ANEXO VII

• *Anexo VII alterado pela Portaria 433/21.*

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 "PUBLICA" 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 "PUBLICA" da unidade: área com retenção temporária, acessível aos demais usuários (com permissão apenas de leitura, por padrão).

6.1.1.1.2. A pasta "PUBLICA" 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 'PUBLICA").

6.1.1.3. Para a exclusão dos dados da área "PUBLICA" 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.

ANEXO VIII

• *Anexo VIII acrescentado pela Portaria 52/19*.

NSI-008 - Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais ETIR

1. Objetivo

1.1. Estabelecer as diretrizes para o funcionamento da Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR) do Tribunal Regional Eleitoral da Bahia.

2. Motivações

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

2.2. Necessidade de formalização da Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR) e seu do funcionamento.

2.3. Proteção do ambiente tecnológico do Tribunal.

3. Referências Normativas

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

3.2. Norma Complementar nº 05/IN01/DSIC/GSIPR, de 14 de agosto de 2009, do Departamento de Segurança da Informação e Comunicações da Presidência da República, que disciplina a criação de Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais ETIR nos órgãos e entidades da Administração Pública Federal, direta e indireta APF.

3.3. Norma Complementar nº 08/IN01/DSIC/GSIPR, de 19 de agosto de 2010, do Departamento de