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.

Institui norma de uso aceitável de ativos de TI relativa à Política de Segurança da Informação 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 (ENTIC-JUD), e 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,

RESOLVE:

Capítulo I

DISPOSIÇÕES PRELIMINARES

Art. 1º Fica instituída a norma de uso aceitável de ativos de Tecnologia da Informação (TI), em consonância com a Política de Segurança da Informação do Tribunal Superior Eleitoral (TSE).

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 8 de julho de 2021.

Capítulo II

DO USO DOS ATIVOS DE TI

Art. 3º A utilização dos ativos de TI, próprios ou de terceiros, ou sua conexão à rede corporativa, requer prévia aprovação da unidade responsável pela gerência da rede de dados corporativa.

Art. 4º O uso dos ativos de TI da rede corporativa está restrito aos usuários autorizados, conforme os acordos de segurança por eles assinados, e deve ser limitado às atribuições necessárias ao desempenho das respectivas atividades.

Art. 5º O uso dos ativos de TI é de responsabilidade do usuário e deve manter afinidade exclusiva com o objeto de seu cargo, função pública, contrato de trabalho ou de prestação de serviços, inclusive em relação ao conteúdo de documentos, arquivos, trabalhos, mensagens, programas, imagens e sons, incumbindo-lhe:

I - proteger as informações e os ativos de TI que estejam sob sua responsabilidade ou custódia de atividades não autorizadas;

II - aplicar às informações e aos ativos de TI sob sua custódia a proteção e o tratamento adequados, conforme sua classificação de segurança;

III - utilizar os ativos de TI exclusivamente para realização das atividades profissionais desempenhadas nos limites dos princípios da ética, moralidade, razoabilidade e legalidade;

IV - bloquear o acesso à seção dos ativos de TI sempre que se ausentar dela;

V - efetuar fechamento (*logoff*) da conta de acesso ao final do uso, em caso de ativos de TI compartilhados por diferentes usuários;

VI - desligar, sempre que possível, os ativos de TI de uso individual ou compartilhado ao final do expediente;

VII - armazenar as informações institucionais, preferencialmente, nos servidores de arquivos disponibilizados na rede corporativa, evitando o uso dos recursos tecnológicos locais;

VIII - utilizar somente os meios de comunicação disponibilizados oficialmente para a troca de informações com outras instituições, observando a classificação que lhes for atribuída;

IX - colaborar na solução de problemas e no aprimoramento dos processos de segurança da informação.

Capítulo III

DA CREDENCIAL (OU CONTA DE ACESSO)

Art. 6º Os direitos de acesso lógico dos usuários à rede corporativa devem ser definidos por meio de conta e perfil de acesso, de acordo com a sua alocação e função, conforme definido pela Portaria TSE nº 454, de 13 de julho de 2021, que institui a Norma de Controle de Acesso Físico e Lógico relativos à Segurança das Informações e Comunicações do Tribunal Superior Eleitoral.

Parágrafo único. Os direitos de acesso devem ser solicitados por meio do sistema de *service desk* da Secretaria de Tecnologia da Informação (STI), segundo orientações da unidade responsável pelo atendimento ao usuário.

Art. 7º A conta de acesso aos sistemas ou serviços de informação e aos ativos de TI da rede corporativa é pessoal e intransferível, qualificando o usuário, inequivocamente, como responsável por quaisquer acessos e ações realizados com a sua credencial, bem como pelos possíveis danos decorrentes de uso indevido.

Art. 8º Os sistemas ou serviços de informação e os ativos de TI da rede corporativa devem ter seu acesso restrito e controlado mediante conta de acesso com o uso de senhas, *token* ou mecanismo de autenticação similar.

Art. 9º Todos os usuários dos ativos de TI são responsáveis por:

I - criar senha segura para sua conta de acesso, segundo as orientações da STI;

II - manter a confidencialidade das informações de sua conta de acesso e não compartilhá-las com outras pessoas;

III - criar mecanismo de memorização das informações de sua conta de acesso e evitar anotações em papel, arquivos ou dispositivos móveis;

IV - alterar a senha de sua conta de acesso conforme periodicidade máxima definida pela STI ou sempre que suspeitar de falha ou risco que possa comprometer a confidencialidade da sua credencial.

Capítulo IV

DA CÓPIA DE SEGURANÇA (*BACKUP*)

Art. 10. A cópia de segurança em estações de trabalho e dispositivos móveis (*smartphones*, *tablets* , *notebooks*, entre outros) é de responsabilidade exclusiva do próprio usuário.

Art. 11. A cópia de segurança de dados armazenados em servidores de rede do Tribunal é de responsabilidade da STI.

Capítulo V

DA DEVOLUÇÃO DOS ATIVOS

Art. 12. Ao realizar a devolução dos ativos de TI, o usuário deverá:

I - apagar todas as informações de cunho particular que porventura neles estejam armazenadas;

II - transferir para os servidores da rede corporativa todas as informações de cunho profissional que neles estejam armazenadas;

III - restituí-los nas mesmas condições em que lhe foram cedidos.

Art. 13. O Tribunal não se responsabilizará por quaisquer informações de cunho particular que o usuário tenha deixado nos ativos de TI após sua devolução.

Capítulo VI

DAS PROIBIÇÕES

Art. 14. São consideradas ações indevidas nos ativos de TI da rede corporativa:

I - instalar *software*, de sua propriedade ou de terceiros, sem prévia aprovação da unidade responsável pelo atendimento ao usuário, o qual poderá ser removido sem prévia comunicação ao usuário;

II - alterar configurações de *hardware* e *software,* sem prévia aprovação da unidade responsável pelo atendimento ao usuário, os quais poderão ser reconfigurados de acordo com o padrão estabelecido, sem prévia comunicação ao usuário;

III - remover lacres ou proteções similares, atribuição exclusiva da unidade responsável pelo atendimento ao usuário;
IV - remanejar ativos de TI da rede corporativa, tais como *desktops* e impressoras, sem autorização da unidade responsável pelo atendimento ao usuário;
V - expor os ativos de TI a fatores de risco, tais como choques, interferências elétricas ou magnéticas, líquidos (corrosivos ou não), ou a outras ações que lhes possam provocar danos físicos.
Art. 15. Salvo quando a execução das atividades funcionais justificarem a sua prática ou dela dependerem, são considerados usos indevidos dos ativos de TI da rede corporativa:
I - armazenar arquivos particulares nos servidores de arquivos disponibilizados na rede corporativa, tais como músicas, fotos, vídeos e documentos, exceto se decorrentes das atividades profissionais no âmbito do TSE;
II - realizar *download*, cópia, transferência ou compartilhamento de arquivos que infrinjam a legislação vigente referente à proteção da propriedade intelectual (direitos autorais, inclusive de *software*, e patentes);
III - realizar *download*, cópia, transferência ou compartilhamento de arquivos que sejam considerados como possíveis portadores de códigos maliciosos ou que coloquem em risco as instalações e os ativos de TI da rede corporativa;
IV - realizar *download*, cópia, transferência ou compartilhamento de material obsceno, preconceituoso, discriminatório, difamatório, político ou ideológico, que promova incitação à violência ou instrua a invasão da rede corporativa ou de redes externas, além de outros contrários à legislação e à regulamentação em vigor;
V - realizar *download*, cópia, transferência ou compartilhamento de arquivos da rede corporativa ou de seus usuários, programas de computador ou procedimentos, instruções de operação ou de controle e listas de endereços de correio eletrônico, sem a devida autorização do responsável ou que vise a fins particulares ou lucrativos;
VI - manter, divulgar ou utilizar mensagens eletrônicas que suscitem dúvidas quanto à potencialidade de afetar de forma negativa a rede corporativa, quer seja pela contaminação por códigos maliciosos, por vírus de computador ou por quaisquer outros meios, principalmente as que apresentem, entre outros, remetente ou *links* desconhecidos no corpo da mensagem ou anexos com extensões que possam conter códigos maliciosos;
VII - acessar sítios com conteúdos que não coadunem com conduta compatível com a moralidade administrativa, inclusive os de pornografia, de pedofilia, de incitação à violência ou ao preconceito, de venda de drogas, de pirataria ou que divulguem número de série para registro de *software* e outros contrários à legislação;
VIII - executar atividades relacionadas a jogos eletrônicos, conteúdo multimídia, mídias sociais ou ferramentas de relacionamento com fins lucrativos, ideológicos ou recreativos;
IX - atacar ou, sem autorização, monitorar ou acessar os ativos de TI da rede corporativa ou de redes externas, utilizando quaisquer meios;
X - configurar o compartilhamento de pastas e arquivos armazenados em estações de trabalho e dispositivos móveis;
XI - utilizar processo criptográfico não autorizado pela STI em arquivos residentes nos ativos de TI da rede corporativa;
XII - realizar todo e qualquer procedimento no uso dos ativos de TI da rede corporativa não previsto nesta norma que possa afetar de forma negativa o Tribunal ou seus colaboradores.
Parágrafo único. Os arquivos e materiais de que tratam os incisos I a IV deste artigo poderão ser apagados sem prévia comunicação ao usuário.

Art. 16. É vedada a solicitação de suporte técnico à STI para a orientação ou a resolução de problemas referentes à utilização de recursos de TI para fins particulares.

Capítulo VII

DO USO DE RECURSOS EXTERNOS

Art. 17. A utilização, aquisição ou contratação de serviços de informação providos por terceiros para o processamento ou armazenamento de informações de propriedade do TSE, executados sobre a infraestrutura de tecnologia da informação do Tribunal ou sobre infraestrutura externa (serviços em nuvem), deve ser precedida por análise e parecer da Comissão Técnica de Tecnologia da Informação (CTTI).

Parágrafo único. Para viabilizar a análise citada no *caput*, o Documento de Oficialização da Demanda (DOD) referente à utilização, aquisição ou contratação pretendida deve ser encaminhado à CTTI, que se manifestará, definitivamente ou provisoriamente, caso sejam necessárias mais informações, no prazo máximo de 15 dias úteis.

Art. 18. É vedada a utilização de serviços em nuvem de caráter particular para o processamento ou armazenamento de informações de propriedade do TSE.

§ 1º Constatada a ocorrência descrita no *caput*, a responsabilidade quanto à confidencialidade, integridade, disponibilidade e autenticidade de tais informações recairá, com exclusividade, sobre o usuário.

§ 2º O incidente de segurança da informação para o TSE resultante da violação ao disposto neste artigo sujeitará o usuário responsável às penalidades cabíveis.

Capítulo VIII

DO ACESSO REMOTO AOS RECURSOS DE TI

Art. 19. O acesso remoto por parte do usuário aos sistemas de informação ou aos ativos de processamento deve manter afinidade exclusiva com o objeto de seu cargo, função pública, contrato de trabalho ou de prestação de serviços.

§ 1º A permissão para acesso remoto deverá ser solicitada formalmente, por meio de documento encaminhado ao Gabinete do Diretor-Geral, segundo orientações da unidade responsável pelo atendimento ao usuário, do qual constarão a justificativa pertinente e a anuência da chefia imediata do solicitante.

§ 2º Os meios tecnológicos a serem utilizados para a realização do acesso remoto deverão ser exclusivamente aqueles homologados e disponibilizados pela STI.

§ 3º A concessão dos direitos de acesso remoto deverá respeitar a disponibilidade de recursos, incluídas as licenças de uso das soluções homologadas e fornecidas pela STI, e a capacidade apta dos meios de comunicação de dados e de outros elementos de infraestrutura necessários ao provimento do acesso.

Art. 20. Os ativos de TI utilizados para fins institucionais, fora da rede corporativa do TSE, devem seguir o mesmo padrão de segurança empregados internamente e seu uso deve ser autorizado pelo proprietário do ativo de informação.

Art. 21. A infraestrutura tecnológica para acesso externo à rede corporativa do TSE é de responsabilidade do próprio usuário, às suas expensas.

Capítulo IX

DO MONITORAMENTO

Art. 22. O uso dos ativos de TI da rede corporativa está sujeito a monitoramento pelo Tribunal, com vistas a proteger a integridade da imagem e das informações institucionais, preservar a segurança de seus sistemas corporativos ou de seus usuários e, também, para fins de apuração de eventual prática indevida, ilegal ou não autorizada, podendo auditar, dentre outros, os objetos e eventos abaixo relacionados:

I - informações recebidas e transmitidas, criptografadas ou não;
II - arquivos residentes nos ativos de TI e afins;
III - programas de computador (*softwares*), inclusive em execução;
IV - bases específicas de registros de eventos (*logs*);
V - acessos realizados a sítios ou serviços na rede corporativa e na internet.
Art. 23. O monitoramento ostensivo ou eventual nos ativos de TI da rede corporativa pode ser usado para fins de segurança e controle disciplinar, quando for o caso, a exclusivo critério fundamentado dos prepostos e mandatários definidos pelo Gabinete do Diretor-Geral.
Capítulo X
DISPOSIÇÕES FINAIS
Art. 24. Durante o período de realização de eleições, a STI poderá restringir a utilização, em termos de desempenho e de segurança, de quaisquer recursos de TI, visando assegurar o resultado das ações pertinentes ao pleito, comunicando previamente às unidades impactadas.
Art. 25. Os casos omissos serão resolvidos pela Comissão de Segurança da Informação (CSI) do TSE.
Art. 26. A revisão desta portaria ocorrerá a cada 3 (três) anos ou sempre que se fizer necessário ou conveniente para o TSE.
Art. 27. 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. 28. Esta portaria entra 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 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=1706299&crc=0E4CBC63, informando, caso não preenchido, o código verificador 1706299 e o código CRC 0E4CBC63.
2020.00.000004513-0

PORTARIA TSE Nº 455 DE 13 DE JULHO DE 2021.

Institui norma de configuração segura de ambientes, relativa à Política de Segurança da Informação 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 (ENTIC-JUD), e 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,
RESOLVE:
Capítulo I
DISPOSIÇÕES PRELIMINARES
Art. 1º Fica instituída a norma de configuração segura de ambientes, em consonância com a Política de Segurança da Informação do Tribunal Superior Eleitoral (TSE).
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 8 de julho de 2021.
Capítulo II
DA PREPARAÇÃO DA INSTALAÇÃO