Atos da Presidência

TRIBUNAL DE JUSTIÇA

INSTRUÇÃO NORMATIVA Nº 07/2018

Estabelece normas para o acesso à Internet no âmbito do Poder Judiciário do Estado do Paraná.

O PRESIDENTE DO TRIBUNAL DE JUSTIÇA DO ESTADO DO PARANÁ, no uso de suas atribuições legais e regimentais, especialmente a estabelecida no artigo 14, inciso III, do Regimento Interno do Tribunal de Justiça do Estado do Paraná;

CONSIDERANDO as diretrizes traçadas por meio do Decreto Judiciário nº 631/2016, que dispõe sobre a Política de Segurança de Tecnologia da Informação - PSTI - do Poder Judiciário do Estado do Paraná;

CONSIDERANDO que a Internet é uma ferramenta fundamental para a função administrativa e a prestação jurisdicional, sendo necessário o alinhamento às normas, regulamentações e melhores práticas quanto ao seu uso, visando a proteção do ambiente tecnológico do TJPR bem como o correto direcionamento e dimensionamento de seus recursos;

CONSIDERANDO o teor do expediente eletrônico SEI nº 0029904-96.2017.8.16.6000;

R E S O L V E :

CAPÍTULO I
DO OBJETIVO

Art. 1º. A presente Instrução Normativa visa estabelecer diretrizes e padrões para o acesso à Internet no âmbito do Poder Judiciário do Estado do Paraná - PJPR.

CAPÍTULO II
DOS CONCEITOS E DEFINIÇÕES

Art. 2º. Para efeito desta Instrução Normativa, fica estabelecido o significado dos seguintes termos e expressões:

I - Aplicações peer-to-peer (ponto-à-ponto): Aplicações que tem como característica conectar e oferecer conexão, para troca de conteúdo, com outros usuários da mesma tecnologia, geralmente sem controle de conexão;

II - Autenticação: Ato de identificação do usuário no sistema de segurança;

III - Banda de Tráfego ou Transferência: Quantidade de dados trocados ou em trânsito na rede;

IV - Criptografia: Tecnologia utilizada para codificar as informações impossibilitando seu entendimento/leitura, cuja reversão ocorre somente com a utilização de uma senha previamente conhecida e/ou dispositivo criptográfico;

V - Disponibilidade: Propriedade de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade;

VI - Download/Upload: Transferência de uma informação que se encontra em rede;

VII - Gerenciamento remoto: Tecnologia que oferece a uma pessoa ou sistema controle à um dispositivo remoto;

VIII - Gestor da unidade: Magistrado e/ou chefia imediata responsável pela unidade;

IX - Grupo de controle: Agrupamento de usuários para o qual são aplicadas restrições e/ou liberações de acesso conforme alguma definição;

X - Hacking: Ação ou conhecimento utilizado para obter soluções e efeitos que extrapolam os limites normais dos sistemas e serviços, muitas vezes desviando limites impostos para o uso dos mesmos;

XI - Incidente de Segurança: evento adverso, confirmado ou sob suspeita, relacionado à segurança das autoridades judiciais, da informação ou dos sistemas de computação ou das redes de computadores;

XII - Integridade: Propriedade de salvaguarda da inviolabilidade do conteúdo da informação na origem, no trânsito e no destino;

XIII - Mascaramento: Característica de uso de algum recurso para ocultar a real intenção da ação;

XIV - Malware (código malicioso): Programa indesejado desenvolvido com a finalidade de executar ações danosas ou atividades maliciosas em um computador ou sistema;

XV - Porta de comunicação: conexão virtual que pode ser usada na transmissão de dados, identificada por um número;

XVI - Protocolo de rede: convenção que controla e possibilita uma conexão, comunicação, transferência de dados entre dois sistemas computacionais;

XVII - Proxy: Serviço responsável por intermediar acesso à internet;

XVIII - Proxy Externo: Serviço responsável por intermediar o acesso à internet não administrado pelo TJPR, possibilitando mascarar o acesso realizado;

XIX - Rede corporativa: Rede de conexão entre dispositivos de TIC administrada pelo TJPR;

XX - Limite de banda ou de tráfego: Limitação de velocidade na troca de informações entre dispositivos em uma conexão de rede;

XXI - Serviço privado de acesso à Internet: Conexão com a internet fornecida por terceiros sem vínculo com o DTIC;

XXII - Sistema de segurança: Ferramenta, sistema ou serviço utilizado para monitorar, bloquear ou controlar o uso de um recurso de TIC visando garantir a segurança;

XXIII - Site: Conjunto de páginas web organizadas a partir de um endereço básico e geralmente armazenadas hierarquicamente nesse endereço;

XXIV - Situação de Contingência: Estado ou condição de falha/problema que reduz a capacidade dos recursos de TIC que suportam a atividade da organização;

XXV - Streaming de vídeo/áudio: Método de transmissão de informações que permite executar vídeo ou áudio durante o download do conteúdo;

XXVI - Unidade: Segmento organizacional destinado para o desempenho de uma atividade específica;

XXVII - Usuário: Pessoa que usa o serviço ou recurso de TIC;

XXVIII - VPN (Virtual Private Network): Serviço ou sistema que permite conexão criptografada entre a rede corporativa e um computador fora desta;

CAPÍTULO III
DA ABRANGÊNCIA

Art. 3º. A presente Instrução Normativa deve ser cumprida por todos os usuários que utilizam acesso à internet provido pelo TJPR.

CAPÍTULO IV
DA UTILIZAÇÃO DA INTERNET

Art. 4º. O acesso à internet, quando conectado à rede corporativa, deverá ser realizado exclusivamente através de sistemas de segurança providos e configurados pelo DTIC.

Parágrafo único: É proibida a realização de conexões à internet que venham a contornar os sistemas de segurança providos pelo DTIC.

Art. 5º. Nas unidades administrativas e judiciais estatizadas o acesso à internet deverá ser realizado exclusivamente através da rede corporativa.

Parágrafo único: É proibido o uso de serviços privados de acesso à internet nestas unidades.

Art. 6º. O acesso à internet é para uso nas atividades relacionadas ao trabalho, observado o disposto nesta norma.

Parágrafo único: Eventuais exceções serão disciplinadas em ato da Supervisão Geral de Informática e Comunicação.

Art. 7º. A categorização do conteúdo acessado ou identificação de aplicações é realizada automaticamente através de ferramenta adquirida para essa finalidade.

Art. 8º. O acesso à internet se realizará:

I - Com autenticação, podendo ser personalizado;

II - Sem autenticação, seguindo regras específicas.

Art. 9º. A personalização do acesso à internet é realizada individualmente pelo gestor da unidade, através do Sistema de Atendimento a Usuários - SAU.

Art. 10. A gerência de acesso à internet é realizada por meio de grupos de controle disponibilizados pelo DTIC.

Parágrafo único: Compete ao DTIC criar/alterar/excluir grupos de controle de acesso, de acordo com a demanda, desuso ou alteração no *modus operandi* no controle de acesso.

Art. 11. Serão bloqueados, através de ferramenta de filtro de conteúdo:

I - Acesso a conteúdo impróprio, adulto, jogos, hacking, malwares, ilegal e sites categorizados como suspeitos e maliciosos;

II - Aplicações peer-to-peer (P2P);

III - Conexão com VPN, proxy e gerenciamento remoto não homologados pelo DTIC;

IV - Sites e/ou sistemas configurados fora das portas de comunicação padrão definidas nos protocolos de rede.

Art. 12. Excepcionalmente será permitida a liberação do conteúdo prevista no artigo anterior através da inclusão do usuário no grupo "Libera Conteúdo Ilegal".

§ 1º. A liberação será solicitada através do SAU, devidamente justificado o motivo do acesso ao conteúdo;

§ 2º. O conteúdo bloqueado será liberado por 24 horas.

§ 3º. Conteúdo considerado malicioso e prejudicial à segurança da rede corporativa não será liberado em nenhuma hipótese.

Art. 13. As liberações de acesso permanente a conteúdo bloqueado, quando necessário ao desempenho das atribuições funcionais, deverá atender ao disposto no § 1º do artigo anterior.

Parágrafo único: Poderão ser encaminhadas para apreciação do Comitê de Segurança da Informação as solicitações que o DTIC considerar necessárias.

Art. 14. Constitui acesso indevido à internet qualquer das seguintes ações:

I - Acessar páginas de conteúdo considerado ofensivo, ilegal, impróprio ou incompatível com as atividades funcionais ou com a política de segurança da informação, tais como pornografia, pedofilia, racismo, jogos, páginas de distribuição de conteúdo ilegal e de compartilhamento de software.

II - Acessar sites que representem ameaça de segurança ou que possam comprometer de alguma forma a integridade, confidencialidade ou disponibilidade dos recursos de TIC.

III - Acessar ou fazer download de arquivos não relacionados ao trabalho, em especial músicas, imagens, vídeos, jogos e programas de qualquer tipo.

IV - Uso de software e serviços de mascaramento.

CAPÍTULO V
DO DESEMPENHO DO ACESSO À INTERNET

Art. 15. Poderão ser adotadas medidas, a critério do DTIC, visando a manutenção da disponibilidade e desempenho do acesso aos sistemas, seja em situações normais de funcionamento, seja em situações de contingência, tais como:

I - Bloqueios totais ou parciais de acessos a determinados sites e serviços;

II - Priorização de acessos a determinados sites e serviços;

III - Limitação de tráfego.

Parágrafo único: Quando implementadas em situação de contingência, as medidas serão comunicadas através da intranet.

Art. 16. O DTIC não garantirá desempenho ao acesso a sites de internet externos.

CAPÍTULO VI

DO MONITORAMENTO E AUDITORIA

Art. 17. O acesso à internet será controlado e inspecionado, de forma automática ou manual, através dos sistemas de segurança, configurados de acordo com esta Instrução Normativa.

Art. 18. Os registros de acessos à internet serão arquivados e utilizados, exclusivamente, para fins de auditoria de incidentes de segurança do acesso à internet.

Parágrafo único: Os registros não se prestam para fins de análise de produtividade no trabalho e controle de ponto.

Art. 19. Os arquivos de auditoria serão armazenados pelo período mínimo de 6 meses, até regulamentação em norma específica.

Art. 20. Os incidentes de segurança do acesso à internet devem ser relatados via Sistema Eletrônico de Informações - SEI, até regulamentação em norma específica, com as seguintes informações:

I - Identificação do recurso de TIC.

II - Identificação dos usuários envolvidos.

III - Horário da identificação do incidente.

IV - Intervalo de tempo da suspeita do incidente.

V - Descrição do incidente de segurança contendo:

a - Eventos que motivaram o relato;

b - Pessoas envolvidas;

c - Criticidade da informação;

d - Eventos correlacionados que possam estar envolvidos no incidente;

e - Demais informações pertinentes.

Art. 21. O DTIC poderá efetuar inspeção de conteúdo criptografado das conexões com sites considerados maliciosos, suspeitos ou não categorizados, a fim de proceder análise de conteúdo para garantir, de forma automatizada, a aplicação desta Instrução Normativa.

Art. 22. Poderá ser realizada a inspeção de conteúdo criptografado, com objetivo de obter informações de auditoria para incidentes de segurança, desde que autorizado pelo Supervisor Geral de Informática e Comunicação, observada a legislação vigente.

CAPÍTULO VII

DAS COMPETÊNCIAS E RESPONSABILIDADES

Art. 23. É responsabilidade do usuário:

I - Relatar qualquer incidente de segurança, mesmo quando não envolvido;

II - Fazer o bom uso do acesso à internet.

Art. 24. É competência do gestor da unidade:

I - Gerir bloqueios e liberações de seus subordinados;

II - Solicitar alterações de liberações ou bloqueios não contemplados pelos padrões de grupos de controle criados, conforme definido no Art. 13;

III - Orientar os usuários sob sua responsabilidade a respeito do uso adequado do recurso de internet, conforme as regras estabelecidas nesta Instrução Normativa, bem como reportar ao DTIC ou Comitê de Segurança da Informação o seu descumprimento.

CAPÍTULO VII

DOS DOCUMENTOS RELACIONADOS

Art. 25. Na elaboração desta Instrução Normativa foram utilizados os seguintes documentos:

I - PSTI-TJPR - Política de Segurança de Tecnologia da Informação;

II - NS-008.0 - Registro de eventos de TIC.

Art. 26. Para a aplicação desta Instrução Normativa é necessário a utilização dos Procedimentos de Segurança abaixo relacionados:

I - Gerência de bloqueio e liberação de acesso dos usuários;

II - Solicitação de grupos de controle;

III - Consulta aos padrões de bloqueios e liberações;

IV - Solicitação de bloqueio e liberação permanente;

V - Aplicação de medidas para garantir disponibilidade e desempenho;

VI - Informação de incidente de segurança do acesso à Internet;

VII - Armazenamento dos arquivos de auditoria de acesso à Internet.

CAPÍTULO IX

DA PERIODICIDADE DE REVISÕES

Art. 27. O disposto na presente Instrução Normativa será atualizado sempre que houver alterações significantes na arquitetura e/ou tecnologia referente, observada, ainda, a periodicidade prevista para a revisão da Política de Segurança da Informação.

Art. 28. Esta Instrução Normativa entrará em vigor a partir de sua publicação.

PUBLIQUE-SE. CUMPRA-SE.

Curitiba, 26 de junho de 2018.

DES. RENATO BRAGA BETTEGA
Presidente do Tribunal de Justiça do Estado do Paraná