ANEXO II

NSI-002 – Gestão de Identidade e Controle de Acesso Físico e Lógico

1. Objetivo e Âmbito de Aplicação

1.1. São objetivos desta norma:

I - Estabelecer diretrizes para gestão de identidade e controle de acesso físico e lógico relativos à segurança da informação no âmbito do Tribunal Regional Eleitoral da Bahia (TRE-BA);

II - Assegurar a confidencialidade, integridade e disponibilidade dos ativos de informação e comunicação sob a responsabilidade deste Tribunal.

1.2. Os usuários de TIC são corresponsáveis pela segurança da informação e comunicação, de acordo com os preceitos estabelecidos neste normativo.

1.3. Os usuários de ativos de TI são responsáveis por:

a) manter o ambiente seguro, incluindo criação de senhas seguras, conforme os padrões estabelecidos nesta norma;

b) manter a confidencialidade das informações acessadas;

c) informar imediatamente qualquer risco identificado ou presumido à segurança da instituição.

2. Princípios

2.1. O controle de acesso é regido pelos seguintes princípios:

I - Necessidade de saber: os usuários deverão ter acesso somente às informações necessárias ao desempenho de suas tarefas;

II - Necessidade de uso: os usuários deverão ter acesso apenas aos ativos (equipamentos de TI, sistemas, aplicações, procedimentos, salas) necessários ao desempenho de suas tarefas;

III - Privilégio mínimo: deverão ser conferidos apenas os privilégios necessários para que o usuário realize a sua função na organização;

IV - Segregação de funções: as funções desempenhadas no controle de acesso se dividem em pedido de acesso, autorização de acesso e administração de acesso.

3. Referências Normativas

3.1. Instrução Normativa GSI nº 1, de 27 de maio de 2020, do Gabinete de Segurança Institucional da Presidência da República, que dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal.

3.2. Portaria TSE nº 262, de 08 de abril de 2024, que dispõe sobre o Controle de Acesso Físico e Lógico Relativos à Segurança das Informações e Comunicações do Tribunal Superior Eleitoral.

3.3. Norma Técnica ABNT NBR ISO/IEC 27001, 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, que fornece diretrizes para práticas de gestão de segurança da informação.

4. Conceitos e Definições

4.1. Para efeitos desta norma, consideram-se os termos e definições previstos na Portaria TSE nº 444/2021, aplicando-se, de forma subsidiária, aqueles estabelecidos no Glossário de Segurança da Informação do Gabinete de Segurança Institucional da Presidência da República, regulamentado por meio da Portaria GSI/PR n.º 93, de 18 de outubro de 2021.

5. Do Gerenciamento de Acesso Lógico

5.1. O acesso aos sistemas de informação será assegurado, unicamente, ao usuário devidamente identificado e autorizado.

5.1.1. As credenciais de acesso são pessoais e intransferíveis, sendo vedado o compartilhamento de credenciais em qualquer situação, inclusive nas hipóteses de substituição temporária de função.

5.1.2. Todas as ações e atividades executadas pelo usuário, utilizando suas credenciais de acesso, serão de sua exclusiva responsabilidade, bem como os possíveis danos decorrentes de uso indevido, devendo zelar pelo sigilo de seu acesso.

5.1.3. As regras de controle de acesso deverão ser baseadas na premissa de mínimo privilégio, para atendimento das demandas de trabalho do usuário.

5.2. Compete aos gestores de sistemas estabelecer regras de concessão, bloqueio e revogação de acesso dos usuários, levando em conta as políticas, princípios e normas de controle de acesso específicas aplicáveis a cada ativo.

5.3. A concessão e a revogação de acesso serão implementadas por meio de um processo formal, preferencialmente automatizado, com estabelecimento de responsáveis pela solicitação, administração, concessão, bloqueio e revogação.

5.3.1. As contas deverão ser desabilitadas, em vez de excluídas, para preservação de trilhas de auditoria.

5.4. Os usuários devem possuir identificação única e exclusiva para permitir relacioná-la às suas ações e responsabilidades.

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

5.6. Compete à chefia imediata, ao gestor do sistema ou ao gestor de contrato solicitar à Secretaria de Tecnologia da Informação e Comunicação:

I – a concessão dos acessos necessários ao desenvolvimento das atividades dos servidores efetivos, requisitados, ocupantes de cargo em comissão sem vínculo efetivo 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 servidores efetivos, requisitados, ocupantes de cargo em comissão sem vínculo efetivo e estagiários 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 servidores efetivos, requisitados, ocupantes de cargo em comissão sem vínculo efetivo e estagiários ou a prestador de serviço de contrato sob sua gestão, imediatamente após o seu afastamento ou desligamento da unidade ou do contrato;

5.6.1. 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.

5.7. Em redes locais, especialmente de 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.

5.8. 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.

5.9. Compete a Secretaria de Gestão de Pessoas (SGP) cadastrar em sistema próprio 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 automatizada dos acessos concedidos aos usuários.

5.9.1. No caso de terceirizados, este cadastramento caberá aos gestores de contratos.

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

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

5.12. Os direitos de acessos dos usuários deverão ser revisados em intervalos regulares, bem como após mudança de função, alteração de lotação ou desligamento.

5.12.1. Compete ao gestor de sistema realizar a revisão de direitos de acesso ao ativo sob sua responsabilidade.

5.13. 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).

5.14. A Secretaria de Tecnologia da Informação e Comunicação efetuará bloqueio automático das credenciais de acesso dos usuários que não realizaram acesso por mais de 90 (noventa) dias consecutivos, incluindo servidores aposentados, cedidos e licenciados.

5.14.1. O desbloqueio de credencial será realizado pela Secretaria de Tecnologia da Informação e Comunicação, mediante solicitação do titular da unidade vinculada ao usuário ou da Secretaria de Gestão de Pessoas.

5.15. 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. Do Acesso Privilegiado

6.1. O acesso privilegiado aos sistemas e ativos de informação somente será concedido aos usuários que tenham como atribuição funcional o dever de administrá-los.

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

6.2. A credencial de acesso privilegiado é de uso pessoal e intransferível, qualificando o usuário, inequivocamente, como responsável por quaisquer acessos e ações realizados com a sua credencial, bem como pelos possíveis danos decorrentes de uso indevido.

6.3. Os direitos de acesso dos usuários privilegiados devem ser revistos trimestralmente, bem como após qualquer mudança de nível institucional que implique em realocação de pessoas, unidades ou papéis, considerando ainda a consistência entre os direitos de acesso e as necessidades e requisitos de segurança.

7. Da Concessão do Acesso à Rede, Sistemas e Serviços de Rede

7.1. A gestão de credenciais de usuários e o controle de acesso se darão de forma centralizada, por meio de serviço de diretório, restrito e controlado pela Secretaria de Tecnologia da Informação e Comunicação.

7.1.1. Os direitos de acesso lógico dos usuários à rede corporativa devem ser definidos por meio de credencial e perfil de acesso, de acordo com a sua alocação e função.

7.2. A criação de nomes de usuário e de contas de e-mail seguirá os seguintes critérios:

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

7.2.2. Cada usuário receberá também um identificador alternativo, sendo formado pelo prenome, seguido do ponto (.) e do último sobrenome, no estilo prenome.sobrenome.

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

7.3. 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.

8. Política de Senhas

8.1. Os sistemas ou serviços de informação, considerados passíveis de controle de acesso, devem ter seu acesso restrito e controlado através do uso de senhas, *token* ou mecanismo de autenticação similar.

8.1.1. O acesso remoto à rede, o acesso administrativo e o acesso a aplicações expostas externamente se darão por autenticação multifatorial (MFA).

8.1.2. A STI poderá implantar a autenticação de multifatores para determinados tipos de acesso, em função de sua criticidade.

8.2. As senhas de acesso do usuário, tokens e outros fatores de autenticação devem ser de uso pessoal e intransferível.

8.3. Na utilização das credenciais de acesso, compete ao usuário observar as recomendações a seguir indicadas, 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, sob pena de responsabilização pelos acessos indevidos.

III – não utilizar senhas com frases ou palavras que possam ser facilmente adivinhadas por terceiros, baseadas em informações relativas ao próprio usuário, tais como nome de parentes, datas de aniversário e números de telefone;

IV – não utilizar senhas formadas por sequência de caracteres triviais, tais como 123456 ou abcde, ou senhas simples que repitam a identificação do usuário, como, por exemplo, usuário joao.silva e senha joao.silva;

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

VI – não utilizar o recurso de salvamento automático das senhas institucionais nos navegadores;

VII – não utilizar as mesmas credenciais (nome de usuário e senha institucionais) para fins particulares e profissionais, sob pena de responsabilização pelos acessos indevidos.

8.4. 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) números (0 a 9);

d) caracteres especiais (!, $, #, % etc.).

8.4.1. Excetuam-se ao quanto estabelecido no item 8.4. os sistemas atualmente disponibilizados que não permitam o atendimento aos requisitos estabelecidos.

8.5. A senha temporária, para primeiro acesso ou no caso de o usuário esquecer a sua senha, deverá ser emitida através de procedimento instruído pela equipe de suporte da Secretaria de Tecnologia da Informação e Comunicação.

8.5.1. Fica vedada a emissão de senha para ciência de terceiros, ainda que chefes imediatos ou superiores do usuário, bem como o seu envio através de texto claro ou correio de terceiro.

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

8.7. 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.

9. O Sistema de Gerenciamento de Senha deve:

9.1. Permitir que os usuários selecionem e modifiquem suas próprias senhas, incluindo procedimento de confirmação para evitar erros;

9.2. Forçar as mudanças de senha em intervalos regulares de, no máximo, 180 (cento e oitenta) dias, conforme necessidade;

9.3. Manter registro, no mínimo, das 10 (dez) senhas anteriores utilizadas e bloquear sua reutilização;

9.4. Armazenar e transmitir as senhas de forma protegida;

9.5. Não mostrar as senhas na tela quando forem digitadas;

9.6. Garantir a modificação das senhas temporárias no primeiro acesso ao sistema ou serviço de informação.

9.7. Monitorar tentativas de acesso a contas desativadas.

10. Procedimentos Seguros de Entrada no Sistema

10.1. O procedimento adequado de entrada no sistema (*login*) deve atender às seguintes recomendações:

I - não fornecer mensagens de ajuda ou informações do sistema, durante o procedimento de entrada, que possam auxiliar usuário não autorizado;

II - validar informações de entrada no sistema somente após todos os dados estarem completamente preenchidos;

III - em caso de erro, não indicar qual parte do dado de entrada está correta ou incorreta;

IV - bloquear o acesso do usuário ao sistema após, no máximo, 10 (dez) tentativas de entrada no sistema;

V - registrar tentativas de acesso ao sistema, sem sucesso e bem-sucedidas;

VI - por ocasião da entrada no sistema, mostrar as seguintes informações:

a) data e hora da última entrada no sistema ou equipamento, com sucesso; e

b) detalhes de qualquer tentativa sem sucesso de entrada no sistema;

VII - encerrar sessões inativas, após um período definido de inatividade de, no máximo, 10 minutos;

VIII - em caso de uso externo, o tempo de conexão deverá ser restringido para reduzir oportunidade de acesso não autorizado.

11. Do Controle de Acesso ao Código-Fonte de Programas

11.1. O código-fonte e os itens associados (esquemas, especificações, planos de validação, etc.) dos sistemas de informação desenvolvidos pelo Tribunal somente serão acessíveis aos usuários que tenham como atribuição funcional seu desenvolvimento, manutenção ou outra atividade para a qual o acesso seja imprescindível.

11.2. As bibliotecas de código-fonte e de itens associados devem ser armazenadas em ferramentas apropriadas para esse fim, em ambientes segregados dos sistemas operacionais em que os respectivos sistemas de informação sejam executados.

11.3. Os eventos de acesso às bibliotecas de código-fonte e de itens associados devem ser registrados, de forma a permitir sua auditoria.

11.4. Códigos-fonte que sejam publicados para entidades externas devem contar com controles adicionais que garantam sua integridade.

12. Registros (*log*) de Eventos

12.1. 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.

12.1.2. 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.

13. Controle de Acesso Físico

13.1. Do Perímetro de Segurança

13.1.1. Fica estabelecido, por meio deste normativo, que as instalações de processamento e armazenamento da informação (datacenter) e das demais áreas de TI que contenham informações críticas ou sensíveis serão tratados como perímetro de segurança física devendo receber proteção adequada e compatível com a importância dos ativos de informação.

13.1.2. As instalações do *datacenter* devem atender às seguintes diretrizes:

I - paredes fisicamente sólidas, sem brechas nem pontos por onde possa ocorrer uma invasão, portas protegidas por mecanismos de controle contra acesso não autorizado;

II - videomonitoramento de sua área interna e de seu perímetro;

III - controle de acesso físico às áreas e instalações, sob a responsabilidade da Secretaria de Tecnologia da Informação e Comunicação (STI), utilizando-se dos mecanismos necessários para o controle e registro de data e hora de todas as entradas e saídas, sejam de servidores, visitantes ou prestadores de serviço, permitindo-lhes o acesso, desde que previamente autorizados;

IV- mecanismos de controle de acesso às áreas críticas, conforme definido pela Secretaria de Tecnologia da Informação e Comunicação;

V - instalações de processamento e armazenamento das informações que sejam projetadas para minimizar os riscos de ameaças físicas potenciais;

VI - edifícios que sejam dotados de proteção contra raios e que, em todas as linhas de entrada de força e de comunicações, tenham filtros de proteção contra raios;

VII - alimentações de energia elétrica e telecomunicações, com rotas físicas diferentes;

VIII - iluminação e comunicação de emergência;

IX - sistema de controle de temperatura e umidade com recurso de emissão de alertas.

13.1.3. As diretrizes para proteção das demais áreas que contenham informações críticas ou sensíveis que não estejam armazenadas no *datacenter* devem ser estabelecidas pelo Comitê de Governança de Segurança da Informação, observadas as legislações vigentes.

13.2. Dos Equipamentos de Processamento e Armazenamento

13.2.1. Para evitar perdas, danos, furtos ou comprometimento de ativos e interrupção das operações da organização, o Tribunal deverá observar as seguintes diretrizes:

I - adotar controles para minimizar o risco de ameaças físicas potenciais e ambientais;

II - verificar se os suprimentos de energia elétrica, telecomunicações, água, gás, esgoto, calefação/ventilação e sistema de ar-condicionado estejam em conformidade com as especificações do fabricante do equipamento e com os requisitos legais da localidade;

III - adotar controles para evitar a retirada de equipamentos do Tribunal sem prévia autorização da unidade competente, conforme regulamentação específica;

IV - utilizar, sempre que possível, racks que disponham de fechaduras com chave ou mecanismo semelhante, garantindo que apenas a(s) equipe(s) responsáveis pelos ativos instalados nos racks possam acessá-los fisicamente.

13.3. Da Segurança do Cabeamento

13.3.1. O cabeamento de energia elétrica e de telecomunicações que transporta dados ou dá suporte aos serviços de informações deve ser protegido contra interceptação, interferência ou danos, conforme as seguintes diretrizes:

I - as linhas de energia elétrica e de telecomunicações que entram nas instalações de processamento da informação devem ser subterrâneas ou ficar abaixo do piso, sempre que possível, e devem atender aos requisitos mínimos de proteção;

II - os cabos de energia elétrica devem ser segregados dos cabos de comunicação, para evitar interferências.

13.4. Da Manutenção Externa dos Equipamentos

13.4.1. A manutenção dos equipamentos de processamento de informações deve seguir as seguintes diretrizes:

I - ser realizada somente por pessoal de manutenção identificado e autorizado;

II - manter registro de todas as falhas, constatadas ou suspeitas, e de todas as operações de manutenção preventiva e corretiva realizadas;

III - eliminar as informações sensíveis do equipamento, quando possível, ou tratar de forma alternativa os riscos de sua exposição;

IV - inspecionar o equipamento, após a manutenção, para garantir que não foi alterado indevidamente e que está em perfeito funcionamento.

13.5. Da Reutilização ou Descarte Seguro dos Equipamentos ou dos Equipamentos em Prova de Conceito

13.5.1. Todos os equipamentos que contenham mídias de armazenamento de dados devem ser examinados antes da reutilização ou descarte, para assegurar que dados sensíveis e softwares licenciados tenham sido removidos ou sobregravados com segurança.

13.5.2. As mídias que contenham informações com acesso restrito de propriedade intelectual devem ser apagadas fisicamente. Da mesma forma, as informações devem ser destruídas, apagadas ou sobrescritas por meio de técnicas que tornem as informações originais irrecuperáveis.

13.6. Da Política de Mesa Limpa e Tela Limpa

13.6.1. Informação com restrição de acesso não deve ser deixada à vista sobre mesas de trabalho ou em quaisquer outros suportes que não disponham de mecanismos de controle de acesso e deve ser destruída antes de ser descartada, seja em papel ou em meio eletrônico.

13.6.1.2. A política de mesa limpa para papéis e mídias de armazenamento removíveis deve considerar a classificação da informação, requisitos contratuais e legais e o risco correspondente.

13.6.2. Computadores pessoais e terminais de computador não devem apresentar senhas na tela e não devem permanecer logados, caso o usuário esteja ausente.

13.6.2.1. A política de tela limpa para computadores e terminais deve ser aplicada por meio de bloqueio de tela por senha, *token* ou mecanismo de autenticação similar.

13.6.3. Os documentos físicos contendo dados pessoais devem ser guardados em local devidamente protegido com chave, com acesso restrito a pessoas autorizadas.

14. Das Disposições Finais

14.1. Os casos omissos serão resolvidos pelo Comitê de Governança de Segurança da Informação (CGSI).

14.2. A revisão desta norma ocorrerá sempre que se fizer necessário, não excedendo o período máximo de 03 (três) anos.

14.3. O descumprimento desta norma será objeto de apuração pela unidade competente do TRE-BA, com a consequente aplicação das penalidades cabíveis a cada caso.