



NSI-002 Norma de Controle de Acessos e Senha

1. Introdução

- 1.1. A Norma de segurança da informação **NSI-002** complementa a Política de Segurança da Informação do Sistema CFT/CRTs, definindo as diretrizes para garantir que o acesso aos ativos de informação ou sistemas de informação do Sistema CFT/CRTs garantam níveis adequados de proteção.

2. Propósito

- 2.1. Estabelecer diretrizes para gestão de identidade e acesso aos ativos e sistemas de informação do Sistema CFT/CRTs.

3. Escopo

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

4. Diretrizes

4.1. Acesso a ativos e sistemas de informação

- 4.1.1. O Sistema CFT/CRTs fornece a seus usuários autorizados contas de acesso que permitem o uso de ativos de informação, sistemas de informação e recursos computacionais como, por exemplo, rede corporativa, SINCETI, conforme Resolução CFT Nº 38, aplicativo e-Técnico e base de dados dos técnicos registrados;
- 4.1.2. As referidas contas de acesso são fornecidas exclusivamente para que os usuários possam executar suas atividades laborais;
- 4.1.3. Cada conta de rede deve conter apenas acesso suficiente para o desempenho das suas atividades profissionais;



SERVIÇO PÚBLICO FEDERAL

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

- 4.1.4. Toda conta de acesso é pessoal do usuário a qual foi delegada e intransferível. Desta forma, o usuário é integralmente responsável por sua utilização, respondendo por qualquer violação ou ato irregular/ilícito, mesmo que exercido por outro indivíduo e/ou organização de posse de sua conta de acesso.
- 4.1.5. Contas com perfil de Administrador deverão ser utilizadas somente por pessoas autorizadas para a execução de tarefas formalmente atribuídas;
- 4.1.6. Os usuários deverão adotar medidas de prevenção para garantir o acesso seguro a ativos e serviços de informação, incluindo:
- 4.1.6.1. Não anotar ou registrar senhas de acesso em qualquer local;
 - 4.1.6.2. Não utilizar sua conta, ou tentar utilizar qualquer outra conta, para violar controles de segurança estabelecidos pelo Sistema CFT/CRTs;
 - 4.1.6.3. Não compartilhar a conta de acesso e senha com outro usuário, colaborador e/ou terceiro;
 - 4.1.6.4. Informar imediatamente ao responsável pelo suporte de T.I caso identifique qualquer falha ou vulnerabilidade que permita a utilização não autorizada de ativos de informação, sistemas e/ou recursos computacionais do Sistema CFT/CRTs;
- 4.1.7. Qualquer utilização não autorizada ou tentativa de utilização não autorizada de credenciais e senhas de acesso a ativos/serviços de informação ou recursos computacionais será tratada como um incidente de segurança da informação, cabendo uma análise da infração pelo Gerente Geral no CRT-RS do Sistema CFT/CRTs, e aplicação das sanções e punições previstas na Política de Segurança do Sistema CFT/CRTs, conforme a gravidade da violação.

4.2. Senha de acesso



SERVIÇO PÚBLICO FEDERAL

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

- 4.2.1. As senhas associadas às contas de acesso a ativos/serviços de informação ou recursos computacionais do sistema CFT/CRTs são de uso pessoal e intransferível, sendo dever do usuário zelar por sua guarda e garantir seu sigilo absoluto;
- 4.2.2. E-mails de contas pessoais as senhas são pessoais e intransferíveis;
- 4.2.3. no caso de e-mails corporativos compartilhados, somente usuários autorizados pelo Gerente Geral e ou Diretoria Executiva CRT-RS terão acesso às informações de logins destes e-mails;
- 4.2.4. A divulgação da senha é expressamente proibida e o usuário está sujeito à responsabilização por danos decorrentes da sua divulgação indevida.
- 4.2.5. As senhas de contas individuais não devem ser trafegadas por e-mail (exceto as senhas de primeiro acesso) ou quaisquer outros tipos de comunicação eletrônica;
- 4.2.6. O Sistema CFT/CRTs adota os seguintes padrões para geração de senhas de acesso a seus ativos/serviços de informação ou recursos computacionais:
 - 4.2.6.1. O profissional de T.I será responsável por fornecer senhas de acesso inicial ao usuário, que deverá proceder com a troca imediata da mesma;
 - 4.2.6.2. O profissional de T.I será responsável por fornecer senhas de acesso aos e-mails corporativos compartilhados aos usuários destes logins de e-mails, autorizados pelo Gerente Geral e ou Diretoria Executiva do CRT-RS;
 - 4.2.6.3. As senhas possuem validade de 2 anos. Passado este prazo, os sistemas solicitarão automaticamente a troca da senha;
- 4.2.7. Ao criar uma nova senha, os usuários devem estar atentos as seguintes recomendações:
 - 4.2.7.1. Não utilizar nenhuma parte de sua credencial na composição da senha;



SERVIÇO PÚBLICO FEDERAL

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

- 4.2.7.2. Não utilizar qualquer um de seus nomes, sobrenomes, nomes de familiares, colegas de trabalho ou informação a seu respeito de fácil obtenção como, por exemplo, placa do carro, data de aniversário, ou endereço;
- 4.2.7.3. Não utilizar repetição ou sequência de caracteres, números ou letras;
- 4.2.7.4. Qualquer parte ou variação do nome do Sistema CFT/CRTs;
- 4.2.7.5. Qualquer variação dos itens descritos acima como duplicação ou escrita invertida.

4.2.8. Recomenda-se:

- 4.2.8.1. Letras e Números aleatórios;
- 4.2.8.2. Letras maiúsculas e minúsculas;
- 4.2.8.3. Caracteres Especiais;

4.3. Autorização de acesso (privilégios de acesso)

- 4.3.1. A autorização e o nível permitido de acesso ativos/serviços de informação do Sistema CFT/CRTs deverá ser feito de acordo com as atividades a serem realizadas pelo colaborador.
- 4.3.2. Autorizações de acesso a perfis são fornecidas e/ou revogadas com base na solicitação dos gestores de cada colaborador. Essas solicitações deverão ser encaminhadas ao responsável de T.I.
- 4.3.3. O acesso do colaborador deve ser inativado ou cancelado imediatamente após desligamento do mesmo ou alteração de função (onde o mesmo não necessitará dos acessos que fazia uso na função anterior).
- 4.3.4. A inativação do acesso dos usuários também deverá ocorrer para os casos de ausência por períodos prolongados.



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

4.3.5. Os colaboradores devem ainda observar as seguintes diretrizes:

- 4.3.5.1. É expressamente proibido o armazenamento de informações de caráter pessoal ou ilícito, que infrinjam direitos autorais ou que não sejam de interesse do Sistema CFT/CRTs tanto na infraestrutura computacional local ou serviços de armazenamento remoto (nuvem);

5. Papéis e Responsabilidades

5.1. Setor de Tecnologia e Informação

5.1.1. É responsabilidade dos colaboradores do Setor de TI:

- 5.1.1.1. Autorizar a concessão e revogação de acesso a ativos/sistemas de informação sob sua responsabilidade, mediante solicitação devidamente expressa;
- 5.1.1.2. Autorizar a concessão e o controle de acesso administrativo a ativos/sistemas de informação sob sua responsabilidade, mediante solicitação devidamente expressa;
- 5.1.1.3. Realizar a revisão periódica de autorizações de acesso, credenciais de acesso e pacotes de permissões à ativos/sistemas de informação sob sua responsabilidade.
- 5.1.1.4. Receber e analisar solicitações para criação de contas de acesso ou fornecimento de privilégios para empregados, terceiros/prestadores de serviços;

5.2. Setor de Recursos Humanos (RH)

5.2.1. É responsabilidade do Setor de RH:

- 5.2.1.1. Reportar em tempo hábil o desligamento de empregados do Sistema do CFT/CRTs ao setor de tecnologia da informação para que contas de acesso e acesso aos sistemas possam ser revogados;



SERVIÇO PÚBLICO FEDERAL

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

- 5.2.1.2. Apoiar o setor de Tecnologia da Informação, enviando relatórios periódicos sobre colaboradores desligados ou que mudaram de posição no Sistema CFT/CRTs;
- 5.2.1.3. Fornecer informações sobre os empregados sempre que solicitado pelo Setor de TI, para revisão das credenciais de acesso e permissões aos ativos/sistemas da informação.

5.3. GESTORES DOS SETORES ADMINISTRATIVOS DO SISTEMA CFT/ CRTs

5.3.1. É responsabilidade dos gestores e dos setores administrativos do Sistema CFT/CRTs:

- 5.3.1.1. Solicitar ao setor de Tecnologia da Informação a concessão de acesso aos novos empregados ou empregados que necessitem de novos acessos conforme mudanças em suas atividades corporativas, mediante solicitação devidamente expressa e pelo gerente do setor ou regional do colaborador;
- 5.3.1.2. Solicitar ao setor de Tecnologia da Informação a concessão de acesso a terceiros/prestadores de serviços contratados justificando a necessidade de acesso a ativos/sistemas de informação, mediante solicitação devidamente expressa e pelo gerente responsável pela supervisão do trabalho exercido pela equipe terceirizada;
- 5.3.1.3. Informar ao setor de TI quanto ao encerramento do contrato com terceiros/prestadores de serviços contratados que tenham ativos/sistemas de informação, mediante solicitação devidamente expressa pelo gerente do setor ou regional do colaborador;

6. Sanções e Punições



SERVIÇO PÚBLICO FEDERAL

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

6.1. Sanções e punições serão aplicadas conforme previsto na Política de Segurança 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 Sistema CFT/CRTs

8. Gestão da Norma

8.1. A norma “**NSI-002 Norma de Controle de Acesso e Senha**” 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 e adaptada no que se refere ao CRT-RS pela Diretoria executiva do regional.