Cartilha de Segurança da Informação
TAIÓPREV

Agosto/2019

CNPJ: 05.287.617/0001-53
Av. Luiz Bertoli, 44, Centro – CEP: 89.190-000 – Taió/SC
Telefone/Fax: (47) 3562 8305 – e-mail: taioprev@taio.sc.gov.br

INTRODUÇÃO

Esta Cartilha tem como objetivo reduzir os riscos relacionados à utilização da Internet e de dispositivos eletrônicos e evitar prejuízos financeiros, bem como impactos negativos a imagem do TAIÓPREV, sendo elaborada visando orientar os servidores, conselheiros e prestadores de serviço, para uma utilização mais segura dos recursos de tecnologia da informação disponibilizados.

CONCEITOS IMPORTANTES:

Segurança da informação são um conjunto de práticas, habilidades, recursos e mecanismos utilizados para proteger sistemas, dados e informações contra o acesso indevido, o ataque de cibercriminosos e o uso impróprio, assim como para prevenir a perda ou o sequestro de dados.

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.

A seguir, traremos orientações sobre acesso à internet, criação de senhas, certificado digital, correio eletrônico, rede local/sem fio, entre outros.

Nos próximos tópicos, serão apresentadas orientações sobre:

1. INTERNET

O acesso à Internet está disponível para servidores, conselheiros e prestadores de serviços, quando no uso de suas funções e ou interesse do Instituto.

Recomendações quanto à utilização da Internet:

- ✓ 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, comunidades de relacionamento pessoal, dentre outros, evitando assim que o desempenho do acesso Internet e serviços relacionados sejam afetados;
- ✓ Somente envie informações pessoais através de sites seguros. Informações pessoais, 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.

2. ESTAÇÕES DE TRABALHO

Constituem estações de trabalho os computadores e notebooks registrados como patrimônio do TAIÓPREV e utilizados pelos servidores e conselheiros no desempenho de suas atividades funcionais.

Recomendações:

- ✓ Não instale softwares sem a autorização da área de TI ou Suporte de Técnico de Informática. Somente softwares devidamente licenciados 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 área de TI ou Suporte de Técnico de Informática, pois tal atitude pode comprometer a segurança e o desempenho da estação de trabalho;
- ✓ Utilize a estação de trabalho somente para fins profissionais.

3. REDE LOCAL

O acesso à rede local está disponível para servidores, conselheiros e prestadores de serviço a partir das estações de trabalho.

Recomendações:

- ✓ Não utilize computadores pessoais, sem autorização da área de TI ou Suporte de Técnico de Informática, na rede local do TAIÓPREV, ou seja, somente acesse a rede local através de computadores e notebooks registrados como patrimônio da instituição, salvo quando previamente for autorizado pela área de TI ou Suporte de Técnico de Informática;
- ✓ Computadores pessoais conectados à rede do TAIÓPREV representam uma porta 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 TAIÓPREV.

4. SENHAS

Normalmente 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).

Cada usuário é responsável pela escolha de suas senhas pessoais.

Recomendações:

- ✓ 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;
- ✓ 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.
- ✓ Altere periodicamente as senhas, com o objetivo de assegurar a confidencialidade das mesmas;
- ✓ 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;

5. 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).

Cada usuário é responsável pela guarda e utilização de seu certificado digital.

Recomendações:

- ✓ Nunca forneça o certificado digital a terceiros. O certificado digital é um documento pessoal e intransferível;

6. CORREIO ELETRÔNICO

O serviço de correio eletrônico institucional é disponibilizado pelo TI da Prefeitura para servidores do TAIÓPREV através de solicitação da Diretoria Administrativa e Executiva, podendo ser acessado pelo Microsoft Outlook instalado pelo TI nas estações de trabalho.

Recomendações:

- ✓ 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 TAIÓPREV somente para fins profissionais, isso reduz o recebimento de spams e de outras mensagens indesejadas;

7. RECOMENDAÇÕES FINAIS

Além do exposto anteriormente, apresentamos, com o intuito de preservar a segurança das informações armazenadas em dispositivos eletrônicos e a imagem da empresa na Internet, recomendamos:

- ✓ Realize backups periódicos de documentos e informações, tendo em vista que códigos maliciosos e falhas de sistema podem levar a exclusão de dados e arquivos importantes. É importante realizar, testes com as referidas cópias de segurança, de forma a garantir que as informações salvas possam ser restauradas e disponibilizadas sempre que necessário;

- ✓ Além disso, deve-se considerar que, especialmente no caso do uso de dispositivos móveis, como smartphones, tablets e laptops por colaboradores, os equipamentos que contêm informações importantes podem ser furtados ou perdidos;
- ✓ Configure os dispositivos informáticos utilizados pelos usuários de modo que o acesso a eles se dê sempre por meio de senha segura, estabelecendo, ainda, regras para bloqueio de tela;
- ✓ Determine a necessidade de criptografar quaisquer documentos que contenham informações confidenciais ou de grande importância para o desenvolvimento das atividades da empresa, instruindo seus colaboradores a evitar trafegar com dispositivos contendo dados sigilosos;
- ✓ Ao encaminhar dispositivos eletrônicos para assistência técnica, exclua, se possível, dados confidenciais e/ou sensíveis, para evitar seu acesso e divulgação por pessoas não autorizadas;
- ✓ Ao se desfazer de um dispositivo eletrônico, apague todas as informações nele contidas e restaure as configurações de fábrica; e
- ✓ Os usuários dos sistemas/ softwares contratados para execução de rotinas administrativas, e ou sistemas disponibilizados por Órgão do Governo como: SIPREV, CADPREV, TCE Virtual, entre outros, devem seguir as rotinas de segurança indicadas por cada Órgão.

INDIANARA SEMAN
Diretora Presidente
TAIÓPREV

VANESSA MANCHEIN
Diretora Administrativa Financeira
TAIÓPREV