TRIBUNAL REGIONAL ELEITORAL DO PIAUI

Portaria Presidência Nº 320/2023 TRE/PRESI/DG/ASSDG, de 06 de agosto de 2023

Institui regras para a Gestão de Identidade e o Controle de Acesso Físico e Lógico ao ambiente cibernético do Tribunal Regional Eleitoral do Piauí.

O PRESIDENTE DO TRIBUNAL REGIONAL ELEITORAL DO PIAUÍ, no uso de suas atribuições legais e regimentais,

CONSIDERANDO a necessidade de definir processos de gestão de identidade e controle de acesso físico e lógico aos ativos de informação;

CONSIDERANDO que a segurança da informação e a proteção de dados pessoais são condições essenciais para a prestação dos serviços jurisdicionais e administrativos;

CONSIDERANDO, ainda, que o acesso à informação, assim como aos recursos de processamento das informações e aos processos de negócios, deve ser controlado com base nos requisitos de negócio e da segurança da informação;

CONSIDERANDO a Resolução CNJ nº 396/2021, que instituiu a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ);

CONSIDERANDO a Resolução TSE nº 23.644/2021, que instituiu a Política de Segurança da Informação (PSI) no âmbito da Justiça Eleitoral;

CONSIDERANDO a Resolução TRE-PI nº 448/2022 que adota a PSI da Justiça Eleitoral estabelecida pela Resolução TSE nº 23.644/2021;

CONSIDERANDO a NC 07/IN01/DSIC/GSIPR, de 15 de julho de 2014, que estabeleceu diretrizes para implantação de controles de acesso relativos à segurança da informação e das comunicações na Administração Pública Federal;

CONSIDERANDO as boas práticas de segurança da informação previstas nas normas ABNT ISO/IEC 27001 e ABNT ISO/IEC 27002; e

CONSIDERANDO as recomendações do Acórdão 1.603/2008-TCU, item 9.1.3, sobre a importância dos controles de acesso,

RESOLVE:

Art. 1º Fica instituída a Norma de Gestão de Identidade e Controle de Acesso Físico e Lógico relativa à segurança da informação e comunicação no âmbito do Tribunal Regional Eleitoral do Piauí.

Art. 2º Esta norma integra a Política de Segurança da Informação da Justiça Eleitoral, estabelecida pela Resolução TSE n. 23.644/2021 e Resolução TRE-PI nº 448/2022.

Capítulo I

Dos conceitos e definições

Art. 3º Para efeitos desta norma consideram-se os termos e definições a seguir:

I - Agente público: todo aquele que exerce, ainda que transitoriamente com ou sem remuneração, por eleição, nomeação, designação, contratação ou qualquer outra forma de investidura ou vínculo, mandato, cargo, emprego ou função nos órgãos e entidades da APF, direta e indireta;

II - Ameaça: causa potencial de um incidente indesejado que pode resultar em dano para um sistema ou organização;

III - Atividades precípuas: conjunto de procedimentos e tarefas que utilizam recursos tecnológicos, humanos e materiais, inerentes à atividade-fim da Justiça Eleitoral;

IV - Ativo de processamento: patrimônio composto por todos os elementos de hardware, software e infraestrutura de comunicação necessários à execução das atividades precípuas da Justiça Eleitoral;

V - Ativo de TI: o mesmo que ativo de processamento;

VI - Ativo: qualquer bem, tangível ou intangível, que tenha valor para a organização;

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

VIII - Confidencialidade: propriedade da informação que garante que ela não será disponibilizada ou divulgada a indivíduos, entidades ou processos sem a devida autorização;

IX - Credencial (ou conta de acesso): permissão, concedida por autoridade competente após o processo de credenciamento, que habilita determinada pessoa, sistema ou organização ao acesso de recursos. A credencial pode ser física (como um crachá), ou lógica (como a identificação de usuário e senha);

X - Custodiante: aquele que, de alguma forma, total ou parcialmente, zela pelo armazenamento, operação, administração e preservação de um sistema estruturante - ou dos ativos de informação que compõem o sistema de informação - que não lhe pertence, mas que está sob sua custódia;

XI - 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;

XII - Incidente em segurança da informação: qualquer indício de fraude, sabotagem, desvio, falha ou evento indesejado ou inesperado que tenha probabilidade de comprometer as operações do negócio ou ameaçar a segurança da informação;

XIII - Informação: conjunto de dados, textos, imagens, métodos, sistemas ou quaisquer formas de representação dotadas de significado em determinado contexto, independentemente do suporte em que resida ou da forma pela qual seja veiculado;

XIV - Integridade: propriedade que garante que a informação mantém todas as características originais estabelecidas pelo proprietário;

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

XVI - Recurso: além da própria informação, é todo o meio direto ou indireto utilizado para o seu tratamento, tráfego e armazenamento;

XVII - Recursos de Tecnologia da Informação: são o conjunto de bens e serviços de tecnologia da informação que constituem a infraestrutura tecnológica de suporte automatizado ao ciclo da informação, que envolve as atividades de produção, coleta, tratamento, armazenamento, transmissão, recepção, comunicação e disseminação;

XVIII - Rede de computadores: rede formada por um conjunto de máquinas eletrônicas com processadores capazes de trocar informações e partilhar recursos, interligados por um subsistema de comunicação, ou seja, existência de dois ou mais computadores, e outros dispositivos interligados entre si de modo a poder compartilhar recursos físicos e lógicos, sendo que estes podem ser do tipo dados, impressoras, mensagens (e-mails), entre outros;

XIX - Risco: potencial associado à exploração de vulnerabilidades de um ativo de informação por ameaças, com impacto negativo no negócio da organização;

XX - Usuário: aquele que utiliza, de forma autorizada, recursos inerentes às atividades precípuas da Justiça Eleitoral;

XXI - Vulnerabilidade: fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças.

Capítulo II

Dos princípios

Art. 4º 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 e 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; e

IV - Segregação de funções: consiste na separação das funções desempenhadas no controle de acesso, por exemplo, pedido de acesso, autorização de acesso e administração de acesso.

Capítulo III

Do escopo e do âmbito de aplicação

Art. 5º O objetivo desta Norma de Gestão de Identidade e Controle de Acesso Físico e Lógico relativos à segurança da informação e comunicação consiste em:

I - Estabelecer diretrizes para implantação de controles de acesso físico e lógico; e

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

Art. 6º Esta Norma se aplica a toda(o)s as magistradas ou magistrados, servidoras ou servidores efetiva(o)s e requisitada(o)s, ocupantes de cargo em comissão sem vínculo efetivo, estagiárias ou estagiários, prestadoras ou prestadores de serviço, colaboradoras ou colaboradores e usuária(o)s externos, outros órgãos

públicos ou entidades privadas contratadas ou com parcerias celebradas, acordos de cooperação de qualquer tipo, convênios e termos congêneres que fazem uso dos ativos de informação e de processamento no âmbito da Justiça Eleitoral.

§ 1º Os contratos celebrados pelo Tribunal deverão atender os requisitos desta política, bem como as normas referentes à proteção de dados pessoais.

§ 2º Os destinatários desta norma, relacionados no *caput*, são corresponsáveis pela segurança da informação, de acordo com os preceitos estabelecidos neste normativo.

Capítulo IV

Do controle de acesso físico

Seção I

Do perímetro de segurança

Art. 7º A Comissão de Segurança da Informação (CSI) deve definir o perímetro de segurança física para proteção das instalações de processamento e armazenamento da informação (*datacenter*) e das demais áreas que contenham informações críticas ou sensíveis.

Art. 8º As instalações do *datacenter* devem atender às seguintes diretrizes:

I - paredes fisicamente sólidas, sem brechas nem pontos por onde possa ocorrer uma invasão, portas externas adequadamente protegidas por mecanismos de controle contra acesso não autorizado, sem janelas ou, na impossibilidade, com janelas com proteção externa;

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 da Secretaria de Administração, Orçamento e Finanças, 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 autenticação de multifatores, para as instalações de processamento, armazenamento e comutação de dados, restritas ao pessoal autorizado;

V - portas corta-fogo com sistema de alarme, monitoradas, que funcionem de acordo com os códigos locais, para minimizar os riscos de ameaças físicas potenciais;

VI - sistemas para detecção de intrusos em todas as portas externas;

VII - instalações de processamento e armazenamento das informações que sejam projetadas para minimizar os riscos de ameaças físicas potenciais, tais como fogo, inundação, enchente, inundação, vibrações danosas, explosão, manifestações civis, contra-ataques maliciosos, fumaça e furtos;

VIII - 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;

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

X - iluminação e comunicação de emergência;

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

Art. 9º As diretrizes para proteção das demais áreas que contenham informações críticas ou sensíveis que não estejam armazenadas no *datacenter* devem ser estabelecidas pela CSI, observadas as legislações vigentes.

Seção I

Dos controles de entrada física

Art. 10. As áreas seguras devem ser protegidas por controles apropriados de entrada para assegurar que somente pessoas autorizadas tenham acesso permitido, conforme as seguintes diretrizes:

I - a data e a hora de entrada e saída de visitantes devem ser registradas e todos os visitantes devem ser supervisionados, exceto se o seu acesso tenha sido previamente aprovado;

II - as permissões de acesso sejam concedidas somente para finalidades específicas e autorizadas, observando as instruções sobre os requisitos de segurança da área e os procedimentos de emergência;

III - as identidades dos visitantes sejam autenticadas por meios apropriados;

IV - o acesso às áreas de processamento ou armazenamento de informações sensíveis seja restrito apenas ao pessoal autorizado pela implementação de controles de acesso apropriados;

V - seja mantido e monitorado de forma segura o registro físico de todos os acessos ou uma trilha de auditoria eletrônica;

VI - os funcionários, fornecedores e partes externas e todos os visitantes tenham alguma forma visível de identificação;

VII - aos fornecedores ou prestadores de serviço externos que realizam serviços de suporte, seja concedido acesso restrito às áreas seguras ou às instalações de processamento da informação sensíveis, somente quando necessário e que este acesso seja autorizado e monitorado.

VIII - os direitos de acesso às áreas seguras devem ser revistos e atualizados em intervalos regulares, e revogados quando necessário.

Seção II

Dos equipamentos de processamento e armazenamento

Art. 11. Para evitar perdas, danos, furtos ou comprometimento de ativos e interrupção das operações da organização, o Tribunal deve seguir as seguintes diretrizes:

I - adotar controles para minimizar o risco de ameaças físicas potenciais e ambientais, como furto, incêndio, explosivos, fumaça, água, poeira, vibração, efeitos químicos, interferência com o suprimento de energia elétrica, interferência com as comunicações, radiação eletromagnética e vandalismo;

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; e

IV - utilizar, sempre que possível, *racks* que disponham de fechaduras com chave ou mecanismo semelhante, garantindo que apenas as equipes responsáveis pelos ativos instalados nos *racks* tenham acesso físico a eles.

Seção III

Da segurança do cabeamento

Art. 12. 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; e

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

Seção IV

Da manutenção externa dos equipamentos

Art. 13. 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; e

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

V - ser realizada nos intervalos recomendados pelo fornecedor e de acordo com as suas especificações;

VI - atender todas as exigências de manutenção estabelecidas nas apólices de seguro.

Seção V

Da reutilização ou descarte seguro dos equipamentos ou dos equipamentos em prova de conceito

Art. 14. 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.

§ 1º 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 sobregravadas por meio de técnicas que tornem as informações originais irrecuperáveis.

§ 2º Devem ser observados os requisitos estabelecidos na Resolução

TRE-PI nº 458/2022 que tratam da Política de Desfazimento dos Equipamentos.

Capítulo V

Do controle de acesso lógico

Seção I

Do gerenciamento de acesso lógico

Art. 15. O acesso aos sistemas de informação será assegurado, unicamente, ao usuário devidamente identificado e autorizado.

§ 1º Os gestores dos ativos devem determinar regras apropriadas de controle de acesso, direitos de acesso e restrições para papéis específicos dos usuários, com nível de detalhe e rigor de controle que reflitam os riscos de segurança da informação associados, observada a consistência entre os direitos de acesso e as políticas de classificação da informação.

§ 2º As regras de controle de acesso deverão ser baseadas na premissa de que “tudo é proibido a menos que expressamente permitido”, em lugar da regra “tudo é permitido, a menos que expressamente proibido”.

Art. 16. A concessão e a revogação de acesso serão implementadas por meio de processo formal, preferencialmente automatizado, com estabelecimento de responsáveis pela solicitação, administração, concessão, bloqueio e revogação.

§ 1º Compete aos proprietários de todos os tipos de ativos estabelecer regras de concessão, bloqueio e revogação de acesso aos ativos para os usuários, levando em conta as políticas, princípios e normas de controle de acesso aplicáveis.

§ 2º Os acessos deverão ser retirados imediatamente após a revogação dos direitos ou o encerramento das atividades, contratos ou acordos, ou ajustados após qualquer mudança destas atribuições.

§ 3º As contas deverão ser desabilitadas, em vez de excluídas, para preservação de trilhas de auditoria.

Art. 17. A criação de nomes de usuário e de contas de e-mail seguirá critério padronizado.

Art. 18. O modelo de controle de acesso será, preferencialmente, baseado no controle de acesso baseado em papéis (*RBAC- Role-based access control*), em que as credenciais recebam privilégios de acesso conforme os papéis e as responsabilidades executadas pelos usuários.

Art. 19. Deverá ser estabelecido e mantido atualizado um inventário de todas as contas gerenciadas, contendo data de início e término, incluindo:

I - contas de usuário e de administrador; e

II - contas de serviço.

§ 1º O inventário das contas de usuário e de administrador deverá conter, no mínimo, o nome da pessoa, o nome de usuário e a sua unidade de lotação, enquanto o das contas de serviço indicará ao menos a unidade gestora, as datas de revisão e o propósito.

§ 2º A Seção de Infraestrutura deve revisar as contas de usuário e de administrador trimestralmente para avaliar se permanecem ativas e autorizadas.

Art. 20. A Secretaria de Tecnologia da Informação deverá manter inventário dos sistemas de autenticação do Tribunal, abrangendo os internos e aqueles

hospedados em provedores remotos.

Seção II

Do acesso às redes e aos serviços de rede

Art. 21. A gestão de contas e o controle de acesso se darão de forma centralizada, por meio de serviço de diretório controlado pela unidade responsável pela infraestrutura de serviços de TI.

Art. 22. As operações de criação de usuários da rede local serão solicitadas por meio de instrumento específico, observada a segregação de funções em todo o fluxo do gerenciamento de acesso, pelos seguintes agentes:

I - Secretaria de Gestão de Pessoas: no caso de magistrados, servidores efetivos, ocupantes de cargo em comissão sem vínculo, requisitados e estagiários; e

II - Chefia imediata da unidade de lotação do usuário, no caso de colaboradores terceirizados e prestadores de serviços.

Parágrafo único. Nos demais casos, será necessária a aprovação da Comissão de Segurança da Informação.

Art. 23. A chefia imediata da unidade de lotação do usuário deverá solicitar a atribuição de direitos de acesso aos recursos computacionais do Tribunal, por meio do sistema de Central de Serviços da Secretaria de Tecnologia da Informação, informando os sistemas ou serviços de informação e o perfil de acesso que o usuário deve possuir.

§ 1º O perfil de acesso do usuário aos sistemas ou serviços de informação deve ser mantido restrito ao desempenho de suas atividades.

§ 2º O gestor do ativo de informação será responsável pela autorização do direito de acesso, que poderá ser operacionalizado por equipe técnica designada.

§ 3º Na análise da solicitação de acesso, o gestor do ativo deverá considerar também a consistência entre a classificação da informação e os direitos de acesso, bem como as normas e legislação vigentes.

§ 4º Estas autorizações devem estar documentadas, para fins de auditoria e levantamento periódico, visando à detecção de usuários com acesso indevido.

§ 5º Deverá ser estabelecido um perfil padrão para usuários, ao qual todos retornarão em caso de mudança de lotação ou qualquer outro motivo que leve à suspensão de suas atividades, antes que sejam solicitados novos perfis de acesso pela nova chefia.

§ 6º A lotação de um usuário em uma unidade permite acesso à área específica de armazenamento de arquivos da unidade, bem como o recebimento de mensagens para o e-mail da mesma.

§ 7º Caso existam mensagens ou arquivos para os quais nem todos tenham acesso, deve-se criar grupo de distribuição de mensagens ou de permissão de acesso distinto do padrão da unidade;

§ 8º O procedimento de atribuição de acesso deve ser efetivado somente após a autorização formal ser finalizada.

§ 9º O gestor de cada Unidade terá gerência e responsabilidade pela autorização do direito de acesso.

Art. 24. Os usuários devem possuir identificação única e exclusiva para permitir relacioná-la às suas ações e responsabilidades.

Parágrafo único. O uso compartilhado de identificação de usuários somente será permitido por razões operacionais, mediante procedimento de atribuição de responsabilidades compartilhado pelas chefias imediatas e autorização do Diretor Geral.

Art. 25. Compete à chefia imediata informar à STI, a movimentação e o desligamento de qualquer usuário alocado em sua unidade, dadas as implicações na manutenção de direitos de acesso aos ativos de informação.

§ 1º A STI deverá comunicar ao gestor do ativo a movimentação e o desligamento do usuário citado no *caput* a fim de obter autorização para modificação de direitos de acesso aos ativos de informação.

§ 2º A retirada do usuário dos acessos citados no art. 23 somente se dará após a mudança de lotação ou desligamento efetuado no sistema de gestão de recursos humanos.

§ 3º Periodicamente, a área de Tecnologia da Informação fará o bloqueio automático das credenciais de acesso dos usuários que não realizaram o acesso por mais de 45 (quarenta e cinco) dias, incluídos os servidores aposentados, cedidos e licenciados.

§ 4º É vedado aos usuários utilizarem a identificação fornecida pelo Tribunal para cadastro em serviços oferecidos por provedores externos, que não tenham sido adotados ou homologados pelo Tribunal, devendo em qualquer situação ser evitada a utilização da mesma senha nesses serviços.

Art. 26. Os direitos de acesso dos usuários devem ser revistos em intervalos regulares, bem como após qualquer mudança de nível institucional que implique em realocação de pessoas, unidades ou papéis.

Art. 27. As atividades de gerenciamento de identidades, acesso e autenticação devem ser registradas e arquivadas.

Parágrafo único. Deverão ser emitidos, frequentemente, relatórios críticos com finalidade de identificar inconsistências nestas atividades, atentando-se às recomendações anteriores bem como para as seguintes:

I - Identificação de forma periódica de usuários redundantes; e

II - Identificação de solicitações de acesso sem segregação de funções.

Art. 28. Devem ser incluídas cláusulas nos contratos de prestadores de serviço elencando sanções nos casos de acesso não autorizado, ou mesmo tentativa, efetuado por pessoa ou agente, mediante ações diretas ou indiretas dos seus colaboradores.

Art. 29. Compete ao Gestor de ativo realizar a revisão de direitos de acesso ao ativo sob sua responsabilidade, podendo a Secretaria de Tecnologia da Informação automatizar o processo de retirada de acessos e alteração de perfil para usuários, nos casos previstos nos arts. 25 e 26, conforme as regras estabelecidas formalmente.

Art. 30. Os dispositivos e serviços de rede, bem como as demais aplicações do Tribunal devem ser configurados mediante regra “tudo é proibido a não ser que expressamente permitido”.

Art. 31. O acesso de novo equipamento à rede é regulamentado pelo

procedimento de autorização específico e deverá ser executado através da abertura de chamado de requisição de serviço na Central de Serviços de TI.

Art. 32. São consideradas redes do TRE-PI, para efeito de controle, a rede cabeada da sede e seus anexos, todas as redes sem fio em suas dependências e por ele provida, o acesso VPN, o perímetro para a Internet e as redes das zonas eleitorais.

Art. 33. É vedada a inclusão de equipamentos pessoais ou de terceiros em qualquer uma das redes internas do TRE-PI, sem autorização do Secretário de Tecnologia da Informação.

Art. 34. A inclusão de equipamentos de terceiros na rede será efetuada em sub-rede segura, distinta das demais e por período definido.

Art. 35. O horário de funcionamento da VPN e do acesso à INTERNET será regulamentado em portaria específica.

Parágrafo único: As situações excepcionais que ensejarem a modificação do horário estabelecido deverão ser submetidas à autorização da Diretoria-Geral.

Art. 36. A inclusão de equipamentos e usuários na VPN será solicitada à Secretaria de Tecnologia da Informação, em formulário específico, registrado em processo SEI.

Art. 37. Os acessos à rede devem ser registrados, arquivados por um período mínimo de 6 (seis) meses, monitorados e frequentemente deve ser emitido relatório crítico com finalidade de identificar acessos indevidos.

Art. 38. Será exigido múltiplo fator de autenticação nas máquinas que acessarem a VPN do TRE-PI.

Art. 39. A conta de usuário terá permissão de uso da rede do TRE-PI suspensa quando ocorrer uma das condições a seguir:

I - quando o usuário ativo não estiver em atividade no Tribunal, por prazo igual ou superior a 30 (trinta) dias consecutivos, em função de licenças e afastamentos;

II - quando servidor ativo estiver em afastamento preventivo do exercício do cargo em decorrência do disposto no art. 147 da Lei nº 8.112, de 1990;

III - em casos de suspeita de infração das normas de segurança da informação.

Art. 40. Os serviços de rede que não estejam em uso devem ser removidos e não apenas desabilitados.

Seção III

Do acesso privilegiado

Art. 41. O acesso privilegiado aos sistemas e ativos de informação somente será concedido aos usuários que tenham como atribuição funcional o dever de administrá-los.

§ 1º O acesso privilegiado deve ser concedido ao usuário por meio de credenciais de acesso exclusivas para este fim, distintas das credenciais de acesso concedidas a tal usuário para a realização de suas atividades normais de negócio.

§ 2º O procedimento de concessão de acesso privilegiado deve manter arquivo de registro contendo informações sobre este pedido para posterior auditoria.

§ 3º A relação de usuários que detenham acesso privilegiado deve ser revista pelo Gestor do ativo de informação em intervalos não superiores a 30 (trinta) dias.

§ 4º O Gestor do ativo de informação deve definir prazos de expiração para as credenciais de acesso privilegiado, após os quais deve ser reavaliado o atendimento aos critérios para a atribuição de acesso privilegiado ao detentor das credenciais expiradas.

§ 5º Na ausência de prazo de expiração definido pelo Gestor do Ativo a STI está autorizada a estabelecer o período de 30 (trinta) dias como padrão.

§ 6º Caso algum ativo de informação, em função de suas características técnicas, exija a manutenção de credenciais de acesso privilegiado de uso compartilhado, o Gestor do ativo deve definir procedimentos específicos para evitar seu uso não autorizado.

§ 7º A solicitação de acesso privilegiado para qualquer unidade que não seja gestora do ativo deverá ser encaminhada através de processo administrativo ao Secretário de Tecnologia da Informação para manifestação e posterior submissão ao Diretor Geral, para análise e autorização.

Art. 42. As competências dos usuários com acesso privilegiado aos sistemas e ativos de informação deverão ser avaliadas periodicamente para que estejam alinhadas às atividades e obedecendo as regras de segregação de funções.

Art. 43. O acesso privilegiado aos sistemas e ativos de informação através do uso de ID de usuário administrador genérico deve ser evitado, se o sistema assim permitir e, quando não houver esta possibilidade, deve ser concedido mediante procedimentos de troca periódica de senha e auditoria dos acessos.

§ 1º Após a saída ou mudança de lotação de usuário com conhecimento de senha de usuário administrador genérico, esta deve ser modificada.

§ 2º A conta de administrador genérico deve ser renomeada e ter sua função apagada, para que não possa ser facilmente identificada.

§ 3º A conta de administrador genérico não deve ser usada para acesso à Internet, iniciar serviços de rede e acessar arquivos externos.

Seção IV

Da política de senhas

Art. 44. Os sistemas ou serviços de informação, considerados passíveis de controle de acesso pelo Gestor de ativo, devem ter seu acesso restrito e controlado através do uso de senhas, *token* ou mecanismo de autenticação similar.

§ 1º Serão concedidas senhas temporárias, mediante concordância e assinatura de termo de confidencialidade de toda senha, ou outro mecanismo de autenticação que estiver em sua posse.

§ 2º O acesso remoto à rede, o acesso administrativo e o acesso a aplicações expostas externamente se darão por autenticação multifatorial (MFA).

§ 3º A Secretaria de Tecnologia da Informação, em conjunto com o Gestor do ativo de informação, podem implantar a autenticação de multifatores para determinados tipos de acesso, em função de sua criticidade.

Art. 45. A senha de acesso do usuário, *tokens,* e outros fatores de autenticação devem ser de uso pessoal e intransferível.

§ 1º O usuário é responsável por garantir a confidencialidade de suas credenciais de acesso, sendo sua obrigação garantir o seu sigilo.

§ 2º Cada usuário deve possuir uma única credencial de acesso à rede do TRE-PI, exceto nos casos excepcionais autorizados pela Secretaria de Tecnologia da Informação.

Art. 46. As senhas devem ser secretas e definidas considerando as seguintes recomendações:

I - utilizar números, letras, alternando-as entre maiúsculas, minúsculas e caracteres especiais, como $@#&%, com, no mínimo 12 (doze) caracteres para todas as contas, inclusive as que utilizam autenticação de multifatores;

Unifica e define para 12 caracteres

II - não utilizar frases ou palavras que possam ser facilmente adivinhadas por terceiros, baseadas nas informações relativas ao próprio usuário, tais como nome de parentes, datas de aniversário e números de telefone. Não usar palavras contidas no dicionário;

III - 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, ou ainda caracteres idênticos repetidos;

IV - não utilizar as mesmas credenciais (nome de usuário e senha) para fins pessoais (em serviços externos ao ambiente de TI da Justiça Eleitoral e profissionais;

V - modificar a senha temporária no primeiro *logon*; e

VI - não expor a senha em local visível para terceiros, como anotações em papéis, sob pena de responsabilização pelos acessos indevidos;

Parágrafo único: A STI deverá regularmente revisar as recomendações supracitadas de modo a configurá-las de forma a garantir a segurança dos serviços de tecnologia da informação.

Art. 47. Sempre que houver indicação de possível comprometimento da senha, o usuário deve realizar sua alteração, bem como comunicar a ocorrência ou a suspeita de comprometimento à Central de Serviços de TI por meio de chamado registrado.

Parágrafo único - A unidade responsável pela gerência de acessos ou da política de senhas está autorizada a realizar o bloqueio de acesso, preventivamente, caso identifique suspeita de comprometimento de senha do usuário.

Art. 48. O sistema de gerenciamento de senha deve:

I - permitir que os usuários selecionem e modifiquem suas próprias senhas, incluindo um procedimento de confirmação para evitar erros;

II - forçar as mudanças de senha a intervalos regulares de, no máximo, 6 (seis) meses, conforme necessidade;

III - manter um registro das senhas anteriores utilizadas e bloquear a reutilização;

IV - empregar criptografia no canal de comunicação utilizado para o tráfego de credenciais de acesso;

V - criptografar ou embaralhar (*hash*) com *salt* as credenciais de

autenticação armazenadas;

VI - não mostrar as senhas na tela quando forem digitadas;

VII - garantir a modificação das senhas temporárias no primeiro acesso ao sistema ou serviço de informação;

VIII - manter, para fins de auditoria, registro dos acessos, das operações e dos respectivos períodos;

IX - desabilitar as contas que não possam ser associadas a um usuário ou processo de negócio; e

X - monitorar tentativas de acesso a contas desativadas.

Art. 49. A senha temporária, para primeiro acesso ou no caso de o usuário esquecer a sua senha, deverá ser emitida através de procedimento instruído pela unidade técnica responsável pelo gerenciamento dos serviços de infraestrutura de tecnologia da informação e aprovado pela Comissão de Segurança da Informação, no qual deverá informar dados pessoais para confirmação de identidade.

Parágrafo único. 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 serviço de correio eletrônico não adotado pelo TRE-PI.

Art. 50. Toda e qualquer senha utilizada para autenticar sistema da Justiça Eleitoral não deverá ser utilizada em sistema externo.

Seção V

Dos procedimentos seguros de entrada no sistema

Art. 51. 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 um usuário não autorizado;

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

III - no 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, 5 (cinco) 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 desde o último acesso com sucesso;

VII - não mostrar a senha que está sendo informada;

VIII - não transmitir senhas em texto claro pela rede;

IX - encerrar sessões inativas após um período definido de inatividade de, no máximo, 10 (dez) minutos; e

X - em caso de uso externo, deve restringir o tempo de conexão para reduzir oportunidade de acesso não autorizado.

Seção VI

Do controle de acesso ao código-fonte de programas

Art. 52. O código-fonte e itens associados (esquemas, especificações, planos de validação etc) dos sistemas de informação desenvolvidos pelo Tribunal somente serão acessíveis pelos usuários que tenham como atribuição funcional seu desenvolvimento, manutenção ou outra atividade para a qual o acesso seja imprescindível.

§ 1º As bibliotecas de código-fonte e itens associados devem ser armazenadas em ferramentas apropriadas para este fim, em ambientes segregados dos sistemas operacionais onde os respectivos sistemas de informação sejam executados.

§ 2º Os eventos de acesso às bibliotecas de código-fonte e itens associados devem ser registrados, permitindo sua auditoria.

§ 3º Os códigos-fonte que sejam publicados para entidades externas devem contar com controles adicionais que garantam sua integridade.

Capítulo VI

Das disposições finais

Art. 53. Os casos omissos serão resolvidos pela Comissão de Segurança da Informação deste Tribunal.

Art. 54. A revisão desta Norma de Gestão de Identidade e Controle de Acesso Físico e Lógico relativos à Segurança da Informação ocorrerá sempre que se fizer necessário ou conveniente para este Tribunal, não excedendo o período de 3 (três) anos.

Art. 55. Esta Política deve ser publicada no portal de intranet do Tribunal pela Comissão de Segurança da Informação.

Art. 56. O descumprimento desta norma será objeto de apuração pela unidade competente do Tribunal, com a consequente aplicação das penalidades cabíveis a cada caso.

Art. 57. Esta Portaria entra em vigor na data de sua publicação e sua implementação inicia-se imediatamente.

Desembargador JOSÉ JAMES GOMES PEREIRA

Presidente do TRE-PI, em exercício

Documento assinado eletronicamente por **José James Gomes Pereira**, **Presidente, em exercício**, em 07/08/2023, às 08:21, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site https://sei.tre-pi.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **0001889763** e o código CRC **905F0A96**.


2022
PRÊMIO
CNJ DE
QUALIDADE
Prata