1. INTRODUÇÃO

A Política de Segurança da Informação do SENAI CIMATEC tem o compromisso com a proteção dos ativos de informação de sua propriedade ou sob sua salvaguarda. Deve, portanto, ser cumprida pelas partes interessadas pertinentes: Alta Direção do SENAI CIMATEC, força de trabalho, fornecedores, parceiros e por qualquer pessoa física ou jurídica vinculada de alguma forma ao SENAI CIMATEC, que tenham acesso a seus dados ou informações sob sua salvaguarda.

Esta Política de Segurança da Informação foi elaborada com base nas normas técnicas ABNT NBR ISO/IEC 27001:2013 e 27002:2013, de acordo com a legislação vigente, realidade e requisitos de negócio.

> "A segurança da informação é alcançada pela implementação de um conjunto adequado de controles, incluindo políticas, processos, procedimentos, estrutura organizacional e funções de software e hardware. Estes controles precisam ser estabelecidos, implementados, monitorados, analisados criticamente e melhorados, quando necessário para assegurar que os objetivos do negócio e a segurança da informação da organização sejam atendidos. "
>
> ABNT NBR ISO/IEC 27002:2013

Para assegurar todos estes aspectos, é necessário que seja colocado em prática um processo de gestão de segurança da informação. A Norma ISO/IEC 27001:2013 ("Information Technology - Security Techniques - Information Security Management Systems - Requirements"), determina a criação do SGSI - Sistema de Gestão de Segurança da Informação (em Inglês, ISMS - Information Security Management System). O SGSI prevê diversas políticas, processos, guias e procedimentos com a missão de reduzir continuamente os riscos à segurança das informações e aos ativos críticos.

2. OBJETIVOS

Definir e padronizar o uso, tratamento, controle e proteção das informações que possam causar impactos no seu desempenho financeiro, na sua participação no mercado, na sua imagem, agregando valor à operação e eficiência na prestação de serviços ou no seu relacionamento com as partes interessadas, contemplando os seguintes objetivos específicos:

- Definir o escopo da segurança da informação do SENAI CIMATEC;
- Definir as responsabilidades na gestão da segurança da informação;
- Definir as responsabilidades das partes interessadas pertinentes na preservação da segurança da informação;
- Orientar as ações de segurança da informação para reduzir riscos e garantir a integridade, confidencialidade e disponibilidade da informação;
- Manter o Sistema de Gestão de Segurança da Informação no âmbito do SENAI CIMATEC;
- Atender aos requisitos da legislação vigente;
- Servir de referência para auditorias, apuração e avaliação de responsabilidades.

3. DEFINIÇÕES

Para compreensão deste documento adotam-se os seguintes termos e definições:

Alta direção: diretoria de tecnologia e inovação (DTI), diretoria adjunta de tecnologia e inovação (DATI), gestores de negócios e gestores de mercado.

Ameaça: causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização. Uma ameaça que se concretiza gera um incidente.

Colaborador: todo e qualquer empregado.

Confidencialidade: é a garantia de sigilo, ou seja, a informação é acessível somente a pessoas autorizadas a terem acesso.

Disponibilidade: é a garantia de que a informação e os ativos associados estejam disponíveis para os usuários legítimos, sempre que necessário.

Força de Trabalho: pessoas que compõem uma organização e que contribuem para consecução de suas estratégias, objetivos e metas ou realizam atividades de aprendizagem, tais como empregados em tempo integral ou parcial, temporários, estagiários, autônomos e contratados de terceiros que trabalham sob a coordenação direta da organização.

Incidente de segurança da informação: evento ou série de eventos indesejados ou inesperados, que tenham grande probabilidade de comprometer as operações do negócio e ameaçar a segurança da informação.

Informação: conjunto de dados, imagens, textos e quaisquer outras formas de representação dotadas de significado dentro de um contexto.

Integridade: é a garantia da preservação da informação e consistência dos dados ao longo do seu ciclo de vida.

Recursos de Tecnologia da Informação: qualquer sistema de armazenamento ou processamento da informação, serviço ou infraestrutura, ou às instalações físicas que os abriguem, tais como: mídias de armazenamento, dispositivos móveis, serviços de armazenamento e transferência de dados, pen drives, smartphones, tablets, e-mail, planilhas, documentos, computadores, notebooks, servidores, equipamentos de rede, dentre outros.

Segurança da Informação (SI): a informação é um ativo das organizações, ou seja, é um bem que possui valor e, portanto, deve ser protegida, independentemente de ser escrita ou impressa em papel, armazenada eletronicamente, transmitida pelo correio ou através de meios eletrônicos, mostrada em filmes ou falada em conversas. A segurança da informação é alcançada através da preservação da integridade, confidencialidade e disponibilidade da informação.

Software malicioso ou malware: qualquer software que realiza ações nocivas aos sistemas, como vírus, worm, ransonware e afins.

Tratamento: toda operação realizada com dados e informações, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle, modificação, comunicação, transferência, difusão ou extração.

Uso compartilhado de dados ou informações: compartilhamento de informações sob salvaguarda dos agentes de tratamento, entre entidades, no cumprimento de suas competências legais, reciprocamente com autorização específica para a modalidade de tratamento permitida.

Vulnerabilidade: fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças.

4. ESCOPO

Esta Política considera a abrangência da segurança da informação nos aspectos físico, lógico, comportamental, pessoas, processos e tecnologias preservando a confidencialidade, integridade e disponibilidade das informações do SENAI CIMATEC ou sob sua salvaguarda.

5. PAPÉIS E RESPONSABILIDADES

A alta direção do SENAI CIMATEC, força de trabalho, fornecedores e parceiros têm responsabilidade sobre as informações que acessam e manipulam. A observância das diretrizes constantes nesta política, independe da existência de controles que, de forma total ou parcial, obriguem o seu cumprimento.

5.1. Comitê de Segurança da Informação SENAI CIMATEC

O Comitê de Segurança da Informação, formado por representantes das diversas áreas do SENAI CIMATEC, será designado pela DTI ou DATI e assume como responsabilidades:

a) propor a Política de Segurança da Informação e documentos relacionados e revisá-la ordinariamente a cada 3 (três) anos, ou a qualquer tempo, quando necessário;

b) viabilizar que as atividades de segurança da informação sejam executadas em conformidade com a Política de Segurança da Informação vigente;

c) avaliar violações ou não conformidades com a Política de Segurança da Informação e propor como tratá-las;

d) assessorar auditorias para verificar o cumprimento da política, guias, procedimentos e outros documentos afins relacionados com a Segurança da Informação;

e) avaliar o resultado de análises, auditorias e incidentes de segurança da informação e propor ações corretivas ou que reduzam a probabilidade da ocorrência;

f) propor capacitação e conscientização em segurança da informação, definindo o conteúdo, a periodicidade e público-alvo dos treinamentos.

g) assessorar a alta direção nos assuntos relativos à segurança da informação.

Para desempenhar as atribuições listadas, o Comitê de Segurança da Informação deve se reunir regularmente, com frequência a ser definida pelos seus membros, podendo, por meio de convocação do coordenador, reunir-se extraordinariamente para tratar de assuntos específicos ou urgentes.

5.2. Coordenador de Segurança da Informação

O Coordenador de Segurança da Informação será designado pela alta direção, sendo o principal responsável pelas iniciativas de segurança. As responsabilidades do Coordenador são:

a) fornecer o embasamento técnico necessário ao Comitê de Segurança da Informação, para apoiar a tomada de decisão;

b) coordenar a implantação dos controles e processos de segurança da informação aprovados pela alta direção;

c) Identificar fragilidades, exposição da informação e dos recursos de processamento da informação e ameaças significativas;

d) coordenar ações emergenciais de segurança da informação, que não possam aguardar uma reunião do Comitê de Segurança da Informação;

e) gerenciar incidentes e fragilidades de segurança da informação para apresentação periódica ao Comitê de Segurança da Informação;

f) realizar periodicamente análise crítica independente da segurança da informação, considerando inclusive auditorias realizadas, para avaliar a efetividade desta Política de Segurança da Informação e dos controles de segurança da informação adotados.

g) realizar avaliações de riscos regulares com o objetivo de monitorar e melhorar continuamente a segurança da informação.

5.3. Diretoria do SENAI CIMATEC, força de trabalho, fornecedores, clientes e parceiros

a) cumprir as determinações desta Política de Segurança da Informação, seus respectivos guias e procedimentos;

b) proteger a informação contra acesso não autorizado, divulgação, modificação, destruição ou interferência, em todo o seu ciclo de vida;

c) notificar, com a maior brevidade possível, quaisquer incidentes, fragilidades ou falhas de segurança, e mau funcionamento de hardware ou software as equipes de suporte e tratamento de incidentes de segurança.

Convém destacar que fragilidades ou falhas de segurança não devem ser testadas pelos usuários, mas apenas notificadas quando percebidas. Da mesma forma, ações corretivas não devem ser adotadas por conta própria.

Adicionalmente, o cumprimento desta Política de Segurança da Informação faz parte das responsabilidades da força de trabalho, que deverá assegurar também que os fornecedores, clientes e parceiros a sigam.

6. NÍVEIS DE SEGURANÇA

O objetivo do SENAI CIMATEC é fornecer serviços de alta qualidade aos seus stakeholders. Portanto, um nível básico da segurança deve ser incorporado nos serviços prestados. Quando a infraestrutura, instalações de TI e recursos do SENAI CIMATEC forem compartilhados entre vários clientes, o nível mínimo de segurança será o nível básico. Este nível não pode ser reduzido, já que isso pode comprometer o nível de segurança de outros clientes.

7. MELHORIA CONTÍNUA

Como em todos os aspectos de seus negócios, o SENAI CIMATEC está comprometido em melhorar e monitorar continuamente a segurança para atender às exigências dos clientes. Com base em avaliações de risco regulares, o Comitê de Segurança da Informação irá aconselhar regularmente a alta direção sobre as melhorias de segurança necessárias em serviços e documentos. A eficácia do processo de melhoria contínua da segurança será constantemente medida por indicadores e auditorias internas / externas.

8. PORTFÓLIO DE SERVIÇOS

A segurança da informação deve ser um tema padrão do processo de criação de qualquer serviço prestado pelo SENAI CIMATEC. Quando o SENAI CIMATEC desenvolver novos serviços, uma análise dos riscos e requisitos de segurança da informação deve ser realizada quando aplicável.

9. PROPRIEDADE INTELECTUAL

O respeito à propriedade intelectual está intimamente relacionado ao negócio do SENAI CIMATEC. As seguintes diretrizes devem ser observadas:

- A força de trabalho do SENAI CIMATEC deve respeitar o uso legal de propriedade intelectual de terceiros, incluindo softwares, livros, artigos, filmes, áudio, imagens, ou qualquer outro conteúdo sujeito à legislação de propriedade intelectual.

- Qualquer trabalho desenvolvido pela força de trabalho pertence ao SENAI CIMATEC, exceto, em casos de negociações específicas aprovadas pela DTI / DATI.

10. ACORDO DE CONFIDENCIALIDADE

Considera-se celebrado o acordo de confidencialidade com a força de trabalho quando da assinatura do mesmo no processo de contratação. Cláusulas referentes a confidencialidade e segurança da informação devem constar em todos os instrumentos celebrados com fornecedores, parceiros e clientes que tenham acesso a quaisquer informações confidenciais do SENAI CIMATEC ou sob sua salvaguarda (tais como contratos, convênios, termos de cooperação, parcerias e de compromisso, prestação de serviços, dentre outras) observando-se que:

- Informações confidenciais compartilhadas devem ser protegidas, utilizando boas práticas de governança e técnicas de segurança da informação;

- Os parceiros, fornecedores e clientes são responsáveis pelas boas práticas de governança e técnicas de segurança da informação;

- O acordo de confidencialidade é valido durante todo o período de vigência do contrato e adicionalmente terá duração mínima de 20 (vinte) anos após o término da vigência ou obedecerá ao prazo que tiver sido especificamente definido no instrumento firmado;

Em quaisquer outros casos, o prazo de validade do acordo de confidencialidade obedecerá a regulamentação que orienta a atividade específica, como: saúde, educação, propriedade intelectual, dentre outras.

11. TREINAMENTO E CONSCIENTIZAÇÃO EM SEGURANÇA DA INFORMAÇÃO

Para toda a força de trabalho deve ser realizada campanha de conscientização referente a segurança da informação.

Todos os colaboradores devem receber orientações periódicas em Segurança da Informação para garantir que eles estão cientes da Política de Segurança da Informação do SENAI CIMATEC, e equipados para apoiar a implementação destas regras no decurso de seu trabalho. Os líderes das áreas devem indicar a participação de seus colaboradores.

12. PROCESSOS ADMINISTRATIVOS

Violações a esta Política de Segurança da Informação e demais documentos complementares sobre segurança da informação serão analisados pelo Comitê de Gestão de Segurança da Informação e superior imediato da área onde o fato ocorreu, conforme a natureza, gravidade e impacto causado.

Poderá ser recomendada a instauração de sindicância para averiguação dos fatos, quando houver indícios de ocorrência de infração funcional, sem prejuízo de responsabilização penal e civil do suposto infrator.

Concluída a apuração, conforme normas específicas e comprovada a ocorrência da infração, poderão ser aplicadas as penalidades previstas na legislação vigente e nos regulamentos internos, observada a proporcionalidade entre a infração e a sanção respectiva, e respeitado os primados da ampla defesa e do contraditório.

13. FORNECEDORES, PARCEIROS E TERCEIROS

O estabelecimento de parceria e terceirizações devem passar por uma análise prévia de risco quando pertinente, estabelecendo-se controles e procedimentos adequados às execuções das parcerias e serviços firmados, a serem definidos e estabelecidos em contrato.

Deve ser assegurado que os fornecedores, parceiros e terceiros terão ciência e cumprirão com políticas, guias, padrões e procedimentos de segurança da informação do SENAI CIMATEC. É de responsabilidade do fornecedor, parceiro ou empresa terceirizada garantir que sua equipe seja informada e que cumprirá a política de segurança da informação do SENAI CIMATEC.

14. CONFORMIDADE COM A POLÍTICA DE SEGURANÇA

O projeto, operação e utilização de cada instalação, rede, sistema, aplicação e suas informações devem estar em conformidade com esta Política de Segurança da Informação e demais documentos complementares sobre segurança da informação, acordos contratuais, as leis relevantes e outros requisitos.

15. VERIFICAÇÃO DE CONFORMIDADE

A gestão da conformidade com esta Política de Segurança da Informação e demais documentos complementares sobre segurança da informação, no SENAI CIMATEC será analisada pelo comitê de segurança da informação. Os gestores devem garantir que a ação oportuna, adequada e auditável é tomada para resolver as não conformidades.

16. GUIAS E DOCUMENTOS COMPLEMENTARES DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

O sistema de gestão de segurança da informação é constituído por políticas, manuais, procedimentos e guias que dão suporte à força de trabalho, parceiros, clientes e terceirizados quanto ao manuseio e guarda das informações, cujo objetivo é a orientação na implementação de processos, mecanismos e procedimentos que visem o fortalecimento da segurança da informação no ambiente corporativo.