Portaria nº 356/2018- Institui Normas de Segurança da Informação (NSI) - NSIs nsº 001 a 006

ANEXO I

NSI-001 – Gestão de Incidentes em Segurança da Informação;

1.0. Objetivos

1.1. Estabelecer as diretrizes e definir o processo de Gestão de Incidentes de Segurança da Informação relacionada ao ambiente tecnológico no âmbito deste Tribunal.

2. Motivações

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

2.2. Tratamento rápido e eficiente dos incidentes de segurança da informação.

2.3. Otimização da aplicação de recursos tecnológicos e humanos na Gestão de Incidentes de Segurança da Informação.

2.4. Formalização de processo sistemático para gestão dos incidentes de segurança da informação, provendo insumos com vistas a minimizar ou evitar eventos futuros.

3. Referências normativas

3.1. Norma Complementar nº 01/IN01/DSIC/GSIPR, de 13 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.

3.2. 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 Segurança da Informação e Comunicações da Presidência da República, que disciplina o gerenciamento de Incidentes de Segurança em Redes de Computadores realizado pelas Equipes de Tratamento e Resposta a Incidentes de Segurança em Redes Computacionais – ETIR dos órgãos e entidades da Administração Pública Federal, direta e indireta – APF.

3.4. 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 da organização.

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

Norma Complementar nº 21/IN01/DSIC/GSIPR, de 08 de outubro de 2014, do Departamento de Segurança da Informação e Comunicações da Presidência da República, que estabelece asDiretrizes para o Registro de Eventos, Coleta e Preservação de Evidências de Incidentes de Segurança em Redes nos órgãos e entidades da Administração Pública Federal, direta e indireta.

4. Conceitos e definições

4.1. Artefato malicioso: é qualquer programa de computador, ou parte de um programa, construído com a intenção de provocar danos, obter informações não autorizadas ou interromper o funcionamento de sistemas e/ou redes de computadores.

4.2. Ativos de Informação: os meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso.

4.3. Usuários: magistrados e servidores ocupantes de cargo efetivo ou em comissão, requisitados e cedidos, desde que previamente autorizados, empregados de empresas prestadoras de serviços terceirizados, consultores, estagiários, e outras pessoas que se encontrem a serviço da Justiça Eleitoral, utilizando em caráter temporário os recursos tecnológicos do TRE.

4.4. Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais – ETIR: Grupo de pessoas com a responsabilidade de receber, analisar e responder às notificações e atividades relacionadas a incidentes de segurança em redes de computadores.

4.5. Evento de segurança da informação: ocorrência identificada de um sistema, serviço ou rede, que indica uma possível violação da política de segurança da informação ou falha de controles, ou uma situação previamente desconhecida, que possa ser relevante para a segurança da informação.

4.6. Incidente de segurança da informação: é indicado por um simples ou por uma série de eventos de segurança da informação indesejados ou inesperados, que tenham uma grande probabilidade de comprometer as operações do negócio e ameaçar a segurança da informação.

4.7. Medida de contenção: controle e/ou ação tomada para evitar que danos causados por um determinado incidente continuem aumentando com o passar do tempo. Além disso, tais medidas visam o restabelecimento do sistema/serviço afetado, mesmo que não seja em sua capacidade total.

4.8. Medida de solução: controle e/ou ação tomada para sanar vulnerabilidades e problemas que sejam a causa-raiz de um ou mais incidentes de segurança da informação.

4.9. Tratamento de Incidentes de Segurança em Redes Computacionais: é o serviço que consiste em receber, filtrar, classificar e responder às solicitações e alertas e realizar as análises dos incidentes de segurança, procurando extrair informações que permitam impedir a continuidade da ação maliciosa e também a identificação de tendências.

4.10. Vulnerabilidade: é qualquer fragilidade dos sistemas computacionais e redes de computadores que permitam a exploração maliciosa e acessos indesejáveis ou não autorizados.

4.11. CTIR GOV: Centro de Tratamento e Resposta a Incidentes de Segurança em Redes de Computadores da Administração Pública Federal, subordinado ao Departamento de Segurança de Informação e Comunicações – DSIC do Gabinete de Segurança Institucional da Presidência da República – GSI; (item incluído pela Portaria nº 7.137/2017).

5. Escopo

A Gestão de Incidentes de Segurança da Informação, definida nesta Norma, tem seu escopo limitado às situações relacionadas ao ambiente, ativos, projetos e processos de TIC, que suportam os principais processos de negócio do Tribunal Regional Eleitoral da Bahia (TRE-BA).

6. Diretrizes

6.1. A Gestão de Incidentes de Segurança da Informação tem como principal objetivo assegurar que incidentes de segurança da informação sejam identificados, registrados e avaliados em tempo hábil, com a tomada de medidas de contenção e/ou solução adequadas.

6.2. Estão abrangidos por esta Norma os eventos, confirmados ou suspeitos, relacionados à segurança de sistemas ou redes computacionais, que comprometam o ambiente tecnológico do TRE-BA, seus ativos, informações e processos de negócio, bem como aqueles que contrariem a Política de Segurança da Informação da Justiça Eleitoral, e dos quais decorram interrupção ou indisponibilidade de serviço essencial ao desempenho das atividades, vulnerabilidades de segurança, divulgação, alteração ou destruição de informações e/ou prática de ato definido como crime ou infração administrativa.

6.3. O Tribunal providenciará dispositivos de monitoramento, ferramentas de segurança e detecção de intrusão, a fim de subsidiar a Gestão de Incidentes de Segurança da Informação.

7. Processo de Gestão de Incidentes de Segurança da Informação

7.1. O processo de Gestão de Incidentes de Segurança da Informação é contínuo e aplicado na implementação e operação do Sistema de Gestão de Segurança da Informação (SGSI).

7.2. O processo de Gestão de Incidentes de Segurança da Informação é composto pelas seguintes etapas:

7.2.1. Detecção e registro: compreende o recebimento, registro e autorizações necessárias para o encaminhamento da investigação.

7.2.2. Investigação e contenção: compreende a investigação e tratamento do incidente, coleta de dados, comunicação às áreas afetadas e proposição e aplicação de ações de contenção, quando necessárias.

7.2.3. Encerramento: compreende a análise do incidente, com verificação da necessidade de outras ações, providências ou comunicações, e após seu cumprimento, o encerramento do incidente.

7.2.4. Avaliação de incidentes: compreende a avaliação do histórico de incidentes, com consolidação das informações e indicadores e verificação das oportunidades de melhoria e lições aprendidas.

7.3. Os incidentes, notificados ou detectados, devem ser objeto de registro, com a finalidade de assegurar a manutenção do histórico e auxiliar na geração de indicadores.

7.4. A notificação de incidente poderá ser feita por qualquer usuário, sem necessidade de prévia autorização do gestor, através de registro na Central de Serviços de TIC (CESTIC) via Intranet ou por contato telefônico.

7.5. Os usuários devem notificar, o mais breve possível, os incidentes de segurança da informação e vulnerabilidades de que tenham conhecimento (constatação ou suspeita).

7.6. Vulnerabilidades ou fragilidades suspeitas não devem ser objeto de teste ou prova pelos usuários, sob o risco de violar a Política de Segurança da Informação da Justiça Eleitoral e/ou provocar danos aos serviços ou recursos tecnológicos.

7.7. As equipes da Secretaria de Tecnologia da Informação responsáveis pelo monitoramento dos ativos, serviços e sistemas devem notificar os incidentes a eles relacionados à Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais – ETIR, para o devido registro e providências.

7.8. O Tribunal poderá receber notificações externas (CTIR.BR, CSIRT ou outras empresas) sobre incidentes (ocorridos ou suspeitos) por meio de sistemas gerenciadores de demandas, e-mail, telefone, etc. que deverão ser remetidas à Comissão de Segurança da Informação (CSI) para o devido encaminhamento.

7.9. O tratamento da informação deve ser realizado de forma a viabilizar e assegurar a disponibilidade, integridade, confidencialidade e autenticidade da informação, com retorno das operações à normalidade no menor prazo possível, bem como evitar futuras ocorrências, com a proposição de ações de solução, quando existentes.

7.10. A ETIR deve, em conjunto com as outras áreas da Secretaria de Tecnologia da Informação, investigar o incidente e artefatos maliciosos, propondo e implementando as ações de contenção, comunicando as áreas afetadas e coletando os dados necessários.

7.11. A coleta de evidência dos incidentes de segurança da informação deve ser realizada pela CSI.

7.12. Quando o incidente de segurança da informação decorrer de suspeita de descumprimento da Política de Segurança da Informação da Justiça Eleitoral, será observado o sigilo durante todo o processo, ficando as evidências, informações e demais registros restritos aos envolvidos na investigação.

7.13. Quando houver indícios de ilícitos criminais durante a gestão dos incidentes de segurança, o Comitê de Segurança da Informação deverá ser comunicado para avaliação das providências cabíveis.

7.14. O encerramento do incidente de segurança da informação será realizado pela CSI, com comunicação a todas as áreas interessadas, bem como ao Centro de Tratamento de Incidentes de Segurança de Redes de Computadores da Administração Pública Federal (CTIR.BR), na forma e nos casos definidos pelo referido órgão.

7.15. A avaliação do processo de gestão de incidentes de segurança da informação ocorrerá através do histórico de incidentes, com verificação das oportunidades de melhoria.

ANEXO II

NSI-002 – Uso de Recursos de Tecnologia da Informação e Controle de Acesso

1. Objetivos

1.1. Estabelecer diretrizes e padrões para a utilização dos recursos de tecnologia da informação e para o controle de acesso no âmbito do Tribunal Regional Eleitoral da Bahia (TRE-BA).

2. Motivações

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

2.2. Garantia de que os acessos aos recursos tecnológicos sejam feitos de forma segura e controlada.

2.3. Necessidade de um processo sistemático para gerenciar o uso de recursos de tecnologia da informação, visando garantir a segurança e continuidade das atividades do Tribunal.

3. Referências normativas

3.1. 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.

3.2. 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.

3.3. Norma Complementar 10/IN01/DSIC/GSIPR, de 30 de janeiro de 2012, que estabelece diretrizes para o processo de Inventário e Mapeamento de Ativos de Informação nos Aspectos Relativos à Segurança da Informação e Comunicações nos órgãos e entidades da Administração Pública Federal.

3.4. Norma Complementar 12/IN01/DSIC/GSIPR, de 30 de janeiro de 2012, que estabelece diretrizes para o Uso de Dispositivos Móveis nos Aspectos relativos à Segurança da Informação e Comunicações nos órgãos e entidades da Administração Pública Federal.

3.5. 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.

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

3.7. Norma Complementar nº 21/IN01/DSIC/GSIPR, de 08 de outubro de 2014, que estabelece as Diretrizes para o Registro de Eventos, Coleta e Preservação de Evidências de Incidentes de Segurança em Redes nos órgãos e entidades da Administração Pública Federal, direta e indireta.

4. Conceitos e definições

4.1. Acesso privilegiado: nível de acesso restrito onde uma pessoa tem permissão para gerenciar um sistema e/ou serviço.

4.2. Acesso remoto: todo acesso externo a recursos da rede de dados interna do TRE-BA.

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

4.4. Controle de acesso: conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso.

4.5. Dispositivo móvel: equipamento portátil dotado de capacidade computacional, que permite conexão à rede cabeada ou à rede sem-fio, podendo acessar recursos de rede e Internet. São exemplos: *smartphones*, *notebooks* e *tablets*, dentre outros.

4.6. Extranet: módulo disponível no sítio eletrônico do TRE-BA, que possibilita, por meio do registro de *login* e senha pessoais, o acesso externo a serviços administrativos da rede de dados interna do Tribunal.

4.7. *Malwares*: programas indesejados, desenvolvidos com a finalidade de executar ações danosas ou atividades maliciosas em um computador ou sistema (ex.: *worm*, *bot*, *spyware*, *backdoor*, cavalo de troia, *ransomware* e *rootkit*).

4.8. Proprietário do ativo de informação: pessoa ou outra entidade que tem a responsabilidade (aprovada pela Administração) para qualificar o ciclo de vida de um ativo.

4.9. Rede cabeada: corresponde ao acesso aos recursos tecnológicos e à transmissão de dados através da utilização de meios físicos (ativos de distribuição de dados, cabos e pontos de rede).

4.10. Rede lógica: rede de dados utilizada pelo Tribunal, abrangendo serviços e sistemas de tecnologia da informação, rede cabeada, rede sem-fio, ativos de distribuição de dados e equipamentos conectados nessa rede.

4.11. Rede sem-fio: também conhecida como rede wireless ou wi-fi, corresponde ao acesso aos recursos tecnológicos e à transmissão de dados sem a utilização de meios físicos (cabeamento), através da utilização de pontos de acesso sem-fio.

4.12. Remoção de acesso: processo que tem por finalidade remover/excluir definitivamente ou parcialmente determinado(s) acesso(s).

4.13. Usuários: magistrados e servidores ocupantes de cargo efetivo ou em comissão, requisitados e cedidos, e, desde que previamente autorizados, empregados de empresas prestadoras de serviços terceirizados, consultores, estagiários e outras pessoas que se encontrem a serviço da Justiça Eleitoral, utilizando em caráter temporário os recursos tecnológicos do Tribunal Regional Eleitoral da Bahia.

4.14. *Virtual Private Network* (VPN): rede virtual privada de comunicação de dados, construída sobre a infraestrutura de uma rede pública ou compartilhada, utilizando tecnologias que garantam a segurança e o sigilo dos dados trafegados, destinada a estabelecer conexão entre dispositivos remotos e a rede de dados interna deste Tribunal.

5. Uso de Recursos de Tecnologia da Informação

5.1. Diretrizes gerais

5.1.1. O uso adequado dos recursos de tecnologia da informação visa a garantir a continuidade das atividades desenvolvidas neste Tribunal.

5.1.2. Os recursos de tecnologia da informação disponibilizados pelo Tribunal Regional Eleitoral da Bahia aos usuários serão utilizados em atividades relacionadas às funções institucionais e abrangem os seguintes elementos:

I – os computadores servidores, os computadores para uso individual ou coletivo, de qualquer porte, os equipamentos de armazenamento e distribuição de dados, os dispositivos móveis, as impressoras, as multifuncionais, bem como os respectivos periféricos e acessórios;

II – a rede lógica do TRE-BA e das respectivas unidades remotas (cartórios eleitorais, postos de atendimento ao eleitor e Centro de Apoio Técnico);

III – as contas de acesso dos usuários e os certificados digitais;

IV – os sistemas computacionais desenvolvidos com recursos providos pelo TRE-BA;

V – os sistemas computacionais contratados de terceiros, sob licença ou na forma de *software* livre ou aberto.

5.1.3. As unidades do Tribunal devem obrigatoriamente submeter à prévia análise da Secretaria de Tecnologia da Informação a intenção em adquirir ou instalar *software*, equipamento ou serviço que não tenha sido provido pela área de TIC e que faça uso ou requeira recursos de tecnologia da informação.

5.1.4. O usuário é responsável por:

I – zelar pelos recursos que lhe sejam destinados para o exercício de suas atribuições, especialmente os de utilização pessoal, tais como computadores, impressoras, dispositivos móveis e demais equipamentos;

II – preservar o sigilo de sua senha ou outro mecanismo de autenticação que venha a ser utilizado para acesso aos recursos tecnológicos disponibilizados;

III – preservar o sigilo das informações a que tiver acesso, sendo vedada sua revelação a usuários ou terceiros não autorizados;

IV – atos praticados e acessos realizados aos recursos de tecnologia por meio de sua credencial de acesso.

5.1.5. Os procedimentos de instalação, configuração e manutenção de equipamentos e *softwares* serão realizados pela Secretaria de Tecnologia da Informação ou por terceiros por ela autorizados, sob a supervisão do gestor da unidade, que verificará a adequação do serviço realizado ao atendimento das atividades desenvolvidas pela unidade.

5.1.6. Não será fornecido suporte a equipamentos particulares (computadores, *notebooks*, *smartphones* e *tablets*), seja quanto à instalação e configuração de sistemas ou aplicativos, ainda que disponibilizados pelo TRE-BA, seja quanto às questões relacionadas à conexão à rede sem-fio.

5.1.7. Os equipamentos servidores e os computadores para uso individual ou coletivo, de qualquer porte, serão dotados de mecanismos de proteção contra *malwares*.

5.2. Rede Lógica

5.2.1. Todos os equipamentos e dispositivos móveis conectados à rede lógica de dados do TRE-BA terão seus acessos monitorados por questões de segurança e para fins de auditoria.

5.2.2. A cada ponto de acesso à rede de dados do TRE-BA poderá ser conectado apenas um equipamento, vedada a utilização de dispositivos multiplicadores de acesso, tais como *hub* e *switch*, dentre outros, salvo mediante expressa autorização da Secretaria de Tecnologia da Informação.

5.2.3. É proibida a conexão de qualquer dispositivo não fornecido pelo TRE-BA na rede cabeada sem a prévia anuência da Secretaria de Tecnologia da Informação.

5.2.3.1. A conexão de qualquer equipamento à rede cabeada da Sede do TRE-BA será feita pela Secretaria de Tecnologia da Informação ou por terceiros por ela autorizados.

5.2.3.2. Em unidades remotas, a conexão poderá ser realizada por pessoal do local mediante suporte da Secretaria de Tecnologia da Informação.

5.2.4. O Tribunal disponibilizará acesso à rede sem-fio para usuários internos e externos.

5.2.4.1. A conexão, para os usuários internos, será feita por meio da credencial (nome de usuário e senha) utilizada para o acesso à rede, e, para os usuários externos, será feita mediante cadastramento prévio em sistema específico do TRE-BA.

5.2.4.2. É permitida a conexão de dispositivos móveis particulares nas redes sem-fio administradas pelo TRE-BA.

5.2.4.3. O acesso à Internet por meio das redes sem-fio observará as regras dispostas na NSI-003 de Controle de Acesso à Internet.

5.2.4.4. Por questões de segurança tecnológica, regras específicas poderão ser implementadas no acesso à Internet via rede sem-fio.

5.2.4.5. Poderão ser bloqueados os acessos à rede sem-fio, temporariamente ou por tempo indeterminado, de dispositivos móveis identificados durante o monitoramento como fonte de ações maliciosas, intencionais ou não, ou em que forem detectadas vulnerabilidades ou problemas de segurança tecnológica.

5.3. Equipamentos fornecidos pelo Tribunal

5.3.1. O fornecimento de equipamentos a magistrados e servidores está condicionado às necessidades de trabalho e à assinatura do Termo de Responsabilidade e do recebimento por meio do sistema de gestão de patrimônio.

5.3.2. Os computadores portáteis possuem instalação padrão, composta por *softwares* e aplicativos necessários ao desempenho das funções de trabalho, além de *softwares* para proteção e monitoramento do equipamento.

5.3.2.1. Os problemas de *software* serão solucionados pela reinstalação padrão, ficando a área de suporte a usuário isenta da responsabilidade sobre eventual perda de dados.

• *Item alterado pela Portaria nº 400/18.*

5.3.2.2. (Revogado pela Portaria 400/18).

5.3.3. Em caso de falecimento, aposentadoria, exoneração, demissão, cedência, remoção, redistribuição, dispensa da função ou término das atividades que ensejaram o fornecimento, o equipamento deverá ser devolvido à Secretaria de Tecnologia da Informação, com todos os acessórios que o acompanharam, em até 20 (vinte) dias, exceto em se tratando de prazo diferente estipulado em norma específica.

5.3.4. Nos casos de perda, furto ou roubo do equipamento, bem como nas hipóteses de ausência de devolução ou verificação de existência de avarias no equipamento devolvido, a Secretaria de Tecnologia da Informação informará à Diretoria – Geral do Tribunal a situação ocorrida, com a documentação respectiva, para as providências cabíveis.

5.3.4.1. Na ocorrência de um dos fatos acima, a reposição, quando autorizada pelo Comitê de Governança de TIC, dependerá da disponibilidade de equipamento para substituição.

5.4. Licenças de *software*

5.4.1. As licenças de *softwares*, de qualquer natureza, contratadas ou adquiridas pelo TRE-BA, são de uso institucional, privativo do Tribunal.

5.4.2. O Tribunal, sempre que possível e necessário, dará preferência ao uso de *software* livre ou de código aberto.

5.4.3. É proibida a instalação de *softwares* não licenciados ou não homologados pela Secretaria de Tecnologia da Informação nos equipamentos conectados à rede do Tribunal.

5.4.3.1. A instalação de *softwares* não homologados poderá ser autorizada excepcionalmente pelo Comitê de Segurança da Informação, desde que demonstrada a necessidade de sua utilização para o desempenho das atribuições funcionais do usuário, observadas as condições de segurança e proteção estabelecidas, bem como a compatibilidade e adequação aos recursos computacionais disponibilizados pelo TRE-BA.

5.4.3.2. As unidades organizacionais do Tribunal poderão encaminhar à Secretaria de Tecnologia da Informação pedido de homologação de *softwares* para uso em suas atividades. Quando necessário, o pedido, acompanhado de parecer técnico, será submetido ao Comitê de Segurança da Informação.

6. Controle de acesso

6.1. Gerenciamento de acessos

6.1.1. Os acessos à rede, serviços e aos sistemas computacionais disponibilizados pelo TRE-BA deverão ser solicitados à Secretaria de Tecnologia da Informação, por meio da Central de Serviços de TIC, quando serão definidos os níveis de acesso adequados às atividades desenvolvidas.

6.1.2. Incumbe à chefia imediata ou ao gestor de contrato solicitar à Secretaria de Tecnologia da Informação:

I – a concessão dos acessos necessários ao desenvolvimento das atividades dos servidores e estagiários vinculados a sua unidade ou de prestadores de serviço de contrato sob sua gestão;

II – a alteração dos níveis de acesso ou a remoção do acesso a sistemas concedidos a servidor ou estagiário da unidade ou a prestador de serviço de contrato sob sua gestão, sempre que necessária sua adequação às atividades desenvolvidas;

III – a remoção dos acessos concedidos a servidor ou estagiário ou a prestador de serviço de contrato sob sua gestão, imediatamente após o seu afastamento ou desligamento da unidade ou do contrato;

6.1.2.1. Quando necessária a concessão, alteração ou remoção de acesso de magistrado, a solicitação deverá ser efetuada pela chefia de cartório, no caso de juízes eleitorais, e pela Secretaria Judiciária, em se tratando de membros da Corte.

6.1.2.2. Em redes locais, especialmente de cartório eleitoral e postos de atendimento, os procedimentos de concessão, alteração e remoção de acesso deverão ser executados pelo respectivo chefe de cartório, podendo ser por ele delegada a outra pessoa, sem, no entanto, haver transferência de responsabilidade.

6.1.2.3. A não solicitação da alteração ou remoção de acesso no momento oportuno poderá ensejar à chefia a responsabilização pelo acesso indevido a informações da unidade.

6.1.3. A Secretaria de Gestão de Pessoas comunicará à Secretaria de Tecnologia da Informação os casos de falecimento, exoneração, demissão, redistribuição, aposentadoria, remoção e cedência a outro órgão, retorno à origem, ou término do estágio de estudantes, imediatamente após a ocorrência do ato, para remoção dos acessos concedidos aos usuários.

6.1.3.1. Os usuários aposentados, afastados e cedidos ou removidos para outros órgãos, terão acesso aos serviços administrativos via Extranet.

6.1.4. A administração dos acessos dos magistrados no PJe é responsabilidade da Secretaria Judiciária.

6.1.5. A Secretaria de Tecnologia da Informação comunicará à unidade respectiva sobre a efetivação do cadastro, fornecendo as informações necessárias ao acesso.

6.1.5.1. As novas senhas solicitadas serão fornecidas por meio de comunicação eletrônica para o correio eletrônico institucional da unidade ou correio eletrônico institucional pessoal do usuário, proibido o fornecimento de senhas por qualquer outro meio, inclusive telefone.

6.1.5.2. É responsabilidade do usuário a alteração da senha inicial fornecida pela Secretaria de Tecnologia da Informação no primeiro acesso realizado.

6.1.6. É dever do chefe da unidade ou do gestor do contrato garantir que o novo usuário dos serviços de TIC tome pleno conhecimento dos normativos de segurança da informação do Tribunal.

6.1.7. O privilégio de administrador na estação de trabalho é restrito aos membros da equipe técnica da Secretaria de Tecnologia da Informação que necessitem de acesso privilegiado para o desempenho das atividades funcionais.

6.1.8. Os acessos privilegiados aos sistemas e serviços de TIC deverão ser concedidos aos membros da equipe técnica da Secretaria de Tecnologia da Informação sempre que necessários ao desempenho das atividades funcionais, de modo a permitir a gestão e configuração do ambiente tecnológico.

6.1.8.1. É responsabilidade da chefia imediata solicitar a concessão, a alteração e a remoção dos acessos privilegiados dos seus subordinados.

6.1.8.2. Os acessos concedidos deverão ser revisados pelo menos uma vez ao ano.

6.1.9. As solicitações de concessão de acesso aos recursos tecnológicos do TRE-BA a prestadores de serviço deverão ser acompanhadas da respectiva justificativa, inclusive quanto ao prazo de concessão (temporário ou indeterminado).

6.1.9.1. No caso de o prestador de serviço necessitar acesso privilegiado, as regras observarão o disposto no item 6.1.8.

6.2. Da conta de rede e respectiva senha para utilização

6.2.1. Para ter acesso aos recursos de tecnologia da informação disponibilizados pelo TRE-BA é necessário que o usuário possua uma conta de rede.

6.2.2. A identificação de usuário se dará por meio do número de seu título eleitoral, contendo 12 (doze) dígitos.

6.2.2.1. Cada usuário receberá também 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.

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

6.2.3. A cada conta de acesso será associada uma senha, de uso pessoal e intransferível.

6.2.3.1. Quando se tratar de alteração de senha pessoal para acesso à rede de dados do Tribunal pela equipe de suporte da Secretaria de Tecnologia da Informação, a nova senha do usuário será encaminhada de forma automática pelo Sistema de Alteração de Senhas ao correio eletrônico pessoal que estiver cadastrado no Sistema de Gestão de Recursos Humanos – SGRH.

• *Item acrescentado pela Portaria 400/18*.

6.2.4. Na utilização das credenciais de acesso, compete ao usuário observar os procedimentos a seguir indicados, bem como adotar outras medidas de segurança de caráter pessoal, com vista a impedir o uso não autorizado dos recursos de tecnologia da informação a partir de sua conta de acesso:

I – não compartilhar a senha com outras pessoas;

II – não armazenar senhas em local acessível por terceiros;

III – não utilizar senhas de fácil dedução como as que contêm nomes próprios e de familiares, datas festivas e sequências numéricas;

IV – ao ausentar-se de sua estação de trabalho, ainda que temporariamente, o usuário deverá encerrar ou bloquear a sessão.

6.2.5. A senha deverá satisfazer os seguintes requisitos de complexidade:

I – não conter o identificador da conta do usuário (*login*) ou mais de dois caracteres consecutivos de partes de seu nome completo;

II – ter pelo menos oito caracteres;

III – conter caracteres de, no mínimo, três das quatro categorias a seguir:

a) caracteres maiúsculos (A-Z);

b) caracteres minúsculos (a-z);

c) dígitos de base (0 a 9);

d) caracteres não alfabéticos (!, $, #, % etc.).

6.2.5.1. Excetuam-se ao quanto estabelecido no item 6.2.5. os sistemas atualmente disponibilizados que não permitam o atendimento aos requisitos estabelecidos.

6.2.6. A senha deverá ser alterada com uma periodicidade máxima de 180 (cento e oitenta) dias desde sua última modificação.

6.2.7. A conta do usuário será bloqueada após 10 (dez) tentativas consecutivas de acesso não reconhecidas, considerando também as tentativas inválidas de acesso à rede sem-fio.

6.2.8. Em caso de suspeita de comprometimento da senha ou de outro recurso de autenticação, o usuário comunicará imediatamente Central de Serviços de TIC, que poderá, como medida preventiva, suspender temporariamente o acesso.

6.2.9. É vedada a criação de conta de acesso à rede e aos sistemas de informática para colaboradores menores de idade, sendo permitido o acesso local à estação de trabalho, bem como acesso à intranet e ao Portal dos Servidores.

- Item acrescentado pela Portaria 409/2022

7. Registros (*log*) de Eventos

7.1. Serão mantidos, por um período mínimo de 3 (três) meses, os registros dos acessos dos usuários e dos acessos privilegiados aos recursos tecnológicos disponibilizados pelo TRE-BA, inclusive para fins de apuração e comprovação de incidentes de segurança.

7.1.1. Serão registrados os seguintes dados:

I – identificação de usuário de quem efetuou o acesso;

II – data e hora de entrada e saída do sistema;

III – origem do acesso;

IV – erros ou falhas de conexão e acesso;

V – troca de senhas de Serviços de Infraestrutura de TI;

VI – outras informações que venham a ser necessárias para os controles de segurança.

ANEXO III

NSI-003 – Controle de Acesso à Internet

1. Objetivos

1.1. Estabelecer diretrizes e padrões para o acesso à Internet no âmbito do Tribunal Regional Eleitoral da Bahia (TRE-BA).

2. Motivações

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

2.2. Proteção do ambiente tecnológico do Tribunal.

2.3. Correto direcionamento e dimensionamento de recursos tecnológicos para prover o serviço de acesso à Internet.

3. Referências normativas

3.1. 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.

3.2. 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.

3.3. 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.

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

4. Conceitos e definições

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

4.2. Código malicioso: termo comumente utilizado para genericamente se referir a programas desenvolvidos para executar ações danosas e atividades maliciosas em um computador ou dispositivo móvel. Tipos específicos de códigos maliciosos são: vírus, worm, bot, spyware, backdoor, cavalo de troia e rootkit.

4.3. Intranet: rede de computadores circunscrita aos limites internos de uma instituição, na qual são utilizados os mesmos programas e protocolos de comunicação empregados na Internet.

4.4. *Proxy*: também conhecido por filtro de conteúdo, é o servidor responsável por intermediar o acesso à Internet, aplicando regras de controle de acesso e mecanismos de proteção contra códigos maliciosos, previamente configurados, e por controlar a alocação de recursos de rede.

4.5. *Proxy* externo: são servidores, não administrados pelo TRE-BA, responsáveis por intermediar o acesso à Internet, mas que não aplicam as regras de controle de acesso e mecanismos de proteção da mesma forma que o *proxy* administrado pelo Tribunal.

4.6. Sítio: conjunto de páginas *web* organizadas e acessíveis a partir de um URL da rede interna (Intranet) ou da Internet.

4.7. Situação de contingência: estado ou condição na qual exista a ocorrência de falha/problema, em um ou mais recursos tecnológicos, que reduzam a capacidade dos sistemas e serviços que suportam a atividade da organização.

4.8. URL: sigla correspondente às palavras inglesas "*Uniform Resource Locator*", traduzidas para o português como “Localizador Uniforme de Recursos”. Trata-se da indicação do endereço de um recurso de informática disponível em uma rede, seja ela a Internet ou a Intranet de uma organização.

5. Diretrizes

5.1. O acesso à Internet dar-se-á, exclusivamente, pelos meios autorizados, configurados e disponibilizados pela Secretaria de Tecnologia da Informação.

5.1.1. É expressamente proibido o uso de *proxies* externos ou similares.

5.2. O acesso à Internet é disponibilizado para uso nas atividades relacionadas ao trabalho, observado o disposto nesta Norma.

5.3. Constitui acesso indevido à Internet qualquer das seguintes ações:

5.3.1. Acessar páginas de conteúdo considerado ofensivo, ilegal, impróprio ou incompatível com as atividades funcionais ou com a Política de Segurança da Informação, tais como pornografia, pedofilia, racismo, jogos e páginas de distribuição e de compartilhamento de *software*.

5.3.2. Utilizar programas de troca de mensagens em tempo real (bate-papo) ou programas para troca de conteúdo via rede ponto-a-ponto (*peer-to-peer*), exceto os autorizados pelo Comitê de Segurança da Informação.

5.3.3. Utilizar programas e/ou acessar páginas de áudio e vídeo em tempo real, ou sob demanda, exceto os autorizados pelo Comitê de Segurança da Informação.

5.3.4. Acessar sítios que representem ameaça de segurança ou que possam comprometer de alguma forma a integridade da rede de computadores do TRE-BA.

5.3.5. Acessar ou fazer *download* de arquivos não relacionados ao trabalho, em especial músicas, imagens, vídeos, jogos e programas de qualquer tipo.

5.4. Todo tráfego de Internet será controlado e inspecionado, de forma automática, pela ferramenta de *proxy* (filtro de conteúdo), configurada de acordo com os limites estabelecidos por esta Norma ou definidos pela Administração do Tribunal.

5.4.1. A liberação de acesso a sítios e serviços bloqueados, mas necessários ao desempenho das atribuições funcionais do usuário, dependerá de solicitação, devidamente justificada, à Secretaria de Tecnologia da Informação, por meio da Central de Serviços de TIC, que a submeterá, quando for o caso, ao Comitê de Segurança da Informação, para deliberação.

5.5. Cabe ao gestor da unidade orientar os usuários sob sua responsabilidade a respeito do uso adequado do recurso de Internet, conforme as regras estabelecidas nesta Norma, bem como reportar ao Comitê de Segurança da Informação o seu descumprimento.

5.6. A critério da Administração, poderão ser adotadas medidas visando a manutenção da disponibilidade e da qualidade do acesso à Internet, seja em situações normais de funcionamento, seja em situações de contingência, tais como:

5.6.1. Bloqueios totais ou parciais e/ou priorização de acessos a determinados sítios e serviços; e

5.6.2. Limitação de banda de tráfego de dados.

5.7. As medidas identificadas no item anterior, quando implementadas, serão comunicadas à Central de Serviços de TIC, a fim de possibilitar o repasse de informações aos usuários interessados.

6. Monitoramento e auditorias

6.1. Por motivos de segurança, todo acesso à Internet será monitorado e os registros serão mantidos pela Secretaria de Tecnologia da Informação.

6.2. Em caso de indícios de descumprimento das diretrizes previstas nesta Norma, a chefia imediata ou superior deverá solicitar, justificadamente, ao Comitê de Segurança da Informação, a realização de auditoria extraordinária.

6.2.1. Em caso de deferimento da solicitação, o Comitê de Segurança da Informação demandará à Secretaria de Tecnologia da Informação a execução da auditoria e a elaboração do respectivo relatório.

6.2.2. Os relatórios decorrentes das auditorias ordinárias e extraordinárias deverão ser encaminhados ao Comitê de Segurança da Informação para os devidos fins.

ANEXO IV

NSI-004 – Acesso Remoto

1. Objetivos

1.1. Estabelecer diretrizes e padrões para o acesso a serviços da rede de dados interna através de portal Extranet e de conexão via VPN no âmbito do Tribunal Regional Eleitoral da Bahia (TRE-BA).

2. Motivações

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

2.2. Garantia de que os acessos remotos aos serviços de tecnologia da informação e comunicação do Tribunal sejam feitos de forma segura e controlada.

3. Referências normativas

3.1. 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.

3.2. 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.

3.3. 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.

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

4. Conceitos e definições

4.1. Acesso remoto: todo acesso externo a recursos da rede de dados interna do TRE-BA.

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

4.3. Controle de acesso: conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso.

4.4. Extranet: módulo disponível no sítio eletrônico do TRE-BA, que possibilita, por meio do registro de *login* e senha pessoais, o acesso externo a serviços administrativos da rede de dados interna do Tribunal.

4.5. Usuários: magistrados e servidores ocupantes de cargo efetivo ou em comissão, requisitados e cedidos, e, desde que previamente autorizados, empregados de empresas prestadoras de serviços

terceirizados, consultores, estagiários e outras pessoas que se encontrem a serviço da Justiça Eleitoral, utilizando em caráter temporário os recursos tecnológicos do Tribunal Regional Eleitoral da Bahia.

4.6. *Virtual Private Network* (VPN): rede virtual privada de comunicação de dados, construída sobre a infraestrutura de uma rede pública ou compartilhada, utilizando tecnologias que garantam a segurança e o sigilo dos dados trafegados, destinada a estabelecer conexão entre dispositivos remotos e a rede de dados interna deste Tribunal.

5. Diretrizes

5.1. Serviços disponíveis

5.1.1. A Secretaria de Tecnologia da Informação disponibilizará acesso externo a sistemas e serviços de tecnologia da informação e comunicação, desde que compatíveis e condicionados às permissões de acesso dos usuários, pelos seguintes meios:

I – Via Extranet: sistemas e serviços administrativos específicos, disponibilizados para acesso externo pelos usuários da rede de dados do Tribunal, conforme divulgado na opção "Catálogo de Serviços de TI" do menu "Serviços" do Portal Intranet;

II – Via VPN individual: acesso externo a aplicações e recursos de TIC disponíveis na rede de dados interna do Tribunal por pessoa devidamente autorizada;

III – Via VPN institucional: acesso a aplicações e recursos disponíveis na rede de dados interna da Justiça Eleitoral (Intranet) por cartórios eleitorais, postos de atendimento ao eleitor, Centro de Apoio Técnico (CAT) e eventos promovidos pelo TRE-BA fora de suas instalações.

5.2. Usuários

5.2.1. Os sistemas ou serviços disponibilizados via Extranet serão acessíveis aos usuários de TIC que possuam contas (*login* e senha) devidamente cadastradas e ativas, conforme as permissões de acesso e uso.

5.2.2. O acesso à rede da Justiça Eleitoral através de VPN individual fica permitido aos servidores e prestadores de serviços terceirizados das áreas de infraestrutura e banco de dados da Secretaria de Tecnologia da Informação para fins exclusivos de manutenção emergencial de serviços de TIC ou quando da realização de plantões de sobreaviso, em caso de necessidade relacionada ao respectivo suporte.

5.2.3. O Diretor-Geral da Secretaria do Tribunal poderá autorizar o acesso à rede da Justiça Eleitoral, através de VPN individual, a outros usuários da rede de dados, por solicitação do interessado ou por necessidade do Tribunal, ouvida a Secretaria de Tecnologia da Informação quanto à viabilidade técnica, por período definido ou indeterminado.

5.3. Acesso remoto

5.3.1. O acesso remoto deverá atender aos requisitos da Política de Segurança da Informação da Justiça Eleitoral.

5.3.2. A utilização do acesso remoto implicará na aceitação tácita das normas da Política de Segurança da Informação do TRE-BA e das responsabilidades decorrentes da utilização indevida dos serviços.

5.3.3. A Secretaria de Tecnologia da Informação realizará, periodicamente, monitoramento e auditoria técnica na infraestrutura dos serviços de acesso remoto.

5.3.4. A critério da Secretaria de Tecnologia da Informação, poderão ser realizados procedimentos de segurança nos equipamentos pessoais dos usuários, utilizados para acesso remoto via VPN individual.

5.3.5. Na hipótese de ser identificada situação de grave ameaça ou alto risco à integridade da rede interna e dos serviços de TIC do TRE-BA, o acesso remoto poderá ser interrompido, a qualquer momento, independentemente de prévia comunicação ao usuário, dando-se imediata ciência do fato ao Comitê de Gestão de Tecnologia da Informação e Comunicação (CGesTIC).

5.4. Acesso via VPN

5.4.1. Para ter acesso à rede da Justiça Eleitoral via VPN individual, todo usuário deverá preencher o formulário de Requerimento de Serviço de Acesso Remoto (Anexo A desta Norma), gerar arquivo PDF e encaminhá-lo como documento PAD assinado eletronicamente à Secretaria de Tecnologia da Informação, devendo a respectiva chefia abrir solicitação na Central de Serviços de TIC, indicando o número do documento PAD.

5.4.1.1. O Requerimento deverá ser previamente submetido ao Diretor-Geral para aprovação quando se tratar de usuários não integrantes das áreas elencadas no item 5.2.2.

5.4.1.2. É responsabilidade do usuário transportar para o TRE-BA o equipamento a ser utilizado na conexão VPN individual para configuração pela unidade técnica responsável, em data a ser acordada.

5.4.2. A implantação de conexão VPN institucional será realizada por determinação da Administração do Tribunal ou após autorização de solicitação formal do interessado.

5.4.2.1. O acesso e uso de recursos e serviços de TIC via VPN institucional estão submetidos aos normativos afins.

5.4.3. O acesso via VPN poderá ser revogado a qualquer tempo.

5.5. Inclusão de serviço no acesso via Extranet

5.5.1. A inclusão de serviço no acesso via Extranet deverá ser solicitada por meio da Central de Serviços de TIC, contendo, no mínimo, os seguintes itens:

I – descrição do serviço;

II – público-alvo;

III – justificativa para inclusão do serviço.

ANEXO A

REQUERIMENTO DE SERVIÇO DE ACESSO REMOTO – VPN

Tipo de vínculo: ☐ Servidor efetivo ☐ Requisitado ☐ Terceirizado	
Requerente:	
Unidade de Lotação:	Ramal:
Matrícula:	Título Eleitoral:

Sr(a). Diretor(a) Geral do Tribunal Regional Eleitoral da Bahia,

O(A) requerente acima identificado(a) solicita a Vossa Senhoria a utilização do serviço de acesso remoto via VPN individual:

☐ no período de_____/_____/_____a_____/_____/_____.

☐ por tempo indeterminado.

DESCRIÇÃO DO EQUIPAMENTO A SER UTILIZADO NO ACESSO REMOTO
JUSTIFICATIVA PARA UTILIZAÇÃO DO SERVIÇO

AUTORIZAÇÃO/DECLARAÇÃO	
☐	Comprometo-me a observar as seguintes regras no acesso remoto via VPN individual: 1. O acesso aos recursos da VPN é concedido a cada usuário de forma pessoal e intransferível; 2. Cada usuário é o único e total responsável pelo seu acesso (login e senha) à rede VPN, assim como por todas as ações resultantes dele; 3. Cada usuário deve manter seu acesso (*login* e senha) à rede VPN em sigilo absoluto e não fornecê-lo a outra pessoa, garantindo assim, a impossibilidade de acesso indevido por pessoas não autorizadas; 4. É vedada a utilização dos recursos da VPN para fins não relacionados às atividades da Instituição; 5. O uso dos recursos da VPN deve restringir-se à esfera profissional ou à colheita de informações com conteúdo estritamente relacionado às atividades desempenhadas pela instituição, observando-se sempre a conduta compatível com a moralidade administrativa; 6. A não observância dessas regras pode resultar na suspensão do acesso aos recursos da VPN de forma temporária ou permanente, bem como levar o responsável a responder, em todas as instâncias, pelas consequências das ações ou omissões que possam por em risco ou comprometer a rede de dados interna da Instituição.
☐	Autorizo a Secretaria de Tecnologia da Informação a realizar procedimentos de segurança no meu equipamento pessoal a ser utilizado para realizar acesso remoto ao TRE-BA via VPN.
☐	Declaro ter ciência da Política de Segurança da Informação da Justiça Eleitoral instituída pela Resolução TSE nº 23.501/2016, regulamentada pela Portaria ASSESP nº 611/2017.

_____, _____de_____de 20____.

_____

(assinatura)

ANEXO V

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

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.

4. 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.

5. 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 necessiteesse 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 geralmentealarmante 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 símboloarroba (@).

9. Lista de distribuição: agrupamento de caixas postais visando a distribuição de uma mensagemeletrônica 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 *backdoor*, cavalo de tróia, *ransomware* e *rootkit*. *Worm*, *bot*,*spyware*,

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 mensagenseletrônicas (e-mails) no âmbito do TRE-BA.

14. *Spam*: mensagem, sem valor institucional ou inútil à atividade funcional, enviada a um grandenúmero 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, pelo chefe de cartório,

quando for para juiz ou promotor eleitoral, e pelo gestor de contrato no tocante a prestador de serviço.

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

NSI-006 – Gestão de Riscos de Tecnologia da Informação e Comunicação

1. Objetivos

1.1. Estabelecer as diretrizes da gestão de riscos relacionadas ao ambiente tecnológico no âmbito do Tribunal Regional Eleitoral da Bahia, aos projetos e processos de Tecnologia da Informação e Comunicação (TIC), e definir o processo de Gerenciamento de Riscos de Segurança da Informação do TRE-BA.

2. Aplicabilidade

2.1. Este documento aplica-se a todas as unidades pertencentes à Secretaria de Tecnologia da Informação, responsáveis por gerenciar, manipular e operar informações, projetos, processos, produtos e serviços relacionados à área de TIC no âmbito do TRE-BA.

3. Motivações

3.1. Necessidade de um processo sistemático para gerenciar riscos referentes à Segurança da Informação, projetos e processos de TIC, provendo insumos para aumentar a proteção contra eventos indesejados.

3.2. Correto direcionamento de esforços e investimentos financeiros, tecnológicos e humanos.

3.3. Conformidade com normatizações e regulamentações relacionadas ao assunto.

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, a qual disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, e dá outras providências.

4.2. Norma Complementar nº 04/IN01/DSIC/GSIPR (Revisão 01), de 15 de fevereiro de 2013, do Departamento de Segurança da Informação e Comunicações da Presidência da República, que estabelece diretrizes para o processo de Gestão de Riscos de Segurança da Informação e Comunicações – GRSIC nos órgãos ou entidades da Administração Pública Federal – APF, direta e indireta.

4.3. Norma Técnica ABNT NBR ISO/IEC 27005:2011, que fornece diretrizes para o processo de gestão de riscos de Segurança da Informação.

4.4. Norma Técnica ABNT NBR ISO 31000:2009, que fornece princípios e diretrizes genéricas para a gestão de riscos.

4.5. Norma ABNT NBR ISO/IEC 27002:2013, que trata de Código de Prática para a Gestão da Segurança da Informação.

4.6. 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.

4.7. Norma Técnica ABNT ISO GUIA 73:2009, que fornece as definições de termos genéricos relativos à gestão de riscos.

5. Conceitos e definições

5.1. Ameaça: conjunto de fatores externos ou causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou uma organização.

5.2. Análise de riscos: uso sistemático de informações para identificar fontes e estimar o risco.

5.3. Análise/avaliação de riscos: processo completo de análise e avaliação de riscos.

5.4. Ativos de Informação: os meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso.

5.5. Avaliação de riscos: processo de comparar o risco estimado com critérios de risco predefinidos para determinar a importância do risco.

5.6. Comunicação do risco: troca ou compartilhamento de informação sobre o risco entre o tomador de decisão e as outras partes interessadas.

5.7. Estimativa de riscos: processo utilizado para atribuir valores à probabilidade e às consequências de um risco.

5.8. Evitar risco: forma de tratamento de risco pela qual se decide não realizar a atividade, a fim de não se envolver ou agir de forma a se retirar de uma situação de risco.

5.9. Gestão de Riscos de Segurança da Informação: conjunto de atividades que permitem identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os seus ativos de informação e equilibrá-los com os custos operacionais e financeiros envolvidos.

5.10. Gestão de Riscos em Projetos de TIC: conjunto de atividades que envolve a identificação, a análise, o planejamento de respostas, o monitoramento e o controle de riscos de um projeto.

5.11. Gestão de Riscos em Processos de TIC: conjunto de atividades, estabelecidas de acordo com as peculiaridades ou normatividades que regem cada processo, que visam a identificar e minimizar ou eliminar os riscos.

5.12. Identificação de riscos: processo para localizar, listar e caracterizar elementos do risco.

5.13. Reduzir risco: forma de tratamento de risco pela qual se decide realizar a atividade, adotando

ações para reduzir a probabilidade, as consequências negativas, ou ambas, associadas a um risco.

5.14. Reter risco: forma de tratamento de risco pela qual se decide realizar a atividade, assumindo as responsabilidades caso ocorra o risco identificado.

5.15. Riscos de Segurança da Informação e Comunicações: potencial associado à exploração de uma ou mais vulnerabilidades de um ativo de informação ou de um conjunto de tais ativos, por parte de uma ou mais ameaças, com impacto negativo no negócio da organização.

5.16. Transferir risco: uma forma de tratamento de risco pela qual se decide realizar a atividade, compartilhando com outra entidade o ônus associado a um risco.

5.17. Tratamento dos riscos: processo e implementação de ações de segurança da informação e comunicações para evitar, reduzir, reter ou transferir um risco.

5.18. Vulnerabilidade: conjunto de fatores internos ou causa potencial de um incidente indesejado que podem resultar em risco para um sistema ou uma organização, os quais podem ser evitados por uma ação interna de Segurança da Informação.

6. Escopo

6.1 A Gestão de Riscos de TIC, definida por esta Norma, tem seu escopo limitado às medidas protetivas dos ativos de informação, bem como dos projetos e processos relacionados à área de TIC, que suportam os principais processos de negócio do TRE-BA.

7. Diretrizes

7.1. A Gestão de Riscos de TIC deverá levar em consideração as definições do Planejamento Estratégico Institucional e do Planejamento Estratégico de TIC e estar alinhada à Política de Segurança da Informação da Justiça Eleitoral e ao Sistema de Gestão de Riscos (SGR) do Tribunal.

7.2. A Gestão de Riscos de TIC deverá ser abordada de forma sistemática, com o objetivo de manter os riscos de TIC em níveis aceitáveis para cada projeto, processo e/ou serviço analisado.

7.3. Os riscos de TIC deverão ser analisados e avaliados em função de sua relevância para os principais processos de negócio do Tribunal e ser tratados de forma a assegurar respostas tempestivas e efetivas.

8. Gestão de riscos em projetos de TIC

8.1. A gestão e comunicação de riscos em projetos de TIC estão definidas na metodologia de gerenciamento de projetos do Tribunal e têm como objetivo aumentar a probabilidade e o impacto dos eventos positivos e reduzir a probabilidade e o impacto dos eventos negativos no projeto.

8.2. As atividades inerentes ao gerenciamento de riscos em projetos relacionados à TIC devem observar o disposto na metodologia de gerenciamento de projetos e Sistema de Gestão de Riscos do Tribunal.

8.3. A gestão de riscos em projetos deverá ser realizada pelo Gerente do Projeto e monitorada pela Seção de Gestão de Riscos e de Gerenciamento de Projetos.

9. Gestão de riscos em processos de TIC

9.1. A gestão e comunicação de riscos em processos de TIC deverão estar definidas na especificação de cada processo e visam à identificação e ao controle dos eventos que possam comprometer seus objetivos, contribuindo para sua melhoria.

9.2. As atividades inerentes à gestão de riscos nos processos de TIC deverão observar as diretrizes do Sistema de Gestão de Riscos do Tribunal e desta Norma.

9.3. A gestão de riscos em processos de TIC deverá ser monitorada pela Seção de Governança e de Gestão de Processos e da Qualidade.

10. Gestão de riscos de segurança da informação

10.1. O processo de gestão de riscos de segurança da informação deverá ser contínuo, fornecendo subsídios e integrando-se à implantação e operação do processo de gestão de incidentes de segurança da informação e de gestão de continuidade de negócios.

10.2. A gestão de riscos de segurança da informação deverá seguir o processo estabelecido no Sistema de Gestão de Riscos do Tribunal.

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

Segurança da Informação e Comunicações da Presidência da República, que disciplina o gerenciamento de Incidentes de Segurança em Redes Computacionais realizado pelas Equipes de Tratamento e Resposta a Incidentes de Segurança em Redes Computacionais ETIR dos órgãos e entidades da Administração Pública Federal, direta e indireta APF.

3.4. Resolução nº 23.501/2016 do Tribunal Superior Eleitoral - TSE, que institui a Política de Segurança da Informação no âmbito da Justiça Eleitoral.

4. Conceitos e definições

4.1. Agente responsável: servidor público ocupante de cargo efetivo incumbido de liderar e coordenar os trabalhos e as entregas da Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais, bem como pelo relacionamento com entes internos e externos quanto às funções e ações da ETIR.

4.2. Artefato malicioso: qualquer programa de computador, ou parte de um programa, construído com a intenção de provocar danos, obter informações não autorizadas ou interromper o funcionamento de sistemas e/ou redes de computadores.

4.3. Equipe de Tratamento e Resposta a Incidentes de Segurança da Informação ETIR: grupo de pessoas com a responsabilidade de receber, analisar e responder às notificações e atividades relacionadas a incidentes de segurança da informação em redes de computadores.

4.4. Incidente de segurança em redes computacionais: qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores.

4.5. Público Alvo: é o conjunto de pessoas, setores, órgãos ou entidades atendidas pela Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais.

4.6. Tratamento de incidentes de segurança em redes computacionais: é o serviço que consiste em receber, filtrar, classificar e responder às solicitações e alertas e realizar as análises dos incidentes de segurança, procurando extrair informações que permitam impedir a continuidade da ação maliciosa e também a identificação de tendências.

4.7. Vulnerabilidade: qualquer fragilidade dos sistemas computacionais e redes de computadores que permitam a exploração maliciosa e acessos indesejáveis ou não autorizados.

5. Missão da ETIR

5.1. Facilitar e coordenar atividades de tratamento e resposta a incidentes em redes computacionais, de modo a contribuir para a garantia da disponibilidade, integridade e confidencialidade das informações do Tribunal, bem como colaborar com o intercâmbio científico-tecnológico relacionado à segurança de redes computacionais no âmbito da Justiça Eleitoral.

6. Público-alvo

6.1. O público-alvo da ETIR é formado por todos os usuários da rede de computadores e sistemas do Tribunal.

6.2. A ETIR relaciona-se, internamente, com as unidades da Secretaria de Tecnologia da Informação e com o Comitê de Segurança da Informação.

6.3. Externamente, a ETIR relaciona-se com a ETIR da Justiça Eleitoral (ETIR/JE).

7. Modelo de Implementação

7.1. A ETIR será composta por servidores da Secretaria de Tecnologia da Informação, que, além de suas funções regulares, desempenharão as atividades relacionadas ao tratamento e resposta a incidentes em redes computacionais

7.2. Devido ao modelo, via de regra, a ETIR desempenhará suas atividades, de forma reativa, sem, todavia, deixar de exercer ações proativas quando necessárias.

7.2.1. Os integrantes da ETIR deverão dedicar, 10% de sua jornada mensal de trabalho às ações proativas,

conforme planejamento acordado com o Agente Responsável.

7.3. As atividades reativas da ETIR terão prioridade sobre aquelas desempenhadas por seus integrantes em suas unidades de lotação.

8. Estrutura Organizacional e Composição

8.1. A ETIR está administrativamente subordinada à Secretaria de Tecnologia da Informação.

8.2. O Gestor de Segurança da Informação, com o apoio do Agente Responsável da ETIR, deverá levantar a infraestrutura (pessoas e recursos materiais e tecnológicos) necessária à prestação dos serviços oferecidos ao público-alvo, bem como propor os meios para a capacitação e o aperfeiçoamento técnico dos integrantes da Equipe.

8.2.1. As necessidades de infraestrutura e de desenvolvimento de competências e habilidades dos integrantes da ETIR serão apresentadas à Secretaria de Tecnologia da Informação e ao Comitê de Segurança da Informação.

8.3. A ETIR deverá atuar como um grupo de trabalho permanente, formado por:

? todos os servidores efetivos lotados na Seção de Infraestrutura Tecnológica;

? Chefe da Seção de Suporte ao Usuário;

? Chefe da Seção de Banco de Dados;

? Chefe da Seção de Soluções Corporativas; e

? Chefe da Seção de Microinformática.

8.3.1. O Agente Responsável da ETIR será o Chefe da Seção de Infraestrutura Tecnológica.

8.3.2. Os Chefes de Seção serão representados, em suas ausências, pelos respectivos substitutos legais, inclusive no tocante ao item 8.3.1.

8.4. Ao Agente Responsável caberá:

8.4.1. Gerenciar a Equipe e as atividades que realizar.

8.4.2. Acompanhar o processo de identificação e classificação de ativos de informação.

8.4.3. Acompanhar o registro dos eventos de segurança.

8.4.4. Utilizar metodologia e ferramentas reconhecidas e recomendadas em referenciais técnicos quanto ao processo de coleta e preservação de evidências.

8.4.5. Elaborar os procedimentos internos a serem observados pela ETIR, com apoio da própria equipe.

8.4.6. Planejar e distribuir tarefas para a ETIR, inclusive as de caráter proativo.

8.4.7. Orientar os integrantes da Equipe para o fiel desempenho de suas atividades.

8.4.8. Efetuar as comunicações da ETIR às instâncias decisórias.

8.4.9. Assegurar que os usuários sejam informados sobre os procedimentos adotados em relação aos incidentes de segurança da informação por eles comunicados.

8.5. Caso necessário, poderão ser convocados outros servidores da Secretaria de Tecnologia da Informação e/ou de outras áreas do Tribunal para auxiliar a Equipe no desenvolvimento de suas atividades.

9. Autonomia

9.1. A ETIR terá autonomia compartilhada, ou seja, recomendará os procedimentos a serem executados quando da detecção de fragilidades em redes e sistemas computacionais e apresentará as ações a serem

tomadas ou as repercussões, se as recomendações não forem seguidas, no mínimo, ao Gestor de Segurança da Informação, aos Coordenadores das áreas técnicas envolvidas e ao Secretário de Tecnologia da Informação.

9.2. Na ocorrência de ataques aos serviços de TIC do Tribunal, a ETIR poderá implementar ações visando à interrupção imediata do incidente em redes computacionais, tais como efetuar bloqueios e tornar indisponíveis os serviços afetados, comunicando, prontamente, as ações às instâncias indicadas no item 9.1.

9.2.1. Quando o tratamento e resposta ao incidente afetar a imagem do Tribunal perante à Sociedade, a exemplo da interrupção de serviços prestados ao cidadão, ou impactar a execução de processos internos críticos, seu custo/benefício deverá ser avaliado em conjunto com as instâncias do item 9.1 e com a área responsável pelo serviço/processo.

9.2.2. Posteriormente, assim que o evento estiver controlado, a ETIR deverá emitir relatório recomendando as ações para sanar em definitivo as falhas que propiciaram o incidente.

10. Atribuições

10.1. Executar o processo de Gestão de Incidentes de Segurança em Redes Computacionais estabelecido na NSI-009.

10.2. Receber e analisar as informações sobre vulnerabilidades, artefatos maliciosos e tentativas de intrusão, com definição de estratégias e ações para sua detecção ou correção.

10.3. Fornecer informações sobre a ocorrência ou prevenção de incidente em redes computacionais à Secretaria de Tecnologia da Informação e ao Comitê de Segurança da Informação e comunicar à ETIR/JE.

10.4. Manter os registros dos incidentes em redes computacionais relacionados aos ativos de tecnologia da informação e comunicação.

10.5. Apresentar ao Comitê de Segurança da Informação, semestralmente, nos meses de março e setembro, relatório estatístico dos incidentes de segurança ocorridos no período, com os respectivos tratamentos adotados, visando à elaboração de estudos de melhoria dos mecanismos e controles de segurança ou para subsidiar decisões estratégicas sobre segurança da informação;

10.6. Implementar mecanismos de monitoramento e tratamento de incidentes em redes computacionais.

10.7. Divulgar alertas ou advertências diante da ocorrência de um incidente em redes computacionais ou, de forma proativa, em face de vulnerabilidades conhecidas, que possam gerar impactos nas atividades do público-alvo.

10.8. Interagir com outras equipes de tratamento e resposta a incidentes em redes computacionais e órgãos relacionados, bem como participar de eventos nacionais e internacionais acerca do tema.

ANEXO IX

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

NSI-009 Gestão de Incidentes de Segurança em Redes Computacionais

1. Objetivo

1.1. Estabelecer o processo de Gestão de Incidentes de Segurança em Redes Computacionais no âmbito do Tribunal Regional Eleitoral da Bahia.

2. Motivações

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

2.2. Necessidade de tratar os incidentes em redes computacionais com respostas rápidas e eficientes.

2.3. Correto direcionamento e dimensionamento de recursos tecnológicos e humanos para prover uma Gestão de Incidentes de Segurança em Redes Computacionais com menor custo e maior qualidade.

2.4. Formalização de um processo sistemático para gerenciamento dos incidentes em redes computacionais, provendo insumos para minimizar e/ou evitar eventos futuros.

3. Referências normativas

3.1. 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.

3.2. Norma Complementar nº 08/IN01/DSIC/GSIPR, de 19 de agosto de 2010, do Departamento de Segurança da Informação e Comunicações da Presidência da República, que disciplina o gerenciamento de Incidentes de Segurança em Redes Computacionais realizado pelas Equipes de Tratamento e Resposta a Incidentes de Segurança em Redes Computacionais ETIR dos órgãos e entidades da Administração Pública Federal, direta e indireta APF.

3.4. 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 da organização.

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

3.6. Norma Complementar nº 21/IN01/DSIC/GSIPR, de 8 de outubro de 2014, do Departamento de Segurança da Informação e Comunicações da Presidência da República, que estabelece as Diretrizes para o Registro de Eventos, Coleta e Preservação de Evidências de Incidentes de Segurança em Redes nos órgãos e entidades da Administração Pública Federal, direta e indireta.

4. Conceitos e definições

4.1. Artefato malicioso: qualquer programa de computador, ou parte de um programa, construído com a intenção de provocar danos, obter informações não autorizadas ou interromper o funcionamento de sistemas e/ou redes de computadores.

4.2. Ativos de Informação: os meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas com acesso aos mesmos.

4.3. Equipe de Tratamento e Resposta a Incidentes de Segurança da Informação ETIR: grupo de pessoas com a responsabilidade de receber, analisar e responder às notificações e atividades relacionadas a incidentes de segurança da informação em redes de computadores.

4.4. Evento adverso: ocorrência relevante para a segurança da informação, identificada em um sistema, serviço ou rede, indicativa de possível violação da Política de Segurança da Informação, ou falha de controles ou representativa de situação desconhecida.

4.5. Incidente de segurança em redes computacionais: qualquer evento adverso, confirmado ou sob suspeita.

4.6. Medida de contenção: controle e/ou ação para evitar que danos causados por um determinado incidente continuem aumentando com o passar do tempo. Além disso, visa o restabelecimento do sistema/serviço afetado, mesmo que não seja em sua capacidade total.

4.7. Medida de solução: controle e/ou ação tomada para sanar vulnerabilidades e problemas que sejam a causa-raiz de um ou mais incidentes de segurança em redes computacionais.

4.8. Tratamento de incidentes de segurança em redes computacionais: é o serviço que consiste em receber, filtrar, classificar e responder às solicitações e alertas, bem como realizar as análises dos incidentes de segurança, procurando extrair informações que permitam impedir a continuidade da ação maliciosa e também a identificação de tendências.

4.9. Usuários: magistrados e servidores ocupantes de cargo efetivo ou em comissão, requisitados e cedidos, desde que previamente autorizados, bem como empregados de empresas prestadoras de serviços terceirizados, consultores, estagiários, e outras pessoas que se encontrem a serviço da Justiça Eleitoral, utilizando em caráter temporário os recursos tecnológicos do TRE-BA.

4.10. Vulnerabilidade: qualquer fragilidade dos sistemas computacionais e redes de computadores que permitam a exploração maliciosa e acessos indesejados ou não autorizados.

5. Escopo

5.1. A Gestão de Incidentes de Segurança em Redes Computacionais, definida nesta Norma, tem seu escopo limitado às situações relacionadas ao ambiente, ativos e processos de TIC que suportam os principais processos de negócio do Tribunal Regional Eleitoral da Bahia.

6. Diretrizes

6.1. A Gestão de Incidentes de Segurança em Redes Computacionais tem de assegurar que incidentes na rede computacional sejam identificados, registrados e avaliados em tempo hábil, com a tomada de medidas de contenção e/ou solução adequadas.

6.2. Estão abrangidos por esta Norma os eventos, confirmados ou suspeitos, relacionados à segurança de sistemas ou redes computacionais, que comprometam o ambiente tecnológico do TRE-BA, seus ativos, informações e processos de negócio, bem como aqueles que contrariem a Política de Segurança da Informação, e dos quais decorram interrupção ou indisponibilidade de serviço essencial ao desempenho das atividades, vulnerabilidades de segurança, divulgação, alteração ou destruição de informações e/ou prática de ato definido como crime ou infração administrativa.

6.3. O Tribunal providenciará dispositivos de monitoramento, ferramentas de segurança e detecção de intrusão, a fim de subsidiar a Gestão de Incidentes de Segurança em Redes Computacionais.

7. Processo de Gestão de Incidentes de Segurança em Redes Computacionais

7.1. O processo de Gestão de Incidentes de Segurança em Redes Computacionais é contínuo e composto pelas seguintes etapas:

a) Detecção e registro: compreende a detecção ou recebimento de notificação de incidente de segurança em redes computacionais, seu registro e obtenção das autorizações necessárias para o encaminhamento da investigação.

b) Investigação e contenção: compreende a investigação e tratamento do incidente, coleta e preservação de evidências, comunicação às áreas afetadas, proposição e aplicação de ações de contenção, quando necessárias.

c) Encerramento: compreende a análise do incidente, com verificação da necessidade de outras ações, providências ou comunicações, e após seu cumprimento, o encerramento do incidente.

d) Avaliação de incidentes: compreende a avaliação do histórico de incidentes, com consolidação das informações e indicadores e verificação das oportunidades de melhoria e lições aprendidas.

7.1.1. O processo de Gestão de Incidentes de Segurança em Redes Computacionais deverá observar as diretrizes das Normas Complementares nº 08/IN01/DSIC/GSIPR e 21/IN01/DSIC/GSIPR.

7.1.2. A ETIR deverá recomendar, às áreas responsáveis, a implementação de diretrizes estabelecidas nas Normas indicadas no item 7.1.1.

7.2. O Tribunal poderá receber notificações externas (cidadão, CTIR.BR, CSIRT ou outras instituições) sobre incidentes (ocorridos ou suspeitos) por meio de sistemas gerenciadores de demandas, e-mail, telefone e outros canais de comunicação, que deverão ser remetidas à ETIR para o devido encaminhamento.

7.3. A notificação de incidente também poderá ser feita por qualquer usuário através da Central de Serviços de TIC ou pelo e-mail etir@treba.jus.br.

7.3.1. Os usuários devem notificar, com brevidade, os incidentes de segurança da informação e

vulnerabilidades de que tenham conhecimento ou suspeita.

7.3.2. Vulnerabilidades ou fragilidades suspeitas não poderão ser objeto de teste ou prova pelos usuários, sob o risco de violar a Política de Segurança da Informação e/ou provocar danos aos serviços ou recursos tecnológicos.

7.4. As equipes da Secretaria de Tecnologia da Informação, responsáveis pelo monitoramento dos ativos, serviços e sistemas deverão notificar os incidentes a eles relacionados à ETIR, para registro e encaminhamento devidos.

7.5. Os incidentes, notificados ou detectados, deverão ser objeto de registro, com a finalidade de assegurar a manutenção do histórico e auxiliar na geração de indicadores.

7.6. O tratamento da informação deverá ser realizado de forma a viabilizar e assegurar a disponibilidade, integridade, confidencialidade e autenticidade da informação, com retorno das operações à normalidade no menor prazo possível, bem como evitar futuras ocorrências, com a proposição de ações de solução, quando existentes.

7.7. A ETIR deverá, em conjunto com outras áreas ou pessoas quando necessário, investigar o incidente e artefatos maliciosos, propor e implementar as ações de contenção, comunicar as áreas afetadas e coletar os dados necessários.

7.8. A coleta de evidência dos incidentes de segurança em redes computacionais deverá ser realizada pela ETIR ou por pessoal competente autorizado.

7.9. Quando o incidente de segurança em redes computacionais decorrer de suspeita de descumprimento da Política de Segurança da Informação, será observado o sigilo durante todo o processo, ficando as evidências, informações e demais registros restritos aos envolvidos na investigação.

7.10. Quando houver indícios de ilícitos criminais durante o gerenciamento dos incidentes de segurança, o Comitê de Segurança da Informação e a Administração do TRE-BA deverão ser comunicados, para avaliação das providências cabíveis.

7.11. O encerramento do incidente de segurança em redes computacionais será realizado pela ETIR, com comunicação a todas as áreas interessadas.

7.12. A ETIR relacionar-se-á com a ETIR/JE, mantendo-a atualizada quanto às ocorrências de incidentes de segurança em redes computacionais e quanto às respectivas ações de tratamento.

7.12.1 O relacionamento da ETIR com o Centro de Tratamento de Incidentes de Segurança de Computadores da Administração Pública Federal CTIR Gov dar-se-á através da ETIR/JE.

7.13. A avaliação do processo de gestão de incidentes de segurança em redes computacionais ocorrerá através do histórico de incidentes, com verificação das oportunidades de melhoria.

7.14. O desenho do processo de Gestão de Incidentes de Segurança em Redes Computacionais, a descrição das atividades, os respectivos papéis e responsabilidades dos envolvidos no processo, bem como os modelos de documentos a serem utilizados nas etapas do processo, serão publicados no Portal de Governança do Tribunal, após aprovação pelo Comitê de Segurança da Informação.

7.15. O processo será revisto anualmente ou em menor prazo, quando necessário, e eventuais alterações propostas nos documentos acima indicados serão objeto de imediata divulgação na forma do item anterior, após aprovação pelo Comitê de Segurança da Informação.

ANEXO X

• *Anexo X acrescentado pela Portaria*

318/19. **NSI-010 Uso de Recursos**

Criptográficos OBJETIVOS

Estabelecer regras para o uso efetivo e adequado da Criptografia na proteção da informação no âmbito do Tribunal Regional Eleitoral da Bahia.

APLICABILIDADE

Este documento aplica-se aos magistrados, membros do Ministério Público, servidores efetivos e requisitados, ocupantes de cargo em comissão sem vínculo efetivo, estagiários, prestadores de serviço e colaboradores do TRE/BA.

MOTIVAÇÕES

Necessidade de proteção com recurso criptográfico de toda informação classificada, em qualquer grau de sigilo, produzida, armazenada ou transmitida pelo Tribunal, em parte ou totalmente, por qualquer meio eletrônico. Resguardar o sigilo das informações que o Tribunal produz e custodia no exercício de suas competências.

REFERÊNCIAS NORMATIVAS

Norma ABNT NBR ISO/IEC 27002:2013, no Objetivo de Controle 10.1.1, quanto à política para uso de controles criptográficos; Norma Complementar nº 09/IN01/DSIC/GSIPR, revisão 02, de 14/07/2014, sobre o uso de recurso criptográfico para a segurança de informações produzidas nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta.

CONCEITOS E DEFINIÇÕES

Algoritmo: função matemática utilizada na proteção de informações restritas, podendo ser:

a) Assimétrico: quando utiliza chaves criptográficas distintas para cifração e decifração de informações restritas.

b) Simétrico: quando utiliza a mesma chave criptográfica tanto para a cifração quanto para a decifração de informações restritas.

Ativo de Informação: os meios de armazenamento, transmissão e processamento da informação; os equipamentos necessários a isso; os sistemas utilizados para tal; os locais onde se encontram esses meios, e também as pessoas que a eles têm acesso;

Autenticidade: propriedade de que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado sistema, órgão ou entidade;

Certificado Digital: funciona como uma identidade virtual que permite a identificação segura e inequívoca do autor de uma mensagem ou transação feita em meios eletrônicos, como a web. Esse documento eletrônico é gerado e assinado por uma terceira parte confiável, ou seja, uma Autoridade Certificadora (AC) que, seguindo regras estabelecidas por um gestor, associa uma entidade (pessoa ou sistema informatizado) a um par de chaves criptográficas. Os certificados contêm os dados de seu titular conforme detalhado na Política de Segurança de cada Autoridade Certificadora;

Cifração: ato de cifrar mediante uso de algoritmo simétrico ou assimétrico, com recurso criptográfico, para substituir sinais de linguagem compreensível, por outros ininteligíveis por pessoas não autorizadas a conhecê-la;

Chave ou chave criptográfica: valor que trabalha com um algoritmo criptográfico para cifração ou decifração;

Controle criptográfico: sistema, programa, processo, equipamento isolado ou em rede que utiliza algoritmo simétrico ou assimétrico para realizar cifração ou decifração;

Credencial: permissões, concedidas por gestor competente após o processo de credenciamento, que habilitam determinada pessoa, sistema ou organização ao acesso. A credencial pode ser física como crachá, cartão e selo

ou lógica como identificação de usuário e senha;

Credenciamento: processo pelo qual o usuário recebe credenciais que concederão o acesso, incluindo a identificação, a autenticação, o cadastramento de código de identificação e definição de perfil de acesso em função de autorização prévia e da necessidade de conhecer;

Custodiante de ativo de informação: refere-se a qualquer indivíduo ou unidade da organização que tenha a responsabilidade formal de proteger um ou mais ativos de informação. Ele é responsável por aplicar os níveis de controles de segurança em conformidade com as exigências de segurança da informação comunicadas pelos proprietários dos ativos de informação;

Decifração: ato de decifrar mediante uso de algoritmo simétrico ou assimétrico, com recurso criptográfico, para reverter processo de cifração original;

Gestão de Riscos de Segurança da Informação e Comunicação: conjunto de processos que permite identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os ativos de informação e equilibrá-los com os custos operacionais e financeiros envolvidos;

ICP-Brasil: Instituido pela Medida Provisória nº 2.200-2, de 24 de Agosto de 2001, a Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil) é uma cadeia hierárquica e de confiança que viabiliza a emissão de certificados digitais para identificação virtual de pessoas físicas, pessoas jurídicas ou sistemas informatizados associados a pessoas físicas ou jurídicas;

Informação restrita: toda a informação que deva ser mantida em sigilo por tempo determinado, com acesso restrito a um grupo credenciado de pessoas que tenham necessidade de conhecê-la, conforme determinado por Lei, norma de classificação da informação e procedimentos de tratamento da informação;

Login de rede: código utilizado para identificação de um usuário da rede de computadores;

Necessidade de conhecer: condição pessoal, inerente ao efetivo exercício de cargo, função, emprego ou atividade, indispensável para o usuário ter acesso à informação, especialmente se for sigilosa, bem como o acesso aos ativos de informação;

Proprietário de ativo de informação: refere-se à parte interessada da unidade da organização, indivíduo legalmente instituído por sua posição e/ou cargo, o qual é responsável primário pela viabilidade e sobrevivência dos ativos de informação;

Recurso criptográfico: mesmo que controle criptográfico;

Senha de rede: informação secreta, de uso individual, utilizada para confirmar (autenticar) a identidade de um usuário da rede de computadores;

Usuário: pessoa que obteve autorização para acesso a Ativos de Informação do TRE/BA mediante a assinatura de Termo de Responsabilidade;

VPN: Virtual Private Network. Rede privada construída sobre uma infraestrutura de rede pública (comumente Internet), com recursos para proteção dos dados transmitidos contra interceptações e capturas.

Regras Gerais

Os controles criptográficos serão usados para assegurar, dentre outros:

a) a confidencialidade, a integridade e a autenticidade de informações sensíveis ou críticas que se encontrem armazenadas ou sob processo de transporte físico ou de transmissão eletrônica;

b) o não-repúdio: provar a ocorrência de um evento ou ação alegados e suas entidades originárias, de forma a resolver disputas sobre a ocorrência ou não ocorrência do evento ou ação e do envolvimento das entidades no evento.

c) a autenticação: confirmar a identidade de usuários ou de sistemas automatizados.

A falta de proteção criptográfica poderá ocorrer quando justificada e aprovada pela unidade gestora de riscos, ou pelo Comitê de Segurança da Informação, ou quando prevista em normativo específico.

A escolha dos tipos, da qualidade e da força de algoritmos, assim como a definição de que tipo de controle criptográfico é apropriado para cada propósito e processo de negócio, tomará como base, sempre que possível, o resultado do processo de gerenciamento de riscos de segurança da informação. Uma tabela relacionando os

controles criptográficos, seus parâmetros e sua aplicação na proteção de informações classificadas, será mantida e comunicada aos proprietários e custodiantes de ativos de informação.

É proibida a implantação de controles criptográficos não homologados pelo TRE-BA ou utilizá-los de forma distinta aos procedimentos estabelecidos para tal finalidade.

O tráfego de login/senha de rede, durante a autenticação de usuários, e de informações classificadas como restritas entre as camadas envolvidas nos sistemas ou serviços disponibilizados pelo TRE-BA, deve ser protegido com o uso de mecanismos de criptografia como HTTPS, SSL, TLS e VPN.

Quando permitido por norma de tratamento da informação, documentos restritos que forem armazenados em dispositivos móveis (notebook, tablet, smartphone etc.) ou em mídias removíveis (cd, dvd, pen drive, etc.) devem ser criptografados para evitar a sua divulgação indevida em caso de perda ou furto do equipamento ou da mídia.

ANEXO XI

• *Anexo X acrescentado pela Portaria 49/21*.

NSI 011 - PROTEÇÃO CONTRA CÓDIGOS MALICIOSOS

1. OBJETIVO

Dispor sobre as regras de segurança que nortearão a definição e a implantação de medidas para a proteção contra a ação de códigos maliciosos no ambiente de rede do Tribunal Regional Eleitoral da Bahia.

2. CONCEITOS E DEFINIÇÕES

Para os efeitos desta norma são estabelecidos os seguintes conceitos e definições:

1. Antivírus: ferramenta desenvolvida para detectar, anular e eliminar vírus e outros tipos de códigos maliciosos de um computador. Pode incluir também a funcionalidade de *firewall* pessoal;

2. Código malicioso: termo genérico que se refere a todos os tipos de programas especificamente desenvolvidos para executar ações danosas em recursos de tecnologia da informação;

3. *Firewall*: dispositivo de segurança usado para dividir e controlar o acesso entre redes de computadores;

4. *Firewall* pessoal: tipo específico de *firewall*. Programa usado para proteger um computador contra acessos não autorizados; e
5. *Log*: registro de atividades gerado por programas e serviços de um computador. Termo técnico que se refere ao registro de atividades de diversos tipos como, por exemplo: de conexão (informações sobre a conexão de um computador à Internet) e de acesso a aplicações (informações de acesso de um computador a uma aplicação de Internet).

3. CONSIDERAÇÕES INICIAIS

1. Conforme estabelecido na NSI-002 - Uso de Recursos de Tecnologia da Informação e Controle de Acesso, os usuários são responsáveis pelos recursos de tecnologia da informação por eles utilizados, devendo contribuir para seu funcionamento e segurança.

2. Códigos maliciosos são agentes potencialmente graves à segurança da informação, pois possibilitam o roubo de informações sigilosas e a paralisação dos serviços.

3. Convém que os recursos de tecnologia da informação estejam protegidos por sistemas de detecção e bloqueio de códigos maliciosos, prevenção e detecção de acesso não autorizado, tais como programas antivírus, programas de análise de conteúdo de correio eletrônico e *firewall*.

4. Padrões e procedimentos para instalação, configuração, utilização e atualização de sistemas de detecção e bloqueio de códigos maliciosos devem ser estabelecidos pela Secretaria de Tecnologia da Informação.

4. CONTROLES

1. É vedada qualquer atividade, por parte dos usuários, que vise à criação ou distribuição de códigos maliciosos.

2. É vedada ao usuário a desativação ou a alteração de configuração de quaisquer de seus componentes de proteção contra códigos maliciosos (por ex.: antivírus, *firewall* pessoal etc.). Caso julgue necessário alguma modificação, o setor responsável deverá ser informado.

3. Antes de sua utilização, é conveniente que toda e qualquer mídia de armazenamento que tenha origem externa ao Tribunal seja verificada quanto à existência de códigos maliciosos.

4. Convém que todo e qualquer arquivo recebido por correio eletrônico ou Internet seja verificado de forma automática quanto à existência de códigos maliciosos.

5. Convém que todos os dispositivos de processamento do Tribunal devam estar configurados de acordo com os padrões de segurança mais adequados aos serviços previstos, de maneira que prestem apenas os serviços previstos.

6. Convém que todos os dispositivos de processamento do Tribunal estejam atualizados conforme as recomendações dos respectivos fabricantes e fornecedores.

7. Os dispositivos de processamento portáteis, sempre que tecnicamente possível, devem possuir *firewall* pessoal instalado e configurado de forma a possibilitar que o dispositivo seja utilizado somente para os fins previstos.

8. Os sistemas de detecção e bloqueio de códigos maliciosos devem prover monitoramento, em tempo de execução, dos arquivos e programas, quanto à contaminação por código malicioso.

9. Os arquivos contaminados por código malicioso devem ser imediatamente descontaminados, isolados ou removidos do sistema pelo programa antivírus. Em caso de persistência do problema, o equipamento deve ser isolado até que seja sanado o problema para não afetar o desempenho das atividades do Tribunal.

5. COMPETÊNCIAS E RESPONSABILIDADES

Ficam definidas as seguintes competências e responsabilidades:

1. À Secretaria de Tecnologia da Informação:

1. auxiliar a Comissão de Segurança da Informação no processo de conscientização dos usuários quanto às melhores práticas de prevenção contra códigos maliciosos;

2. proceder com a instalação dos sistemas de detecção e bloqueio de códigos maliciosos nos equipamentos computacionais, mantendo-os atualizados conforme disponibilização do fabricante; e
3. monitorar os *logs* dos sistemas de detecção e bloqueio de códigos maliciosos, prevenção e detecção de acesso não autorizado, com objetivo de atuar de forma proativa na identificação de ameaças.

2. Ao usuário:

1. utilizar somente programas homologados pela Secretaria de Tecnologia da Informação;

2. observar se o programa de antivírus está instalado e ativo no equipamento computacional;

3. utilizar mídia de armazenamento que tenha origem externa à organização conforme disposto no item 4.3; e
4. notificar imediatamente à Comissão de Segurança da Informação e/ou Secretaria de Tecnologia da Informação qualquer suspeita de ataque por código malicioso à dispositivo de processamento sob sua custódia, ou mesmo a sua rede local.

6. DISPOSIÇÕES FINAIS

1. As atualizações e as correções para os sistemas de detecção e bloqueio de códigos maliciosos devem ser homologadas pela Secretaria de Tecnologia da Informação antes de aplicadas ao ambiente de produção.

2. As correções ou atualizações para os sistemas de detecção e bloqueio de códigos maliciosos, depois de homologadas, devem ser implementadas, a fim de se evitar que estes sistemas fiquem vulneráveis a códigos maliciosos ou a qualquer tentativa de acesso não autorizado.

3. Os casos omissos e as dúvidas surgidas na aplicação desta norma serão dirimidos pelo Comitê Gestor de Segurança da Informação.

7. VIGÊNCIA E ATUALIZAÇÃO

A atualização desta norma ocorrerá de forma periódica ou sempre que se fizer necessário, não excedendo o período máximo de 02 (dois) anos.

Anexo XIII

• *Anexo XIII acrescentado pela Portaria 654/21*.

(NSI 013 - Gerenciamento de Contas de Usuários Terceirizados, Estagiários, Requisitados, Juízes e Servidores Aposentados)

1 OBJETIVO

Estabelecer diretrizes para o gerenciamento das contas de rede, usuários de sistemas e e-mail institucional de terceirizados, estagiários, requisitados, magistrados e servidores aposentados no a âmbito do Tribunal Regional Eleitoral da Bahia.

2 CONCEITOS E DEFINIÇÕES

Bloquear contas de acesso - Ação de impedir que a conta seja utilizada para acesso aos recursos computacionais correspondentes (rede, e-mail ou banco de dados). Uma conta bloqueada não poderá ser usada, mas permanece consumindo cotas e espaço de armazenamento.

Excluir contas de acesso - Ação de remover definitivamente uma conta, de modo que os recursos por

ela consumidos passam a estar liberados para uso por outros usuários.

Princípio do "privilégio mínimo" - estratégia de segurança, aplicável a diferentes áreas, que se baseia na ideia de conceder autorizações apenas quando estritamente necessárias para o desempenho de uma atividade específica.

3 DIRETRIZES

3.1 Cabe à unidade responsável pelos contratos do TRE-BA o cadastramento dos contratos de terceirização firmados por este Regional em sistema apropriado.

3.2 As unidades gestoras dos contratos dos colaboradores terceirizados deverão manter os dados dos contratados atualizados em sistema destinado a esse fim, inclusive quanto à data de desligamento.

3.2.1 Ocorrido o desligamento do colaborador contratado, as unidades da STI (Secretaria de Tecnologia da Informação e Comunicação), de acordo com a sua área de competência, promoverão o bloqueio imediato das contas de acesso à rede de dados, e-mail institucional e sistemas. Transcorridos 10 (dez) dias do fim do desligamento do colaborador contratado, a STI promoverá a exclusão das contas de acesso à rede, e-mail institucional e sistemas.

3.3 A unidade gestora dos contratos de estágio deverá manter os dados atualizados em sistema de informática destinado ao cadastramento de estagiários, inclusive quanto à data fim do contrato.

3.3.1 Na data posterior ao fim do contrato de estágio, unidades da STI, de acordo com a sua área de competência, promoverão o bloqueio imediato das contas de acesso à rede de dados, e-mail institucional e sistemas dos referidos estagiários. Transcorridos 10 (dez) dias do fim do contrato de estágio, a STI promoverá a exclusão das contas de acesso à rede, e-mail institucional e sistemas.

3.4 Cabe à unidade gestora de informações de servidores requisitados registrar no Sistema de Gestão de Recursos Humanos a data de retorno de servidores requisitados ao órgão de origem, após comunicação formal da unidade requisitante

3.4.1Transcorrido 1 (um) dia útil do registro da data de retorno, a STI providenciará o bloqueio ou exclusão das contas de acesso à rede, e-mail institucional e sistemas.

3.5 A unidade gestora de dados de magistrados deverá informar em sistema de informática utilizado para cadastramento de juízes e desembargadores a data fim do biênio dos mesmos neste Regional, ao final do efetivo exercício.

3.5. Após o fim do biênio dos desembargadores eleitorais e juízes eleitorais, a STI providenciará o bloqueio imediato das contas de acesso à rede de dados, e-mail institucional e sistemas. A STI promoverá a exclusão definitiva desses acessos atendendo às seguintes regras:

I - imediatamente, para os Desembargadores Eleitorais titulares e substitutos, pertencentes à Classe dos Advogados, para os juízes das zonas eleitorais da capital e para os juízes indicados para substituir por tempo determinado em uma unidade zonal;

II - após 4 (quatro) meses, para os Desembargadores Eleitorais titulares e substitutos, pertencentes às Classes de Desembargador, Juiz de Direito e Juiz Federal, bem como para os juízes eleitorais das zonas eleitorais do interior.

3.6 A unidade responsável pela gestão dos dados dos servidores aposentados deverá manter atualizadas as informações de e-mail pessoal e telefone no Sistema de Gestão de Recursos Humanos adotado pela Justiça Eleitoral.

3.6.1 Quando do registro da data de aposentadoria de um servidor no Sistema de Gestão de Recursos

Humanos, a STI providenciará o bloqueio imediato das contas de acesso à rede de dados, e-mail institucional e sistemas. Transcorridos 10 (dez) dias do registro da data de aposentadoria de um servidor, a STI promoverá a exclusão definitiva desses acessos.

3.6.2A unidade responsável pela gestão dos dados dos servidores aposentados deverá atualizar o endereço de e-mail pessoal de servidor inativo e proceder à devida comunicação no prazo de 180 dias. Após esse período, as contas de e-mail institucional de servidores aposentados que se encontrarem ativas serão excluídas.

3.7 As ações para bloqueio imediato, bem como para a exclusão definitiva de contas de rede, e-mail e sistemas se darão através de procedimentos automatizados a serem desenvolvidos pela STI, num prazo de 180 dias.

3.8 As contas de acesso à rede, e-mail e sistemas atualmente ativas que se encontrem sem uso pelo período de um ano no momento em que esta norma entrar em vigor deverão ser imediatamente bloqueadas. A STI promoverá a sua exclusão definitiva após novo prazo de 3 (três) meses contatos a partir do bloqueio, caso não ocorra solicitação explícita para sua reativação.

3.9 No caso da exclusão definitiva das contas de acesso a sistemas, deve haver mecanismo automático de auditoria, armazenando dados identificadores da exclusão (conta excluída, titular da conta, responsável pela exclusão, data e hora da exclusão, permissões a objetos de banco de dados) para fins de posterior necessidade de recuperação.

3.10 No caso de exclusão definitiva das contas de e-mail, em atenção ao disposto na Política de Segurança da Informação da Justiça Eleitoral, deve-se manter cópias de segurança desses dados pelo prazo de 240 dias, para eventual necessidade de análise e investigação de incidentes.

3.11 A STI dará conhecimento às unidades competentes de quais dados são pré-requisito para a possível criação de recursos (contas de rede, e-mail e sistemas) para colaboradores. Dessa forma, caso o indivíduo não esteja cadastrado adequadamente em seu sistema correspondente, não haverá a criação das contas.

4 PAPÉIS E RESPONSABILIDADES

4.1 Constitui incumbência dos fiscais de contratos de terceiros comunicar à STI, no prazo de 30 dias contados a partir da entrada em vigor dessa NSI, a relação nominal de colaboradores terceirizados que necessitem de recursos de TIC fornecidos pelo TRE/BA, com justificativa fundamentada, em atenção ao princípio do "privilégio mínimo".

4.1.1 A comunicação deverá abranger tanto os acessos já existentes quanto os novos, que vierem a ser concedidos.

4.1.2 Enquanto não disponibilizada pela STI a solução técnica citada no item 3.7, essa comunicação se dará, preferencialmente, através de abertura de chamados na Central de Serviços de TIC.

4.1.2.1 O mesmo se aplica com relação ao desligamento dos terceiros, ao término do contrato. Nessa hipótese, a comunicação deve ser imediata.

4.1.3 Transcorrido o prazo de 10 (dez) dias sem manifestação dos fiscais de contratos, os acessos serão revogados e as contas excluídas, até o advento de nova solicitação com as informações requeridas.

5 VIGÊNCIA E ATUALIZAÇÃO

A atualização desta norma ocorrerá de forma periódica ou sempre que se fizer necessário, não excedendo o período máximo de 02 (dois) anos.