ÁREA	CÓDIGO / VERSÃO
GERÊNCIA SENIOR DE TECNOLOGIA DA INFORMAÇÃO	PSI v.05

TÍTULO	VIGÊNCIA A PARTIR DE
POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE	23.02.2021 CLASSIFICAÇÃO: **PÚBLICA**

SUMÁRIO

1. OBJETIVO

Estabelecer diretrizes, normas e procedimentos para adoção de mecanismos relacionados à segurança dos **ativos de informação** do SESI-SP e SENAI-SP, prezando pela confidencialidade, integridade, disponibilidade, autenticidade, legalidade e privacidade.

A constituição da presente Política de Segurança da Informação visa minimizar os riscos de falhas, danos e prejuízos que possam comprometer a operação, imagem ou missão do SESI-SP e do SENAI-SP.

Sua divulgação visa também apresentar os requisitos e conceitos de Segurança da Informação aplicados pelas entidades SESI-SP e SENAI - SP, delimitando e esclarecendo o tema para relação institucional com colaboradores, clientes, fornecedores e órgãos de controle.

2. DEFINIÇÕES

2.1. Com a finalidade de aplicação desta Política de Segurança, serão considerados como "**Ativos de Informação**":

2.1.1. Hardware – elementos tais como: equipamentos computacionais, periféricos, smartphones corporativos, infraestrutura física e de rede, dispositivos de processamento, armazenamento de dados e instalações físicas.

2.1.2. Software – elementos tais como: aplicativos, sistemas operacionais, bancos de dados, navegadores e ferramentas de desenvolvimento e sistemas corporativos.

2.1.3. Dados: unidade básica da informação, correspondendo a um conteúdo quantificado que, isoladamente, não permite a compreensão ou transmissão de conhecimento.

2.1.4. Informação: resultado do processamento de dados através de um sistema de informação, permite a compreensão e transmissão de conhecimento.

2.1.5. Sistema de Informação: elementos manuais ou automatizados, que tem o objetivo de coleta, armazenamento, processamento, transformação ou transmissão de dados e informações.

3. ABRANGÊNCIA

3.1. Esta política abrange as entidades SESI-SP e SENAI-SP, devendo ser aplicada por dirigentes, empregados efetivos e temporários, estagiários e aprendizes, bem como por terceiros que manuseiam ou custodiam qualquer ativo de informação das instituições.

3.2. Todas as normas e diretrizes desta Política de Segurança devem ser seguidas e aplicadas durante toda relação trabalhista ou comercial com as Instituições SESI-SP e SENAI-SP, seja qual for o local onde a ações sejam exercidas, podendo ainda por força de contrato ou termos específicos ter sua aplicação e alcance estendidos.

4. COMITÊ GESTOR DE SEGURANÇA DA INFORMAÇÃO – CGSI

4.1. Ao Comitê Gestor de Segurança da Informação do SESI-SP e SENAI-SP compete:

4.1.1. Analisar e recomendar para aprovação superior a Política de Segurança da Informação – PSI;

4.1.2. Acompanhar a implantação das estratégias e planos de ação para aplicação da PSI;

4.1.3. Promover a articulação entre as estratégias do SESI-SP, do SENAI-SP e a PSI;

4.1.4. Divulgar atividades de Segurança da Informação;

4.1.5. Requisitar informações às Diretorias, Gerências Sênior, Assessorias, Áreas Técnicas e Unidades Operacionais do SESI-SP do SENAI-SP sobre o cumprimento da PSI;

4.1.6. Dirimir dúvidas e deliberar sobre questões não contempladas na Política de Segurança da Informação - PSI, normas ou procedimentos associados;

4.1.7. Rever anualmente a Política de Segurança da Informação – PSI.

4.2. Os membros do Comitê de Segurança da Informação – CGSI, serão designados através de Resolução Conjunta entre o Diretor Regional do SENAI-SP e o Superintendente Operacional Regional do SESI-SP.

4.3. A indicação de representantes será feita pelo responsável de cada Área.

4.4. O Comitê de Segurança da informação do SESI-SP e do SENAI-SP, será presidido pelo representante da Área de Tecnologia da Informação, que deverá organizar mesa diretiva para condução dos seus trabalhos.

4.5. Os temas relacionados à segurança da informação serão deliberados através de reuniões dos representantes do Comitê, em periodicidade definida pela área de tecnologia informação ou através de convocação extraordinária.

5. PREMISSAS E DECLARAÇÕES INSTITUCIONAIS

5.1. As instituições SESI-SP e SENAI-SP respeitam a privacidade de todos colaboradores internos e externos, bem como daqueles com quem se relacionam comercialmente. No mesmo sentido existe especial atenção com as informações pessoais de nossos alunos, clientes e fornecedores.

5.2. Para efetiva proteção de dados e informações, bem como o irrestrito cumprimento de leis e marcos legais, esta Política de Segurança da Informação orienta o SESI-SP e SENAI-SP através dos seguintes princípios e obrigações:

5.3. INTEGRIDADE

O acesso e utilização de ativos de informação que permitem a modificação de um dado e/ou informação, deverão ser autorizados somente a sistemas de informação ou pessoas que possuam efetiva e justificada necessidade.

5.3.1. Todo sistema de informação deverá possuir documentação que apresente a necessidade, justificativa e finalidade de coleta, utilização, processamento e transformação dos dados e informações.

5.3.2. Trilhas de auditoria e logs em bancos de dados devem permitir no mínimo, identificar o autor do acesso, dados confidenciais e informações modificados, data e hora do evento, meio de acesso e dispositivo utilizado na ação.

5.4. CONFIDENCIALIDADE, PRIVACIDADE E CLASSIFICAÇÃO DAS INFORMAÇÕES

5.4.1. À partir de sua vigência, é dever institucional do SESI-SP e SENAI-SP o pleno e irrestrito cumprimento da Lei Geral de Proteção de dados (LGPD – Lei 13.709/18), onde são delimitadas as bases e regulamentações relacionadas aos dados pessoais, garantindo ao titular dos dados o controle sobre a coleta, finalidade de utilização, processamento, transformação, compartilhamento, acesso, arquivamento, armazenamento e eliminação.

5.4.2. Todo processo existente ou futuro que necessite aplicar tratamento e operação com dados pessoais, deverá o seu responsável pelo processo

apresentar justificativas e definições para coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, modificação, comunicação, transferência, difusão ou extração.

5.4.3. Qualquer colaborador, fornecedor ou parceiro do SESI-SP e do SENAI-SP está obrigado a aplicar as atuais e futuras orientações relacionadas à Lei Geral de Proteção Dados, sob pena de responsabilização.

5.4.4. Toda relação contratual, sejam elas as já estabelecidas ou por estabelecer, deverão possuir itens ou anexos que definam as obrigações e responsabilidades relativas aos dados pessoais, em alinhamento com as orientações do SESI-SP e SENAI-SP.

5.4.5. Qualquer informação ou dado sob responsabilidade do SESI-SP e SENAI-SP, deverá ser classificado como público, interno, confidencial ou pessoais, sendo a primeira categoria acessível a quaisquer pessoas, a segunda apenas por áreas internas do SESI-SP e SENAI-SP e a terceira apenas por usuários devidamente autorizados.

5.4.5.1. As estipulações e obrigações relativas à confidencialidade não serão aplicadas a qualquer dado que:

5.4.5.1.1. Seja de domínio público no momento da revelação e ou divulgação;

5.4.5.1.2. Já esteja em poder de outra parte, como resultado de sua própria pesquisa, desde que este fato seja comprovado;

5.4.5.1.3. Seja revelado em razão de uma autorização válida ou de uma ordem judicial, somente até a extensão de tais decisões;

5.4.5.1.4. Seja divulgado em cumprimento à exigência legal.

5.4.5.2. A Área de Tecnologia da Informação deverá realizar, com o auxílio dos demais departamentos, o mapeamento das informações, apresentando proposta para implementação da Classificação das Informações ao Comitê Gestor de Segurança da Informação.

5.4.5.2.1. A proposta de classificação das informações deverá conter, no caso de confidencialidade, os procedimentos de compartilhamento e acesso.

5.4.5.2.2. O mapeamento e classificação das informações deverão ser atualizados sempre que necessário.

5.4.5.2.3. Qualquer compartilhamento de dados ou informações, que não possua autorização ou procedimento definido, deverá ser imediatamente interrompido.

5.5. DISPONIBILIDADE

5.5.1. O acesso aos ativos de tecnologia é fundamental para o correto desenvolvimento das atividades do SESI-SP e SENAI-SP. É entendimento das instituições que a disponibilização dos recursos e ativos de tecnologia devem seguir padrões compatíveis com a estratégia do negócio.

5.5.2. Deverá ser mantido Plano de Recuperação de Desastres, refletindo os recursos disponíveis e expectativas das instituições em relação às estratégias de operações e recuperação de situações graves de indisponibilidade.

5.5.3. Equipamentos, sistemas e demais elementos relacionados aos ativos das informações devem ser dimensionados e desenvolvidos seguindo padrões de qualidade que garantam a disponibilidade e minimizem falhas, refletindo assim a expectativa do SESI-SP e SENAI-SP.

5.6. AUTENTICIDADE

5.6.1. A autenticidade é componente essencial na produção, transformação e transmissão de dados e informações, principalmente para garantir os aspectos legais e de interesse institucional.

5.6.2. Sempre que possível ou recomendado, a manipulação dos ativos de tecnologia, produção e transmissão de informações deverão fazer uso de mecanismos criptográficos e/ou certificados digitais, bem como qualquer outro meio único ou complementar que possa garantir a individualização e identificação do ativo de informação e quem o manipulou.

5.7. PROPRIEDADE INTELECTUAL

5.7.1. No sentido de garantir os interesses Institucionais e de relações com o mercado, bem como atender dispositivos legais vigentes, o SESI-SP e o SENAI-SP tem suas atividades baseadas, mas não restritas, pelas seguintes leis e declarações relacionadas à propriedade intelectual:

i. Lei nº 9.279/96 – Lei de Marcas e Patentes;
ii. Lei nº 9.609/98 – Lei de Software;

iii. Lei nº 9.610/98 – Lei sobre Direitos Autorais;
iv. Artigo 5º - Incisos XXII, XXVII, XXVIII e XXIX – Constituição Federal;

5.7.2. Todo e qualquer documento, arquivo, material técnico ou literário, artigos, projetos, processos, patentes, marcas comerciais, nomes de domínios, desenhos industriais, logotipos, lista de clientes, invenções, entre outros, produzidos durante as relações trabalhistas com colaboradores ou contratuais com pessoa de direito jurídico são considerados propriedade intelectual do SESI-SP e do SENAI-SP, não sendo permitida a cópia, divulgação ou eliminação sem autorização expressa.

5.7.3. Qualquer dado ou informação produzido e armazenados nos ativos de informação são propriedade do SESI-SP e do SENAI-SP, desde que os procedimentos para criação e obtenção tenham seguido as premissas desta Política de Segurança da Informação.

6. NORMAS GERAIS PARA USO DOS ATIVOS DE TECNOLOGIA DA INFORMAÇÃO

6.1. HORÁRIO DE UTILIZAÇÃO

6.1.1. Todo colaborador deverá utilizar os ativos de tecnologia da informação de acordo com a jornada de trabalho estabelecida e formalizada pela área de recursos humanos do SESI-SP e do SENAI-SP.

6.1.2. Qualquer necessidade de acesso aos ativos de tecnologia da informação, em horários diferentes daqueles estabelecidos pela área de recursos humanos, deverá obrigatoriamente ser autorizado de forma expressa pelo superior imediato do colaborador, sendo considerada falta grave a desobediência desta disposição;

6.1.3. Nenhuma autorização de uso dos ativos de tecnologia da informação poderá infringir disposições legais ou regras definidas pelo SESI-SP e SENAI-SP.

6.1.4. É responsabilidade de todo gestor o efetivo acompanhamento das atividades de seus subordinados quanto ao uso dos ativos de tecnologia da informação, garantindo que as orientações sobre jornada de trabalho emanadas pela Área de Recursos Humanos sejam plenamente atendidas.

6.1.5. A utilização dos ativos de tecnologia da informação em horário diferente daquele estabelecido pela área de recursos humanos, sem a autorização expressa do superior imediato, será considerada grave infração às normas estabelecidas nesta PSI.

6.1.6. Todo prestador de serviços que demandar o uso de ativos de tecnologia deverá obedecer às determinações desta Política de Segurança da Informação, normas legais vigentes e disposições firmadas na relação contratual com as entidades SESI e SENAI-SP.

6.2. UTILIZAÇÃO DE LOGIN E SENHA

6.2.1. O acesso aos recursos computacionais do SESI-SP e do SENAI-SP é autorizado mediante a apresentação de credenciais de acesso, formadas no mínimo por login e senha.

6.2.2. É responsabilidade do colaborador garantir o sigilo da sua senha, bem como a definição da mesma em conformidade com as orientações emanadas pela área de tecnologia da informação do SESI-SP e SENAI-SP.

6.2.3. As credenciais de acesso são intransferíveis, sendo o seu compartilhamento considerado grave infração à presente política de segurança, seja qual for o propósito ou necessidade.

6.2.4. A suspeita ou uso indevido de credenciais de acesso deverão ser reportados imediatamente à área de tecnologia da informação para que medidas de segurança e controle sejam adotadas.

6.3. UTILIZAÇÃO DOS RECURSOS COMPUTACIONAIS

6.3.1. Os ativos de tecnologia da informação são disponibilizados aos colaboradores e terceirizados para que suas atribuições e atividades sejam desempenhadas dentro dos mais satisfatórios padrões.

6.3.2. Não é autorizada, sob qualquer hipótese, a utilização dos ativos de tecnologia da informação para finalidade diferente daquelas previstas ao uso corporativo, sejam as delimitadas nesta política ou em qualquer outra norma complementar.

6.3.3. É vedada a utilização dos recursos computacionais para fins pessoais, inclusive o armazenamento de informações do colaborador, tais como programas, arquivos, músicas, fotos etc.

6.3.4. Fica garantido ao SESI-SP e ao SENAI-SP o direito remover, sem prévio aviso, qualquer conteúdo particular armazenado nos ativos de tecnologia, bem como a interrupção do acesso à serviços que não estejam sendo utilizados dentro das expectativas das instituições.

6.3.5. Conforme previsto nesta política, os ativos de tecnologia da informação são propriedades do SESI-SP e SENAI-SP, desta forma e a critério destas, o acesso aos ativos poderá ser revogado a qualquer momento.

6.3.6. No ato de desligamento de colaboradores do quadro de funcionários do SESI-SP e do SENAI-SP ou término de contrato de terceiros, os acessos aos ativos computacionais serão interrompidos de forma imediata e irrevogável, não sendo permitidas ações de cópias de informações.

6.3.7. O acesso aos ativos de tecnologia da informação, tais como e-mails, arquivos, equipamentos, etc. pertencentes a outros colaboradores ou ex-colaboradores, somente será permitido após apresentação de justificativa e autorização expressa do diretor ou gerente das unidades ou áreas corporativas.

6.4. NORMAS ESPECÍFICAS E COMPLEMENTARES

6.4.1. A área de tecnologia da informação do SESI-SP e do SENAI-SP disponibiliza, em sua intranet corporativa, normas complementares que deverão ser seguidas da mesma forma daquelas contidas na presente Política de Segurança da Informação – PSI.

6.4.2. As normas complementares podem ser acessadas através da intranet, por meio das abas *DOCUMENTAÇÃO > CORPORATIVO.*
"GESTÃO DOCUMENTAL > DOCUMENTAÇÃO CORPORATIVO > POLITICAS E OBJETOS > POLITICA DE SEGURANÇA DA INFORMAÇÃO > NORMAS".

6.4.3. Dada a finalidade e informações técnicas presentes em tais normas, a disponibilização não pode ser pública. O acesso dos órgãos de controle a estes documentos é garantido conforme previsões legais vigentes.

7. MONITORAMENTO

7.1. Com o intuito de garantir o cumprimento das disposições contidas na presente Política de Segurança da Informação, visando a segurança institucional, dos colaboradores, bem como dos ativos de tecnologia da informação de sua propriedade ou sob sua custódia, o SESI-SP e o SENAI-SP dentro dos limites legais poderá:

7.1.1. Implantar ferramentas ou sistemas de monitoramento dos ativos de tecnologia da informação, tais como estações de trabalho, servidores, correio eletrônico, acesso à internet, dispositivos móveis, redes físicas e wireless.

7.1.2. Empregar informações obtidas através de sistemas de monitoramento em procedimentos de auditoria, processos administrativos disciplinares e processos judiciais.

7.1.3. Realizar inspeção nos equipamentos a qualquer momento sem prévio aviso ou autorização do usuário, procedimento este executado de forma física local ou remotamente.

8. VIOLAÇÃO DE SEGURANÇA

8.1. Todo descumprimento dos dispositivos ou premissas da presente Política de Segurança da Informação e de suas normas complementares, bem como qualquer ação que coloque em risco os Ativos de Informação do SESI-SP e do SENAI-SP, serão considerados violação de segurança.

8.2. As violações de segurança deverão ser analisadas pela área de tecnologia da informação, que poderá solicitar a apreciação do Comitê Gestor de Segurança da Informação e a apuração de responsabilidade para adoção de medidas disciplinares, sem prejuízo da adoção de eventuais medidas judiciais a serem avaliadas pela Área Jurídica.

8.3. A área de tecnologia da informação poderá adotar medidas emergenciais para garantir a segurança dos ativos de tecnologia da informação, tais como suspender, cancelar, bloquear ou alterar autorizações de acesso, excluir ou isolar arquivos, remover hardware ou softwares, bem como requisitar a devolução de equipamentos pertencentes ao SESI-SP e SENAI-SP.

9. DISPOSIÇÕES GERAIS

9.1. A presente Política de Segurança da Informação deverá ser amplamente divulgada a todos usuários dos ativos de tecnologia da informação.

9.2. Todo usuário dos ativos de tecnologia da informação deverá atestar o conhecimento da presente Política de Segurança da Informação, seja pela assinatura de aceite ou qualquer outro meio oficial divulgado pelo SESI-SP e SENAI-SP para esta finalidade de comprovação.

9.3. Itens que preveem a garantia do sigilo e privacidade das informações, em conformidade com as premissas desta política, deverão estar presentes ou anexos aos contratos firmados pelo SESI-SP e SENAI-SP.

9.4. As situações não previstas neste instrumento e relacionadas aos ativos de informação do SESI-SP e SENAI-SP deverão ser submetidas à deliberação do Comitê Gestor de Segurança da Informação.

10. CONTROLE DE REVISÕES

- A presente Política de Segurança da Informação é resultado da reformulação estrutural e conceitual em relação à versão 04.
- Todo histórico anterior detalhado de alterações pode ser consultado na versão 4 da PSI.

VER.	DATA	NATUREZA DA ALTERAÇÃO
01	12.09.13	Primeira emissão.
02	01.11.14	Ajustes diversos.
03	01.02.16	Ajustes diversos.
04	01.12.16	Ajustes diversos.
05	12.12.20	Reestruturação e revisão PSI. Adequação para divulgação Pública.

Documento
Política de Segurança da Informação e Privacidade

Elaboração
Kleder Augusto de Andrade Silva
Gerência Sênior de Tecnologia da Informação

Supervisão
César Farah Domingues
Gerência Sênior de Tecnologia da Informação

Aprovação
CGSI
Comitê Gestor de Segurança da Informação

Publicação
25/02/2021

Versão
5.0

Classificação
Pública