PORTARIA PRE Nº 215, DE 16 DE SETEMBRO DE 2024

Institui Norma de Segurança Cibernética — NSC3 — Gestão de Identidade e Controle de Acesso do Tribunal Regional Eleitoral de Minas Gerais.

O PRESIDENTE DO TRIBUNAL REGIONAL ELEITORAL DE MINAS GERAIS, no uso de suas atribuições conferidas pelo inciso XV do art. 22 da Resolução TRE-MG nº 1.277, de 29 de maio de 2024, o Regimento Interno,

CONSIDERANDO o disposto no art. 4° da Resolução TRE-MG nº 1.240, de 6 de fevereiro de 2023, que determina que a "revisão e a atualização das normas complementares de Segurança da Informação ocorrerão sempre que necessário, por meio de portaria da Presidência do Tribunal.";

CONSIDERANDO as normas técnicas NBR ISO 27001 e NBR ISO 27002,

RESOLVE:

CAPÍTULO I

DAS DISPOSIÇÕES PRELIMINARES

Art. 1° Fica instituída a Norma de Segurança Cibernética — NSC3 — Gestão de Identidade e Controle de Acesso do Tribunal Regional Eleitoral de Minas Gerais.

Parágrafo único. A norma de segurança de que trata o *caput* abrange todas as atividades relacionadas à Gestão de Identidade e ao Controle de Acesso físico e lógico aos ativos de Tecnologia da Informação que estejam sob responsabilidade ou custódia do Tribunal Regional Eleitoral de Minas Gerais, no contexto de segurança da informação, e consiste em:

I — estabelecer diretrizes para a gestão de identidades e controles de acesso aos ativos de Tecnologia da Informação e Comunicação — TIC — do Tribunal;

II — reforçar os mecanismos de garantia da confidencialidade, integridade e disponibilidade dos ativos de informação e comunicação sob a responsabilidade e/ou custódia deste Tribunal.

Art. 2º Esta portaria integra a Política da Segurança da Informação do Tribunal Regional Eleitoral de Minas Gerais, regulamentada pela Resolução TRE-MG nº 1.240, de 6 de fevereiro de 2023.

Art. 3° Para os efeitos desta portaria, aplicam-se os termos e definições da

Norma de Segurança Cibernética — NSC1 — Termos e Siglas de Segurança da Informação.

Art. 4° Esta portaria se aplica aos 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 façam, ou venham a fazer, uso dos ativos de TIC na Justiça Eleitoral Mineira.

Parágrafo único. Os destinatários, relacionados no *caput* deste artigo, são corresponsáveis pela segurança da informação e comunicação, de acordo com os preceitos estabelecidos nesta portaria.

Art. 5° Os contratos celebrados pelo Tribunal deverão, sempre que pertinente, estar alinhados aos requisitos desta portaria.

CAPÍTULO II

DOS PRINCÍPIOS

Art. 6° O controle de acesso será regido pelos seguintes princípios:

I — necessidade de saber: os usuários terão acesso somente às informações necessárias ao desempenho pleno de suas atividades;

II — necessidade de uso: os usuários terão acesso apenas aos ativos de TIC necessários ao desempenho pleno de suas atividades;

III — privilégio mínimo: serão conferidos apenas os privilégios minimamente necessários e suficientes para que o usuário realize a sua função na organização;

IV — segregação de funções: as funções desempenhadas na gestão do controle de acesso serão separadas de forma que, sempre que possível, haja distinção de papéis entre quem pede, quem autoriza e quem faz a administração dos acessos.

Parágrafo único. As regras de controle de acesso serão baseadas na premissa de que "tudo é proibido a menos que expressamente permitido" em lugar daquela onde "tudo é permitido, a menos que expressamente proibido".

CAPÍTULO III

DA GESTÃO DE IDENTIDADES

Art. 7° O Tribunal adotará um sistema informatizado de Gestão de Identidade e Acessos — IAM —, ou solução equivalente, de forma a centralizar e unificar o inventário de contas de acesso, bem como os procedimentos de identificação, autenticação, autorização e auditoria dos acessos à rede e aos seus sistemas de informação.

Art. 8° A solução de IAM adotada seguirá padrões de compatibilidade adotados amplamente no mercado, tendo como exemplos os protocolos de autenticação e autorização SAML 1.0/2.0, *OpenID Connect* — OIDC— e OAuth 2.0.

Art. 9º. Os novos sistemas de informação, desenvolvidos internamente ou por empresa contratada para essa finalidade, serão projetados e construídos para utilizarem a solução de IAM adotada.

Art. 10. Durante os trabalhos de análise para adoção de sistemas de terceiros ou aquisição de sistemas prontos, a compatibilidade com a solução de IAM adotada será um dos focos da avaliação.

Art. 11. Os sistemas legados de informação, que não são compatíveis com a solução de IAM adotada no Tribunal, terão seus processos de autenticação, autorização e auditoria bem documentados e, para esses sistemas, também será apresentado um plano de atualização tecnológica ou sua equivalente substituição, de forma a buscar-se a conformidade com os processos de Gestão de Identidade e Acessos.

Art. 12. Será mantido atualizado o inventário de todas as contas de usuário, de administrador e de serviço, bem como de quaisquer outras contas gerenciadas pelo Tribunal.

Art. 13. O inventário das contas de acesso contará com um conjunto de informações que permita apurar informações históricas de propriedade, autorização, alteração, exclusão e temporalidade.

Art. 14. Recomenda-se, para as contas de acesso, a adoção de mecanismos de integração com o sistema de gestão de recursos humanos em uso no Tribunal, de forma a se automatizar as ações relacionadas às revogações de acesso quando da troca de lotação e nos desligamentos permanentes ou provisórios.

§ 1º Nos casos de alteração de lotação, é vedado ao usuário o uso dos privilégios de acesso concedidos a ele em sua lotação anterior, ainda que disponíveis, devendo o usuário informar, de imediato, ao gestor da área de origem sobre a disponibilidade dos mesmos.

§ 2º A utilização de tais credenciais poderá ser alvo de apuração de acesso indevido a recursos e sistemas de informação.

Art. 15. A Secretaria de Tecnologia da Informação manterá inventário dos sistemas de autenticação em uso no Tribunal.

CAPÍTULO IV

DAS CONTAS COM PRIVILÉGIOS ADMINISTRATIVOS

Art. 16. Caberá aos gestores dos ativos de TIC, passíveis de acesso com credenciais administrativas, estabelecer os requisitos e procedimentos para operacionalização da gestão das contas de administrador associadas aos respectivos ativos.

§ 1º Considerando-se o potencial maior de dano, é recomendado o uso de critérios mais rígidos durante a definição dos requisitos e procedimentos relativos às contas de administrador de ativos.

§ 2º Os processos cobrirão as ações e atribuições de solicitação, autorização e revogação de acesso.

Art. 17. O número de usuários com credenciais administrativas em um determinado ativo de TIC será limitado ao menor quantitativo possível.

Art. 18. Excluídos os casos de limitação técnica, o acesso mediante credenciais com privilégios administrativos fará uso de mais de um fator de autenticação.

Art. 19. As contas de administrador possuirão identificadores que sejam associados aos seus respectivos usuários.

Art. 20. Com o objetivo de garantir a rastreabilidade e responsabilização por ações, os ativos de TIC passíveis de acesso privilegiado contarão, sempre que possível, com solução que impeça o uso de credenciais padrão compartilhadas para acesso administrativo.

Art. 21. É facultada aos gestores de ativos de TIC a terceirização das operações de gestão das contas com privilégios administrativos, sendo, entretanto, fortemente recomendado que a aprovação das requisições seja feita pelo próprio gestor ou por pessoa do mesmo setor por ele designada.

Art. 22. Sem prejuízo de outros requisitos e restrições aplicáveis, os administradores de ativos de TIC observarão os seguintes requisitos:

I — é vedada a criação de outras contas administrativas ou alteração de nomes daquelas já existentes sem a respectiva autorização do gestor do ativo;

II — é vedada a alteração de senhas de outras contas administrativas sem a respectiva solicitação formal, *via* requisição de serviço, do titular ou do responsável pela gestão da conta;

III — é vedada a alteração das políticas de conta e de senhas atribuídas à sua conta de administrador de ativo, como alterar intervalos de troca de senha ou desativação da sua expiração;

IV — a conta de administrador de ativo será utilizada, única e exclusivamente, na execução de atividades de competência do setor e estará associada a uma requisição de serviço ou requisição de mudança;

V — a possibilidade de acesso a informações confidenciais ou restritas, naturalmente associadas às credenciais com acesso privilegiado, se limitará àquelas estritamente necessárias à realização das atividades de competência do usuário, sendo que eventual abuso poderá ensejar a apuração de acesso indevido.

Art. 23. A perda de vínculo com o setor do qual partiu a solicitação da credencial de acesso privilegiado (alteração de lotação, aposentadoria, exoneração, cessão, etc.) desautoriza, automaticamente, o uso da conta de administrador de ativo, independentemente do bloqueio ou desativação da conta.

Art. 24. A senha utilizada na conta de administrador de ativo de TIC seguirá as políticas de tamanho e complexidade em vigor, sendo diferente de outras senhas utilizadas pelo portador da conta em quaisquer outros serviços internos ou externos ao Tribunal.

Art. 25. No caso de um usuário detentor de uma conta de administrador de ativo de TIC deixar de ter vínculo direto com o setor que solicitou a respectiva credencial privilegiada ou passar a exercer atividades que não mais demandem privilégios administrativos, sua conta será imediatamente desativada, cabendo à chefia do setor solicitante, ou a seus substitutos regulamentares em substituição, solicitar a exclusão da respectiva conta *via* requisição de serviço na ferramenta de *Information Technology Service Management* — ITSM.

Art. 26. No caso de uma conta de serviço, com privilégios administrativos, deixar de ser utilizada devido à modificação, interrupção permanente ou exclusão do serviço a

ela vinculada, essa conta será imediatamente desativada, cabendo à chefia do setor solicitante, ou a seus substitutos regulamentares em substituição, solicitar a exclusão da respectiva conta via requisição de serviço na ferramenta de ITSM.

Art. 27. No caso de um usuário administrador de ativos de TIC se afastar temporariamente de suas atividades no setor solicitante (licenças, férias, compensações e situações análogas) por mais de 45 (quarenta e cinco) dias, a respectiva conta será desativada em até 24 (vinte e quatro) horas úteis após o início do afastamento, cabendo à chefia do setor solicitante, ou a seus substitutos regulamentares em substituição, solicitar a desativação da respectiva conta *via* requisição de serviço na ferramenta de ITSM.

Art. 28. Todas as ações de criação, alteração, desativação, exclusões e demais atividades relacionadas às contas de administrador de ativo de TIC serão registradas na ferramenta de ITSM e, quando for o caso, devidamente autorizadas.

Art. 29. Em alinhamento à segregação de funções, salvo nos casos devidamente justificados, as ações de gerenciamento de contas de administrador de ativos de TIC será efetuada por usuário distinto daquele alvo da operação.

Art. 30. É facultado ao gestor do ativo de TIC, a qualquer tempo e devidamente motivado, proceder ao bloqueio de qualquer conta de administrador de ativo de TIC, ao que dará conhecimento posterior de sua ação e respectiva motivação, sempre com registro da operação na ferramenta de ITSM.

Art. 31. No caso de um administrador de ativo de TIC identificar que sua conta está bloqueada, salvo nas situações previstas de desativação por afastamento ou a critério do gestor do ativo, será registrado na ferramenta de ITSM um incidente para averiguação da causa do bloqueio.

Art. 32. Será adotada padronização dos nomes de contas de usuário e de serviço que tenham privilégios administrativos.

Art. 33. A solicitação de contas de serviço com privilégios administrativos seguirá procedimento formalmente definido, no qual deverá constar, dentre outras informações, detalhamento claro do uso pretendido para a conta e a indicação do responsável pela mesma.

Art. 34. É vedado o uso da conta de serviço para fins pessoais e diversos daqueles elencados durante o processo de solicitação de sua criação.

Art. 35. Durante a homologação de novos serviços ou em situações que envolvam a continuidade ou restabelecimento emergencial de serviços, é facultado ao gestor do ativo ou a terceiros por ele autorizados, a criação de contas temporárias para administração de ativos de TIC, sempre com registro na ferramenta de ITSM.

Art. 36. As contas com acesso privilegiado serão revisadas regularmente pelas áreas responsáveis pelos respectivos ativos, em intervalos médios sugeridos de 120 (cento e vinte) dias, para avaliar se essas contas permanecem autorizadas e necessárias.

CAPÍTULO V

DA POLÍTICA DE SENHAS

Art. 37. Os sistemas e outros ativos de informação, considerados passíveis de controle de acesso pelo gestor do ativo, terão seu acesso restrito e controlado através do uso de credenciais de acesso protegidas por senhas.

Parágrafo único. Os ativos de informação de TIC, categorizados como críticos, serão considerados como passíveis de controle de acesso.

Art. 38. O acesso inicial aos sistemas de informação, bem como o acesso imediatamente após ações de troca ou recuperação de senha, será feito com o uso de senha temporária e aleatória.

Art. 39. As senhas utilizadas para acesso aos sistemas de informação, os *tokens* e outros fatores de autenticação são de uso pessoal e intransferível.

Art. 40. Na ausência de restrições técnicas, as senhas conterão caracteres que estejam em, pelo menos, 3 (três) dos conjuntos a seguir:

I — letras minúsculas, exceto aquelas acentuadas e o cedilha;

II — letras maiúsculas, exceto aquelas acentuadas e o cedilha;

III — algarismos arábicos;

IV — caracteres especiais (demais caracteres do teclado, incluindo acentuações, cedilha, espaço, etc.).

Art. 41. Salvo nos casos de limitação técnica, as senhas utilizadas para acesso aos ativos de TIC terão, no mínimo, 12 (doze) caracteres para contas sem privilégios administrativos e 16 (dezesseis) para aquelas com acesso privilegiado.

Art. 42. A criação de senhas observará os seguintes requisitos:

I — nunca utilizar frases ou palavras que possam ser facilmente deduzidas por terceiros a partir de informações relativas ao próprio usuário, tais como o seu nome ou de parentes, datas comemorativas e números de telefone;

II — evitar o uso de palavras presentes em dicionários;

III — nunca utilizar sequência consecutiva de caracteres triviais, como “123456” ou “abcde”;

IV — nunca utilizar, parcial ou integralmente, o respectivo usuário de *login* da conta, tal como usuário “joao.silva” e senha “joao.silva”;

V — nunca utilizar sequência de caracteres repetidos, como “www”.

Art. 43. As senhas temporárias devem ser obrigatoriamente alteradas no próximo *logon*.

Art. 44. É vedada a exposição da senha em local visível ou seu armazenamento em locais de fácil acesso por outras pessoas, como anotações em papéis, sob pena de responsabilização pelos eventuais acessos indevidos.

Art. 45. É vedada a repetição de credenciais (nome de usuário e senha) em

mais de um sistema e/ou serviço, quer seja interno ou externo, quer seja para fins profissionais ou pessoais.

Art. 46. Sempre que houver indícios de possível comprometimento da senha, o respectivo usuário realizará sua alteração imediatamente, bem como comunicará a ocorrência, ou a suspeita de comprometimento, mediante o registro de incidente de segurança da informação na ferramenta de ITSM.

Art. 47. Os mecanismos adotados para gerenciamento de senhas por parte dos usuários suportarão os seguintes requisitos:

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

II — impedir que as senhas em digitação sejam mostradas na tela;

III — garantir a modificação das senhas temporárias no primeiro acesso ao sistema ou serviço de informação.

Art. 48. A senha temporária, para primeiro acesso ou após ações de troca/recuperação de senha, será emitida através de procedimento formal, do qual deverão constar mecanismos de verificação e confirmação de identidade.

Art. 49. É vedada a emissão e repasse de senha para terceiros que não o usuário detentor da conta ou o responsável pela gestão da mesma, ainda que chefes imediatos ou superiores do usuário, bem como o seu envio no formato de texto legível e/ou com utilização de serviço de correio que não aquele adotado no Tribunal de forma corporativa.

Art. 50. Resguardados os casos motivados por limitação técnica, os quais devem ser devidamente documentados, as senhas de acesso aos ativos de TIC serão alteradas em intervalos de tempo regulares não superiores a:

I — 120 (cento e vinte) dias para contas sem acesso privilegiado;

II — 90 (noventa) dias para contas com privilégios administrativos.

§ 1º Sempre que possível, os processos de controle de prazos e notificação aos usuários quanto à necessidade de troca da senha serão nativos da solução ou passíveis de automatização.

§ 2º A partir de 7 (sete) dias antes da data de expiração da senha, o usuário será notificado diariamente para que troque sua senha.

§ 3º Expirado o prazo para a troca da senha, a conta será automaticamente bloqueada, devendo seu desbloqueio ser solicitado à Central de Serviços com a devida justificativa pela não troca dentro do prazo concedido.

CAPÍTULO VI

DA GESTÃO DE ACESSO

Art. 51. De acordo com as características dos ativos, os respectivos gestores estabelecerão as regras apropriadas de controle e gestão, bem como direitos e restrições de acesso, cujo nível de rigor e detalhes deverá refletir os riscos de segurança da informação associados, observada a consistência entre os direitos de acesso e as políticas de classificação da informação.

Art. 52. A concessão e a revogação de acesso serão implementadas por meio de um processo formal, preferencialmente automatizado, com clara identificação do solicitante e dos responsáveis pela autorização e operacionalização da atividade.

Parágrafo único. Em situações em que houver risco elevado de ocorrência de incidente de segurança ou de amplificação de um incidente ocorrido, aos gestores de ativos é facultada a concessão e revogação de acessos de forma imediata, devendo, posteriormente, providenciar as devidas documentações com registro da motivação.

Art. 53. O procedimento de atribuição de acesso estabelecerá mecanismos que impeçam a ativação da permissão antes que a autorização formal seja concedida.

Art. 54. Serão adotados processos para retirada de acessos tão logo haja a revogação dos direitos ou o encerramento das atividades, contratos ou acordos, ou para ajustes após mudança de atribuições.

Art. 55. As contas de acesso terão suas exclusões precedidas por um período de quarentena, no qual permanecerão desativadas, de forma a se preservar informações para ações de auditoria.

§ 1º O prazo padrão de quarentena, na situação de conta desativada, será de 12 (doze) meses.

§ 2º A critério do gestor do ativo ou mediante solicitação de uma parte interessada, devidamente justificada e aprovada pelo Gestor de Segurança da Informação, as contas poderão ter o prazo de quarentena dispensados, ampliados, reduzidos ou encerrados.

Art. 56. A criação de contas de acesso e de contas de *e-mail* seguirá critérios padronizados.

Art. 57. O controle de acesso será, preferencialmente, fundamentado no modelo de controle de acesso baseado em função *Role Based Access Control* — RBAC.

Art. 58. Serão estabelecidos meios seguros e adequados para repasse de senhas temporárias ou compartilhadas aos respectivos destinatários, em especial quanto aos mecanismos de identificação do usuário.

CAPÍTULO VII

DAS REDES

Art. 59. São consideradas redes do Tribunal as redes sem fio e cabeadas de sua sede, seus anexos, cartórios eleitorais, unidades itinerantes e demais unidades administrativas de uso permanente ou temporário, fixas ou móveis, e a partir das quais são oferecidos serviços aos usuários internos e externos, bem como aquelas estabelecidas mediante o acesso *Virtual Private Network* — VPN.

Art. 60. É vedada a conexão de novos equipamentos — próprios, pessoais ou de terceiros — às redes do Tribunal sem a devida aprovação formal, a qual deve ser solicitada através da abertura de requisição de serviço *via* ferramenta de ITSM.

Parágrafo único. Excepcionalmente, a inclusão de equipamentos de terceiros na rede será efetuada em *Virtual Local Area Network* — VLAN — específica, isolada das demais e por período definido.

Art. 61. Os acessos externos às redes do Tribunal e demais ativos de TIC, salvo aqueles nativamente associados a sistemas de informação em uso, serão realizados mediante o uso de solução de VPN formalmente adotada.

Art. 62. Os sistemas de informação que lidam com dados pessoais e informações sensíveis farão uso de criptografia da comunicação entre o *frontend* e *backend*, bem como entre a interface do sistema e o usuário, mediante o uso de certificado digital com o protocolo *Hypertext Transfer Protocol Secure* — HTTPS.

Art. 63. Diariamente, no período das 22 (vinte e duas) às 6 (seis) horas, as conexões remotas *via* VPN e o acesso à *internet* serão restritos às equipes técnicas de TIC, previamente identificadas e autorizadas.

Parágrafo único. As áreas que necessitarem, de forma excepcional, acessar a VPN ou a *internet*, no período de restrição previsto no *caput* deste artigo, deverão encaminhar, *via* ferramenta de ITSM, a respectiva requisição, devidamente justificada, até as 17 (dezessete) horas do dia útil imediatamente anterior ao período pleiteado, sob pena de não liberação do acesso.

Art. 64. O cadastro para acesso *via* VPN será solicitado à Central de Serviços através de formulário específico na ferramenta de ITSM.

Art. 65. Os acessos às redes serão monitorados, com registro e guarda dos dados conforme política de armazenamento de *logs* específica.

Art. 66. Serão adotados meios, preferencialmente automatizados, para apuração, em intervalos regulares, dos acessos indevidos ou de suas tentativas.

Art. 67. Será exigido múltiplo fator de autenticação nos computadores que acessarem a VPN do Tribunal.

Art. 68. Os serviços de rede que não estejam em uso serão removidos e não apenas desabilitados.

CAPÍTULO VIII

DO ACESSO ÀS REDES E AOS SISTEMAS DE INFORMAÇÃO

Art. 69. O acesso à rede e aos sistemas de informação do Tribunal somente será permitido ao usuário que possuir uma conta de acesso válida, ativa e previamente cadastrada em um sistema de autenticação e autorização centralizado, seguindo-se um processo formalmente estabelecido.

Art. 70. A criação de contas de usuário para acesso à rede e aos sistemas de informação será precedida de solicitação formal, mediante instrumento específico, devendo-se observar a segregação de funções.

§ 1º No caso de contas de acesso para magistrados e promotores, o pedido será efetuado pela Secretaria de Gestão de Pessoas — SGP.

§ 2º No caso de contas de acesso para servidores efetivos e requisitados,

ocupantes de cargo em comissão sem vínculo efetivo e estagiários, o pedido será efetuado pela chefia da unidade de lotação do usuário ou ainda pela coordenadoria, secretaria ou assessoria à qual a unidade pertence.

§ 3º No caso de contas de acesso para colaboradores e prestadores de serviços, o pedido será efetuado pela chefia imediata da unidade de lotação do usuário.

§ 4º Nos demais casos, será necessária a aprovação da Comissão de Segurança da Informação.

Art. 71. A chefia da unidade de lotação do usuário solicitará a atribuição de direitos de acesso aos recursos computacionais do Tribunal por meio da ferramenta de ITSM disponibilizada pela Secretaria de Tecnologia da Informação — STI —, informando os sistemas ou serviços de informação e o perfil de acesso que o usuário deve possuir.

Art. 72. O gestor do ativo de informação será responsável pela autorização do direito de acesso, que poderá ser operacionalizado por equipe técnica designada.

Art. 73. Durante a análise da solicitação de acesso, o gestor do ativo considerará também a consistência entre a classificação da informação e os direitos de acesso solicitados.

Art. 74. Sempre que possível, será 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.

Art. 75. Os usuários possuirão identificação única e exclusiva para permitir relacioná-la às suas ações e responsabilidades.

Parágrafo único. O uso compartilhado de identificação de usuários, em casos excepcionais, somente será permitido por razões operacionais, mediante procedimento de atribuição de responsabilidades compartilhadas pelas chefias imediatas e autorização da Comissão de Segurança da Informação.

Art. 76. 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.

Art. 77. A retirada dos acessos dos usuários se dará após a mudança de lotação ou desligamento efetuado no sistema de gestão de recursos humanos.

Art. 78. A área de Tecnologia da Informação bloqueará automaticamente as credenciais de acesso dos usuários que não realizaram o acesso por mais de 90 (noventa) dias, incluídos os servidores aposentados, cedidos e licenciados.

Art. 79. Os direitos de acesso dos usuários serão revistos semestralmente, bem como após qualquer mudança de nível institucional que implique em realocação de pessoas, unidades ou funções.

Art. 80. As atividades de gerenciamento de identidades, de acessos e de autenticação serão registradas formalmente em sistemas apropriados.

Parágrafo único. Serão adotados mecanismos, preferencialmente automatizados, para apurar a existência de credenciais redundantes ou que não tenham sido criadas mediante o processo formal estabelecido.

Art. 81. Serão incluídas cláusulas nos contratos de prestadores de serviço elencando sanções para os casos de acesso não autorizado ou de sua simples tentativa, efetuado por pessoa ou agente, mediante ações diretas ou indiretas dos seus colaboradores.

Art. 82. 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, conforme as regras estabelecidas formalmente.

Art. 83. O acesso privilegiado aos sistemas e ativos de informação somente será concedido aos usuários que tenham como atribuição funcional o dever de administrá-los.

Art. 84. O acesso privilegiado será 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.

Art. 85. O gestor do ativo de informação definirá prazo de expiração para as credenciais de acesso privilegiado, após o qual será reavaliado o atendimento aos critérios para a renovação do acesso privilegiado ao detentor das credenciais expiradas.

Art. 86. A autorização de acesso privilegiado para qualquer unidade que não seja a gestora do ativo será aprovada pelo Gestor de Sistema de Informação — GSI.

Art. 87. O acesso privilegiado aos sistemas e ativos de informação, mediante o uso de credencial padrão, será evitado, se o sistema assim o suportar e, quando não houver essa possibilidade, será concedido mediante procedimentos de troca periódica de senha e auditoria dos acessos.

Art. 88. Sem prejuízo das políticas de troca regular de senhas, as credenciais padrão terão suas senhas alteradas sempre que algum usuário, utilizador dessa credencial, mudar de lotação ou deixar de ter necessidade de uso da mesma.

Art. 89. Sempre que o sistema de informação suportar, as credenciais padrão com acesso privilegiado serão renomeadas e terão sua descrição apagada ou alterada, para que não possam ser facilmente identificadas.

Art. 90. As credenciais padrão com privilégios administrativos não serão usadas para acessar a *internet*, iniciar serviços de rede ou quaisquer outros serviços.

CAPÍTULO IX

DOS PROCEDIMENTOS SEGUROS DE ENTRADA NO SISTEMA

Art. 91. Os processos e as interfaces de autenticação para acesso aos ativos de TIC atenderão, salvo impossibilidade técnica, aos seguintes requisitos:

I — nunca exibir mensagens ou informações que possam contribuir, direta ou indiretamente, para a obtenção de acessos não autorizados;

II — validar as informações de entrada no sistema somente após o preenchimento de todos os dados;

III — nunca indicar, no caso de falha de autenticação, qual parte da credencial está incorreta;

IV — bloquear a conta após a quinta tentativa inválida de acesso, realizada no intervalo de:

a) 30 (trinta) minutos, para contas sem privilégio administrativo;

b) 5 (cinco) minutos, para contas com privilégio administrativo;

V — registrar em sistema de *log*s os acessos e as tentativas de acesso ao sistema;

VI — mostrar ao usuário, após o acesso bem-sucedido, a data e hora do último acesso ou tentativa de acesso.

Art. 92. Sempre que possível, serão estabelecidos e configurados prazos de desconexão automática das sessões por inatividade, os quais equilibrarão os aspectos de segurança aos de usabilidade e produtividade.

CAPÍTULO X

DO CONTROLE DE ACESSO FÍSICO

Art. 93. São considerados ambientes com Acesso Restrito aqueles utilizados para:

I — hospedar ativos de TIC, em operação ou em vias para tal, relacionados ao processamento, armazenamento, transmissão e comunicação de dados;

II — hospedar ativos de energia que dão suporte ao fornecimento e manutenção dos serviços de TIC.

Art. 94. São considerados ambientes com Circulação Controlada aqueles com áreas adjacentes aos ambientes com Acesso Restrito, a partir das quais seja possível o acesso, direto ou indireto, a estes ambientes.

Art. 95. Será mantido registro atualizado de todos os ambientes com Acesso Restrito e de Circulação Controlada, descritos nesta portaria, e seus respectivos gestores responsáveis.

Parágrafo único. A gestão e a responsabilidade pelos ambientes com Acesso Restrito, que abriguem ativos de área diversa da STI, se dará de forma compartilhada entre as respectivas áreas.

Art. 96. Caberá aos gestores dos ambientes com Acesso Restrito:

I — estabelecer um processo formal de solicitação, autorização e revogação de acesso aos ambientes;

II — autorizar e revogar acesso aos ambientes sob sua gestão;

III — manter controle atualizado de todas as pessoas autorizadas a ingressarem nesses ambientes, bem como os registros históricos de acesso, pelo prazo mínimo de 12 (doze) meses;

IV — acompanhar o registro de eventos relativos aos ambientes e tomar as ações necessárias para direcionar o tratamento daqueles que tem potencial de gerar incidentes ou problemas.

Parágrafo único. Nas ausências dos gestores, as atribuições recairão para as respectivas chefias imediatas ou para os respectivos substitutos formalmente definidos.

Art. 97. Será estabelecido um processo formal de solicitação, autorização e revogação de acessos aos ambientes com Acesso Restrito.

Art. 98. Os ambientes com Acesso Restrito e Circulação Controlada contarão com monitoramento 24 (vinte quatro) horas por vídeo, com número de câmeras suficientes para evitar pontos cegos.

Parágrafo único. Sempre que possível, a solução de monitoramento por vídeo contará, no mínimo, com os seguintes recursos:

I — detecção de eventos de presença e de movimento em tempo real;

II — registro em sistema centralizado dos *logs* dos eventos detectados;

III — capacidade de envio de notificações por métodos padrão de mercado;

IV — capacidade de captação de imagens na ausência completa de iluminação.

Art. 99. Os ambientes com Acesso Restrito contarão, pelo menos, com os seguintes controles de segurança:

I — portas com mecanismos de controle de acesso centralizado que permita o ingresso no ambiente somente às pessoas previamente autorizadas e corretamente autenticadas, preferencialmente, com uso de mais de um fator de autenticação;

II — sistemas para detecção de intrusos nas portas e também nas janelas acessíveis;

III — restrição de acesso por datas e horários.

Art. 100. Os ambientes com Acesso Restrito e Circulação Controlada serão visivelmente identificados, conforme a seguir:

I — os ambientes com Acesso Restrito terão em suas respectivas portas de acesso uma placa com a informação "Acesso Restrito a pessoas autorizadas";

II — os ambientes com Circulação Controlada terão afixadas em local visível placas com a informação "Ambiente Monitorado 24 horas".

Art. 101. No ingresso e na permanência em ambientes com Acesso Restrito, prestadores externos de serviços, visitantes e demais pessoas alheias às atividades rotineiras do ambiente, serão sempre acompanhados por pessoa previamente autorizada ou pelo gestor do ambiente, durante todo o tempo de permanência no local, devendo, ainda, ser mantidos registros com dados de identificação, motivo do acesso, data e horário de início e término do acesso, guardados por, no mínimo, 12 (doze) meses.

Art. 102. O número de pessoas com autorização de acesso aos ambientes com Acesso Restrito será o mínimo necessário para a correta manutenção e operação dos serviços.

Art. 103. No caso de mudança de lotação, desligamento ou qualquer outro evento que implique na perda da necessidade de acesso a um ambiente com Acesso Restrito, o gestor será imediatamente comunicado para revogação dos direitos de acesso do respectivo

usuário.

Parágrafo único. Durante o intervalo de tempo entre a comunicação ao gestor e a efetiva desativação do acesso, considera-se revogado o direito de acesso e o ingresso nos ambientes com Acesso Restrito, estando a pessoa sujeita à apuração de responsabilidade por acesso indevido.

CAPÍTULO XI

DAS DISPOSIÇÕES FINAIS

Art. 104. O descumprimento desta portaria será imediatamente registrado como incidente de segurança da informação e encaminhado para tratamento inicial pelo gestor do ativo, o qual, de acordo com a necessidade e gravidade do incidente, poderá escalar o problema às instâncias superiores.

Parágrafo único. O previsto no *caput* deste artigo não impede a comunicação de eventos ou incidentes relacionados à segurança da informação diretamente às instâncias hierarquicamente acima do gestor do ativo.

Art. 105. Os casos omissos serão resolvidos pela Comissão de Segurança da Informação.

Art. 106. Esta portaria será revisada de acordo com a periodicidade prevista na Resolução TRE-MG nº 1.240, de 2023, que instituiu a Política de Segurança da Informação, ou sempre que houver necessidade de atualização de seus termos para se alinhar a novos regramentos ou evoluções tecnológicas.

Art. 107. Na eventualidade de sobreposição de definições normativas, existentes ou futuras, com aquelas estabelecidas nesta portaria, serão consideradas, para efeito de sua aplicação, aquelas que forem mais restritivas e/ou que trouxerem mais segurança aos ativos de TIC do Tribunal.

Art. 108. Esta portaria entra em vigor na data de sua publicação.

Belo Horizonte, 16 de setembro de 2024.

Desembargador Ramom Tácio de Oliveira
Presidente

Documento assinado eletronicamente por **RAMOM TÁCIO DE OLIVEIRA**, **Presidente**, em 16/09/2024, às 16:51, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade deste documento pode ser conferida no site https://sei.tre-mg.jus.br/controlador_externo.php?acao=documento_conferir&acao_origem=documento_conferir&lang=pt_BR&id_orgao_acesso_externo=0, informando o código verificador **5680198** e o código CRC **74B663C4**.