Art. 15. Cabe ao usuário:
I - Zelar pela segurança do certificado digital recebido, não compartilhando o seu uso e a sua senha com terceiros;
II - Assinar termo de compromisso no ato do recebimento de certificado digital;
III - Informar imediatamente à SECTI em caso de extravio ou comprometimento do certificado digital para adoção das providências de revogação;
IV - O usuário deve estar ciente de que a assinatura ou login realizados por meio de certificado digital são irretratáveis, não podendo alegar que não efetuou a ação.
CAPÍTULO VIII
DISPOSIÇÕES FINAIS
Art. 16. No caso de algum equipamento, aplicação, aplicativo, sistema ou banco de dados não permitir a adoção de protocolos seguros, a informação deverá constar em documento de análise de riscos de segurança da informação, sendo imediatamente submetido à apreciação do CGSIPDP.
Art. 17. Os casos omissos serão resolvidos pelo CGSIPDP.
Art. 18. A SECTI elaborará, em até 1 (um) ano a partir da publicação desta norma, os procedimentos operacionais para sua aplicação, que levem em conta as boas práticas de cibersegurança e os recursos tecnológicos disponíveis.
Art. 19. Qualquer descumprimento desta norma deve ser imediatamente comunicado e registrado pelo Gestor de Segurança da Informação, com consequente adoção das providências cabíveis.
Art. 20. Esta norma será revisada sempre que se fizer necessário.
Art. 21. No prazo de 1 (um) ano a partir da publicação desta norma, a SECTI deverá informar ao Gestor de Segurança da Informação quais ativos de informação não poderão se adequar às regras previstas nesta instrução normativa.
Art. 22. Esta instrução normativa entrará em vigor na data de sua publicação.
Curitiba, 28 de maio de 2025.
SOLANGE MARIA VIEIRA
Diretora-Geral

INSTRUÇÃO NORMATIVA Nº 04/2025

Institui norma de Gestão de Identidade e Controle de Acesso Lógico e Físico ao ambiente de TI no âmbito da Justiça Eleitoral do Paraná.
A DIRETORA-GERAL DO TRIBUNAL REGIONAL ELEITORAL DO PARANÁ, no uso das atribuições que lhe são conferidas pelo art. 43, inc. VII, do Regulamento da Secretaria deste Tribunal;
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 que o acesso à informação, assim como aos recursos de processamento das informações e aos processos de negócios, devem ser controlados com base nos requisitos de negócio e da segurança da informação;
CONSIDERANDO a Resolução CNJ nº 370, de 28/01/2021, que estabelece a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD);
CONSIDERANDO a Resolução CNJ nº 396, de 07/06/2021, que institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ);
CONSIDERANDO a Resolução TSE nº 23.644, de 1º/07/2021, que institui a Política de Segurança da Informação (PSI) no âmbito da Justiça Eleitoral;

CONSIDERANDO a Resolução TRE nº 940 de 04/11/2024, que institui o Código de Ética e Integridade no âmbito da Justiça Eleitoral do Paraná, e dá outras providências;
CONSIDERANDO a Instrução Normativa nº 01 GSI/PR/2008, de 13/06/2008, 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;
CONSIDERANDO a Norma Complementar nº 07/IN01/DSIC/GSIPR, de 15/07/2014, que estabelece 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 e privacidade previstas nas normas: ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002, ABNT NBR ISO/IEC 27701; ABNT NBR/ISO/IEC 27002:2013, ABNT NBR/ISO/IEC 27001:2013, ABNT NBR ISO/IEC 27005: 2019, ABNT NBR ISO/IEC 27701:2019;
CONSIDERANDO as recomendações do Acórdão TCU 1.603/2008-Plenário, item 9.1.3, no sentido de normatizar os procedimentos de controle de acesso;
CONSIDERANDO o contido no Processo SEI nº 0001692-66.2025.6.16.8000,
RESOLVE:
CAPÍTULO I
DISPOSIÇÕES PRELIMINARES
Art. 1º Fica instituída norma de Gestão de Identidade e Controle de Acesso Lógico e Físico ao ambiente de Tecnologia da Informação (TI), relativa à segurança da informação e comunicação, no âmbito da Justiça Eleitoral do Paraná.
Art. 2º Esta norma observa a Política de Segurança da Informação da Justiça Eleitoral, estabelecida pela Resolução TSE nº 23.644/2021.
CAPÍTULO II
DOS CONCEITOS E DEFINIÇÕES
Art. 3º Para efeitos desta instrução normativa, consideram-se os termos e definições previstos no Anexo Único.
CAPÍTULO III
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 de TI 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 São objetivos da presente instrução normativa:
I - Estabelecer diretrizes para implantação de controles de acesso físico e lógico ao ambiente de TI; e
II - Assegurar a confidencialidade, integridade e disponibilidade dos ativos de TI 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 TI no âmbito da Justiça Eleitoral do Paraná.

§ 1º Os contratos celebrados pelo Tribunal deverão observar as regras previstas nesta instrução normativa.

§ 2º Os destinatários 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 O Comitê Gestor de Segurança da Informação e Proteção de Dados Pessoais (CGSIPDP) 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 dotadas de 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 (SECTI), 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 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 pelo CGSIPDP, observadas as legislações vigentes.

Seção II

Dos equipamentos de processamento e armazenamento

Art. 10. Para evitar perdas, danos, furtos ou comprometimento de ativos de TI 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, e
IV - utilizar, sempre que possível, racks que disponham de fechaduras com chave ou mecanismo semelhante, garantindo que apenas a(s) equipe(s) responsável(is) 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 sobre gravadas por meio de técnicas que tornem as informações originais irrecuperáveis.

CAPÍTULO VI

DO CONTROLE DE ACESSO LÓGICO

Seção I

Do gerenciamento de acesso lógico

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 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.

§ 2º 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 critérios padronizados.

Art. 17. O modelo de controle de acesso será, preferencialmente fundamentado no controle de acesso baseado em papéis (RBAC).

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.

Art. 19. A SECTI 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 sistema de gestão de identidade.

Art. 21. A criação de usuários da rede local será realizada automaticamente a partir de fontes autoritativas, observada a segregação de funções em todo o fluxo do gerenciamento de acesso, mantidas pelos seguintes agentes:

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

II - Secretaria de Administração (SECAD), no caso de colaboradores e prestadores de serviços.

Parágrafo único. Nos demais casos, será a SECTI.

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 da Central de Serviços da SECTI, 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 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.
Art. 23. Os usuários devem possuir identificação única e exclusiva para permitir relacioná-la às suas ações e responsabilidades.
Art. 24. Compete à chefia imediata informar aos gestores dos ativos 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 nas fontes autoritativas.
§ 2º Periodicamente, a SECTI fará o bloqueio automático das credenciais de acesso dos usuários que não realizaram o acesso por mais de 40 (quarenta) 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 do ativo realizar a revisão de direitos de acesso ao ativo sob sua responsabilidade, podendo a SECTI 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 Secretário de Tecnologia 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 por meio do uso de identidade digital (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.
§ 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.
Art. 32. O acesso privilegiado aos sistemas e ativos de informação deverá ser realizado através de ferramenta de controle de acesso privilegiado, definida e gerenciada pela unidade responsável pela segurança cibernética.
Art. 33. O acesso dos usuários da SECTI para login às estações de trabalho deve conter autenticação de multifatores (MFA) com ferramenta definida pela unidade de segurança cibernética.
Seção IV
Da política de senhas
Art. 34. Os sistemas 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 MFA.
§ 3º A SECTI, em conjunto com o gestor do ativo, podem implementar a MFA para determinados tipos de acesso, em função de sua criticidade.
Art. 35. A senha de acesso do usuário, tokens, e outros fatores de autenticação devem ser de uso pessoal e intransferível.
Art. 36. As senhas devem ser secretas e definidas considerando as seguintes recomendações:
I - Utilizar números, letras, alternando-as entre maiusculas, minúsculas e caracteres especiais, com no mínimo, 8 (oito) caracteres para contas com autenticação de multifatores e 14 (quatorze) para as demais;
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 login;

V - Não expor a senha em local visível para terceiros, como anotações em papéis, sob pena de responsabilização pelos acessos indevidos.

Art. 37. 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. 38. 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 da SECTI.

Art. 39. 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, 3 (três) 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. 40. 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, 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.

Seção V

Dos procedimentos seguros de entrada no sistema

Art. 41. 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, 30 (trinta) minutos; e

Seção VI

Do acesso dos equipamentos à rede e aos serviços de rede

Art. 42. 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. 43. O acesso de novo equipamento à rede é regulamentado pelo procedimento de autorização específico e deverá ser executado mediante abertura de chamado de requisição de serviço em sistema da Central de Serviços da SECTI.
Art. 44. São consideradas redes do TRE-PR, para efeito de controle, a rede cabeada da sede e seus anexos, todas as redes wi-fi em suas dependências e por ele provida, o acesso a rede privada virtual (VPN), o perímetro para a Internet e as redes das zonas eleitorais.
Art. 45. É vedada a inclusão de equipamentos pessoais ou de terceiros em qualquer uma das redes internas do TRE, sem autorização da SECTI.
Art. 46. O horário de funcionamento da VPN e do acesso à Internet será regulamentado em portaria interna e qualquer alteração excepcional deverá ser solicitada ao Comitê de Segurança da Informação.
Art. 47. A inclusão de equipamentos e usuários na VPN será solicitada através de procedimento administrativo.
Art. 48. Os acessos à rede devem ser registrados, arquivados por um período mínimo de 3 (três) meses, monitorados e frequentemente deve ser emitido relatório crítico com finalidade de identificar acessos indevidos.
Art. 49. Poderá, a critério da SECTI, ser exigido múltiplo fator de autenticação nas máquinas que acessam a VPN do TRE-PR.
Art. 50. 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. 51. O código-fonte e itens associados (esquemas, especificações, planos de validação, entre outros) 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. 52. Os casos omissos serão resolvidos pela SECTI ou pelo CGSIPDP, observadas suas competências.
Art. 53. Esta norma será revisada pelo Gestor de Segurança da Informação, sempre que se fizer necessário, e encaminhada para apreciação superior.
Art. 54. O descumprimento desta norma será objeto de apuração específica, com a consequente aplicação das penalidades cabíveis, se for o caso.
Art. 55. Esta instrução normativa entrará em vigor na data de sua publicação.
SOLANGE MARIA VIEIRA
Diretora-Geral
ANEXO ÚNICO
TERMOS E DEFINIÇÕES

Para os efeitos desta instrução normativa, considera-se:
I - Ativos de TI: todo e qualquer componente de hardware, software e rede de dados em uso no Tribunal, nos Cartórios Eleitorais e pelos servidores do quadro funcional da Justiça Eleitoral do Paraná, quando no exercício de suas funções;
II - Ativos de informação: meios de armazenamento, transmissão e processamento de informação, sistemas de informação e locais onde se encontram esses meios e as pessoas que a eles têm acesso;
III - Ativos de processamento: são elementos físicos (hardware) e lógicos (software) que processam informações e dados na organização.
IV - Ativos de hardware: componentes físicos dos equipamentos de Informática;
V - Ativos de software: itens de solução de tecnologia da informação e comunicação constituídos por software que é classificado, quanto a sua estrutura, em:
a) estruturante: ativo de software desenvolvido, evoluído ou sustentado pelo TRE-PR que contenha informações em sua construção que sejam de responsabilidade restrita a um agente público;
b) não estruturante: todo ativo não classificado como estruturante;
VI - Autenticação: processo que busca verificar a identidade digital de uma entidade de um sistema, no momento em que ela requisita acesso a esse sistema. O processo é realizado por meio de regras preestabelecidas, geralmente pela comparação das credenciais apresentadas pela entidade com outras já pré-definidas no sistema, reconhecendo como verdadeiras ou legítimas as partes envolvidas em um processo;
VII - Autenticação de Multifatores (MFA): utilização de dois ou mais fatores de autenticação para concessão de acesso a um sistema. Os fatores de autenticação se dividem em: algo que o usuário conhece (senhas, frases de segurança, PIN, dentre outros); algo que o usuário possui (certificado digital, tokens, códigos enviados por SMS, dentre outros); algo que o usuário é (aferível por meios biométricos, tais como digitais, padrões de retina, reconhecimento facial, dentre outros); e onde o usuário está (quando o acesso só pode ser feito em uma máquina específica, cujo acesso é restrito);
VIII - Controle de Acesso Baseado em Papéis (RBCA): é uma abordagem para restringir o acesso a usuários autorizados. Definem os direitos e permissões baseados no papel que determinado usuário desempenha na organização. Esta estratégia simplifica o gerenciamento das permissões dadas aos usuários;
IX - Criptografia - arte de proteção da informação, por meio de sua transformação em um texto cifrado (criptografado), com o uso de uma chave de cifragem e de procedimentos computacionais previamente estabelecidos, a fim de que somente o(s) possuidor(es) da chave de decifragem possa (m) reverter o texto criptografado de volta ao original (texto pleno). A chave de decifragem pode ser igual (criptografia simétrica) ou diferente (criptografia assimétrica) da chave de cifragem;
X - Desenvolvimento de software: construção de novos ativos de software;
XI - Evolução de software: inclusão de novas funcionalidades ou de melhorias nas funcionalidades existentes no ativo de software em produção;
XII - Gestor do Ativo: O responsável por gerenciar todo o ciclo de vida dos recursos de Tecnologia da Informação;
XIII - Identidade Digital (ID): representação unívoca de um indivíduo dentro do espaço cibernético;
XIV - Rede Privada Virtual (VPN): refere-se à construção de uma rede privada, utilizando redes públicas (por exemplo, a Internet) como infraestrutura. Esses sistemas utilizam criptografia e outros mecanismos de segurança para garantir que somente usuários autorizados possam ter acesso à rede privada e que nenhum dado será interceptado enquanto estiver passando pela rede pública;

XV - Sistema de Informação: conjunto de elementos materiais ou intelectuais, colocados à disposição dos usuários, em forma de serviços ou bens, que possibilitam a agregação dos recursos de tecnologia, informação e comunicações de forma integrada;
XVI - Token: algo que o usuário possui e controla (tipicamente uma chave, senha e/ou módulo criptográfico) e que é utilizado para autenticar a identidade do requerente e/ou a requisição em si.

SECRETARIA DE GESTÃO DE PESSOAS

PORTARIAS

PORTARIA GAB2 N. 003/2025

A DESEMBARGADORA ELEITORAL, TATIANE DE CASSIA VIESE,
usando das atribuições que lhe são conferidas pelo artigo 21, inciso III, da Portaria n.º 103/2023, e conforme PAD n.º 3580/2023,
R E S O L V E
Art. 1.º PRORROGAR a participação em TELETRABALHO do servidor FRANCISCO GONÇALVES SIMÕES, ocupante do cargo de Analista Judiciário - Área Judiciária, do Quadro de Servidores deste Tribunal, lotado no Gabinete do Jurista 1 - GAB02, no período de 01/05/2025 à 30/04/2027.
Art. 2.º A participação no regime de teletrabalho não constitui direito ou dever do(a) servidor(a), podendo, a qualquer tempo, ser suspensa ou cancelada em função da conveniência do serviço, e cancelada em razão da inadequação do(a) servidor(a) à modalidade, desempenho inferior ao estabelecido, infração aos termos da Portaria TRE/PR n.º 103/2023, ou a pedido do(a) servidor(a), cabendo à autoridade competente decidir.
Art. 3.º Esta Portaria entra em vigor na data de sua publicação, com efeitos a partir de 01/05/2025.
Curitiba, 27 de maio de 2025.
TATIANE DE CASSIA VIESE
Desembargadora Eleitoral

PORTARIA DG Nº 223/2025

A BACHARELA SOLANGE MARIA VIEIRA, DIRETORA-GERAL DA SECRETARIA DO TRIBUNAL REGIONAL ELEITORAL DO PARANÁ,
usando das atribuições que lhe são conferidas pelo artigo 43, inciso VIII do Regulamento da Secretaria deste Tribunal e considerando o contido no PAD nº 8529/2024,
RESOLVE
Art. 1º LOTAR a servidora MARIANGELA DE SOUZA MELO, ocupante do cargo de Analista Judiciário - Área Administrativa, do Quadro de Pessoal deste Tribunal, na Seção de Planejamento Orçamentário - SPO.
Art. 2º Esta Portaria entra em vigor na data de sua publicação, com efeitos a partir de 05/05/2025.
Curitiba, 29 de maio de 2025.
SOLANGE MARIA VIEIRA
Diretora Geral

SECRETARIA JUDICIÁRIA

DOCUMENTOS ELETRÔNICOS PUBLICADOS PELO PJE

RECURSO ELEITORAL(11548) Nº 0600809-74.2024.6.16.0153

PROCESSO : 0600809-74.2024.6.16.0153 RECURSO ELEITORAL (General Carneiro - PR)