Política de Segurança da Informação

Documento de Normas Administrativas

SisNormas Senac São Paulo

V. 10

Histórico de revisões

Versão	Data	Alteração
Versão 1.0	06/12/2010	Lançamento da Primeira versão
Versão 2.0/7.0	---	Arquivadas
Versão 8.0	29/04/2019	Adequação da política, termos tecnológicos e entrada das normas administrativas.
Versão 9.0	29/06/2021	Adequação da política, termos tecnológicos, comunicadores instantâneos, suporte aos alunos via VPN e LGPD.
Versão 10	24/04/2024	Adequação da política, termos tecnológicos, política de Senhas, redes sem fio, segmentação de ambiente, publicações internas e externas e inovação e uso de novas tecnologias.

Este documento deve:

1. Estar sempre atualizado;
2. Ter cópia controlada e somente gerada pela área responsável pela divulgação dos Instrumentos Normativos;
3. Ser divulgado a todos os funcionários, prestadores de serviços, estagiários e afins da instituição.

Sumário

1. Sobre a Política de Segurança da Informação (PSI)

A Política de Segurança da Informação (PSI) é o documento que orienta e estabelece as diretrizes corporativas do Senac São Paulo para a proteção dos ativos de informação e a prevenção da responsabilidade legal para todos os usuários. Deve, portanto, ser cumprida e aplicada em todas as áreas da instituição.
A PSI segue as leis vigentes no Brasil e foi elaborada com base nas recomendações propostas pela norma ABNT NBR ISO/IEC 27002:2022, NIST Cybersecurity Framework 2.0, CIS Critical Security Controls Version 8, reconhecidos mundialmente como um código de prática para a gestão da segurança da informação.

Paralelamente, foi desenvolvida uma Política de Segurança da Informação Educacional para aumentar a segurança da infraestrutura tecnológica direcionada ao uso acadêmico. O objetivo é orientar os nossos clientes a utilização dos ativos oferecidos.
Tais documentos encontram-se disponíveis na intranet do Senac, seção SisNormas.

2. Conceitos e Definições

Ativo: todo e qualquer bem do Senac que possui valor econômico, incluindo a informação, e todo o recurso utilizado para o seu tratamento, tráfego e armazenamento.

Ativo Crítico e Sensível: todo ativo considerado essencial para o Senac, cujo acesso por pessoas não autorizadas ou a falta de acesso por quem é permitido podem causar danos à instituição.

Cavalo de Troia (*Trojan horse*): programa malicioso que cria abertura para outros programas e invasões indesejadas.

Código Executável: arquivo interpretado pelo computador como um comando de execução para determinadas funções.

Código Malicioso: programa que possibilita ações danosas, como vírus, worms, trojans, spywares, malware, botnet, ransomware, entre outros.

Colaborador Interno: qualquer pessoa que execute atividade profissional e que possua algum tipo de contrato de trabalho com o Senac (Exemplos: funcionários e estagiários).

Colaborador Externo: qualquer pessoa contratada por empresa terceirizada que execute alguma atividade profissional nas dependências do Senac, sem vínculo empregatício (Exemplos: consultores e prestadores de serviços).

Confidencialidade: garantia de que o acesso à informação seja obtido somente por pessoas autorizadas.

Comunicadores Instantâneos: aplicativos que permitem interatividade, troca de conversas e conteúdos em tempo real. Ex. WhatsApp, Telegram, outros.

Custodiante: quem detém a guarda da informação, mas não é necessariamente seu proprietário.

Cyberbullying: prática negativa de assédio moral que afeta o psicológico de outra pessoa por meio de recursos tecnológicos, como publicações na internet e o envio de fotos e vídeos com mensagens ofensivas pelo celular ou qualquer outro dispositivo móvel.

Dados Pessoais: informação relacionada a pessoa natural/física identificada ou identificável.

Dados Pessoais Sensíveis: dado pessoal sobre origem racial, ou étnica, convicção religiosa, opinião política, filiação à sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

Disponibilidade: garantia de que os usuários autorizados obtenham, sempre que necessário, acesso à informação e aos ativos correspondentes.

Informação: todo e qualquer conteúdo ou dado que tenha valor para alguma organização ou pessoa. Ela pode estar guardada para o uso restrito ou exposta ao público para consulta ou aquisição.

Informação Sensível: toda informação sigilosa que, se divulgada, pode resultar em danos e/ou, prejuízos de qualquer ordem, perda de vantagem, inclusive financeira, bem como impacto negativo para o Senac.

Integridade: capacidade de garantir que a informação esteja mantida em seu estado original, conforme foi concebida, a fim de protegê-la contra alterações indevidas, intencionais ou acidentais na guarda ou transmissão.

Parceiros: Empresas, órgãos públicos e demais instituições que possuem contrato com o Senac com objetivos em comum, unindo esforços em suas competências e expertises, sem que haja remuneração, mas apenas empenho de serviços por cada parte.

Peer to Peer*:* arquitetura de redes de computadores em que cada um dos pontos funciona como cliente e servidor possibilitando o compartilhamento de arquivos. Habitualmente são utilizadas para o compartilhamento de vídeos e músicas.

Segurança da Informação: preservação da confidencialidade, integridade e disponibilidade da informação.

Spam: e-mails não solicitados e normalmente enviados para um grande número de pessoas.

Usuário: todo funcionário, prestador de serviço, estagiário e afins que tenham acesso aos recursos tecnológicos oferecidos pelo Senac.

Vírus: programa malicioso que se propaga e infecta o computador.

Worm: programa semelhante ao vírus, que infecta o sistema, tendo como característica a auto replicação.

3. Objetivos da Política de Segurança da Informação

- Estabelecer diretrizes e normas que permitam aos funcionários, prestadores de serviços, estagiários e afins do Senac seguir padrões de comportamento desejáveis e aceitáveis, de acordo com a legalidade e as boas práticas mundiais, a fim de mitigar riscos técnicos e jurídicos;
- Nortear a definição de procedimentos específicos de Segurança da Informação e a implementação de controles e processos para o atendimento de seus requisitos;
- Preservar a confidencialidade, a integridade e a disponibilidade das informações do Senac;
- Prevenir possíveis incidentes e responsabilidade legal da instituição e de seus funcionários, prestadores de serviços, estagiários e afins;
- Garantir a normalidade e a continuidade das atividades do Senac, protegendo os processos críticos contra falhas ou desastres significativos;
- Atender aos requisitos legais, regulamentares e contratuais pertinentes à atividade do Senac;
- Minimizar os riscos de danos, perdas financeiras, participação no mercado, confiança de clientes e de parceiros ou qualquer outro impacto negativo nas atividades do Senac resultante de uma falha de segurança;
- Assegurar o treinamento contínuo e atualizado das políticas e dos procedimentos de Segurança da Informação, enfatizando as obrigações das pessoas em relação à respectiva segurança;
- Garantir que todas as responsabilidades da Segurança da Informação sejam claramente definidas preservadas.

4. Aplicação da Política de Segurança da Informação

Todas as normas aqui estabelecidas devem ser aplicadas por toda a rede e seguidas por todos os funcionários, prestadores de serviços, estagiários e afins para a proteção da informação e para o uso de recursos tecnológicos.

Esta PSI compromete e responsabiliza cada usuário a manter-se atualizado sobre este documento e as normas relacionadas, buscando orientação do gestor ou da Gerência de Tecnologia da Informação (GTI) sempre que não estiver absolutamente seguro quanto à aquisição e/ou ao descarte de informações.

A área de Segurança da Informação é composta pelas subáreas de Segurança operacional (SecOps) e SoC.

Esta PSI também deve ser aplicada e respeitada, no que for oportuno, pelos alunos e professores. Para esses grupos, recomenda-se o uso da Política de Segurança da Informação do Ambiente Educacional.

5. Princípios da Política de Segurança da Informação

Os equipamentos de informática, de comunicação, os sistemas e as informações devem ser utilizados para a realização de atividades profissionais, com senso de responsabilidade e preceitos éticos comuns à sociedade e dentro da legalidade.

Os alunos também devem usá-los para estudos, atividades educacionais e pesquisas acadêmicas.

Respeitar a privacidade dos usuários, agindo de forma ética e atendendo aos princípios da Lei Geral de Proteção de Dados Pessoais.

O Senac reserva-se o direito de monitorar e registrar todo e qualquer uso das informações geradas, armazenadas ou veiculadas na instituição. Para tanto, são criados e implantados controles apropriados, trilhas de auditoria ou registros de atividades em todos os pontos e sistemas que o Senac julgar necessário para reduzir os riscos, pautando-se na ética e na legalidade de forma a detalhar as ações na Norma de Monitoramento de Ativos.

6. Requisitos da Política de Segurança da Informação

A PSI deve ser comunicada a todos os funcionários, prestadores de serviços, estagiários e afins visando à efetividade e à real cultura de uso ético e legal dos recursos tecnológicos, bem como a Segurança da Informação do Senac.

Sempre que uma parceria ou contratação de empresa terceirizada envolver acesso a informações e/ou recursos tecnológicos do Senac, a gerência contratante deverá informar à GTI.

A PSI e as Normas serão revisadas e atualizadas com periodicidade mínima de um ano ou sempre que houver um fato novo e relevante, conforme análise e decisão do Comitê Consultivo.

Todos os contratos do Senac devem constar o anexo ou a cláusula de confidencialidade para garantir o acesso aos ativos de informação. Mais informações, consulte a Norma de Uso de Ativos.

Já o uso de sistemas do Senac só é permitido para usuários que formalizarem a ciência sobre a PSI. Entre os alunos, a formalização deve ser feita com base na Norma de Segurança da Informação Educacional.

A responsabilidade em relação à Segurança da Informação deve ser atribuída na fase de contratação, de forma a ser incluída nos contratos e monitorada durante a sua vigência.

Para funcionários, prestadores de serviços, estagiários e afins, contratados em período anterior à publicação desta política, e que não tenham assinado os respectivos documentos, deverá ser entregue um Termo de Ciência e Responsabilidade da PSI para a respectiva assinatura de forma física ou eletrônica.

Todos os funcionários, prestadores de serviços, estagiários e afins que tenham acesso a informações do Senac, devem passar por treinamento e conscientização sobre os procedimentos de segurança e o uso correto dos ativos oferecidos pela instituição. A finalidade é minimizar possíveis riscos de segurança, explicitar as responsabilidades e comunicar os procedimentos para a notificação de incidentes.

Todos os requisitos de Segurança da Informação e os aspectos legais, incluindo a necessidade de planos de contingência, devem ser identificados na fase de levantamento de um projeto ou sistema. Também devem ser justificados, acordados, documentados, implementados e testados durante a fase de execução.

Serão criados e implementados também controles apropriados e trilhas de auditoria ou registros de atividades em todos os pontos e sistemas que o Senac julgar necessário para reduzir os riscos dos ativos de informação.

Os ambientes de produção e de desenvolvimento tecnológico devem ser segregados e rigidamente controlados.

Um plano de contingência e continuidade tecnológico deverá ser implementado e testado anualmente integrado com plano de contingência e continuidade do negócio da instituição. O objetivo é reduzir riscos de perda de confidencialidade, integridade e disponibilidade dos ativos de informação, por meio da combinação de ações de prevenção e recuperação.

Os ativos críticos ou sensíveis devem ser mantidos em áreas seguras, protegidas por um perímetro de segurança definido, com barreiras de segurança apropriadas aos riscos identificados, além de ter o acesso controlado, registrado e monitorado. Para mais informações sobre ativos, consulte a Norma de Uso de Ativos.

Todo ativo de informação deve ser protegido de divulgação, modificação, furto ou roubo por meio da aplicação de controles.

Devem ser estabelecidas e comunicadas normas e responsabilidades pela propriedade e custódia dos ativos de informação. Bem como ser estabelecidos procedimentos e responsabilidades específicas para o uso e o gerenciamento dos ativos de informação oferecidos pelo Senac, quando estiverem fora das instalações da instituição.

Todas as pessoas devem ser distintamente identificadas. Sejam visitantes, alunos, estagiários, parceiros, funcionários ou prestadores de serviços. Os dados coletados e armazenados devem ser

segmentados a fim de que sejam aplicados controles especiais e sejam adequados às legislações pertinentes sobre a proteção de dados pessoais. Devem, ainda, ser estabelecidas regras para a coleta, o armazenamento e o tratamento de dados pessoais por meio de norma específica.

O uso de dispositivos móveis, assim como comunicadores instantâneos devem ser devidamente regrados em normativos próprios, atendendo sempre aos princípios da privacidade, respeito ao usuário e à necessidade da coleta de autorização, quando aplicável, devendo ser informado na Política de Privacidade, informações sobre as condições de tratamento.

Quando razões tecnológicas ou determinações superiores tornarem impossível a aplicação desta norma, ou ainda o uso apropriado de controles mínimos adequados à garantia da segurança dos ativos de informação, o responsável e/ou solicitante deverá documentá-las imediatamente à GTI. Dessa forma será possível adotar medidas alternativas para minimizar riscos, bem como organizar um plano de ação para corrigi-los, monitorá-los ou eliminá-los.

O Senac exonera-se de toda e qualquer responsabilidade decorrente do uso indevido, negligente e/ou imprudente dos recursos e serviços concedidos aos usuários. Reservando-se o direito de tomar as medidas administrativas e judiciais cabíveis contra os infratores, bem como analisar dados e evidências para a obtenção de provas a serem usadas em processos investigatórios e judiciais.

Esta atualização da PSI será implementada no Senac por meio de procedimentos específicos e obrigatórios a todos os funcionários, prestadores de serviços, estagiários e afins, independentemente do nível hierárquico ou função na instituição.

Todo incidente que afete a Segurança da Informação deverá ser comunicado inicialmente à GTI, que, se julgar necessário, deverá encaminhar posteriormente ao Comitê de Segurança da Informação para análise. Toda e qualquer atividade que não estejam tratadas nesta política ou normativos específicos, devem ser realizados apenas após consulta e autorização do gestor da área.

O não cumprimento dos requisitos previstos nesta PSI e nas Normas de Segurança da Informação acarretará violação às regras internas da instituição, e o usuário estará sujeito a medidas administrativas e legais cabíveis.

7. Monitoramento e Auditoria

Para garantir as regras mencionadas nesta PSI, bem como para fins de segurança e prevenção à fraude, o Senac reserva-se o direito de:

- Implantar sistemas de monitoramento de acesso às estações de trabalho, servidores internos e externos, correio eletrônico, navegação, internet, dispositivos móveis ou wireless, entre outros componentes da rede. A informação gerada por esses sistemas de monitoramento poderá ser usada para identificar usuários e respectivos acessos efetuados;

- Inspecionar qualquer arquivo que esteja em rede, no disco local da estação ou em qualquer outro ambiente para assegurar o rígido cumprimento desta PSI;

- Instalar sistemas de proteção e detecção de invasão para garantir a segurança das informações e dos perímetros de acesso;

- Instalar câmeras em suas dependências.

Os funcionários, prestadores de serviços, estagiários e afins tomam ciência de que ambientes, recursos tecnológicos, telefones, sistemas, computadores, dispositivos móveis e redes da instituição estão sujeitos a monitoramento e a gravação, atendendo à conformidade legal.

As regras de monitoramento no ambiente educacional poderão ser consultadas na Política de Segurança da Informação Educacional. Outros detalhes sobre monitoramento no ambiente administrativo podem ser obtidos na Norma de Monitoramento.

O uso de dispositivos móveis pessoais, deverá ser objeto de norma própria, no entanto, o colaborador ou prestador de serviços tomam ciência, neste ato, de que ao aceitar ou optar pelo uso de dispositivos pessoais para fins corporativos, o SENAC SP poderá auditar e inspecionar os recursos de TIC que estiverem em suas dependências ou que interajam com seus ambientes lógicos, sempre que considerar necessário, atentando-se à não discriminação e à proporcionalidade devida, respeitando a razoabilidade e privacidade.

8. Responsabilidades Específicas

8.1. Dos Usuários em geral

Funcionários, prestadores de serviços, estagiários e afins do Senac, em qualquer nível hierárquico, na sua esfera de competência, serão responsáveis por cumprir e zelar pela materialização e realização eficaz das normas e princípios da segurança da informação. Em atenção especial ao compromisso com os critérios legais e éticos que envolvam a instituição.

É de inteira responsabilidade do usuário qualquer prejuízo ou dano sofrido ou causado ao Senac e/ou a terceiros, em decorrência da não obediência às diretrizes e às normas aqui referidas.

Cabe a todos os usuários as seguintes práticas:

- Cumprir fielmente políticas, normas e procedimentos de Segurança da Informação, incluindo regras estabelecidas neste documento;

- Buscar orientação do superior quando houver dúvidas relacionadas à Segurança da Informação;

- Assinar o Termo de Responsabilidade, formalizando a ciência da PSI e das Normas de Segurança da Informação, bem como assumindo a responsabilidade pelo seu

cumprimento;

- Proteger as informações contra o acesso, a modificação, a divulgação ou a destruição não autorizada pelo Senac;

- Assegurar que os recursos tecnológicos sejam utilizados apenas para fins profissionais aprovados e de interesse da instituição;

- Prezar pela segurança das informações confidenciais, incluindo todo e quaisquer dados pessoais a que tiverem acesso;

- Atender à Lei Geral de Proteção de Dados Pessoais, protegendo os dados a que tiver acesso ou que venha a manuseá-los, sempre em conformidade às regras do SENAC SP.

- Comunicar imediatamente à GTI sobre qualquer descumprimento ou violação da PSI e/ou de suas Normas e Procedimentos; à GEP, quando se tratar de infrações administrativas causadas por funcionários, prestadores de serviços, estagiários e afins; além de outras áreas, quando for necessário.

8.2. Política de Senhas

Os colaboradores, terceiros e passantes assumem inteiramente a responsabilidade pela usuário (credencial) fornecido para acesso a rede, aplicações intenas, externas (Cloud / SaaS), aplicativos móveis, internet e sistemas de forma individual e intrasferível.

O Senac SP sempre adotará quando disponível pelo lado das aplicações, plataformas a validação de dois fatores (2FA/MFA) via aplicativo, e-mail ou sms. A verificação em duas etapas ajuda o uso das contas com mais segurança porque as senhas podem ser esquecidas, roubadas ou comprometidas. A verificação em duas etapas usa uma segunda etapa como seu telefone para dificultar a entrada de outras pessoas em sua conta. Recomendamos o uso do aplicativo gratuito Microsoft Authenticator.

O uso de senha segura é obrigatório para os sistemas, serviços, dispositivos e devem ser configurados conforme o padrão definido pelo Senac SP. Sendo obrigatória a alteração da senha conforme periodicidade e recomendações de segurança determinada pelo Senac SP.

- Para se obter uma senha de acesso forte, que ofereça mais segurança aos alunos e colaboradores, deve-se considerar as seguintes condições:Tamanho mínimo de 12 caracteres;Conter pelo menos uma letra maiúscula e uma minúscula;Conter números;
- Conter símbolos, incluindo:!@#$%^&*-_+=[]{}|\',.?/` ~"<>();
    - Exemplo: Um novo dia de Sol = Umn0v0d14d35@L

- Não repetir senhas anteriores (últimas 3 senhas).
- Mandatório alterar a senha a cada 90 dias.
- Evitar a utilização de:
    - Nomes, sobrenomes, dados de família, números de documentos, telefone, placas de carros, palavras de uso comum, bordões, nomes de times, filmes, series, músicas, produtos, sequência númericas, de teclado (ex.: 09876543 / poiuy876) ou datas comemorativas;

Caso o usuário erre a senha após cinco tentativas, ocorrerá o bloqueio de sua credencial. A conta permanecerá bloqueada por 30 minutos, após esse periodo a conta é automaticamente desbloqueada. Caso o bloqueio persista, será necessário solicitar a abertura de chamado, da mesma forma, para casos de dúvidas ou outras questões.

Caso o usuário erre a senha após cinco tentativas, ocorrerá o bloqueio de sua credencial. Neste caso será necessário solicitar a abertura de chamado, da mesma forma, para casos de dúvidas ou outras questões.

Todo acesso deve ser identificado de forma individual, seja ele interno ou externo, sendo proibido o compartilhamento de credencial e uso de usuários genéricos.

Camadas de segurança como regras de geolocalização, comportamento do usuário serão aplicadas para aumentar e garantir a segurança do ambiente.

Para os sistemas e serviços municipais, estaudais e do governo federal, onde é disponibilizado uma única credencial, o coordenador ou líder responsável da aréa será o responsável pelo gerenciamento da credencial.

Por razões de segurança, compliance e conformidade todos os usuário que utilizem dispositivos fornecidos e devidamente ingressados ao dominio do Senac, deverão fazer parte de grupos de usuários comuns, estando vetado o ingresso de usuários comuns ao grupo de administradores locais dos dispositivos.

É proibido a retirada dos equipamentos do Senac SP dos pontos de rede para conexão de dispositivos pessoais ou de terceiros.

As senhas, chaves de API (Keys), tokens não devem ser introduzidas, trafegadas pela rede, e-mail, aplicativos de mensagem instantaneo, anotadas e ou armazenadas em banco de dados, códigos fontes, linhas de comando, scripts, aplicações, sistemas web, APP ou API em texto simples, sendo necessário a utilização de criptografia forte e sempre aplicando o conceito de menor previlegio.

Recomendamos o uso de aplicativos específico para armanezamento de senhas que utilize criptografia forte e duplo fator de autenticação, sendo de responsabilidade do usuário buscar um recurso seguro e de boa reputação no mercado.

Para os usuários de sistemas, dominios e servidores com previlegios de administratores (domain

admins, administrators, root, sysadmin, sa, etc), deverão utilizar a solução de cofre de senhas ofertada pelo Senac SP, quando possível renomeadas ou desabilitadas.

Fica vetado o acesso ao ambiente de servidores por terceiros sem o devido acompanhamento da GTI ou gerência solicitante.

Para garantir um perimetro de segurança os acessos privilegiados, devem ser realizados por uma quantidade mínima de usuários, via cofre de senhas.

As utilizadas para serviços deverão ser renomeadas e classificadas como "contas de serviço", não sendo utilizadas para qualquer tipo de acesso, o coordenador ou líder responsável da aréa será o responsável pelo gerenciamento da credencial.

Para os casos extraordinários onde o gerente ou coordenador responsável da aréa assuma totalmente o risco, deverá ocorrer mediante assinatura do documento de Análise e Avaliação de Risco (AAR) e validação do Núcleo de Segurança e Privacidade (DPO) e setores juridicos do Senac SP.

8.3 Redes sem fio

O Senac SP disponibiliza rede sem fio (wireless) para o uso de dispositivos móveis nas suas dependências que trazem regras, monitoramento, configurações especificas e acessos conforme a necessidade e com intuito de garantir a privacidade dos nossos usuários e em atendimento e respeito à Lei Geral de proteção de Dados Pessoais. É de inteira responsabilidade do proprietário do equipamento ou dispositivo, tanto por sua guarda quanto pelos conteúdos nele instalados, sejam softwares, músicas, fotos, entre outros.

- **SSID WIFIZONE:** Esta rede permite aos colaboradores do SENAC que desejam acessar a rede sem fio (wireless) por meio de estações de trabalho, notebooks, smartphones ou dispositivos similares fornecidos ou pertencentes ao patrimônio do SENAC de São Paulo, devidamente ingressadas no domínio administrativo. Ela possinilita o acesso a rede corporativa e à utilização de todos os recursos do domínio SENAC.CORP, sistemas corporativos, Intranet e Internet.
- **SSID EDUCACIONAL:** Esta rede permite a mobilidade das unidades na montagem dos laboratórios móveis, possibilitando o acesso a rede educacional do SENAC utilizando por intermedio da rede sem fio (wireless). Garantindo o acesso e à utilização de todos os recursos do domínio EDUCACIONAL e Internet. Destinada atender os laboratórios móveis por meio dos notebooks pertencentes ao domínio e com patrimônio do SENAC de São Paulo.
- **SSID CONECTA SENAC:** Esta rede permite acesso gratuito à Internet. Seu modo de operação e independente e não permite acesso a rede Administrativa ou Educacional. Destinada atender todos os usuários da rede SENAC, sendo eles alunos, professores, palestrantes, visitantes, serviços terceirizado. Como se trata de um acesso totalmente gratuito é obrigatório apenas o cadastro no portal do Senac São Paulo.

- **SSID TERCEIROS:** Esta rede permite aos consultores de tecnologia do SENAC que precisam acessar a rede administrativa e aso ambientes internos do Senac São Paulo por meio de notebooks, não fornecidos ou pertencentes ao patrimônio do SENAC de São Paulo. Ela possinilita o acesso a rede corporativa e à utilização de recursos do domínio SENAC.CORP, sistemas corporativos, Intranet e Internet.

Como os SSIDs WIFIZONE, EDUCACIONAL, TERCEIROS recebem as mesmas regras de segurança e monitoramento é proibido o uso de dipositivos móveis pessoais (notebooks, smartphones, etc.), para o acesso simples à Internet, para essa finalidade e disponibilizado a rede sem fio Conecta Senac.

8.4 Segmentação de ambiente, Publicações internas e externas

Toda aplicação publicada com origem do Datacenter do Senac São Paulo deverá ser devidamente validada pelas area de segurança da informação, segurança operacional e com a arquiterura e ambiente aprovado pela Coordenação de Middleware.

Os equipamentos, servidores, appliances físicos ou virtuais que forem adicionados no DataCenter do Senac SP, precisam ser:

- Classificados e adicionados ao seu segmento de rede (Produção, Homologação ou Desenvolvimento);
- Devidamente adicionados as regras de acesso e ao cofre de senhas;
- Com todos agentes de segurança instalados;
- Sistema devidamente atualizado, se póssivel na sua ultima versão e com todos os patches aplicados;

Somente após essas etapas os equipamentos, servidores, appliances físicos ou virtuais poderão ser liberados no ambiente.

Todo acesso ao DataCenter precisam de acompanhamento pela equipe da Missão Critica e devem conter no máximo 5 pessoas por vez.As aplicações, apis, aplicativos deverão ser classificadas como de uso interno ou externo para adequação correta ao ambiente de publicação, considenrando aplicações:

Internas: Aplicações que disponibilizam informações direcionadas aos colaboradores de Senac SP (Ex.: Intranet, Net-Drive, CRM, Etc.).

- É exclusivamente acessada por dentro da rede interna do Senac SP;
- O acesso externo ocorre via VPN.
- Podendo ser dos ambiente de produção, homologação e desenvolvimento.

Externas: São aplicações que disponibilizam informações direcionadas para público externos (Ex.: Portal Senac, EAD, BlackBoard, etc.) e internos.

- É acessada diretamente pela Internet, não necessitando da VPN.
- Somente aplicações do ambiente de publicação (DMZ) podem ser expostas externamente.

Requesito de segurança para as aplicações:

a) Para ambiente de integração ou validação com o AD (Active Directory Azure) recomendamos que seja feito via a API (Tokem aplicação) para permitir o uso do mesmo usuário e senha utilizados na rede local com uso do MFA nativamente com aplicação (Microsoft App Authenticator);

b) Toda a transmissão de dados em rede ou via aplicação deve ser feita de forma autenticada e criptografada entre as integrações, (API), sessões clientes e a infraestrutura servidora.

c) A troca de informações para autenticação deverá ser realizada de acordo com os padrões:

   a. SSO (Single Sign-On Middleware)

   b. SAMLv2 (Security Assertion Markup Language).

   c. OIDC/OAuth2

d) Para as soluções em nuvem recursos contra robôs (reCaptcha v3 ou superior), 2FA/MFA, confirmação de usuário após o primeiro cadastro via e-mail e demais camadas devem ser nativas da solução;

e) Para as aplicações que terão integração com ambiente do Senac (Ex: AD) precisa apresentar de forma nativa bloqueio de acesso após um número X de tentativas erradas, bloqueio contra brute-force por IP, tendo ainda painel de gerenciamento e liberação independente do Senac.

f) Para fins de exercício regular de direitos, atendimento de obrigação legal (Marco Cívil da Internet - Lei nº 12.965/2014) e legítimo Interesse, é necessário que as aplicações contenham registros de LOGS de criação de usuário, acesso a aplicação contendo as informações de identificação, registro de usuário, perfil, horário, ação e endereço IP (Público/Interno).

g) **Análise de Vulnerabilidade:** A análise de vulnerabilidade poderá ser realizada de forma automatizada para identificar vulnerabilidades conhecidas, falhas conhecidas, portas abertas, configurações inadequadas, falta de patches de segurança nas camadas de sistemas e aplicações, sendo tratada internamente em norma especifica.

h) **Pentest (Teste de Penetração):** O pentest será realizado de forma direcional, envolvendo a simulação controlada de ataques pela equipe de segurança da informação do Senac SP e em alguns casos por empresas terceirizadas, com o objetivo de identificar e explorar vulnerabilidades reais a serem identificadas no sistema. Deverão ser utilizadas técnicas avançadas, como por exemplo, mas não se limitando a engenharia social, tentativas de invasão ativas e exploração de vulnerabilidades específicas encontradas durante a análise (código ou serviço), para avaliar o impacto potencial dessas vulnerabilidades e fornecer recomendações

específicas para mitigá-las.

Com base nos testes de segurança executados, as soluções de software oferecidas deverão trazer nativamente camadas de proteção contra-ataques:

a. OWASP Top 10 (Vigente);

b. OWASP API Security Top 10 (Vigente);

c. OWASP AI Security and Privacy (Vigente).

d. Server Side (SQL injection / Authentification / Director traversal / Command injection / Business logic vulnerabilities / Information disclosure / Access control / File upload vulnerabilities / Server-side request forgery (SSRF) / XXE injection)

e. Client Side (Cross-site scripting (XSS) / Cross-site request forgery (GSRF) / Cross-origin resource sh

Para os itens "G" e "H" os resultados serão direcionados para a coordenação responsável e tratado pelo processo gerenciamento de vulnerabilidade da area de segurança da informação, podendo ser associado ao processo de gerenciamento de risco tecnologico mediante assinatura do documento de Análise e Avaliação de Risco (AAR) e validação do Núcleo de Segurança e Privacidade (DPO) e setores juridicos do Senac SP.

8.5 Dos Gestores/Gerentes

Cabe a todo gestor de área:

- Garantir a implementação de mecanismos necessários para o descarte seguro das informações;
- Manter postura em relação à Segurança da Informação e servir de modelo de conduta para os funcionários, prestadores de serviços, estagiários e afins sob a sua gestão;
- Cumprir esta política, as normas e os procedimentos de Segurança da Informação;
- Garantir acesso e conhecimento a esta política, bem como as normas e os procedimentos aqui estabelecidos;
- Inserir em contratos com prestadores de serviços, clientes, terceirizados e parceiros, quando estes necessitarem ter contato com informações do Senac São Paulo, cláusula de responsabilidade, de Proteção de Dados Pessoais, de ciência da PSI e de confidencialidade, exigindo o repasse das obrigações a seus próprios empregados e colaboradores.

- Solicitar previamente a permissão de acesso à GTI elencando os ativos de informação que serão oferecidos a terceiros;
- Adaptar as normas, processos, procedimentos e sistemas sob sua responsabilidade para atender à PSI;
- Observar e zelar pela aplicação das regras e legislação de Proteção de Dados Pessoais;
- Comunicar imediatamente à GTI toda e qualquer violação de Segurança da Informação, incluindo violação de dados pessoais, que deverá informar à GEP a ocorrência de infrações provenientes de funcionários, bem como informar as demais áreas quando houver necessidades específicas.

8.6 Dos Proprietários de Ativos de Informação

O proprietário da informação pode ser um gerente, coordenador e equipes de liderança de uma determinada área ou projeto, e será o responsável pela manutenção, revisão e cancelamento de autorização à determinada informação ou conjunto de informações pertencentes ao Senac ou sob a sua guarda.

Cabe ao proprietário da informação:

- Elaborar, para toda informação sob a sua responsabilidade, matriz que relaciona cargos e funções do Senac às autorizações de acesso concedidas;
- Manter registro e controle atualizados de todas as autorizações de acessos concedidas determinando, sempre que necessário, a pronta suspensão do acesso ou a alteração da autorização concedida;
- Reavaliar as autorizações de acesso, sempre que necessário ou solicitado, cancelando aquelas que não se fizerem mais necessárias;
- Observar e zelar pela aplicação das regras e legislação de Proteção de Dados Pessoais;
- Participar, sempre que convocado, das reuniões do Comitê de Segurança da Informação prestando esclarecimentos quando solicitado.
- Todos os notebooks e dipositivos móveis que suportem o armazenamento de dados utilizados em transito deverão receber criptografia de disco.

8.7 Descarte seguro para ativos de informação

Todos os ativos de informação do Senac SP que suportem o armazenamento de dados precisam ser verificados antes da entrega para leilão, remanejamento ou reutilização, com intuito de assegurar que todos os dados pessoais, informações sigilosas, softwares tenham sobregravados com segurança por meio de técnicas e softwares que tornem as informações originais irrecuperáveis (sanitização) em vez de usarem apenas as funções padrão de formatação.

Para os dispositivos, equipamentos e midias que tenham a necessidade de remoção externa para manutenção pelas empresas prestadora de serviço ou garantia, pode ser necessário realizar uma análise/avaliação de riscos para determinar se convém a liberação para conserto ou se será necessário realizar a sanitização do disco antes do envio.No caso de fita, drivers, mídias ou dispositivos de armazenamento que serão encaminhados para descarte (defeituosos ou não) que contenham informações sigilosas do Senac SP, devem ser destruídas fisicamente antes de serem descartadas.

8.8 Da Gerência de Tecnologia da Informação

A Gerência de Tecnologia da Informação (GTI) será responsável pela gestão do uso de tecnologias necessárias ao bom andamento dos negócios do Senac e de ações preventivas. Também oficializou uma equipe de Segurança da Informação para o planejamento e execução de ações preventivas para o tratamento de incidentes, a fim de garantir um nível maior de segurança.

Cabe à GTI:

- Apresentar as atualizações da PSI e das Normas de Segurança da Informação ao Comitê de Segurança da Informação para aprovação e posterior publicação;
- Propor as metodologias e processos específicos para a Segurança da Informação, como a avaliação de risco;
- Propor e apoiar iniciativas que visem à segurança dos ativos de informação do Senac;
- Promover com a GEP, a GMS e a GCR a conscientização dos funcionários, prestadores de serviços, estagiários e afins quanto à relevância da Segurança da Informação para as atividades do Senac por meio de campanhas, palestras, treinamentos, entre outros meios;
- Apoiar a avaliação e a adequação dos controles específicos da Segurança da Informação para novos sistemas ou serviços;
- Desenvolver normas e regras específicas conforme à Lei de Proteção de Dados Pessoais;

- Promover adequação dos recursos técnicos e de infraestrutura necessários para atender à Lei de Proteção de Dados Pessoais;
- Indicar o encarregado pela Proteção de Dados Pessoais;
- Analisar criticamente incidentes com o Comitê Consultivo;
- Manter a comunicação efetiva com o Comitê Consultivo para mantê-lo informado sobre assuntos relacionados ao tema e que afetem ou tenham potencial para afetar o Senac;
- Outras responsabilidades a serem formalizadas em norma específica.

8.9 Do Comitê Consultivo

O Comitê Consultivo deve ter um perfil multidisciplinar e contar com a participação de gestores de diferentes áreas do Senac.

Deve ser formado por um representante das principais instâncias da instituição. Entre elas a própria GTI, a GPG, a AJ, a GEP, as GDs, além do CAS. Pode, ainda, utilizar especialistas internos ou externos para apoiarem nos assuntos que exijam conhecimento técnico específico.

O Comitê Consultivo deve reunir-se formalmente, no mínimo, uma vez a cada seis meses. Reuniões adicionais devem ser realizadas sempre que for necessário deliberar algum incidente grave ou definição relevante para o Senac.

São atribuições do Comitê Consultivo:

- Propor investimentos relacionados à Segurança da Informação com o objetivo de maximizar a redução de riscos;
- Propor alterações nas versões da PSI e a inclusão, eliminação ou alteração de normas complementares;
- Discutir e propor iniciativas para aprimorar, melhorar e dar continuidade à segurança das informações;
- Avaliar os incidentes de segurança e propor ações corretivas;Discutir e propor medidas cabíveis no processo disciplinar para os casos de descumprimento da PSI e/ou das Normas de Segurança da Informação complementares.
- Deliberar sobre questões relacionadas à Proteção de Dados Pessoais.

As atas e os resumos das reuniões do Comitê Consultivo ficarão sob a responsabilidade da GTI.

8.10 Da Assessoria Jurídica

O Senac, quando solicitado pela GTI, contará com apoio jurídico da AJ para análise, parecer e estudo de casos.

Para questões voltadas à tecnologia, como a Segurança da Informação, contratos de tecnologia, Proteção de Dados Pessoais, entre outros assuntos, o Senac terá o apoio de um escritório terceirizado especializado em direito digital, que terá as seguintes funções:

- Dar apoio, respaldo e embasamento legal para ações voltadas à Segurança da Informação, à exposição na mídia, ao uso dos recursos tecnológicos e à proteção de dados pessoais;
- Acompanhar incidentes;
- Orientar a melhor forma de coletar e preservar uma prova eletrônica, com o propósito de manter sua eficácia para o uso em juízo, quando necessário;
- Elaborar e revisar documentos jurídicos relacionados a contratos de tecnologia e Segurança da Informação;
- Acompanhar o processo disciplinar, validando as sanções e exceções, quando houver;
- Revisar periodicamente e sugerir adaptações a esta Política e a normas de Segurança da Informação, de acordo com as necessidades e o perfil de incidentes causados ao longo do tempo;
- Analisar e adequar toda e qualquer regulamentação interna a fim de que esteja alinhada à Constituição Federal, ao Código Civil, ao Marco Civil da Internet e à Lei Anticorrupção e à Lei de Geral de Proteção de Dados Pessoais, bem como qualquer legislação futura ou pertinente que não tenha sido mencionada;
- Analisar e promover o compliance a projetos de leis, quando aprovado, e que impactem no negócio do Senac e no uso dos recursos tecnológicos e da legislação pertinente a sua área de atuação;
- Atender e propor demandas judiciais.

8.11 Da Gerência de Pessoal

Cabe à Gerência de Pessoal (GEP):

- Atribuir, na fase de contratação dos funcionários, prestadores de serviços, estagiários e afins, e formalizar nos contratos individuais de trabalho, a responsabilidade quanto ao cumprimento da PSI e sua responsabilidade para com a Proteção de Dados Pessoais;'
- Colher e arquivar a assinatura do Termo de Responsabilidade e ciência da Política e Normas de Segurança da Informação dos profissionais já contratados;
- Comunicar formalmente e imediatamente à GTI toda e qualquer alteração no quadro funcional da instituição, contratações, demissões, alterações de cargos, funções, entre outros, no prazo mínimo de 24 horas, e de imediato em casos específicos, a fim de evitar acessos não autorizados e/ou desnecessários;
- Receber da GTI informações sobre violações da Política e Normas e promover as tratativas e a instauração de processo disciplinar, quando cabível;
- Apoiar e promover com a GTI ações de conscientização e de capacitação em Segurança da Informação e Proteção de Dados Pessoais para todos os profissionais do Senac;
- Zelar e promover a devida proteção de dados pessoais, em conformidade com as normas internas e legislação pertinentes.

9. Da Inovação e Uso de Novas Tecnologias

O Senac SP incentiva a inovação e desenvolvimento de novas tecnologias, para fins educacionais. No entanto, toda tecnologia a ser utilizada em nome da instituição ou como ferramenta de apoio na prestação de serviços, como sites, aplicativos, IoT, robótica, ambientes virtuais como o metaverso e Plataformas em Nuvem (SaaS) e o uso de Inteligência Artificial, deve ser homologada pela Gerência de Tecnologia da Informação, Gerência de Desenvolvimento ou pela Gerência de Tecnologias Aplicadas à Educação.

As tecnologias para atividade-meio são homologadas pela GTI. As tecnologias de uso transversal, para o processo de ensino e aprendizagem, são homologadas pela GTAE. As tecnologias de uso específico das áreas de conhecimento, para o processo de ensino e aprendizagem, são homologadas pelas respectivas GDs. Todos os processos de homologação são alinhados a parâmetros definidos pela GTI.

Isso inclui análise prévia com base em riscos relacionados à Segurança da Informação e Proteção de Dados Pessoais, além dos riscos envolvidos na gestão do próprio negócio. Tais tecnologias quando aprovadas e homologadas passam a ser entendidas como uso institucional, devendo ser criado normas internas para sua utilização. A criação de perfis pessoais ou qualquer interação entre alunos e professores que não sejam por ferramentas ou assinaturas institucionais são de responsabilidade do próprio usuário, não possuindo, o SENAC SP, qualquer gestão ou responsabilidade por referidas ações ou qualquer ocorrência em tais ambientes.

Tecnologias inovadoras quando ainda em fase experimental e a utilização de equipamentos e ferramentas digitais, como sites, aplicativos, IoT, Robótica, ambientes virtuais como o metaverso e Plataformas em Nuvem (SaaS) e o uso de Inteligência Artificial, podem ser utilizadas apenas para fins educacionais, enquanto objeto de discussão e aprendizado e não como ferramenta institucional, não sendo permitido criação de contas pessoais para utilização em nome do SENAC SP ou inserção de dados corporativos, bem como não será permitido a criação de contas corporativa/ institucional sem que haja autorização do gestor e homologação pela Gerência de Tecnologia da Informação, Gerência de Desenvolvimento ou pela Gerência de Tecnologias Aplicadas à Educação.

10. Da Proteção de Dados Pessoais

O Senac SP em atendimento e respeito à Lei Geral de Proteção de Dados Pessoais deverá garantir a disponibilidade, integridade e confidencialidade dos dados pessoais, em todo seu ciclo de vida, sendo esta categoria de dados tratados de forma permanente como dados confidenciais.

Todo tratamento de dados pessoais deverá estar atrelado a uma finalidade específica, informada ao titular e devidamente atrelada a uma ou mais bases legais previstas nos artigos 7º e 11º da Lei Geral de Proteção de Dados Pessoais, atentando-se aos princípios da necessidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação e prestação de contas.

O detalhamento dos requisitos e regras para tratamento de dados pessoais serão disponibilizados em norma específica, sendo necessário que todos os colaboradores e prestadores de serviços tomem ciência e sejam sensibilizados sobre o tema e a respectiva norma.

Toda e qualquer alteração ou criação de sistemas, serviços ou produtos que envolvam tratamento de dados pessoais deverão aplicar o "Privacy by Design / Privacidade desde a concepção".

Além dos princípios mencionados o Senac SP deverá elaborar um plano de resposta à violação de dados pessoais, elaborar o Relatório de Impacto sempre que necessário, utilizar processo de anonimização e pseudonimização sempre que necessário, fazer registro das operações de tratamento de dados pessoais, utilizar protocolos de criptografia na transmissão e armazenamento de dados pessoais, bem como implementar um sistema de gestão de dados pessoais.

11. Das Disposições Finais

As infrações a esta PSI e às Normas de Segurança da Informação serão passíveis de processo disciplinar, podendo resultar de mera advertência até demissão por justa causa.

A qualquer tempo, e em qualquer um dos casos previstos, prevalecendo o descumprimento das regras expostas, a GTI poderá bloquear temporariamente o acesso do usuário e comunicar os motivos ao profissional e ao gestor da área.

Não é permitido, dar suporte ou utilizar software, dispositivos, scripts, robôs ou quaisquer outros meios ou processos (incluindo crawlers, plugins e add-ons para navegadores ou quaisquer outras tecnologias) para fazer varredura no website ou copiar materiais e/ou quaisquer dados nele constantes. É vedado, a realização de testes de vulnerabilidades dos mecanismos de segurança do website, app, aplicações ou da infraestrutura de tecnologia da informação utilizada em relação aos websites, assim como conduzir quaisquer pentestes no ambiente do Senac SP. O Senac não possui nenhum programa de Bug Bounty, estando expressamente vedada a realização de atividades com tais fins.

O uso de qualquer recurso do Senac para atividades ilegais é motivo de demissão por justa causa e a instituição vai cooperar ativamente com as autoridades.

A PSI do Senac será complementada por Normas de Segurança da Informação que tratem assuntos relacionados ao uso de correio eletrônico, rede corporativa, internet, Proteção de Dados Pessoais, entre outros. E serão consideradas partes integrantes desta PSI.

Esta PSI e as Normas de Segurança da Informação estarão disponíveis em documentos internos, em local de fácil localização e acesso restrito. Já a Norma Educacional deve ficar disponível ao público.

Normas específicas relacionadas a questões técnicas e confidenciais, e que requeiram acesso por equipes e pessoas específicas, devem ser colocadas à disposição apenas a pessoas autorizadas.

Assim como a ética, a segurança deve ser entendida como parte fundamental da cultura interna do Senac.

12. Documentos Relacionados

Documentos administrativos:

- Norma de Acesso Remoto;
- Norma de Acesso e Uso do Correio Eletrônico;
- Norma de Gestão de Usuários e Direitos de Acesso a Sistemas;
- Norma de Monitoramento de Ativos;
- Norma de Uso e Acesso à Internet e às Redes Sociais;
- Norma de Uso de Ativos;
- Norma de Uso de Dispositivos Móveis;
- Norma de Gestão de cópias de Segurança (Backup);
- Norma de Gestão do Datacenter;

Política de Mídias Sociais do Senac São Paulo;

Política de Privacidade do Senac São Paulo;

Política de Cookies do Senac São Paulo;

Política de Segurança da Informação Educacional;

Código de Conduta do Senac São Paulo;