Política de Segurança da Informação / PSI

Documento de Diretrizes e Normas Administrativas

Política de Segurança da Informação / PSI 2019-2021

Administração Regional
Itelvino Pisoni
Presidente

Comitê Gestor de TI

Lunáh Brito Gomes	Diretora Regional
Cláudia Oneide Silva	Gerente Administrativa e Financeira
Dirce Betânia de O. Faustino	Gerente de Educação Profissional
Edmilson Teles Ribeiro	Coordenador de Tecnologia da Informação
Antônio Xavier de Barros Junior	Coordenador de Compras e Licitações
Weslley Luis Araújo Silva	Coordenador do Departamento Pessoal
Danillo Soares Milhomens	Analista de Sistemas
Geraldo Magela	Assessor de Recursos Humanos

Equipe de elaboração do PSI

Edmilson Teles Ribeiro
Danillo Soares Milhomens
Denilson Félix Pinto
Nathália Dias Maciel Pinheiro
Felipe Fernandes de Albuquerque

HISTÓRICO DE ALTERAÇÕES DO PSI

Data	Versão	Descrição	Autor
02-abril-2019	v.2		Equipe TI

ÍNDICE

1. APRESENTAÇÃO

A Política de Segurança da Informação, também referida como PSI, é o documento que orienta e estabelece as diretrizes corporativas do SENAC-TO para a proteção dos ativos de informação e a prevenção de responsabilidade legal para todos os usuários. Deve, portanto, ser cumprida e aplicada em todas as áreas da instituição.

A presente PSI baseia-se recomendações dispostas na norma ABNT NBR ISO/IEC 27001 e 27002, reconhecida como um código de práticas para a gestão da Segurança da Informação, alinhada com as leis em vigor no país.

Com a intenção de aumentar a segurança da infraestrutura tecnológica direcionada ao uso administrativo, foi desenvolvido este documento com a finalidade nortear ou direcionar o usuário a fazer o bom uso dos ativos de tecnologia da informação disponibilizados.

2. OBJETIVO

A informação é um dos principais patrimônios do mundo dos negócios. Um fluxo de informação de qualidade é capaz de decidir o sucesso de um empreendimento. Mas esse poder, somado à crescente facilidade de acesso, faz desse "ativo" um alvo de constantes ameaças internas e externas.

Quando não gerenciados adequadamente, tais riscos e ameaças podem causar consideráveis danos ao SENAC e prejudicar o crescimento da instituição e sua vantagem competitiva. Em atenção a esse fato, é publicado a Política de Segurança da Informação, o alicerce dos esforços de proteção à informação desta instituição.

É público o conhecimento de que gerenciar a Segurança da Informação requer esforços contínuos para a proteção dos ativos de informação, auxiliando o SENAC-TO a cumprir sua missão. Para tanto, visa-se atingir os seguintes objetivos:

Confidencialidade: garantir que as informações tratadas sejam de conhecimento exclusivo de pessoas especificamente autorizadas;

Integridade: garantir que as informações sejam mantidas íntegras, sem modificações indevidas – acidentais ou propositais;

Disponibilidade: garantir que as informações estejam disponíveis a todas as pessoas autorizadas a tratá-las.

Autenticidade: garantir a identidade e veracidade da autoria da informação, com a garantia de que o emissor não poderá negar a autoria da mensagem (atributo de não-repúdio).

3. PREMISSAS

3.1. APLICAÇÕES DA PSI

As diretrizes aqui estabelecidas deverão ser seguidas por todos os colaboradores, bem como pelos prestadores de serviços, e se aplicam à informação em qualquer meio ou suporte.

Esta política dá ciência a cada colaborador de que os ambientes, sistemas, computadores e redes da empresa poderão ser monitorados e terem geração de documentações de registros de uso e acesso.

É também obrigação de cada colaborador manter-se atualizado em relação a esta PSI e aos procedimentos e normas relacionadas, buscando orientação do seu gestor ou da Coordenação de TI sempre que não estiver absolutamente seguro quanto à aquisição, uso e/ou descarte de informações.

3.2. PRINCÍPIOS DA PSI

Toda informação produzida ou recebida pelos colaboradores, como resultado da atividade profissional contratada pelo SENAC Tocantins, pertence à referida instituição. As exceções devem ser explícitas e formalizadas em contrato entre as partes.

Os equipamentos de informática e comunicação, sistemas e informações são utilizados pelos colaboradores para a realização das atividades profissionais. O uso pessoal dos recursos é permitido desde que não prejudique o desempenho dos sistemas e serviços.

Toda informação relacionada às operações, ações e/ou atividades gerada ou desenvolvida nas dependências do SENAC, pertence unicamente ao ativo desta instituição. Torna-se obrigatório a documentação de toda solução desenvolvida por este departamento como: local onde está hospedado, linguagem e versão, banco de dados e versão dentre outros.

Independentemente da forma apresentada ou do meio pelo qual é compartilhada ou armazenada, a informação deve ser utilizada unicamente para a finalidade a qual foi autorizada.

A modificação, divulgação e destruição não autorizadas e oriundas de erros, fraudes, vandalismo, espionagem ou sabotagem consequentemente causam danos aos negócios do SENAC.

É atributo da TI que toda informação de propriedade do SENAC seja amparada de riscos e ameaças que possam comprometer a confidencialidade, integridade ou a disponibilidade.

3.3. REQUISITOS DA PSI

Para a uniformidade da informação, a PSI deverá ser comunicada a todos os colaboradores do SENAC Tocantins a fim de que a política seja cumprida dentro e fora da empresa.

Tanto a PSI quanto as normas, deverão ser revistas e atualizadas periodicamente, sempre que algum fato relevante ou evento motive sua revisão antecipada, conforme análise e decisão percebida pelos integrantes deste setor.

Todo incidente que afete a segurança da informação deverá ser comunicado inicialmente à Coordenação de TI. Um plano de contingência e a continuidade dos principais sistemas e serviços deverão ser implantados e testados no mínimo anualmente, visando reduzir riscos de perda de confidencialidade, integridade e disponibilidade dos ativos de informação.

Deverão constar nos contratos de trabalho dos funcionários alocados na área de TI (vinculados à Coordenação de Tecnologia da Informação) do SENAC, o anexo de Acordo de Confidencialidade ou Cláusula de Confidencialidade, como condição imprescindível para que possa ser concedido o acesso aos ativos de informação disponibilizados pela instituição.

A responsabilidade em relação à segurança da informação deve ser comunicada na fase de contratação dos colaboradores. Todos os funcionários deverão ser orientados quanto aos procedimentos de segurança, bem como do uso correto dos ativos, afim de mitigar possíveis riscos.

Todo incidente que afete a segurança da informação deverá ser comunicado inicialmente à Coordenação de TI e ela, se julgar necessário, deverá encaminhar posteriormente ao Comitê de Segurança da Informação para análise.

Todos os requisitos de segurança da informação, incluindo a necessidade de planos de contingência, devem ser identificados na fase de levantamento de escopo de um projeto ou sistema, e justificados, acordados, documentados, implantados e testados durante a fase de execução.

Deverão ser criados e instituídos controles apropriados, trilhas de auditoria ou registros de atividades, em todos os pontos e sistemas em que a instituição julgar necessário para reduzir os riscos dos seus ativos de informação como, por exemplo, nas estações de trabalho, notebooks, nos acessos à internet, no correio eletrônico, nos sistemas comerciais e financeiros desenvolvidos pelo SENAC Tocantins ou por terceiros.

Os ambientes de produção devem ser separados e rigidamente controlados, garantindo o isolamento necessário em relação aos ambientes de desenvolvimento, testes e homologação.

O SENAC exonera-se de toda e qualquer responsabilidade decorrente do uso indevido, negligente ou imprudente dos recursos e serviços concedidos aos seus colaboradores, reservando-se o direito de analisar dados e evidências para obtenção de provas a serem utilizadas nos processos investigatórios, bem como adotar as medidas legais cabíveis.

O não cumprimento dos requisitos previstos nesta PSI e das Normas de Segurança da Informação acarretará violação às regras internas da instituição e sujeitará o usuário às medidas administrativas e legais cabíveis.

3.4. SOFTWARES DE CONVERSAÇÃO INSTANTÂNEA (Instant Messengers)

Os softwares de conversação instantânea, ou IM-Instant Messengers, são programas que permitem aos usuários se comunicarem remotamente (à distância), através de conexão com a Internet. Por meio destes programas, é possível enviar mensagens de texto entre equipamentos fisicamente distantes. Também é possível enviar arquivos ou iniciar sessões de conversação com áudio e/ou com vídeo, em tempo real.

Os IM apareceram como a solução para muitas empresas/setores que não possuíam linha telefônica externa ou que pretendiam reduzir custos com ligação. As sessões de áudio substituíam o telefone convencional e o envio de arquivos superava a remessa via correio, pelo fato de serem instantâneos (em menos de um minuto o arquivo já estava no micro do destinatário) e a custo zero. Hoje, no SENAC-TO, padronizou-se entre seus colaboradores a utilização dos recursos advindos de uma ferramenta Open Source, através da implantação da solução Openfire. O mesmo utiliza como cliente o aplicativo conhecido como "Spark". Essa solução veio ao encontro da redução considerável de ligações e consequentemente deduzindo os valores financeiros em custos mensais pagos as operadoras de telefonias seja ela fixa ou móvel, além de ter ou manter registro de conversações, podendo servir de registro ou documento no futuro.

A não utilização do software proposto e adotado por esta instituição poderá trazer problemas de segurança, visto que uma vez conectado, o computador ficará altamente vulnerável à ataques externos. As portas de entrada/saída ficarão abertas, sem qualquer restrição de leitura ou gravação de dados. Desta forma, vírus ou outras ameaças virtuais que exploram esse tipo de vulnerabilidade não encontrarão empecilhos para se instalarem e iniciarem seus processos danosos, não só para aquele computador em específico, mas também para todos os que a ele estiverem conectados em rede.

Estabelece-se nesta PSI, que as conversas ou registros de conversação realizados através da ferramenta Spark, só poderão ser fornecidas às gerências ou diretoria deste regional, mediante solicitação aberta através do sistema GLPI. Tal serviço também permite ao usuário efetuar o acompanhamento de seus chamados, bem como efetuar buscas por solicitações já realizadas, através do fornecimento de filtros como: data, horário, pessoas envolvidas, palavras chaves, dentre outros.

Todos os registros de conversas são de extrema confidencialidade e somente o coordenador de TI possui acesso à base de dados do mensageiro. Por este motivo, quanto maior o número de informação disponível para consulta, menor será o tempo e a demanda de serviço para apropriação de uma determinada conversa.

3.5. DIREITOS DE PROPRIEDADE

Todo produto resultante do trabalho dos colaboradores deste departamento regional (coleta de dados e documentos, sistema, metodologia, dentre outros) é propriedade do SENAC-TO. Em caso de extinção ou rescisão do contrato de prestação de serviços, independente do motivo de seu desligamento, o funcionário deverá devolver todas as informações confidenciais geradas e/ou manuseadas em decorrência de seu trabalho junto ao SENAC-TO, ou emitir declaração de que as destruiu.

3.6. A REALIZAÇÃO DE DOWNLOADS

O processo de realização de downloads exige banda considerável de navegação do servidor e, quando realizados em demasia ou forma descriteriosa, congestiona o tráfego, tornando a navegação para os demais usuários, inviável. Prejudica também diretamente o uso dos sistemas corporativos que dependem da internet para a execução de suas atividades.

Por esse motivo, existe nos servidores do SENAC um Controle de Downloads, que reduz a velocidade de descarga desses arquivos, visando evitar o congestionamento ou lentidão no acesso à internet. Havendo a necessidade de baixar arquivos "pesados", o usuário poderá entra em contato com Coordenação de TI solicitando que o setor de Suporte efetue o download.

3.7. EXECUÇÕES DE MÍDIAS ON-LINE

Não havendo pertinência com as finalidades institucionais propostas pelo SENAC-TO, é terminantemente proibida a execução de jogos, TV, vídeos, músicas ou rádios on-line, visto que esta prática demanda banda de navegação de internet, dificultando a execução de outros serviços do SENAC-TO que necessitam deste recurso. Excetua-se desta regra, os usuários autorizados através de solicitação advinda de sua chefia imediata.

3.8. DO SIGILO E CONFIDENCIALIDADE.

3.8.1. A análise dos casos de violação desta PSI e suas penalidades serão analisadas pelo respectivo chefe imediato em conjunto com o Comitê Gestor de Tecnologia da Informação (CGTI).

3.8.2. O CGTI é de natureza deliberativa e é do tipo estratégico, responsável pela deliberação de políticas, diretrizes e planos relativos a TI, pela análise de investimentos e pelo uso estratégico e seguro da informação no âmbito do SENAC Tocantins. Seu corpo dirigente é formado pelo Diretor(a) Regional, Gerente de Administrativo e Financeiro, Gerente de Educação Profissional, Coordenador de Tecnologia da Informação, Comissão Permanente de Licitação, Coordenador do Departamento Pessoal, pelo Analista de Sistemas do SENAC e pelo Coordenador de Recursos Humanos da instituição.

3.8.3. A não observância pelo funcionário das normas desta PSI, seja isolada ou cumulativamente, implicará as seguintes punições: Aviso de Descumprimento, Advertência ou Suspensão, Demissão por Justa Causa e abertura de processo civil ou criminal, se for o caso.

3.8.4. O Aviso de Descumprimento será enviado por e-mail ao funcionário infrator e ao chefe imediato na primeira violação cometida, indicando qual a norma que foi violada.

3.8.5. A Advertência ou Suspensão Disciplinar será aplicada por escrito nos casos de infrações de menor gravidade ou na hipótese de reincidência e será registrada na ficha pessoal do funcionário.

3.8.6. A Demissão por justa causa será aplicada nos casos legais e de natureza grave ou nas hipóteses previstas no artigo 482 da Consolidação das Leis do Trabalho, resumidas a seguir:

a) Ato de Improbidade – todo ato no qual o funcionário descumpre um dever legal, cuja conduta pode ser considerada abusiva e desonesta, causando prejuízos ao patrimônio do empregador.

b) Incontinência de conduta ou mau procedimento – A incontinência de conduta refere-se a quaisquer atos imorais praticados no ambiente de trabalho, tais como: exibir fotos pornográficas, desrespeitando os colegas e a Instituição. O mau procedimento ocorre toda vez que o funcionário age de forma incompatível com as regras da empresa.

c) Ato de Indisciplina ou de Insubordinação – O ato de indisciplina é caracterizado por descumprimento de ordens gerais do empregador a todos os funcionários. Ato de Insubordinação é o descumprimento de ordens pessoais do chefe imediato a determinado empregado.

d) Violação de segredo da empresa –Consiste no ato do empregado, passar a outrem informação sigilosa ou sem autorização do empregador.

4. USO DO CORREIO ELETRÔNICO.

O uso do correio eletrônico do SENAC-TO é exclusivamente para fins corporativos relacionados às atividades de trabalho do setor. O uso desta atividade para fins pessoais não é recomendado já que a prática para fins pessoais pode ocorrer insucessos e acabar prejudicando a imagem desta instituição.

Para fortalecer nossa segurança, o corpo técnico do SENAC deverá seguir as seguintes orientações:

4.1. Caixas postais de correio eletrônico (criação, alteração e exclusão):

4.1.1. As caixas postais são identificadas unicamente por meio de seu endereço eletrônico;
4.1.2. No âmbito do SENAC, o domínio do endereço eletrônico é “to.senac.br”;
4.1.3. A capacidade máxima de armazenamento das caixas postais será de 1,5 terabytes (GB);
4.1.4. Somente será criada caixa postal institucional pessoal, caixa postal institucional do setor ou caixa postal de sistema;
4.1.5. As solicitações de criação, alteração e exclusão de caixas postais devem ser encaminhadas à Coordenação de Tecnologia da Informação (CTI);
4.1.6. No caso de alteração de endereço eletrônico, o endereço antigo será mantido apenas pelo período de 1 (um) mês, a contar da alteração;

4.2. Caixa Postal Institucional Pessoal:

4.2.1. Colaboradores e prestadores de serviço do SENAC:

4.2.1.1. Todo colaborador poderá ter uma caixa postal institucional pessoal;
4.2.1.2. A solicitação de caixa postal institucional pessoal para colaboradores incumbe à sua chefia imediata.

4.2.1.3. O identificador do endereço de correio eletrônico será formado pelo primeiro nome e pelo último sobrenome do colaborador, separados pelo sinal de ponto.

4.2.1.4. Em situações justificadas, o identificador dos endereços de correio eletrônico poderá ser formado segundo outra ordem ou abreviação do nome do usuário.

4.2.1.5. A adequação dos endereços de correio eletrônico que não correspondam ao padrão estabelecido nesta norma será solicitada à Coordenação de Tecnologia da Informação (CTI) pelo usuário interessado.

4.2.1.6. A caixa postal institucional pessoal de colaboradores e/ou contratados temporários será excluída definitivamente nos casos de falecimento, demissão, aposentadoria ou quaisquer situações que impliquem em desvinculo com o SENAC.

4.2.1.7. Ocorridos os fatos descritos no item anterior, incumbe ao Departamento Pessoal comunicá-los à Coordenação de Tecnologia da Informação (CTI).

4.2.1.8. Nos casos de demissão ou quaisquer situações que impliquem em desvinculo com o SENAC, haverá suspensão imediata da caixa postal institucional, a partir da comunicação do Departamento Pessoal;

4.2.1.9. A exclusão da caixa postal será realizada somente após comunicada pelo Departamento Pessoal a decisão definitiva sobre o afastamento.

4.2.2. Estagiários:

4.2.2.1. O gestor da unidade operativa ou chefia imediata poderá solicitar, por escrito, a criação de caixa postal institucional pessoal ao estagiário somente quando houver essa necessidade para o serviço a ser desempenhado.

4.2.2.2. O envio de mensagens por estagiários será restrito a endereços eletrônicos mantidos pelo SENAC, exceto quando expressamente solicitado o envio a endereços externos pelo gestor da unidade operativa ou coordenação de setor a que forem vinculados, com a devida justificativa.

4.2.2.3. O uso do correio eletrônico pelo estagiário autorizado será de responsabilidade do coordenador da unidade a que está vinculado.

4.2.2.4. O identificador do endereço eletrônico do estagiário será formado pela primeira letra do seu nome seguida do último sobrenome, acrescido pela palavra “estagiário”, separados pelo sinal de ponto.

4.2.2.5. A caixa postal institucional pessoal de estagiários será excluída definitivamente quando da comunicação do Departamento Pessoal sobre o término do estágio.

4.3. Caixa Postal Institucional da Unidade/Setor:

4.3.1. As unidades ou setores administrativos previstos na estrutura organizacional do SENAC poderão ter caixa postal institucional da unidade.

4.3.2. O gestor da unidade ou setor será também o gestor da respectiva caixa postal, competindo-lhe:

a) *solicitar a criação, a alteração e a exclusão da caixa postal institucional da unidade/setor;*

b) *autorizar o acesso de outros colaboradores, mediante delegação no sistema de correio eletrônico, bem como excluir esse acesso.*

4.3.3. A caixa postal institucional da unidade terá um único endereço de correio eletrônico, cujo identificador será formado pela denominação da unidade ou por sigla que permita a sua identificação.

4.3.4. Em casos excepcionais, devidamente justificados, e a critério das unidades operativas ou chefias de setores, poderão ser criadas caixas postais institucionais, a fim de atender comissões, grupos de trabalho ou núcleos formalmente constituídos, bem como demandas de trabalho específicas e eventos temporários.

4.3.5. Nessa hipótese, quando da solicitação de criação da caixa postal, deverão ser indicados o colaborador que será responsável pelo respectivo gerenciamento, bem como, se for o caso, o período em que a caixa postal deverá ser mantida.

4.4. Caixa Postal de Sistemas:

4.4.1. A caixa postal de sistema será criada quando houver essa necessidade para o funcionamento de um sistema informatizado.

4.4.2. O gestor da unidade responsável pelo desenvolvimento ou manutenção do sistema informatizado será também o gestor da respectiva caixa postal, competindo-lhe:

a) *solicitar a criação, alteração e exclusão da caixa postal de sistema;*

b) *autorizar o acesso de outros colaboradores, mediante delegação no sistema de correio eletrônico, bem como excluir esse acesso.*

4.4.3. O identificador do endereço de correio eletrônico será formado pela denominação ou sigla que permita a identificação do respectivo sistema informatizado.

4.5. Listas de Distribuição (criação, alteração e exclusão):

4.5.1. É permitida a criação de lista de distribuição, com o objetivo de facilitar e otimizar a troca de informações sobre assuntos de interesse do SENAC.

4.5.2. A criação de lista de distribuição pode ser solicitada pelo gestor da unidade a qual se destina ou pela Diretoria Regional.

4.5.3. A solicitação deve ser encaminhada, por escrito, à Coordenação de Tecnologia da Informação (CTI), acompanhada de justificativa e de informações sobre a finalidade da lista, nome do gestor da lista, e, quando destinada à atividade temporária, do período de sua duração.

4.5.4. Cada lista de distribuição terá um gestor, a quem incumbe:

a) *manter permanentemente atualizado o rol de integrantes da lista de distribuição;*

b) *solicitar exclusão como gestor e indicar, simultaneamente, o novo responsável pela lista de distribuição;*

c) *solicitar exclusão da lista de distribuição, quando esta não for mais necessária.*

4.5.5. O identificador do endereço eletrônico será formado pela denominação ou sigla, que permita, de forma clara, a identificação de sua finalidade, ou do grupo de endereços eletrônicos nela reunidos, seguido da palavra "lista", separados por hífen.

4.5.6. No caso de alteração de endereço eletrônico, o endereço antigo será mantido pelo período máximo de 1 (um) mês, a contar da alteração.

4.5.7. O envio de mensagem eletrônica para lista de distribuição que englobe elevado número de endereços eletrônicos somente é permitido em caráter excepcional e por aquelas unidades administrativas autorizadas pela Diretoria Regional.

4.6. Utilização dos Recursos do sistema de correio eletrônico:

4.2.1. O uso do correio eletrônico institucional restringe-se a mensagem cujo objeto seja, necessariamente, inerente à atividade funcional do usuário, sendo vedado o uso para fins particulares.

4.2.2. Fica proibido a divulgação de informações não autorizadas ou imagens de tela, sistemas, documentos e afins sem autorização expressa e formal concedida pelo proprietário desse ativo de informação;

4.2.3. Não abrir anexos com as extensões, .bat, .exe, .src, .lnk e .com, ou de quaisquer outros formatos alertados pela Coordenação de TI ou suporte de TI, se não tiver certeza absoluta de que solicitou esse e-mail;

4.2.4. Julgar todo e qualquer e-mail com assuntos estranhos, fornecido por pessoas que não a conheça ou em inglês;

4.2.5. O acesso ao correio eletrônico, a partir de estações de trabalho fornecidas pelo SENAC, será feito apenas a partir do navegador de internet.

4.2.6. É vedada a tentativa de acesso a caixas postais às quais o usuário não tenha autorização de acesso.

4.2.7. Após 3 (três) tentativas de acesso à caixa de e-mail com senha ou nome de usuário incorretos, o referido e-mail é automaticamente bloqueado. Caso isto ocorra, o usuário deve abrir um chamado documentando o ocorrido através da ferramenta GLPI, havendo fatores adversos como, GLPI inacessível e urgência em relação dependência desse fator para conclusão ou resolução de sua atividade, deve-se contatar a Coordenação de TI ou suporte de TI;

4.2.8. Adotar o hábito de ler sua caixa de e-mails diariamente, de modo a evitar que se acumulem os e-mails;

4.2.9. Utilizar o e-mail para comunicações oficiais internas, as quais não necessitem obrigatoriamente do meio físico escrito. Isto diminui custo com impressão e aumenta a agilidade na entrega e leitura do documento. Observar: para aqueles documentos que necessitarão do meio físico (os que irão gerar processos e outros documentos aos quais serão anexados outros comprovantes etc), utilizar o meio convencional impresso.

4.2.10. A Coordenação de Tecnologia da Informação (CTI) não se responsabiliza pelo conteúdo armazenado nos correios eletrônicos, ou pela realização de eventuais

backups, bem como pela perda de e-mails advinda da utilização descuidada da ferramenta de correio eletrônico.

4.2.11. É de responsabilidade do usuário:

a) *utilizar o correio eletrônico institucional de acordo com os preceitos desta Norma;*

b) *eliminar periodicamente as mensagens eletrônicas desnecessárias contidas nas caixas postais;*

c) *manter apenas o seu acesso à conta institucional pessoal de correio eletrônico, sendo vedada a disponibilização desse acesso a terceiros;*

d) *informar à Coordenação de Tecnologia da Informação (CTI) o recebimento de mensagem que contrarie o disposto no item 7.7.*

4.2.12. É vedado aos usuários o envio de qualquer mensagem eletrônica contendo:

a) *informações privilegiadas, confidenciais e/ou de propriedade do SENAC para destinatários não autorizados;*

b) *materiais obscenos, ilegais ou antiéticos;*

c) *materiais preconceituosos ou discriminatórios;*

d) *materiais caluniosos ou difamatórios;*

e) *propaganda com objetivo comercial;*

f) *listagem com endereços eletrônicos institucionais;*

g) *malwares (item 2.8);*

h) *material de natureza político-partidária, associativa ou sindical, que promova a eleição de candidatos para cargos eletivos;*

i)material protegido por lei de propriedade intelectual;

j)entretenimentos e "correntes";

k) *assuntos ofensivos;*

l)músicas, vídeos ou animações que não sejam de interesse específico do trabalho;

m) *Spam, phishing e hoax (itens 2.7, 2.8 e 2.11);*

n) *materiais criptografados.*

4.3. Monitoramento e Auditoria:

4.6.1. O uso do correio eletrônico será monitorado por meio de ferramentas com o intuito de impedir o recebimento de spam, hoax, phishing, mensagens contendo vírus e outros arquivos, que coloquem em risco a segurança da infraestrutura tecnológica do SENAC ou que contenham conteúdo impróprio.

4.6.2. As auditorias ordinárias ou extraordinárias serão coordenadas pela Coordenação de Tecnologia da Informação (CTI) e os relatórios serão encaminhados à Direção Regional.

4.6.3. As auditorias extraordinárias deverão ser precedidas de autorização da Direção Regional.

5. LICENCIAMENTO DE SOFTWARE

Ter uma Política de Licenciamento de Software efetiva, proporciona ao SENAC a garantia de confiabilidade, integridade e disponibilidade das informações tratadas no ambiente corporativo da empresa. São reais os benefícios na utilização de softwares licenciados, além do cumprimento da lei e das garantias do produto: acesso periódico a atualizações e melhorias; acessos a patches de segurança contra ameaças cibernéticas; melhor desempenho e produtividade; acesso a suporte, dentre outras vantagens.

O principal propósito deste item é definir critérios para garantir a integridade e a segurança da informação deste Departamento Regional, estabelecendo práticas recomendadas a todos os funcionários quanto ao uso e operacionalidade de software. Evidencia-se que o descumprimento deste documento implicará em penalidades aos que o infringirem.

Estão estabelecidos e devidamente catalogados todos os softwares e suas licenças na base de conhecimento no sistema GLPI (Gerenciamento de Livre de Parque de Informática. Sua integração ao OCS (Open Computer and Software) terá a finalidade efetuar análises de toda a rede computacional do SENAC/TO, visando assim evitar a instalação de softwares piratas nesta instituição.

5.1. Pontos relevantes e de cumprimento do departamento de TI do DR-TO:

5.1.1. O usuário deve conhecer as instruções, regras e penalidades de funcionamento do serviço que esteja a utilizar, devendo ainda observar o previsto em lei e normas da empresa;
5.1.2. Revisão dos termos e condições de cada licença para assegurar utilização apropriada;
5.1.3. Criação de um repositório para as mídias;
5.1.4. Arquivamento dos termos e condições em um local de fácil acesso aos membros de TI;
5.1.5. Gerenciamento do ciclo de vida dos softwares com notificações quando suas datas de vencimentos estiverem próximo ao fim;
5.1.6. Monitoramento das atividades de instalação de software por usuários;
5.1.7. Inventário de software;
5.1.8. Gerenciamento de permissões para instalação;
5.1.9. Fornecimento de suporte técnico apenas a aplicativos e dispositivos licenciados;
5.1.10. Não permitir ao usuário final opções de adicionar ou remover programas;
5.1.11. Software não licenciados serão desinstalados;
5.1.12. Qualquer software que, por necessidade do serviço daquele setor, necessitar ser instalado, deverá ser comunicado com antecedência à Coordenação de Informática.
5.1.13. Fica permanentemente proibida a instalação de quaisquer softwares que o SENAC-TO não detenha a licença de uso.
5.1.14. A Coordenação de Informática poderá valer-se de sua autonomia para desinstalar, sem aviso prévio, todo e qualquer software sem licença de uso, em atendimento à Lei 9.609/98 (Lei do Software).
5.1.15. Pedidos de instalação de Softwares ou Sistemas Operacionais deverão ser comunicados à Coordenação de Tecnologia da Informação, seja

pelos setores administrativos ou pedagógicos, com antecedência de 3 (três) dias uteis.

A adesão a essa política evitará ao DR-TO os riscos punitivos descritos em lei, minimizará consideravelmente a redução de infecção por vírus ou outras pragas virtuais, proporcionará maior garantia de segurança, reduzirá o número de chamados ao suporte de TI, garantirá a longevidade de seu equipamento, acarretará no aumento da produção de trabalho, aumentará a segurança de seus registros, bem como diminuirá falhas e/ou imprevistos de segurança, contribuindo também na manutenção atualizada do inventário, enfim, aspectos estes garantidos através do cumprimento das diretrizes da Política de Segurança da Informação (PSI).

6. USO DE RECURSOS DE TI

Os equipamentos disponíveis aos colaboradores são de propriedade do SENAC Tocantins, cabendo a cada um utilizá-los e manuseá-los corretamente para as atividades de interesse da instituição. Para tanto, enseja-se importante o seguimento de diretrizes visando utilizar tais recursos de forma eficiente, tais como:

6.1. Diretrizes Gerais:

6.1.1. O uso adequado dos recursos de tecnologia da informação visa garantir a continuidade das atividades desenvolvidas no SENAC.

6.1.2. Os recursos de tecnologia da informação disponibilizados pelo SENAC aos usuários serão utilizados em atividades relacionadas às funções institucionais, e abrangem os seguintes elementos:

6.1.2.1.1. os computadores servidores, os computadores para uso individual ou coletivo, de qualquer porte, os equipamentos de armazenamento e distribuição de dados, os dispositivos móveis, as impressoras, as copiadoras e os equipamentos multifuncionais, assim como os respectivos suprimentos, periféricos e acessórios;

6.1.2.1.2. a rede lógica do SENAC e os respectivos canais e pontos de distribuição;

6.1.2.1.3. as contas de acesso dos usuários, assim como os certificados digitais;

6.1.2.1.4. os sistemas computacionais desenvolvidos com base nos recursos providos pelo SENAC;

6.1.2.1.5. os sistemas computacionais contratados de terceiros, sob licença ou na forma de software livre ou aberto, incluídas as soluções baseadas em nuvem.

6.1.3. O usuário é responsável por:

6.1.3.1.1. zelar pelos recursos que lhe sejam destinados para o exercício de suas atribuições, especialmente os de utilização pessoal, tais como computadores, impressoras, dispositivos móveis e demais equipamentos;

6.1.3.1.2. preservar o sigilo de sua senha ou outro mecanismo de autenticação que venha a ser utilizado para acesso aos recursos tecnológicos disponibilizados;

6.1.3.1.3. preservar o sigilo das informações a que tiver acesso, sendo vedada sua revelação a usuários ou terceiros não autorizados;

6.1.3.1.4. atos praticados e acessos realizados aos recursos de tecnologia por meio de sua credencial de acesso.

6.1.4. Os procedimentos de instalação, configuração e manutenção de equipamentos e softwares serão realizados pela Coordenação de Tecnologia da Informação (CTI) ou por terceiros por ela autorizados, sob a supervisão do gestor da unidade ou setor, que verificará a adequação do serviço realizado ao atendimento das atividades desenvolvidas pela unidade/setor.

6.1.5. Os sistemas e computadores devem ter versões do software antivírus instalados, ativados e atualizados permanentemente. O usuário, em caso de suspeita de vírus ou problemas na funcionalidade, deverá acionar o departamento técnico responsável mediante registro de chamado GLPI.

6.1.6. É terminantemente proibido o consumo de alimentos ou bebidas próximo aos equipamentos de informática.

6.1.7. Não será fornecido suporte a equipamentos particulares (computadores, notebooks, smartphones, tablets e demais dispositivos de informática), seja quanto à instalação e configuração de sistemas ou aplicativos, ainda que disponibilizados pelo SENAC, seja quanto às questões relacionadas à conexão à rede sem-fio.

6.1.8. Os equipamentos servidores e os computadores para uso individual ou coletivo, de qualquer porte, serão dotados de mecanismos de proteção contra malwares.

6.2. Da Rede Lógica:

6.2.1.1. Todos os equipamentos e dispositivos móveis conectados à rede lógica de dados do SENAC terão seus acessos monitorados por questões de segurança e para fins de auditoria.

6.2.2. A cada ponto de acesso à rede de dados do SENAC poderá ser conectado apenas um equipamento, vedada a utilização de dispositivos multiplicadores de acesso, salvo mediante expressa autorização da Coordenação de Tecnologia da Informação (CTI).

6.2.3. É proibida a conexão de qualquer dispositivo não fornecido pelo SENAC na rede cabeada da instituição, sem a prévia anuência da Coordenação de Tecnologia da Informação.

6.2.3.1. É permitida a conexão de dispositivos móveis particulares nas redes sem-fio administradas pelo SENAC.

6.2.3.2. O acesso à internet por meio das redes sem-fio observará as regras dispostas da Política para Controle de Acesso à Internet, da Política de Segurança da Informação.

6.2.3.3. Por questões de segurança tecnológica, regras específicas poderão ser implementadas no acesso à internet via rede sem-fio.

6.2.3.4. Poderão ser bloqueados os acessos à rede sem-fio, temporariamente ou por tempo indeterminado, de dispositivos móveis identificados durante o monitoramento como fonte de ações maliciosas, intencionais ou não, ou em que detectadas vulnerabilidades ou problemas de segurança tecnológica.

6.2.4. Cada unidade do SENAC terá disponível área de armazenamento em rede para salvaguardar os arquivos relacionados ao trabalho desenvolvido, com garantia de integridade, disponibilidade, controle de acesso e cópia de segurança.

6.2.4.1. Os dados armazenados nas estações de trabalho dos usuários não estão contemplados pelas garantias mencionadas nesse item, cabendo aos usuários providenciar eventual cópia de segurança e a eliminação periódica dos arquivos armazenados nos discos rígidos locais.

6.2.4.2. É proibido o armazenamento, em qualquer diretório na rede do SENAC ou nas soluções baseadas em nuvem, de arquivos não relacionados ao trabalho, tais como:

a) fotos, músicas e filmes de qualquer formato;

b) programas não homologados ou não licenciados;

c) programas de conteúdo prejudicial à segurança do parque computacional do SENAC.

6.3. Nuvem Corporativa:

6.3.1. Ao armazenamento de arquivos na nuvem corporativa aplicam-se as regras previstas no item 5.2.6.2.

6.3.2. Os arquivos armazenados na nuvem corporativa deverão ser vinculados (ter como proprietário) à caixa postal institucional da unidade, quando existente, ou outra designada pelo gestor da unidade para tal fim.

6.3.3. Nos casos de afastamentos previstos na Política para Uso de Correio Eletrônico Institucional (casos de exclusão da caixa postal), o gestor deverá solicitar ao colaborador ou estagiário, de forma antecipada, sempre que possível, a verificação da existência de arquivos que digam respeito às atividades da unidade e que permaneçam na propriedade do colaborador/estagiário, para que sejam transferidos para a caixa postal institucional da unidade ou outra designada pelo gestor.

6.3.4. Caso persistam arquivos vinculados à caixa postal institucional do colaborador/estagiário quando de sua exclusão, eles serão transferidos para a caixa postal institucional da unidade, ou outra designada pelo gestor, para triagem e definição da necessidade ou não de manutenção dos arquivos.

6.3.5. Nos casos de exclusão da caixa postal institucional de unidade ou setor, os arquivos serão transferidos para a conta da unidade designada como

nova responsável pelas atividades ou para colaborador designado para tal fim .

6.4. Equipamentos fornecidos pelo SENAC:

6.4.1. O fornecimento de equipamentos a colaboradores está condicionado às necessidades de trabalho e à assinatura do Termo de Responsabilidade e Recebimento.

6.4.2. Os computadores portáteis possuem instalação padrão desenvolvida pelo SENAC, composta por softwares e aplicativos necessários ao desempenho das funções de trabalho, além de softwares para proteção, monitoramento e auditoria do equipamento.

6.4.2.1. Os problemas de software serão solucionados pela reinstalação padrão desenvolvida pelo SENAC, que fica desobrigado de reinstalar e configurar programas que o usuário tenha instalado por iniciativa própria e isento da responsabilidade sobre eventual perda de dados.

6.4.2.2. A instalação, manutenção e suporte de qualquer software/sistema não fornecido pelo SENAC, bem como o backup de dados locais, é de exclusiva responsabilidade do usuário.

6.4.3. Em caso de falecimento, aposentadoria, demissão, dispensa da função ou término das atividades que ensejaram o fornecimento, o equipamento deve ser devolvido ao SENAC, com todos os acessórios que o acompanharam, no prazo máximo de 10 dias, se outro prazo não houver sido estipulado em norma específica.

6.4.4. Nos casos de perda, furto ou roubo do equipamento, bem como nas hipóteses de ausência de devolução ou verificação de existência de avarias no equipamento devolvido, a Coordenação de Tecnologia da Informação e informará à Diretoria Regional a situação ocorrida, com a documentação respectiva, para as providências cabíveis.

6.4.4.1. Ocorridos um dos fatos acima, a reposição, quando autorizada pela Diretoria Regional, dependerá da disponibilidade do equipamento para substituição.

6.5. Penalidades:

6.5.1. O usuário que infringir qualquer uma das diretrizes de segurança expostas neste instrumento estará passível das seguintes penalidades (sem prévio aviso):

a) Descredenciamento da senha da rede.
b) Cancelamento da caixa de e-mail
c) Desativação do ponto de rede do setor

6.5.2. O usuário infrator poderá ser notificado e a ocorrência da transgressão imediatamente comunicada ao seu chefe imediato, à Diretoria deste Regional, os quais tomarão as medidas de advertência cabíveis.

6.5.3. A Coordenação de Informática poderá valer-se da autonomia de gestora da informação para indeferir em privilégios a quaisquer usuários se houver descumprimento das diretrizes desta PSI.

7. USO DA REDE CORPORATIVA, COM E SEM FIO.

Esta política tem a finalidade de estabelecer as regras e orientar as ações e procedimentos quanto a utilização das redes sem fio ou cabeada, além de garantir a segurança e a continuidade dos serviços no SENAC-TO. As diretrizes a seguir serão seguidas pela instituição:

7.1. Direito de Uso:

7.1.1. A utilização desse recurso está disponível para fins acadêmicos como, por exemplo, pesquisa para os seguintes usuários:

a) Alunos que estão ativos e matriculados na instituição;

b) Professores e funcionários ativos na instituição;

c) Usuários autorizados pela direção da instituição;

7.2. Acesso e Funcionamento:

7.2.1. Dentro do período letivo da instituição fica aberto o cadastramento dos usuários interessados em usar os recursos da rede do SENAC.

7.3. Utilização da Rede SENAC:

7.3.1. Os usuários deverão conhecer as normas de acesso à rede e estar ciente das penalidades que poderão ocorrer caso haja violação das políticas de uso.

7.3.2. O login e senha são de total responsabilidade do usuário e intransferível, não sendo permitido o compartilhamento de informações sobre a utilização do wifi às pessoas e computadores não cadastrados;

7.3.4. Não é permitido:

7.3.4.1. Download de músicas, jogos, filmes, programas etc.;

7.3.4.2. Utilização de meios alternativos para burlar o sistema de controle de acesso à Internet da instituição;

7.3.4.3. Acesso a sites com conteúdo impróprio, pornográficos e afins;

7.3.4.4. Utilização de programas de downloads P2P, como: Limewire, Kazaa, Ares, Emule, uTorrent, biTorrent, entre outros;

7.3.4.5. Ligação de aparelhos a fim de redistribuir o acesso a terceiros;

7.3.4.6. Se fazer passar por outra pessoa ou dissimular sua identidade quando utilizar os recursos computacionais.

7.3.5. Considera-se violação das regras, os seguintes dispostos:

7.3.5.1. Divulgar sua conta de usuário e sua senha de acesso para qualquer pessoa. Estas informações são de caráter pessoal e intransferível;

7.3.5.2. Utilizar o serviço para fins ilícitos e proibidos;

7.3.5.3. Utilizar o serviço para transmitir ou divulgar material ilícito, proibido ou difamatório que viole a privacidade de terceiros, ou que seja abusivo, ameaçador, discriminatório, injurioso ou calunioso;

7.3.5.4. Acessar conteúdo pornográfico e jogos on-line;

7.3.5.5. Utilizar o serviço para transmitir/divulgar material que incentive discriminação ou violência;

7.3.5.6. Transmitir e/ou divulgar qualquer material que viole direitos de terceiros, incluindo direitos de propriedade intelectual;

7.3.5.7. Obter ou tentar obter acesso não-autorizado a outros sistemas ou redes de computadores conectados ao serviço;

7.3.5.8. Interferir ou interromper o serviço, as redes ou os servidores conectados ao serviço;

7.3.5.9. Usar de falsa identidade ou utilizar dados de terceiros para obter acesso ao serviço;

7.3.5.10. Tentar enganar ou subverter as medidas de segurança dos sistemas e da rede de comunicação;

7.3.5.11. Utilizar o serviço para intimidar, assediar, difamar ou aborrecer qualquer pessoa;

7.3.5.12. Utilizar serviço de proxy para burlar sites com acesso não autorizado;

7.3.5.13. Mostrar, armazenar ou transmitir texto, imagens ou sons que possam ser considerados ofensivos ou abusivos;

7.3.5.14. Utilizar o acesso à internet para instigar, ameaçar ou ofender, abalar a imagem, invadir a privacidade ou prejudicar outros membros da comunidade Internet;

7.3.5.15. Acessar sites pornográficos ou quaisquer outros sites que seu conteúdo não seja informativo ou educacional;

7.3.5.16. Efetuar ou tentar qualquer tipo de acesso não autorizado aos recursos computacionais do SENAC;

7.3.5.17. Violar ou tentar violar os sistemas de segurança;

7.3.5.18. Provocar interferência em serviços de outros usuários ou o seu bloqueio, provocando congestionamento da rede de dados, inserindo vírus ou tentando a apropriação indevida dos recursos computacionais do SENAC;

7.3.5.19. Desenvolver, manter, utilizar ou divulgar dispositivos que possam causar danos aos sistemas e às informações armazenadas, tais como criação e propagação de vírus e worms, criação e utilização de sistemas de criptografia que causem ou tentem causar a indisponibilidade dos serviços e/ou destruição de dados, e ainda, engajar-se em ações que possam ser caracterizadas como violação da segurança computacional;

7.3.5.20. Utilizar os recursos computacionais do SENAC para ganho indevido;

7.3.5.21. Utilizar os recursos computacionais do SENAC para intimidar, assediar, difamar ou aborrecer qualquer pessoa;

7.3.5.22. Consumir inutilmente os recursos computacionais do SENAC de forma intencional;

7.3.5.23. Fica proibido qualquer outro dispositivo afim de rotear ou compartilhar o link sem a homologação do setor de TI deste regional;

7.3.5.24. Desenvolver qualquer outra atividade que desobedeça às normas apresentadas acima;

7.4. Penalidades:

7.4.1. O usuário é responsável por qualquer atividade a partir de sua conta (login) e também por seus atos no uso dos recursos computacionais oferecidos. Assim, o mesmo responderá por qualquer ação judicial e administrativa apresentada à instituição e que o envolva.

7.4.2. Em caso de descumprimento das regras, o usuário estará sujeito ao infrator as penalidades apresentadas a seguir:

a) 1º infração: imediata suspensão do acesso por 7 dias;

b) 2ª infração: suspensão do acesso por período de 30 dias;

c) 3ª infração: suspensão permanente do uso da rede;

7.4.3. Os registros de reincidência serão armazenados enquanto perdurar o vínculo ou contrato do usuário para com o SENAC.

7.4.4. Caso alguma violação de regra seja identificada, através do sistema de monitoramento, o usuário será bloqueado e notificado pelo telefone ou e-mail.

7.5. Considerações:

7.5.1. Caso o usuário perceba o uso indevido de sua senha de acesso por terceiros, não conseguir alterar sua senha de acesso ou a mesma encontra-se bloqueada, informar ao centro de informática;

7.5.2. O login de acesso aos recursos da rede só terá validade enquanto perdurar o vínculo do colaborar, prestador de serviço ou do aluno com a instituição;

7.5.3. O uso da internet estará vinculado à conta de acesso (login e senha) do usuário na instituição. Caso constem outros acessos e estes forem indevidos, os usuários serão notificados e as punições serão aplicadas ao infrator;

7.5.4. A instituição se reserva no direito de suspender o acesso do equipamento que estiver consumindo excessivamente o link de internet devido à existência de programas maliciosos nos equipamentos autorizados, tais como: vírus, spyware, worms, entre outros.

7.5.5. Equipamentos de propriedade do colaborador ou aluno, como: notebook, Smartphone e outros, os sistemas de proteção como, antivírus, firewall, anti-spyware são de sua exclusiva responsabilidade do proprietário. Em nenhum caso a instituição se responsabilizará por qualquer dano e/ou prejuízo que o usuário possa sofrer ao utilizar o serviço.

7.5.6. Equipamentos proprietários, configuração do equipamento será de responsabilidade do usuário. Não sendo de responsabilidade do setor de TI qualquer configuração no aparelho.

7.5.7. A instituição se reserva o direito de cancelar o serviço de acesso as redes wifi sem prévio aviso.

8. MESA LIMPA E TELA LIMPA

A política conhecida como “mesa limpa e tela limpa” são práticas recomendadas de Segurança da Informação (SI) para o ambiente de trabalho a fim de se evitar a exposição desnecessária de informações consideradas sensíveis, evitando assim o comprometimento da informação.

Visando reduzir riscos de acesso não autorizado, perdas ou danos às informações fora e durante o horário de expediente, o SENAC adotará a política de mesas limpas para os papéis e mídias de armazenamento removível. Outrossim, adotará uma política de telas limpas, para computadores e similares.

Nenhuma informação confidencial ou sensível deverá ser deixada à vista de pessoas indevidas, seja em papel ou em quaisquer dispositivos, sejam estes eletrônicos ou não. Informações deixadas sobre mesas, monitores ou outros mobiliários são passíveis de serem destruídas, danificadas ou furtadas. Sendo assim, a aplicação dessa política será em definir diretrizes e procedimentos que reduzam o risco de violações de segurança, fraudes ou furto de informações importantes ocasionadas pela exposição inadequada de documentos no ambiente de trabalho.

8.1. Diretrizes:

8.1.1. Documentos impressos, relatórios, mídias eletrônicas (pendrives, CD´s, DVD´s, HD´s, cartões de memória, etc) e publicações diversas, deverão ser armazenados em móveis trancados e/ou em outras espécies de mobiliário de segurança, quando não estiverem em utilização, principalmente fora do expediente de trabalho.

8.1.2. Na ausência do colaborador no local de trabalho, computadores, impressoras ou demais terminais de computação não deverão ser deixados logados/autenticados/registrados, devendo serem protegidos por keylocks, senhas ou outros controles de segurança quando não estiverem em utilização.

8.1.3. Equipamentos de impressão/fotocópia deverão ser protegidos de acesso/uso não autorizado, fora ou durante o horário normal de trabalho.

8.1.4. Documentos impressos, quando sensíveis ou confidenciais, deverão ser retirados das impressoras imediatamente.

8.1.5. Caso o colaborador ausente-se do trabalho por longo período de tempo, deverá limpar a mesa de trabalho, retirando papéis, livros e/ou qualquer informação.

8.1.6. As informações relativas ao SENAC em poder do colaborador são de responsabilidade do mesmo.

8.1.7. O colaborador deverá evitar manter em sua mesa, papéis, impressos, recados, anotações ou lembretes, fora do expediente de trabalho (política de mesa limpa).

8.1.8. Descarte os itens referentes a informações de clientes internos, externos, alunos ou de propriedade da empresa, em locais seguros.

9. RECURSOS DE IMPRESSÃO E DIGITALIZAÇÃO.

O SENAC Tocantins tem o compromisso institucional de promover a governança de serviços de TIC e isto inclui os serviços de impressão e digitalização.

A adoção de uma norma de utilização de tais serviços, justifica-se: pelo intuito de se promover o uso racional do recurso, reduzindo custos e o impacto ambiental decorrente da produção e descarte dos insumos; pela busca em se regular o uso dos serviços de acordo com a legislação vigente e aplicável; em reunir a documentar práticas adotadas na instituição e, por fim, esclarecer aos usuários, direitos e responsabilidades no uso de impressões e digitalizações.

9.1. Diretrizes:

9.1.1. O serviço de Impressão/Digitalização destina-se exclusivamente a atividades de cunho institucional;

9.1.2. A sustentabilidade ambiental é elemento chave na utilização do serviço – a impressão de documentos deve ser evitada sempre que for possível;

9.1.3. Deve-se buscar a tramitação de processos administrativos sempre na forma eletrônica, fazendo uso da impressão apenas nos casos onde se requer assinatura ou carimbos impressos;

9.1.4. Após imprimir em uma determinada central de impressão, faz-se obrigatória a verificação e a busca dos impressos, com o intuito de evitar o acúmulo de documentos em bandejas.

9.1.5. Em caso de falhas de impressão, deve ser verificada a possibilidade de reaproveitamento de papel.

9.1.6. É proibido deixar impressões erradas na bandeja das impressoras.

9.1.7. Para evitar que futuros pedidos de impressão sejam prejudicados, é aconselhável o reabastecimento de papéis em qualquer impressora que esteja utilizando;

9.1.8. É importante que sejam tomadas medidas de economia de toners, cartuchos e afins;

9.1.9. As impressoras são alocadas nos centros de custo conforme demandas apresentadas;

9.1.10. É de responsabilidade dos centros de custo a alocação racional deste recurso, reduzindo custos pelo compartilhamento de equipamentos;

9.1.11. Toda impressão realizada através do serviço é associada a um único usuário;

9.1.12. Informações sobre o número de páginas e título dos documentos, assim como data e hora da impressão, são registradas e mantidas por tempo indeterminado;

9.1.13. Os centros de custo são responsáveis por indicar um responsável pelo acompanhamento do serviço em sua unidade;

9.1.14. Os custos associados ao serviço serão repassados aos respectivos centros de custos.

9.1.15. O serviço de Impressão e Digitalização é provido em nível departamental – ele é composto por ilhas de impressão e digitalização para uso departamental, visando racionalizar recursos de energia elétrica, espaço físico, consumo de papel, gestão de suprimentos, administração e gerência;

9.1.16. As unidades contempladas recebem equipamentos que são contratados na forma de serviço e incluem manutenção de defeitos, fornecimento de toner e outros suprimentos, descarte e reciclagem de partes e peças substituídas. Somente o papel deve ser fornecido pela unidade usuária do serviço;

9.1.17. A manutenção do serviço opera de modo proativo, substituindo insumos antes que gerem parada do serviço (por exemplo, troca de toner);

10. USO DAS ESTAÇÕES DE TRABALHO.

A orientação tratada neste item é direcionada ao uso de quaisquer equipamentos de informática, tais como desktops, notebooks, impressoras, escâners, dentre outros, que estão inseridos no ambiente de trabalho dos colaboradores do SENAC, que possuam patrimônio pertencente à instituição e que foram devidamente instalados e configurados pelos técnicos da Coordenação de Tecnologia da Informação (CTI).

Objetiva-se com essa norma reduzir riscos de danos materiais à estrutura tecnológica do SENAC, bem como da integridade das informações armazenadas nos equipamentos de informática, através da boa utilização das estações de trabalho.

10.1. Diretrizes:

10.1.1. Não se deverá ligar na mesma tomada do computador, outros equipamentos, tais como impressoras, escâner, aparelhos celulares e demais dispositivos, evitando assim a utilização de extensões ou conectores do tipo “benjamim”. Assim, pretende-se evitar que haja sobrecarga elétrica que poderá ocasionar em danos aos equipamentos conectados ou mesmo um princípio de incêndio.

10.1.2. Ao se perceber alterações na rede elétrica, deve-se salvar os documentos em aberto no computador e por medida de segurança, desligar os equipamentos por um período, até que se tenha normalização do fornecimento da energia elétrica. As principais características de alterações na rede elétrica são: lâmpadas piscando ou com fraca luminosidade; constantes bips dos equipamentos como nobreaks e estabilizadores, várias interrupções no fornecimento de energia por um curto período de tempo.

10.1.3. Havendo necessidade de o colaborador ausentar-se do local de trabalho, recomenda-se desligar o monitor para economia de energia.

10.1.4. Ao se ligar impressoras ou o escâner, deve-se aguardar o tempo necessário para que o sistema interno desses dispositivos seja carregado (em média 3 minutos).

10.1.5. Evitar abastecer as impressoras com a quantidade além do máximo de papéis permitidas pela bandeja. Assim, evitar-se-á problema na tração das roletas que acarretam em atolamento de papel e/ou outros defeitos físicos no equipamento.

10.1.6. Quando ocorrer atolamento de folhas dentro da impressora, primeiramente deverá ser cancelado o processo de impressão e só após o desligamento do equipamento da rede elétrica, efetuar a retirada do papel entulhado. Caso a remoção exija a necessidade de aplicação de “força”, solicite a presença de um técnico da Coordenação de Tecnologia da

Informação (CTI) para que este remova as folhas. A remoção descuidada do papel entulhado poderá causar desalinhamento das peças internas da impressora e até avarias.

10.1.7. Evite a troca dos tonners/cartuchos com ações bruscas ou descuidadas, pois uma má utilização poderá ocorrer derramamento do pó ou tinta de impressão, ocasionando acúmulo de sujeira dentro e fora do equipamento.

10.1.8. As impressoras em geral, possuem tempo mínimo de carregamento de dados a serem impressos. Somente após esse procedimento realizado, que a impressão será concluída. Orienta-se que o usuário, após enviar o arquivo para impressão, aguarde a finalização o processo, não havendo, portanto, a necessidade de se reenviar outras vezes o documento para impressão até que seja concluído. Havendo demora na impressão ou a não impressão do documento desejado, o colaborador deverá acionar o suporte técnico em TI para resolução do incidente.

10.1.9. Evitar deixar os cabos que conectam a impressora, escâner ou o computador, esticados ou mal encaixados.

10.1.10. Prezar pela limpeza do computador, evitando acúmulo de poeira e umidade.

10.1.11. Não conectar ou desconectar nenhum cabo com o computador ligado, com exceção aos cabos USB.

10.1.12. Não bata, empurre ou mude de lugar o computador com ele em funcionamento, pois poderá causar avarias ao hardware do equipamento.

10.1.13. Não colocar outros equipamentos, itens ou material pesado em cima de monitores ou dos gabinetes.

10.1.14. Não colocar o aparelho de telefone em cima do gabinete do computador.

10.1.15. Não consumir alimentos ou bebidas próximo à sua estação e trabalho.

10.1.16. Mantenha o gabinete e o local onde o computador está instalado, sempre muito bem arejado.

10.1.17. Não desligar e ligar o computador por diversas vezes consecutivas. Tal atitude poderá danificar algum componente interno ou acarretar em perdas de informações armazenadas no equipamento.

11. UTILIZAÇÃO DA INTERNET. INTRANET E EXTRANET

A Internet é, indiscutivelmente, uma das mais poderosas ferramentas de trabalho da atualidade. Entretanto, é preciso definir o que é ou não permitido no que tange à utilização desta ferramenta em ambiente comercial, bem como à utilização da intranet e extranet.

Faz-se necessário, portanto, a instituição de uma política para o correto direcionamento e dimensionamento de recursos tecnológicos para prover o serviço de acesso à internet/intranet/extranet pelo SENAC Tocantins, conforme orientações a seguir:

11.1. Diretrizes:

11.1.1. O acesso à internet dar-se-á, exclusivamente, pelos meios autorizados, configurados pela Coordenação de Tecnologia da Informação (CTI) do SENAC.

11.1.2. É expressamente proibido o uso de proxies externos ou similares.

11.1.3. O acesso à internet é disponibilizado pelo SENAC para uso nas atividades relacionadas ao trabalho, observado o disposto nesta norma.

11.1.4. O SENAC permite o uso da Internet para fins particulares dos usuários da rede, desde que este uso não exceda os limites da ética, do bom senso e da razoabilidade.

11.1.5. Para se ter acesso à rede corporativa, o usuário deverá autenticar-se através de login e senha.

11.1.6. Constitui acesso indevido à internet quaisquer das seguintes ações:

11.1.7. Acessar páginas de conteúdo considerado ofensivo, ilegal, impróprio ou incompatível com as atividades funcionais ou com a política de segurança da informação, tais como pornografia, pedofilia, racismo, jogos e páginas de distribuição e de compartilhamento de software.

11.1.8. Utilizar programas de troca de mensagens em tempo real (bate-papo) ou programas para troca de conteúdo via rede ponto-a-ponto (peer-to-peer), exceto os autorizados pela Coordenação de Tecnologia da Informação (CTI).

11.1.9. Utilizar programas e/ou acessar páginas de áudio e vídeo em tempo real, ou sob demanda, exceto autorizados pela Coordenação de Tecnologia da Informação

11.1.10. Acessar sites que representem ameaça de segurança ou que possam comprometer de alguma forma a integridade da rede de computadores do SENAC.

11.1.11. Acessar ou fazer download de arquivos não relacionados ao trabalho, em especial músicas, imagens, vídeos, jogos e programas de qualquer tipo.

11.1.12. Todo tráfego de internet será controlado e inspecionado, de forma automática, pela ferramenta de proxy (filtro de conteúdo), configurada de

acordo com os limites estabelecidos por esta norma ou definidos pela Coordenação de Tecnologia da Informação (CTI).

11.1.13. A liberação de acesso a sites e serviços bloqueados, mas necessários ao desempenho das atribuições funcionais do usuário, dependerá de solicitação, devidamente justificada, à Coordenação de Tecnologia da Informação.

11.1.14. Cabe ao gestor da unidade operativa orientar os usuários sob sua responsabilidade a respeito do uso adequado do recurso de internet, conforme as regras estabelecidas nesta norma, bem como reportar à Coordenação de Tecnologia da Informação (CTI) o seu descumprimento.

11.1.15. É atribuição exclusiva da área de TI homologar os softwares definidos como viáveis e seguros para o uso da Internet (ex.: como browser, softwares de mensageria, aqueles que necessitam de conexão com a internet, etc);

11.1.16. A critério da Administração, poderão ser adotadas medidas visando a manutenção da disponibilidade e da qualidade do acesso à internet, seja em situações normais de funcionamento, seja em situações de contingência, tais como:

11.1.17. Bloqueios totais ou parciais e/ou priorização de acessos a determinados sites e serviços; e

11.1.18. Limitação de banda de tráfego de dados.

11.1.19. As medidas identificadas no item anterior, quando implementadas, serão comunicadas aos colaboradores do SENAC, a fim de possibilitar o repasse de informações aos usuários interessados.

11.1.20. O acesso à internet pelo usuário da rede corporativa será obrigatoriamente cancelado em caso de desligamento do SENAC.

11.2. Monitoramento e Auditorias.

11.2.1. Por motivos de segurança, todo acesso à internet será monitorado, e os registros serão mantidos pela Coordenação de Tecnologia da Informação (CTI).

11.2.2. Em caso de indícios de descumprimento das diretrizes previstas nesta norma, a chefia imediata ou superior solicitará, justificadamente, à Coordenação de Tecnologia da Informação a realização de auditoria extraordinária.

12. ACESSO REMOTO.

O ambiente tecnológico do SENAC é passível de ter seus recursos computacionais acessados remotamente. Através desta norma, define-se os requisitos e regras de segurança para uso do acesso remoto no ambiente interno da instituição, realizados pelos técnicos da Coordenação de Tecnologia da Informação (CTI), conforme segue:

12.1. Diretrizes:

12.1.1. O acesso remoto de uma rede externa às estações de trabalho e servidores do SENAC deverá ser rigorosamente controlado, autorizado, utilizando criptografia por uma VPN e autenticação com senha forte.

12.1.2. As solicitações de acesso remoto aos usuários devem ser realizadas através de chamado ao suporte técnico e formalizada através de formulário específico, com justificativa e período de trabalho. Essas solicitações devem ser autorizadas pelo gestor da área ou superior e arquivado para fins de auditoria.

12.1.3. A disponibilização de acesso remoto deve ser autorizada pelo gestor da área ou supervisor em conformidade com o perfil funcional, priorizando o acesso em expediente regulamentar de trabalho, salvo em casos de exceção devidamente justificado.

12.1.4. O usuário com acesso remoto autorizado, acessará os mesmos ambientes que visualiza internamente, ou seja, terá o mesmo perfil de acesso.

12.1.5. Os usuários autorizados ao acesso remoto, devem proteger suas credenciais e em nenhum momento devem disponibilizar seu login e senha da rede, email, VPN, ou quaisquer informações de acesso, para outra pessoa.

12.1.6. Os usuários com acesso remoto devem garantir a não utilização de ser perfil de acesso remoto a outras pessoas.

12.1.7. Recomenda-se que o usuário com autorização e acesso remoto utilize redes externas seguras, para acessar o ambiente tecnológico do SENAC.

12.1.8. Os usuários que acessam a rede remotamente, devem estar atentos para que usa estação de trabalho, notebook, etc, não esteja também acessando outra rede ao mesmo tempo.

12.1.9. O usuário, quando da utilização do acesso remoto, deverá permanecer conectado apenas à rede do SENAC, quando estiver efetivamente usando os serviços disponibilizados, devendo desconectar-se nas interrupções e términos de trabalho.

12.1.10. Os usuários com acesso remoto devem cuidar para que as informações sigilosas não sejam capturadas por terceiros que estejam próximos ao equipamento.

13. USO DE DISPOSITIVOS MÓVEIS.

A utilização de dispositivos móveis como smartphones, notebooks, tablets, etc, está cada vez mais difundida dentro das organizações, seja para proporcionar mobilidade para as atividades de trabalho ou para otimizar a iteração entre os usuários. Aliando-se nessas premissas, o SENAC Tocantins deseja facilitar a mobilidade e o fluxo de informações entre seus colaboradores. Para isto, permite que seus funcionários utilizem dispositivos móveis.

Um documento de política para dispositivos móveis deverá informar aos funcionários o que se esperar deles quando se tratar da utilização de smartphones, tablets e outros wearables no ambiente de trabalho, bem como esclarecer as responsabilidades da empresa sobre esse assunto.

Essa política possui múltiplos propósitos, sendo de maior importância os seguintes:

- Proteção de dados e ativos corporativos;
- Permitir produtividade, acessibilidade e a colaboração de forma segura e disponível, fora ou dentro da empresa;

13.1. Diretrizes:

13.1.1. Esta norma visa estabelecer critérios de manuseio, prevenção e responsabilidade sobre o uso de dispositivos móveis e deverá ser aplicada a todos os colaboradores que utilizem tais equipamentos.

13.1.2. O Senac Tocantins, na qualidade de proprietário dos equipamentos fornecidos, reserva-se o direito de inspecioná-los a qualquer tempo, caso seja necessário realizar uma manutenção de segurança.

13.1.3. O colaborador, portanto, assume o compromisso de não utilizar, revelar ou divulgar a terceiros, de modo algum, direta ou indiretamente, em proveito próprio ou de terceiros, qualquer informação, confidencial ou não, que tenha ou venha a ter conhecimento em razão de suas funções no Senac Tocantins, mesmo depois de terminado o vínculo contratual mantido com a instituição.

13.1.4. Todo colaborador deverá realizar periodicamente cópia de segurança (backup) dos dados de seu dispositivo móvel. Deverá, também, manter estes backups separados de seu dispositivo móvel, ou seja, não os carregar juntos.

13.1.5. O suporte técnico aos dispositivos móveis de propriedade do Senac Tocantins e aos seus usuários deverá seguir o mesmo fluxo de suporte contratado pela instituição.

13.1.6. Todo colaborador deverá utilizar senhas de bloqueio automático para seu dispositivo móvel.

13.1.7. Não será permitida, em nenhuma hipótese, a alteração da configuração dos sistemas operacionais dos equipamentos, em especial os referentes à segurança e à geração de logs, sem a devida comunicação e a autorização da área responsável e sem a condução, auxílio ou presença de um técnico da Coordenação de Tecnologia da Informação.

13.1.8. O colaborador deverá responsabilizar-se em não manter ou utilizar quaisquer programas e/ou aplicativos que não tenham sido instalados ou autorizados por um técnico da Coordenação de Tecnologia da Informação (CTI) do SENAC Tocantins.

13.1.9. A reprodução não autorizada dos softwares instalados nos dispositivos móveis fornecidos pela instituição constituirá uso indevido do equipamento e infração legal aos direitos autorais do fabricante.

13.1.10. É permitido o uso de rede banda larga de locais conhecidos pelo colaborador como: sua casa, hotéis, fornecedores e clientes.

13.1.11. É responsabilidade do colaborador, no caso de furto ou roubo de um dispositivo móvel fornecido pelo SENAC, notificar imediatamente seu gestor direto e a Coordenação de TI. Também deverá procurar ajuda das autoridades policiais, registrando, assim que possível, um boletim de ocorrência (BO).

13.1.12. O colaborador deverá estar ciente de que o uso indevido do dispositivo móvel caracterizará a assunção de todos os riscos da sua má utilização, sendo o único responsável por quaisquer danos, diretos ou indiretos, presentes ou futuros, que venha causar ao Senac Tocantins e/ou a terceiros.

13.1.13. O colaborador que deseje utilizar equipamentos portáteis particulares ou adquirir acessórios e posteriormente conectá-los à rede do Senac deverá submeter previamente tais equipamentos ao processo de autorização da Coordenação de Tecnologia da Informação (CTI).

13.1.14. Equipamentos portáteis, como smartphones, palmtops, pen drives e players de qualquer espécie, quando não fornecidos ao colaborador pela instituição, não serão validados para uso e conexão em sua rede corporativa.

13.1.15. Monitoramento e Auditorias.

13.1.15.1. Por motivos de segurança, todo acesso à internet será monitorado, e os registros serão mantidos pela Coordenação de Tecnologia da Informação (CTI).

13.1.15.2. Em caso de indícios de descumprimento das diretrizes previstas nesta norma, a chefia imediata ou superior solicitará, justificadamente, à Coordenação de Tecnologia da Informação (CTI), a realização de auditoria extraordinária.

13.1.15.3. Os relatórios decorrentes das auditorias ordinárias e extraordinárias realizadas pela Coordenação de TI serão encaminhados para a Diretoria Regional para os devidos fins.

14. ACESSO AOS AMBIENTES FÍSICOS COMPUTACIONAIS (DATACENTER)

Esta norma estabelece diretrizes e padrões para a implementação da política de acesso aos ambientes físicos computacionais do SENAC, alinhando-se às melhores práticas relacionadas ao tema, conforme é descrito a seguir:

Diretrizes:

14.1. O acesso de visitantes ou terceiros somente será realizado com acompanhamento de colaborador autorizado pela Coordenação de Tecnologia da Informação (CTI).

14.2. Deverão existir duas cópias de chaves da porta do Datacenter. Uma delas, ficará sob posse do Coordenador de Tecnologia da Informação (CTI) e a outra de posse do Analista de TI ou gestor de Segurança da Informação.

14.3. O Datacenter deverá ser mantido limpo e organizado. Qualquer procedimento que gere lixo ou sujeira nesse ambiente somente poderá ser realizado com a colaboração do Departamento de Serviços Gerais.

14.4. Não é permitida a entrada de nenhum tipo de alimento, bebida, produto fumígeno ou inflamável.

14.5. A entrada ou retirada de quaisquer equipamentos do Datacenter somente se dará com o preenchimento da solicitação de liberação pelo colaborador solicitante e a autorização formal desse instrumento pela Coordenação de Tecnologia da Informação (CTI).

15. PLANO DE CONTINGÊNCIA.

O plano de contingência é um conjunto de diretrizes prévias e decisões que devem ser tomadas visando reduzir o impacto negativo que pode ser causado pelo advento de situação desastrosa. Esse documento contém todos os procedimentos que devem ser realizados em objetivo de mitigar o tempo de suspensão forçada dos serviços e, consequentemente, evitar que mais danos sejam causados em razão do incidente.

O plano de contingência de TI do SENAC foi elaborado com base na análise dos riscos pelos quais a instituição está sujeita, considerando os recursos disponíveis para a definição de melhores maneiras de lidar com possíveis problemas como falhas técnicas, invasões, falta de energia e outras situações.

Para fins de consulta, o SENAC publicará em anexo ao PSI o seu atual plano de contingência.

16. CÓPIA DE SEGURANÇA (BACKUP).

No ambiente de Tecnologia da Informação, o backup e a proteção dos dados são utilizados para prover continuidade de negócios, replicação e dados, recuperação de desastre e mitigação nos custos de infraestrutura tecnológica. Porém, a melhor maneira para assegurar os dados, seja local ou remotamente, pode ser um desafio desanimador, se não forem estabelecidas normas estratégias para esta finalidade.

Visando proteger suas informações e buscando atenderem a padrões de segurança e regulamentações, as organizações estabelecem um conjunto de políticas de SI. Mesmo estabelecendo políticas de segurança, as organizações não estão livres de erros humanos, ataques virtuais, catástrofes naturais e outras ameaças. E caso ocorram perdas de informações, é preciso recuperá-las, e isto se torna possível se o processo de backup e restauração de dados for seguro.

Neste item serão tratados detalhes quanto à política implantada de backup e restauração de arquivos digitais armazenados no parque tecnológico do SENAC Tocantins.

16.1. Estratégia (5W2H)

	Objetivo	**Definir uma política de backup**
Passo		**Detalhes**
1	What - O que faremos?	Cópia de segurança dos: arquivos, servidores físicos e virtuais, bancos de dados;
2	Why - Por que fazer?	Garantir a restauração das informações com eficiência;
3	Where - Onde faremos?	Em Disco Rígido;

4	Who - Quem fará?	Departamento de tecnologia da informação;
5	When - Quando faremos?	1 copia por dia mantida por 30 dias, 1 copia por mês mantida por 12 meses;
6	How - Como faremos?	Automaticamente por meio de Software de backup;
7	How much - Quanto vai custar?	R$ 0.00

16.2. Especificações:

Os donos dos dados deverão ter ciência dos tempos de retenção aqui estabelecidos para cada tipo de informação e os administradores / operadores de backup deverão zelar pelo cumprimento das diretrizes aqui estabelecidas.

O serviço de backup deve ser orientado para a restauração das informações no menor tempo possível, principalmente havendo indisponibilidade de serviços que dependam da operação de restore.

16.3. Orientações gerais:

16.3.1. Testes periódicos de restauração;
16.3.2. Evitar execução em horário de produção (horário comercial);
16.3.3. As mídias deverão ser armazenadas em cofre corta-fogo;
16.3.4. As solicitações de restauração de arquivos deverão ser abertas formalmente.

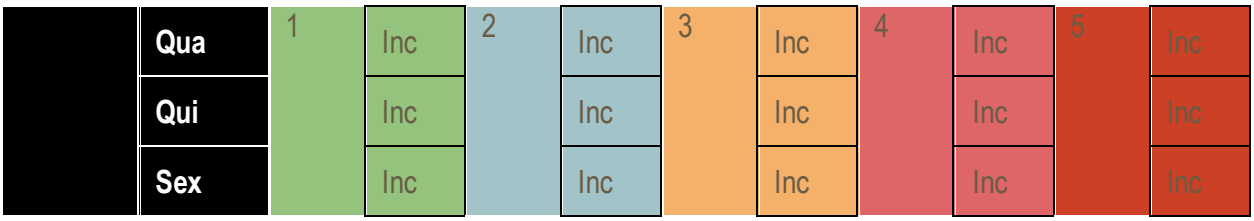
16.4. Orientações específicas:

16.4.1. Realizar cópias de segurança completas (full) nos backups mensais;
16.4.2. Realizar cópias de segurança completas e incrementais nos backups diários;
16.4.3. Planejamento do backup:

Planejamento do backup

Mensal	Mês	Jan	Fev	Mar	Abr	Mai	Jun	Jul	Ago	Set	Out	Nov	Dez
		6	7	8	9	10	11	12	13	14	15	16	17

		Semana 1		Semana 2		Semana 3		Semana 4		Semana 5	
	Dia	Disco	Tipo	Disco	Tipo	Disco	Tipo	Disco	Tipo	Disco	Tipo
Diário	Dom		Full		Full		Full		Full		Full
	Seg		Inc		Inc		Inc		Inc		Inc
	Ter		Inc		Inc		Inc		Inc		Inc



17. CONTROLE DE ACESSO E USO DE CHAVES E SENHAS.

17.1. Do controle e gerenciamento de acesso:

17.1.1. O acesso à rede, serviços e aos sistemas computacionais disponibilizados pelo SENAC serão solicitados à Coordenação de Tecnologia da Informação (CTI), por meio do sistema de atendimento, em que definidos os níveis de acesso adequados às atividades desenvolvidas.

17.1.2. Incumbe à chefia imediata solicitar à Coordenação de Tecnologia da Informação (CTI):

a) os acessos necessários ao desenvolvimento das atividades dos colaboradores e estagiários vinculados a sua unidade/setor.

b) a alteração dos níveis de acesso ou a remoção do acesso a sistemas concedidos a colaboradores ou estagiário da unidade, sempre que necessária sua adequação às atividades desenvolvidas.

c) a remoção dos acessos concedidos ao colaborador ou estagiário, imediatamente após o afastamento ou desligamento da unidade.

I) Não solicitada a alteração ou exclusão no momento oportuno, a chefia poderá ser responsabilizada pelo acesso indevido do colaborador/estagiário a informações da unidade/setor.

17.1.3. A Coordenação de Tecnologia da Informação (CTI) comunicará à unidade/setor respectiva (o) sobre a efetivação do cadastro, fornecendo as informações necessárias ao acesso, e encaminhará a Política de Segurança da Informação, em formato eletrônico, para a caixa postal institucional pessoal do usuário, para ciência.

17.1.4. As novas senhas solicitadas serão fornecidas por meio de comunicação eletrônica para a caixa postal institucional da unidade ou caixa postal institucional pessoal do usuário, proibido o fornecimento de senhas por qualquer outro meio, inclusive telefone.

17.1.5. É responsabilidade do usuário a alteração da senha inicial fornecida pela Coordenação de Tecnologia da Informação (CTI) no primeiro acesso realizado.

17.1.6. O Departamento Pessoal comunicará à Coordenação de Tecnologia da Informação os casos de falecimento, demissão, aposentadoria, ou término de vínculo de estágio de estudantes ou demais contratados em geral, para remoção dos acessos concedidos aos usuários.

17.1.7. Nos casos em que autorizada a prestação de trabalho remoto, o Departamento Pessoal comunicará à Coordenação de Tecnologia da Informação (CTI) o término das atividades que o ensejaram, para retirada dos acessos necessários ao trabalho à distância.

17.1.8. O privilégio de administrador na estação de trabalho é restrito aos membros da equipe técnica da Coordenação de Tecnologia da Informação (CTI) (ou a quem a Coordenação delegar), que necessitem de acesso privilegiado para o desempenho das atividades funcionais.

17.1.9. Os acessos privilegiados aos sistemas e serviços de TIC serão concedidos aos membros da equipe técnica da Coordenação de Tecnologia da Informação (CTI), sempre que necessários ao desempenho das atividades funcionais, de modo a permitir a gestão e configuração do ambiente tecnológico.

I) É responsabilidade da chefia imediata solicitar a concessão, a alteração e a remoção dos acessos privilegiados dos seus subordinados.

II) Os acessos concedidos deverão ser revisados pelo menos uma vez ao ano.

17.1.10. Nos computadores portáteis disponibilizados pelo SENAC, os colaboradores destinatários dos equipamentos terão privilégio de administrador.

17.1.11. As solicitações de acessos de prestadores de serviço aos recursos tecnológicos do SENAC terão caráter temporário e deverão ser acompanhadas da respectiva justificativa, bem como do prazo previsto para a realização das atividades.

I) No caso do prestador de serviço necessitar de acesso privilegiado, as regras observarão o disposto no item 17.1.11.

17.2. Da conta da rede e respectiva senha para utilização.

17.2.1. Para ter acesso aos recursos de tecnologia da informação disponibilizados pelo SENAC é necessário que o usuário possua uma conta de rede.

17.2.2. A identificação de usuário será composta pelo seu prenome, adicionado pela primeira letra de dois de seus sobrenomes. Ex: José da Silva Sousa, a identificação ficará "josess".

17.2.3. Em situações justificadas, poderá ser utilizado outro prenome ou sobrenome para a composição da identificação.

17.2.4. A cada conta de acesso será associada uma senha, de uso pessoal e intransferível.

17.2.5. Na utilização das credenciais de acesso, compete ao usuário observar os procedimentos a seguir indicados, bem como adotar outras medidas de segurança de caráter pessoal, com vista a impedir o uso não autorizado dos recursos de tecnologia da informação a partir de sua conta de acesso:

I) não compartilhar a senha com outras pessoas;

II) não armazenar senhas em local acessível por terceiros;

III) não utilizar senhas de fácil dedução como as que contém nomes próprios e de familiares, datas festivas e sequências numéricas;

IV) ao ausentar-se de sua estação de trabalho, ainda que temporariamente, o usuário deverá encerrar ou bloquear a sessão;

17.2.6. A senha deverá satisfazer os seguintes requisitos de complexidade:

i) não conter nome da conta do usuário (login) ou mais de dois caracteres consecutivos de partes de seu nome completo;

ii) ter pelo menos seis caracteres;

iii) conter caracteres de, no mínimo, três das quatro categorias a seguir:

a) caracteres maiúsculos (A-Z);

b) caracteres minúsculos (a-z);

c) dígitos de base (0 a 9);

d) caracteres não alfabéticos (como !, $, #, %).

17.2.6.1. Excetuam-se da regra do item 6.2.7 os sistemas atualmente disponibilizados que não permitam o atendimento aos requisitos estabelecidos.

17.2.7. A senha deverá ser alterada com uma periodicidade mínima de 1 (um) dia e máxima de 180 (cento e oitenta) dias desde a última modificação.

17.2.8. A conta do usuário será bloqueada após 03 (três) tentativas consecutivas de acesso não reconhecidas, considerando também as tentativas inválidas de acesso à rede sem-fio.

17.2.9. Em caso de suspeita de comprometimento da senha ou de outro recurso de autenticação, o usuário comunicará imediatamente à Coordenação Tecnologia da Informação, que poderá, como medida preventiva, suspender temporariamente o acesso.

17.3. Registros (logs) de eventos:

17.3.1. Serão mantidos, por um período mínimo de doze (12) meses, os registros dos acessos dos usuários e dos acessos privilegiados aos recursos tecnológicos disponibilizados pelo SENAC, inclusive para fins de apuração e comprovação de incidentes de segurança.

17.3.2. Serão registrados os seguintes dados:

17.3.2.1.1.1. identificação de usuário de quem efetuou o acesso;

17.3.2.1.1.2. data e hora de entrada e saída do sistema;

17.3.2.1.1.3. origem do acesso;

17.3.2.1.1.4. erros ou falhas de conexão e acesso;

17.3.2.1.1.5. troca de senhas de Serviços de Infraestrutura de TI;

17.3.2.1.1.6. outras informações que venham a ser necessárias para os controles de segurança.

18. ATUALIZAÇÃO DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO.

O disposto na presente Política de Segurança da Informação será atualizado sempre que alterados os procedimentos das normativas estabelecidas nesse documento, observada, ainda, a periodicidade prevista para a revisão da Política de Segurança da Informação.

A revisão da PSI ocorrerá anualmente, advinda de análise realizado pelos técnicos da Coordenação de Tecnologia da Informação e/ou por solicitação do Comitê Gestor de Tecnologia da Informação (CGTO) do Departamento Regional do Tocantins.

19. REFERÊNCIAS NORMATIVAS:

- Norma Técnica ABNT NBR ISO/IEC 27001:2013, que especifica os requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão da segurança da informação dentro do contexto da organização.
- Norma Técnica ABNT NBR ISO/IEC 27002:2013, que fornece diretrizes para práticas de gestão de segurança da informação.
- Decreto nº 3.505, de 13 de junho de 2000, que institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal.
- Norma Complementar nº 01 IN01/DSIC/GSI/PR, de 30 de junho de 2009, que estabelece critérios e procedimentos para elaboração, atualização, alteração, aprovação e publicação de normas complementares sobre Gestão de Segurança da Informação e Comunicações.
- Norma Complementar nº 15/IN01/CSIC/GSIPR, que estabelece diretrizes de Segurança da Informação e Comunicações para o uso de redes sociais, nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta.
- Instrução Normativa GSI/PR nº 1, de 13.06.2008, do Gabinete de Segurança Institucional da Presidência da República, que disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, e dá outras providências.
- Norma Complementar nº 01/IN01/DSIC/GSIPR, de 15.10.2008, do Departamento de Segurança da Informação e Comunicações da Presidência da República, que estabelece critérios e procedimentos para elaboração, atualização, alteração, aprovação e publicação de normas complementares sobre Gestão de Segurança da Informação e Comunicações, no âmbito da Administração Pública Federal, direta e indireta.
- Norma Complementar nº 07/IN01/DSIC/GSIPR (Revisão 01), de 15.07.2014, do Departamento de Segurança da Informação e Comunicações da Presidência da República, que estabelece diretrizes para a implementação de controles de acesso à Segurança da Informação e Comunicações, nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta.
- Norma Complementar 10/IN01/DSIC/GSIPR, de 30 de janeiro de 2012, que estabelece diretrizes para o processo de Inventário e Mapeamento de Ativos de Informação nos Aspectos Relativos à Segurança da Informação e Comunicações nos órgãos e entidades da Administração Pública Federal.
- Norma Complementar 12/IN01/DSIC/GSIPR, de 30 de janeiro de 2012, que estabelece diretrizes para o Uso de Dispositivos Móveis nos Aspectos relativos à Segurança da Informação e Comunicações nos órgãos e entidades da Administração Pública Federal.
- Norma Complementar 14/IN01/DSIC/GSIPR, de 30 de janeiro de 2012, que estabelece diretrizes relacionadas à Segurança da Informação e Comunicações para o Uso de Computação em Nuvem nos órgãos e entidades da Administração Pública Federal.
- Norma Complementar nº 21/IN01/DSIC/GSIPR, de 08 de outubro de 2014, que estabelece as Diretrizes para o Registro de Eventos, Coleta e Preservação de Evidências de Incidentes de Segurança em Redes nos órgãos e entidades da Administração Pública Federal, direta e indireta.

20. MEMBROS DA EQUIPE DE SEGURANÇA DA INFORMAÇÃO

Os servidores abaixo qualificados, estão diretamente responsáveis pela implantação e implementação da presente política, devendo reportar-se a eles todo e qualquer usuário e/ou setor para tratar de assuntos pertinentes à segurança da informação tratados por esse instrumento.

Edmilson Teles Ribeiro - Coordenador de TI– cti@to.SENAC.br
Denilson Felix Pinto – Suporte de TI – ci@to.senac.br
Nathalia Dias Maciel Pinheiro – Suporte TI – ci@to.senac.br
Danillo S. Milhomens – Analista de Sistemas – ti.desenvolvimento@to.senac.br
Felipe Fernandes de Albuquerque – Suporte TI – ci@to.senac.br

21. DAS DISPOSIÇÕES FINAIS

Assim como a ética, a segurança da informação deve ser entendida como parte fundamental da cultura interna do SENAC Tocantins. O cumprimento das diretrizes estabelecidas neste documento, produzirá ações e valores que nortearão as boas práticas no ambiente de trabalho. Quaisquer incidentes que venham a comprometer a integridade dos dados da empresa, será entendido como alguém agindo contra a ética e os bons costumes regidos pela instituição.