Documento assinado eletronicamente em 20/07/2021, às 14:34, conforme art. 1º, §2º, III, b, da Lei 11.419/2006.
A autenticidade do documento pode ser conferida em https://sei.tse.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0&cv=1706360&crc=8A3413E4, informando, caso não preenchido, o código verificador 1706360 e o código CRC 8A3413E4.
2020.00.000004513-0

PORTARIA TSE Nº 454 DE 13 DE JULHO DE 2021.

Dispõe sobre a instituição da Norma de Controle de Acesso Físico e Lógico Relativos à Segurança das Informações e Comunicações do Tribunal Superior Eleitoral.
O DIRETOR-GERAL DA SECRETARIA DO TRIBUNAL SUPERIOR ELEITORAL, no uso de suas atribuições legais e regimentais, considerando a Resolução-CNJ nº 370, de 28 de janeiro de 2021, que institui a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário; a Resolução-TSE nº 23.501, de 19 de dezembro de 2016, que institui a Política de Segurança da Informação (PSI) no âmbito da Justiça Eleitoral; a Resolução-TSE nº 23.360, de 13 de outubro de 2011, que regulamenta, entre outros, o ingresso de pessoas, objetos e volumes nas dependências do Tribunal; as orientações de controles de segurança da informação dispostas na norma ISO NBR /IEC 27002:2013;a Revisão 1 da Norma Complementar nº 07/IN01/DSIC/GSIPR, homologada em 15 de julho de 2014, que estabelece diretrizes para implantação de controles de acesso relativos à segurança da informação e das comunicações na administração pública federal; e as recomendações do Acórdão-TCU nº 1.603, de 13 de agosto de 2008, item 9.1.3, sobre a importância dos controles de acesso,
RESOLVE:
Art. 1º Fica instituída a Norma de Controle de Acesso Físico e Lógico relativa à segurança das informações e comunicações, em consonância com a Política de Segurança da Informação do Tribunal Superior Eleitoral.
Capítulo I
DOS CONCEITOS E DEFINIÇÕES
Art. 2º Para os efeitos da Política de Segurança da Informação do TSE, aplicam-se os termos e definições conceituados na Portaria TSE nº 444, de 08 de julho de 2021.
Capítulo II
DOS PRINCÍPIOS
Art. 3º Esta norma tem como princípio norteador a garantia da confidencialidade, integridade e disponibilidade dos ativos de informação.
Art. 4º O acesso, físico ou lógico, deve ser concedido aos usuários deste Tribunal, atendendo aos princípios do perfil de acesso aos ativos de informação.
Capítulo III
DO ESCOPO
Art. 5º O objetivo desta Norma de Controle de Acessos Físico e Lógico Relativos à Segurança das Informações e Comunicações consiste em:
I - estabelecer diretrizes para implantação de controles de acesso físico e lógico;
II - preservar os ativos de informação;
III - assegurar a confidencialidade, integridade e disponibilidade dos ativos de informação sob a responsabilidade deste Tribunal.
Art. 6º 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 que utilizam os ativos de informação deste Tribunal.

Parágrafo único. Todos são corresponsáveis pela segurança da informação, devendo, para tanto, conhecer e seguir esta portaria.

Capítulo IV

DO CONTROLE DO ACESSO FÍSICO

Seção I

DO PERÍMETRO DE SEGURANÇA

Art. 7º A Comissão de Segurança da Informação (CSI) deve definir, juntamente com a Assessoria Especial de Segurança e Inteligência (Aesi),o perímetro de segurança física para proteção das instalações de processamento e armazenamento da informação (*datacenter*) e das demais áreas que contenham informações críticas ou sensíveis.

Art. 8º As instalações do *datacenter* devem atender às seguintes diretrizes:

I - paredes fisicamente sólidas, sem brechas nem pontos por onde possa ocorrer uma invasão, portas externas adequadamente protegidas por mecanismos de controle contra acesso não autorizado, sem janelas ou, na impossibilidade, com janelas com proteção externa;

II- videomonitoramento de sua área interna e de seu perímetro;

III - controle de acesso físico às áreas e instalações, sob a responsabilidade da Aesi, utilizando-se dos mecanismos necessários para o controle e registro de data e hora de todas as entradas e saídas, sejam de servidores, visitantes ou prestadores de serviço, permitindo-lhes o acesso, desde que previamente autorizados;

IV- mecanismos de autenticação de multifatores, 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, terremoto, explosão, manifestações civis, contra-ataques maliciosos, fumaça, furtos;

VIII - edifícios que sejam dotados de proteção contra raios e que, em todas as linhas de entrada de força e de comunicações, tenham filtros de proteção contra raios;

IX - alimentações alternativas de energia elétrica e telecomunicações, com rotas físicas diferentes;

X - iluminação e comunicação de emergência;

XI - sistema de controle de temperatura e umidade com recurso de emissão de alertas.

Art. 9º As diretrizes para proteção das demais áreas que contenham informações críticas ou sensíveis que não estejam armazenadas no *datacenter* devem ser estabelecidas pela CSI, observadas as legislações vigentes.

Seção II

DOS EQUIPAMENTOS DE PROCESSAMENTO E ARMAZENAMENTO

Art. 10. Para evitar perdas, danos, furtos ou comprometimento de ativos e interrupção das operações da organização, o Tribunal deve seguir as seguintes diretrizes:

I - adotar controles para minimizar o risco de ameaças físicas potenciais e ambientais, como furto, incêndio, explosivos, fumaça, água, poeira, vibração, efeitos químicos, interferência com o suprimento de energia elétrica, interferência com as comunicações, radiação eletromagnética e vandalismo;

II - verificar se os suprimentos de energia elétrica, telecomunicações, água, gás, esgoto, calefação /ventilação e sistema de ar-condicionado estejam em conformidade com as especificações do fabricante do equipamento e com os requisitos legais da localidade;

III - adotar controles para evitar a retirada de equipamentos do Tribunal sem prévia autorização da unidade competente, conforme regulamentação específica;

IV - utilizar, sempre que possível, *racks* que disponham de fechaduras com chave ou mecanismo semelhante, garantindo que apenas a(s) equipe(s) responsáveis pelos ativos instalados nos *racks* tenham acesso físico a eles.

Seção III

DA SEGURANÇA DO CABEAMENTO

Art. 11. O cabeamento de energia elétrica e de telecomunicações que transporta dados ou dá suporte aos serviços de informações deve ser protegido contra interceptação, interferência ou danos, conforme as seguintes diretrizes:

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

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 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.

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 sobre gravados com segurança.

Parágrafo único. As mídias que contenham informações com acesso restrito de propriedade intelectual devem ser apagadas fisicamente. Da mesma forma, as informações devem ser destruídas, apagadas ou sobregravadas por meio de técnicas que tornem as informações originais irrecuperáveis.

Seção VI

DA POLÍTICA DE MESA LIMPA E TELA LIMPA

Art. 14. Informação com restrição de acesso não deve ser deixada à vista sobre mesas de trabalho ou em quaisquer outros suportes que não disponham de mecanismos de controle de acesso e deve ser destruída antes de ser descartada, seja em papel ou em meio eletrônico.

Parágrafo único. A política de mesa limpa para papéis e mídias de armazenamento removíveis deve considerar a classificação da informação, requisitos contratuais e legais e o risco correspondente.

Art. 15. Computadores pessoais e terminais de computador não devem apresentar senhas na tela e não devem permanecer logados, caso o usuário esteja ausente.

Parágrafo único. A política de tela limpa para computadores e terminais deve ser aplicada por meio de bloqueio de tela por senha, *token* ou mecanismo de autenticação similar.

Capítulo V

DO CONTROLE DE ACESSO LÓGICO

Seção I

DO GERENCIAMENTO DE ACESSO

Art. 16. As operações de criação e exclusão de usuário da rede local devem ser efetuadas pelo Service Desk da Secretaria de Tecnologia da Informação (STI).

§ 1º Quando se tratar de magistrados, servidores efetivos e requisitados, ocupantes de cargo em comissão sem vínculo efetivo e estagiários, devem ser solicitadas à Secretaria de Gestão de Pessoas (SGP).

§ 2º Quando se tratar de colaboradores e prestadores de serviços, devem ser solicitadas à chefia imediata da unidade de lotação do usuário.

§ 3º Para os demais casos, devem ser solicitadas à Diretoria-Geral.

Art. 17. É de responsabilidade da chefia imediata da unidade de lotação do usuário solicitar a atribuição de direitos de acesso aos recursos computacionais do Tribunal por meio do Service Desk, informando os sistemas ou serviços de informação a serem acessados e o perfil de acesso que o usuário deverá possuir.

§ 1º O perfil de acesso do usuário aos sistemas ou serviços de informação deve ser restrito ao desempenho de suas atividades.

§ 2º O gestor do ativo de informação será responsável pela autorização do direito de acesso.

§ 3º Deve ser estabelecido um perfil inicial padrão para novos usuários, ao qual retornarão em caso de mudança de lotação ou por qualquer outro motivo que leve à suspensão de suas atividades.

Art. 18. Os usuários devem possuir identificação única e exclusiva para permitir relacioná-la às suas ações e responsabilidades.

Art. 19. Compete à chefia imediata informar aos responsáveis estabelecidos no art. 15 deste normativo, tempestivamente, a movimentação e, antecipadamente, o desligamento de usuário alocado sob sua responsabilidade, dadas as implicações na manutenção de direitos de acesso aos ativos de informação.

§ 1º Periodicamente, a área de Tecnologia da Informação efetuará bloqueio automático das credenciais de acesso dos usuários que não realizaram acesso por mais de 90 (noventa) dias, incluindo servidores aposentados, cedidos e licenciados.

§ 2º É vedado aos usuários utilizarem a identificação fornecida pelo TSE para cadastro em serviços externos que não tenham sido adotados ou homologados pelo Tribunal.

Art. 20. Os direitos de acesso dos usuários devem ser revistos em intervalos regulares, bem como após mudança de função, alteração de lotação ou desligamento.

Parágrafo único. Compete ao gestor de ativo realizar a revisão de direitos de acesso ao ativo sob sua responsabilidade.

Seção II

DO ACESSO PRIVILEGIADO

Art. 21. 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 A relação de usuários que detêm acesso privilegiado deve ser revista pelo gestor do ativo de informação em intervalos não superiores a 1 (um) mês.

§ 3º O gestor do ativo de informação pode 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 para o detentor das credenciais expiradas.

§ 4º Caso o ativo de informação, em função de suas características técnicas, exija a manutenção de credenciais de acesso privilegiado de uso compartilhado, o gestor do ativo deve definir procedimentos específicos para evitar seu uso não autorizado.

Seção III

DA POLÍTICA DE SENHAS

Art. 22. Os sistemas ou serviços de informação considerados passíveis de controle de acesso pelo gestor de ativo devem ter seu acesso restrito e controlado por meio do uso de senha, *token* ou mecanismo de autenticação similar.

Parágrafo único. A STI, em conjunto com o gestor do ativo de informação, pode implantar a autenticação de multifatores para determinados tipos de acesso, em função de sua criticidade.

Art. 23. 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 - uso de números, letras, alternando-as entre maiúsculas e minúsculas, e caracteres especiais, como $@#&%, totalizando, no mínimo, 8 (oito) caracteres;

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

III - não utilização de 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;

IV - não utilização das mesmas credenciais (nome de usuário e senha) para fins pessoais (serviços externos ao ambiente de TI do TSE) e profissionais;

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

Art. 24. Sempre que houver indicação de possível comprometimento da senha, o usuário deve realizar sua alteração, bem como comunicar a ocorrência ou a suspeita de comprometimento ao Service Desk.

Art. 25. O sistema de gerenciamento de senha deve:

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

II - forçar as mudanças de senha em intervalos regulares de, no máximo,6 (seis) meses, conforme necessidade;

III - manter registro das senhas anteriores utilizadas e bloquear sua reutilização;

IV - armazenar e transmitir as senhas de forma protegida;

V - não mostrar as senhas na tela quando forem digitadas;

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

Seção IV

DOS PROCEDIMENTOS SEGUROS DE ENTRADA NO SISTEMA

Art. 26. O procedimento adequado de entrada no sistema (*login)* deve atender às seguintes recomendações:

I - não fornecer mensagens de ajuda, durante o procedimento de entrada, que possam auxiliar usuário não autorizado a realizar o *login*;
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;
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, 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;
VII - não mostrar a senha que está sendo informada;
VIII - não transmitir senhas em texto claro pela rede;
IX - encerrar sessões inativas após período definido de inatividade de, no máximo, 10 (dez) minutos.
Seção V
DO CONTROLE DE ACESSO AO CÓDIGO-FONTE DE PROGRAMAS
Art. 27. O código-fonte e os itens associados (esquemas, especificações, planos de validação, etc.) dos sistemas de informação desenvolvidos pelo Tribunal somente serão acessíveis aos 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 de itens associados devem ser armazenadas em ferramentas apropriadas para esse 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 de itens associados devem ser registrados, de forma a permitir sua auditoria.
§ 3º Códigos-fonte que sejam publicados para entidades externas devem contar com controles adicionais que garantam sua integridade.
Capítulo VI
DISPOSIÇÕES FINAIS
Art. 28. Os casos omissos serão resolvidos pela CSI deste Tribunal.
Art. 29. A revisão desta portaria ocorrerá a cada 3 (três) anos ou sempre que se fizer necessária ou conveniente para o TSE.
Art. 30. O descumprimento desta portaria deve ser imediatamente registrado como incidente de segurança e comunicado à CSI para apuração e consequente adoção das providências cabíveis.
Art. 31. Esta portaria entrará em vigor na data de sua publicação e sua implementação se fará no prazo de 12 (doze) meses a contar dessa data.
RUI MOREIRA DE OLIVEIRA
Documento assinado eletronicamente em 19/07/2021, às 19:10, conforme art. 1º, §2º, III, b, da Lei 11.419/2006.
A autenticidade do documento pode ser conferida em https://sei.tse.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0&cv=1706262&crc=1F2D904D, informando, caso não preenchido, o código verificador 1706262 e o código CRC 1F2D904D.
2018.00.000016039-7

PORTARIA TSE Nº 456 DE 13 DE JULHO DE 2021.