POLÍTICA DE SEGURANÇA INTERNA

Conselho Federal dos Técnicos Industriais

Conselho Regional dos Técnicos Industriais do RS

1. Introdução

1.1. O Conselho Federal dos Técnicos Industriais e os Conselhos Regionais dos Técnicos Industriais tem como missão regulamentar e garantir livre exercício das atividades profissionais dos técnicos e técnicas a nível nacional, por meio da Lei 5.524/68, do Decreto 90.922/85 e Lei 13.639/18. O Conselho provém amparo legal aos profissionais registrados.

1.2. O Sistema CFT/CRTs compreende que a manipulação de informações e tratamento dos dados corporativos e dos técnicos registrados passam por diferentes meios de suporte, armazenamento e comunicação, sendo estes vulneráveis a fatores externos e internos que podem comprometer sua segurança e integridade.

1.3. Dessa forma, o Sistema CFT/CRTs estabelece sua Política de Segurança da Informação (PSI-CFT), como parte integrante do seu sistema de gestão corporativo, alinhada as boas práticas e normas internacionalmente aceitas, com o objetivo de garantir níveis adequados de proteção as informações da organização ou sob sua responsabilidade.

2. Propósito

2.1. Esta política tem por finalidade estabelecer diretrizes e normas de Segurança da Informação que permitam aos colaboradores do sistema CFT e CRTs adotar padrões de comportamento seguro no ambiente de trabalho para com os dados tratados por esta Instituição;

2.2. Orientar aos colaboradores quanto à adoção de controles e processos para atendimento dos requisitos para Segurança da Informação e sua importância no ambiente de trabalho.

2.3. Resguardar as informações do Sistema CFT/CRTs, garantindo os pilares da Segurança da Informação (confidencialidade, integridade e disponibilidade);

2.4. Prevenir possíveis causas de incidentes e responsabilidade legal da Instituição e seus colaboradores, técnicos registrados e parceiros;

2.5. Mitigar os riscos, vulnerabilidades e seus impactos, oriundos de falhas de segurança.

3. Escopo

3.1. Esta política se aplica a todos os usuários da informação do Sistema CFT/ CRTs, incluindo qualquer indivíduo ou organização que possui ou possuiu vínculo com o Sistema CFT/CRTs, tais como empregados, ex-empregados, prestadores de serviço, ex-prestadores de serviço, que possuíram, possuem ou virão a possuir acesso às informações do CFT/CRTs e/ou fizeram, fazem ou farão uso de recursos computacionais compreendidos na infraestrutura do sistema CFT e CRTs.

4. Diretrizes

4.1. O objetivo da Gestão de Segurança da Informação do Sistema CFT/ CRTs é garantir a gestão efetiva de todas as questões relacionadas à segurança da informação, visando sempre a minimização dos riscos e ameaças identificadas e seus eventuais impactos a estes órgãos federais.

4.2. A Presidência, Diretoria Executiva e o Centro de Serviços Compartilhados (TI) estão comprometidos com uma gestão efetiva de Segurança da Informação no Sistema CFT/CRTs. Desta forma, adotam todas medidas cabíveis para garantir que esta política seja adequadamente comunicada, entendida e seguida em todos os níveis da organização. Revisões periódicas serão realizadas para garantir sua contínua pertinência e adequação às necessidades do Sistema CFT/CRTs.

4.3. É política do Sistema CFT/CRTs:

4.3.1. Elaborar, implantar e seguir políticas e normas complementares, garantindo que os 3 pilares da segurança da informação (confidencialidade, integridade e disponibilidade) sejam atingidos através da adoção de controles contra ameaças provenientes de fontes externas e internas;

4.3.2. Disponibilizar políticas e normas complementares a todos os empregados e terceirizados, garantindo a conscientização dos mesmos sobre as práticas de segurança da informação adotadas pelo Sistema CFT/CRTs;

4.3.3. Atender integralmente requisitos de segurança da informação aplicáveis ou exigidos principalmente pela Lei Geral de Proteção de Dados Pessoais e outras regulamentações, leis ou cláusulas contratuais vigentes.

4.3.4. Tratar incidentes de segurança da informação, garantindo que os mesmos sejam adequadamente registrados, classificados, investigados, corrigidos, documentados e comunicados aos envolvidos;

4.3.5. Melhorar continuamente a Gestão de Segurança da Informação através da definição e revisão periódica de objetivos de segurança em todos os níveis do Sistema CFT/CRTs.

5. Papéis e Responsabilidades

5.1 É responsabilidade do Centro de Serviços Compartilhados e equipe de TI:

5.1.1. Analisar, revisar e propor a aprovação de políticas e normas relacionadas à segurança da informação;

5.1.2. Garantir a disponibilidade dos recursos necessários para uma efetiva Gestão de Segurança da Informação do SINCETI e suas tecnologias;

5.1.3. Garantir que as atividades de segurança da informação sejam executadas em conformidade com a Política de Segurança do Sistema CFT/CRTs;

5.1.4. Promover a divulgação da Política de Segurança da Informação do Sistema CFT/CRTs e tomar as ações necessárias para disseminar uma cultura de segurança da informação no ambiente do Sistema CFT/CRTs.

5.1.5. Identificar e avaliar as principais ameaças à segurança da informação, bem como propor e, quando aprovado, implantar medidas corretivas para reduzir o risco;

5.1.6. Tomar as ações cabíveis para se fazer cumprir os termos desta política;

5.1.7. Realizar a gestão dos incidentes de segurança da informação, garantindo tratamento adequado.

5.1.8. Gerenciar as informações sob responsabilidade do Sistema CFT/CRTs durante todo o seu ciclo de vida, incluindo a criação, manuseio e descarte conforme as normas estabelecidas;

5.1.9. Periodicamente revisar as informações geradas ou sob a sua responsabilidade, ajustando a classificação das mesmas, conforme necessário;

5.1.10. Autorizar e revisar os acessos à informação e sistemas de informação sob sua responsabilidade;

5.1.11. Atender as solicitações internas e dos Regionais de concessão ou revogação de acesso à informação ou sistemas de informação, de acordo com os procedimentos adotados pelo Sistema CFT/CRTs.

5.2. **É responsabilidade dos Usuários da Informação e empregados desta Instituição:**

5.2.1. Ler, compreender e cumprir integralmente os termos da Política de Segurança da Informação, bem como as demais normas de segurança complementares;

5.2.2. Encaminhar quaisquer dúvidas e/ou pedidos de esclarecimento sobre a Política de Segurança da Informação e suas normas complementares à Gerência de Segurança da Informação (Centro de Serviços Compartilhados);

5.2.3. Comunicar à Gerência de Segurança da Informação (Centro de serviços compartilhados) qualquer evento que viole esta Política ou

coloque/possa vir a colocar em risco a segurança das informações ou dos recursos computacionais do Sistema CFT/CRTs;

5.2.4. Assinar o Termo de Confidencialidade do Sistema CFT/CRTs, formalizando a ciência e o aceite integral das disposições da Política de Segurança da Informação do Sistema CFT/CRTs, bem como as demais normas complementares de segurança, assumindo responsabilidade pelo seu cumprimento;

5.2.5. Responder pelo descumprimento das normas listadas nesta Política de Segurança.

6. Sanções e Punições

6.1. As violações, mesmo que por mera omissão ou tentativa não consumada, desta política, bem como demais normas e procedimentos de segurança, serão passíveis de penalidades que incluem advertência verbal, advertência por escrito, suspensão não remunerada e a demissão por justa causa;

6.2. A aplicação de sanções e punições será realizada conforme a análise da Diretoria Executiva do CRT-RS, devendo-se considerar a gravidade da infração, efeito alcançado, recorrência e as hipóteses previstas no artigo 482 da Consolidação das Leis do Trabalho, cabendo ao CRT-RS, no uso do poder disciplinar que lhe é atribuído, aplicar a pena que entender cabível.

6.3. No caso de terceiros contratados ou prestadores de serviço, CRT-RS deve analisar a ocorrência e deliberar sobre a efetivação das sanções e punições conforme termos previstos em contrato de trabalho;

6.4. Para o caso de violações que impliquem em atividades ilegais, ou que possam incorrer em danos ao Sistema CFT/CRTs, o infrator será responsabilizado pelos prejuízos, cabendo aplicação das medidas judiciais pertinentes sem prejuízo aos termos descritos nos itens 6.1, 6.2 e 6.3 desta política.

7. Casos Omissos

7.1. Os casos omissos serão avaliados pela Gestão de Segurança da Informação e Diretoria para posterior deliberação.

7.2. Temos ciência que a tecnologia está em constante evolução e novas ameaças surgem incessantemente. Sendo assim, consideramos obrigação do usuário da informação do Sistema CFT/CRTs adotar, sempre que possível, outras medidas de segurança além das aqui previstas, com o objetivo de garantir proteção as informações do sistema.

8. Glossário

8.1. **Sistema CFT/CRTs:** Conselho Federal dos Técnicos Industriais/Conselhos Regionais dos Técnicos Industriais;

8.2. **CSC:** Centro de Serviços Compartilhados;

8.3. **PSI- CFT:** Política de segurança da informação do Conselho Federal dos técnicos industriais;

8.4. **Ativo:** Tudo aquilo que possui valor para o CFT/CRTs;

8.5. **Ativo de informação:** Patrimônio intangível do Sistema CFT/CRTs, constituído por suas informações de qualquer natureza, além dos documentos em suporte físico, ou mídia eletrônica transitados dentro e fora de sua estrutura física.

8.6. **Usuário da informação:** Empregados com vínculo empregatício de qualquer área do Sistema CFT/CRTs ou terceiros alocados na prestação de serviços ao Sistema CFT/CRTs, e indivíduos ou organizações devidamente autorizadas a manipular qualquer ativo de informação do Sistema CFT/CRTs para o desempenho de suas atividades profissionais.

8.7. **Confidencialidade:** Garantia que somente pessoas autorizadas tenham acesso à informação

8.8. **Controle:** Medida de segurança adotada para o tratamento de um risco específico.

8.9. **Disponibilidade:** Garantia que a informação estará disponível quando for solicitada por pessoas autorizadas.

8.10. **Integridade:** Propriedade dos ativos da informação do Sistema CFT/CRTs, de serem exatos e completos.

8.11. **Ameaça**: Causa potencial de um incidente, que pode vir a prejudicar o Sistema CFT/CRTs.

8.12. **Risco de segurança da informação:** Efeito da incerteza sobre os objetivos de segurança da informação do Sistema CFT/CRTs.

8.13. **Incidente de segurança da informação:** Um evento ou conjunto de eventos indesejados de segurança da informação que tem possibilidade significativa de afetar as operações ou ameaçar as informações do Sistema CFT/CRTs.

8.14. **Segurança da informação:** A preservação das propriedades de confidencialidade, integridade e disponibilidade das informações do Sistema CFT/CRTs.

8.15. **Vulnerabilidade:** Causa potencial de um incidente de segurança da informação, que pode vir a prejudicar as operações ou ameaçar as informações do sistema CFT/CRTs.

9. Revisões

9.1. Esta política é revisada com periodicidade anual ou conforme o entendimento do Comitê Gestor da segurança da informação (CSC)

10. Gestão da Política

10.1. A Política Geral de Segurança da Informação do sistema CFT e CRTs foi elaborada pela Analista de Segurança do CFT – Camila Alves de Oliveira, 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.

10.2. A presente Política entra em vigor a partir da data de sua publicação.

Assinatura CRT-RS