PODER JUDICIÁRIO
JUSTIÇA DO TRABALHO
TRIBUNAL REGIONAL DO TRABALHO DA 6ª REGIÃO
Gabinete da Presidência

ATO TRT-GP nº 408/2013

Estabelece normas complementares à Política de Segurança da Informação, no âmbito do Tribunal Regional do Trabalho da Sexta Região, conforme disposições constantes no seu Anexo.

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

CONSIDERANDO a necessidade de estabelecer diretrizes e padrões para garantir um ambiente tecnológico eficiente e seguro, que favoreça as atividades jurisdicionais e administrativas deste Tribunal,

CONSIDERANDO o contido no inciso II do artigo 8º da Resolução Administrativa TRT nº 30/2009,

CONSIDERANDO as deliberações do Comitê Gestor de Segurança da Informação deste Tribunal, contidas na Ata de reunião realizada no dia 6 de agosto do corrente,

RESOLVE:

Art. 1º Estabelecer regras de segurança as quais dispõem sobre a identificação e concessão de acesso lógico; responsabilidades quanto ao uso de senhas, estações de trabalho, softwares e rede; uso do serviço de acesso à internet; uso do serviço de correio eletrônico e de geração e restauração de cópias de segurança, no âmbito do Tribunal Regional do Trabalho da Sexta Região, cabendo aos seus usuários observar as disposições contidas neste Ato, as quais são parte integrante da Política de Segurança da Informação desta Corte.

Art. 2º As normas que compõem o Anexo a este Ato serão atualizadas de forma periódica ou sempre que se fizer necessário, não excedendo o período máximo de 2 (dois) anos.

Art. 3º Os casos omissos e as dúvidas surgidas na aplicação destas normas serão dirimidos pelo Comitê Gestor de Segurança da Informação.

Art. 4º Este Ato entra em vigor na data de sua publicação.

Dê-se ciência e publique-se.

Recife, 17 de setembro de 2013.

IVANILDO DA CUNHA ANDRADE
Desembargador Presidente do TRT da Sexta Região

Anexo ao ATO TRT GP nº 408 /2013

I - CONTROLE DE ACESSO LÓGICO

1 OBJETIVO

Este documento dispõe sobre as regras de segurança que nortearão a definição e implantação de medidas para identificação e controle de acesso lógico aos ativos de informação do Tribunal Regional do Trabalho da Sexta Região.

2 CONCEITOS E DEFINIÇÕES

Para os efeitos desta norma são estabelecidos os seguintes conceitos e definições:

2.1 **Acesso**: ato de ingressar, transitar, conhecer ou consultar a informação, bem como a possibilidade de usar os ativos de informação do Regional;

2.2 **Acesso lógico**: permissão de acesso aos ativos de informação concedida ao usuário mediante apresentação de uma identidade válida;

2.3 **Administrador de ativo de informação**: usuário ou grupo de usuários responsável por definir critérios de utilização e autorizar, conceder ou modificar permissões de uso sobre o ativo de informação;

2.4 **Administrador de grupo**: usuário responsável pela criação e manutenção de grupos de usuários;

2.5 **Ativos de informação**: os meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso;

2.6 **Autenticação**: processo de validação da identidade do usuário, que pode ser feito por diversos meios, tais como: combinação de usuário/senha, reconhecimento biométrico ou utilização de certificado digital;

2.7 **Autorização**: processo de enumerar as permissões que um determinado usuário possui após a verificação de sua identidade;

2.8 **Bloqueio de acesso**: processo que tem por finalidade suspender temporariamente o acesso;

2.9 **Conta**: identificação única de usuário, com senha associada, para acesso aos ativos de informação do Regional;

2.10 **Conta de uso coletivo**: conta para acesso aos ativos de informação do Tribunal utilizada por mais de um usuário, com finalidade específica;

2.11 **Controle**: políticas, procedimentos, práticas e estruturas organizacionais criadas para prover uma razoável garantia de que os objetivos do Tribunal serão atingidos e que eventos indesejáveis serão evitados ou detectados e corrigidos;

2.12 **Identidade**: conjunto de atributos (lógicos e/ou físicos) que identifica univocamente um usuário, previamente cadastrado, para concessão de acesso aos sistemas ou serviços de informação;

2.13 **Identificação**: processo pelo qual o usuário apresenta uma identidade aos sistemas e serviços de informação;

2.14 **Necessidade de conhecer**: condição pessoal, inerente ao efetivo exercício de cargo, função, emprego ou atividade, indispensável para o usuário ter acesso à informação, especialmente se for sigilosa, bem como o acesso aos ativos de informação;

2.15 **Quebra de segurança**: ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação e comunicações;

2.16 **Permissões**: conjunto de direitos que um usuário possui para acessar/alterar informações nos sistemas ou serviços de informação;

2.17 **Privilégio**: permissão concedida a usuário e grupos de usuários de um recurso de TI;

2.18 **Princípio de privilégio mínimo**: as permissões concedidas a cada identidade devem ser as mínimas necessárias para o exercício do cargo, função ou papel do seu detentor;

2.19 **Rede de computadores do Tribunal**: conjunto de computadores, funcionalidades e outros dispositivos, de propriedade do Regional ou por ele providos, que, ligados em uma rede de comunicação de dados, possibilitam a prestação de serviços de TI;

2.20 **Senha**: conjunto de caracteres, de uso e conhecimento exclusivo do usuário, que permite autenticá-lo e, assim, conceder o acesso aos sistemas ou serviços de informação; e

2.21 **Usuários**: magistrados e servidores ocupantes de cargo efetivo ou em comissão, requisitados, cedidos e, 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 os recursos tecnológicos deste Regional.

3 CONSIDERAÇÕES INICIAIS

3.1 O objetivo do controle é sistematizar a concessão de acesso, a fim de evitar a quebra de segurança da informação e da comunicação.

3.2 A identificação, a autorização, a autenticação, o interesse do serviço, o princípio do privilégio mínimo e a necessidade de conhecer são condicionantes prévias para concessão de acesso aos ativos de informação no âmbito do Tribunal.

4 TIPOS DE USUÁRIOS

São usuários do Tribunal do Trabalho da Sexta Região:

4.1 **Usuário interno**: autoridade ou servidor ativo do Tribunal que tenha acesso, de forma autorizada, a informações produzidas ou custodiadas pelo Regional;

4.2 **Usuário colaborador**: prestador de serviço terceirizado, estagiário ou qualquer outro colaborador do Tribunal que tenha acesso, de forma autorizada, a informações produzidas ou custodiadas pelo Regional;

4.3 **Usuário externo**: servidor inativo, pessoa física ou jurídica que tenha acesso, de forma autorizada, a informações produzidas ou custodiadas pelo Tribunal e que não se enquadre nas definições contidas nos itens 4.1 e 4.2; e

4.4 **Usuário visitante**: pessoa física, que não se enquadre na definição disposta nos itens 4.1, 4.2 e 4.3 desta norma, com acesso temporário, somente à internet, autorizado a partir da rede do Tribunal.

5 DAS CONTAS DE ACESSO

5.1 Cada usuário deve possuir uma única conta para acesso aos ativos de informação do Tribunal, exceto nos casos explicitamente definidos e autorizados pela Secretaria de Informática.

5.2 A criação e a atualização de conta de usuário interno para acesso aos ativos de informação do Tribunal devem ser realizadas pela Secretaria de Informática com base nos registros contidos no sistema informatizado de gestão de pessoas:

a) a Secretaria de Informática deve definir e divulgar os procedimentos a serem executados com vistas à criação e à desativação de contas de usuários externos, colaboradores e visitantes; e

b) a utilização de conta de uso coletivo é permitida para usuário em treinamento e nos casos em que não seja possível trabalhar com conta de usuário individual.

5.3 **Da identificação**

5.3.1 A identificação do usuário, qualquer que seja o meio e a forma, deve ser pessoal e intransferível, permitindo de maneira clara e inequívoca o seu reconhecimento.

5.3.2 A alteração da identificação do usuário para acesso aos ativos de informação do Regional, quando não disponível nos próprios sistemas, deverá ser feita de forma presencial pelo usuário, com a apresentação de documento oficial com foto deste ou memorando da autoridade competente, junto ao setor responsável da Secretaria de Informática.

5.4 **Da Senha**

5.4.1 **Composição da senha:**

a) as senhas devem ser criadas em conformidade com os procedimentos e regulamentos vigentes quanto à qualidade e período de validade; e
b) é proibida a utilização de senhas sem nenhum processo criptográfico aplicado, excetuando-se os casos em que não houver alternativa.

5.4.2 **Senha de uso coletivo**

A senha associada à conta de uso coletivo só deve ser divulgada para as pessoas que efetivamente utilizam a conta para o treinamento ou para a finalidade para a qual foi criada.

5.4.3 **Alteração da senha:**

a) a alteração da senha associada à conta de usuário para acesso aos ativos de informação do Tribunal pode ser solicitada ou efetuada pelo próprio usuário ou, mediante seu pedido, pela chefia imediata; e
b) a alteração de senha associada à conta de uso coletivo deve ser solicitada por quem demandou a criação ou pelo responsável pelo treinamento a ser ministrado.

5.5 **Prazo de Validade das Contas de Acesso**

As contas para acesso aos ativos de informação do Tribunal têm os seguintes prazos de validade:

a) contas de magistrados e de servidores ativos e inativos: enquanto durar o vínculo com o Tribunal;
b) contas de usuários colaboradores: durante o exercício de suas atividades para o Tribunal;
c) contas de usuários externos, à exceção daquelas relativas a servidores inativos: sem prazo de validade previamente fixado, ressalvados os casos em que norma específica defina os prazos pertinentes; e
d) contas de usuários visitantes e contas de uso coletivo: pelo período necessário para a execução das atividades que motivaram a criação.

6 DA AUTENTICAÇÃO

6.1 Os ativos de informação do Tribunal somente serão acessíveis aos usuários que apresentem uma identidade válida e que possuam as permissões necessárias.

6.2 O processo de autenticação deve ser realizado de forma segura, visando evitar que informações sobre a identidade sejam acessíveis por outras pessoas.

6.3 Sempre que possível, o controle de acesso aos ativos de informação do Tribunal deverá possuir, pelo menos, dois fatores de autenticação.

7 DAS PERMISSÕES DE ACESSO AOS ATIVOS DE INFORMAÇÃO

As permissões de acesso aos sistemas e serviços de informação do Tribunal somente serão concedidas ou revogadas com base em atos de autoridade ou órgão competente.

7.1 **Do usuário interno**

Disponibilizar ao usuário interno que não exerce funções de administração de ativo de informação do Tribunal somente uma única conta institucional de acesso à rede local e ao correio eletrônico institucional, pessoal e intransferível.

7.1.1 **Das permissões de acesso para exercício da função**

As permissões de acesso aos ativos de informação do Tribunal, diferentes da rede local e do correio eletrônico institucional, são concedidas a grupos de usuários pelo respectivo administrador do ativo de informação:

a) os grupos de usuários relativos a unidades de lotação são criados e atualizados pela Secretaria de Informática, com base nas informações lançadas no sistema informatizado de gestão de pessoas; e
b) para os grupos de usuários com atualização manual, cabe ao administrador do grupo a verificação periódica de seus componentes e a inclusão ou retirada tempestiva de membros.

7.1.2 **Do privilégio de administrador:**

a) os usuários da Secretaria de Informática deverão possuir privilégio de administrador de ativos de informação apenas se necessário para o cumprimento de suas atividades, obedecido ao princípio de privilégio mínimo; e
b) nenhum usuário que não pertença ao corpo técnico da Secretaria de Informática deverá possuir privilégio de administrador de ativos de informação. As exceções ocorrerão apenas caso a Secretaria de Informática não consiga alternativas que permitam o desenvolvimento das atividades do usuário.

7.1.3 **Das mudanças nas atribuições e/ou lotação**

Sempre que houver mudança nas atribuições e/ou lotação de determinado usuário, os seus privilégios de acesso aos ativos de informação do Regional devem ser adequados imediatamente por procedimentos automáticos, ou tempestivamente no caso manual, devendo ser cancelados em caso de desligamento do Regional ou bloqueados em caso de afastamento.

7.1.4 **Das alterações a pedido do superior hierárquico:**

a) as permissões de acesso dos usuários aos ativos de informação do Tribunal poderão ser concedidas ou modificadas a pedido de superior hierárquico, mediante solicitação formal justificada à Secretaria de Informática; e
b) as identidades e permissões de acesso poderão ser restringidas ou suspensas para determinados usuários, a pedido de superior hierárquico, mediante solicitação formal justificada à Secretaria de Informática.

7.2 **Dos usuários colaboradores**

Poderão ser concedidas aos usuários colaboradores identidades e permissões de acesso aos ativos de informação do Tribunal durante o período de prestação dos serviços, observando as normas aqui enumeradas, mediante solicitação formal justificada do dirigente da unidade, onde será prestado o serviço colaborativo, à Secretaria de Informática.

8 AUDITORIA

8.1 Os acessos aos sistemas e serviços de informação do Tribunal, bem como as operações realizadas, sempre que possível devem ser registrados, permitindo auditoria.

8.2 As informações das identidades e os registros de acessos devem ser protegidos contra alterações e acessos indevidos.

9 COMPETÊNCIAS E RESPONSABILIDADES

9.1 Da Secretaria de Informática:

9.1.1 Propor regulamentação sobre os tipos de identidades homologadas para acesso aos ativos de informação deste Tribunal, bem como os seus requisitos mínimos;

9.1.2 Implantar políticas para criação, renovação, bloqueio, suspensão e expiração de senhas, com o intuito de aumentar o nível de segurança aos ativos de informação do Tribunal;

9.1.3 Propor regulamentação de procedimentos formais referentes à concessão e revogação de identidade de acesso aos ativos de informação deste Tribunal;

9.1.4 Definir e documentar os procedimentos operacionais relacionados a esta norma;

9.1.5 Divulgar amplamente esta política, procedimentos e regulamentos afins junto aos usuários dos ativos de informação deste Tribunal;

9.1.6 Manter a base de identidades e permissões de acesso aos ativos de informação deste Tribunal;

9.1.7 Emitir, suspender e modificar identidades e permissões de acesso aos ativos de informação deste Tribunal;

9.1.8 Implantar controles visando garantir a criação de senhas em conformidade com os procedimentos e regulamentos vigentes quanto à qualidade e período de validade;

9.1.9 Implantar demais controles necessários para o cumprimento desta política, deixando os sistemas e serviços de informação deste Tribunal em conformidade com a mesma; e,

9.1.10 Comunicar qualquer irregularidade ao Comitê Gestor de Segurança da Informação, a fim de que sejam tomadas as providências cabíveis.

9.2 Dos Usuários

9.2.1 Os atos decorrentes pela utilização dos sistemas de informática, através de conta de acesso com identificação e autenticação, são de responsabilidade do usuário para o qual a conta está formalmente vinculada; e

9.2.2 A senha associada à conta (identificação) de usuário para acesso à rede do Tribunal é pessoal, intransferível e o devido sigilo é de responsabilidade exclusiva do titular da conta.

9.3 Do Administrador do Ativo

É responsabilidade do administrador do ativo de informação verificar e adequar periodicamente as permissões de acesso.

9.4 Da Chefia Imediata

Compete à chefia imediata do usuário verificar a observância das disposições desta norma no âmbito de sua unidade, comunicando à Secretaria de Informática as irregularidades detectadas.

9.5 Da Secretaria de Gestão de Pessoas

A Secretaria de Gestão de Pessoas será responsável pelo envio imediato à Secretaria de Informática da informação de desligamento, aposentadoria ou movimentação de desembargadores, servidores, estagiários e aprendizes integrantes do Regional, para os devidos ajustes das credenciais de acesso.

II - USO DE SENHAS, ESTAÇÕES DE TRABALHO, *SOFTWARES* E REDE

1 OBJETIVO

Esta norma tem por objetivo dispor sobre as responsabilidades dos usuários quanto ao uso seguro de senhas, estações de trabalho, *softwares* e rede local.

2 CONCEITOS E DEFINIÇÕES

Para os efeitos desta norma são estabelecidos os seguintes conceitos e definições:

2.1 **Estação de Trabalho**: qualquer computador registrado como patrimônio do Tribunal, incluindo estações de trabalho móvel, utilizado pelos usuários no desempenho de suas atividades;

2.2 ***Hardware***: qualquer componente, acessório ou dispositivo eletro-eletrônico que seja parte de um computador;

2.3 **Incidentes de Segurança**: é qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores;

2.4 **Programa**: consiste de *softwares* adquiridos pelo tribunal ou que podem ser baixados pela Internet;

2.5 **Recurso de tecnologia da informação**: qualquer equipamento, dispositivo, serviço, infraestrutura ou sistema de processamento da informação e as instalações físicas que os

abrigam;

2.6 **Rede local**: conjunto de computadores, funcionalidades e outros dispositivos, de propriedade do Tribunal ou por ele providos, que, ligados em uma rede de comunicação de dados, possibilitam a prestação de serviços de TI;

2.7 **Senha**: conjunto de caracteres, de uso e conhecimento exclusivo do usuário, que permite autenticá-lo e, assim, conceder o acesso aos sistemas ou serviços de informação;

2.8 **Sistema**: *softwares* desenvolvidos pelo Tribunal para auxiliar as realizações de suas atividades jurisdicionais e administrativas; e

2.9 ***Software***: parte lógica, ou seja, instruções e dados processado pelos circuitos eletrônicos do *hardware* para executar um conjunto de ações previamente definidas. Consiste de programas e sistemas.

3 CONSIDERAÇÕES INICIAIS

3.1 Os recursos de TI devem ser utilizados somente em atividades estritamente relacionadas às funções institucionais.

3.2 Os parâmetros de configuração das estações de trabalho serão definidos pela Secretaria de Informática, que levará em conta os requisitos de segurança, estabilidade, confiabilidade e padronização do ambiente computacional do Tribunal.

3.3 A concessão de acesso aos recursos de TI deve obedecer ao princípio do privilégio mínimo, isto é, será concedido acesso ao usuário unicamente àqueles recursos de TI que forem indispensáveis à realização de suas atividades.

3.4 Os usuários são responsáveis pelos recursos de TI por eles utilizados, devendo contribuir para seu funcionamento e segurança.

3.5 É vedada a utilização dos recursos de TI disponíveis com o objetivo de praticar ações maliciosas contra outros recursos da rede de computadores do Tribunal ou redes externas.

4 REGRAS E RESPONSABILIDADES

4.1 Das Senhas

4.1.1 As senhas são de uso pessoal e intransferível, não sendo permitida a utilização de senha de outras pessoas ou fornecimento de senha pessoal a terceiros.

4.1.2 É vedada a utilização de quaisquer programas ou dispositivos para interceptar ou decodificar senhas ou similares.

4.1.3 O usuário deve notificar imediatamente à Secretaria de Informática sobre qualquer uso

não autorizado de sua conta ou qualquer quebra de segurança de seu conhecimento.

4.2 Das Estações de Trabalho

4.2.1 As estações de trabalho devem ser utilizadas apenas por usuários com identificação de acesso à rede do Tribunal e que não tenham infringido as disposições contidas nesta norma.

4.2.2 Prestadores de serviços terceirizados, consultores e estagiários poderão utilizar estações de trabalho durante o período de prestação dos serviços, observando as normas aqui enumeradas, mediante solicitação formal justificada do dirigente da unidade, onde será prestado o serviço terceirizado ou estágio, à Secretaria de Informática.

4.2.3 A guarda da estação de trabalho móvel é de inteira responsabilidade do magistrado ou servidor, devidamente registrada pela Coordenadoria de Material.

4.2.4 O usuário deve bloquear a estação de trabalho que lhe foi confiado sempre que dela se ausentar.

4.2.5 A homologação de *softwares*, componentes de *hardwares* e equipamentos passíveis de serem instalados e utilizados no ambiente do Tribunal é procedimento de competência da Secretaria de Informática, sendo vedada a instalação dos que não tenham sido homologados, salvo em razão de testes, se feita pela própria Secretaria.

4.2.6 As estações de trabalho serão instaladas e configuradas pela Secretaria de Informática.

4.2.7 Não compete à Secretaria de Informática instalar e configurar equipamentos que não estejam registrados como patrimônio do Tribunal.

4.3 Dos *Softwares*

4.3.1 Os *softwares* utilizados pelo Tribunal somente podem ser instalados nas estações de trabalho por pessoas autorizadas pela Secretaria de Informática, podendo ser feita por meio de programas de gerenciamento remoto.

4.3.2 É vedada a cópia de programas, licenças dos programas e sistemas implantados nas estações de trabalho, quer seja para uso externo, quer seja para uso em outra estação de trabalho do Órgão.

4.4 Da Rede Local e Armazenamento Lógico

4.4.1 É vedada a utilização de dispositivos particulares, portáteis ou não, na rede cabeada do Tribunal, exceto em casos de comprovada necessidade, e mediante anuência da Secretaria de Informática, que velará para que sejam, obrigatoriamente, adotados os padrões de segurança estabelecidos pelo Tribunal.

4.4.2 É vedado adicionar sem autorização à rede do Tribunal quaisquer recursos que possam interferir de alguma forma no desempenho ou na segurança da rede, como pontos de acesso *wireless*, acesso móvel e impressoras de rede.

4.4.3 É vedado o uso de ferramentas de *hardware* e *software* para sondagem, análise de vulnerabilidade, monitoramento de rede, comprometimento de sistemas, ataques e captura de dados, exceto quando autorizado pela Secretaria de Informática.

4.4.4 A Secretaria de Informática poderá restringir o espaço disponível para o usuário nas unidades de armazenamento de rede, considerando as limitações dos recursos de informática e as atividades desenvolvidas pelo usuário.

4.4.5 O usuário deve manter, sempre que possível, a cópia dos arquivos de trabalho nas unidades lógicas de armazenamentos de rede disponibilizadas pela Secretaria de Informática.

4.4.6 É vedado o armazenamento de arquivos não relacionados com as atividades institucionais nas unidades de rede, tais como: músicas, vídeos e fotos.

4.4.7 A Secretaria de Informática executará cópias de segurança dos arquivos de trabalho armazenados nas unidades de armazenamento de rede.

5 MONITORAMENTO E AUDITORIA

Compete à Secretaria de Informação realizar o monitoramento da utilização dos recursos de tecnologia da informação, com a finalidade de detectar divergências entre as responsabilidades definidas e os registros de eventos monitorados, fornecendo evidências nos casos de incidentes de segurança.

6 DISPOSIÇÃO FINAL

Avaliado o risco, a Secretaria de Informática poderá proceder à desinstalação sumária dos *softwares* que não se enquadrarem nos critérios estabelecidos nesta norma.

III - USO DO SERVIÇO DE ACESSO À INTERNET

1 OBJETIVO

Esta norma tem por objetivo dispor sobre as regras relativas ao uso seguro do serviço de acesso à internet.

2 CONCEITOS E DEFINIÇÕES

Para os efeitos desta norma são estabelecidos os seguintes conceitos e definições:

2.1 **Acesso à internet**: ato de acessar qualquer recurso disponível na Internet, como sites, salas de bate-papo, fóruns de discussão, entre outros;

2.2 **Bloqueio de acesso**: processo que tem por finalidade suspender temporariamente o acesso;

2.3 ***Download***: (significa descarregar ou baixar, em português) é a transferência de dados de um computador remoto para um computador local;

2.4 **Exclusão de acesso**: processo que tem por finalidade suspender definitivamente o acesso;

2.5 **Identificação de acesso à rede**: conjunto de atributos (lógicos e/ou físicos) que identifica univocamente um usuário, previamente cadastrado, para concessão de acesso aos sistemas ou serviços de informação;

2.6 **Internet**: consiste na rede mundial de computadores interconectados. É utilizada como uma grande plataforma para a provisão de inúmeros serviços;

2.7 ***Proxy***: computador ou sistema que serve de intermediário entre um navegador da Web e a Internet; e

2.8 **Site ou sítio**: conjunto de páginas web, disponibilizadas na Internet.

3 CONSIDERAÇÕES INICIAIS

3.1 O acesso à internet através da rede corporativa do Regional dar-se-á, exclusivamente, por intermédio dos meios autorizados pela Secretaria de Informática.

3.2 Excetuando-se os casos previstos nesta norma, o acesso à internet provido pela rede do Tribunal deve restringir-se às páginas com conteúdo estritamente relacionado às atividades desempenhadas pelo Órgão.

3.3 A conexão de acesso à Internet deve passar por equipamentos de segurança garantindo o controle de acesso e a aplicação dos demais mecanismos de segurança e, em caso contrário, o equipamento deve estar isolado da rede da entidade institucional.

3.4 Para garantir a utilização adequada para fins diretos e complementares às atividades funcionais, a Secretaria de Informática poderá impor limitações ao acesso através de ferramentas automáticas.

4 PERMISSÃO DE ACESSO

4.1 Possuem acesso à internet os magistrados e servidores em exercício, com identificação de acesso à rede do Tribunal.

4.2 Prestadores de serviços terceirizados e estagiários poderão ter acesso à internet durante o período de prestação dos serviços desde que seja formalmente solicitado e justificado pelo responsável da unidade onde está sendo prestado o serviço terceirizado ou estágio.

5 RESTRIÇÃO DE ACESSO

O acesso à internet poderá ser bloqueado ou excluído para determinados usuários, a pedido de superior hierárquico, mediante solicitação formal justificada à Secretaria de Informática, ou por uso indevido do serviço.

6 USO DO SERVIÇO

6.1 Constituem uso indevido do serviço de acesso à internet:

a) acessar páginas de conteúdo considerado ofensivo, ilegal ou impróprio, tais como: pornografia, pedofilia, racismo, apologia ao crime, calúnia, difamação, injúria, comunidades de relacionamento pessoal, jogos, fóruns não-profissionais, dentre outros;
b) utilizar programas de troca de mensagens em tempo real (bate-papo), exceto os definidos como ferramenta de trabalho e homologados pela Secretaria de Informática;
c) acessar páginas de áudio e vídeo em tempo real, ou sob demanda, exceto nos casos de comprovada necessidade, através de solicitação à Secretaria de Informática;
d) obter na Internet arquivos (*download*) que não estejam relacionados com suas atividades funcionais, a saber: imagens, áudio, vídeo, jogos e programas de qualquer tipo;
e) acessar sítios que apresentem vulnerabilidade de segurança ou possam comprometer de alguma forma a segurança e integridade da rede de computadores do TRT;
f) utilizar sítios, serviços Internet ou softwares para acesso anônimo, como *proxies* externos e similares; e
g) utilizar sítios, serviços Internet ou softwares para controle remoto de equipamentos, exceto os definidos como ferramenta de trabalho e homologados pela Secretaria de Informática.

6.2 Não constitui utilização indevida o acesso a sítios bancários, sítios de notícias e de pesquisa e busca.

6.3 O acesso aos sítios e serviços que estejam enquadrados como uso indevido, mas que sejam necessários ao desempenho das atribuições funcionais do usuário, será liberado mediante solicitação do dirigente da unidade à Secretaria de Informática.

6.4 É vedado aos usuários utilizar mecanismos com o objetivo de descaracterizar o uso indevido do serviço.

7 MONITORAMENTO

7.1 Compete à Secretaria de Informação realizar o monitoramento e o controle do serviço de acesso à internet do Tribunal, a fim de garantir o cumprimento desta norma.

7.2 A Secretaria de Informática, sempre que possível, deverá registrar os endereços das páginas acessadas pelos usuários. Comprovada a utilização indevida, o acesso à internet do usuário poderá ser bloqueado e sua chefia imediata comunicada para as providências cabíveis.

8 DISPOSIÇÕES FINAIS

8.1 Os direitos de acesso dos usuários em afastamento definitivo da organização devem ser excluídos.

8.2 Os direitos de acesso dos usuários em afastamento temporário devem ser bloqueados no período da ausência.

IV - CORREIO ELETRÔNICO

1 OBJETIVO

Esta norma tem por objetivo dispor sobre as regras relativas ao uso seguro do serviço de correio eletrônico.

2 CONCEITOS E DEFINIÇÕES

Para os efeitos desta norma são estabelecidos os seguintes conceitos e definições:

2.1 **Bloqueio de acesso**: processo que tem por finalidade suspender temporariamente o acesso;

2.2 **Caixa postal**: conta de correio eletrônico onde são armazenadas as mensagens recebidas pelo usuário;

2.3 **Certificado Digital**: credencial emitida por autoridade certificadora, que no país é a ICP-Brasil, responsável pela emissão de certificados digitais com validade legal;

2.4 **Código malicioso**: termo genérico que se refere a todos os tipos de *software* que executam ações maliciosas em um computador, a exemplo, os vírus e os "cavalos de tróia";

2.5 **Corrente**: mensagem enviada com o objetivo de propagar um boato ou determinado assunto sem relação com as atividades da Instituição;

2.6 **Exclusão de acesso**: processo que tem por finalidade suspender definitivamente o acesso;

2.7 ***Scam***: mensagem enviada com o objetivo de obter informações sensíveis, tais como senhas e números de cartão de crédito, para utilização em fraudes;

2.8 **Serviço de correio eletrônico institucional**: serviço de envio e recebimento de mensagens eletrônicas (e-mails) do Tribunal gerenciado pela Secretaria de Informática;

2.9 **Serviço externo de correio eletrônico**: qualquer serviço de correio eletrônico disponibilizado por terceiros;

2.10 ***Spam***: mensagem não solicitada enviada para vários destinatários; e

2.11 ***Webmail***: serviço de correio eletrônico disponível através de um site.

3 CONSIDERAÇÕES INICIAIS

3.1 O usuário deverá utilizar o correio eletrônico institucional para os objetivos e funções próprios e inerentes às suas atribuições funcionais.

3.2 A Secretaria de Informática poderá estabelecer limites de utilização do correio eletrônico que se façam necessários para o bom funcionamento do serviço, aí incluídos os de quantidade de destinatários, o tamanho máximo da caixa postal e das mensagens enviadas ou recebidas, dos tipos permitidos de arquivos anexados às mensagens.

3.3 A denominação do endereço de correio eletrônico do usuário será composta valendo-se preferencialmente de um nome e um sobrenome, separados por um sinal de ponto e acrescidos do sufixo "@trt6.jus.br".

3.4 É de responsabilidade do usuário efetuar periodicamente a manutenção de sua caixa postal.

3.5 O acesso a serviços de correio eletrônico externos somente poderá ser feito via *Webmail*, podendo este ser bloqueado a qualquer momento se confirmados abusos em sua utilização.

4 PERMISSÃO DE ACESSO

4.1 Possuem acesso ao correio eletrônico institucional os usuários com identificação de acesso para utilização do serviço.

4.2 Prestadores de serviços terceirizados, consultores e estagiários poderão ter acesso ao correio eletrônico institucional durante o período de prestação dos serviços mediante solicitação formal justificada do dirigente da unidade, onde será prestado o serviço terceirizado ou estágio, à Secretaria de Informática.

4.3 As unidades administrativas poderão ter listas de correio eletrônico observada no endereço a sigla usualmente utilizada no Tribunal.

4.4 Sistemas ou aplicativos que necessitem enviar e-mails poderão ser configurados para ter acesso a uma conta de correio eletrônico.

4.5 Solicitações para criação ou exclusão de caixas postais de servidores deverão ser encaminhadas formalmente à Secretaria de Informática.

5 RESTRIÇÃO DE ACESSO

O acesso ao serviço de correio eletrônico institucional poderá ser bloqueado ou

excluído para determinados usuários, a pedido de superior hierárquico, mediante solicitação formal justificada à Secretaria de Informática, ou por uso indevido do serviço.

6 USO DO SERVIÇO

6.1 Caracteriza-se por uso recomendável do serviço de correio eletrônico:

h) eliminar, periodicamente, as mensagens desnecessárias da caixa postal pessoal de forma a não exceder o limite de tamanho definido;
i) evitar clicar em links de acesso a páginas de Internet existentes em mensagens de correio eletrônico recebidas de origem desconhecida, pois esses podem tratar-se de golpes que objetivam o roubo de informações pessoais;
j) evitar abrir ou executar arquivos anexados às mensagens recebidas pelo correio eletrônico, sem antes verificá-los quanto à sua procedência;
k) fazer o uso, preferencialmente, do campo de cópia oculta (BCC/CCO) do cliente de correio eletrônico sempre que enviar uma mensagem para mais de um destinatário; e
l) evitar o envio de documentos anexos, como boletins, periódicos, memorandos e ofícios, substituindo o anexo por uma referência (*link*) ao documento no corpo da mensagem.

6.2 Caracteriza-se por uso não apropriado do serviço de correio eletrônico enviar mensagens contendo:

a) material obsceno, ilegal ou antiético;
b) material preconceituoso ou discriminatório;
c) material calunioso ou difamatório;
d) material considerado apologia ao crime, racismo ou pedofilia;
e) listas de endereços eletrônicos dos usuários do correio eletrônico do TRT;
f) vírus, códigos maliciosos anexados ou qualquer programa danoso;
g) material de natureza político-partidária ou sindical, que promova a eleição de candidatos para cargos públicos eletivos, clubes, associações e sindicatos;
h) material protegido por leis de propriedade intelectual;
i) entretenimentos, *scam* e correntes;
j) assuntos ofensivos;
k) imagens, áudio ou vídeo que não estejam relacionados ao desempenho das atividades funcionais;
l) arquivos executáveis de qualquer tipo;
m) mensagens comerciais não solicitadas, também conhecidas como spam;
n) mensagens que representem riscos de segurança ou que afetem o desempenho dos recursos de tecnologia do Tribunal, ou ainda que possam comprometer, de alguma forma, a integridade, a confidencialidade ou a disponibilidade das informações institucionais; e
o) outros conteúdos notadamente fora do contexto do trabalho desenvolvido.

6.3 Caracteriza-se por uso vedado do serviço de correio eletrônico:
a) utilizar clientes de correio eletrônico que não sejam homologados pela Secretaria de Informática;
b) utilizar mecanismos com o objetivo de descaracterizar o uso indevido do serviço;

c) acessar a caixa postal de outro usuário, salvo mediante prévia autorização;
d) configurar o redirecionamento automático de mensagens para serviços externos de correio eletrônico;
e) o envio de mensagens destinadas a todos os usuários, cujo conteúdo esteja relacionado somente a um pequeno grupo de magistrados e servidores.

7 MONITORAMENTO

7.1 Compete à Secretaria de Informação realizar o monitoramento e o controle do serviço de correio eletrônico, a fim de garantir o cumprimento desta norma.

7.2 A Secretaria de Informática poderá rastrear ou varrer o conteúdo das mensagens, de forma automática, por *softwares* especiais, a fim de verificar a adequação de seu conteúdo às disposições estabelecidas.

7.3 Os anexos das mensagens de correio eletrônico poderão ser bloqueados quando oferecerem riscos à segurança da informação.

8 DISPOSIÇÕES FINAIS

8.1 Caso o usuário venha a receber mensagens externas de conteúdo não apropriado, o mesmo deverá excluí-las no primeiro acesso à caixa postal após o recebimento das mesmas;

8.2 É permitida a criação de listas de correio eletrônico, com o objetivo de atender necessidades específicas de determinados grupos de usuários;

8.3 O envio de mensagens a todos os usuários é restrito a assuntos de interesse geral dos magistrados e servidores, sendo de responsabilidade das unidades administrativas e seus representantes;

8.4 É permitida a participação em Listas de Discussão com assuntos relacionados exclusivamente ao interesse do trabalho tanto profissional quanto educativo;

8.5 As mensagens ou arquivos eletrônicos com Assinaturas Digitais e cujos Certificados forem emitidos por entidades certificadoras que façam parte da ICP-Brasil são considerados documentos oficiais no âmbito deste Tribunal.

V - GERAÇÃO E RESTAURAÇÃO DE CÓPIAS DE SEGURANÇA

1. OBJETIVO

Esta norma tem por objetivo estabelecer as diretrizes para a geração de cópias de segurança das informações e sua restauração em tempo proporcional à criticidade do serviço afetado.

2. CONCEITOS E DEFINIÇÕES

Para os efeitos desta norma são estabelecidos os seguintes conceitos e definições:

2.1 **Arquivo ativo:** arquivo em uso (atual);

2.2 **Controle de acesso lógico:** conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso, utilizando para isto barreiras lógicas.

2.3 **Controle de acesso físico:** conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso, utilizando para isto barreiras físicas.

2.4 **Cópia de segurança das informações (backup):** é a cópia das informações fundamentais para a continuidade da prestação jurisdicional armazenadas em recursos de tecnologia da informação que permitem a recuperação após um desastre ou falha de uma mídia;

2.5 **Informação sigilosa:** aquela submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado;

2.6 **Recursos de tecnologia da informação:** qualquer equipamento, dispositivo, serviço, infraestrutura ou sistema de processamento da informação e as instalações físicas que os abrigam;

2.7 **Sistemas críticos:** sistemas fundamentais para a continuidade da prestação jurisdicional do Tribunal; e

2.8 **Tipos de backup:** completo (copia todos os arquivos selecionados e os marca como arquivos que passaram por backup), incremental (copia somente os arquivos criados ou alterados desde o último backup completo ou incremental e os marca como arquivos que passaram por backup) e diferencial (copia arquivos criados ou alterados desde o último backup completo ou incremental, mas não marca os arquivos como arquivos que passaram por backup).

3. CONSIDERAÇÕES INICIAIS

3.1 A realização de cópias de segurança das informações é fundamental para a continuidade da prestação jurisdicional, em caso de perda de dados ou desastres.

3.2 As cópias de segurança das informações devem ser efetuadas e testadas regularmente pela secretaria de informática.

3.3 A infraestrutura para a geração de cópias de segurança deve ser adequada para garantir que toda informação essencial possa ser recuperada.

4. PROCEDIMENTOS

4.1 Cabe à Secretaria de Informática definir procedimentos para a geração e restauração das cópias

de segurança, mantendo os registros completos e fidedignos das cópias.

4.2 Para sistemas críticos, os procedimentos de geração e restauração das cópias devem abranger todas as aplicações, dados, configurações e informações essenciais para a completa recuperação do sistema em caso de necessidade.

4.3 Os procedimentos de restauração de cópias de segurança devem ser verificados regularmente, de forma a garantir que estes são efetivos e que podem ser concluídos dentro dos prazos definidos nos procedimentos operacionais de recuperação.

4.4 Os procedimentos de cópia de segurança das informações devem ser automatizados para facilitar o processo de geração e recuperação das cópias.

4.5 Deve ser implantado um controle de acesso físico e lógico para as informações das cópias de segurança.

5. CÓPIAS DE SEGURANÇA DA INFORMAÇÃO

5.1 A Secretaria de Informática é a responsável pelo processo de cópias de segurança das informações no âmbito do Regional.

5.2 A frequência, tipo (completa, diferencial e incremental) e tempo de retenção das cópias de segurança das informações geradas serão definidos pela Secretaria de Informática, considerando os requisitos legais e a criticidade dos dados envolvidos com as atividades da Instituição.

5.3 Os equipamentos envolvidos no processo de cópias de segurança devem garantir que os dados das cópias de segurança sejam gravados na sua totalidade.

5.4 As informações sigilosas devem ser salvaguardadas criptografadas nas cópias de segurança.

5.5 A Secretaria de Informática não realizará cópias de informações armazenadas em estações de trabalho do Regional.

5.6 **Horário para a realização das cópias**

5.6.1 As cópias de segurança serão realizadas em horário de baixa utilização das informações, preferencialmente fora do horário de expediente.

5.6.2 Sendo inevitável a realização de cópias de segurança no horário do expediente, deverá ser justificado antecipadamente caso haja necessidade de parada do serviço ou queda substancial no desempenho dos recursos de Tecnologia da Informação.

5.6.3 Na situação de erro de cópia de segurança das informações, é necessário que ela seja refeita logo no primeiro horário disponível, assim que o responsável tenha identificado e solucionado o problema.

6. TESTES

6.1 A Secretaria de Informática deve realizar testes periódicos de restauração das cópias de segurança, visando a garantir que as cópias geradas são confiáveis para uso em caso de necessidade.

6.2 Os registros das evidências dos testes devem ser devidamente documentados.

6.3 Por se tratar de uma simulação, as informações devem ser restauradas em local diferente do original, para que assim não sobreponha os arquivos ativos.

7 RESTAURAÇÃO DE CÓPIAS DE SEGURANÇA

7.1 A Secretaria de Informática é a responsável pelo processo de restauração de segurança das informações no âmbito do Regional.

7.2 Solicitações de restauração de cópias de segurança devem ser encaminhadas formalmente à Secretaria de Informática para as devidas providências.

7.3 Na situação de erro de restauração de cópia de segurança das informações é necessário que ela seja refeita logo no primeiro horário disponível, assim que o responsável tenha identificado e solucionado o problema.

8 MANUSEIO DE MÍDIAS

Para cada tipo de mídia devem ser observadas as recomendações dos fabricantes quanto aos seus requisitos de utilização.

8.1 Armazenamento

8.1.1 As mídias com cópias de segurança devem ser armazenadas em local remoto, que possua um nível apropriado de proteção física e ambiental, a distância do local principal suficiente para evitar danos ocasionados por um eventual sinistro.

8.1.2 O local onde as mídias devem ser armazenadas deve ter acesso restrito e controlado somente a usuários autorizados.

8.1.3 As mídias devem ser devidamente identificadas de forma a permitir sua rápida localização e recuperação.

8.2 Transporte

Quando necessário, as mídias serão transportadas por um colaborador autorizado pela Secretaria de Informática, para um local seguro, dentro de embalagem lacrada que proteja adequadamente seu conteúdo.

8.3 **Descarte e Substituição de mídias**

8.3.1 Deverão ser adotados mecanismos seguros para o descarte de mídias (incineração, trituração, etc.) a fim de garantir que informações armazenadas e sem uso sejam irrecuperáveis, observando as legislações pertinentes.

8.3.2 Mídias a serem descartadas devem ser registradas e suas informações de identificação devem ser removidas.

8.3.3 Mídias que apresentam erros devem primeiramente ser formatadas e testadas. Caso o erro persista, deverão ser inutilizadas.

9 MONITORAMENTO

9.1 Para formalizar o controle de execução de cópias de segurança de informações e restaurações, deverá haver um formulário de controle rígido de execução dessas rotinas, o qual deverá ser preenchido pelos responsáveis e auditado nos termos desta Norma e dos procedimentos dela derivados.

9.2 Nos processos automatizados, o formulário poderá ser substituído por relatórios devidamente assinados pelos responsáveis.

10 DISPOSIÇÕES FINAIS

10.1 A Secretaria de Informática deverá comunicar ao Comitê Gestor de Segurança da Informação qualquer irregularidade concernente a falhas de segurança, a fim de que sejam tomadas as providências cabíveis.

10.2 É necessária a previsão, em orçamento anual, da renovação das mídias em razão de seu desgaste natural, bem como deverá ser mantido um estoque constante das mídias para qualquer uso emergencial.

***