Nacional de Justiça - SCA. CIENTIFIQUE-SE. PUBLIQUE-SE. CUMPRA-SE. Fortaleza, 6 de fevereiro de 2023.
Desembargador INACIO DE ALENCAR CORTEZ NETO
PRESIDENTE

PORTARIA Nº 151/2023 - SEGURANÇA DA INFORMAÇÃO

Institui regras para a Gestão de Identidade e o Controle de Acesso Físico e Lógico ao ambiente cibernético do Tribunal Regional Eleitoral do Ceará
O PRESIDENTE DO TRIBUNAL REGIONAL ELEITORAL DO CEARÁ no uso das atribuições que lhe confere o artigo 23, inciso LX, do Regimento Interno deste Tribunal,
CONSIDERANDO o que dispõe os artigos 7 e 9 da Res. TRE/CE n.º 920/2022, e
CONSIDERANDO o disposto no Processo Administrativo Digital SEI n.º 2022.0.000004655-9,
CONSIDERANDO à Resolução TRE nº 793/2020, que dispõe sobre o Planejamento Estratégico da Justiça Eleitoral do Ceará,
CONSIDERANDO à Resolução TRE nº 618/2016,, que regulamenta a aplicação, no âmbito do Tribunal Regional Eleitoral do Ceará, da Lei nº 12.527, de 18 de novembro de 2011, que versa sobre o acesso à informação,
CONSIDERANDO à Portaria TRE-CE nº 784/2021, que insitui o Plano de Logística Sustentável da Justiça Eleitoral do Ceará,
CONSIDERANDO a Res. CNJ 396/2021, que institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ);
CONSIDERANDO a Res. TSE 23.644/2021, que institui a Política de Segurança da Informação (PSI) no âmbito da Justiça Eleitoral.
CONSIDERANDO a portaria DG/TSE 444/2021, que dispõe sobre a instituição da norma de termos e definições relativa à Política de Segurança da Informação do Tribunal Superior Eleitoral.
CONSIDERANDO as boas práticas em segurança da informação previstas nas normas ABNT ISO /IEC 27001 e ABNT NBR ISO/IEC 27002.
CONSIDERANDO as boas práticas em segurança da informação previstas no modelo CIS Controls V.8.
CONSIDERANDO a necessidade de implementar controles para o tratamento de dados pessoais, de acordo com a lei 13.709/2018 (LGPD);
CONSIDERANDO as diretivas da lei nº 12.527, de 18 de novembro de 2011, que regula o acesso à informações;
CONSIDERANDO a Res. TRE-CE NN/2022, que institui a Política de Segurança da Informação (PSI) no âmbito da Justiça Eleitoral do Ceará.
CONSIDERANDO a lei nº 12.527, de 18 de novembro de 2011, que regula o acesso a informações previsto no inciso XXXIII do art. 5º , no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal;
CONSIDERANDO que a segurança da informação e a proteção de dados pessoais são condições essenciais para a prestação dos serviços jurisdicionais e administrativos do Tribunal Regional Eleitoral do Ceará;
RESOLVE:
CAPÍTULO I
DAS DISPOSIÇÕES GERAIS
INSTITUIÇÃO E ALINHAMENTO DA NORMA COM NORMA DO TSE
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 Ceará.

Art. 2º Esta norma integra a Política de Segurança da Informação da Justiça Eleitoral, estabelecida pela Resolução TSE n. 23.644/2021.

CAPÍTULO II

DOS CONCEITOS E DEFINIÇÕES

ALINHAMENTO COM GLOSSÁRIOS UTILIZADOS

Art. 3º Para efeitos desta norma, consideram-se os termos e definições previstos na Portaria DG /TSE n. 444/2021, aplicando-se, de forma subsidiária, aqueles estabelecidos no Glossário de Segurança da Informação do Gabinete de Segurança Institucional da Presidência da República.

CAPÍTULO III

DOS PRINCÍPIOS

(IMPORTÂNCIA DOS PRINCÍPIOS E ORIENTAÇÃO PARA INTERPRETAÇÃO DA NORMA)

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, 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 IV

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 todos os magistrados, servidores efetivos e requisitados, ocupantes de cargo em comissão sem vínculo efetivo, estagiários, prestadores de serviço, colaboradores e usuários 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 e comunicação, de acordo com os preceitos estabelecidos neste normativo.

CAPÍTULO V

DO CONTROLE DE ACESSO FÍSICO

SEÇÃO I

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 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 autenticação de multifator, 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 e janelas acessíveis;

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

DOS EQUIPAMENTOS DE PROCESSAMENTO E ARMAZENAMENTO

Art. 10. Para evitar perdas, danos, furtos ou comprometimento de ativos e interrupção das operações da organização, o Tribunal deve observar 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 a(s) equipe(s) responsáveis pelos ativos instalados nos *racks* tenham acesso físico a eles.

SEÇÃO III

DA SEGURANÇA DO CABEAMENTO

Art. 11. 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. 12. 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.

SEÇÃO V

DA REUTILIZAÇÃO OU DESCARTE SEGURO DOS EQUIPAMENTOS OU DOS EQUIPAMENTOS EM PROVA DE CONCEITO

Art. 13. 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.

Parágrafo único. 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.

CAPÍTULO VI

DO CONTROLE DE ACESSO LÓGICO

SEÇÃO I

Art. 14. 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 terem acesso aos ativos, 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. 15. 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.

§ 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 de atribuições.

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

Art. 16. A criação de nomes de usuário e de contas de e-mail seguirá critério padronizado.

Art. 17. O modelo de controle de acesso será, preferencialmente fundamentado no controle de acesso baseado em papéis (RBAC), em que as credenciais recebam os privilégios de acesso conforme os papéis e as responsabilidades executadas pelos usuários;

Art. 18. 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 As contas deverão ser revisadas trimestralmente, pela unidade responsável, para avaliar se as contas ativas permanecem autorizadas.
§ 3º Ficará a cargo da Coordenadoria de Infraestrutura - COINT, através de sua seção de Cibersegurança - CIBER, o gerenciamento operecional.
Art. 19. 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, SISTEMAS INTERNOS E SERVIÇOS DE REDE
Art. 20. A gestão de contas internas e o controle de acesso se darão de forma centralizada, por meio de serviço de diretório pela Coordenadoria de Infraestrutura - COINT, através de sua seção de Cibersegurança - CIBER.
Art. 21. 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, chefia imediata da unidade de lotação do usuário ou ainda coordenadoria, secretaria ou assessoria a qual a unidade pertence, no caso de magistrados, servidores efetivos e requisitados, ocupantes de cargo em comissão sem vínculo efetivo e estagiários; e
II - Chefia imediata da unidade de lotação do usuário, no caso de colaboradores e prestadores de serviços.
Parágrafo único. Nos demais casos, será necessária a aprovação da Comissão de Segurança da Informação.
Art. 22. 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 *service desk* 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 não deve permitir que a permissão seja efetivada antes que a autorização formal seja finalizada.

§ 9º O gestor de cada unidade (Secretária, Coordenadoria, Assessoria ou Seção) terá gerência e responabilidade pela autorização do direito de acesso.

Art. 23. 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 da Comissão de Segurança da Informação.

Art. 24. Compete à chefia imediata informar aos gestores do ativo 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 retirada do usuário dos acessos citados no art. 22 somente se dará após a mudança de lotação ou desligamento efetuado no sistema de gestão de recursos humanos.

§ 2º 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.

Art. 25. 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. 26. 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:

a) Identificação de forma periódica de usuários redundantes;

b) Identificação de solicitações de acesso sem segregação de funções.

Art. 27. 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. 28. 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. 24 e 25, conforme as regras estabelecidas formalmente.

SEÇÃO III

DO ACESSO PRIVILEGIADO

Art. 29. 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 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.
§ 4º A solicitação de acesso privilegiado para qualquer unidade que não seja gestora do ativo deverá ser encaminhada através de processo administrativo ao Presidente da Comissão de Segurança da Informação, para análise e autorização.
Art. 30. As competências dos usuários com acesso privilegiado aos sistemas e ativos de informação deverão ser avaliadas em intervalos não superiores a um mês, para que estejam alinhadas às atividades e obedecendo as regras de segregação de funções.
Art. 31. 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, criados pelo gestor do ativo.
§ 1º Após a saída ou mudança de lotação de usuário com conhecimento de senha de usuário administrador genérico, esta deve ser modificada.
§ 2 º A conta de administrador genérico deve ser renomeada e ter sua função apagada, para que não possa ser facilmente identificada.
§ 3 º 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. 32. 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. 33. A senha de acesso do usuário, *tokens,* e outros fatores de autenticação devem ser de uso pessoal e intransferível.
Art. 34. 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, 8 (oito) caracteres para contas com autenticação;
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.
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 - Modificar a senha temporária no primeiro logon;
§ 1º Não expor a senha em local visível para terceiros, como anotações em papéis, sob pena de responsabilização pelos acessos indevidos.
Art. 35. 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.

Art. 36. 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 ao *service desk* da Secretaria de Tecnologia da Informação.

Art. 37. 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 - Recomendar ou 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;

X - Monitorar tentativas de acesso a contas desativadas.

Art. 38. 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 de Segurança 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 correio de terceiro.

SEÇÃO V

DOS PROCEDIMENTOS SEGUROS DE ENTRADA NO SISTEMA

Art. 39. 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 - Encerrar sessões inativas após um período definido de inatividade de, no máximo, 10 (dez) minutos; e

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

IX - Sempre que possível, prioridade de login através de certificado digital.

SEÇÃO VI

DO ACESSO DOS EQUIPAMENTOS À REDE E AOS SERVIÇOS DE REDE

Art. 40. 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. 41. 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 em sistema de *service desk*;

Art. 42. São consideradas redes do Tribunal Regional Eleitoral do Ceará, para efeito de controle, a rede cabeada da sede e seus anexos, todas as redes wifi em suas dependências e por ele provida, o acesso VPN, o perímetro para a Internet e as redes das zonas eleitorais.

Art. 43. É vedada a inclusão de equipamentos pessoais ou de terceiros em qualquer uma das redes internas do TRE, sem autorização do Presidente da Comissão de Segurança da Informação.

Art. 44. A inclusão de equipamentos de terceiros na rede será efetuada em subrede segura, distinta das demais e por período definido.

Art. 45. O horário de funcionamento da VPN e do acesso à INTERNET será regulamentado em portaria interna e qualquer alteração excepcional deverá ser solicitada à Comissão de Segurança da Informação.

Art. 46. A inclusão de equipamentos e usuários na VPN será solicitada através de sistema *service desk*, em formulário específico.

Art. 47. Os acessos à rede devem ser registrados, arquivados por um período mínimo de 6 meses, monitorados e frequentemente deve ser emitido relatório crítico com finalidade de identificar acessos indevidos.

Art. 48. Será exigido múltiplo fator de autenticação nas máquinas que acessarem a VPN do Tribunal Regional Eleitoral do Ceará.

Art. 49. Os serviços de rede que não estejam em uso devem ser removidos e não apenas desabilitados.

SEÇÃO VII

DO CONTROLE DE ACESSO AO CÓDIGO-FONTE DE PROGRAMAS

Art. 50. 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 VII

DISPOSIÇÕES FINAIS

Art. 51. Os casos omissos serão resolvidos pela Comissão de Segurança da Informação deste Tribunal.

Art. 52. Esta norma complementar deve ser revisada a cada 12 meses pelo Gestor de Segurança da Informação e encaminhada para nova apreciação do Comitê Gestor de Segurança da Informação.

Art. 53. O descumprimento desta norma será objeto de apuração pela unidade competente do Tribunal, com a consequente aplicação das penalidades cabíveis a cada caso.

Art. 54. Esta Portaria entra em vigor na data de sua publicação e sua implementação inicia-se imediatamente.

ANEXO I

REFERÊNCIAS NORMATIVAS

- Lei n. 8.112, de 11 de dezembro de 1990, que dispõe sobre o regime jurídico dos servidores públicos civis da União, das autarquias e das fundações públicas federais;
- Lei n. 8.159, de 8 de janeiro de 1991, que dispõe sobre a Política Nacional de Arquivos Públicos e Privados e dá outras providências;
- Lei n. 9.983, de 14 de julho de 2000, que dispõe sobre a responsabilidade administrativa, civil e criminal de usuários que cometam irregularidades em razão do acesso a dados, informações e sistemas informatizados da Administração Pública;
- Lei n. 12.527, de 18 de novembro de 2011, que regula o acesso a informações previsto na Constituição Federal;
- Lei n. 12.965, de 23 de abril de 2014 (Marco Civil da Internet), que estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil;
- Lei n. 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais), que dispõe sobre o tratamento de dados pessoais;
- Decreto n. 5.482, de 30 de junho de 2005, que dispõe sobre a divulgação de dados e informações pelos órgãos e entidades da administração pública federal, por meio da Rede Mundial de Computadores (Internet);
- Decreto n. 7.845, de 14 de novembro de 2021, que regulamenta procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo, e dispõe sobre o Núcleo de Segurança e Credenciamento;
- Decreto n. 9.637, de 26 de dezembro de 2018, que institui a Política Nacional de Segurança da Informação e dispõe sobre a governança de segurança da informação;
- Resolução CNJ n. 370, de 28 de janeiro de 2021, que estabelece a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD);
- Resolução CNJ n. 396/2021, que instituiu a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ);
- Resolução n. 23.644, de 1º de julho de 2021, do Tribunal Superior Eleitoral, que dispõe sobre a Política de Segurança da Informação (PSI) no âmbito da Justiça Eleitoral;
- Resolução n. 23.650, de 9 de setembro de 2021, do Tribunal Superior Eleitoral, que institui a Política Geral de Privacidade e Proteção de Dados Pessoais no âmbito da Justiça Eleitoral;
- Resolução n. 601 de 21 de outubro de 2015, que institui o Código de ética dos servidores do Tribunal Regional Eleitoral do Ceará.
- Norma ABNT NBR/ISO/IEC 27002:2013, que institui o código de melhores práticas para controles de segurança da informação;
- Norma ABNT NBR/ISO/IEC 27001:2013, que estabelece requisitos para sistemas de gestão da segurança da informação;
- Norma ABNT NBR ISO/IEC 27005:2019, que fornece as diretrizes para a gestão de riscos de segurança da informação;
- Norma ABNT NBR ISO/IEC 27701:2019, que trata da gestão da privacidade da informação;
- Instrução Normativa nº 01 GSI/PR/2008, 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.

CIENTIFIQUE-SE, PUBLIQUE-SE E CUMPRA-SE.

Fortaleza, 6 de fevereiro de 2023.
DESEMBARGADOR INACIO DE ALENCAR CORTEZ NETO
PRESIDENTE

PORTARIA TRE/CE N.º 61/2023

(SEI nº 2023.0.000000044-0)
O PRESIDENTE DO TRIBUNAL REGIONAL ELEITORAL DO CEARÁ, no uso das atribuições que lhe são conferidas pelo artigo 23, XXVI, do Regimento Interno deste Tribunal,
CONSIDERANDO a Resolução TRE-CE nº 806, de 23 de abril de 2021, que institui o Sistema Eletrônico de Informações - SEI - como sistema oficial de gestão de processos administrativos eletrônicos no âmbito da Justiça Eleitoral do Ceará.
RESOLVE, *ad referendum* deste Tribunal:
Art. 1° Estabelecer o dia 31/3/2023 como data limite para tratamento dos processos ativos no sistema de Processo Administrativo Digital - PAD, devendo estes ser arquivados no referido sistema ou, no caso de haver providências pendentes, migrados para o Sistema Eletrônico de Informações - SEI.
Art. 2º Esta Portaria entra em vigor na data de sua publicação.
CIENTIFIQUE-SE, PUBLIQUE-SE E CUMPRA-SE.
Fortaleza-CE, 18 de janeiro de 2023.
Desembargador INACIO DE ALENCAR CORTEZ NETO
Presidente

PORTARIA Nº 149/2023 - SEGURANÇA DA INFORMAÇÃO

Dispõe sobre a instituição da Norma de Gestão de Ativos relativa à Política de Segurança da Informação do Tribunal Regional Eleitoral de Ceará.
O PRESIDENTE DO TRIBUNAL REGIONAL ELEITORAL DO CEARÁ no uso das atribuições que lhe confere o artigo 23, inciso LX, do Regimento Interno deste Tribunal,
CONSIDERANDO o que dispõe os artigos 7 e 9 da Res. TRE/CE n.º 920/2022, e
CONSIDERANDO o disposto no Processo Administrativo Digital SEI n.º 2022.0.000003576-0,
CONSIDERANDO à Resolução TRE nº 793/2020, que dispõe sobre o Planejamento Estratégico da Justiça Eleitoral do Ceará,
CONSIDERANDO à Resolução TRE nº 618/2016,, que regulamenta a aplicação, no âmbito do Tribunal Regional Eleitoral do Ceará, da Lei nº 12.527, de 18 de novembro de 2011, que versa sobre o acesso à informação,
CONSIDERANDO a Res. CNJ 396/2021, que institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ);
CONSIDERANDO a Res. TSE 23.644/2021, que institui a Política de Segurança da Informação (PSI) no âmbito da Justiça Eleitoral.
CONSIDERANDO a portaria DG/TSE 444/2021, que dispõe sobre a instituição da norma de termos e definições relativa à Política de Segurança da Informação do Tribunal Superior Eleitoral.
CONSIDERANDO as boas práticas em segurança da informação previstas nas normas ABNT ISO /IEC 27001 e ABNT NBR ISO/IEC 27002.
CONSIDERANDO as boas práticas em segurança da informação previstas no modelo CIS Controls V.8.
CONSIDERANDO a necessidade de implementar controles para o tratamento de dados pessoais, de acordo com a lei 13.709/2018 (LGPD);
CONSIDERANDO as diretivas da lei nº 12.527, de 18 de novembro de 2011, que regula o acesso à informações;