



MINISTÉRIO PÚBLICO DO TRABALHO
COMITÊ ESTRATÉGICO DE TECNOLOGIA DA INFORMAÇÃO – CETI
SAUN Quadra 5, Lote C, Torre A- Brasília - DF - CEP 70040-250
Telefone: (61) 3314-8579 – e-mail: mpt.ceti@mpt.mp.br

Resolução CETI n.º 5, de 7 de março de 2016.

Disciplina o uso dos recursos de Tecnologia da Informação no Ministério Público do Trabalho conforme diretrizes da Política de Segurança da Informação.

O COMITÊ ESTRATÉGICO DE TECNOLOGIA DA INFORMAÇÃO (CETI) do Ministério Público do Trabalho, no uso das atribuições que lhe conferem a Portaria n.º 723, de 9 de setembro de 2015;

CONSIDERANDO que, de acordo com a Resolução CNMP n. 70, compete ao CETI definir padrões de funcionamento, integração, qualidade e segurança dos serviços e sistemas de Tecnologia da informação;

CONSIDERANDO a necessidade de aprimorar os padrões de governança em Tecnologia da Informação no Ministério Público do Trabalho;

CONSIDERANDO as diretrizes da resolução n.º 4, de 7 de março de 2016, que institui a Política Nacional de Segurança da Informação do Ministério Público do Trabalho;

CONSIDERANDO a necessidade de estabelecer mecanismos de controle que garantam o uso adequado dos recursos de Tecnologia da Informação no âmbito institucional e, nesse sentido, a necessidade de definir e implementar parâmetros, procedimentos e instrumentos que orientem a forma de uso adequado dos recursos de Tecnologia da Informação, em consonância com o interesse institucional;

CONSIDERANDO a importância do uso dos recursos de Tecnologia da Informação como ferramenta de apoio para a manutenção dos processos de trabalho e a geração do conhecimento no âmbito institucional.

CONSIDERANDO os padrões ISO/IEC 27.000 (*Information Technology - Security Techniques - Information Security Management Systems - Overview and Vocabulary*), ABNT/NBR ISO/IEC 27.001 (Tecnologia da informação - Técnicas de segurança - Sistema de gestão da segurança da informação – Requisitos) e ABNT/NBR ISO/IEC 27.002 (Tecnologia da informação - Técnicas de segurança - Código de prática para controles de segurança da informação).

RESOLVE

Art. 1º Disciplinar o uso dos recursos de Tecnologia da Informação no âmbito do Ministério Público do Trabalho, nos termos desta resolução.

§ 1º O uso dos recursos de Tecnologia da Informação do MPT por membros, servidores e colaboradores deverá respeitar os interesses institucionais e da sociedade, com respeito



à lei, aos requisitos de segurança da informação e a diretrizes de eficiência e de governança.

§ 2º Para efeito do disposto nesta resolução, o conjunto de recursos de Tecnologia da Informação (TI) compreende os bens, sistemas e serviços que compõem a arquitetura tecnológica do MPT e o ambiente no qual a informação é criada, manipulada, transmitida, armazenada e descartada.

CAPÍTULO I

Das Regras Gerais

Art. 2º Os procedimentos de administração, instalação, configuração, operação e manutenção dos recursos de TI são de responsabilidade do Departamento de Tecnologia da Informação da Procuradoria Geral do Trabalho (TI-PGT) e, respeitados os padrões nacionais, das áreas de TI nas Procuradorias Regionais do Trabalho e nas Procuradorias do Trabalho nos Municípios (TI-Regional).

§ 1º Os procedimentos referidos no caput deverão ser progressivamente homologados em rotinas padronizadas de âmbito nacional.

§ 2º A execução dos procedimentos descritos neste artigo em equipamentos particulares ou de terceiros é proibida, ressalvada a necessidade de realização de atividades de interesse institucional, desde que respeitados os padrões nacionais previamente documentados.

§ 3º Não havendo orientação técnica para a hipótese prevista no § 2º, a TI-PGT elaborará documentação e providenciará sua ampla divulgação como rotina de suporte, consoante resolução CETI n.º 2/2016.

Art. 3º O uso dos recursos de TI será destinado ao apoio de membros e servidores e colaboradores do MPT na realização de suas atividades institucionais e funcionais:

§ 1º É proibido o uso de recursos de TI:

I. Em atividades de natureza particular;

II. Para exercer atividades vedadas em dispositivo constitucional, legal, regulamentar ou convencional;

III. Mediante utilização de identificação que não seja a sua própria;

IV. Mediante conexão, na rede corporativa do MPT, de equipamento ou dispositivo particular ou de terceiros, ressalvada a permissão temporária expressa em decisão do



chefe da unidade, desde que fundada em necessidade institucional e em parecer prévio da TI-PGT ou da TI-Regional;

V. Para acessar, visualizar, armazenar, divulgar, manter, publicar, transmitir ou fazer utilização:

a) de qualquer material classificado como ofensivo ao princípio da urbanidade, ao decoro, à honra e à dignidade de pessoas, instituições e autoridades;

b) de músicas, vídeos, jogos, animações ou fotografias que não sejam de interesse institucional ou que causem elevado consumo de recursos computacionais na rede do MPT;

c) de mensagem com conteúdo publicitário, comercial, religioso, esportivo ou de entretenimento;

d) de conteúdo difamatório, preconceituoso, discriminatório, pornográfico ou tipificado como crime ou contravenção;

e) de redes sociais ou de relacionamentos, salvo quando necessário para a atividade institucional;

f) de conteúdo que veicule assédio moral ou sexual;

g) de conteúdo político-partidário.

VI. Acessar serviços de comunicações instantâneas não homologados como solução nacional;

VII. Acessar serviços que possam afetar a segurança ou o desempenho da rede corporativa do MPT;

VIII. Realizar transferências de arquivos, por meio de conexão ponto-a-ponto ou multiponto, em desacordo com as atividades e necessidades institucionais;

IX. Monitorar ou interceptar transmissões de dados, voz ou imagem na rede corporativa do MPT ou em qualquer outro meio de comunicação de dados, de responsabilidade institucional ou não, ressalvado o monitoramento realizado, no âmbito de suas atribuições, pela TI-PGT ou pela TI-Regional;

X. Desenvolver, manter, divulgar, utilizar ou executar aplicativos de testes ou qualquer outro programa que ofereça risco de prejuízos à disponibilidade, à integridade, à confidencialidade, à autenticidade e ao não repúdio das informações e, em geral, aos recursos de TI do MPT, ressalvadas as atividades estritamente necessárias aos fins institucionais realizadas pela TI-PGT ou, sob supervisão desta, pela TI-Regional;



XI. Utilizar aplicações não institucionais de armazenamento em nuvem, excetuadas as suas plataformas web, desde que o uso se destine a finalidade institucional;

XII. Tentar transpor ou efetivamente vulnerar mecanismos de segurança implementados para a proteção da segurança da informação ou dos recursos de TI do MPT;

XIII. Tentar alcançar ou efetivamente acessar informações de terceiros, em qualquer grau de sigilo, sem expressa autorização do proprietário, do gestor da informação ou de autoridade do MPT no exercício de suas atribuições;

XIV. Distribuir ou instalar aplicativos não homologados pela TI-PGT;

XV. Acessar, copiar, armazenar ou divulgar informações de propriedade do MPT, em qualquer grau de sigilo, ainda que sob sua tutela, sem autorização formal do gestor da informação;

XVI. Utilizar os servidores de arquivos corporativos para armazenar conteúdos que excedam os limites de armazenamento previamente definidos pelo gestor da TI-Regional, respeitados os padrões nacionais.

§ 1º As prescrições desta Resolução se aplicam, no que couber, aos contratos de prestação de serviço de hospedagem de recursos de TI em ambientes fora das dependências das unidades do MPT.

§ 2º A TI-PGT, a TI-Regional ou as equipes nacionais designadas, conforme o caso, deverão:

I. Limitar, bloquear ou neutralizar qualquer uso de recursos de TI em desconformidade com esta Resolução;

II. Utilizar ferramentas automatizadas de monitoramento e análise estatística e heurística que forneçam subsídios para as decisões de limitação, bloqueio ou neutralização referidas no inciso I.

CAPÍTULO II

Do Uso de Dispositivos Móveis

Art. 4º O uso de dispositivos móveis funcionais fornecidos pelo MPT respeitará o interesse institucional.



§1º Consideram-se dispositivos móveis funcionais os computadores portáteis, tablets, smartphones e equipamentos similares fornecidos pelo MPT a membros, servidores ou colaboradores.

§2º A conexão de dispositivos móveis funcionais à rede corporativa será realizada exclusivamente via autenticação criptografada de credencial pessoal e intransferível.

§3º Será utilizada, para a conexão de dispositivos móveis funcionais, a rede sem fio da unidade, em segmento de rede local exclusivo para tal fim e protegido por firewall.

§4º No caso de equipamentos que possuam conexão para rede cabeada, o acesso dependerá de autorização prévia da TI-PGT ou da TI-Regional, conforme o caso, desde que esses sejam os únicos recursos disponíveis ao membro ou ao servidor para acessar a rede corporativa do MPT.

§5º O método de autenticação do dispositivo móvel à rede corporativa do MPT deverá registrar, no mínimo, a data e a hora da conexão, a identificação do usuário, o endereço IP, a data e a hora da desconexão e a situação do dispositivo no que tange ao pertencimento ao domínio institucional.

§6º O uso de dispositivos móveis particulares do tipo tablet ou smartphone, com consumo de recursos da rede corporativa do MPT, será permitido desde que a utilização se limite a aplicações e sistemas relacionados à atividade institucional.

Art. 5º A TI-PGT e a TI-Regional, em coordenação, utilizarão mecanismos de detecção e prevenção de acessos intrusos.

§ 1º Os mecanismos de detecção e prevenção de acessos intrusos devem ser configurados para inspecionar conexões oriundas de dispositivos móveis, bloqueando-as sempre que necessário para evitar vulneração das diretrizes e normas de segurança do MPT, sobretudo em relação à ocorrência de:

I. Eventos classificados, pelos mecanismos de detecção e prevenção, com gravidade alta ou média;

II. Eventos classificados com gravidade baixa e posteriormente ratificados pela área de TI da unidade do MPT como eventos potencialmente danosos aos sistemas e serviços da rede corporativa;

III. Eventos que causem alto consumo dos recursos de TI e que prejudiquem a disponibilidade de sistemas e serviços corporativos.

§ 2º A TI-PGT e a TI-Regional estão autorizadas a efetuar manualmente os bloqueios definidos neste artigo nos casos em que se verificar lacunas de operação nos mecanismos automáticos.



CAPÍTULO III

Dos Acessos Remotos

Art. 6º Os acessos remotos realizados a partir da internet para a rede corporativa do MPT só poderão ser ultimados por intermédio de programas ou serviços que garantam a autenticação dos usuários e a criptografia dos dados nas camadas de rede, transporte ou aplicação, conforme arquiteturas e modelos de comunicação adotados nacionalmente pelo MPT, em modalidades nas quais:

I. a máquina remota se conecte à rede MPT por meio de um circuito privado virtual com recebimento de endereçamento interno e demais parâmetros da rede, de modo que o usuário tenha a experiência de utilizar seu equipamento como se estivesse na rede interna.

II. a máquina remota se conecte a um ambiente de área de trabalho virtual existente na rede corporativa do MPT, de modo que o usuário tenha a experiência de utilizar diretamente essa área de trabalho como se estivesse na rede interna.

III. um programa instalado na máquina remota do usuário acesse um servidor interno na rede corporativa do MPT, proporcionando ao usuário a experiência de utilizar a interface de linha de comando como se estivesse acessando diretamente o console do servidor interno.

§1º Os requisitos de acesso nas modalidades descritas nos incisos I e II serão definidos pelo Comitê Estratégico de Tecnologia da Informação (CETI).

§2º A modalidade de acesso descrita no inciso III será realizada exclusivamente por servidores da TI-PGT ou da TI-Regional, desde que previamente autorizados pelo respectivo dirigente, considerada a natureza da atividade especializada a ser desempenhada.

§3º O método de autenticação, em qualquer modalidade, deverá registrar, no mínimo, a data e a hora da conexão, a identificação do usuário, o endereço IP, a data e a hora da desconexão e a situação do dispositivo no que tange ao pertencimento ao domínio institucional.

§4º No caso da modalidade I, deve-se alocar um bloco de endereços IP específicos para atribuí-los às máquinas que realizarão o acesso remoto.

§5º Em razão dos riscos inerentes ao serviço de acesso remoto, todas as conexões realizadas por meio das modalidades descritas neste artigo deverão se sujeitar a filtragem via firewall, com regras específicas padronizadas em âmbito nacional.

§6º O acesso remoto será realizado por intermédio de computador ou dispositivo móvel funcional ou de uso particular do membro ou servidor.



§7º É proibida a instalação dos programas e aplicativos de acesso remoto em computadores e dispositivos de uso público ou de outras instituições.

CAPÍTULO IV

Dos Serviços de Correio Eletrônico e de Comunicação Instantânea

Art. 7º O serviço de correio eletrônico do MPT será administrado pela TI-PGT com a finalidade de manter instrumento de troca de mensagens digitais a serem armazenadas nos seguintes tipos de caixas postais:

I. Funcionais, com acesso concedido à pessoa física do membro ou servidor e identificada, para autenticação, de acordo com as informações constantes do serviço de diretório corporativo institucional;

II. Setoriais, com a função servir a necessidades de áreas das unidades do MPT, com acesso concedido a um ou mais usuários, devidamente identificados, cadastrados no serviço de diretório corporativo institucional;

§1º As caixas postais funcionais devem ser utilizadas exclusivamente para fins institucionais, vedada a troca de mensagens pessoais.

§2º A criação de caixas setoriais dependerá de pedido formal do chefe da respectiva área, mediante abertura de chamado em serviço de atendimento da TI-PGT, nos termos da Resolução CETI n.º 2/2016.

§3º Serão criadas, em caráter complementar, listas de distribuição e listas de discussão, no interesse da instituição, com endereço no domínio mpt.mp.br, respeitadas as limitações de licenciamento da plataforma tecnológica que suporta o serviço.

§4º O funcionamento do serviço de correio eletrônico deverá ser otimizado de modo que mecanismos de detecção de mensagens indesejadas – maliciosas ou enviadas em lote, em rajadas ou em massa – sejam configurados para redirecionamento desse conteúdo para áreas de quarentena ou de retenção e de forma a permitir que o usuário possa oportunamente acessá-las, respeitada a capacidade operacional da plataforma tecnológica que suporta o serviço.

§5º O serviço de correio eletrônico tramitará mensagens sob o domínio público “@mpt.mp.br”, registrado no Comitê Gestor da Internet no Brasil.

Art. 8º Para garantir a disponibilidade e a integridade das informações trafegadas e armazenadas no sistema de correio eletrônico do MPT, o CETI definirá, mediante parecer técnico da TI-PGT, os seguintes limites para os parâmetros de configuração do sistema:

I. tamanho máximo das caixas postais;



II. quantidade máxima de arquivos anexados por mensagem;

III. tamanho máximo de anexos de mensagens;

IV. quantidade máxima de destinatários por mensagem.

§1º O parecer prévio da TI-PGT deverá observar as melhores práticas definidas pelo fabricante ou desenvolvedor da solução tecnológica do sistema de correio eletrônico, bem como os limites de processamento e armazenamento da infraestrutura corporativa de produção do MPT.

§2º Em virtude de requisitos técnicos e de limites de armazenamento, a TI-PGT não se responsabilizará pela disponibilidade permanente e ilimitada de arquivos recebidos ou enviados com mais de 2 (dois) anos.

§3º O usuário de caixas postais funcionais ou setoriais deverá, periodicamente, armazenar arquivos de seu interesse em sua estação de trabalho ou nos servidores de arquivos corporativos disponibilizados pela TI-PGT ou pela TI-Regional.

§4º A TI-PGT, sempre que necessário, poderá, mediante comunicado geral com antecedência mínima de 60 (sessenta dias), realizar operações de arquivamento definitivo de mensagens que possuam mais de 2 (dois) anos.

§5º Após o arquivamento definitivo de mensagens, a recuperação de seus conteúdos deverá ocorrer apenas mediante requerimento fundamentado a ser examinado pelo CETI.

§6º A TI-PGT e a TI-Regional MPT não se responsabilizarão por problemas de funcionamento derivados do uso do serviço de correio eletrônico em desconformidade com o que estipula esta Resolução.

§7º O conteúdo relevante de arquivos intercambiados em listas de discussões de membros deverá ser semestralmente indexado em ferramentas de busca institucionais que permitam seu fácil acesso no âmbito da rede corporativa do MPT.

Art. 9º Respeitados os limites estabelecidos pelo artigo 3º desta Resolução, é proibido:

I. Cadastrar ou utilizar o endereço de correio eletrônico funcional ou setorial como informação pessoal em serviços eletrônicos, existentes na internet, com fins particulares;

II. Persistir na tentativa de envio de mensagens que, consoante notificações de alerta recebidas, excedam os limites estabelecidos para o bom funcionamento do sistema de correio eletrônico;

III. Enviar como anexos quaisquer arquivos cujos tipos sejam bloqueados pelo administrador do serviço de correio eletrônico;



IV. Fornecer a sindicatos, associações ou órgãos de classe os endereços de listas de distribuição ou listas de discussão de membros ou servidores;

V. Fornecer a serviços de divulgação de mensagens em massa (spam) os endereços de correio funcional ou setorial ou os endereços de listas de distribuição ou discussão institucionais;

VI. Encaminhar a terceiros ou fazer uso indevido de mensagens recebidas por engano em caixas postais funcionais ou setoriais;

VII. Tentar utilizar ou efetivamente fazer uso do servidor de correio eletrônico do MPT como ponto de encaminhamento (relay) de mensagens cujos endereços de origem ou destino não sejam do MPT;

VIII. Utilizar programas clientes de correio eletrônico diferente dos homologados pela TI-PGT;

§ 1º Consideram-se serviços eletrônicos, para os fins do inciso I, as ferramentas, os sítios ou os portais de relacionamento, pornografia, comércio eletrônico, jogos, entretenimento, transferências de arquivos ou qualquer outro que dependa do uso do endereço eletrônico como forma de acesso, credenciamento ou identificação pessoal;

§ 2º Consideram-se indesejados, para os fins do inciso III, arquivos executáveis, scripts autoexecutáveis ou qualquer outro conteúdo que apresente risco para a rede, para os serviços ou para os sistemas corporativos do MPT;

§ 3º Os sindicatos, associações ou órgãos de classe que representem membros ou servidores poderão ser autorizados a enviar mensagens a seus sindicalizados ou associados mediante pedido formal dirigido à TI-PGT, desde que identificada a pessoa responsável pelo envio e o endereço de origem.

Art. 10 O serviço de comunicação instantânea do MPT será administrado pela TI-PGT com a finalidade de manter instrumento de diálogo em tempo real no interesse das atividades institucionais de membros, servidores e colaboradores.

§1º A comunicação instantânea ocorrerá por meio de mensagens de texto ou pelo compartilhamento de imagens, áudio, vídeo e recursos computacionais.

§2º O serviço de comunicação instantânea será mantido em integração com o serviço correio eletrônico mediante compartilhamento da mesma base de autenticação de usuários e lista de contatos.

§3º É vedado o uso de serviços de comunicação instantânea não homologados pela TI-PGT.



MINISTÉRIO PÚBLICO DO TRABALHO
COMITÊ ESTRATÉGICO DE TECNOLOGIA DA INFORMAÇÃO – CETI
SAUN Quadra 5, Lote C, Torre A- Brasília - DF - CEP 70040-250
Telefone: (61) 3314-8579 – e-mail: mpt.ceti@mpt.mp.br

§4º A aplicação padrão de comunicação instantânea será configurada para acionamento e funcionamento automático em todas as estações de trabalho do MPT, independentemente de comandos do usuário.

§ 5º A TI-PGT e a TI-Regional deverá fomentar o uso do serviço de comunicação instantânea como instrumento preferencial em relação ao uso de telefones fixos ou móveis institucionais.

CAPÍTULO V

Dos Serviços de Acesso à Internet

Art. 11 O acesso a conteúdo em hipertexto ou de transferência de arquivos na internet deve ser realizado por meio de navegadores ou aplicações análogas previamente homologadas pela TI-PGT.

§1º O acesso das estações de trabalho à internet deverá ser controlado por meio de mecanismos intermediários de verificação de conformidade às prescrições desta Resolução.

§2º A fim de otimizar o uso de recursos de TI, o CETI poderá definir grupos de usuários com perfis de acessos e permissões específicas.

§3º A TI-Regional poderá limitar a capacidade de dados do circuito de comunicação com serviços na Internet para garantir o funcionamento dos serviços e sistemas corporativos no âmbito de sua circunscrição.

§ 4º O monitoramento do uso dos recursos deverá ser permanente, sob responsabilidade da TI-PGT, em âmbito local e nacional, e pela TI-Regional, em âmbito local.

§ 5º Serão desenvolvidos mecanismos de alertas automáticos que desencadeiem medidas saneadoras diante de cenários críticos.

§ 6º A restrição de conteúdo, em âmbito nacional, deverá respeitar as diretrizes fixadas pelo CETI.

CAPÍTULO VI

Das Responsabilidades Gerais

Art. 12 Constitui responsabilidade do CETI a promoção do aprimoramento constante da política de uso de recursos de TI do MPT e do monitoramento de sua efetividade.

Art. 13. Incumbe à TI-PGT coordenar nacionalmente o seguimento, pela TI-Regional, dos padrões nacionais estabelecidos nesta Resolução, propondo ao CETI, sempre que



MINISTÉRIO PÚBLICO DO TRABALHO
COMITÊ ESTRATÉGICO DE TECNOLOGIA DA INFORMAÇÃO – CETI
SAUN Quadra 5, Lote C, Torre A- Brasília - DF - CEP 70040-250
Telefone: (61) 3314-8579 – e-mail: mpt.ceti@mpt.mp.br

necessário e mediante pareceres técnicos, a adoção de medidas saneadoras do uso dos recursos de TI.

Art. 14. É responsabilidade da TI-Regional promover o respeito aos padrões nacionais estabelecidos nesta Resolução, comunicando à TI-PGT, na forma da resolução CETI n.º 2/2016, todas as não conformidades detectadas no âmbito de sua circunscrição.

CAPÍTULO VII

Das Disposições Finais e Transitórias

Art. 15 Os pedidos de aplicação de exceções às vedações definidas nesta norma devem ser encaminhados, pelo dirigente da TI-Regional, com a devida fundamentação, ao Diretor da TI-PGT, que submeterá ao CETI na primeira reunião subsequente ao requerimento.

§ 1º Os pedidos oriundos da Procuradoria Geral do Trabalho deverão ser dirigidos ao Diretor da TI-PGT, que submeterá ao CETI na primeira reunião colegiada subsequente ao requerimento.

§ 2º Os pedidos urgentes serão apreciados pelo Presidente do CETI, *ad referendum* do Comitê.

Art. 16 No prazo de 90 (noventa) dias a contar da publicação desta Resolução, a TI-Regional e a TI-PGT submeterá ao CETI um relatório de não conformidades aos padrões estabelecidos, com o respectivo cronograma de ajustamento.

Art. 17 Os casos omissos serão resolvidos pelo CETI, em Nota Técnica, ouvidos os interessados.

Art. 18 Esta resolução entra em vigor na data de sua publicação.

Luis Fabiano de Assis
Procurador do Trabalho
Presidente do Comitê Estratégico de Tecnologia da Informação do MPT