



## **NSI-001 Norma de Controle de Uso dos Recursos Computacionais**

### **1. Introdução**

- 1.1. A Norma de Segurança da Informação **NSI-001** complementa Política de Segurança da Informação do Sistema CFT/CRTs, definindo a conduta para o uso aceitável de ativos de informática e acesso à rede por seus usuários autorizados.

### **2. Propósito**

- 2.1. Estabelecer conduta para o uso aceitável dos equipamentos computacionais e acesso à rede do Sistema CFT/CRTs por seus usuários autorizados.

### **3. Escopo**

- 3.1. Esta norma obedece ao escopo definido na Política de Segurança da Informação do Sistema CFT/CRTs.

### **4. Diretrizes**

#### **4.1. Uso de equipamento computacional**

- 4.1.1. O Sistema CFT/CRTs fornece recursos computacionais necessários para que seus colaboradores executem, exclusivamente, suas atividades profissionais.
- 4.1.2. Todo usuário deve observar as seguintes disposições quanto ao uso de equipamentos de propriedade do Sistema CFT/CRTs:
- 4.1.2.1. Os equipamentos computacionais disponibilizados para que os usuários desenvolvam suas atividades profissionais são de propriedade do Sistema CFT/CRTs, sendo expressamente proibida a utilização para fins particulares, inclusive à acesso de uso pessoal;



- 4.1.2.2. A alteração e/ou a manutenção de qualquer equipamento de propriedade do Sistema CFT/CRTs é uma atribuição específica do setor de TI que, a seu critério exclusivo, poderá delegar formalmente outro responsável. Demais usuários são expressamente proibidos de realizar qualquer tipo de manutenção ou modificação nos equipamentos;
  - 4.1.2.3. Os equipamentos do Sistema CFT/CRTs devem ser utilizados com cuidado visando garantir sua preservação e seu funcionamento adequado;
  - 4.1.2.4. A desconexão (*log off*) deverá ser efetuada nos Computadores de mesa (*desktops*) ou móveis (*notebooks*) no final do expediente. E sempre desligados quando o usuário estiver ausente por um período prolongado.
  - 4.1.2.5. O bloqueio de tela protegido por senha deverá ser ativado sempre que o usuário se afastar do computador de mesa ou móvel que esteja utilizando;
  - 4.1.2.6. Ao final do contrato de trabalho, os equipamentos disponibilizados para a execução de atividades profissionais devem ser devolvidos em estado de conservação adequado;
  - 4.1.2.7. Qualquer dano aos equipamentos do Sistema CFT/CRTs será devidamente analisado pela área de tecnologia da informação. Havendo a constatação de que tal dano decorreu de ação direta ou omissão do usuário, caberá ao Sistema CFT/CRTs exercer seu direito de reparação ao prejuízo, através da tomada de medidas cabíveis.
- 4.1.3. O Sistema CFT/CRTs disponibiliza ferramentas para proteção dos seus ativos/serviços de informação e recursos computacionais, incluindo estações de usuários e servidores corporativos, contra ameaças e códigos maliciosos tais como vírus, ferramentas de captura de tela e dados digitados, software de propaganda e similares;



4.1.4. Mesmo com a existência de ferramentas para proteção contra códigos maliciosos, os colaboradores do Sistema CFT/CRTs devem adotar um comportamento seguro, reduzindo a probabilidade de infecção ou propagação de códigos maliciosos e reportando imediatamente ao setor de TI qualquer suspeita de código malicioso.

4.1.5. É proibida a utilização dos recursos tecnológicos e sistemas corporativos do Sistema CFT/CRTs fora do horário de trabalho, exceto nos casos que a utilização tenha sido permitida previamente pelo gestor imediato.

#### **4.2. Dispositivos de Armazenamento Removível**

4.2.1. O Sistema CFT/CRTs poderá, a seu critério exclusivo, fornecer a seus usuários dispositivos móveis ou com capacidade de armazenamento removível para execução de atividades profissionais, devendo ser observadas além das diretrizes acima, as seguintes:

4.2.1.1. O usuário é o responsável direto pela segurança física e lógica dos dispositivos móveis sob sua guarda. Portanto, os mesmos não devem ficar fora de seu alcance em locais públicos onde haja acesso não controlado de pessoas;

4.2.1.2. A instalação de ferramentas de proteção para dispositivos móveis é realizada pelo setor de tecnologia da informação e é obrigatória para todos os equipamentos corporativos;

4.2.1.3. Em caso de ocorrência de furto, roubo perda ou extravio de algum dispositivo de armazenamento removível, o usuário deve comunicar imediatamente ao seu superior imediato e ao setor de TI do Sistema CFT/CRTs, ou, caso tenha sido ele o servidor envolvido nos fatos, para seu superior hierárquico imediato, deverá observar imediatamente os seguintes procedimentos:



a) Providenciar, no prazo máximo de 48 horas da ocorrência ou ciência do fato, a emissão do Boletim de Ocorrência - BO junto à autoridade policial da cidade em que o fato ocorreu.

b) Encaminhar formalmente, por meio do Termo de Instauração de Processo Administrativo, devidamente preenchido e assinado, o original do BO e outros documentos afetos ao fato para o Setor de Patrimônio.

#### **4.3. Equipamentos de cópia e impressão**

4.3.1. O uso de equipamentos de cópia e impressão deve ser feito exclusivamente para a impressão/reprodução de documentos que sejam de interesse do Sistema CFT/CRTs ou que estejam relacionados com o desempenho das atividades profissionais do usuário.

4.3.2. O usuário deve observar as seguintes disposições específicas quanto ao uso de equipamentos de cópia e impressão:

4.3.2.1. Ao solicitar impressão de algum documento, o usuário deve retirar imediatamente os mesmos da impressora;

4.3.2.2. A impressão ou cópia de documento em suporte físico deve ser limitada à quantidade exata necessária para a tarefa determinada;

4.3.2.3. Páginas impressas que contenham informações confidenciais do Sistema CFT/CRTs e/ou dados dos técnicos não deverão ser reaproveitadas, devendo as mesmas ser descartadas de acordo com os procedimentos adotados pelo Sistema CFT/CRTs.

#### **4.4. Serviço de E-mail**

4.4.1. O Sistema CFT/CRTs fornece serviço de e-mail para seus usuários autorizados para desempenho de suas atividades profissionais;



## SERVIÇO PÚBLICO FEDERAL

### CONSELHO REGIONAL DOS TÉCNICOS INDUSTRIAIS DO RIO GRANDE DO SUL – CRT-RS

4.4.2. Em relação ao uso de e-mail oferecido pelo Sistema CFT/CRTs, não é permitido:

- 4.4.2.1. Praticar crimes e infrações de qualquer natureza;
- 4.4.2.2. Utilizar do serviço de e-mail em caráter pessoal ou para fins que não sejam de interesse do Sistema CFT/CRTs;
- 4.4.2.3. Utilizar termos ou palavras ofensivas e de baixo calão na redação das mensagens;
- 4.4.2.4. Enviar informações como USO INTERNO ou CONFIDENCIAL para endereços eletrônicos que não fazem parte do domínio corporativo do Sistema CFT/CRTs, exceto quando expressamente autorizados.
- 4.4.2.5. Fazer uso de qualquer técnica de forja ou simulação de falsa identidade;
- 4.4.2.6. Utilizar o e-mail corporativo para cadastro em site de compras, sites de relacionamento e redes sociais;
- 4.4.2.7. É proibido abrir arquivos ou links com origens desconhecidas ou suspeitas;

4.4.3. Os colaboradores do Sistema CFT/CRTs deverão adotar a assinatura padrão, de acordo com o seguinte formato:

- **Nome Completo**
- **Cargo – Número da Matrícula**
- **Telefone ou Ramal**

#### 4.5. Acesso à Internet

4.5.1. O acesso à Internet é disponibilizado a colaboradores e visitantes, através de rede cabeada e sinal de Wi-Fi.

4.5.2. Atualmente, a Internet disponibilizada pelo sistema CFT/CRTs pode ser utilizada para fins pessoais, desde que o uso não envolva conteúdo pornográfico, obscenos, difamatório ou que tenha



qualquer tipo de vinculação a algum tipo de discriminação racial, religiosa, política ou ética e para quaisquer tipos de jogos online.

4.5.3. Não é permitido propagar qualquer tipo de conteúdo malicioso.

4.5.4. O descumprimento dos itens acima é passível de punições e sanções, conforme previsto na Política de Segurança da Informação do Sistema CFT/CRTs.

#### **4.6. Segurança física**

4.6.1. As instalações de processamento das informações do Sistema CFT/CRTs serão mantidas em áreas seguras, cujo perímetro é fisicamente isolado contra o acesso não autorizado.

4.6.2. O usuário deve observar as seguintes disposições específicas quanto à segurança física:

**4.6.2.1.** Uso de Crachás de identificação, inclusive temporários. Crachá é pessoal e intransferível. Sob nenhuma circunstância será permitido o seu compartilhamento;

4.6.2.2. Visitantes ou terceiros nunca deverão ser deixados sozinhos em áreas sensíveis;

4.6.2.3. É proibida qualquer tentativa de se obter ou permitir o acesso a indivíduos não autorizado a áreas sensíveis do Sistema CFT/CRTs;

### **5. Papéis e Responsabilidades**

#### **5.1. SETOR DE TECNOLOGIA E INFORMAÇÃO**

5.1.1. É responsabilidade do Setor de Tecnologia e Informação do sistema CFT e CRT:

5.1.1.1. Estabelecer e manter atualizados os procedimentos complementares a esta norma;



## SERVIÇO PÚBLICO FEDERAL

CONSELHO REGIONAL DOS TÉCNICOS INDUSTRIAIS DO RIO GRANDE DO SUL – CRT-RS

- 5.1.1.2. Comunicar à Gerencia Geral e Diretoria eventuais tentativas, bem sucedidas ou não, de desvio de conduta dos termos dessa norma.

## 6. Sanções e Punições

- 6.1. O descumprimento das diretrizes apresentadas incorrerá em sanções e punições que serão aplicadas conforme previsto na Política Segurança da Informação do Sistema CFT/CRTs.

## 7. Revisões

- 7.1. Esta norma é revisada com periodicidade anual ou conforme o entendimento do Setor de Tecnologia da Informação do CFT.

## 8. Gestão da Norma

- 8.1. A norma **NSI-001 “Norma de Controle do Uso dos Recursos Computacionais”** foi elaborada pela Analista de Segurança do CFT – Camila Alves de Oliveira e aprovada pelo Comitê Nacional De LGPD, em conjunto com a Diretoria do Conselho Federal dos Técnicos Industriais - CFT e adaptada no que se refere ao CRT-RS pela Diretoria executiva do regional.