Tribunal Regional do Trabalho
13ª Região | Paraíba

CARTILHA DE SEGURANÇA DA INFORMAÇÃO: TELETRABALHO

Secretaria de Governança e Gestão Estratégica

Assessoria de Governança de Segurança da Informação

Autor: Rodrigo Mafra

João Pessoa – 2022
Versão 1.1

Sumário

1. Objetivo.....3
2. Introdução.....3
3. Equipamentos particulares.....3
4. Redes sem fio.....4
5. Senhas.....4
6. Ambiente de teletrabalho.....5
7. Referências.....5

1. Objetivo

Divulgar, para magistrados e servidores do TRT 13, boas práticas em Segurança da Informação voltadas ao teletrabalho, em conformidade com a Política de Segurança da Informação e Comunicações da instituição.

2. Introdução

Teletrabalho, também conhecido como trabalho remoto ou *home office*, consiste no desempenho das atividades funcionais por magistrados e servidores em ambiente externo à instituição.

Recursos relacionados à tecnologia da informação são ferramentas indispensáveis no desempenho do teletrabalho. Porém, tais recursos devem ser utilizados de forma segura, visando evitar o comprometimento da confidencialidade, integridade e disponibilidade das informações institucionais.

Nos próximos tópicos serão apresentadas boas práticas em Segurança da Informação no teletrabalho.

3. Equipamentos particulares

- **Mantenha os equipamentos atualizados.** É recomendável que computadores, *tablets* e *smartphones* utilizados no teletrabalho estejam com o sistema operacional, antivírus e demais *softwares* devidamente atualizados e nas versões mais recentes sempre que possível, reduzindo assim a exploração de vulnerabilidades por códigos maliciosos e outras ameaças. Consulte os manuais ou os suportes técnicos dos produtos sobre como proceder;

- **Utilize apenas *softwares* originais.** O uso de programas não originais pode colocar em risco a segurança, já que muitos fabricantes não permitem a realização de atualizações quando detectam versões não licenciadas. Além disto, a instalação de programas deste tipo, obtidos de mídias e sites não confiáveis ou via programas de compartilhamento de arquivos, pode incluir a instalação de códigos maliciosos;

- **Utilize *softwares* de proteção**, como antivírus e *firewall,* nos computadores, *tablets* e *smartphones* utilizados no teletrabalho. Tal medida aumenta a proteção contra códigos maliciosos e outras ameaças;

- **Efetue configurações de segurança nos equipamentos.** Ative recursos de segurança presentes na maioria dos computadores, *tablets* e *smartphones,* como: exigência de autenticação de acesso, bloqueio automático após um período de inatividade, criptografia de arquivos, rastreamento da localização, *backup*, entre outros. Consulte os manuais ou os suportes técnicos dos produtos sobre como proceder;

- **Seja cuidadoso ao enviar equipamentos para manutenção.** Em caso de necessidade de manutenção, envie seu equipamento somente para empresas com boa reputação no mercado, lembrando de antes remover arquivos e informações armazenadas relacionadas ao TRT 13;
- **Seja cuidadoso ao descartar equipamentos.** Ao descartar, doar ou se desfazer de um equipamento, não esqueça de remover todos os arquivos, *softwares* e informações do TRT 13 armazenadas no mesmo. Se possível, realize o procedimento de formatação das unidades de armazenamento do equipamento;
- **Em caso de perda ou roubo de equipamentos,** registre o boletim de ocorrência junto à autoridade policial, informando a localização caso o recurso de rastreamento esteja ativado. Alguns equipamentos permitem ainda o seu bloqueio ou remoção de dados remotamente;

4. Redes sem fio

- **Altere a senha padrão do seu roteador *wi-fi*,** trocando esta por uma outra senha bem elaborada e difícil de ser descoberta, evitando assim que suas configurações sejam alteradas por pessoas não autorizadas. Consulte o manual ou o suporte técnico do roteador sobre como proceder;
- **Utilize sua rede no modo mais seguro,** ativando no roteador *wi-fi* a autenticação WPA2 com uma senha bem elaborada e difícil de ser descoberta. Consulte o manual ou o suporte técnico do roteador sobre como proceder;
- **Evite utilizar redes públicas ou abertas no teletrabalho,** como as presentes em aeroportos, hotéis, cafés, *shoppings* e lojas, evitando assim que informações do TRT 13 sejam interceptadas por pessoas não autorizadas;
- **Desative as redes *bluetooth* em seus equipamentos.** Somente habilite o *bluetooth* durante o uso do mesmo, uma vez que este tipo de rede é mais suscetível a ameaças. Consulte os manuais ou os suportes técnicos dos equipamentos sobre como proceder;

5. Senhas

- **Não anote as senhas** utilizadas no ambiente de teletrabalho. O recomendável é apenas memorizar as senhas;
- **Não salve as senhas** utilizadas no ambiente de teletrabalho. Configure o navegador e outros *softwares* para não salvarem senhas, evitando assim que pessoas não autorizadas acessem sistemas e serviços de TI do TRT 13;
- **No caso de manutenção, descarte, perda ou roubo de equipamentos,** altere as senhas utilizadas no teletrabalho imediatamente;

- **Observe a norma institucional para utilização de senhas,** disponível em: *https://normasinternas.trt13.jus.br/xmlui/handle/bdtrt7/36648*

6. Ambiente de teletrabalho

- **Utilize somente os recursos e procedimentos divulgados pela SETIC** para o acesso remoto durante o teletrabalho, os quais estão em conformidade com as normas de Segurança da Informação da instituição;
- **Não exponha dados sensíveis a pessoas não autorizadas.** Evite que familiares, prestadores de serviços e outros tenham acesso a documentos do TRT 13;
- **Mantenha uma política de mesa limpa,** não deixando documentos impressos no local de teletrabalho;
- **Bloqueie o acesso** ao seu computador, *tablet* ou *smartphone* sempre que se ausentar do local de teletrabalho, evitando assim acessos não autorizados;
- **Não utilize equipamentos de ambientes públicos ou compartilhados no teletrabalho**, como *lan houses*, cafés, hotéis, dentre outros, pois estes são mais suscetíveis a ameaças;
- **Seja cuidadoso ao armazenar arquivos e documentos eletrônicos.** Utilize somente os locais providos pelo ambiente de teletrabalho disponibilizado pela SETIC, garantindo assim a devida proteção e o *backup* dos dados;
- **Observe a política, normas e procedimentos institucionais de Segurança da Informação,** que devem ser observados por todos os usuários do TRT 13;

7. Referências

- **Política de Segurança da Informação e Comunicações**
  www.trt13.jus.br/institucional/seguranca-da-informacao/estrutura-normativa/politica-de-seguranca-da-informacao-e-comunicacoes
- **Normas de Segurança da Informação**
  www.trt13.jus.br/institucional/seguranca-da-informacao/estrutura-normativa/normas
- **Procedimentos de Segurança da Informação**
  www.trt13.jus.br/institucional/seguranca-da-informacao/estrutura-normativa/procedimentos