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 s problemas de *software* serão solucionados pela reinstalação padrão, ficando a área de suporte a usuário desobrigada de reinstalar e configurar programas que o usuário tenha instalado por iniciativa própria e isento da responsabilidade sobre eventual perda de dados.~~

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. (Redação dada pela Portaria nº 400/2018)

~~5.3.2.2. A instalação, manutenção e suporte de qualquer *software*/sistema não fornecido pelo Tribunal, bem como o *backup* de dados locais, são de exclusiva responsabilidade do usuário.~~ (Revogado pela Portaria nº 400/2018)

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 Secretaria 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. (Incluído pela Portaria nº 400/2018)

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. (Incluído pela Portaria nº 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.