Política de Segurança da Informação

Documento de Normas Educacionais

SisNormas Senac São Paulo

V. 6.0

Histórico de revisões

Versão	Data	Alteração
Versão 1.0	06/12/2010	Lançamento da Primeira versão
Versão 2.0/3.0	---	Arquivadas
Versão 4.0	21/02/2013	Adequação da política e termos tecnológicos.
Versão 5.0	29/06/2021	Adequação da política, termos tecnológicos, comunicadores instantâneos, suporte aos alunos via VPN e LGPD.
Versão 6.0	11/04/2024	Adequação da política, termos tecnológicos, políticas de senha, regras de 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)

O **SENAC SP** tem como negócio central a educação, pois seus serviços visam proporcionar o desenvolvimento de pessoas e organizações para contribuir com a formação da sociedade do conhecimento. Com o avanço das tecnologias, mudam o perfil da sociedade, que está cada vez mais conectada com uma realidade digital, e as formas de agir, gerir e produzir conhecimento e informação. Por isso, os atos e as responsabilidades devem acompanhar esse movimento.

Em um cenário moderno e ao mesmo tempo prezando pela qualidade de seus serviços educacionais, a instituição não poderia deixar de acompanhar tal evolução. Dessa forma, passa a interagir os recursos da tecnologia da informação em sua rotina educacional.

Com o aumento de recursos tecnológicos, crescem igualmente os riscos de incidentes que envolvem, em especial, o uso da rede. O Senac São Paulo desenvolveu esta política de segurança da informação para o ambiente educacional a fim de prevenir esses riscos e orientar os usuários de tais tecnologias.

O objetivo da instituição com esta política, que deve ser observada e seguida pelos usuários de toda a rede, é estimular o uso dos recursos tecnológicos aplicados ao processo de ensino e aprendizagem de forma consciente e sistematizada, preservando as questões legais, principalmente no que tange a proteção de dados pessoais.

2. Conceitos e Definições

Ambiente educacional: qualquer ambiente utilizado com finalidade pedagógica. Por exemplo: salas de aula convencionais, laboratórios, auditórios, bibliotecas, business center, entre outros.

Ambiente virtual de aprendizagem (Learning Management System – LMS): sistema de gerenciamento da aprendizagem que possibilita a comunicação e a interação entre alunos e docentes. Permite a disponibilização e o armazenamento de conteúdo, bem como a produção colaborativa e a integração de diversas mídias e recursos.

Ativo: bens da empresa que tem valor econômico, incluída a informação e todo o recurso utilizado para o seu tratamento, tráfego e armazenamento.

Ativo Crítico e Sensível: todo ativo considerado como essencial para a empresa, cujo acesso por pessoas não autorizadas ou a falta de acesso por quem é permitido seja necessário podem causar danos à organização.

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

Estação de trabalho: sistema informatizado integrado por um conjunto de recursos tecnológicos destinados a auxiliar os profissionais ou acadêmicos no exercício de suas funções.

Documentos educacionais: são todos os documentos relacionados aos Serviços educacionais da instituição. Por exemplo: Projeto Pedagógico, Programa de Curso, Plano de Curso, Plano de Orientação para Oferta, entre outros.

BlackBoard: Ambiente virtual de aprendizagem pelo Senac São Paulo, focado em dar apoio às atividades do Ensino Superior.

Blogs: originados como diários de bordo, hoje são empregados como diários pessoais em ambientes virtuais, frequentemente atualizados e direcionados para o uso do público em geral.

Aplicativos de vídeo chamada: Todo e qualquer aplicativo que permita interação em tempo real de vídeo e áudio.

Cavalo de Tróia: (*Trojan Horse*) é um programa malicioso que cria uma abertura para outros aos programas e invasões indesejadas.

Chats: programas que habilitam um canal de comunicação por meio de computadores ou dispositivos móveis em tempo real.

Código Executável: um arquivo cujo computador interpreta como um comando de execução para determinadas funções.

Código Malicioso: programas que possibilitam ações danosas, tais como vírus, *Worms*, *trojans*, *spywares*, scripts, robôs dentre outros.

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

Cyberbullying: prática negativa de assédio moral que afeta o psicológico de outra pessoa, através de recursos tecnológicos, como publicações na internet e envio de fotos e vídeos com mensagens ofensivas por celular ou quaisquer outros dispositivos móveis.

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 acesso à informação e aos ativos correspondentes sempre que necessário.

Dispositivos móveis: toda e qualquer ferramenta ou mídia que permita aos usuários a portabilidade de dados. Por exemplo: notebook, pendrive, CD, MP3, câmeras fotográficas, smarthphones, palmtops, IoT.

Fóruns: espaços virtuais de debate com caráter temático, nos quais a comunicação é constituída de mensagens propagadas por meio da rede.

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

Informação Sensível: é toda informação sigilosa que, se divulgada, pode resultar em uma perda de vantagem, inclusive, financeira, bem como impacto negativo para a marca.

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

Login: identificação de um usuário no computador, dispositivo móvel ou rede.

Login Portal Senac: identificação criada pelo aluno, colaborador, terceiro, etc... no portal do Senac, por intermédio do seu e-mail pessoal, para acesso ao portal do Senac e outros serviços correlacionados.

Login Educacional: Identificação fornecida pelo Senac para acesso aos computadores dos laboratórios e bibliotecas. O Login educacional também é utilizado para acessos aos serviços da Microsoft, como o Office 365 e as salas de aula virtuais no Teams. A senha é a mesma utilizada no acesso a área exclusiva do Portal Senac (para os alunos que possuem cadastro).

Email Educacional: endereço eletrônico fornecido pelo Senac, formado pelo login educacional + domínio educacional (loginaluno@senacsp.edu.br). O acesso é através do Outlook (correio eletrônico da Microsoft) disponível no pacote do Office 365. Este e-mail também deve ser utilizado para acesso ao ambiente remoto de sala de aula MS Teams.

Microsoft Teams: é uma plataforma unificada de comunicação e colaboração que combina bate-papo, videoconferências, armazenamento de arquivos e integração de aplicativos, utilizada pelo Senac como apoio às atividades educacionais de todas as modalidades (com exceção do Ensino Superior).

Recursos tecnológicos: ferramentas computacionais ou de comunicação eletrônica disponibilizadas, como e-mail, internet, computador, VPN, chat, ambientes colaborativos, blogs, fóruns, entre outros.

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

Servidor de proxy: servidor intermediário entre um usuário e outro servidor.

SPAM: *e-mails* não solicitados, normalmente enviados para um grande número de pessoas.

Storyboard: é um guia visual que traz as principais cenas de um produto audiovisual de forma rápida e objetiva.

Plishing: mensagens de e-mail que solicitam dados do usuário de forma direta ou através de redirecionamentos para sites ou números de telefone, a fim de roubar a identidade do usuário.

Peer-to-peer (P2P): arquitetura de rede em que cada computador tem funcionalidades e responsabilidades equivalentes. Esse tipo de rede é implementado por sistemas P2P, que permitem conectar o computador de um usuário ao de outro para compartilhar ou transferir dados.

Podcast: É um material entregue na forma de áudio, muito semelhante a um rádio, mas que fica disponível para que o consumidor escute quando quiser - não é um programa ao vivo.

Spywares: Programa espião ou software mal-intencionado, tipo de programa automático intruso destinado a infiltrar-se em um sistema de computadores e smartphones, para coletar informações pessoais ou confidenciais do usuário de forma ilícita, e encaminhar para uma entidade externa via Internet para fins maliciosos, ou análise de marketing e financeiros.

Streaming: tecnologia usada para transmissão, em tempo real, de dados de áudio e vídeo em uma rede.

Usuário: são todos os docentes, discentes, empregados e prestadores de serviços do Senac São Paulo que utilizam o ambiente educacional da instituição, acessando-o no local ou remotamente, com os recursos tecnológicos e/ou as informações.

Usuário aluno: são todos os usuários que estão formalmente matriculados em uma das modalidades de cursos oferecidos pelo Senac São Paulo.

Usuário colaborador: professores, coordenadores, professores carta convite, técnicos de desenvolvimento profissional, consultores ou pessoas, físicas ou jurídicas, que exerçam função ligada à educação por vínculo empregatício ou terceirizado.

Vírus: programa malicioso que se propaga infectando a máquina.

VPN: Rede privada virtual, do inglês Virtual Private Network, é uma rede de comunicações privada construída sobre uma rede de comunicações pública. O tráfego de dados dos laboratórios do Senac é levado aos dispositivos pessoais dos alunos para que consigam acessar softwares instalados nesses ambientes. Essa rede é exclusivamente direcionada para esta finalidade e não pode ser usada para outras ações, sob pena e responsabilidade do aluno e colaborador.

Vulnerabilidade: fragilidade de um ativo que pode ser explorada e gerar danos à organização.

Worm: é um programa independente que se replica com o objetivo de se espalhar para outros computadores. Geralmente, usa uma rede de computadores para se espalhar, ou mesmo unidades USB, contando com falhas de segurança no computador de destino para acessá-lo.

3. Objetivos da Política de Segurança da Informação

Esta política tem como objetivo:

Definir padrões e critérios a serem seguidos de uso e manuseio adequados dos recursos tecnológicos, bem como das informações pertencentes e/ou disponibilizadas pelo **SENAC SP**, segundo preceitos de ética, legalidade, segurança da informação e proteção de Dados Pessoais.

Garantir padrões básicos de segurança a fim de permitir o manuseio de dados, incluindo por meio de ferramentas tecnológicas de forma adequada sem que haja prejuízo aos fins educacionais ao qual se destina.

Prevenir possíveis causas de incidentes e responsabilidade legal da instituição e seus colaboradores internos, externos e parceiros.

Atender aos requisitos legais, regulamentares e contratuais pertinentes à sua atividade.

Garantir que todas as responsabilidades pela Segurança da Informação sejam claramente definidas e atribuídas a quem for devido.

Promover a cultura de Ética, Educação, Segurança da Informação e Proteção de Dados Pessoais.

4. Aplicação e Abrangência

A presente política abrange toda a rede do Senac São Paulo.

As regras e diretrizes aqui estabelecidas aplicam-se a todo manuseio de informação e utilização dos recursos tecnológicos disponibilizados no ambiente educacional, para todos os usuários, alunos e colaboradores em todos os níveis hierárquicos do Senac São Paulo, considerando as características dos serviços educacionais.

Esta Política compromete e responsabiliza cada usuário, estando todos cientes de sua responsabilidade em manter-se atualizado sobre este documento e normas relacionadas, buscando orientação da instituição em caso de dúvidas.

5. Regras de Uso Geral

Os equipamentos de informática e comunicação, sistemas e informações devem ser utilizados pelos usuários para a realização das atividades profissionais quando se tratar do colaborador e educacionais quando se tratar de alunos, com senso de responsabilidade, preceitos éticos comuns à sociedade e dentro da legalidade.

Os colaboradores e alunos, através desta Política, tomam ciência de que, para fins de segurança, exercício regular de direitos e prevenção à fraude, os ambientes, telefones, sistemas, computadores e redes da empresa estão sujeitos a monitoramento e gravação, atendendo à conformidade legal e de acordo com a Política de Privacidade e Proteção de Dados Pessoais.

O **SENAC SP** considerando a finalidade de manutenção da segurança, reserva-se ao direito, de monitorar e registrar todo o uso das informações geradas, armazenadas ou veiculadas pelos recursos da instituição. Para tanto, são criados e implantados controles apropriados e trilhas de auditoria ou registros de atividades em todos os pontos e sistemas que a instituição julgar necessário para reduzir os riscos.

Toda informação que é acessada, transmitida, recebida ou produzida com recursos tecnológicos oferecidos pela instituição, além de monitoramento está sujeita a auditoria que podem envolver inspeção física de equipamentos e registro de acessos à internet, tendo em vista a necessidade de manutenção da conformidade legal das operações do **SENAC SP**.

Como os equipamentos, tecnologias e serviços fornecidos para o acesso à internet e ao e-mail são propriedade da instituição, ela tem o direito de inspecionar e bloquear qualquer arquivo, site, correio eletrônico, domínio ou aplicação armazenados na rede/internet, que estejam em disco local na estação ou em áreas privadas da rede.

O Senac, ao monitorar a rede interna, visa garantir a integridade de seus dados e programas, bem como promover a segurança de seus usuários. Qualquer tentativa de alteração dos parâmetros de segurança, sem o devido credenciamento e a autorização para tal, acarretará a aplicação das penalidades administrativas e as previstas por lei pelos danos ou prejuízos ocasionados.

O uso indevido de qualquer recurso para atividades ilícitas ou que cause danos a terceiros será considerado violação às regras internas e terá as consequências previstas na legislação civil e criminal. Nesses casos, a instituição cooperará ativamente com as autoridades competentes.

O **SENAC SP** não é conivente com o comportamento indevido, ilegal ou antiético e, por isso, não autoriza o uso anônimo de seus recursos informacionais e tecnológicos, sendo que o tratamento de dados pessoais será feito em conformidade com a legislação pertinente.

Qualquer tentativa de burlar essa política será objeto de denúncia e aplicação de penalidades, especialmente se houver danos a terceiros e/ou à instituição.

A internet disponibilizada aos usuários da área educacional deve ser utilizada com finalidade educacional, sendo proibida sua utilização para a exposição de conteúdo íntimo ou de vida privada, tampouco vexatório e que possam de alguma forma gerar dano à terceiros e à própria instituição, lembrando que o ambiente está sujeito a monitoramento.

Na hipótese do uso indevido dos recursos disponibilizados, o usuário ficará ciente de que o conteúdo poderá ser retirado dos equipamentos independentemente de aviso prévio e após análise da gravidade e consequências de seus atos, poderá resultar na rescisão de seu contrato e/ou impedimento de matrículas futuras, considerando nesta última hipótese para usuário aluno.

Tendo em vista que os recursos tecnológicos pertencentes à instituição são destinados à uso exclusivamente profissional (quando pelo colaborador) e educacionais (quando pelo aluno), o **SENAC SP** não assume o compromisso de preservar conteúdos de caráter particular em seus equipamentos e/ou rede, isentando-se de qualquer responsabilidade por sua perda temporária ou definitiva.

O acesso pelo usuário dos computadores dos laboratórios e da biblioteca deve ser feito por meio de seu login educacional.

5.1. Política de Senhas

Alunos e colaboradores 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 de 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 obrigatório 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.

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.

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.

Recomenda-se o uso de aplicativo específico para armanezamento de senhas que utilize criptografia forte e duplo fator de autenticação, sendo de responsabilidade do usuário buscar um aplicativio seguro de boa reputação no mercado.

Regras para os acessos aos servidores e serviços educacionais, gerenciados pela Gerência de Tecnologia da Informação (Não se aplicam ao ambiente de ensino ou praticas de aula utilizada pelo docente).

- 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.

Nos 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.

5.2. A instituição não permite:

• o uso, a instalação, a cópia ou a distribuição não autorizada de material (conteúdo, software, imagens, áudios e outros) que esteja protegido por direitos autorais de terceiros, possua marca registrada ou patente na internet, sem que haja autorização prévia e formal de seu titular.

• a exposição, o armazenamento, a distribuição, a edição, a impressão ou a gravação, por meio de qualquer recurso, de material de cunho sexual que não esteja alinhado às áreas da instituição, devendo, nesses casos, atender aos preceitos éticos e legais.

• a publicação de aplicativos, sites ou sistemas web em servidores de hospedagem e nas lojas do Google Play, Apple Store, ou aplicação não devem ser vinculados as contas corporativas do Senac SP. Alunos e colaboradores assumem inteiramente a responsabilidade pelo uso do software, liberação para finalidade de publicação, registro de domínio e o pagamento à terceiros, como as lojas do Apple Store. Google Play e o REGISTROBR (ou similar). Dependendo do caso eles devem ser previamente autorizados pela Gerência de Tecnologia da Informação e pela gerência de desenvolvimento 2.

• o acesso a sites de proxy ou anonimizadores.

• o uso dos recursos tecnológicos do SENAC SP para deliberadamente propagar qualquer tipo de vírus, worm, cavalo de troia, spam, assédio, perturbação ou programas de controle de outros computadores.

O usuário que utilizar dispositivos móveis pessoais, mesmo quando autorizado pela instituição, é responsável pelos softwares e arquivos contidos em seus equipamentos.

Para o acesso à rede wifi do Senac São Paulo mediante dispositivos móveis pessoais, o usuário deverá preencher um cadastro prévio e solicitar os dados necessários para acessar a rede.

6. Regras de Uso para o Usuário Aluno

O acesso aos blogs, sites, fóruns e outras ferramentas nas salas de aula e laboratórios do **SENAC SP** poderá ser realizado quando descrito nos documentos pedagógicos.

Se por algum motivo o usuário aluno vier a tomar conhecimento ou acessar informações de propriedade da instituição ou dados pessoais e/ou sensíveis, ainda que de forma acidental, ele deverá preservar a sua confidencialidade, respondendo legalmente pelos danos materiais e morais que possam ser causados por sua divulgação, bem como por todas as despesas que a instituição incorrer com processos judiciais e honorários advocatícios.

O usuário aluno que divulgar informações não autorizadas do **SENAC SP**, não importando se a divulgação foi deliberada ou inadvertida, poderá sofrer as penalidades estabelecidas pelo Comitê de Segurança da Informação, sem prejuízo de eventual processo judicial.

Os conteúdos e mídias disponibilizados nos repositórios da instituição nos ambientes de aprendizagem virtuais utilizados oficialmente por ela têm finalidade educacional estando sob a proteção de Direitos Autorias e não podem ser copiados ou distribuídos sem autorização prévia.

Por se tratar de instituição educacional, o usuário aluno apenas poderá fazer download de arquivos da internet que sejam necessários ao desempenho de suas atividades nas salas de aula, laboratórios e bibliotecas, desde que previstos nos documentos educacionais e/ou autorizados pelo docente do curso.

Não é permitido o acesso, com fins pessoais, aos sites de instituições financeiras (internet banking) e de compras on-line pelo usuário aluno por meio dos equipamentos disponibilizados pelo **SENAC SP** em salas de aula, bibliotecas e laboratórios. A instituição não se responsabiliza pelas informações fornecidas por ele nesses acessos.

Não é permitida a publicação de aplicativos em lojas virtuais vinculadas ao Senac SP. Para publicação, os alunos poderão criar suas contas diretamente nas plataformas, responsabilizando-se pelo aceite do contrato e pelo (s) pagamento(s) referente(s) ao(s) software(s) e à terceiros.

Como regra geral, não poderá ser exposto, armazenado, distribuído, editado, impresso ou gravado através de qualquer recurso do **SENAC SP,** material que contenha:

a) Qualquer programa de computador que não seja prévia e formalmente homologado pela área de TI, notadamente programas de origem suspeita, pirateados ou com recursos de: camuflagem e/ou apagamento de histórico de navegação e desvio de Proxy;
b) Qualquer espécie de exploração sexual;
c) Qualquer forma de erotismo, pornografia ou pedofilia;
d) Qualquer forma de ameaça, chantagem e assédio moral ou sexual;
e) Qualquer ato calunioso, difamatório, infamante, vexatório, aviltante ou atentatório à moral e aos bons costumes da sociedade;

f) Preconceito baseado em cor, sexo, opção sexual, raça, origem, condição social, crença, religião, deficiências e necessidades especiais;
g) Incentivo ao consumo excessivo ou recorrente de bebidas alcoólicas, fumo e substâncias entorpecentes, sejam essas lícitas ou não;
h) A prática e/ou a incitação de crimes ou contravenções penais;
i) A prática de propaganda política nacional ou internacional;
j) A prática de quaisquer atividades comerciais desleais;
k) O desrespeito aos direitos de propriedade intelectual e industrial do **SENAC SP** e de terceiros;
l) A disseminação de códigos maliciosos tais como, mas não se limitando a, vírus e cavalos de Tróia;
m) Capaz de expor a infraestrutura computacional do **SENAC SP** e qualquer uma de suas unidades.

Entende-se por conteúdo difamatório e/ou ilícitos, mas não se limitando a estes exemplos, aqueles que prejudiquem a imagem de terceiros, afetem sua honra e decoro, que contenham ameaças, montagem de fotos, xingamentos, entre outros.

6.1 Dispositivos Móveis

O uso de dispositivos móveis particulares nas dependências do **SENAC SP** é de inteira responsabilidade de seu proprietário, tanto por sua guarda quanto pelos conteúdos nele instalados, sejam softwares, músicas, fotos, entre outros.

Para acesso à internet por meio de seus dispositivos móveis, o usuário aluno deverá obter um login e uma senha mediante cadastro no setor indicado na unidade e utilizar a rede sem fio (SSID) CONECTA SENAC.

A publicação de aplicativos de autoria do aluno feita em dispositivos móveis pessoais seguem a regra do item 5.2, portanto, não devem ser vinculados as contas corporativas do Senac SP. Alunos e colaboradores assumem inteiramente a responsabilidade pelo uso do software, liberação para finalidade de publicação e o pagamento à terceiros, como as lojas do Apple Store e Google Play (ou uso similar).

Tendo em vista que a Constituição Federal Veda o anonimato e que o Marco Civil da Internet exige a guarda de dados que possibilitem a identificação de usuários, todo acesso efetuado pela rede do SENAC SP deverá ser registrado e identificado, sendo que tais informações poderão ser utilizadas para investigação interna de ilícitos e infrações à Normas internas, bem como entregues às autoridades mediante ordem judicial.

6.2 Correio Eletrônico

O SENAC SP disponibiliza uma conta de e-mail que pode ser acessada através do Outlook no Portal do Office 365. A plataforma pode ser acessada em qualquer lugar e navegador e ser instalada em até 15 dispositivos (cinco computadores, cinco smartphones e cinco tablets) por usuário. O sistema também permite o armazenamento de arquivos em nuvem, por meio do OneDrive. O Senac não se responsabiliza por backups de materiais salvos na nuvem. Isso é de responsabilidade do aluno.

O usuário aluno com acesso à internet poderá usar seu correio eletrônico pessoal no ambiente do **SENAC SP** desde que essa ferramenta não seja utilizada de modo indevido, ilegal ou antiético.

É de inteira responsabilidade do aluno, a manutenção e segurança de seu e-mail e senha pessoal.

O **SENAC SP** não se responsabiliza por eventuais fraudes ou qualquer incidente que venha a ocorrer no e-mail pessoal do aluno, ainda que tenha sido no ambiente virtual da instituição.

O uso indevido do correio eletrônico pode acarretar processo judicial para identificação de autoria e ressarcimento de eventuais danos. Nestes casos o **SENAC SP** envidará seus esforços a fim de auxiliar autoridades na identificação de usuários, devendo entregar, conforme marco regulatório, às autoridades judiciais as informações que lhe couber.

6.3 Redes Sociais

Não será permitido o acesso às Redes Sociais pelos equipamentos do Senac SP nos laboratórios e bibliotecas – para exceções, a intencionalidade pedagógica e a liberação do acesso devem ser previamente acordados com a coordenação ou gerência.

Não é permitido ao aluno criar perfis, páginas ou grupos em redes sociais ou sites semelhantes, com o título de SENAC ou SENAC São Paulo, uma vez que se trata de marca protegida por questões legais.

O Senac SP não se responsabiliza pela criação de páginas, perfis e grupos de alunos, que não sejam institucionais, incluindo grupos em comunicadores instantâneos, cuja será de inteira responsabilidade do administrador e seus participantes.

Qualquer ação institucional do **SENAC SP** junto a seus alunos será devidamente divulgada como "Oficial" ou "Ação Institucional".

6.4 Uso de Comunicadores Instantâneos

O aluno poderá a qualquer momento disponibilizar seus dados de celular para comunicação via aplicativo de comunicação instantânea, caso em que poderá lhe ser encaminhado mensagens para informações relacionadas à prestação de serviços, à exemplo de, mas não se limitando à informações administrativas sobre cancelamento/ adiamento de cursos, suspensão de aulas etc, podendo ser enviadas para grupos de alunos/turmas e/ou pais e responsáveis.

As informações detalhadas sobre como tratamos os dados pessoais poderão ser encontradas em nossa Política de Privacidade.

6.5 Pesquisas

O Senac poderá, a fim de promover avaliação institucional, bem como para fins de melhorias de seus serviços, promover pesquisas junto a seus alunos e colaboradores.

Toda pesquisa disponibilizada pelo Senac SP deverá atender às regras da Políticas de Privacidade e Norma de Gestão e Proteção de Dados Pessoais.

A fim de atender ao princípio da transparência o Senac SP deverá informar, antes da coleta de dados pessoais ou sensíveis, a finalidade da pesquisa e tratamento a ser aplicado aos dados coletados, bem como a coleta do consentimento quando aplicável.

6.6 Alunos do Ensino Médio

Aos alunos do ensino médio deverão ser aplicadas as mesmas regras e normas, sem deixar de considerar a especificidade do segmento e consequentemente a devida proteção de dados pessoais e dados pessoais sensíveis, tendo em vista se tratar, na maioria dos casos, dados de titulares menores de dezoito anos.

O Senac SP disponibilizará acesso à ferramenta Teams da Microsoft, cujos pais ou responsável legal tem ciência de sua responsabilidade na orientação de seus filhos para uma conduta lícita, ética e respeitosa, orientando-os também a respeitar as regras internas da instituição.

É de inteira responsabilidade dos alunos e seus pais/responsável legal a guarda de sua identificação de acesso à ferramenta.

6.7 Do Suporte Técnico aos alunos

O SENAC SP poderá por critério próprio disponibilizar serviço de suporte técnico ao aluno para manutenção de seus equipamentos pessoais, com finalidade exclusiva de acesso aos ambientes educacionais e ferramentas necessárias à participação de aulas nos cursos disponibilizados pelo SENAC SP.

A assistência técnica será executada por terceirizado contratado pelo SENAC SP, considerado pela :GPD como agente Operador.

O Serviço estará sujeito a regras próprias a serem disponibilizadas na adesão do serviço, em local de fácil acesso, ficando o usuário sujeito ao tratamento de dados pessoais na forma disposta na Política de Privacidade em vigor na data de solicitação.

6.8 Recomendações

Recomenda-se que a internet seja utilizada com ética e cuidado, seguindo-se algumas premissas:

a. Uso estritamente educacional;
b. Não acesso de sites que não sejam relacionados ao seu curso;
c. Ao participar de redes sociais, nunca falar em nome do **SENAC SP** sendo prudente não expor suas informações pessoais;
d. Ter em mente que o **SENAC SP** é um local de estudo e o zelo pelo ambiente e pela proteção de dados pessoais e segurança das informações da instituição é responsabilidade de todo usuário.
e. Lembre-se que as leis se aplicam a nossa conduta independente do meio utilizado para nossas ações.
f. Perfil falso e conteúdos ofensivos geram responsabilidade.

O uso de conteúdos e imagens copiados da internet devem atender à legislação em vigor.

7. Regras de Uso para o Usuário Colaborador

O Senac é uma instituição educacional que preza pela capacitação e a atualização de seus colaboradores, bem como incentiva a utilização da tecnologia no processo de ensino aprendizagem.

Portanto, em ambientes educacionais ou durante as atividades com alunos, permite o uso de sites de notícias, buscadores, portais educacionais, blogs, chats, fóruns ou outros serviços para fins de atualização e pesquisa, em conformidade com os preceitos éticos, legais e alinhados com a proposta pedagógica e os documentos educacionais da instituição.

Não é recomendável o acesso, com fins pessoais, aos sites de instituições financeiras (internet banking) e de compras on-line pelo usuário colaborador por meio dos equipamentos disponibilizados pelo Senac São Paulo em salas de aula, bibliotecas e laboratórios. O usuário tem ciência de que o SENAC SP não se responsabiliza pelas informações fornecidas pelo colaborador nesses acessos.

Somente os usuários que estão devidamente autorizados a falar em nome do **SENAC SP** poderão se manifestar nos meios de comunicação em nome da instituição, seja por e-mail, entrevista on-line, podcast, seja por documento físico, entre outros.

O acesso aos sites ou o uso de jogos será permitido apenas para fins de pesquisa ou atividades didáticas nos cursos em que eles estejam previstos nos respectivos documentos educacionais e sejam requisito para o aprendizado do tema.

7.1 Propriedade Intelectual

As informações produzidas pelos usuários colaboradores no exercício de suas funções ou ainda pelos consultores, quando contratados para tanto, pertencem ao **SENAC SP**, como plano de aula, plano de curso, *storyboard*, conteúdos, mídias, entre outros.

Não é permitido o compartilhamento indevido de informações de propriedade da instituição, bem como de dados pessoais e dados pessoais sensíveis em mídias, como: listas de discussão, sites ou comunidades de relacionamento, salas de bate-papo ou chat, comunicadores instantâneos ou qualquer outra tecnologia correlata que venha surgir.

O usuário colaborador que divulgar informações não autorizadas do **SENAC SP**, não importando se a divulgação foi deliberada ou inadvertida, poderá sofrer as penalidades estabelecidas pelo Comitê de Segurança da Informação e também as previstas em lei.

Ao criar e ou manusear documentos o colaborador deverá atentar-se à Norma de Classificação da Informação e Proteção de Dados Pessoais.

Por se tratar de instituição educacional, o usuário colaborador poderá fazer download de arquivos da internet que sejam necessários ao desempenho de suas atividades, desde que devidamente

alinhados à proposta pedagógica da instituição e não infrinjam os direitos autorais.

Eventual autorização de uso privilegiado de recurso tecnológico poderá ser concedida em caráter temporário após análise do caso concreto, com justificativa plausível e podendo ser revogada a qualquer momento.

O acesso a softwares peer-to-peer e serviços de streaming (rádios on-line, canais de broadcast e similares), bem como serviços de comunicação instantânea, são permitidos ao usuário colaborador desde que estejam alinhados aos documentos educacionais ou tenham intencionalidade pedagógica em qualquer atividade educacional na instituição.

Para exceções, a intencionalidade pedagógica deve ser previamente acordada com a coordenação ou gerência.

7.2 Uso de Dispositivos Móveis

A regra para uso de dispositivos móveis disponibilizado pela instituição ou de uso particular, estarão previstas em norma específica do ambiente administrativo: **Norma de Uso de Dispositivos Móveis**.

7.3 Identificação

Cada usuário colaborador receberá um *login* e uma senha para acesso à rede. Ambos são pessoais, de uso individual, intransferíveis e confidenciais, não sendo permitido o seu empréstimo ou a revelação a quem quer que seja.

O usuário colaborador que ceder seus dados ou utilizar *logins* e senhas de terceiros estará sujeito às sansões administrativas previstas pelo Comitê de Segurança da Informação.

A responsabilidade perante a instituição e a terceiros em relação ao uso de sua identidade digital é do usuário, cuja identidade está associada ao *login*, respondendo ainda de acordo com a legislação brasileira na esfera cível e penal.

Caso o usuário esqueça sua senha, deverá requisitar formalmente sua troca pelo service desk e o usuário efetue a troca de senha após a resolução deste processo imediatamente, considerando sempre uma senha forte acima de 10 caracteres, contendo: Números, letras maiúsculas, minúsculas e caracteres especiais.

7.4 Uso de Correio Eletrônico

Para o uso de correio eletrônico disponibilizado pela instituição ao usuário colaborador, deverá ser seguida a Norma de Uso de E-mail do ambiente administrativo.

7.5 Redes Sociais

Não é permitido ao usuário colaborador falar em nome da instituição sem prévia autorização, seja nas redes sociais, em blogs ou entrevistas.

Ações institucionais deverão seguir as regras divulgadas mediante cada projeto.

Ações isoladas deverão constar no título que informe a inexistência de vinculação com a instituição.

O colaborador poderá sugerir ações institucionais ou oficiais para a instituição que deverá passar por aprovação da gerência responsável, caso em que se aprovado deverá sempre acompanhar o nome a extensão "oficial".

Sugerem-se as recomendações do item 6.4 desta Política.

7.6 Uso de Comunicadores Instantâneos

A utilização de comunicadores instantâneos pelas equipes educacionais deve seguir as regras internas e Manual de Uso disponibilizados pelo SENAC SP.

As informações detalhadas sobre como tratamos os dados pessoais poderão ser encontradas em nossa Política de Privacidade.

8. Do Ambiente Virtual De Aprendizagem

O SENAC SP utiliza-se de ambientes específicos para aprendizagem virtual (Blackboard para o Ensino Superior e MS Teams para as demais modalidades), considerados pela instituição como ferramentas oficiais.

O uso dos demais ambientes virtuais de aprendizagem serão permitidos, mediante prévia autorização, apenas para fins de pesquisa e, quando possível, para acesso por meio virtual.

Os conteúdos e mídias disponibilizados nos ambientes de aprendizagem virtuais têm finalidade educacional estando sob a proteção de Direitos Autorias e não podem ser copiados ou distribuídos sem autorização prévia.

Para o acesso ao Blackboard, o usuário deverá acessar a sua Área Exclusiva dentro do Portal do Senac SP, utilizando para isso o login utilizado durante o seu processo de matrícula. Ao realizar o primeiro acesso ao ambiente virtual de aprendizagem, o usuário deverá trocar imediatamente a sua senha conforme as orientações apresentadas nesse próprio ambiente e no manual do aluno.

A fim de garantir e preservar a segurança do usuário, do ambiente e os bons costumes, o **SENAC SP** reserva-se o direito de monitorar os meios de comunicação por ele disponibilizados e todos os recursos do ambiente virtual de aprendizagem.

Para atendimento de questões legais dados de registros de acesso e identificação permanecerão armazenados pelo tempo que a instituição entender necessário atendendo o prazo exigido por lei ou tempo necessário à execução do contrato ou ainda para outras finalidades previamente informadas ou autorizadas na Política de Privacidade e Proteção de Dados Pessoais.

Aplicam-se ao ambiente virtual de aprendizagem todas as demais regras contidas nesta Política, incluindo regras de conduta e abstenção de publicações ofensivas e demais conteúdos ilícitos, direitos autorias, bem como regras de privacidade e monitoramento.

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 Privacidade e Proteção de Dados Pessoais

Nos termos do art. 5, IV, da Lei 13.709/2018, o Senac SP enquanto instituição de ensino, para com seus alunos assume o papel de agente Controlador, portanto, responsável pelo tratamento de dados pessoais que promove, sendo que estes ocorrem para atendimento das finalidades, cuja devem estar informadas em sua Política de Privacidade e Proteção de Dados Pessoais.

O tratamento de dados pessoais de crianças e adolescentes terá como base no Enunciado n. 01 da ANPD de forma que poderá ser realizado com base nas hipóteses legais previstas no art. 7º ou no art. 11 da Lei Geral de Proteção de Dados Pessoais (LGPD), desde que observado e prevalecente o seu melhor interesse, a ser avaliado no caso concreto, nos termos do art. 14 da Lei.

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.

11. Das Disposições Finais

Os computadores das bibliotecas da rede **SENAC SP** destinam-se prioritariamente para fins de pesquisa, estudo e realização de trabalhos escolares. Será permitido o uso para outros fins desde que atenda às regulamentações e orientações institucionais.

Para o uso de computadores e o acesso à internet nas bibliotecas da rede, o usuário deverá solicitar seu cadastro no setor de atendimento da biblioteca. Essa recomendação não se aplica ao usuário colaborador.

O e-mail e login educacional (login e senha) é pessoal e intransferível.

Todo software educacional disponibilizado ao aluno regularmente matriculado é pessoal e intransferível. Por isso, o aluno não pode transferir, vender, compartilhar, sublicenciar, ceder ou emprestar sua conta de acesso. Após o término do vínculo com o Senac, o acesso ao software será automaticamente cancelado, devendo o aluno tratar diretamente com o fabricante.

Todo recurso de Tecnologia da informação e comunicação (TIC) particular, trazido para as dependências das unidades do Senac é de inteira responsabilidade de seu proprietário, incluindo os dados e softwares nele armazenados ou instalados

Não é permitida a alteração da disposição física dos computadores.

Será permitido o acesso aos sites de jogos, músicas, imagens, textos, inclusive o download de arquivos, desde que estejam de acordo com as diretrizes do guia de uso da biblioteca e relacionados ao processo de aprendizagem, não atrapalhem o correto tráfego de dados na rede nem infrinjam os direitos autorais.

Não é permitido o acesso aos softwares peer-to-peer, apenas aos serviços de streaming (rádios on-line, canais de broadcast e similares.

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.

Não é permitido o acesso, com fins pessoais, aos sites de instituições financeiras (internet banking) e de compras on-line pelo usuário por meio dos equipamentos disponibilizados pelo Senac São Paulo nas bibliotecas. A instituição não se responsabiliza pelas informações fornecidas pelo colaborador nesses acessos.

A instituição também não responde por imprecisões, incompatibilidades, erros, fraudes, falhas, inexatidão, divergência, perdas ou quaisquer outros danos durante o uso dos equipamentos, sendo todos de plena responsabilidade do usuário.

Aos professores se aplicam subsidiariamente as regras da Política de Segurança da Informação Administrativa.

Assim como a ética, a segurança deve ser entendida como parte fundamental da cultura interna do **SENAC SP**. Ou seja, qualquer incidente de segurança subtende-se como alguém agindo contra a ética e os bons costumes regidos pela instituição.

12. Documentos Relacionados

Política de Segurança da Informação Administrativa;

- 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;

Código de Conduta do Senac São Paulo;