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 27001:2022 e 27002:2022, de acordo com a legislação vigente, realidade e requisitos de negócio.

Para assegurar todos os seus aspectos, é necessário que seja colocado em prática um processo de gestão de segurança da informação. A Norma ISO/IEC 27001:2022 (“Information Security, Cybersecurity and Privacy Protection - 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 de serviços e operações (DSO), 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.

Anonimização: utilização de meios técnicos que desassociam um dado ou informação pessoal de um indivíduo, de modo que o dado não possa mais ser vinculado, direta ou indiretamente, ao seu titular;

ANPD: autoridade Nacional de Proteção de Dados, órgão da administração pública federal, responsável por zelar, implementar e fiscalizar o cumprimento da LGPD.

Colaborador: todo e qualquer empregado.

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

Consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada.

Controlador: pessoa jurídica a quem compete a tomada de decisões acerca do tratamento de dados pessoais pela entidade.

Dado pessoal: informação relacionada a pessoa física/natural identificada ou identificável, que poderá ser classificado como dado pessoal sensível, quando se referir origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, vinculado a uma pessoa natural.

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

Encarregado de Proteção de Dados (DPO): pessoa física ou jurídica, indicada pelo controlador, para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).

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.

LGPD: Lei Geral de Proteção de Dados Pessoais.

Operador: é uma pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.

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.

Titular do dado ou da informação pessoal: pessoa física a quem se referem os dados ou informações pessoais que são objetos de tratamento.

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. LIDERANÇA

A liderança do SENAI CIMATEC é representada pelo Diretor Geral, Diretor de Tecnologia e Inovação, Diretor de Serviços e Operação, Superintendente de Novos Negócios, Superintendente de Educação e Ciência, Gestores de Negócio e Gestores de Mercado.

5.1. LIDERANÇA E COMPROMISSO

A liderança SENAI CIMATEC evidencia o seu comprometimento com o desenvolvimento, implementação, manutenção e melhoria contínua do Sistema de Gestão, comunicando à organização da importância do atendimento aos requisitos de clientes, requisitos estatutários e regulamentares, com o estabelecimento da Política de Segurança da Informação, assegurando a disponibilidade de recursos, entre outras ações de fundamental importância para a eficácia do Sistema de Gestão de Segurança da Informação.

6. 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.

6.1. 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 DSO 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.

6.2. 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.

6.3. 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.

6.4. Controlador

O Controlador é o responsável por determinar as ações de tratamento de dados pela organização, podendo ser responsabilizado judicial e administrativamente em caso de incidentes de dados ou falha de segurança, ou de descumprimento à legislação protetiva da privacidade.

O Controlador possui as seguintes responsabilidades:

a) Tomar decisões referentes aos processos de gestão, atentando para as diretrizes da segurança das informações e privacidade dos dados pessoais;

b) Adotar medidas de boas práticas para tratamento de dados pessoais pela organização, observadas as exigências legais;

c) Responsabilizar-se junto a instituições públicas e privadas acerca das decisões sobre segurança da informação da organização e tratamento de dados pessoais pela organização.

6.5. Operador

Refere-se como Operador o terceiro, pessoa física ou jurídica, que realiza tratamento de dados pessoais em nome do Controlador, nos termos do instrumento contratual firmado. O Operador poderá ser

responsabilizado solidariamente em caso de incidente de dados pessoais, devendo, portanto, adotar boas práticas de proteção de dados ao executar suas atividades.

Compete ao Operador:

a) Realizar as atividades de tratamento das informações de acordo com as orientações do controlador;

b) Responsabilizar-se pelas ações executadas, respondendo pela inobservância das orientações do Controlador e/ou da legislação vigente, para o tratamento dos dados em nome do Controlador.

6.6. Encarregado de Proteção de Dados / DPO

O Encarregado é o responsável pela execução das atividades de tratamento de dados pelo Controlador/Entidade. É a pessoa que detém conhecimento acerca de sistemas, processos e legislação sobre tratamento de dados e segurança das informações, cabendo-lhe adotar práticas condizentes com o negócio das entidades e realidade de mercado. As informações de identificação e contato do Encarregado devem ser amplamente divulgadas e inseridas em documentos relacionados ao tratamento de dados pessoais.

Compete ao Encarregado de Proteção de Dados:

a) Gerir o recebimento das solicitações, reclamações e comunicações dos titulares dos dados, prestar esclarecimentos e adotar providências;

b) Receber notificações da Autoridade Nacional de Proteção de Dados e demais órgãos públicos e adotar providências;

c) Orientar dirigentes, colaboradores e prestadores de serviços contratados pelas entidades acerca das práticas a serem executadas para a proteção de dados pessoais e segurança das informações;

d) Executar as demais atribuições determinadas pelo Controlador, ou estabelecidas em normas complementares, ou requeridas pela ANPD;

e) Acompanhar o processo de adequação das atividades de tratamento de dados às exigências legais;

f) Fiscalizar as ações de tratamento de dados pessoais pelas entidades e indicar a necessidade de melhorias em processos e sistemas, para garantia da conformidade à lei.

g) Subsidiar o Controlador acerca das ações a serem adotadas para a garantia da segurança da informação e proteção dos dados pessoais;

h) Orientar as atividades desenvolvidas pelo Comitê de Segurança da Informação e operadores do Sistema de Gestão de Segurança da Informação;

7. TRATAMENTO DOS DADOS

Em conformidade com a legislação vigente, em especial com a Lei Federal nº 13.709/18 – Lei Geral de Proteção de Dados Pessoais (LGPD), o tratamento de dados pessoais deve observar os seguintes fundamentos:

- Respeito à privacidade;
- Autodeterminação informativa;
- Liberdade de expressão;
- Inviolabilidade da intimidade, honra e imagem;
- Desenvolvimento econômico, tecnológico e inovação;

As ações referentes a tratamento de dados pessoais pelo SENAI CIMATEC devem atentar para a finalidade e necessidade do tratamento, a adequação dos processos e tecnologias, a qualidade dos dados coletados, assegurando tratamento isonômico, livre acesso aos dados por seu titular, transparência nas ações e segurança das informações.

8. TRATAMENTO DOS DADOS PESSOAIS

O tratamento de dados pessoais consiste nas operações de coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração das informações pela organização.

Para o tratamento de dados pessoais, o SENAI CIMATEC deverá observar a legislação protetiva da privacidade e dos dados pessoais, em especial à Lei Federal nº 13.709/2018, e as seguintes diretrizes:

- Tratar somente os dados estritamente necessários para a execução do serviço;

- Eliminar os dados, após o tratamento concluído/finalizado, salvo, se a legislação exigir a guarda das informações por período superior;

- Sempre que possível, tratar os dados de forma anonimizada;

- Observar os fundamentos e princípios da legislação na execução de suas atividades;

- Preservar a segurança e o sigilo das Informações para o tratamento dos dados pessoais pela organização;

- Utilizar/Manter os Sistemas digitais em conformidade com as boas práticas de Segurança da Informação, quanto à disponibilidade, confidencialidade e autenticidade, adicionalmente empregando sempre que possível os princípios de Security By Design em seus processos, sistemas digitais e infraestrutura;

- Tratar os dados exclusivamente para as finalidades definidas nos instrumentos firmados com os titulares dos dados ou em conformidade com a legislação;

- Manter um canal de comunicação direto com os titulares de dados, assim como a ANPD, para interlocução com o Encarregado;

- Observar os direitos do titular dos dados e atender às suas solicitações, em conformidade com a lei;

- Comunicar à ANPD e ao titular a ocorrência de incidente de dados que possa acarretar riscos ou danos efetivos a este último;

- Elaborar e executar planos de resposta a incidentes de dados;

Toda operação envolvendo dados pessoais realizada por esta organização deverá estar enquadrada nas hipóteses de tratamento previstas na legislação, e atender às finalidades legais e/ou especificadas no instrumento celebrado com o titular do dado.

9. DIREITO DO TITULAR

O tratamento de dados pessoais pelo SENAI CIMATEC deve resguardar os direitos do titular dos dados especificados na lei.

Devem estar assegurados os direitos do titular de requerer, durante o período de tratamento de seus dados, as seguintes informações:

- Esclarecimentos sobre a possibilidade de não fornecer o consentimento e as consequências da negativa;
- Confirmação da existência do tratamento de seus dados pessoais;
- Acesso facilitado às informações sobre o tratamento de seus dados, sendo-lhe garantido conhecimento sobre: os dados existentes e suas formas de tratamento; a finalidade e duração do tratamento; o compartilhamento dos dados e sua finalidade;
- Atualização de seus dados, correção de dados incompletos, inexatos ou desatualizados;

- Anonimização, bloqueio ou eliminação de dados desnecessários; excessivos ou tratados em desconformidade com o disposto na lei;

- Eliminação dos dados – exclusão das informações pessoais dos bancos de dados e sistemas da organização - Direito ao esquecimento:

    - Quando os dados coletados não forem mais necessários para cumprimento do objeto da coleta (finalidade alcançada) e das exigências legais;
    - Fim do período de tratamento;
    - Revogação do consentimento.

10. 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 é definido pelas políticas, normas, guias e procedimentos implementados pela organização e não pode ser reduzido, já que isso pode comprometer o nível de segurança de outros clientes.

11. 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.

12. 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.

13. 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 / DSO.

14. 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.

15. 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.

16. 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.

17. 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.

18. 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.

19. 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.

20. 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.

21. HISTÓRICO DE ALTERAÇÕES

Versão	Resumo da Alteração
08	Atualização de logomarca.

22. HISTÓRICO DE APROVAÇÃO

Elaboração/Revisão:	**Verificação/Validação:**	**Emissão/Disponibilização:**	**Aprovação:**
Roald Holum (Coordenador de Segurança)	Comitê de Segurança da Informação	Benisane Maria de Santana (NGQ)	Rodrigo Vasconcelos Alves Data: 09/2025