

Portaria nº 4.772, de 23 de setembro de 2008.

Institui a Política de Segurança da Informação no âmbito do Tribunal Regional do Trabalho da 4ª Região.

O PRESIDENTE DO TRIBUNAL REGIONAL DO TRABALHO DA 4ª REGIÃO, no uso de suas atribuições legais e regimentais,

considerando a necessidade de estabelecer diretrizes e padrões para garantir um ambiente tecnológico controlado e seguro de forma a oferecer todas as informações necessárias aos processos deste Tribunal com integridade, confidencialidade e disponibilidade;

considerando que a credibilidade da instituição na prestação jurisdicional deve ser preservada;

considerando a constante preocupação com a qualidade e celeridade na prestação de serviços à sociedade;

considerando o parecer favorável da Comissão de Informática deste Tribunal, no desempenho de suas atribuições regimentais;

RESOLVE:

Art. 1º Estabelecer a Política de Segurança da Informação no âmbito do Tribunal Regional do Trabalho da 4ª Região, da qual são parte integrante todas as normas e procedimentos complementares e afins editados pelo Tribunal.

Art. 2º Para os efeitos deste Ato aplicam-se as seguintes definições:

I – Confidencialidade: Garantia de que o acesso à informação seja obtido apenas por pessoas autorizadas;

II – Integridade: Salvaguarda de exatidão e completeza da informação e dos métodos de processamento;

III – Disponibilidade: Garantia de que os usuários autorizados obtenham acesso à informação e aos recursos correspondentes sempre que necessário;

IV – Recurso de tecnologia de informação: qualquer equipamento, dispositivo, serviço, infra-estrutura ou sistema de processamento da informação, instalações físicas que os abriguem.

V – Usuários: magistrados e servidores ocupantes de cargo efetivo ou em comissão, requisitados e cedidos, desde que previamente autorizados, empregados de

empresas prestadoras de serviços terceirizados, consultores, estagiários, e outras pessoas que se encontrem a serviço da Justiça do Trabalho, utilizando em caráter temporário os recursos tecnológicos do TRT.

VI - Plano de Continuidade da Prestação dos Serviços: conjunto de ações de prevenção e procedimentos de recuperação a serem seguidos para proteger os processos críticos de trabalho contra efeitos de falhas de equipamentos, acidentes, ações intencionais ou desastres naturais significativos, assegurando a disponibilidade das informações.

Art. 3º As disposições deste Ato aplicam-se a todos os usuários de recursos de tecnologia da informação do Tribunal Regional do Trabalho da 4ª Região.

Parágrafo único – Os convênios e os contratos firmados pelo Tribunal que envolvam utilização de recursos de tecnologia da informação devem observar as disposições deste Ato.

Art. 4º O uso adequado dos recursos de tecnologia da informação visa a garantir a continuidade da prestação jurisdicional deste Tribunal.

Parágrafo único – Os recursos de tecnologia da informação pertencentes ao Tribunal Regional do Trabalho da 4ª Região, disponíveis para o usuário, serão utilizados em atividades relacionadas às suas funções institucionais.

Art. 5º A utilização dos recursos de tecnologia da informação será monitorada, com a finalidade de detectar divergências entre as normas que integram a Política de Segurança da Informação e os registros de eventos monitorados, fornecendo evidências nos casos de incidentes de segurança.

§ 1º Serão realizadas auditorias ordinárias periódicas, cujos relatórios serão encaminhados ao Comitê de Segurança da Informação.

§ 2º As auditorias extraordinárias serão realizadas com o intuito de apurar eventos que deponham contra a segurança e as boas práticas no uso dos recursos de tecnologia da informação.

Art. 6º Toda informação gerada no Tribunal será classificada em termos de seu valor, requisitos legais, sensibilidade, criticidade e necessidade de compartilhamento.

Parágrafo único – O Tribunal providenciará dispositivos de proteção proporcionais ao grau de confidencialidade e de criticidade da informação, independentemente do suporte em que resida ou da forma pela qual seja veiculada, capazes de assegurar a sua autenticidade, integridade e disponibilidade.

Art. 7º As informações, sistemas e métodos gerados ou criados pelos usuários, no exercício de suas funções, independentemente da forma de sua apresentação ou armazenamento, são propriedade do Tribunal e serão utilizadas exclusivamente para fins relacionados às atividades a ele afetas.

Parágrafo único – Quando as informações, sistemas e métodos forem gerados ou criados por terceiros para uso exclusivo do Tribunal, ficam os criadores obrigados ao sigilo permanente de tais produtos, sendo vedada a sua reutilização em projetos para outrem.

Art. 8º Será criado o COMITÊ DE SEGURANÇA DA INFORMAÇÃO, composto por

dois magistrados, um integrante da Comissão de Informática do Tribunal, que o presidirá, e um Juiz de primeiro grau indicado pela Comissão de Informática, assim como por um representante da Presidência, Corregedoria, Direção-Geral de Coordenação Judiciária, Direção-Geral de Coordenação Administrativa e Secretaria de Informática.

Art. 9º Compete ao COMITÊ DE SEGURANÇA DA INFORMAÇÃO:

I - Elaborar e submeter à Presidência do Tribunal, ouvida a Comissão de Informática, propostas de normas e políticas de uso dos recursos de informação, tais como:

- a) Classificação das informações,
- b) Gerenciamento de identidade e controle de acesso lógico,
- c) Controle de acesso físico,
- d) Controle de acesso à Internet,
- e) Utilização do correio eletrônico,
- f) Utilização de equipamentos de tecnologia da informação,
- g) Utilização de programas e aplicativos,
- h) Utilização de armazenamento lógico,
- i) Contingência e Continuidade do Negócio;

II - Rever periodicamente essa Política de Segurança e normas relacionadas sugerindo possíveis alterações;

III - Estabelecer diretrizes e definições estratégicas para a elaboração do Plano Diretor de Segurança da Informação;

IV - Dirimir dúvidas e deliberar sobre questões não-contempladas nessa política e normas relacionadas;

V - Propor e acompanhar planos de ação para aplicação dessa política, assim como campanhas de conscientização dos usuários;

VI - Receber as comunicações de descumprimento das normas referentes à Política de Segurança da Informação deste Tribunal, instruindo-as com os elementos necessários à sua análise e apresentando parecer à autoridade/órgão competente à sua apreciação;

VII - Solicitar, sempre que necessário, a realização de auditorias extraordinárias ao Escritório de Segurança da Informação, relativamente ao uso dos recursos de tecnologia da informação, no âmbito do Tribunal;

VIII - Avaliar relatórios e resultados de auditorias apresentados pelo Escritório de Segurança; e

IX - Apresentar à Administração os resultados da Política de Segurança da Informação;

Art. 10 O Escritório de Segurança da Informação, vinculado à Secretaria de Informática, tem por objetivo prover soluções de segurança que agreguem valor aos serviços prestados pelo TRT da 4ª Região, pautadas na conscientização e no

comprometimento de seus servidores para com a preservação da confidencialidade, da integridade e da disponibilidade das informações, a segurança nas operações e a excelente imagem perante a sociedade.

Art. 11 Compete ao Escritório de Segurança da Informação:

I - Elaborar um Plano Diretor de Segurança da Informação, com base nas definições estratégicas estabelecidas pelo Comitê de Segurança da Informação;

II – A gestão da Política de Segurança da Informação e do Plano de Continuidade do Negócio;

III – Fornecer subsídios para as atividades do Comitê de Segurança da Informação;

IV – Coordenar as ações do Plano Diretor de Segurança da Informação e dos projetos a ele relacionados;

V – Promover palestras e treinamentos para conscientização dos usuários e atualização das ações de segurança;

VI – Realizar análises de risco periódicas no que tange à tecnologia, ambientes, processos e pessoas;

VII – Manter os registros de monitoramento sobre o uso dos recursos de tecnologia;

VIII – Realizar auditorias ordinárias e extraordinárias, com emissão de relatórios sobre o uso dos recursos de tecnologia, apontando, quando existentes, irregularidades e não-conformidades na utilização;

IX – Coordenar as ações necessárias na ocorrência de incidentes de segurança da informação;

X – Atuar de forma coordenada com outras áreas nos assuntos de Segurança da Informação;

XI - Informar ao Comitê de Segurança da Informação:

a) Nível de segurança alcançado nos ambientes tecnológicos, por meio de relatórios gerenciais provenientes das análises de risco;

b) Incidentes de segurança tecnológica.

Art. 12 Incumbe à chefia imediata e superior do usuário verificar a observância da Política de Segurança no âmbito de sua unidade, comunicando, de imediato, ao Comitê de Segurança da Informação, as irregularidades constatadas, para as providências cabíveis.

Art. 13 O descumprimento das normas referentes à Política de Segurança da Informação deste Tribunal poderá acarretar, isolada ou cumulativamente, nos termos da legislação vigente, sanções administrativas, civis e penais.

Art.14 Fazem parte da presente Portaria os Anexos editados conforme as matérias elencadas no inciso I do art. 9º.

Art. 15 O presente Ato entra em vigor a partir da data de sua publicação

Art. 16. Fica revogada a Portaria nº 2.316, de 04.7.2001 (DOE 05.7.2001).

João Ghisleni Filho,
Presidente – TRT 4ª Região.

ANEXO 1

NSI001 – Controle de Acesso à Internet

1 Acesso à Internet

1.1 O acesso à Internet dar-se-á, exclusivamente, por intermédio dos meios autorizados, configurados pela Secretaria de Informática.

1.2 É expressamente proibido o uso de *proxies* externos ou similares.

2 Perfis de acesso

2.1 Os usuários que possuem acesso à rede do Tribunal também possuem acesso à Internet, sempre seguindo o item 3 de melhores práticas;

2.2 Prestadores de serviços terceirizados e estagiários poderão ter acesso à Internet durante o período de prestação dos serviços, observando as normas aqui enumeradas, desde que seja formalmente solicitado e justificado pelo responsável da área onde está sendo prestado o serviço terceirizado ou estágio.

3 Melhores práticas

3.1 Qualquer acesso à Internet partindo de computadores situados nas unidades deste Tribunal deverá ser feito seguindo as normas aqui apresentadas.

3.2 Constitui uso indevido do serviço de acesso 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, tais como pornografia, pedofilia, racismo, comunidades de relacionamento, sítios de compras, jogos e páginas de distribuição e de compartilhamento de software;

II – utilizar programas de troca de mensagens em tempo real (bate-papo) ou programas para troca de conteúdo via rede ponto-a-ponto (peer-to-peer), exceto os definidos como ferramenta de trabalho e homologados pela Secretaria de Informática.

III – utilizar programas e/ou acessar páginas de áudio e vídeo em tempo real, ou

sob demanda, exceto as definidas como ferramenta de trabalho.

IV – acessar sítios que representem ameaça de segurança ou que possam comprometer de alguma forma a integridade da rede de computadores do TRT.

3.3. A liberação de acesso a sítios e serviços não-autorizados, mas necessários ao desempenho das atribuições funcionais do usuário, dependerá de solicitação por escrito do dirigente da unidade à Secretaria de Informática, que a submeterá, quando for o caso, ao Comitê de Segurança da Informação.

4. Monitoramento e auditorias

4.1. Por motivos de segurança, será monitorado todo acesso à Internet, cujos registros serão mantidos pelo Escritório de Segurança.

4.2. Os relatórios decorrentes das auditorias ordinárias realizadas pelo Escritório de Segurança da Informação serão encaminhados ao Comitê de Segurança da Informação.

4.3. Em caso de indícios de incidentes de segurança específicos, a chefia imediata ou superior solicitará ao Comitê de Segurança da Informação a realização de auditoria extraordinária.

ANEXO 2

NSI002 – Controle de Uso do Correio Eletrônico

1. Política de Utilização do Correio Eletrônico

O presente tópico estabelece regras e padrões para a utilização do serviço de Correio Eletrônico no âmbito do TRT, disciplina a troca de mensagens eletrônicas e estabelece critérios para que sejam utilizados em conformidade com a política de segurança da informação e com a legislação vigente.

1.1. Endereços eletrônicos

1.1.1. A denominação do endereço de correio eletrônico será composta valendo-se de um prenome e um sobrenome do servidor, em letras minúsculas, sem acentos, cedilhas ou caracteres especiais, separados pelo sinal de ponto e acrescidos do sufixo "@trt4.jus.br".

Parágrafo único. Em situações justificadas, as porções iniciais dos endereços de correio eletrônico poderão ser compostas segundo outra ordem ou abreviação do nome do servidor.

1.1.2. As unidades administrativas poderão ter contas de correio eletrônico observada no endereço a sigla usualmente utilizada no TRT.

1.1.3. As contas de que trata o subitem 1.1.2 serão de uso dos responsáveis pelas unidades, admitindo-se a designação de até dois servidores para operá-las. Em casos justificáveis poderá haver mais de dois servidores para tanto.

1.1.4. É vedada a tentativa de acesso não-autorizado às caixas postais de terceiros.

1.1.5. Prestadores de serviços terceirizados e estagiários poderão, durante o período de prestação dos serviços, a critério do responsável e no interesse do serviço, ter acesso ao correio eletrônico institucional, observando as normas aqui enumeradas.

1.1.6. As mensagens de correio eletrônico de terceirizados e estagiários só poderão ser enviadas para endereços dentro do âmbito do TRT. Caso seja necessário, para interesse do serviço, o envio de mensagens para endereço externo, o responsável pela unidade administrativa deverá solicitar o acesso à Subsecretaria de Suporte aos Usuários.

1.2. Caixas Postais

1.2.1. As solicitações de novas caixas postais deverão ser encaminhadas à Secretaria de Informática, pela chefia imediata ou superior com os respectivos dados cadastrais.

1.2.2. Cabe à chefia imediata ou superior comunicar à Secretaria de Informática o desligamento de empregados terceirizados, temporários e estagiários sob sua responsabilidade para a exclusão definitiva da caixa postal.

1.2.3. A caixa postal sem movimentação por um período igual ou superior a três meses será bloqueada automaticamente pela Administração do Correio Eletrônico.

1.2.4. As caixas postais de servidores e magistrados afastados em decorrência de exoneração, aposentadoria, cedência ou retorno à origem serão excluídas 48 horas após a publicação do ato.

1.2.5. As caixas postais deste Tribunal estarão limitadas a 120 megabytes (MB).

1.2.6. A Secretaria de Informática manterá um processo sistemático para gravação e retenção de arquivos de registro de mensagens (logs) de correio eletrônico.

1.2.7. Os arquivos de registro de mensagens (logs) de correio eletrônico serão mantidos pelo período de três meses, pelo menos.

1.2.8. A eliminação dos arquivos de registro de mensagens e de caixas postais deverá ser adiada em caso de auditoria, ou qualquer outro tipo de notificação administrativa ou judicial.

1.2.9. É de responsabilidade do usuário:

I - utilizar o correio eletrônico institucional para os objetivos e funções próprios e inerentes às suas atribuições funcionais, observando as melhores práticas do item 1.6;

II - eliminar periodicamente as mensagens contidas nas caixas postais;

III - não permitir acesso de terceiros à sua conta de correio eletrônico;

IV - atualizar seus dados cadastrais utilizando os meios disponíveis.

1.3. Envio e Recebimento de Mensagens

1.3.1. O tamanho máximo da mensagem enviada ou recebida, incluindo todos os seus anexos, não excederá 8MB.

1.3.2. A quantidade máxima de destinatários por mensagem não excederá 30 endereços.

1.3.2.1. Em caso de necessidade de serviço deverá ser solicitado ao Comitê de Segurança da Informação a alteração do limite acima previsto.

1.3.2.2. O envio de e-mails a listas de distribuição deverá atender ao interesse de seus componentes, a ser utilizado de forma criteriosa e restrita.

1.3.3. É vedado ao usuário o envio de qualquer mensagem que contrarie o especificado no item 1.6 desta Norma (Melhores Práticas).

1.3.4. No recebimento de e-mails, o TRT fará uso de ferramentas especializadas a fim de reduzir a incidência de spams, e de remover qualquer conteúdo considerado impróprio ou indevido, enumerado no item 1.6.4.

1.3.5. O recebimento de mensagens que contrariem o disposto no item 1.6 desta

Norma (melhores práticas) será informado pelos usuários ao Escritório de Segurança para as providências cabíveis.

1.4. Uso de Certificação Digital

1.4.1. As mensagens eletrônicas com Assinaturas Digitais e cujos Certificados forem emitidos por entidades certificadoras que façam parte da ICP-Brasil são consideradas documentos oficiais no âmbito do TRT.

1.5. Uso de Serviços Externos de Correio Eletrônico

1.5.1. Não será permitido o acesso a serviços de correio eletrônico externos, exceto necessidades devidamente justificadas e previamente autorizadas.

1.6. Melhores práticas

1.6.1. O uso do correio eletrônico está restrito a funções e atividades inerentes ao trabalho deste Tribunal.

1.6.2. Somente clientes de correio eletrônico homologados pela Secretaria de Informática pode ser utilizados.

1.6.3. O campo de cópia oculta (BCC/CCO) do cliente de correio eletrônico deve ser usado, preferencialmente, sempre que for enviada uma mensagem para mais de um destinatário.

1.6.4. Considera-se envio não-apropriado de mensagens de Correio Eletrônico contendo:

I – informações proprietárias, confidenciais e privilegiadas para indivíduos ou organizações não-autorizadas;

II - materiais obscenos, ilegais ou antiéticos;

III - materiais preconceituosos ou discriminatórios;

IV – materiais caluniosos ou difamatórios;

V – propagandas com objetivos comerciais;

VI – listas de endereços eletrônicos dos usuários do Correio Eletrônico do TRT;

VII - vírus ou qualquer programa danoso;

VIII - material de natureza político-partidária ou sindical, que promova a eleição de candidatos para cargos públicos eletivos, clubes, associações e sindicatos;

IX – material protegido por leis de propriedade intelectual;

X - entretenimentos e “correntes”;

XI - assuntos ofensivos;

XII - músicas, vídeos ou animações que não sejam de interesse específico do trabalho;

XIII – *SPAM*;

XIV- materiais criptografados.

1.6.5. Não será permitido o uso do correio eletrônico funcional em Listas de Discussão com assuntos não relacionados à atividade profissional.

1.7. Monitoramento e Auditorias

1.7.1. O uso do correio eletrônico será monitorado por meio de ferramentas específicas com o intuito de impedir o recebimento nas caixas postais de *spams*, *phishings*, mensagens contendo vírus e outros arquivos que coloquem em risco a segurança da infra-estrutura tecnológica do Tribunal ou que sejam considerados como de conteúdo impróprio (item 1.6.4).

1.7.2. Os relatórios decorrentes das auditorias ordinárias realizadas pelo Escritório de Segurança da Informação serão encaminhados ao Comitê de Segurança da Informação.

1.7.3. Em caso de indícios de incidentes de segurança específicos, a chefia imediata ou superior solicitará ao Comitê de Segurança da Informação a realização de auditoria extraordinária.