Cartilha de Segurança da Informação
Boas práticas para usuários

Tribunal Regional do Trabalho – 13ª Região
Núcleo de Tecnologia e Suporte Técnico – NTST
suporte@trt13.gov.br

Versão 1.0

Autor: Rodrigo Mafra

07 de Maio de 2008

Resumo

Este documento tem por objetivo divulgar, no ambiente interno do TRT, boas práticas em Segurança da Informação (SI), buscando orientar os usuários para uma utilização segura dos recursos de tecnologia da informação disponibilizados pela instituição, em conformidade com a Política de Segurança da Informação, regulamentada pela RA nº 065/2007.

1. Introdução

O termo tecnologia da informação (TI) pode ser definido como o conjunto de recursos tecnológicos e computacionais para geração e uso da informação, abrangendo todas as atividades desenvolvidas na sociedade pelos recursos da informática.

Recursos relacionados à TI, como Internet, correio eletrônico, redes sem fio, entre outros, são atualmente ferramentas de trabalho indispensáveis no desempenho das mais diversas atividades. Porém, tais recursos podem ser explorados para fins ilícitos, como roubo de informações, disseminação de vírus, envio de spam, etc.

Diante deste cenário, esta cartilha foi elaborada visando orientar magistrados e servidores para uma utilização segura dos recursos de tecnologia da informação disponibilizados pela instituição, em conformidade com a Política de Segurança da Informação, regulamentada pela RA nº 065/2007.

Nos próximos tópicos, serão apresentadas orientações sobre:

- Senhas;
- Certificado digital;
- Internet;
- Correio eletrônico;
- Estações de trabalho;
- Rede local.

2. Senhas

Via de regra, o acesso aos diversos serviços de informática, como sistemas, e-mail, rede local, entre outros, ocorre mediante autenticação do usuário através de seu *nome de usuário* (login) e *senha* (password). Tal processo visa garantir que o acesso à informação seja obtido apenas por pessoas autorizadas (garantia de confidencialidade).

Cada usuário é responsável pela escolha de suas senhas pessoais. Algumas recomendações importantes:

- **Selecione senhas de boa qualidade.** Uma senha bem elaborada reduz as chances de ser comprometida. Algumas recomendações para elaboração de senhas:
  - Utilize senhas com pelo menos 6 caracteres;
  - Não elabore senhas baseadas em informações pessoais, como nomes, sobrenomes, número de documentos, placas de carros, telefones e datas;
  - Não elabore senhas baseadas em palavras que constem no dicionário de qualquer idioma;
  - Não elabore senhas com caracteres repetidos ou seqüenciais. Ex.: aa22, abcde, ab123;
  - Não elabore senhas com caracteres seguidos no teclado do computador. Ex.: qwer, zxcv;
  - Procure elaborar senhas baseadas em frases. Desse modo, basta lembrar a frase para lembrar a senha.
    Ex. 1: A partir da frase *"João Pessoa é a capital da Paraíba"* podemos criar a senha JPeacdP utilizando as iniciais da mesma.
    Ex. 2: A partir da frase *"Flamengo é pentacampeão brasileiro de futebol"* podemos criar a senha Fe5bdf;

- **Nunca divulgue ou compartilhe senhas pessoais.** As senhas são utilizadas no processo de identificação do usuário perante os serviços de informática. Sua confidencialidade é importante, de forma a evitar que terceiros acessem informações sensíveis, como e-mails e arquivos pessoais, documentos sigilosos, etc.
  Cada magistrado e servidor possui logins e senhas individuais, não sendo necessário divulgar ou compartilhar tais dados;
- **Altere periodicamente as senhas,** com o objetivo de assegurar a confidencialidade das mesmas. É recomendável que as senhas sejam alteradas a cada dois ou três meses no máximo;
- **Quando possível, não utilize senhas iguais para serviços diferentes.** Ex.: Utilize senhas distintas para o SUAP e o e-mail;
- **Evite registrar senhas em locais inseguros**, como anotações em papel, embaixo do teclado, adesivos colados no monitor, etc. O recomendável é apenas memorizar a senha;
- **Sempre altere as senhas temporárias no primeiro acesso.** Ex.: Alterar a senha inicial do SUAP no primeiro acesso;
- **Não digite senhas quando observado,** evitando assim que outras pessoas descubram suas senhas;
- **Sempre altere uma senha quando suspeitar que a mesma foi descoberta.**

3. Certificado digital

Certificado digital é um documento eletrônico que identifica pessoas e instituições, provando sua identidade e permitindo acessar serviços informatizados com a garantia de autenticidade, integridade e não-repúdio, assim como assinar digitalmente documentos.

O certificado digital destina-se a qualquer pessoa, física ou jurídica, sendo emitido por uma Autoridade Certificadora (AC). Os certificados utilizados no TRT da 13ª Região são emitidos pela Caixa Econômica Federal (certificados AC Caixa-JUS).

Cada usuário é responsável pela guarda e utilização de seu certificado digital. Algumas recomendações importantes:

- **Nunca forneça o certificado digital a terceiros.** O certificado digital é um documento pessoal e intransferível. Assim como outros documentos pessoais, como CPF, RG e passaporte, não deve ser fornecido a terceiros por questões de segurança;
- **Aplique as recomendações descritas no item *2. Senhas* para as senhas do certificado digital.** Um certificado digital possui duas senhas: PIN e PUK.
  O PIN (Personal Identification Number) é fornecido pelo usuário na utilização do certificado, como por exemplo para assinar um documento eletrônico.
  O PUK (Personal Unblocking Key) é utilizado pelo usuário para alterar o seu PIN em caso de necessidade.

4. Internet

O acesso à Internet no TRT está disponível para magistrados e servidores a partir das estações de trabalho conectadas à rede local da instituição. Algumas recomendações quanto à utilização da Internet:

- **No Tribunal, utilize somente os meios de acesso Internet homologados pela Secretaria de Informática,** que são a rede local e a rede sem fio da instituição. Demais formas de acesso,

como modem (acesso discado), acesso sem fio fornecido por empresas (Ex.: Oi, TIM, Claro), entre outras, não devem ser utilizadas no âmbito da instituição, pois podem comprometer a segurança da rede e das informações institucionais;

- **Não acesse sites e serviços Internet suspeitos,** como os relacionados à pornografia, software ilegal, spam, etc. Tais sites costumam ser utilizados para disseminação de vírus e roubo de informações pessoais;
- **Não acesse sites e serviços Internet sem relação com as atividades desempenhadas pela instituição,** como sites de jogos, fóruns não profissionais, comunidades de relacionamento pessoal, bate-papo, áudio e vídeo , dentre outros, evitando assim que o desempenho do acesso Internet e serviços relacionados sejam afetados;
- **Não utilize softwares e serviços Internet não homologados pela Secretaria de Informática,** como aqueles relacionados a compartilhamento de arquivos (Ex.: eMule, Kazaa, eDonkey), troca de mensagens em tempo real (Ex.: Windows Live Messenger, ICQ), transmissão de áudio e vídeo (Ex.: RealPlayer, YouTube), telefonia Internet (Ex.: Skype), evitando assim que a segurança e o desempenho da rede institucional sejam afetados;
- **Somente envie informações pessoais através de sites seguros.** Informações pessoais, como senhas e números de cartões de crédito, devem ser fornecidas somente em sites considerados seguros. Para identificar se um site é seguro, verifique se o endereço do mesmo (URL) é iniciado por https:// e se o navegador (Ex.: Internet Explorer, Firefox) exibe a figura de um cadeado fechado;
- **Somente acesse sites de instituições financeiras e públicas digitando o endereço diretamente no navegador**, nunca clicando em outro site ou em um e-mail recebido, evitando assim que dados pessoais sejam furtados através de sites fraudulentos;
- **Não utilize computadores públicos ou compartilhados**, como terminais em aeroportos, cafés e shopping centers, para acessar serviços disponibilizados no site do TRT, Gabinete Virtual, webmail, etc. Computadores compartilhados são ambientes inseguros, onde informações sigilosas podem ser obtidas por terceiros.

5. Correio eletrônico

O serviço de correio eletrônico institucional está disponível para magistrados e servidores a partir de qualquer estação com acesso à Internet. Algumas recomendações quanto à utilização do serviço de correio eletrônico:

- **Não abra e-mails e anexos considerados suspeitos,** como os relacionados à pornografia, propagandas, correntes, arquivos executáveis, remetentes desconhecidos, dentre outros. Tais e-mails e anexos costumam ser utilizados para disseminação de vírus e roubo de informações pessoais. Caso considere um e-mail ou anexo suspeito, apague o mesmo de sua caixa postal;
- **Limpe periodicamente sua caixa postal,** apagando e-mails antigos, spams, etc. Tal procedimento previne o não recebimento de e-mails devido ao "estouro" do limite da caixa postal;
- **Evite enviar e-mails para um grande número de destinatários,** pois tal atitude compromete o desempenho da rede local e do serviço de correio eletrônico;
- **Utilize o serviço de correio eletrônico somente para fins profissionais,** pois o envio de e-mails sem relação com as atividades desempenhadas pela instituição compromete o desempenho da rede local e do serviço de correio eletrônico;
- **Divulgue seu e-mail do TRT somente para fins profissionais,** evitando informar o mesmo em sites e serviços Internet não seguros. Tal procedimento reduz o recebimento de spams e de outras mensagens indesejadas;

- **Para maiores informações, consulte a Cartilha de SI – Correio eletrônico,** disponível em http://intranet.trt13.gov.br/documentacao/manuais/seguranca/cartilha-correio.pdf.

6. Estações de Trabalho

Constituem estações de trabalho os computadores e notebooks registrados como patrimônio do Tribunal e utilizados pelos magistrados e servidores no desempenho de suas atividades funcionais. Algumas recomendações quanto à utilização das estações de trabalho:

- **Não instale softwares sem a autorização da Secretaria de Informática.** Somente softwares devidamente licenciados para utilização no Tribunal e homologados pela Secretaria de Informática podem ser utilizados nas estações de trabalho. A utilização de software não licenciado ou considerado "pirata" constitui infração prevista na Lei nº 9.609/1998 (http://www.planalto.gov.br/ccivil_03/Leis/L9609.htm);
- **Não instale, remova ou modifique qualquer software ou hardware sem a autorização da Secretaria de Informática,** pois tal atitude pode comprometer a segurança e o desempenho da estação de trabalho;
- **Acesse a estação de trabalho somente com sua conta de usuário,** ou seja, nunca utilize uma estação de trabalho através do nome de usuário (login) e senha (password) de outra pessoa. Tal procedimento visa garantir a confidencialidade das informações processadas;
- **Ao se afastar da estação de trabalho, efetue o bloqueio ou "logoff" da mesma,** evitando assim que outra pessoa acesse a estação de trabalho através do seu nome de usuário (login) e senha (password);
- **Utilize a estação de trabalho somente para fins profissionais.**

7. Rede local

O acesso à rede local do Tribunal está disponível para os magistrados e servidores a partir das estações de trabalho. Algumas recomendações importantes:

- **Não utilize computadores pessoais na rede local do Tribunal,** ou seja, somente acesse a rede local através de computadores e notebooks registrados como patrimônio da instituição. Computadores pessoais conectados à rede do Tribunal representam uma das principais portas de entrada de vírus e outras ameaças à segurança da informação;
- **Armazene na rede somente arquivos relacionados com suas atividades funcionais,** ou seja, não utilize a rede para armazenar arquivos pessoais, como fotos, músicas, vídeos ou qualquer tipo de arquivo sem relação com as atividades do Tribunal. A má utilização do espaço disponível para armazenamento de arquivos afeta a performance de serviços essenciais;
- **No Tribunal, nunca utilize redes sem fio de terceiros.** Caso seja necessário acesso sem fio, utilize somente a rede local sem fio disponibilizada pela instituição, evitando assim que informações sensíveis sejam interceptadas por terceiros.