Tribunal Regional Eleitoral de Goiás

Secretaria Judiciária

Coordenadoria de Gestão da Informação

Seção de Legislação e Editoração

PORTARIA N° 78/2022 - DG

Institui norma de uso aceitável de ativos de TI relativa à Política de Segurança da Informação do Tribunal Regional Eleitoral de Goiás.

O DIRETOR-GERAL DO TRIBUNAL REGIONAL ELEITORAL DE GOIÁS, no uso das atribuições que lhe são conferidas pelo artigo 46, inciso II, da Resolução TRE/GO n° 275, de 18 de dezembro de 2017 (Regulamento Interno), alterada pela Resolução TRE-GO nº 349/2021,

CONSIDERANDO o disposto na Resolução CNJ nº 370, de 28 de janeiro de 2021, que institui a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTICJUD);

CONSIDERANDO o disposto na Resolução TSE nº 23.644, de 1º de julho de 2021, que institui a Política de Segurança da Informação (PSI) no âmbito da Justiça Eleitoral;

CONSIDERANDO a instrução contida no SEI nº 22.0.000000042-0;

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 Regional Eleitoral de Goiás, Resolução TRE-GO nº 355/2021.

Art. 2º Para os efeitos da Política de Segurança da Informação do TRE-GO, 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 Tecnologia da Informação (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 (tela do computador com todos sistemas e aplicativos abertos) sempre que se ausentar dela;

V - efetuar fechamento (logoff) da conta de acesso ao final do uso;

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;

X - proteger as informações institucionais, evitando o risco de imagem, diante de possível percepção negativa do TRE-GO por parte dos agentes externos e cidadãos em decorrência do mau uso dos ativos de TI.

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.

§ 1º Os direitos de acesso devem ser solicitados por meio da Central de Serviços da Secretaria de Tecnologia da Informação (STI), segundo orientações da unidade responsável pelo atendimento ao usuário.

§ 2º 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 da Central de Serviços, informando os sistemas ou serviços de informação a serem acessados e o perfil de acesso que o usuário deverá possuir.

§ 3º É de responsabilidade da chefia imediata da unidade de lotação do usuário solicitar a exclusão ou a alteração de direitos de acesso aos recursos computacionais do Tribunal por meio da Central de Serviços, informando quais os acessos do usuário aos sistemas ou serviços de informação devem ser retirados ou alterados.

§ 4º Quando se tratar de Juízes Eleitorais ou Juízes Membros, a responsabilidade pela solicitação tratada no parágrafo anterior será da chefia do cartório ou assessor de gabinete, conforme o caso.

§ 5º Caberá à Secretaria de Gestão de Pessoas comunicar, mensalmente, à Secretaria de Tecnologia da Informação, as ocorrências de desligamentos permanentes de servidores em exercício neste Regional, requisitados e estagiários, bem como o afastamento em caso de licença por interesse particular.

§ 6º Em se tratando de colaboradores contratados por empresas de terceirização de serviços, caberá ao gestor do contrato, a comunicação dos desligamentos à Secretaria de Tecnologia da Informação.

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, ou mecanismo token 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 de dados gravados em estações de trabalho e dispositivos móveis (notebooks, smartphones, tablets, entre outros) é de responsabilidade exclusiva do próprio usuário.

Parágrafo único. Em caso de defeito no dispositivo de armazenamento local, que

resulte na perda de dados profissionais ou particulares, que eventualmente não sejam recuperados pela equipe de suporte da STI, em hipótese alguma será liberado para recuperação em empresas especializadas, de modo a preservar a confidencialidade dos dados institucionais.

Art. 11. A cópia de segurança de dados institucionais 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 software 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 controle patrimonial ou 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 justificar a sua prática ou dela depender, 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 TRE-GO;

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 TRE-GO, 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 Gestão da Tecnologia da Informação (CTGTI).

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 CTGTI, 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 TRE-GO.

§ 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 TRE-GO resultante da violação ao disposto neste artigo sujeitará o usuário responsável às penalidades administrativas, cíveis e penais 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 à Secretaria de Tecnologia da Informação, por meio de formulário de abertura de chamado, 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 TRE-GO, 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 TRE-

GO 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, dados pessoais, 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 pelo Comitê/Comissão de Segurança da Informação (CSI) do TRE-GO.

Art. 26. A revisão desta portaria ocorrerá a cada 3 (três) anos ou sempre que se fizer necessário ou conveniente para o TRE-GO.

Art. 27. O descumprimento desta portaria deve ser imediatamente registrado como incidente de segurança e comunicado ao Comitê/Comissão de Segurança da Informação para apuração e consequente adoção das providências cabíveis.

Art. 28. Esta portaria entra em vigor na data de sua publicação.

Goiânia, 06 de junho de 2022.

Wilson Gamboge Júnior

Diretor Geral