3.9. Fitas LTO - são mídias magnéticas de alta capacidade utilizadas para armazenar arquivos de *backup* de dados por longos períodos, em local protegido e diverso do ambiente dos dados originais.

3.10. RPO (Recovery-Point Objective) - o quanto é necessário voltar no tempo para encontrar um backup dos dados, ou seja, o tempo máximo de perda de dados.

3.11. RTO (*Recovery-Time Objective*) - tempo estimado para restaurar os dados ou para tornar novamente operacionais os sistemas afetados.

3.12. Sistema de Proteção de Dados - serviço automatizado de cópia e restauração de dados instalado no Datacenter do Tribunal.

4. Referências Normativas

4.1. Instrução Normativa GSI/PR nº 1, de 13 de junho de 2008, do Gabinete de Segurança Institucional da Presidência da República, que disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, e dá outras providências.

4.2. Norma Técnica ABNT NBR ISO/IEC 27001:2013, que especifica os requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão da segurança da informação dentro da organização.

4.3. Norma Técnica ABNT NBR ISO/IEC 27002:2013, que fornece diretrizes para práticas de gestão de segurança da informação.

5. Procedimentos de *backup* institucional

5.1. Os procedimentos de *backup* realizados pela Secretaria de Tecnologia da Informação serão executados de forma automática, de acordo com as especificações configuradas no Sistema de Proteção de Dados e abrangem os dados armazenados nos equipamentos servidores do Datacenter do Tribunal.

5.1.1. Excepcionalmente, procedimentos manuais de *backup* poderão ser realizados.

5.2. Os dados serão transferidos para fitas LTO que serão guardadas em cofre instalado em local diverso e afastado do Datacenter do Tribunal.

5.2.1. A retenção de dados padrão para as fitas será de 10 semanas.

5.2.2. *Backups* completos gerados na última semana de cada mês terão proteção permanente.

5.2.3. Outras mídias poderão ser armazenadas no cofre, desde que contendo dados corporativos do Tribunal.

5.3. Os *backups* diferenciais serão configurados para se iniciarem diariamente em horário entre 0h e 4h.

5.4. Os *backups* completos serão configurados para se iniciarem nas madrugadas dos sábados.

5.5. A Secretaria de Tecnologia da Informação deverá elaborar e submeter à aprovação do CGovTIC planilha contendo os esquemas de *backup*, os quais devem abranger as seguintes informações:

I - Tipo do *backup*: diferencial, completo, mensal e eventual (de ocorrência pontual ou sazonal);

II - Especificação;

III - Horário de início do *backup*;

IV - Duração estimada do *backup*;

V - Tempo de retenção;

VI - Tempo máximo de perda dos dados (RPO);

VII - Tempo estimado para a restauração dos dados (RTO).

5.5.1. Após aprovação, a planilha deverá ser publicada na Intranet do Tribunal.

5.5.2. A planilha deverá ser revisada anualmente ou em menor tempo, quando necessário.

5.6. As atividades técnicas relativas aos procedimentos de *backup* institucional deverão estar documentadas em base de conhecimento da Intranet do Tribunal e estar acessível somente ao pessoal da unidade responsável pela infraestrutura de tecnologia da informação e comunicação.

5.7. As mídias de *backup* deverão estar identificadas por etiqueta e, quando se tratarem de fitas LTO, com descrição que as associem às especificações do Sistema de Proteção de Dados.

5.7.1. A movimentação de mídias de *backup* deverá ser realizada por servidor da área de infraestrutura de tecnologia da informação e comunicação, com a devida proteção contra extravios e eventos que possam causar dano físico.

6. Procedimentos de *backup* de dados corporativos

6.1. Todos os arquivos corporativos digitais relacionados ao trabalho das unidades da Secretaria do Tribunal e cartórios eleitorais devem ser armazenados, exclusivamente, nos equipamentos de armazenamento de arquivos providos pela Secretaria de Tecnologia da Informação.

6.1.1. Na Secretaria do Tribunal e cartórios eleitorais da Capital, os arquivos corporativos deverão ser armazenados diretamente nos equipamentos do Datacenter, acessíveis através de mapeamento de rede.

6.1.1.1. O mapeamento padrão (pastas "PÚBLICA" e "RESTRITA") deverá ser utilizado da seguinte maneira:

- Pasta "RESTRITA" da unidade: área com acesso controlado que deverá armazenar os arquivos permanentes da unidade;
- Pasta "PÚBLICA" da unidade: área com retenção temporária, acessível aos demais usuários (com permissão apenas de leitura, por padrão).

6.1.1.1.2. A pasta "PÚBLICA" será excluída diariamente, não sendo realizado backup do seu conteúdo.

6.1.1.2. Os arquivos compartilhados permanentemente entre as unidades administrativas do TRE /BA devem utilizar o Repositório Digital (link <http://repositorio.tre-ba.jus.br/share/page/>), que é a área oficial para compartilhamento de dados (em substituição à pasta "PÚBLICA").

6.1.1.3. Para a exclusão dos dados da área "PÚBLICA" será concedido o prazo de 10 (dez) dias, a partir da publicação desta norma, devendo cada unidade, caso queira, providenciar a cópia para o Repositório Digital.

6.1.2. Nos cartórios eleitorais do interior do Estado, os arquivos corporativos deverão ser armazenados, de modo centralizado, em equipamento específico (mini NAS) a ser provido pela Secretaria de Tecnologia da Informação.

6.1.2.1. Os arquivos corporativos serão regularmente replicados para o Datacenter do Tribunal, de modo que integrem o *backup* institucional.

6.1.3. É vedada a gravação de arquivos pessoais nos equipamentos de armazenamento.

6.1.3.1. Se constatada a existência de arquivos pessoais armazenados nos servidores de arquivos, tal fato será comunicado ao titular da unidade responsável pelos dados, com indicativo de exclusão.

6.1.4. A Secretaria de Tecnologia da Informação não se responsabilizará pela salvaguarda de arquivos pessoais e corporativos armazenados no disco rígido local das estações de trabalho e *notebooks*, nem prestará suporte à realização de *backup* desses dados pelo usuário.

6.1.4.1. A salvaguarda das pastas locais de clientes de correio eletrônico é de responsabilidade do usuário para a qual poderá obter orientações e suporte.

7. Recuperação de dados

7.1. A recuperação de dados, sempre que não puder ser realizada pelo próprio usuário, deverá ser solicitada à Secretaria de Tecnologia da Informação, por meio da Central de Serviços de TIC (CESTIC).

8. Testes de recuperação de dados

8.1. Mensalmente deverão ser realizados testes de recuperação de dados.

8.2. Os testes deverão ser baseados em dados pré-selecionados que garantam a efetividade, eficiência e confiabilidade do procedimento, para todas as especificações de *backup* definidas no Sistema de Proteção de Dados.

8.3. Os meios para viabilização dos testes deverão ser implementados pelas áreas técnicas responsáveis.

8.4. A validação se dará por amostragem e verificação de alguns arquivos ou serviços recuperados.

8.4.1. A área responsável pelos procedimentos de salvaguarda institucional de dados deverá manter, em sua base de conhecimento, documentação atualizada de testes e validação de dados recuperados, descrevendo os procedimentos, as especificações de *backup*, as equipes responsáveis pela recuperação, o escopo da recuperação, as equipes responsáveis pela validação dos dados ou sistemas recuperados e como se deverá efetuar a validação.

9. Revisões de documentação técnica

9.1. Toda documentação técnica relacionada a procedimentos de *backup* e recuperação de dados deverá ser revisada em ciclos máximos de um ano e submetida ao CGesTIC para aprovação.

ATOS DO CORREGEDOR REGIONAL ELEITORAL

PORTARIAS

PORTARIA CRE-BA Nº 12/2021

O CORREGEDOR REGIONAL ELEITORAL, DESEMBARGADOR MÁRIO ALBERTO SIMÕES HIRS, no uso de suas atribuições legais e regimentais e considerando os objetivos da Secretaria da Corregedoria Regional Eleitoral da Bahia firmados no Plano Estratégico Setorial;

RESOLVE

Art. 1º Determinar a realização de mutirão, no período de 16 de novembro a 17 de dezembro do corrente ano, a fim de auxiliar nos trabalhos atinentes às unidades da Coordenadoria de Assuntos Jurídicos e Correcionais (COAJUC) da Secretaria da Corregedoria Regional Eleitoral (SCR).

§ 1º Os trabalhos serão realizados no município de Salvador, na Coordenadoria de Assuntos Jurídicos e Correcionais (COAJUC).

§ 2º A coordenação dos trabalhos ficará sob a responsabilidade da servidora Carmen Lúcia Costa Brotas.

Art. 2º Designar os servidores abaixo relacionados para integrar a equipe que desenvolverá os trabalhos:

Arivaldo Fraga Carvalho Júnior - 136ª ZE (Itajuípe)

Arnaldo Santana Neves Sobrinho - 135ª ZE (Coaraci)

Luisa Fonseca Tapioca - 103ª ZE (Miguel Calmon)

Manuela Gomes da Silva - 115ª ZE (Saúde)