Tribunal Regional Eleitoral
do Espírito Santo

Sede: Vitória/ES
Av. João Baptista Parra, 575
Praia do Suá - Vitória - ES
CEP 29052-123
Tel.: (27) 2121.8595
Endereço eletrônico:
www.tre-es.jus.br

Comissão de Segurança da Informação

NSI-011	V1.0 – FEV-2025	SEGURANÇA DA INFORMAÇÃO

Norma de Gestão de Identidade e Controle de Acesso Lógico relativos à segurança da informação e comunicação

Referência(s):

Lei 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD)

Resolução CNJ 396/2021 – ENSEC-PJ

Resolução TSE 23.644/2021 – PSI/JE

Resolução TSE 23.650/2021 – Política Geral de Privacidade e Proteção de Dados Pessoais

Portaria DG/TSE 444/2021, instituição da norma de termos e definições relativa à Política de Segurança da Informação do Tribunal Superior Eleitoral

NC 07/IN01/DSIC/GSIPR

ABNT ISO/IEC 27001 e ABNT ISO/IEC 27002

Boas práticas do Ciscontrols 8.0

Acórdão 1.603/2008-TCU, item 9.1.3, sobre a importância dos controles de acesso.

Palavras Chave: segurança, norma, acesso, lógico, login, senhas	14 áginas

1. Prefácio

A presente norma está alinhada às diretrizes de Segurança da Informação e dos Dados Pessoais estabelecidas na Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ) e na Política de Segurança da Informação da Justiça Eleitoral (PSI-JE).

2. Conceitos e Definições

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. Alem deles:

Acesso Privilegiado: refere-se a contas com recursos elevados que vão além dos usuários normais, por exemplo, administradores de ambientes de redes, servidores ou sistemas.

Administrador padrão: usuário com perfil de administração em um ativo que normalmente vem estabelecido pelo fabricante, comumente com login de usuário: administrador ou admin.

Ativos de informação: são os meios de armazenamento, transmissão e processamento da informação, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso.

Gestão de identidade: administração dos dados cadastrais referentes ao vínculo do usuário com o TRE/ES.

Gestão de Acesso: administração das permissões de uso dos ativos de informação.

Gestor de Ativo: pessoa que tenha a atribuição de conceder ou revogar permissões em sistemas ou equipamentos para outros usuários, definindo o tipo de acesso que será concedido.

3. Princípios

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

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

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

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.

4. Dos Objetivos

4.1. Estabelecer diretrizes para implantação de controles de acesso lógico e de gestão de identidades; e

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

5. Do escopo e do âmbito de aplicação

5.1. 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 de outros órgãos públicos ou entidades privadas contratadas ou com parcerias celebradas, que fazem uso dos ativos de informação e de processamento no âmbito da Justiça Eleitoral.

5.1.1. Os contratos e parcerias celebrados pelo Tribunal que envolvam acesso por terceiros a ativos de informação devem prever, como condição, que os colaboradores envolvidos conheçam e aceitem os termos desta norma.

5.1.2. Os destinatários desta norma, relacionados(as) no item 5.1, são corresponsáveis pela segurança da informação e comunicação, de acordo com os preceitos estabelecidos neste normativo.

6. Da gestão de identidades

6.1. Cabe à área de gestão de pessoas do Tribunal a gestão de identidade dos servidores, magistrados e estagiários, incluindo o cadastramento, alteração de informações - inclusive lotação - e desativação dos usuários nos sistemas informatizados criados para este fim.

6.2. Cabe aos gestores contratuais a gestão de identidade de colaboradores com acesso a infraestrutura tecnológica do Tribunal, incluindo o cadastramento, alteração de informações e desativação dos usuários nos sistemas informatizados criados para este fim.

7. Do gerenciamento de acesso lógico

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

7.2. 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”.

7.3. O modelo de controle de acesso será, preferencialmente, fundamentado no controle de acesso baseado em papéis (RBAC) que, basicamente, consiste em

atribuir-se uma ou mais "funções" a cada usuário, concedendo permissões diferentes a cada função.

7.3.1. Os gestores dos ativos devem definir regras, perfis e restrições de acesso específicos para cada papel, garantindo que o controle seja proporcional aos riscos de segurança, ou seja, que o nível de acesso de cada papel esteja alinhado com a importância e a confidencialidade dos dados.

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

7.5. A concessão e a revogação de acesso serão implementados por meio de processos formais, tendo como base, no mínimo, as seguintes regras:

7.5.1. A nomenclatura das contas de acesso deve seguir critério padronizado.

7.5.2. 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.

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

7.5.4. Devem ser incluídas cláusulas nos contratos de prestadores de serviço, que envolvam acesso por terceiros a ativos de informação, elencando sanções nos casos de acesso não autorizado, ou mesmo tentativa, efetuado por pessoa ou agente, mediante ações diretas ou indiretas dos seus colaboradores.

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

8. Do inventário de contas de acesso

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

8.1.1. contas de usuário

8.1.2. contas de administrador; e

8.1.3. contas de serviço.

8.2. O inventário das contas de usuário e de administrador deverá conter, no mínimo, o nome completo da pessoa, o nome de usuário de rede, data de início de acesso, data de término de acesso (quando disponível) 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.

8.3. A área técnica de segurança cibernética deverá manter o inventário dos sistemas de autenticação do TRE-ES, abrangendo os internos e aqueles hospedados em provedores remotos.

9. Da concessão do acesso às redes, aos sistemas internos e aos serviços informatizados

9.1. A gestão de contas e do controle de acesso dar-se-á de forma centralizada, por meio de serviço de diretório, ou provedor SSO, onde houver suporte.

9.2. As operações de concessão de permissões de acesso serão solicitadas por meio de ferramenta de abertura de chamados, observada a segregação de funções em todo o fluxo do gerenciamento de acesso.

9.3. Cabe à chefia imediata da unidade de lotação do usuário a solicitação de permissões de acesso aos recursos computacionais do Tribunal, informando os sistemas, serviços e o perfil de acesso que o usuário deve possuir.

9.3.1. A solicitação de acesso à rede e/ou a sistemas para colaborador terceirizado deve conter obrigatoriamente a comprovação de que o colaborador assinou Termo de Sigilo e Confidencialidade para não divulgação de informações do Tribunal.

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

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

9.5.1. A fim de agilizar o processo de concessão de permissões de acesso, sem perda da segurança, o gestor do ativo pode definir previamente os papéis específicos a serem aplicados a cada tipo de usuário do ativo.

9.5.2. As autorizações, sejam elas individuais ou para grupos de usuários, devem estar documentadas para fins de auditoria e levantamento periódico, visando à detecção de usuários com acesso indevido.

9.6. 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 enviadas para o endereço eletrônico da mesma.

9.6.1. Se houver mensagens eletrônicas que precisam ser restritas a determinados usuários da unidade, é necessário estabelecer um grupo de distribuição exclusivo, composto apenas pelas pessoas autorizadas a acessar tais mensagens.

9.6.2. Se houver arquivos que precisam ser restritos a determinados usuários da unidade é necessário solicitar à área técnica a criação de um conjunto de permissões distinto do padrão utilizado para as unidades.

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

9.7.1. O uso compartilhado de identificação de usuários somente será permitido em caráter excepcionalíssimo, por razões operacionais, mediante procedimento de atribuição de responsabilidades compartilhado pelas chefias imediatas e com autorização da Comissão de Segurança da Informação.

10. Da alteração de lotação e do bloqueio de acesso às redes, aos sistemas internos e aos serviços informatizados

10.1. As operações de revogação de direitos de acesso serão solicitadas por meio de ferramenta de abertura de chamados, observada a segregação de funções em todo o fluxo do gerenciamento de acesso.

10.2. Compete à chefia imediata solicitar a revogação de permissões de acesso de qualquer usuário alocado em sua unidade, informando os sistemas, serviços e perfis de acesso que o usuário deve deixar de possuir.

10.2.1. A chefia imediata também deve obrigatoriamente revogar as permissões de acesso destes usuários aos ativos cuja gestão está sob sua responsabilidade.

10.2.2. A revogação do acesso dar-se-á somente após o efetivo desligamento do usuário da unidade, que deve ser efetuado pela área responsável no respectivo sistema de gestão de identidade.

10.2.3. No caso de término do vínculo com o TRE/ES de servidores, estagiários e magistrados, ou ainda de servidor que passa da situação ativo para inativo, a área de gestão de pessoas deve comunicar formalmente, via sistema de processo administrativo, à Secretaria de Tecnologia da Informação para que sejam efetuados os procedimentos de revogação das permissões de acesso.

10.2.4. No caso de término do vínculo com o TRE/ES de colaboradores vinculados a contratos, o gestor contratual deve comunicar formalmente, via sistema de processo administrativo, à Secretaria de Tecnologia da Informação para que sejam efetuados os procedimentos de revogação das permissões de acesso.

10.3. As contas de usuários deverão ser revisadas trimestralmente para avaliar se todas as contas ativas permanecem autorizadas.

10.3.1. As áreas técnicas de segurança cibernética e gestão de infraestrutura e redes devem, em conjunto, estabelecer o procedimento formal que será utilizado para efetuar a revisão.

10.3.2. Cabe à área de gestão de infraestrutura e redes a execução do procedimento de verificação.

10.4. Usuários que não realizarem o acesso à rede de dados por mais de 60 (sessenta) dias, terão o seu acesso bloqueado temporariamente até que solicitem o reestabelecimento do acesso por meio de ferramenta de abertura de chamados.

10.4.1. O bloqueio temporário não se aplica ao acesso de servidores inativos, que já é restrito aos módulos necessários.

10.4.2. Sempre que disponível, os sistemas com bases de usuários próprias devem ser configurados para efetuar o bloqueio temporário nos termos descritos **no item 10.4**

10.5. Compete ao gestor de ativo realizar a revisão de permissões de acesso ao ativo sob sua responsabilidade.

11. Do acesso privilegiado

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

11.2. 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.

11.3. As competências dos usuários com acesso privilegiado aos sistemas e ativos de informação deverão ser avaliadas em intervalos não superiores a seis meses, para que estejam alinhadas às atividades e obedecendo as regras de segregação de funções.

11.4. O acesso privilegiado aos sistemas e ativos de informação através do uso de ID de usuário administrador padrão 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.

11.4.1. A conta de administrador padrão deve ser renomeada e ter sua função apagada, para que não possa ser facilmente identificada.

11.4.2. A conta de administrador padrão não deve ser usada para acesso à Internet, iniciar serviços de rede e acessar arquivos externos.

12. Da política de senhas

12.1. 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.

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

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

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

12.4.1. Utilizar números, letras, alternando-as entre maiúsculas, minúsculas e caracteres especiais, como $@#&%, com, no mínimo, 14 (quatorze) caracteres;

12.4.2. 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. Evitar palavras contidas no dicionário;

12.4.3. 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;

12.4.4. 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;

12.4.5. Modificar a senha temporária no primeiro logon; e

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

12.5. 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 Secretaria de Tecnologia da Informação através do sistema de registro de chamados.

12.6. Sempre que disponível, a emissão de senha temporária para primeiro acesso ou senha necessária em virtude de esquecimento, deve ocorrer por procedimento totalmente automatizado, sem intervenção de terceiros.

12.6.1. Para os sistemas e serviços que não suportam a automação:

a) O gestor do ativo, com apoio da área de segurança cibernética, deve submeter à Comissão de Segurança um procedimento formal;

b) Analisado e aprovado o procedimento, devem ser executados pelo próprio usuário, sempre instruído pela área de tecnologia da informação.

c) Devem ser solicitados dados pessoais do usuário para confirmação da identidade.

d) 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.

13. Do sistema de gerenciamento de senhas

O sistema de gerenciamento de senhas deve:

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

13.2. Forçar as mudanças de senha a intervalos regulares de, no máximo, 6 (seis) meses, conforme necessidade;

13.3. Empregar criptografia no canal de comunicação utilizado para o tráfego de credenciais de acesso;

13.4. Criptografar ou embaralhar (hash) com *salt* as credenciais de autenticação armazenadas;

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

13.6. Manter, para fins de auditoria, registro dos acessos, das operações e dos respectivos períodos;

13.7. Desabilitar as contas que não possam ser associadas a um usuário ou processo de negócio; e

13.8. Monitorar tentativas de acesso a contas desativadas.

14. Dos procedimentos seguros de entrada no sistema

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

14.1. Não fornecer mensagens de ajuda ou informações do sistema que possam auxiliar um usuário não autorizado;

14.2. Validar informações de entrada somente após todos os dados estarem completamente preenchidos;

14.3. No caso de erro, não indicar qual parte do dado de entrada está correta ou incorreta;

14.4. Bloquear o acesso do usuário ao sistema após, no máximo, 5 (cinco) tentativas de entrada no sistema;

14.5. Registrar tentativas de acesso ao sistema, sem sucesso e bem sucedidas; e

14.6. Caso o usuário não bloqueie sua sessão ao se ausentar de seu posto de trabalho, encerrar sessões inativas após um período definido de inatividade de, no máximo, 15 (quinze) minutos;

15. Do acesso dos equipamentos à rede e aos serviços de rede

15.1. 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”.

15.2. A requisição de acesso de novo equipamento à rede deverá ser solicitado através da abertura de chamado em sistema apropriado e deverá ser previamente aprovado pela unidade responsável;

15.3. São consideradas redes internas do TRE-ES, para efeito de controle:

a) as redes cabeadas da sede e seus anexos.

b) as redes sem fio que se comunicam com a rede cabeada da Sede.

c) o acesso VPN.

d) a rede de perímetro para a Internet.

e) as redes cabeadas das Zonas Eleitorais.

15.4. É vedada a inclusão de equipamentos pessoais ou de terceiros em qualquer uma das redes internas.

15.5. O horário de funcionamento do acesso remoto e do acesso à INTERNET será proposto pela Comissão de Segurança da Informação e aprovado pela Administração.

15.6. Os acessos à rede devem ser registrados, monitorados e arquivados por um período mínimo de 6 (seis) meses.

15.7. Será exigido múltiplo fator de autenticação nas máquinas que acessarem a rede do TRE-ES através do acesso remoto.

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

16. Do controle de acesso ao código-fonte de programas

16.1. 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, teste, verificação de segurança ou outra atividade para a qual o acesso seja imprescindível.

16.2. 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.

16.3. O código fonte deve ser mantido em ferramenta de controle de versão, que registre as submissões do código, o autor e a data, assim como as versões publicadas em ambientes de homologação e produção.

17. Disposições finais

17.1. Os casos omissos serão resolvidos pela Comissão de Segurança da Informação do TRE-ES.

17.2. Esta norma complementar deve ser revisada sempre que necessário.

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

17.4. Esta norma entra em vigor na data de sua publicação e sua implementação inicia-se imediatamente.