DIRETORIA GERAL

INSTRUÇÕES NORMATIVAS

INSTRUÇÃO NORMATIVA DG Nº 12 , DE 1º DE DEZEMBRO DE 2023

Institui a Norma de Gestão de Identidade e Controle de Acesso Físico e Lógico ao Ambiente Cibernético do Tribunal Regional Eleitoral do Rio de Janeiro.

A DIRETORA-GERAL DO TRIBUNAL REGIONAL ELEITORAL DO RIO DE JANEIRO, no uso das

atribuições que lhe são conferidas pelo art. 19, I, da Resolução TSE n.º 23.644, de 1º de julho de 2021 (Política de Segurança da Informação da Justiça Eleitoral),

CONSIDERANDO a Resolução CNJ n.º 396/2021, que instituiu a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ);

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

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

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 Rio de Janeiro;

CONSIDERANDO 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; e

CONSIDERANDO, ainda, o teor do processo SEI n.º 2021.0.000030921-9, RESOLVE:

CAPÍTULO I DISPOSIÇÕES GERAIS

Art. 1º As atividades relativas à segurança das informações e comunicações no âmbito do Tribunal Regional Eleitoral do Rio de Janeiro obedecerão ao disposto na presente Norma de Gestão de Identidade e Controle de Acesso Físico e Lógico ao Ambiente Cibernético.

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

CAPÍTULO II

DEFINIÇÕES E CONCEITOS TÉCNICOS

Art. 3º Para efeitos desta Instrução Normativa, consideram-se os termos e definições previstos na Portaria DG/TSE n.º 444/2021, aplicando-se, de forma subsidiária, aqueles estabelecidos no Glossário de Segurança da Informação do Gabinete de Segurança Institucional da Presidência da República (Portaria PR/GSI n.º 93, de 26 de setembro de 2019).

CAPÍTULO III

DO ESCOPO E ÂMBITO DE APLICAÇÃO

Art. 4º Esta Instrução Normativa tem o objetivo de estabelecer as diretrizes e regras gerais que regulamentarão as atividades de gestão de identidade e o controle de acesso físico e lógico ao ambiente cibernético do TRE-RJ, a fim de zelar pela confidencialidade, integridade e disponibilidade dos ativos de informação.

Art. 5º Esta norma se aplica aos magistrados e magistradas, servidores e servidoras efetivos e requisitados, ocupantes de cargo em comissão sem vínculo efetivo, estagiários e estagiárias, prestadores e prestadoras de serviço, colaboradores e colaboradoras, usuários e usuárias externos e órgãos públicos ou entidades privadas, contratadas ou em parcerias celebradas, que utilizam os ativos de informação e processamento do Tribunal Regional Eleitoral do Rio de Janeiro. Parágrafo único. Os destinatários desta norma são corresponsáveis pela segurança da informação e comunicação, devendo, para tanto, conhecer e seguir esta Instrução Normativa.

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

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

IV - Segregação de funções: consiste na separação das funções desempenhadas no controle de acesso, por exemplo, pedido de acesso, autorização de acesso e administração de acesso. Para evitar conflitos de interesses, é necessário repartir funções entre os servidores para que não exerçam atividades incompatíveis, como executar e fiscalizar uma mesma atividade.

CAPÍTULO IV DOS PRINCÍPIOS

Art. 6º O controle de acesso é regido pelos seguintes princípios:

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

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

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

IV - Segregação de funções: consiste na separação das funções desempenhadas no controle de acesso, por exemplo, pedido de acesso, autorização de acesso e administração de acesso. Para evitar conflitos de interesses, é necessário repartir funções entre os servidores para que não exerçam atividades incompatíveis, como executar e fiscalizar uma mesma atividade.

CAPÍTULO V

DO CONTROLE DO ACESSO FÍSICO E DA SEGURANÇA FÍSICA E AMBIENTAL

Seção I

Do perímetro de segurança

Art. 7º Compete à Comissão de Segurança da Informação (COMSI) definir, juntamente com o proprietário do ativo e a Polícia Judicial (POLJUD), o perímetro de segurança e as regras de acesso físico para proteção das instalações de processamento e armazenamento da informação (como o data center) e das demais áreas que contenham ativos de informação críticos ou sensíveis, observando as regras previstas nesta norma.

Parágrafo único. Nas instalações do data center e demais áreas que contenham ativos de informação ou de processamentos críticos ou sensíveis não é permitido o uso de máquinas fotográficas, gravadores de vídeo ou áudio ou outros equipamentos de gravação, salvo quando para coleta de evidências ou nas hipóteses do inciso VI do artigo 8º desta norma e de autorização prévia da Diretoria-Geral, ouvida a Assessoria de Segurança da Informação.

Art. 8º As instalações do data center, área considerada sigilosa, devem atender às seguintes diretrizes:

I - paredes 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;

II - controle de acesso físico em todas as portas para que somente pessoas autorizadas tenham acesso ao data center, registrando-se data e hora de todas as entradas e saídas, sejam de servidores, visitantes ou prestadores de serviço.

III - A entrada de terceiros somente poderá ser realizada mediante prévia autorização da unidade SEPROD, unidade gestora do data center, que indicará o responsável por acompanhar o servidor, visitante ou prestador de serviço durante toda a sua permanência.

IV - controles para minimizar o risco de incêndio e para proteger o ambiente contra poeira, fumaça, explosão, inundação, enchente, furto, vandalismo, interferência com o suprimento de energia elétrica, interferência com as comunicações, campo eletromagnético e arrombamento;

V - filtros de proteção contra raios e instalação em prédios com para-raios; VI - videomonitoramento de sua área interna e de seu perímetro;

VII - alimentações alternativas de energia elétrica e telecomunicações, com rotas físicas diferentes; VIII - iluminação de emergência;

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

X - 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;

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

Seção II

Dos equipamentos de processamento e armazenamento

Art. 9º Para evitar perdas, danos, furtos ou comprometimento de ativos e interrupção das operações da organização, o Tribunal deve obedecer às seguintes diretrizes:

I - adotar controles para minimizar o risco de ameaças físicas potenciais e ambientais, como furto, incêndio, explosivos, fumaça, água, poeira, 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 - manter controles para evitar a retirada de equipamentos do Tribunal sem prévia autorização da unidade competente, conforme regulamentação específica.

Seção III

Da segurança do cabeamento

Art. 10. O cabeamento de energia elétrica e de telecomunicações que transporta dados ou dá suporte aos serviços de informações deve ser protegido contra interceptação, interferência ou danos, conforme as seguintes diretrizes:

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

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

Seção IV

Da manutenção externa dos equipamentos

Art. 11. A manutenção dos equipamentos de processamento e armazenamento de informações deve seguir as seguintes diretrizes:

I - ser realizada somente por pessoal de manutenção autorizado;

II - manter registro de todas as falhas - suspeitas ou reais - 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.

Parágrafo único. Aplica-se às manutenções realizadas por técnicos externos no local do data center o disposto no inciso III do art. 8º.

Seção V

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

Art. 12. 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, todas as demais 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

Das disposições gerais de gerenciamento de acesso lógico

Art. 13. O acesso aos sistemas será assegurado a usuário devidamente autorizado e vedado a usuário não autorizado.

§ 1º Os gestores dos ativos devem determinar formalmente regras apropriadas do controle de acesso, direitos de acesso e restrições para papéis específicos dos usuários acessarem seus ativos, com nível de detalhe e rigor dos controles 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 mais fraca, na qual "Tudo é permitido, a menos que expressamente proibido".

Art. 14. Compete aos gestores 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, com estabelecimento de responsáveis pela solicitação, administração, concessão, bloqueio e revogação.

§ 1º A concessão, revogação de acesso e demais operações de segurança serão objeto de registro, preferencialmente automatizado.

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

§ 4º As contas deverão ser desabilitadas, em vez de excluídas, para preservação de trilhas de auditoria.

§ 5º Caberá à STI o controle e a gestão do Inventário de Ativos de Informação, a fim de assegurar que todo ativo de informação tenha gestor e custodiante designado, assim como Regras de Acesso e Regras de Uso formalmente criadas pelos respectivos gestores.

§ 6º A designação de gestores e custodiantes de Ativos de Informação bem como a criação das Regras de Acesso e Uso de cada ativo de informação deverão ser formalmente registradas em sistema oficial do Tribunal.

§ 7º Caberá ao gestor do ativo de informação formalmente designado a criação e atualização periódica das Regras de Acesso e Uso.

§ 8º O acesso aos sistemas somente poderá ser concedido ao usuário após registro da ciência das Regras de Acesso e de Uso e de Termo de Confidencialidade.

Art. 15. O modelo de controle de acesso será, preferencialmente, fundamentado no controle de acesso baseado em papéis (RBAC).

Art. 16. Os usuários devem possuir identificação única e exclusiva para permitir relacioná-la às suas ações e responsabilidades.

Parágrafo único. A criação de nomes de usuário e de contas de e-mail seguirá critério padronizado.

Art. 17. O uso de contas compartilhadas deve ser evitado.

§ 1º Caso o ativo de informação, em função de razões operacionais ou de negócio, exija a manutenção de credenciais de acesso de uso compartilhado, o proprietário do ativo deve definir procedimentos específicos para evitar seu uso não autorizado, incluindo disposições sobre a troca da senha sempre que um usuário com acesso deixar o Tribunal ou mudar suas atribuições.

§ 2º O uso de conta compartilhada, em razão de representar assunção de riscos para a organização, deve ser documentado em processo e autorizado pela Diretoria-Geral.

§ 3º Contas de serviços e contas de administração de servidores de TI compartilhadas, podem ser autorizadas pela STI ou unidade formalmente designada.

Art. 18. Deverá ser estabelecido e mantido atualizado inventários de todas as contas gerenciadas, contendo data de início e término, incluindo:

I - contas de usuário e de administrador;

II - contas compartilhadas;

III - 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 proprietária, as datas de revisão e o propósito.

§ 2º As contas deverão ser revisadas trimestralmente ou em intervalos menores, pelo respectivo gestor ou pelo custodiante, mediante delegação, para avaliar se as contas ativas permanecem autorizadas.

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.

Art. 20. Contas inativas por mais de 45 (quarenta e cinco) dias devem ser bloqueadas, onde for suportado, podendo o gestor do ativo determinar prazo maior, se as peculiaridades do sistema assim exigirem.

Art. 21. Os gestores dos ativos deverão analisar criticamente as Regras de Acesso e Regras de Uso em intervalos regulares, não maiores que 6 (seis) meses.

Art. 22. Os custodiantes dos ativos devem revisar periodicamente a conformidade de suas atividades com as Regras de Acesso e Regras de Uso.

Art. 23. Cabe aos custodiantes manter registros de todos os eventos relevantes, relativos ao uso e gerenciamento das identidades dos usuários.

Art. 24. Todo ativo que seja cópia, réplica, reprodução de um outro, tais como backups, espelhos, clones e reprodução de ambientes de bancos de dados terão, sempre que possível, as mesmas regras de uso e de acesso.

Seção II

Do acesso às redes, sistemas internos e serviços de rede

Art. 25. O gestor das redes e dos serviços de rede deverá observar as disposições gerais e estabelecer as regras de acesso às redes e serviços de rede pelos usuários.

Art. 26. A gestão de contas e o controle de acesso se darão de forma centralizada, por meio de serviço de diretório, sempre que tecnicamente viável.

Art. 27. 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. Quando não se tratar de nenhum dos usuários citados nos incisos I e II, será necessária aprovação da Diretoria Geral, ouvida a Assessoria de Segurança da Informação.

Art. 28. 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 os perfis de acesso, quando aplicáveis, 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 custodiante do ativo de informação será responsável pela autorização do direito de acesso, conforme o estabelecido pelo proprietário do ativo;

§ 3º Estas autorizações devem estar documentadas, para fins de auditoria e levantamento periódico, visando à detecção de usuários com acesso indevido.

§ 4º O procedimento de atribuição de acesso não deve permitir que a permissão seja efetivada antes que a autorização formal seja finalizada.

Art. 29. Compete à chefia imediata informar aos custodiantes (ou gestor, se não houver), antecipadamente, 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.

Parágrafo único. A retirada dos acessos dos usuários, citados no art. 27 se dará imediatamente após a mudança de lotação ou desligamento efetuado no sistema de gestão de recursos humanos. Art. 30. As regras de acesso aos ativos devem ser revistas, pelos seus gestores, em intervalos regulares, bem como após qualquer mudança de nível institucional que implique em realocação de pessoas, unidades ou papéis.

Seção III

Do acesso privilegiado

Art. 31. São considerados acessos privilegiados todo e qualquer privilégio que:

I - permita a um usuário conceder, alterar ou suprimir privilégios de outro;

II - permita acessar, destruir, criar ou alterar dados ou informações em nome de outro usuário;

III - permita acessar, destruir, criar ou alterar dados de forma irrestrita em ativos como bancos de dados, sistemas operacionais, redes, servidores, sistemas de arquivos, aos quais não tenha acesso em razão de sua função exercida no TRE-RJ.

Art. 32. 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 esse fim, distintas das credenciais de acesso já concedidas 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 As relações de contas que detêm acesso privilegiado devem ser revistas pelos gestores dos ativos de informação em intervalos não superiores a 1 (um) mês.

§ 4º O gestor do ativo de informação, quando tecnicamente viável, deve definir prazo 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.

Art. 33. O acesso privilegiado aos sistemas e ativos de informação através de credenciais de uso compartilhado deve ser evitado se o sistema assim permitir. Quando não houver esta possibilidade, deve ser concedido mediante procedimentos de troca periódica de senha e auditoria dos acessos, criados pelo proprietário 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 para que tenha sua função ocultada, de modo que não possa ser facilmente identificada.

§ 3 º As contas de administrador genérico não devem ser usadas para atividades distintas daquelas para quais são necessárias.

CAPÍTULO VII

DA POLÍTICA DE SENHAS

Art. 34. Os sistemas ou serviços de informação considerados passíveis de controle de acesso pelo proprietário de ativo devem ter seu acesso restrito e controlado por meio do uso de senha, token ou mecanismo de autenticação similar.

§ 1º O acesso remoto à rede, o acesso administrativo e o acesso a aplicações expostas externamente se darão por autenticação multifatorial (MFA), sempre que tecnicamente viável.

§ 2º A Secretaria de Tecnologia da Informação, em conjunto com o proprietário do ativo de informação, pode implementar a autenticação multifator para outros tipos de acesso, em função de sua criticidade para o órgão ou do caráter restrito das informações.

Art. 35. As senhas de acesso do usuário, tokens e outros fatores de autenticação devem ser de uso pessoal e intransferível. As senhas, adicionalmente, devem ser secretas e definidas conforme as seguintes recomendações:

I - utilizar números e letras (alternando-as entre maiúsculas e minúsculas) além de caracteres especiais, como $@#&%, com, no mínimo, 12 (doze) caracteres;

II - não utilização de frases ou palavras que possam ser facilmente adivinhadas por terceiros, baseadas em informações relativas ao próprio usuário ou óbvias, tais como nome de parentes, datas de aniversário, números de telefone e nome do animal de estimação;

III - não utilização na composição da senha de sequências formadas por caracteres triviais, tais como 123456 ou abcde, nem padrões de teclado comuns, como qwert e asdfg;

IV - modificar a senha temporária após o primeiro logon;

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

Art. 36. É vedado aos usuários utilizarem nomes de usuário (e-mail, matrícula, logins, etc.) fornecidos pelo Tribunal para cadastro em serviços externos que não tenham sido adotados ou homologados pelo Tribunal e é proibida a utilização da mesma senha utilizada em sistemas da Justiça Eleitoral em qualquer serviço externo.

Art. 37. 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 Equipe de Tratamento e Resposta a Incidentes de Segurança Cibernética (ETIR).

Art. 38. O sistema de gerenciamento de senha deve, sempre que viável tecnicamente:

I - admitir que os próprios usuários escolham e alterem as suas senhas, incluindo um procedimento de confirmação para evitar erros;

II - ocultar os caracteres na tela quando as senhas forem digitadas;

III - aplicar criptografia no canal de comunicação utilizado para o tráfego de credenciais de acesso;

IV - criptografar ou embaralhar (hash) com salt as credenciais de autenticação armazenadas;

V - forçar que as senhas temporárias sejam modificadas no primeiro acesso ao sistema ou serviço de informação;

VI - no caso de erro, não indicar qual parte do dado de entrada está correta ou incorreta;

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

VIII - bloquear após 5 (cinco) tentativas inválidas e consecutivas de logon;

IX - registrar tentativas de acesso ao sistema, sem sucesso e bem-sucedidas, assim como operações e períodos para fins de auditoria;

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

a) data, hora e equipamento utilizado na última entrada com sucesso no sistema;

b) detalhes de qualquer tentativa sem sucesso de entrada no sistema desde o último acesso bem- sucedido;

XI - encerrar sessões inativas após período definido de inatividade, preferencialmente de 20 (vinte) minutos, podendo este intervalo ser modificado pelo gestor de acordo com a criticidade dos dados tratados na aplicação;

XII - obrigar que a senha seja alterada em intervalos regulares de, no máximo, 6 (seis) meses;

XIII - manter registro das senhas anteriores utilizadas e impedir sua reutilização;

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

XV - monitorar tentativas de acesso a contas desativadas;

XVI - em caso de uso externo, deve restringir o tempo de conexão para reduzir a oportunidade de acesso não autorizado;

XVII - bloquear o reuso de senhas anteriores.

CAPÍTULO VIII

DO ACESSO A CÓDIGO-FONTE

Art. 39. O acesso ao código-fonte e recursos relacionados (esquemas, especificações, roteiros de publicação, planos de validação etc.) dos sistemas de informação desenvolvidos no

Tribunal, deve ser restrito aos usuários que tenham como atribuição funcional seu desenvolvimento, manutenção ou outra atividade para a qual o acesso seja imprescindível.

§ 1º. Os gestores dos ativos deverão criar regras de acesso aos respectivos ativos, considerando as seguintes diretrizes:

I - as bibliotecas de código-fonte e todos os itens associados (bibliotecas, plugins, imagens, etc.) devem ser armazenadas em ferramentas apropriadas para este fim, em ambientes segregados dos sistemas operacionais onde os respectivos sistemas de informação sejam executados;

II - manter os códigos-fonte de programas e todos os itens associados (bibliotecas, imagens, etc.) em um ambiente seguro;

III - manter um registro de auditoria de todos os acessos a código-fonte de programas e criar um mecanismo de registro dos códigos-fontes colocados em ambiente de produção;

IV - evitar que as credenciais de acesso a bancos de dados estejam em texto claro (informação legível, compreensível a quem tenha acesso) dentro de arquivos de configuração da própria aplicação;

V - manter um registro das versões dos códigos-fonte passados para produção, de onde constem: número da versão, autor(es), um código de resumo (hash) aplicado sobre o conjunto de arquivos alterados, e descrição das modificações. Os autores do código não deverão possuir permissão para excluir registros do log.

§ 2º Os códigos-fonte que sejam publicados para entidades externas devem contar com controles adicionais que garantam a sua integridade.

CAPITULO IX

DAS DISPOSICOES FINAIS

Art. 40. As regras de acesso dos ativos, criadas pelos gestores, serão cadastradas em sistema próprio.

Art. 41. Os contratos celebrados pelo Tribunal deverão, sempre que possível, atender os requisitos desta política, bem como as normas referentes à proteção de dados pessoais.

Parágrafo único. 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. 42. O descumprimento desta normativa deve ser imediatamente registrado como incidente de segurança da informação, com envio de e-mail à Equipe de Tratamento e Resposta a Incidentes de Segurança Cibernética - ETIR, para promover a apuração e consequente adoção das providências necessárias.

Art. 43. O descumprimento desta norma poderá ser objeto de apuração disciplinar pela unidade competente do Tribunal, com a consequente aplicação das penalidades cabíveis a cada caso.

Art. 44. A revisão desta Instrução Normativa ocorrerá a cada 3 (três) anos, ou antes, se necessário, pela Assessoria de Segurança da Informação, juntamente com a Secretaria de Tecnologia da Informação, e encaminhada para nova apreciação da Comissão de Segurança da Informação.

Art. 45. Os casos omissos serão resolvidos pela Diretoria-Geral, ouvida a Comissão de Segurança da Informação.

Art. 46. Esta Instrução Normativa entra em vigor na data da sua publicação e sua implementação se fará no prazo de 18 (dezoito) meses a contar desta data.

Rio de Janeiro, 1 de dezembro de 2023.

ELINE IRIS RABELLO GARCIA DA SILVA

Diretora-Geral