FIESP SESI SENAI IRS

SESI SENAI

# Política de Segurança da Informação

Comitê Gestor de Segurança da Informação - CGSI

*Vigente - 2013*

SESI

CONSELHO REGIONAL

**Presidente**
Paulo Skaf

**Representantes das Atividades Industriais**

**Titulares**
Elias Miguel Haddad
Fernando Greiber
Luis Eulalio de Bueno Vidigal Filho
Vandermir Francesconi Júnior

**Suplentes**
Nelson Abbud João
Nelson Antunes
Nilton Torres de Bastos
Sylvio Alves de Barros Filho

**Representantes das Categorias Econômicas dos Transportes, das Comunicações e da Pesca**

**Titular**
Massimo Andrea Giavina-Bianchi

**Suplente**
Nelson Luis de Carvalho Freire

**Representante do Ministério do Trabalho e Emprego**

**Titular**
Carlos Frederico Zimmermann Neto

**Representantes do Governo Estadual**

**Titular**
Ronaldo Bianchi

**Suplente**
Sérgio Tiezzi Júnior

**Representantes dos Trabalhadores da Indústria**

**Suplente**
Emílio Alves Ferreira Júnior

SENAI

CONSELHO REGIONAL

**Presidente**
Paulo Skaf

**Representantes das Atividades Industriais**

**Titulares**
Heitor Alves Filho
Jackson Medeiros de Farias Schneider
Luiz Adelar Scheuer
Saulo Pucci Bueno

**Suplentes**
Carlos Antonio Cavalcante
Carlos Lazzaro Junior
Ronald Moris Masijah
Sergio Tiaki Watanabe

**Representantes das Categorias Econômicas dos Transportes, das Comunicações e da Pesca**

**Titular**
Dorival Biasia

**Suplente**
Newton José Leme Duarte

**Diretor Regional**
Walter Vicioni Gonçalves

**Representante do Ministério do Trabalho e Emprego**

**Titular**
Carlos Frederico Zimmermann Neto

**Representantes do Ministério da Educação**

**Titular**
Garabed Kenchian

**Suplente**
Arnaldo Augusto Ciquielo Borges

**Representantes dos Trabalhadores da Indústria**

**Titular**
Antônio de Sousa Ramalho Júnior

**Suplente**
Nelson Antonio Dias

# ÍNDICE

# 1. APRESENTAÇÃO

## 1.1 Objetivo

Estabelecer as diretrizes, normas e procedimentos para a adoção de mecanismos relacionados à segurança da informação do SESI-SP e SENAI-SP, prezando pela sua confidencialidade, integridade e disponibilidade.

## 1.2 Campo de aplicação

Abrange a todos os colaboradores do SESI-SP e SENAI-SP.

## 1.3 Conceito

A Política de Segurança da Informação é uma declaração formal do SESI-SP e do SENAI-SP acerca do compromisso com a proteção das informações de sua propriedade ou sob sua guarda, devendo ser comunicada a todos os seus colaboradores a fim de que os seus preceitos sejam cumpridos.

## 1.4 Benefício

A adoção da Política de Segurança da Informação visa minimizar os riscos de falhas, danos e prejuízos que possam comprometer as imagens e as missões do SESI-SP e do SENAI-SP.

## 1.5 Estrutura

A Política de Segurança da Informação é formada por diretrizes, normas e procedimentos.

### *1.5.1 Componentes*

**Diretrizes:** as diretrizes expressam os objetivos e as expectativas das instituições em relação à segurança da informação, devendo estar alinhadas as missões do SESI-SP e do SENAI-SP. Palavra-chave: **Definição.**

**Normas**: são regras táticas adotadas para atender as diretrizes.
Palavras chave: **O que fazer?**

**Procedimentos:** são manuais operacionais, que fornecem instruções aos colaboradores para a execução de determinada tarefa a ser realizada, de forma a atender a definição tática.
Palavras chave: **Como fazer?**

### 1.5.2. Distribuição hierárquica

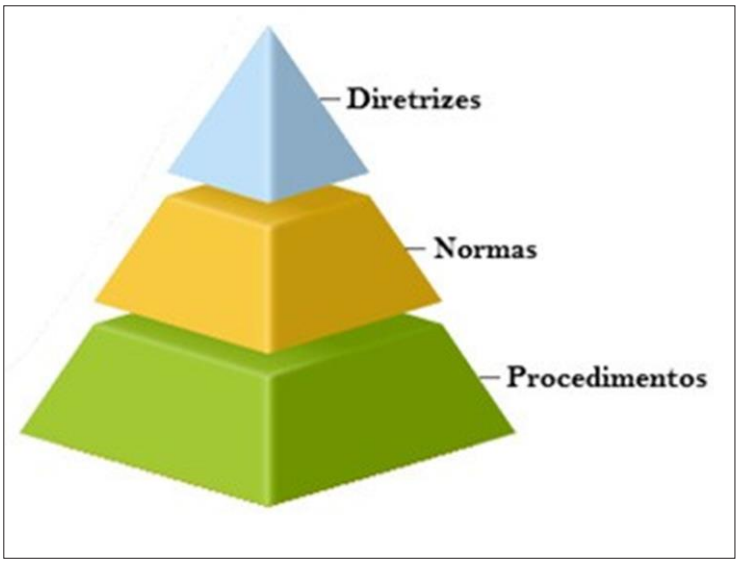
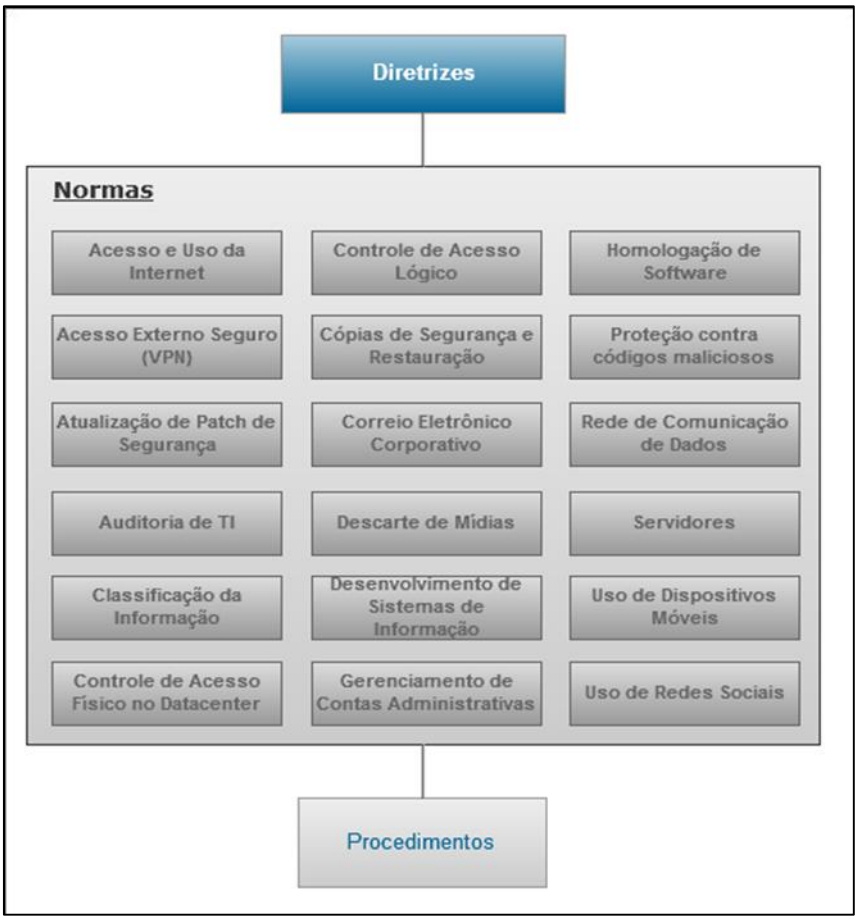



**Figura 1**. Estrutura da Política de Segurança da Informação

### 1.5.3. Distribuição lógica



## 1.6 Como consultar a Política de Segurança da Informação?

Todos os colaboradores deverão conhecer a Política de Segurança da Informação. A anuência quanto ao conteúdo se dá após a leitura e entendimento das diretrizes e assinatura individual do Termo de Aceite.

As normas e procedimentos deverão ser consultados de acordo com a abrangência, atribuições e necessidades dos colaboradores. Integram o conteúdo das normas, referências aos procedimentos recomendados por assunto.

## 1.7 Informações adicionais

*1.7.1.* O Comitê Gestor de Segurança da Informação do SESI-SP e SENAI-SP possui atribuições de acordo com a resolução conjunta RC-01/12, retificada através da RC-03/14.

*1.7.2.* Os documentos referentes à Política de Segurança da Informação estão no Portal de Gestão do SESI-SP e Portal de Gestão do SENAI-SP, na área de Políticas e Objetivos.
Os procedimentos, manuais, instruções de serviços e formulários também encontram-se nos portais mencionados acima, porém na área de Documentação da Diretoria de Tecnologia da Informação.

*1.7.3.* A Política de Segurança da Informação foi elaborada em alinhamento com o Código de Ética do SESI-SP e SENAI-SP.

*1.7.4.* O não cumprimento dos requisitos previstos nesta Política de Segurança da Informação sujeitará o colaborador às medidas administrativas cabíveis.

# 2. DIRETRIZES

**2.1)** Todas as ações referentes à segurança da informação devem ter comprometimento e responsabilidade com as missões institucionais do SESI-SP e SENAI-SP.

**2.2)** Os colaboradores, devem estar cientes das regras descritas no conjunto de documentos que compõem a Política de Segurança da Informação, incluindo as diretrizes, normas e procedimentos, sendo os dois últimos acessados conforme sua necessidade.

**2.3)** O conhecimento desta política é obrigatório para todos os colaboradores e após a assinatura do Termo de Aceite, a alegação do desconhecimento da mesma não será aceita como resguardo de seu não cumprimento.

**2.4)** A identificação de qualquer colaborador deve ser única e intransferível, qualificando-o como responsável pelas ações realizadas.

**2.5)** A senha é utilizada como assinatura eletrônica e deve ser mantida secreta, ficando sob responsabilidade do colaborador zelar por sua confidencialidade.

**2.6)** O acesso às informações e demais recursos deve ser devidamente autorizado.

**2.7)** A concessão de acessos deve obedecer ao critério de menor privilégio, no qual os usuários têm acesso somente aos recursos da informação imprescindíveis ao pleno desempenho de suas atividades.

**2.8)** Todos os serviços contratados pelo SESI-SP e SENAI-SP devem possuir o documento termo de confidencialidade, devidamente firmado pela empresa contratada.

**2.9)** Toda informação do SESI-SP e SENAI-SP deve ser classificada de acordo com a sua confidencialidade, conforme o documento norma de “Classificação da Informação”.

**2.10)** Todas as informações das instituições deverão ser descartadas respeitando o documento norma para “Descarte de Mídias”.

# 3. NORMAS

**Tabela referencial para acesso às normas**

| Item | Norma | Objetivo | Destinado a... |
|---|---|---|---|
| **3.1** | **Acesso e Uso da Internet** | Estabelecer regras para garantir o uso adequado dos serviços de Internet disponibilizados pelo SESI-SP e SENAI-SP. | **Todos os colaboradores** do SESI-SP e SENAI-SP |
| **3.2** | **Acesso Externo Seguro (VPN)** | Estabelecer normas para o acesso remoto seguro às redes do SESI-SP e SENAI-SP através de conexão em rede privada virtual – VPN. | **Todos os colaboradores** do SESI-SP e SENAI-SP |
| **3.3** | **Atualização de Patch de Segurança** | Estabelecer normas para a aplicação de patchs de segurança nos serviços críticos de Tecnologia da Informação do SESI-SP e SENAI-SP. | Colaboradores da Diretoria de Tecnologia da Informação do SESI-SP e SENAI-SP |
| **3.4** | **Auditoria de TI** | Fornecer informações sobre os processos de auditoria dos serviços de Tecnologia da Informação do SESI-SP e SENAI-SP. | **Todos os colaboradores** do SESI-SP e SENAI-SP |
| **3.5** | **Classificação da Informação** | Definir a estrutura de classificação das informações do SESI-SP e SENAI-SP e atribuir critérios e responsabilidades associadas a esta classificação. | **Todos os colaboradores** do SESI-SP e SENAI-SP |
| **3.6** | **Controle de Acesso Físico ao Datacenter** | Estabelecer normas para prevenir o acesso físico não autorizado no ambiente de Datacenter do SESI-SP e SENAI-SP. | Colaboradores da Diretoria de Tecnologia da Informação do SESI-SP e SENAI-SP |
| **3.7** | **Controle de Acesso Lógico** | Estabelecer métodos de controle de acesso lógico às informações do SESI-SP e SENAI-SP. | **Todos os colaboradores** do SESI-SP e SENAI-SP |
| **3.8** | **Cópias de Segurança e Restauração** | Fornecer instruções para o processo de cópia de segurança e restauração das informações, visando manter as informações relevantes ao pleno funcionamento das atividades do SESI-SP e SENAI-SP. | **Todos os colaboradores** do SESI-SP e SENAI-SP |
| **3.9** | **Correio Eletrônico Corporativo** | Estabelecer regras para o uso adequado dos serviços de correio eletrônico e ferramentas do Office 365 do SESI-SP e SENAI-SP. | **Todos os colaboradores** do SESI-SP e SENAI-SP |
| **3.10** | **Descarte de Mídias** | Estabelecer normas para o descarte adequado e seguro das mídias do SESI-SP e SENAI-SP, quando não forem mais necessárias. | **Todos os colaboradores** do SESI-SP e SENAI-SP |

| | | | |
|---|---|---|---|
| **3.11** | **Desenvolvimento de Sistemas de Informação** | Regulamentar os requisitos de segurança para o processo de desenvolvimento e manutenção de sistemas do SESI-SP e SENAI-SP. | Colaboradores da Diretoria de Tecnologia da Informação do SESI-SP e SENAI-SP |
| **3.12** | **Gerenciamento de Contas Administrativas** | Estabelecer normas para o gerenciamento adequado de contas administrativas da rede do SESI-SP e SENAI-SP. | Colaboradores da Diretoria de Tecnologia da Informação do SESI-SP e SENAI-SP |
| **3.13** | **Homologação de Software** | Estabelecer critérios de homologação de software do SESI-SP e SENAI-SP. | **Todos os colaboradores** do SESI-SP e SENAI-SP |
| **3.14** | **Proteção Contra Códigos Maliciosos** | Estabelecer normas para a proteção dos recursos de Tecnologia da Informação do SESI-SP e SENAI-SP contra ação de códigos maliciosos, programas impróprios e acesso não autorizado. | **Todos os colaboradores** do SESI-SP e SENAI-SP |
| **3.15** | **Rede de Comunicação de Dados** | Garantir o uso adequado da rede do SESI-SP e SENAI-SP, de forma a minimizar os riscos e impactos. | **Todos os colaboradores** do SESI-SP e SENAI-SP |
| **3.16** | **Servidores de Rede** | Estabelecer diretrizes no que se refere aos servidores de Tecnologia da Informação do SESI-SP e SENAI-SP. | Colaboradores da Diretoria de Tecnologia da Informação do SESI-SP e SENAI-SP |
| **3.17** | **Uso de Dispositivos Móveis** | Estabelecer critérios para o uso adequado e seguro dos dispositivos móveis no ambiente do SESI-SP e SENAI-SP. | **Todos os colaboradores** do SESI-SP e SENAI-SP |
| **3.18** | **Uso de Redes Sociais** | Preservar a imagem do SESI-SP e SENAI-SP nas redes sociais, evitando que mensagens inapropriadas sejam veiculadas em nome das instituições. | **Todos os colaboradores** do SESI-SP e SENAI-SP |

# 3.1. Norma para Acesso e Uso da internet

## 1. OBJETIVO

Estabelecer regras para garantir o uso adequado dos serviços de Internet disponibilizados pelo SESI-SP e SENAI-SP.

## 2. CAMPO DE APLICAÇÃO

Abrange a todos os colaboradores do SESI-SP e SENAI-SP.

## 3. CRITÉRIOS DE UTILIZAÇÃO

Qualquer informação que é acessada, transmitida, recebida ou produzida na internet está sujeita a divulgação e auditoria. Portanto, o SESI-SP e SENAI-SP, em total conformidade legal, reservam-se o direito de monitorar e registrar todos os acessos a ela.

- Os equipamentos, tecnologia e serviços fornecidos para o acesso à internet são de propriedade do SESI-SP e SENAI-SP, que podem analisar e se necessário, bloquear qualquer arquivo, site, correio eletrônico, domínio ou aplicação armazenados na rede/internet, estejam eles em disco local, na estação ou em áreas privadas da rede.

- O SESI-SP e SENAI-SP, ao monitorarem a rede interna, pretendem garantir a integridade dos dados e programas. Toda tentativa de alteração dos parâmetros de segurança, por qualquer colaborador, sem o devido credenciamento e a autorização para tal, será julgada inadequada e os riscos relacionados serão informados ao colaborador e ao respectivo superior. O uso de qualquer recurso para atividades ilícitas poderá acarretar as ações administrativas e as penalidades decorrentes de processos civil e criminal, sendo que nesses casos a instituição cooperará ativamente com as autoridades competentes.

- Como é do interesse do SESI-SP e SENAI-SP que seus colaboradores estejam bem informados, o uso de sites de notícias ou de serviços, por exemplo, é aceitável, desde que não comprometa a conexão de acesso em horários estritamente comerciais, que não perturbe o bom andamento dos trabalhos e nem implique conflitos de interesse com os seus objetivos de negócio.

- Os colaboradores não poderão em hipótese alguma utilizar os recursos do SESI-SP e SENAI-SP para fazer o download ou distribuição de software ou dados pirateados, atividade considerada delituosa de acordo com a legislação nacional.

- Colaboradores com acesso à internet não poderão efetuar upload de qualquer software licenciado ao SESI- SP e SENAI-SP ou de dados de sua propriedade aos seus parceiros e clientes, sem expressa autorização do responsável pelo software ou pelos dados.

- Os colaboradores não poderão utilizar os recursos do SESI-SP e SENAI-SP para deliberadamente propagar qualquer tipo de vírus, worm, cavalo de troia, spam, assédio ou perturbação.

- A Diretoria de Tecnologia da Informação define os perfis padrões de acesso e compartilhamento dos recursos e serviços de Tecnologia da Informação, de acordo com as necessidades profissionais dos colaboradores e prestadores de serviços do SESI-SP e SENAI-SP. Tais perfis podem ser modificados com base em justificativa técnica encaminhada formalmente à DTI pela área interessada.

- Para garantir a segurança e integridade dos serviços, não é permitida a utilização de acessos secundários à Internet (linha discada, ADSL, 3G, 4G, cable modem, dentre outros), em equipamentos conectados à rede do SESI-SP e SENAI-SP, sem o conhecimento e autorização formal de uso emitida pela Diretoria de Tecnologia da Informação.

## 3.1 Condições de uso

- Em qualquer dos serviços de Internet disponibilizados pelo SESI-SP e SENAI-SP, é expressamente proibido o uso nos seguintes casos:
  - ✓ Uso particular para operações de venda, oferta de serviços e propagandas, exceto os previamente autorizados (ex.: quadro de anúncios na Intranet);
  - ✓ Atividades de caráter político-partidário;
  - ✓ Operações que acarretem o alto volume de transmissão, salvo para fins profissionais;
  - ✓ Obtenção, armazenamento, uso ou repasse de material protegido por leis de salvaguarda de propriedade intelectual, brasileiras ou estrangeiras, inclusive arquivos de músicas, filmes, livros ou versões de programas;
  - ✓ Obtenção, armazenamento, uso ou repasse de material com conteúdo pornográfico;
  - ✓ Uso de serviço de correios eletrônicos internos do SESI-SP e SENAI-SP para envio de mensagens ofensivas;
  - ✓ Tentativa de violação de sistemas;
  - ✓ Obtenção e propagação intencional de vírus ou cavalos de Tróia;
  - ✓ Uso de ferramentas para tentativa de descobrir vulnerabilidades ou invadir computadores;
  - ✓ Uso de ferramentas de monitorização e programas para obtenção de senhas;
  - ✓ Violação do Código de Ética do SESI-SP e SENAI-SP;
  - ✓ Envio, transmissão, distribuição ou armazenamento na Internet de informações de propriedade do SESI-SP e SENAI-SP, correios eletrônicos internos, dados, segredos comerciais, financeiros ou tecnológicos ou quaisquer outras informações pertencentes às instituições, a não ser que expressamente autorizado pelo gestor da informação.

## 3.2 Perfis de Acesso

- Para controle do acesso aos sites e serviços da Internet, o sistema que gerencia o acesso possui, de forma incorporada, uma ferramenta que procura e categoriza automaticamente os sites, conforme as categorias listadas no quadro Grupos e Categorias de Acesso.

- Todos os colaboradores são relacionados em grupos preliminarmente configurados de acordo com o tipo e necessidade de acesso. Cada colaborador com acesso à Internet está enquadrado em apenas um dos grupos de acesso. As categorias marcadas abaixo como “Bloqueadas” não estão acessíveis a nenhum colaborador.

- As solicitações de mudanças do grupo de acesso à Internet deverão ser realizadas pelo Diretor, Gerente, Coordenador ou Supervisor da unidade operacional ou corporativa através de chamado técnico aberto direcionado a Central de Serviços de TI, informando o nome do colaborador, o número de identificação, o grupo de acesso pleiteado (1, 2, 3, 4 ou 5) e a justificativa para alteração.

- As solicitações para liberação de sites devem ser realizadas pelo colaborador por chamado técnico.

## Grupos e Categorias de Acesso

"X" representa Bloqueio de Acesso

| | Categorias | Grupo1 | Grupo2 | Grupo3 | Grupo4 | Grupo5 |
|---|---|---|---|---|---|---|
| A | Áudio/Vídeo | X | X | | | |
| B | Bate Papo | X | X | | | X |
| C | Compras | | | | | |
| D | Comunicação via Internet | X | X | | | X |
| E | Crenças | | | | | |
| F | Downloads | X | | | | X |
| G | Educação | | | | | |
| H | Webmail | X | | | X | X |
| I | Entretenimento | | | | | |
| J | Esporte | | | | | |
| K | Gastronomia | | | | | |
| L | Imóvel / Construção | | | | | |
| M | Notícias | | | | | |
| N | Organizações / Negócios | | | | | |
| O | Política | | | | | |
| P | Relacionamento | | | | | |
| Q | Saúde / Medicina | | | | | |
| R | Veículos | | | | | |
| S | Viagem e Turismo | | | | | |
| T | Conteúdo Ilícito ou Indesejável | X | X | X | X | X |
| U | Drogas | X | X | X | X | X |
| V | Hacker/Proxy | X | X | X | X | X |
| X | Jogos de Azar | X | X | X | X | X |
| Y | Material Adulto | X | X | X | X | X |

**Grupos de acesso**

| Nome do grupo | Descrição |
|---|---|
| **Grupo1** | Tipo comum de acesso, aplicado para maioria dos colaboradores do SESI-SP e SENAI-SP |
| **Grupo2** | Acesso permitido a Webmail e Download de todos os tipos de arquivos |
| **Grupo3** | Acesso permitido a todas as categorias, com exceção das rotuladas de **T** a **Y**, que são bloqueadas a todos os grupos. |
| **Grupo4** | Acesso permitido a todas as categorias, exceto webmail. |
| **Grupo5** | Acesso permitido a Áudio/Vídeo (Youtube). |

## 3.3 Solicitação de Acesso

### *3.3.1 Login*

- ✓ Todo colaborador, quando cadastrado na rede, recebe o acesso à internet.
- ✓ Toda solicitação de cadastramento, ou mudança de perfil de acesso à Internet deverá ser realizada através de chamado técnico via Central de Serviços de TI, conforme descrito no procedimento DTI-001. O manual está publicado no Portal de Gestão do SESI-SP e Portal de Gestão do SENAI-SP SP e pode ser acessado seguindo as instruções do item 1.7.2 “Informações adicionais”, página 7 da Política de Segurança da Informação através ou através do link documento .

### *3.3.2 Liberação e acesso a serviços específicos de Internet*

• É necessária a aprovação do superior imediato para a liberação dos seguintes serviços:

- ✓ Acesso a sites bloqueados;
- ✓ Acesso às portas específicas;
- ✓ Serviços de comunicação;
- ✓ Serviço de File Transfer Protocol (FTP);
- ✓ Serviço de Virtual Private Network (VPN) externa;
- ✓ Com aprovação do superior imediato, o colaborador deverá abrir um chamado junto à Central de Serviços de TI, que irá analisar a solicitação e liberar o acesso.

## 3.4 Exclusão do Acesso

• A exclusão do colaborador da internet é realizada pela Diretoria de Tecnologia da Informação, mediante a desvinculação do colaborador do quadro de colaboradores do SESI-SP e SENAI-SP, através de comunicação recebida da Diretoria de Recursos Humanos ou por chamado técnico solicitado via Central de Serviços de TI, realizada pela própria unidade de lotação do colaborador.

• É de responsabilidade do superior direto, a solicitação de exclusão do acesso à Internet de um colaborador, seja ele colaborador por prazo definido, indefinido ou terceiro. A solicitação de exclusão deverá ser realizada através de chamado técnico.

## 3.5 Revisão dos Acessos

• Periodicamente a Diretoria de Tecnologia da Informação, solicitará as unidades operacionais e diretorias corporativas através de plano de comunicação, a revisão dos tipos de acessos dos colaboradores, de acordo com suas respectivas atribuições.

# 3.2. Norma para Acesso Externo Seguro(VPN)

## 1. OBJETIVO

Estabelecer norma para o acesso remoto seguro às redes do SESI-SP e SENAI-SP através de conexão em rede privada virtual – VPN.

## 2. CAMPO DE APLICAÇÃO

Abrange a todos os colaboradores do SESI-SP e SENAI-SP.

## 3. CRITÉRIO DE UTILIZAÇÃO

- Os recursos de VPN serão utilizados somente para acessos externos, ou seja, quando o colaborador estiver fora da rede do SESI-SP e SENAI-SP.

- A liberação do acesso externo aos recursos corporativos do SESI-SP e SENAI-SP está habilitada aos colaboradores, porém só deve ser acessada em período comercial durante atividades em outros locais, salvo solicitação e liberação da chefia imediata.

- O uso dos recursos da VPN deverá ser utilizado para fins estritamente profissionais, de forma a cumprir as normas e procedimentos de segurança, ficando sob responsabilidade do colaborador a utilização adequada dos recursos de VPN.

- Todos os dispositivos externos conectados às redes internas do SESI-SP e SENAI-SP via VPN devem estar com as versões mais atualizadas de seus sistemas, com os últimos “patches” de segurança instalados, antivírus e lista de vírus atualizados. Em caso de desatualização dos sistemas durante a conexão, o colaborador estará expondo o SESI-SP e SENAI-SP ao risco de propagação de códigos maliciosos nas redes internas. Portanto, é de responsabilidade do colaborador garantir a atualização e a procedência dos recursos (equipamentos e links de comunicação) utilizados para conexão.

- A DTI do SESI-SP e SENAI-SP monitora o volume de dados das conexões VPN e se reserva ao direito de limitar o período de funcionamento, desconectar qualquer sessão onde se verifique taxas divergentes da média normal das outras sessões ou quando houver comprometimento da segurança.

- Todo acesso via VPN é registrado em log e a DTI poderá auditar todos os sistemas clientes VPN e toda a comunicação entre esses sistemas e as redes internas do SESI-SP e SENAI-SP, para verificar a aderência aos requerimentos de segurança.

- A DTI disponibiliza dois tipos de acesso via VPN:
  - ✓ **VPN/SSL**: é de uso dos colaboradores do SESI-SP e SENAI-SP;
  - ✓ **VPN/IPSec**: é de uso exclusivo dos colaboradores terceirizados (Contratos de Apoio da DTI).

## 3.1 VPN/SSL

- Todos os funcionários do SESI-SP e SENAI-SP possuem acesso VPN/SSL, através do portal no endereço https://entrada.sesisenaisp.org.br, conforme figura a seguir:

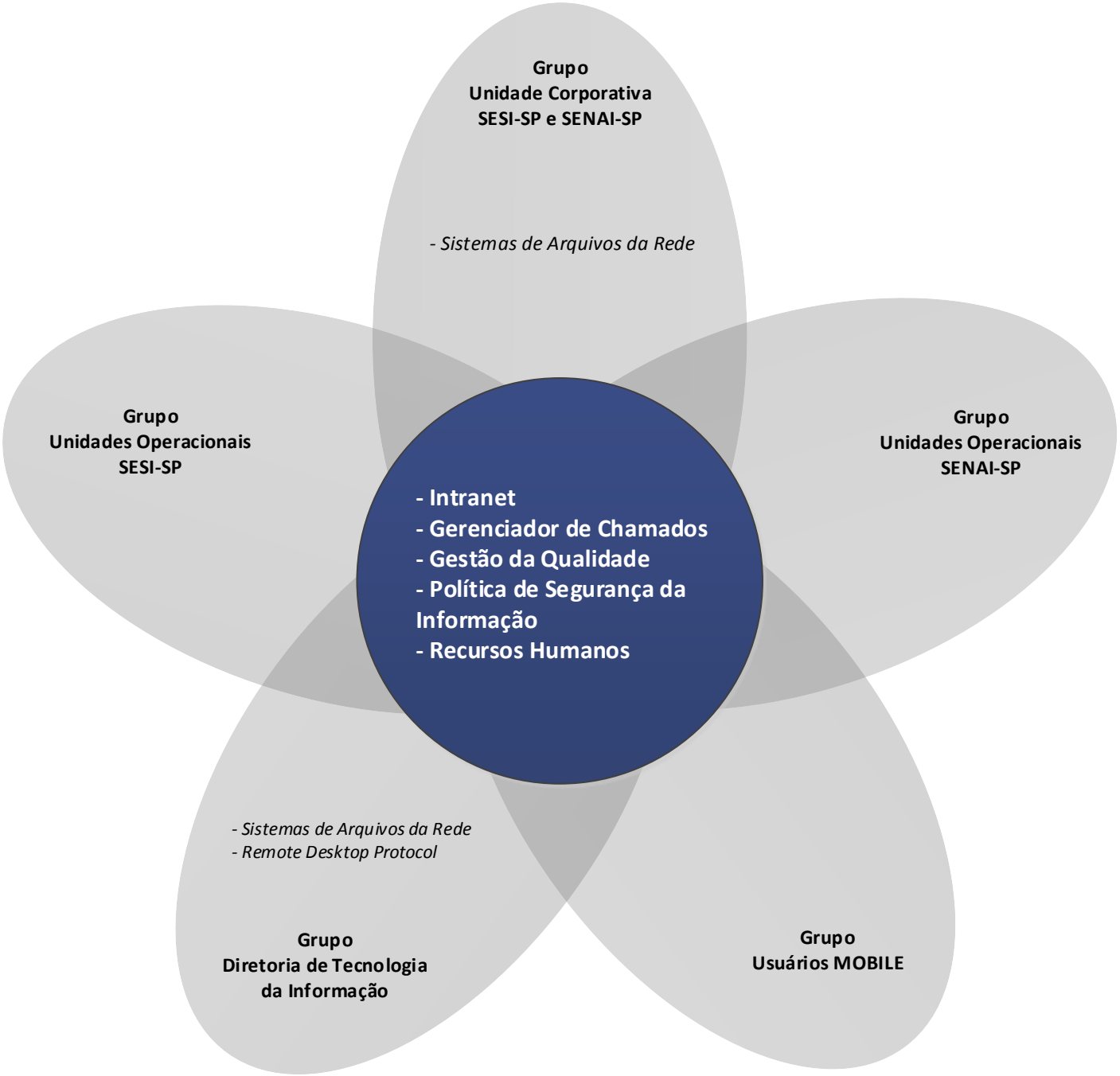



**Figura 2**: Grupo de acesso VPN/SSL

## 3.2 VPN/IPSec

- Os colaboradores vinculados aos Contratos de Apoio devem possuir usuário TC individual cadastrado, não podendo gerar login único “funcional” para a empresa.

- Para que o Contrato de Apoio tenha acesso à VPN, a empresa deve assinar o termo de confidencialidade com o SESI-SP e SENAI-SP.

- Somente o gestor do Contrato de Apoio pode solicitar a criação, alteração ou exclusão da estrutura de VPN através de abertura de chamado técnico via Central de Serviços de TI. Para criação de perfil na VPN, o gestor do Contrato de Apoio deverá fornecer as seguintes informações: nome e IP da máquina, nome do colaborador, porta de conexão e tempo de contrato. Serão fornecidos os dados para acesso (login e senha) aos funcionários terceirizados autorizados.

- É de total responsabilidade do gestor do Contrato de Apoio garantir que a empresa contratada não esteja acessando informações além das que precisa, portanto, o mesmo deve possuir o perfil de VPN instalado para realizar os testes necessários antes de liberação para a empresa.

- É necessária à instalação e configuração do cliente VPN/IPSec. Para isso, o colaborador deve seguir as instruções contidas no manual DTI-046, para instalação e configuração do cliente VPN-IPSec. O manual está publicado no Portal de Gestão do SESI-SP e Portal de Gestão do SENAI-SP e pode ser acessado seguindo as instruções do item 1.7.2 “Informações adicionais”, página 7 da Política de Segurança da Informação, ou através do link documento.

### *3.2.1 Exclusão do perfil de colaboradores terceirizados*

- A exclusão do acesso de conexão VPN/IPSec poderá ocorrer das seguintes formas:
  - ✓ Por solicitação do requisitante através de chamado técnico via Central de Serviços de TI;
  - ✓ Por desligamento do colaborador no SESI-SP e SENAI-SP;
  - ✓ Por término do contrato.

## 3.3 Horário permitido para acesso

- O horário permitido para acesso pode ser consultado no item da PSI de número 3.7 - Norma para Controle de Acesso Lógico, subitem “3.3 Acesso lógico aos recursos corporativos”.

# 3.3. Norma para Atualização de Patch de Segurança

## 1. OBJETIVO

Estabelecer normas para a aplicação de patchs de segurança nos serviços críticos de tecnologia da informação do SESI-SP e SENAI-SP.

## 2. CAMPO DE APLICAÇÃO

Abrange aos colaboradores da Diretoria de Tecnologia da Informação (DTI) do SESI-SP e SENAI-SP.

## 3. CRITÉRIO DE UTILIZAÇÃO

- A aplicação de patches é uma tarefa a ser realizada pelos administradores dos serviços, para garantir que os serviços permaneçam em operação de forma segura e estável.

- Havendo correções ou atualizações disponibilizadas pelo fabricante aos sistemas operacionais das estações e dos servidores, ou sistemas de detecção e bloqueio de códigos maliciosos, as mesmas devem ser implementadas em até 15 (quinze) dias, a fim de se evitar que estes sistemas fiquem vulneráveis.

- É necessário diariamente monitorar a liberação de patches de segurança para os serviços críticos de tecnologia da informação, definidos no documento DTI – 044. O manual está publicado no Portal de Gestão do SESI-SP e Portal de Gestão do SENAI-SP SP e pode ser acessado seguindo as instruções do item 1.7.2 “Informações adicionais”, página 7 da Política de Segurança da Informação ou através do link documento.

- Para serviços Microsoft, deverá ser utilizada a ferramenta para gerenciamento da distribuição de patches chamada WSUS ou similar.

- Os patches de segurança devem ser instalados sempre que disponíveis, porém antes da instalação eles deverão ser:
  - ✓ Homologados em ambiente segregado;
  - ✓ Analisados e documentados no plano de implantação, contendo plano de teste e de Disaster Recovery;
  - ✓ Aprovados pela diretoria.

# 3.4. Norma para Auditoria de TI

## 1. OBJETIVO

Fornecer informações sobre os processos de auditoria dos serviços de Tecnologia da Informação (TI) do SESI-SP e SENAI-SP.

## 2. CAMPO DE APLICAÇÃO

Abrange a todos os colaboradores do SESI-SP e SENAI-SP.

## 3. CRITÉRIO DE UTILIZAÇÃO

- A auditoria de Tecnologia da Informação (TI) é um procedimento de verificação de conformidade de requisitos e de melhorias nos serviços e processos existentes de TI.

- Considera-se que todo processo contendo informação, dado armazenado, modificado ou transportado pelos sistemas e serviços de Tecnologia da Informação providos pelo SESI-SP e SENAI-SP, constitui-se patrimônio de conhecimento e propriedade intelectual das entidades e por esse motivo são passíveis de auditoria para verificação quanto à conformidade de seu uso.

- A Diretoria de Tecnologia da Informação poderá realizar periodicamente ou não, processo de auditoria incluindo verificação dos dados contidos nos equipamentos, nas mídias (ex.: PENDRIVES, HDD externos, CD/DVD, etc.), nos correios eletrônicos, nas unidades compartilhadas ou em demais serviços do SESI- SP e SENAI-SP estando eles isolados ou em rede, com o objetivo de avaliar o atendimento à conformidade dos serviços e processos.

- O resultado das auditorias, deverá ser documentado e as ações de melhoria ou correção deverão ser transformadas em plano de ação a ser lançado no sistema de Gestão da Qualidade.

- O escopo dos serviços auditados está descrito no procedimento DTI-089. O procedimento está publicado no Portal de Gestão do SESI-SP e Portal de Gestão do SENAI-SP e pode ser acessado seguindo as instruções do item 1.7.2 “Informações adicionais”, página 7 da Política de Segurança da Informação, ou através do link documento.

### 3.1 Das responsabilidades do auditor de TI

- Analisar e avaliar a eficácia do recurso de TI e os processos de gestão de desempenho.

- Analisar e avaliar a conformidade com as exigências legais, ambientais e de qualidade de informações, fiduciárias e de segurança da informação.

- Avaliar os controles de TI do SESI-SP e SENAI-SP.

- Gerar relatório, descrevendo as atividades de auditoria realizadas, os itens não conformes identificados e os pontos de melhoria sugeridos.

### 3.2 Evidências dos serviços auditados

- Todo item de tecnologia da informação passível de auditoria deverá gerar arquivos de registro (log), contendo: quem, quando e a ação realizada.

- Os arquivos de registro (log) devem ser armazenados no local de origem por no mínimo 45 (quarenta e cinco) dias corridos. Após esse período, devem ser armazenados em backup por no mínimo 5 anos.

## 3.3 O processo de prevenção de perda de dados

- A conformidade aos requisitos descritos na Norma de Classificação da Informação é avaliada através de ferramenta específica para esse propósito denominada DLP.

- Os procedimentos que mapeiam o processo de Prevenção de Perda de Dados e a utilização da ferramenta de DLP se encontram no documento DTI-120. O manual está publicado no Portal de Gestão do SESI-SP e Portal de Gestão do SENAI-SP SP e pode ser acessado seguindo as instruções do item 1.7.2 “Informações adicionais”, página 7 da Política de Segurança da Informação ou através do link documento.

## 3.4 Incidentes de Segurança da Informação

- Investigações deverão ser tratadas de acordo com o procedimento DTI-082. O manual está publicado no Portal de Gestão do SESI-SP e Portal de Gestão do SENAI-SP SP e pode ser acessado seguindo as instruções do item 1.7.2 “Informações adicionais”, página 7 da Política de Segurança da Informação ou através do link documento.

- Em caso de confirmação de atividades ilícitas o colaborador ficará sujeito a sanções administrativas.

# 3.5. Norma para Classificação da Informação

## 1. OBJETIVO

Definir a estrutura de classificação das informações do SESI-SP e SENAI-SP e atribuir critérios e responsabilidades associadas a classificação.

## 2. CAMPO DE APLICAÇÃO

Abrange a todos os colaboradores e todos os documentos do SESI-SP e SENAI-SP.

## 3. CRITÉRIO DE UTILIZAÇÃO

- Toda informação corporativa, não classificada será considerada por padrão como interna.
- O conhecimento da informação deve ser usado apenas para os propósitos de interesse do SESI-SP e SENAI-SP.
- Toda informação deve possuir uma classificação quanto a sua confidencialidade.
- Todos os documentos eletrônicos, planilhas e apresentações do SESI-SP e SENAI-SP devem exibir em seu cabeçalho ou rodapé a classificação da informação de seu conteúdo.
- Toda informação deve possuir um proprietário, responsável por sua classificação que deverá ser determinada no momento de criação.
- A classificação de uma informação deve ser preservada. Caso haja necessidade de alterar esta classificação, deve haver justificativa plausível e aprovação do superior responsável.
- Alterações de classificação devem ser providas preferencialmente por quem a classificou originalmente e na sua ausência, por colaboradores que assumiram a sua função ou possuem nível hierárquico superior ao exigido para a sua classificação.
- O descarte de informações classificadas como confidenciais deve ser feito de forma que impossibilite a recuperação. Para mais informações sobre descarte, consulte a Norma de Descarte de Mídias.

### 3.1 Classificação da Informação

- A classificação da informação deve seguir os critérios da tabela a seguir:

| Classificação | Critério |
|---|---|
| Confidencial | A informação confidencial é restrita para o mínimo possível de colaboradores do SESI-SP e SENAI-SP.<br>Seu acesso deve ser controlado e auditado.<br>Deve ser mantida em sigilo e repassada somente às pessoas que irão utilizá-las em suas atribuições. |
| Interna | A informação interna é restrita às áreas internas do SESI-SP e SENAI-SP, podendo ser compartilhada entre todos os colaboradores e prestadores de serviço, porém não pode ser repassada a indivíduos que não pertençam às instituições, isto é, não deve ser divulgada publicamente. |
| Pública | A informação pública não possui restrições de divulgação, podendo ser repassada a qualquer indivíduo, dentro ou fora do SESI-SP e SENAI-SP, podendo ser publicada na internet. |

# 3.6. Norma para Controle de Acesso Físico ao Datacenter

## 1. OBJETIVO

Estabelecer normas para prevenir o acesso físico não autorizado no ambiente de Datacenter do SESI-SP e SENAI-SP.

## 2. CAMPO DE APLICAÇÃO

Abrange aos colaboradores da Diretoria de Tecnologia da Informação (DTI) do SESI-SP e SENAI-SP.

## 3. CRITÉRIO DE UTILIZAÇÃO

- O ambiente de Datacenter do SESI-SP e SENAI-SP é o local onde estão as instalações principais para o processamento das informações das instituições, o acesso a esse ambiente deve ser restrito, monitorado e controlado utilizando dispositivos de restrição de acessos.

- Acessos de pessoa não autorizada só serão permitidos com o acompanhamento de colaborador autorizado.

- No caso de desligamento de colaborador que possua acesso ao Datacenter, é de responsabilidade do superior imediato do colaborador providenciar com antecedência o bloqueio do seu acesso.

- Para maiores informações consulte o procedimento DTI-001. O procedimento está publicado no Portal de Gestão do SESI-SP e Portal de Gestão do SENAI-SP e pode ser acessado seguindo as instruções do item 1.7.2 “Informações adicionais”, página 7 da Política de Segurança da Informação, ou através do link documento.

# 3.7. Norma para Controle de Acesso Lógico

## 1. OBJETIVO

Estabelecer métodos de controle de acesso lógico às informações do SESI-SP e SENAI-SP.

## 2. CAMPO DE APLICAÇÃO

Abrange a todos os colaboradores do SESI-SP e SENAI-SP.

## 3. CRITÉRIO DE UTILIZAÇÃO

- O controle de acesso lógico visa garantir a proteção das informações dos serviços do SESI-SP e SENAI-SP, restringindo-as apenas aos colaboradores autorizados.

- Para fins de rastreabilidade, o controle de acesso deve prever a identificação do colaborador, local, data e horário de acesso.

- No caso de o colaborador mudar de área de atuação no SESI-SP e SENAI-SP, os seus privilégios anteriores deverão ser revogados, sendo responsabilidade do seu ex-gestor requisitar a alteração de perfil junto a central de serviços.

- Todo sistema cujo conteúdo da informação está classificado como confidencial, deverá ser acessado através de protocolo criptografado, exigirá login e senha ao colaborador.

### 3.1 Credenciais

#### *3.1.1 Identificação dos usuários*

Todo colaborador deverá possuir conta de acesso lógico com as seguintes regras:

- ✓ Funcionário do SENAI: SN + Número de Identificação;
- ✓ Funcionário do SESI: SS + Número de Identificação;
- ✓ Terceiros ou Visitantes: TC + Número de Identificação;
- ✓ Administração de domínios: AD + Número de Identificação.

- Para cadastramento de contas de terceiros e visitantes, o responsável deverá gerar chamado técnico através da Central de Serviços de TI, com as seguintes informações: nome completo; CPF; RG; número para contato; prazo de validade da conta; grupo de acesso conforme Norma de Acesso e Uso da Internet; e o tipo de acesso (internet ou rede). Caso for rede, deverá ser informada a área a ser acessada.

- Conforme diretrizes, os usuários terceirizados somente poderão acessar dados na rede corporativa após assinatura de contrato e do termo de confidencialidade.

#### *3.1.2 Contas de sistemas (serviços)*

- A DTI deverá possuir controle da relação das contas de serviço e seus responsáveis.

### 3.2 Senhas

- Para evitar roubo, deturpação das informações e para possibilitar rastreabilidade no processo de controle de acesso, é definido que toda senha é pessoal, intransferível e deve ser mantida sob sigilo pelo próprio colaborador. Em caso de situações comprovadas de acesso e manipulação indevida da informação, o colaborador será sujeito à advertência ou medidas administrativas cabíveis.

- Após o retorno do período de férias, as senhas do colaborador serão expiradas sendo automaticamente solicitadas novas senhas.

- Para colaboradores terceiros, será obrigatória a troca de senha anualmente, que acontecerão na data de renovação do contrato.

- No primeiro acesso, o colaborador deve trocar a senha temporária.

- Em caso de dúvida sobre o sigilo da senha, o colaborador responsável pelo login e senha deverá solicitar a troca da mesma através da abertura de chamado técnico via Central de Serviços de TI.

- O login será bloqueado automaticamente após 5 (cinco) tentativas de acesso inválidas, ou seja, com a senha errada.

- O colaborador poderá acessar a rede e sistemas através de seus dispositivos, tendo direito de até 3 (três) acessos simultâneos.

- Os colaboradores poderão acessar a rede e os sistemas nos horários de trabalho, podendo ser desconectados fora desse período. Exceções deverão ser solicitadas pelos superiores imediatos através de chamado técnico.

- A reutilização de senhas obedecerá ao ciclo mínimo de 2 (duas) trocas, ou seja, as últimas duas senhas não poderão ser reutilizadas.

- As senhas deverão ter no mínimo 8 dígitos.

- Na criação ou troca de senhas, devem ser adotadas senhas fortes, respeitando as recomendações do Manual DTI-102. O manual está publicado no Portal de Gestão do SESI-SP e Portal de Gestão do SENAI-SP e pode ser acessado seguindo as instruções do item 1.7.2 “Informações adicionais”, página 7 da Política de Segurança da Informação, ou através do link documento.

## 3.3 Acesso lógico aos recursos corporativos

- O acesso lógico externo à rede corporativa é facultado aos colaboradores que estejam fora do local de trabalho (Unidade Corporativa ou Unidades Operacionais), em horário de expediente, e que necessitem de acesso pela Internet as informações e serviços do SESI-SP e SENAI-SP com fins estritamente profissionais.

Para maiores informações de como acessar os recursos corporativos externamente, consultar a “Norma de Acesso Externo Seguro (VPN) e Correio Eletrônico Corporativo”.

- O acesso aos recursos lógicos do SESI-SP e SENAI-SP deverá ser restringido enquanto o funcionário estiver em período de gozo das férias ou em licença, salvo funcionários que possuam cargos comissionados.

- Na hipótese de haver a necessidade do uso fora dos horários permitidos, essa condição deverá ser solicitada previamente pelo diretor da área/unidade operacional junto à Central de Serviços de TI.

## 3.4 Bloqueio da estação de trabalho

- Sempre que o colaborador se afastar de seu posto de trabalho é necessário bloquear a tela do microcomputador, a fim de evitar que pessoas não autorizadas manipulem os recursos habilitados (dados na rede, sistemas corporativos, correio eletrônico entre outros). Para maiores informações, consulte o manual DTI-104. O manual está publicado no Portal de Gestão do SESI-SP e Portal de Gestão do SENAI-SP e pode ser acessado seguindo as instruções do item 1.7.2 “Informações adicionais”, página 7 da Política de Segurança da Informação, ou através do link documento.

### 3.5 Exclusão do acesso

- A exclusão do colaborador dos sistemas informatizados do SESI-SP e SENAI-SP será realizada automaticamente, através de processo eletrônico instituído entre o DRH e a DTI, mediante a desvinculação do quadro de funcionários do SESI-SP e SENAI-SP.

- Para colaborador terceirizado, a solicitação da exclusão do acesso é responsabilidade do gestor e deverá ser solicitada através de chamado técnico via Central de Serviços de TI, gerado pela própria unidade de lotação do colaborador, após o final do contrato ou desvinculação do quadro de terceiros do SESI-SP e SENAI-SP.

# 3.8. Norma para Cópias de Segurança e Restauração

## 1. OBJETIVO

Fornecer instruções para o processo de cópia de segurança e restauração das informações, visando manter as informações relevantes ao pleno funcionamento das atividades do SESI-SP e SENAI-SP.

## 2. CAMPO DE APLICAÇÃO

Abrange a todos os colaboradores do SESI-SP e SENAI-SP.

## 3. CRITÉRIO DE UTILIZAÇÃO

- São executados periodicamente procedimentos de salvaguardas das informações geradas e armazenadas pelo SESI-SP e SENAI-SP, de forma a garantir o andamento das atividades realizadas pelos colaboradores em caso de perda parcial ou total de informações, seja por falha humana ou eletrônica.

- Fazem parte da rotina de backup os arquivos de:

  - ✓ Banco de dados;
  - ✓ Sistemas corporativos (programas e dados);
  - ✓ Informações armazenadas nos compartilhamentos de rede;
  - ✓ Imagem de máquinas hospedadas em nuvem pública;
  - ✓ Dados de sistemas e imagem de servidores hospedados em nuvem privada.

- Os requisitos das cópias de segurança e restauração são:
  - ✓ A lista de itens cujo backup deve ser feito com frequência inclui dados, arquivos de configuração e logs;
  - ✓ A frequência e abrangência das cópias de segurança estão organizadas da seguinte forma:

| Frequência | Unidade |
|---|---|
| Diárias | Corporativa e Operacionais |
| Semanais | |
| Mensais | |
| Anuais | Corporativa |

- ✓ Os recursos tecnológicos do SESI-SP e SENAI-SP deverão ser utilizados exclusivamente para atividades das instituições, dados ou arquivos que forem armazenados sem atender a esse requisito, não terão garantias quanto a sua confidencialidade, integridade e disponibilidade, podendo inclusive ser excluídos sem aviso prévio;
- ✓ Os arquivos corporativos devem ser armazenados na rede e não localmente;
- ✓ Informações armazenadas localmente, fora das unidades da rede, não possuem garantia de restauração (restore);
- ✓ É de responsabilidade do colaborador a realização do backup dos arquivos locais, HDs e dispositivos removíveis;
- ✓ As mídias de backup semanais, mensais e anuais devem ser acondicionadas em local seco, climatizado, seguro, restrito e distante o suficiente da unidade corporativa do SESI-SP e SENAI-SP, a fim de evitar que um mesmo desastre físico atinja simultaneamente os dados em utilização e o de backup;
- ✓ As mídias de backup devem ser transportadas de forma adequada, através de maletas especiais trancadas, visando garantir a proteção contra possíveis danos durante a locomoção;
- ✓ As fitas de backup devem ser devidamente identificadas com etiquetas e numeração sequencial;
- ✓ O tempo de vida e uso das mídias de backup deve ser monitorado e controlado pelos responsáveis, com o objetivo de excluir mídias que possam apresentar riscos de gravação ou de restauração decorrentes do uso prolongado, além do prazo recomendado pelo fabricante. Portanto, as mídias deverão ser descartadas em no máximo 2 (dois) meses antes do término de seu prazo de validade, conforme “Normas de Descarte de Mídias”;
- ✓ Os procedimentos de restauração das mídias de cópias de segurança devem ser verificados e testados conforme tabela abaixo e controlado conforme documento DTI-IS37-09. A instrução de serviço está publicada no Portal de Gestão do SESI-SP e Portal de Gestão do SENAI-SP e pode ser acessada seguindo as instruções do item 1.7.2 “Informações adicionais”, página 7 da Política de Segurança da Informação, ou através do link documento.

| Periodicidade | Quando? |
|---|---|
| Mensal | Primeira semana do mês |
| Anual | Primeiro trimestre do ano |

- ✓ As cópias de segurança bem como sua restauração devem ser feitas de modo a atender os requisitos do plano de recuperação de desastres do SESI-SP e SENAI-SP;
- ✓ Para formalizar o controle de execução de cópias e restauração, deverá haver um documento que registre este controle, conforme estabelecido pelo DTI-001. O manual está publicado no Portal de Gestão do SESI-SP e Portal de Gestão do SENAI-SP SP e pode ser acessado seguindo as instruções do item 1.7.2 “Informações adicionais”, página 7 da Política de Segurança da Informação ou através do link documento.

# 3.9. Norma para Uso do Correio Eletrônico Corporativo

## 1. OBJETIVO

Estabelecer regras para o uso adequado do serviço de correio eletrônico do SESI-SP e SENAI-SP.

## 2. CAMPO DE APLICAÇÃO

Abrange a todos os colaboradores do SESI-SP e SENAI-SP.

## 3. DEFINIÇÕES

As definições dos termos técnicos utilizados nesse documento podem ser consultadas no Glossário da Política de Segurança da Informação (PSI).

## 4. SERVIÇOS OFERECIDOS

• Os serviços de uso permitido pelo SESI-SP e SENAI-SP são:

- ✓ Correio eletrônico - Microsoft Office 365;
- ✓ Ferramenta de mensagem instantânea com funções de colaboração - Microsoft Lync ou Skype Corporativo;
- ✓ Disco virtual na nuvem - OneDrive.

## 5. CONDIÇÕES DE USO

• Não é permitido o uso dos serviços disponibilizados para:

1. Denúncias ou campanhas contra pessoas, autoridades constituídas, empresas, entidades, organizações e os poderes constitucionais;
2. Anúncios de compra e venda de produtos e serviços;
3. Propaganda de atividades pessoais e de participação em eventos socioculturais;
4. Atividades de caráter político-partidário;
5. Divulgações de mensagens de utilidade pública, feitas por colaboradores sem atribuição para tal;
6. Mensagens de autoajuda ou de cunho religioso;
7. Listas de adesão ou de manifestação de solidariedade, exceto as autorizadas pela Direção do SESI-SP e SENAI-SP;
8. Transportar arquivos de som e vídeo (MP3, MPEG, etc.) exceto quando atender as necessidades de serviço;
9. Mensagens sobre datas comemorativas, festividades e celebrações em geral, exceto as autorizadas pela Direção do SESI-SP e SENAI-SP;
10. Transmissão, recebimento e/ou armazenamento de mensagens contendo programas de computador que possam ser considerados nocivos ao ambiente de rede do SESI-SP e SENAI-SP;
11. Correntes e pirâmides que circulam na Internet, qualquer que seja sua finalidade;
12. Envio, transmissão ou distribuição para endereços externos ao SESI-SP e SENAI-SP, de informações de propriedade das instituições, tais como, mensagens internas, confidenciais, dados, segredos comerciais, financeiros ou tecnológicos, a não ser que expressamente autorizado pelo superior;
13. Violação do Código de Ética do SESI-SP e SENAI-SP;
14. Qualquer tipo de conteúdo sem vinculação estrita às atividades profissionais;
15. Veiculação de conteúdo ilícito como pedofilia, apologia à drogas e terrorismo;
16. Veiculação de conteúdo pornográfico.

# 6. CRITÉRIOS DE UTILIZAÇÃO

• O conjunto de ferramentas integrantes do Office 365 deve ser utilizado exclusivamente para as atividades profissionais e corporativas durante jornada pré-estabelecida em contrato de trabalho, salvo por autorização superior.

## 6.1 Solicitação de acesso

• A solicitação de acesso ao correio eletrônico deverá ser realizada através de chamado técnico via Central de Serviços de TI, conforme descrito no procedimento DTI-001. O manual está publicado no Portal de Gestão do SESI-SP e Portal de Gestão do SENAI-SP SP e pode ser acessado seguindo as instruções do item 1.7.2 “Informações adicionais”, página 7 da Política de Segurança da Informação ou através do link documento.

• As caixas de e-mail poderão ser funcionais ou nominais, conforme quadro abaixo. A definição de e-mail nominal e funcional pode ser consultada no item 5. Glossário.

• As caixas de e-mail funcionais deverão ser individuais.

**Quadro referencial para definição de tipos de e-mail**

| Categoria | E-mail Funcional | E-mail Nominal | Significado |
|---|---|---|---|
| Conveniados | Sim | Não | São profissionais que prestam serviços com a cooperação técnica do SENAI. Isso ocorre por meio de Convênios firmados com outras Entidades, empresas e até mesmo Prefeituras. Nestes casos o que regula a relação jurídica são os “Convênios de Cooperação Técnica”. |
| Estagiários | Sim | Sim | Não se aplica. |
| Terceirizados (Ex.: recepcionistas, etc.) | Sim | Sim | São profissionais que prestam serviços na qualidade de empregados de uma empresa prestadora de serviços. Esta empresa é contratada por meio de processo licitatório e o que regula a relação jurídica é o contrato de prestação de serviços firmado com as Entidades. |
| Prazo Determinado | Não | Sim | São profissionais que prestam serviços com data de término definida. |
| Prazo Indeterminado | Não | Sim | São profissionais que prestam serviços sem data de término definida. |
| Temporários (Com empresas interpostas – Ex.: Real Parceria) | Sim | Não | São profissionais contratados na forma da lei 6.019/74. Através de processo licitatório que compreende a contratação de empresa especificamente para serviços temporários. |

## 6.2 Criação de caixa de e-mail temporária

• A critério do SESI-SP e SENAI-SP poderá ser criada caixa de e-mail temporária destinadas a programas, projetos e eventos, estando o responsável desses, incumbido de solicitar a sua criação, backup e exclusão, quando da conclusão dos mesmos. Para isso, o responsável deve abrir chamado técnico via Central de Serviços de TI.

• O acesso a caixa de e-mail temporária deverá ser individual.

## 6.3 Uso dos grupos de correio eletrônico corporativo mantido pela diretoria de tecnologia da informação

- O envio de mensagens eletrônicas a grupos de usuários é prerrogativa dos níveis de gerência e superiores ou, excepcionalmente, dos demais técnicos, desde que autorizados, em cada situação, pelos primeiros.

- Respeitados os critérios acima, quando do endereçamento a Grupos de Usuários, os seguintes cuidados devem ser tomados:
  - ✓ As mensagens devem ser objetivas e o conteúdo relevante para todos os destinatários;
  - ✓ O remetente da mensagem deve avaliar criteriosamente quais grupos pode incluir no endereçamento e conhecer a composição de cada um. (Abrindo grupo na lista de endereços).

- Os grupos de usuário estão divididos conforme estrutura abaixo:

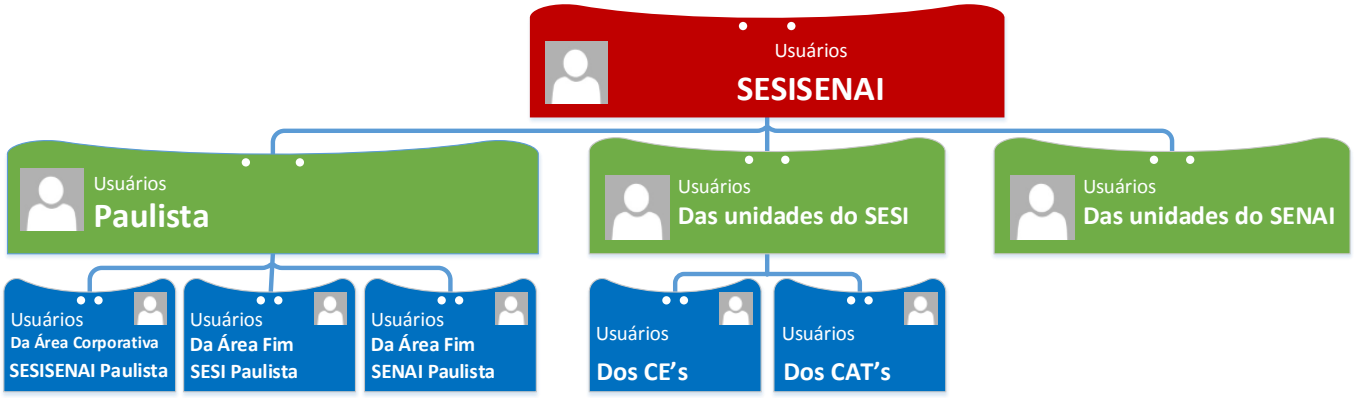



**Figura 3**: Estrutura de Grupos de Usuários

## 6.4 Criação de grupos de usuários locais

- A responsabilidade da criação de grupos localmente é do próprio colaborador, e deve ser feita somente quando se tratar de grupo específico não contemplado pelos grupos previamente cadastrados na lista de endereço corporativa administrada pela DTI.

## 6.5 Acesso à caixa de e-mail de outro colaborador

- O acesso às mensagens de Caixas de e-mail Nominais ou Funcionais de um colaborador será facultado mediante a autorização do Diretor Regional do SENAI-SP ou pelo Superintendente do SESI-SP.

## 6.6 Acesso à agenda de outro colaborador

- A disponibilidade a agenda eletrônica de um colaborador pode ser consultada pelos colaboradores que queiram agendar uma reunião com o mesmo.

## 6.7 Registro de acesso

- Os registros de acesso do sistema do Office 365 serão mantidos por no mínimo 6 (seis) meses com rastreabilidade de ações: data, hora de uso a partir de um determinado endereço IP.

## 6.8 Horário de acesso

- O horário permitido para acesso pode ser consultado no item da PSI de número 3.7 - Norma para Controle de Acesso Lógico, subitem “3.3 Acesso lógico aos recursos corporativos”.

## 6.9 Foto no perfil do Office 365

- O Código de Ética do SESI-SP e SENAI-SP, define que o colaborador deverá ter cuidado com suas atitudes e comportamento para que não coloque em risco a sua imagem pessoal e a das instituições, portanto, as fotos utilizadas no perfil do Office 365 deverão ser vestindo trajes formais e em ambiente de trabalho.

## 6.10 Meios de acesso às mensagens

- O acesso ao correio eletrônico do Office 365 pode ser feito via Web ou pelo cliente Microsoft Outlook.

## 6.11 Armazenamento das mensagens

- A capacidade de armazenamento da caixa de e-mail do usuário é de 50 gigabytes. Fica a critério do colaborador excluir as mensagens que não forem mais necessárias, porém deve-se ter ciência de que:
  - ✓ O tempo de retenção das mensagens excluídas referente as contas de colaboradores com cargos comissionados, é indeterminado desde que a pasta “itens excluídos” não seja esvaziada;
  - ✓ O tempo de retenção das mensagens excluídas referente aos demais colaboradores é de 30 dias desde que a pasta “itens excluídos” não seja esvaziada;
  - ✓ O sistema não permite backup em mídia das mensagens, portanto as mensagens excluídas serão mantidas no ambiente, na pasta “itens excluídos” conforme prazos informados acima. Após esse período, ou após a limpeza da pasta “itens excluídos”, as mensagens não poderão ser recuperadas.

## 6.12 Ferramenta Lync ou Skype Corporativo

- O Lync ou Skype corporativo são as ferramentas de mensagens instantânea oficiais do SESI-SP e SENAI-SP, sendo as únicas dessa categoria cujo uso é permitido:
  - ✓ Através de uma conta do SESI-SP e SENAI-SP;
  - ✓ Para comunicação com usuários que não são colaboradores do SESI-SP e SENAI-SP, desde que seja para atividades corporativas;
  - ✓ Por questão de segurança, as ferramentas não deverão ser utilizadas para trafegar arquivos e nem para compartilhamento de área de trabalho.

## 6.13 Ferramenta OneDrive

- Por questão de segurança, a ferramenta OneDrive não deverá ser utilizada para:
  - ✓ Publicar informações classificadas como confidencias;
  - ✓ Arquivos que contenham nudez;
  - ✓ Arquivos protegidos por leis de propriedade intelectual;
  - ✓ Compartilhar arquivos com usuários que não sejam colaboradores do SESI-SP e SENAI-SP.

## 6.14 Auditoria

- As ações executadas com as contas administrativas do Office 365 serão auditadas conforme Norma para Auditoria de TI, DTI-089. O manual está publicado no Portal de Gestão do SESI-SP e Portal de Gestão do SENAI-SP SP e pode ser acessado seguindo as instruções do item 1.7.2 “Informações adicionais”, página 7 da Política de Segurança da Informação através do ou através do link documento.

## 6.15 Retenção

- Conforme documento DTI-001, as informações do Office 365 deverão ser mantidas por 5 anos após o desligamento do colaborador. O procedimento está publicado no Portal de Gestão do SESI-SP e

Portal de Gestão do SENAI-SP e pode ser acessado seguindo as instruções do item 1.7.2 “Informações adicionais”, página 7 da Política de Segurança da Informação, ou através do link documento.

## 6.16 Regras para controle de lixo eletrônico (Antispam)

- É de responsabilidade do colaborador gerenciar a sua pasta de Lixo eletrônico (spams).
- Regras de AntiSpam para o Correio Eletrônico gerenciadas pela DTI:
  - ✓ DISCLAIMER: Aviso Legal de Isenção de Responsabilidade anexado no rodapé das mensagens enviadas pelos colaboradores do SESI-SP e SENAI-SP;
  - ✓ Liberação de Domínio: Regra criada para adicionar domínios confiáveis (ex: empresas parceiras, clientes). As mensagens enviadas pelos domínios são consideradas confiáveis, e não são retidas na quarentena (Lixo Eletrônico);
  - ✓ Liberar e-mails: Regra criada para adicionar remetentes (e-mails) confiáveis. As mensagens enviadas pelos remetentes são consideradas confiáveis, e não são retidas na quarentena (Lixo Eletrônico);
  - ✓ Bloqueio de Domínio: Regra criada para bloqueio de domínios indesejados (domínios fora da organização);
  - ✓ Bloqueio de e-mail: Regra criada para bloqueio de remetentes indesejados (e-mails fora da organização);
  - ✓ Bloqueio de Anexo – Executáveis: Regra criada para bloqueio de arquivos anexos executáveis (dll,pif,vbs,scr,exe,bat);
  - ✓ Bloqueio de Anexo - Compactados: Regra criada para bloqueio de arquivos anexos compactados (.zip, .rar, .arj);
  - ✓ Bloqueio de Subject: Regra criada para bloqueio de mensagens enviadas por remetentes externos (fora da organização) por Subject (Assunto);
  - ✓ Bloqueio de Body: Regra criada para bloqueio de mensagens enviadas por remetentes externos (fora da organização) por Body (Corpo da Mensagem);
- Exceções devidamente autorizadas pelo gestor responsável, deverão ser tratadas através de chamados técnicos junto a Central de Serviços de TI.

## 6.17 Criação de Assinaturas

- As assinaturas de correio eletrônico devem respeitar as instruções contidas no Manual para geração de arquivos para correio DTI-038. O manual está publicado no Portal de Gestão do SESI-SP e Portal de Gestão do SENAI-SP SP e pode ser acessado seguindo as instruções do item 1.7.2 “Informações adicionais”, página 7 da Política de Segurança da Informação através do ou através do link documento.

## 6.18 Procedimentos operacionais da ferramenta

- Os procedimentos operacionais da ferramenta podem ser encontrados nos manuais DTI-116, DTI-117 e DTI-118 publicados no Portal de Gestão do SESI-SP e Portal de Gestão do SENAI-SP e seu acesso poderá ser realizado através dos “links” constantes no item 4 desse documento ou lista abaixo:
  - DTI-116;
  - DTI-117;
  - DTI-118.

## 6.19 Envio de e-mail em massa

- Não é permitido utilizar o Office 365 para o envio de e-mail em massa, que ultrapasse o número de 100 (cem) e-mails. Em caso de necessidade do envio para divulgação ou publicidade das entidades, deve ser utilizado ferramenta disponibilizada pela DTI.

- Esta ação visa tratar a inserção dos domínios SESI-SP e SENAI-SP em blacklists dos provedores de internet e podem prejudicar a utilização dos serviços de e-mail.

# 3.10. Norma para Descarte de Mídias

## 1. OBJETIVO

Estabelecer normas para o descarte adequado e seguro das mídias do SESI-SP e SENAI-SP, quando as mesmas não forem mais necessárias.

## 2. CAMPO DE APLICAÇÃO

Abrange a todos colaboradores do SESI-SP e SENAI-SP.

## 3. CRITÉRIO DE UTILIZAÇÃO

- Quando uma mídia não for mais utilizada, é necessário o descarte seguro da mesma, para minimizar o risco de acesso não autorizado de informações.

- O lixo tecnológico deve receber destinação adequada, que não provoque danos ou impactos negativos ao meio ambiente e à sociedade.

- Os requisitos do documento DITEC-034, devem ser atendidos. O manual está publicado no Portal de Gestão do SESI-SP e Portal de Gestão do SENAI-SP SP e pode ser acessado seguindo as instruções do item 1.7.2 “Informações adicionais”, página 7 da Política de Segurança da Informação ou através do link documento.

- Todo o descarte de mídias deve ser registrado no formulário “DTI-109-FR001 Controle de Descarte de Mídias”, os campos do formulário deverão ser preenchidos e o arquivamento do formulário deverá ser realizado e controlado por cada unidade. O manual DTI-109, explica como fazê-lo e detalha o descritivo de todos os requisitos necessários. O formulário e o manual estão publicados no Portal de Gestão do SESI-SP e Portal de Gestão do SENAI-SP e podem ser acessados seguindo as instruções do item 1.7.2 “Informações adicionais”, página 7 da Política de Segurança da Informação, ou através do link documento.

### 3.1 Requisitos gerais

- As embalagens deverão ser separadas da (s) mídia (s).

- As embalagens que possuírem informações e não comprometerem os processos a que serão envolvidos, poderão ser reutilizadas, caso contrário, deverão ser descartadas de acordo com o programa de coleta seletiva.

### 3.2 CD/DVD

- Os CDs e DVDs deverão ser inutilizados riscando-os ou de forma que as informações se tornem irrecuperáveis.

### 3.3 Discos rígidos

- Os discos rígidos (HD) deverão ser formatados e ser destruídos fisicamente ou passar por um processo de desmagnetização antes de serem descartados, de forma que as informações fiquem irrecuperáveis.

### 3.4 Fitas magnéticas

- As fitas magnéticas deverão ter seus materiais plásticos (estojo, rolo, invólucro, etc.) separados da fita e essa cortada em várias partes ou de forma que as informações fiquem irrecuperáveis.

### 3.5 Pendrives

- Os pendrives e outros dispositivos removíveis deverão, quando possível, serem formatados e destruídos de forma que as informações fiquem irrecuperáveis.

### 3.6 Documentos em papel

- Os documentos em papel classificados como confidenciais ou internos, deverão ser fragmentados em pedaços ilegíveis de forma que as informações se tornem irrecuperáveis. Recomenda-se o uso de fragmentadora de papel.

  *NOTA:* Por questões legais, mesmo que digitalizado ou microfilmado, recomenda-se que nenhum documento "original" seja destruído, sem que haja uma consulta prévia junto a Diretoria Jurídica do SESI-SP e SENAI-SP quanto a legalidade da cópia do original.

# 3.11. Norma para o Desenvolvimento de Sistemas de Informação

## 1. OBJETIVO

Regulamentar a segurança para o processo de desenvolvimento e manutenção de sistemas do SESI-SP e SENAI-SP.

## 2. CAMPO DE APLICAÇÃO

Abrange aos colaboradores da Diretoria de Tecnologia da Informação (DTI) do SESI-SP e SENAI-SP.

## 3. CRITÉRIO DE UTILIZAÇÃO

### 3.1 Desenvolvimento

- Os conceitos de segurança da informação devem estar presentes em todas as fases do desenvolvimento de sistemas, desde a reunião inicial do projeto, viabilidade, até a fase de entrega.

- Os controles de segurança devem ser concebidos junto com o sistema, e não implantados após o sistema ficar pronto.

- A área de upload de arquivos dos sistemas deve estar localizada em um diretório isolado que não seja acessado pelo lado cliente.

- Os sistemas devem validar o tipo de arquivo durante o processo de upload.

- Todos os campos de entrada de dados dos sistemas devem ser validados, de forma a impedir a entrada de dados indesejados e de injeção de comandos nos sistemas.

- Todos os sistemas cujo conteúdo da informação esteja classificado como confidencial, devem obrigatoriamente possuir um mecanismo de autenticação e identificação.

- Após 5 (cinco) tentativas inválidas de autenticação nos sistemas, o perfil deve ser bloqueado.

- A autenticação dos sistemas deve ser integrada com o Active Directory (AD) existente. Em caso de alguma limitação técnica que impossibilite a integração do sistema com o AD, a autenticação deverá ser realizada por usuário único, o login e senha do colaborador deverá ser armazenado, controlado e trocado semestralmente.

- Todas as páginas que possuem formulário de cadastro deverão confirmar os dados informados pelo colaborador. Essa confirmação deverá ser realizada através de um e-mail a ser enviado para o endereço eletrônico fornecido pelo colaborador durante o processo de cadastro. Esse e-mail deverá conter um link de confirmação e somente após a confirmação do usuário, esse formulário deverá ser considerado válido.

- Todas as páginas da aplicação que contenham formulários de cadastro web ou acesso às informações cadastrais do usuário deverão possuir um código “captcha”, a fim de evitar o envio de dados por robôs.

- Caso a aplicação utilize e-mail para contato com o usuário, deve utilizar apenas servidores SMTP “autenticados”, evitando a prática de spam.

- Os códigos de programação .NET devem ser convertidos em código ASCII do HTML, a fim de Impossibilitar que um atacante identifique a linguagem de programação e descubra vulnerabilidades de segurança que a linguagem possui.

- Os códigos das aplicações devem funcionar sem a função “parent path” do IIS.

- As páginas de erros de todos os sistemas devem ser customizadas e genéricas, com a finalidade de impossibilitar de que os atacantes obtenham a versão do sistema operacional, servidor web e outros dados que possam ser explorados em caso de vulnerabilidades de segurança.

- Deve ser gerado log para todos os sistemas, coletando minimamente informações sobre quem (login e IP), quando (dia/hora/minutos padrão UTC), o que foi acessado (sistema/banco/tabela/registro) e o tipo de transação (remoção/modificação/leitura) realizada pelo colaborador.

- Os códigos de todos os sistemas devem ser documentados, para que futuras alterações sejam realizadas de forma fácil e acessível a qualquer desenvolvedor.

- A camada de front-end dos sistemas deve ser entregue de modo que o usuário não consiga identificar em qual linguagem o sistema foi desenvolvido.

- Não devem estar na produção os sistemas com “maintenance hook”.

- O acesso aos códigos fontes deve ser controlado e restrito aos desenvolvedores envolvidos, em seus respectivos projetos.

- Ambientes de testes e de produção devem ser isolados entre si, para evitar o risco de acessos ou modificações não autorizadas, conforme descrito no DTI-001. O manual está publicado no Portal de Gestão do SESI-SP e Portal de Gestão do SENAI-SP SP e pode ser acessado seguindo as instruções do item 1.7.2 “Informações adicionais”, página 7 da Política de Segurança da Informação ou através do link documento.

- Recomenda-se que testes em ambiente de desenvolvimento sejam realizados apenas com bases contendo dados fictícios.

- Cabe ao desenvolvedor informar a Supervisão de Implantação e a Supervisão de Qualidade e Segurança de TI se a aplicação será publicada na internet e assim sendo, deverá informar se será para uso administrativo, educacional ou misto. Sendo para uso administrativo, a mesma será acessada somente através do portal VPN SSL, que possui uma limitação total de 2000 conexões simultâneas.

- O desenvolvedor deve informar a Supervisão de Implantação e a Supervisão de Qualidade e Segurança de TI sobre a expectativa de acessos simultâneos na aplicação e de transição de dados em MB, para gestão de capacidade do firewall e do VPN SSL, de forma a definir a estratégia de implantação da aplicação e avaliar a necessidade de novas aquisições e capacidades dos equipamentos envolvidos.

- O desenvolvedor deve informar a Supervisão de Suporte de TI se será necessária rotina de backup de dados na aplicação e a sua periodicidade.

- O desenvolvedor deve informar a Supervisão de Implantação, Supervisão de Qualidade e Segurança de TI e a Supervisão de Suporte de TI se o novo sistema é um serviço crítico de TI. Sendo, deverá passar por análise de risco, possuir um plano de recuperação e fazer parte da relação de serviços críticos de TI, DTI-044 ou através do link documento.

## 3.2 Segurança da Informação

- Todas as aplicações web que possuem função de autenticação devem possuir certificado HTTPS para conferir maior segurança na troca de dados entre usuário e servidor.

- Realizar validação de expressões regulares no firewall de entrada da rede de forma a inibir ataques XSS e SQL Injection. A partir da validação de expressões regulares, os códigos SQLs podem ser eliminados antes de chegar à aplicação.

- Evitar a criação de NAT de aplicação e utilizar um servidor que já possua NAT cadastrado, a fim de reduzir o processamento do firewall e utilizar eficientemente o número de IPs válidos do SESI-SP e SENAI-SP.

- É necessário realizar testes de segurança da informação nos sistemas antes de serem publicados no ambiente de produção.

## 3.3 Infraestrutura

- Deve atribuir REMOTEONLY na opção MODE ATTRIBUTE do arquivo web.config local, de modo a apresentar mensagem de erro apenas para os usuários que se encontram na mesma rede do servidor, ocultando-as caso o acesso seja realizado de forma remota. Isso inibe que atacantes explorem vulnerabilidades de segurança ou falhas de programação.

# 3.12. Norma para o Gerenciamento de Contas Administrativas

## 1. OBJETIVO

Estabelecer normas para o gerenciamento adequado de contas administrativas da rede do SESI-SP e SENAI-SP.

## 2. CAMPO DE APLICAÇÃO

Abrange aos colaboradores da Diretoria de Tecnologia da Informação (DTI) do SESI-SP e SENAI-SP.

## 3. CRITÉRIO DE UTILIZAÇÃO

- Os administradores de rede devem possuir duas contas: uma para tarefas rotineiras e outra para administração de servidores.

- Sempre que possível, as contas administrativas não devem ser usadas diretamente. O administrador deve entrar no sistema usando sua conta pessoal e a partir dela realizar suas tarefas, usando os privilégios mais elevados apenas quando estritamente necessário.

- Na criação ou troca das senhas de contas administrativas, devem ser adotadas senhas fortes.

- As contas administrativas devem ser auditadas periodicamente.

- Manter lista atualizada contendo os colaboradores autorizados a utilizarem as contas administrativas.

- O pedido de concessão de contas com poderes administrativos deve ser feito através de chamado técnico via Central de Serviços de TI, com as seguintes informações:
  - ✓ Nome do colaborador de TI que terá acesso à conta administrativa;
  - ✓ Nome e autorização do supervisor responsável;
  - ✓ Justificativa.

- A concessão de contas administrativas poderá ser feita somente após prévia autorização da Supervisão de Qualidade e Segurança de TI.

- As senhas de contas administrativas devem ser trocadas anualmente.

- Deve excluir as credenciais de acesso administrativo aos ativos de TI quando do desligamento do colaborador, atualizando a lista de colaboradores com contas administrativas.

# 3.13. Norma para Homologação de Softwares

## 1. OBJETIVO

Estabelecer critérios de homologação de software do SESI-SP e SENAI-SP.

## 2. CAMPO DE APLICAÇÃO

Abrange a todos os colaboradores do SESI-SP e SENAI-SP.

## 3. CRITÉRIO DE UTILIZAÇÃO

- Os softwares instalados e executados em qualquer recurso de informática do SESI-SP e SENAI-SP devem ser devidamente licenciados e previamente homologados pela DTI.

- Cada software deve reunir a documentação para a sua instalação e configuração.

### 3.1 Softwares homologados

- Os softwares homologados são aqueles cujo funcionamento no ambiente operacional de informática do SESI- SP e SENAI-SP foi aprovado e está relacionado na “Lista de softwares homologados do SESI-SP e SENAI-SP” que se encontra publicada na http://intranet.sesisenaisp.org.br, seção de Downloads, Diretoria de Tecnologia da Informação, Documentos, Relação de Softwares Homologados.

- O fato, de um software estar relacionado na lista de softwares homologados, não atribui a liberação e autorização para instalação e utilização do mesmo. Para a instalação de um software homologado, o colaborador deverá solicitar autorização ao seu superior imediato, e se autorizado, abrir um chamado técnico via Central de Serviços de TI, para que técnicos habilitados pela DTI avaliem e realizem a instalação.

### 3.2 Softwares não homologados

- Não está autorizado o uso de softwares que não estejam contidos na relação de softwares homologados, independente da sua modalidade de licenciamento (freeware, open source e shareware), sendo responsabilidade do Diretor da área ou Unidade a permissão do seu uso.
- Para a homologação de um software, o colaborador deverá solicitar autorização ao seu superior imediato, e se autorizado, abrir um chamado técnico via Central de Serviços de TI.

# 3.14. Norma para Proteção Contra Códigos Maliciosos

## 1. OBJETIVO

Estabelecer normas para a proteção dos recursos de Tecnologia da Informação do SESI-SP e SENAI-SP contra ação de códigos maliciosos, programas impróprios e acesso não autorizado.

## 2. CAMPO DE APLICAÇÃO

Abrange a todos os colaboradores do SESI-SP e SENAI-SP.

## 3. CRITÉRIO DE UTILIZAÇÃO

- Os recursos de TI do SESI-SP e SENAI-SP devem estar providos de sistemas de detecção e bloqueio de códigos maliciosos, prevenção e detecção de acesso não autorizado, tais como programas de antivírus, programas de análise de conteúdo de correio eletrônico, e firewall.

- O sistema de antivírus deve realizar varreduras semanais nas estações e servidores, a fim de identificar e eliminar códigos maliciosos.

- As atualizações do sistema de antivírus nas estações devem ser feitas de forma transparente ao colaborador e ocorrer em até 5 (cinco) dias após a disponibilização do fabricante.

- Os servidores da Unidade Corporativa deverão estar com o sistema de antivírus atualizado em até 3 (três) dias após disponibilização do fabricante.

- O serviço de proteção em tempo real não pode ser desabilitado nas estações ou servidores de rede.

- Os serviços de IPS (Intrusion Prevention System) e firewall devem estar habilitados em todas as estações do SESI-SP e SENAI-SP.

- Todo dispositivo de armazenamento (pendrive, cdrom, hd removível e etc.), devem ser varridos, para detecção de vírus, antes do seu uso efetivo em rede.

- Todo recurso ligado na rede, ou seja, que possuir acesso aos arquivos e pastas corporativas, deverá estar provido do software de antivírus oficial do SESI-SP e SENAI-SP e estar com a lista de vírus atualizada. O manual para verificação da lista de vírus é o DTI-101. O manual está publicado no Portal de Gestão do SESI-SP e Portal de Gestão do SENAI-SP e pode ser acessado seguindo as instruções do item 1.7.2 “Informações adicionais”, página 7 da Política de Segurança da Informação, ou através do link documento.

# 3.15. Norma para Uso da Rede de Comunicação de Dados

## 1. OBJETIVO

Garantir o uso adequado da rede do SESI-SP e SENAI-SP, de forma a minimizar riscos e impactos.

## 2. CAMPO DE APLICAÇÃO

Abrange a todos os colaboradores do SESI-SP e SENAI-SP.

## 3. CRITÉRIOS DE UTILIZAÇÃO

- As solicitações para adição, instalação e manutenção dos recursos de rede de dados deverão ser feitas através de abertura de chamado técnico via Central de Serviços de TI.

- A Diretoria de Tecnologia da Informação define perfis padrões de acesso e compartilhamento dos recursos e serviços de Tecnologia da Informação, de acordo com as necessidades profissionais dos colaboradores e prestadores de serviços do SESI-SP e SENAI-SP. Tais perfis podem ser modificados com base em justificativa técnica encaminhada formalmente pela área interessada à DTI.

- Todo recurso ligado na rede, ou seja, que possuir acesso aos arquivos e pastas corporativas, deverá estar provido do software de antivírus oficial do SESI-SP e SENAI-SP e estar com a lista de vírus atualizada. O manual para verificação da lista de vírus é o DTI-101. O manual está publicado no Portal de Gestão do SESI-SP e Portal de Gestão do SENAI-SP SP e pode ser acessado seguindo as instruções do item 1.7.2 “Informações adicionais”, página 7 da Política de Segurança da Informação, ou através do link documento.

- Equipamentos pessoais ou de visitantes, não poderão ter acesso aos arquivos e pastas corporativas do SESI-SP e SENAI-SP. Para maiores informações, consulte a “Norma para uso de Dispositivos Móveis”.

- É vedada a conexão de qualquer outro tipo de rede ou provedores externos de acesso à Internet ou à rede de comunicação de dados, sem o conhecimento e autorização da DTI.

### 3.1 Uso da Rede Wireless

- A conexão com a rede wireless está sendo disponibilizada somente dentro das dependências físicas das Unidades do SESI-SP e SENAI-SP e em área delimitada.

- Todos os colaboradores e dispositivos que se conectarem à rede wireless devem ser autenticados e identificados.

- Não é permitida a utilização e conexão da rede wireless por terceiros (fornecedores ou visitantes), sem o prévio conhecimento, acompanhamento e autorização da diretoria da área ou unidade. Existindo a autorização, a habilitação deverá ser realizada através da abertura de chamado técnico via Central de Serviços de TI e o tipo de utilização liberada será a de conexão com a Internet, através de login de acesso do responsável da área/unidade que estiver acompanhando o terceiro.

- O acesso a dados corporativos só será autorizado mediante a solicitação via chamado à Central de Serviços de TI, realizada pelo responsável da área/unidade solicitante.

- É vedada a instalação de qualquer equipamento do tipo “Access Point”, “3G” e “4G” ou similar em qualquer uma das áreas ou unidades do SESI-SP e SENAI-SP sem o conhecimento e autorização da DTI, que deverá ser obtida através de abertura de chamado técnico via Central de Serviços de TI, onde serão verificadas as seguintes características: funcionalidade, segurança e disponibilidade de

recurso.

### *3.1.1 Configuração dos dispositivos de rede sem fio*

- ✓ As senhas padrão de administração dos dispositivos de rede sem fio devem ser trocadas por senhas fortes, conforme recomendações do Manual DTI-102. O manual está publicado no Portal de Gestão do SESI-SP e Portal de Gestão do SENAI-SP SP e pode ser acessado seguindo as instruções do item 1.7.2 “Informações adicionais”, página 7 da Política de Segurança da Informação ou através do link do documento.

- ✓ A rede sem fio deve ser configurada para usar apenas o protocolo de comunicação WPA2;
- ✓ O Algoritmo de criptografia usado com o WPA2 deve ser o AES;
- ✓ A autenticação PIN deve estar desabilitada;
- ✓ É recomendado desabilitar o broadcast de SSID;
- ✓ Deve existir rastreabilidade nas ações executadas na rede sem fio;
- ✓ As senhas dos dispositivos devem ser trocadas no momento da instalação e depois periodicamente
- ✓ Filtros de endereço “MAC” devem ser aplicados sempre que os dispositivos de rede sem fio tiverem clientes fixos.

## 3.2 Rede 3G/4G

- O modem USB oferece conexão 3G/4G para os colaboradores que necessitem acessar remotamente a rede corporativa do SESI-SP e SENAI-SP para realizar suas atividades profissionais.

- Para adquirir o modem USB 3G/4G, os colaboradores, mediante autorização do superior imediato, devem abrir chamado técnico via Central de Serviços de TI. É expressamente proibida a utilização do modem USB 3G/4G do SESI-SP e SENAI-SP em equipamentos que não sejam de propriedade das entidades.

## 3.3 Locais de Rede

- Os dados corporativos e de trabalho devem ser armazenados nas unidades compartilhadas da rede, sendo assim possível recuperar os dados perdidos, graças ao backup automatizado. No caso em que os dados estiverem armazenados em unidades locais, caberá ao próprio colaborador do microcomputador a realização do backup de seus documentos.

- Não é permitido o compartilhamento local do computador.

- As unidades compartilhadas da rede devem ser utilizadas para armazenamento de dados de fins estritamente profissionais, nos seguintes tipos:
  - ✓ Apresentações e textos;
  - ✓ Áudio (MP3, MP4, WAV, entre outros);
  - ✓ Imagens (JPG, BMP, entre outras);
  - ✓ Softwares (aplicativos);
  - ✓ Vídeos (AVI, MPEG, entre outros).

- Durante o processo de manutenção ou auditoria das unidades compartilhadas de rede, a DTI providenciará:
  - ✓ Relação por nome em uma tabela, que será enviada à chefia direta do colaborador;
  - ✓ Posterior remoção dos arquivos nas unidades compartilhadas, caso não existam justificativas autorizadas.

## 3.4 Distribuição dos compartilhamentos de rede

- A organização em pastas e o gerenciamento das informações armazenadas em compartilhamentos públicos são atribuições de cada diretoria de área ou unidade.

- Os limites definidos de espaço poderão ser alterados para mais ou para menos de acordo com necessidade técnica.

- Alterações individuais de aumento de limites poderão ser solicitadas através da abertura de chamado técnico via Central de Serviços de TI, sendo avaliadas tecnicamente e autorizadas caso não haja restrições.

**Unidade Corporativa**

| Letra | Descrição | Limite definido |
|---|---|---|
| **F:** | Unidade de armazenamento dos sistemas corporativos compartilhados. | Sem limite |
| **T:** | Unidade de armazenamento de informações públicas para a diretoria. Cada diretoria possui uma exclusiva | Sem limite |
| **S:** | Unidades de armazenamento de informações públicas para as divisões das diretorias. Cada divisão da diretoria possui uma exclusiva. | Sem limite |
| **P:** | Unidade de armazenamento de informações públicas das diretorias. Todas as diretorias veem as mesmas informações. | Sem limite |
| **U:** | Unidade de armazenamento de informações individuais. Cada usuário possui uma exclusiva | 20mb |

**Unidade Operacional do SESI-SP e SENAI-SP**

| Letra | Descrição | Limite definido |
|---|---|---|
| **F:** | Unidade de armazenamento dos sistemas da unidade compartilhados. | Sem limite |
| **T:** | Unidade de armazenamento das informações públicas por grupo de trabalho da unidade. | Sem limite |
| **U:** | Unidade de armazenamento de informações individuais. Cada usuário possui uma exclusiva. | 20mb |

## 3.5 Solicitação de Acesso

### *3.5.1 Login*

✓ As solicitações de acesso à rede deverão ser realizadas através de chamado técnico via Central de Serviços de TI.

### *3.5.2 Acesso às pastas e arquivos do local de rede de outro usuário*

✓ O acesso às pastas e arquivos armazenados na unidade de armazenamento de informações individuais (U:) de outro usuário, será facultada mediante a autorização da Diretoria Regional do SENAI-SP ou pelo Superintendente do SESI-SP.

# 3.16. Norma para Servidores de Rede

## 1. OBJETIVO

Estabelecer diretrizes no que se refere aos servidores de Tecnologia da Informação do SESI-SP e SENAI-SP.

## 2. CAMPO DE APLICAÇÃO

Abrange aos colaboradores da Diretoria de Tecnologia da Informação (DTI) do SESI-SP e SENAI-SP.

## 3. CRITÉRIO DE UTILIZAÇÃO

- Os relógios de todos os servidores e sistemas do SESI-SP e SENAI-SP devem estar sincronizados com o relógio do Observatório Nacional. Para isso, deve-se utilizar o protocolo de sincronização de relógios (NTP – Network Time Protocol).

- Os relógios devem estar ajustados na hora padrão de Greenwich (GMT), sendo o fuso horário configurado adequadamente.

- Os logs gerados devem ser armazenados nos sistemas por no mínimo 45 (quarenta e cinco) dias.

- Os logs dos sistemas de RH e Financeiros que deverão ser mantidos por no mínimo 5 (cinco) anos, podendo ser armazenados no próprio sistema, fitas ou discos.

- Os servidores devem possuir, no mínimo, duas partições, sendo uma para o sistema operacional e outra para os sistemas.

- Deve haver uma política de tolerância a falhas RAID-1.

- Todos os patchs de segurança referentes ao sistema operacional e seus aplicativos devem ser aplicados.

- Todos os servidores devem estar com o cliente de antivírus oficial do SESI-SP e SENAI-SP instalado e atualizado.

- O host IPS deve ser instalado e configurado, de modo a garantir somente a execução de aplicações mapeadas no servidor.

- O filtro de pacotes deve ser habilitado, deixando aberta somente as portas usadas pelo servidor em seu processo de comunicação com a rede.

- As permissões no servidor devem ser concedidas seguindo as diretrizes da Política de Segurança da Informação.

- Os servidores com aplicações web publicadas devem ser isolados através de estrutura DMZ separada da rede administrativa, a fim de preservar os demais servidores e aplicações que se encontram na rede administrativa do SESI-SP e SENAI-SP.

- Deve haver documentação para instalação e configuração dos sistemas presentes nos servidores, detalhando os componentes a serem instalados e todas as modificações necessárias na sua configuração.

- Os serviços que não estão em uso devem ser desativados.

## 3.1 Servidores Windows

- Em servidores Windows, o sistema de arquivos deve ser o NTFS.

- Os servidores Windows devem estar com todas as versões do Service Pack instaladas.

- Deve ser utilizado o Internet Information Server (IIS) versão 7 ou superior – devidamente configurado – ou executar o IIS Lockdown para automatizar a configuração de outras versões de IIS, fornecendo maior segurança ao servidor web onde a aplicação será hospedada.

- Em servidores Windows, a conta “convidado” deve ficar desabilitada e a conta “administrador” deve ser renomeada.

- Todas as recomendações apresentadas pelo software Microsoft Baseline Security Analyzer (MBSA) da Microsoft nos servidores da DMZ devem ser implantadas e mantidas atualizadas, a fim de fornecer maior segurança ao sistema operacional e aos aplicativos instalados no servidor e suportados pela Microsoft.

- Em servidores Windows, as permissões em pastas devem ser concedidas usando a estratégia AGLP da Microsoft.

## 3.2 Servidores Linux

- Em servidores Linux, o sistema de arquivos deve ser o ext3.

- Em servidores Linux, as aplicações e serviços devem executar como chroot.

- Sempre que possível, em servidores Linux deve ser utilizado o comando “sudo” ao invés de acessar como root para executar as tarefas do servidor.

- Em servidores Linux, o acesso via “sudo” deve garantir que o colaborador acesse apenas as informações e os recursos necessários à sua atividade.

## 3.3 Servidores Virtuais

- A camada de Hypervisor deve estar protegida por sistema de antivírus e host IPS.

- Maquinas virtuais da DMZ devem ser hospedadas em hosts físicos separados dos hosts físicos da LAN.

## 3.4 Provedores de nuvens pública e privada que hospedam servidores do SESI-SP e SENAI-SP

- Todos os aspectos que envolvem segurança e privacidade de dados devem estar presentes no planejamento do projeto.

- Deve ser mantida rastreabilidade nos sistemas de informação hospedados em nuvens observando a lei 12.965 (Marco civil da internet) e demais aspectos legais e necessidades do SESI-SP e SENAI-SP.

- Caso existam servidores que precisem ser expostos na internet, uma zona desmilitarizada deve ser criada para hospeda-los separadamente de servidores de rede local.

- Somente poderão ser contratados provedores de nuvens cujo o contrato especifique foro Brasileiro para resolução de questões judiciais.

- O provedor de nuvem não deverá hospedar dados em países cujo acesso aos mesmos pode ser feito pelo governo local sem a necessidade de autorização do proprietário ou mandato judicial.

- No contrato de prestação de serviços não poderá conter uma clausula explicita apontando o provedor de nuvem como dono da informação.

- O provedor de nuvem deve ter certificações reconhecidas no mercado que ateste suas premissas básicas de segurança: climatização, controle de acesso, sistema de combate ao incêndio a gás F-200 ou similar, cabeamento estruturado, instalações e proteções elétricas adequadas, cabeamento estruturado e demais boas práticas de mercado.

- A comunicação entre o cliente e provedor de nuvem deverá ser criptografada através de um algoritmo avaliada como “uso aceitável” pelo NIST (National Institute of Standards Technology).

- O provedor de serviço de nuvem deverá possibilitar o uso de uma ferramenta de backup em nuvem bem como o download de todos os dados nela armazenados.

- As estratégias de backup e retenção dos backups dos dados hospedados em provedores de nuvens estão descritas na norma para cópias de segurança e restauração que fazem parte da PSI.

- O provedor de nuvem deverá possibilitar o controle e gerenciamento de portas de comunicação do protocolo de rede TCP/IP.

- O provedor de nuvem deverá permitir a instalação ou a contratação de um serviço de Antivírus para os ativos de informação nas nuvens.

- O provedor de nuvem deverá permitir a instalação ou a contratação de um serviço de IPS (Intrusion Prevention System) para os ativos de informação nas nuvens.

- O provedor de nuvem deverá permitir a instalação ou a contratação de um serviço de WAF (Web Application Firewall) para os ativos de informação nas nuvens.

- O provedor de nuvem deverá permitir a instalação ou a contratação de um serviço contra-ataques de negação de serviço distribuído.

- No contrato de prestação de serviços de nuvem privada, recomenda-se que haja uma clausula exigindo segmentação física do ambiente contratado.

- O provedor de serviço de nuvem privada deverá disponibilizar uma equipe comercial e uma equipe técnica para atender as demandas do SESI-SP e SENAI-SP.

- O provedor do serviço de nuvem privada deverá apresentar relatórios mensais cobrindo os principais pontos sobre o serviço, como ataques bloqueados, disponibilidade do ambiente e demais pontos relevantes conforme escopo do contrato.

- O responsável pela implantação ou seus superiores podem autorizar a inclusão de uma conta com “privilégios administrativos” na nuvem pública.

- Administradores da nuvem pública devem ser cadastrados através de contas cujo domínio pertença ao SESI-SP e SENAI-SP ou contrato de apoio pertinente (não podem ser usados domínios gratuitos como Gmail e Hotmail).

## 3.6 Perímetro da DMZ

- Apenas sistemas de uso externo podem ser publicados na DMZ.
- Antes da publicação de um sistema, o mesmo deve ser submetido a uma análise de vulnerabilidade.
- Os sistemas web publicados na Internet devem estar protegidos pelo WAF.
- Recomenda-se que o perímetro deve estar protegido contra-ataques de negação de serviço distribuído.

# 3.17. Norma para Uso de Dispositivos Móveis

## 1. OBJETIVO

Estabelecer o uso adequado e seguro dos dispositivos móveis no ambiente do SESI-SP e SENAI-SP.

## 2. CAMPO DE APLICAÇÃO

Abrange a todos os colaboradores do SESI-SP e SENAI-SP.

## 3. CRITÉRIO DE UTILIZAÇÃO

### 3.1 Dispositivos móveis corporativos

- Dispositivo móvel corporativo, é o equipamento eletrônico móvel de propriedade do SESI-SP e SENAI-SP, entregue aos colaboradores para uso exclusivo em suas funções.

- O SESI-SP e SENAI-SP, 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.

- O suporte técnico aos dispositivos móveis de propriedade do SESI-SP e SENAI-SP e aos seus usuários deve ser dar através da abertura de chamado técnico via Central de Serviços.

- Todos os dispositivos móveis corporativos, com exceção de equipamentos da Apple que utilizem o sistema operacional iOS, devem estar com sistema de antivírus oficial instalado e configurado para atualização automática.

- Todo colaborador deverá utilizar senhas de bloqueio automático para seu dispositivo móvel, estando de acordo com a norma de controle de acesso lógico.

- Não deverão ser realizadas, alterações de configuração dos sistemas operacionais dos equipamentos de propriedade do SESI-SP e SENAI-SP, em especial os referentes à segurança, sem a devida comunicação e autorização da Diretoria de Tecnologia da Informação.

- O colaborador de posse do dispositivo móvel corporativo possui a responsabilidade de realizar periodicamente cópia de segurança (backup) dos dados do dispositivo e de garantir a existência de antivírus com a lista de vírus devidamente atualizada. O manual para verificação da lista de vírus é o DTI-101. O manual está publicado no Portal de Gestão do SESI-SP e Portal de Gestão do SENAI-SP e pode ser acessado seguindo as instruções do item 1.7.2 “Informações adicionais”, página 7 da Política de Segurança da Informação, ou através do link documento.

- A reprodução não autorizada dos softwares instalados nos dispositivos móveis corporativos constituirá uso indevido do equipamento e infração legal aos direitos autorais do fabricante.

- Os dispositivos móveis corporativos não devem ser conectados a redes sem fio públicas.

- Para utilização de notebooks, é necessária a utilização de trava física de segurança, prendendo o notebook a algo fixo (mesa, coluna e etc.), a fim de dificultar qualquer ação de extravio. Todos os notebooks são fornecidos juntamente com uma trava de cabo de aço, que em caso de perda, deverá ser solicitada através de chamado técnico via Central de Serviços de TI.

- No caso de furto ou roubo de um dispositivo móvel fornecido pelo SESI-SP e SENAI-SP, o colaborador deverá registrar a ocorrência junto as autoridades policiais e informar a Central de Serviços de TI sobre o fato, para bloqueio do equipamento junto à operadora.

- O colaborador deverá estar ciente de que o uso indevido do dispositivo móvel corporativo 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 SESI-SP e SENAI-SP e/ou a terceiros.

- O acesso à rede Bluetooth deverá estar habilitado somente durante o uso, após a utilização ele deve ser desabilitado.

- Os critérios para o uso dos celulares corporativos podem ser verificados no manual DTI-108. O manual está publicado no Portal de Gestão do SESI-SP e Portal de Gestão do SENAI-SP e pode ser acessado seguindo as instruções do item 1.7.2 “Informações adicionais”, página 7 da Política de Segurança da Informação, ou através do link documento.

- Os notebooks, deverão utilizar criptografia para proteger as informações corporativas, sendo que para seu uso, é necessário solicitar a instalação junto a Central de Serviços de TI. Após a instalação consulte o manual DTI-106. O manual está publicado no Portal de Gestão do SESI-SP e Portal de Gestão do SENAI-SP e pode ser acessado seguindo as instruções do item 1.7.2 “Informações adicionais”, página 7 da Política de Segurança da Informação, ou através do link documento.

- Antes de conectar um notebook a rede é necessário verificar se o mesmo está contaminado por vírus. O manual para verificação da lista de vírus é o DTI-101. O manual está publicado no Portal de Gestão do SESI-SP e Portal de Gestão do SENAI-SP e pode ser acessado seguindo as instruções do item 1.7.2 “Informações adicionais”, página 7 da Política de Segurança da Informação, ou através do link documento. Caso o notebook esteja infectado, é necessário solicitar a remoção do vírus através da Central de Serviços de TI.

- Equipamentos infectados por vírus, não podem ser conectados à rede do SESI-SP e SENAI-SP.

## 3.2 Dispositivos móveis pessoais

- Dispositivo móvel pessoal é o equipamento eletrônico móvel de propriedade particular do colaborador do SESI-SP e SENAI-SP.

- Equipamentos pessoais não devem ser utilizados para fins profissionais das instituições, portanto acesso a arquivos e pastas nas unidades de rede não serão autorizados.

- Para acessar a internet através da estrutura tecnológica do SESI-SP e SENAI-SP com dispositivo móvel pessoal, o colaborador deve solicitar a aprovação formal do diretor de sua unidade ou área de lotação.

- Para configuração do dispositivo pessoal para acessar a internet, o colaborador, com a autorização formal de seu diretor, deverá solicitar o serviço a Central de Serviços de TI.

- Antes da liberação do acesso, a equipe da Central de Serviços de TI, irá verificar a existência de antivírus atualizado e confirmar se não há infecção por vírus, com exceção de equipamentos da Apple que utilizem o sistema operacional IOS.

- É de responsabilidade do colaborador adquirir e manter atualizado o programa de antivírus em seu equipamento. O SESI-SP e SENAI-SP não irão fornecer cópia do antivírus.

- É expressamente proibida a utilização do modem USB 3G do SESI-SP e SENAI-SP em equipamentos pessoais.

## 3.3 Dispositivos móveis de visitantes

- Dispositivo móvel de visitantes é o equipamento eletrônico móvel de propriedade particular de visitantes do SESI-SP e SENAI-SP.

- Entende-se como visitantes, empresas e pessoas que visitam a unidade corporativa ou unidades operacionais do SESI-SP e SENAI-SP, em pequenos períodos, de 01(uma) hora até 15(quinze) dias e que não possuem vinculo através de contrato firmado direta ou indiretamente com as instituições. Todo aquele que possui vinculo, deverá necessariamente receber uma identificação para acesso à rede, deixando de ser visitante e se tornando um colaborador.

- Equipamentos de visitantes não devem ser utilizados para fins profissionais das instituições, portanto acesso a arquivos e pastas nas unidades de rede não serão autorizados.

- Para acessar a internet através da estrutura tecnológica do SESI-SP e SENAI-SP com dispositivo móvel pessoal, o responsável pelo visitante deve solicitar a aprovação formal do diretor de sua unidade ou área de lotação.

- Para configuração do dispositivo do visitante para acessar a internet, o colaborador responsável, com a autorização formal de seu diretor, deverá solicitar o serviço a Central de Serviços de TI.

- O equipamento do visitante deverá possuir antivírus. É de responsabilidade do visitante possuir o programa de antivírus em seu equipamento. O SESI-SP e SENAI-SP não irão fornecer cópia do antivírus.

- Antes da liberação do acesso, a equipe da Central de Serviços de TI, irá verificar a existência de antivírus atualizado e confirmar se não há infecção por vírus, com exceção de equipamentos da Apple que utilizem o sistema operacional IOS.

- Após a verificação de vírus a equipe irá registrar em controle próprio, informações sobre o dispositivo e solicitará assinatura do termo de responsabilidade ao visitante e ao responsável pelo mesmo.

- É expressamente proibida a utilização do modem USB 3G do SESI-SP e SENAI-SP em dispositivos móveis de visitantes.

## 3.4 Dispositivos de armazenamento removíveis

- Dispositivos de armazenamento removível (pendrive, hd externo, dvd-rw, cartões de memória, dentre outros) são facilitadores de transporte de dados, porém há de se atentar que eles podem se tornar vetores que facilitam o desvio da informação, se não forem utilizados com cuidado e idoneidade.

- A autorização para utilização de dispositivos de armazenamento removível, bem como a garantia da segurança da informação que será manipulada, é de decisão restrita de cada diretoria de área ou unidade.

- As informações corporativas armazenadas por dispositivos de armazenamento removíveis devem ser protegidas conforme manual DTI-106. O manual está publicado no Portal de Qualidade do SESI-SP e Portal de Qualidade do SENAI-SP e pode ser acessado seguindo as instruções do item 1.7.2 “Informações adicionais”, página 7 da Política de Segurança da Informação, ou através do link documento.

- Ao conectar os dispositivos de armazenamento removível de fonte externa (particulares, visitantes, etc.) em equipamentos do SESI-SP e SENAI-SP, o colaborador deverá verificar antes, a existência de vírus nos dispositivos removíveis. O manual para verificação da lista de vírus é o DTI-101. O manual está publicado no Portal de Gestão do SESI-SP e Portal de Gestão do SENAI-SP e pode ser acessado seguindo as instruções do item 1.7.2 “Informações adicionais”, página 7 da Política de Segurança da Informação, ou através do link documento.

- A cópia de dados corporativos do SESI-SP e SENAI-SP por parte de terceiros, parceiros, visitantes só é permitida com autorização da diretoria da área.

# 3.18. Norma para Uso de Redes Sociais

## 1. OBJETIVO

Preservar a imagem do SESI-SP e SENAI-SP nas redes sociais, evitando que mensagens inapropriadas sejam veiculadas em nome das instituições.

## 2. CAMPO DE APLICAÇÃO

Abrange a todos os colaboradores do SESI-SP e SENAI-SP.

## 3. CRITÉRIO DE UTILIZAÇÃO

- As mídias sociais são ferramentas que auxiliam o SESI-SP e SENAI-SP a divulgar os seus serviços e promover cooperação com os clientes, colegas e com o mundo em geral.

- Os colaboradores devem utilizar as mídias sociais de forma adequada, pois todas as mensagens publicadas no ambiente da rede corporativa, estão diretas ou indiretamente ligadas ao nome do SESI-SP e SENAI-SP. Assim, os colaboradores devem respeitar os seguintes princípios:
  - ✓ Mantenha-se na sua área de especialização e forneça uma perspectiva individual exclusiva sobre o que está acontecendo no SESI-SP e SENAI-SP e no mundo;
  - ✓ Divulgue comentários respeitosos e significativos, evitando spams, comentários ofensivos e não relacionados ao tema;
  - ✓ Sempre pare e pense antes de postar. Considerando isso, responda aos comentários de forma oportuna, quando for apropriado;
  - ✓ Respeite informações, conteúdos proprietários e confidencialidade;
  - ✓ Quando não concordar com a opinião de outras pessoas, seja educado e conveniente;
  - ✓ Siga o Código de Ética do SESI-SP e SENAI-SP;
  - ✓ As recomendações e orientações de participação das mídias sociais podem ser verificadas no documento manual DTI-107. O manual está publicado no Portal de Gestão do SESI-SP e Portal de Gestão do SENAI-SP e pode ser acessado seguindo as instruções do item 1.7.2 “Informações adicionais”, página 7 da Política de Segurança da Informação, ou através do link documento.

- O SESI-SP e SENAI-SP devem possuir um registro de todas as contas de mídias sociais das instituições, com o nome dos serviços (ex.: Twitter, Facebook, YouTube, etc.) e dos colaboradores responsáveis pelas contas.

- O colaborador não possuirá autorização para acesso às contas das mídias sociais que representam as instituições em caso de desvinculação do mesmo do quadro de funcionários do SESI-SP e SENAI-SP.

### 3.1 Rede Social – Yammer.

- O Yammer é uma rede social corporativa e está disponível nos serviços do Office 365 para uso dos colaboradores do SESI-SP e SENAI-SP.

- Os registros de acesso e postagem devem ser mantidos conforme determinação legal.

- O Yammer não dever ser utilizado para:
  - ✓ Publicar ou anexar informações classificadas como confidenciais;
  - ✓ Publicar ou anexar material com conteúdo ilícito como pedofilia, apologia às drogas, terrorismo e pornográfico;
  - ✓ Publicar ou anexar materiais protegidos por leis de propriedade intelectual;

- ✓ Publicar ou anexar material de caráter político-partidário;
- ✓ Violar o Código de ética do SESI-SP e SENAI-SP;
- ✓ Anunciar compra e venda de produtos e serviços;
- ✓ Denegrir a imagem de terceiros.

- A postagem de informações no grupo “Toda a Companhia” é prerrogativa dos Diretores, Assessores, Gerentes e publicações de programas específicos das Diretorias/Assessorias. Desta forma, é recomendado aos colaboradores que procurem e ingressem nos grupos de suas afinidades ou criem seus próprios grupos.

- Qualquer colaborador pode criar grupos no Yammer.

- Os procedimentos e informações do uso do Yammer podem ser encontrados nos manuais que se encontram no link: https://www.yammer.com/sesisenaisp.org.br/#/groups/5498260/files.

# 4. REFERÊNCIAS

| Assunto | Documento | Local de Publicação |
|---|---|---|
| Cria o comitê de segurança da informação do SESI-SP e SENAI-SP | **RC 01/12** | http://intranetwidgets.sesisenaisp.org.br/RamaisCorporativos/Documentos_render_Pdf.aspx?ID=1748 |
| Ratifica o comitê de segurança da informação do SESI-SP e SENAI-SP | **RC 03/14** | http://intranetwidgets.sesisenaisp.org.br/RamaisCorporativos/Documentos_render_Pdf.aspx?ID=2267 |
| Procedimento Segurança do Ambiente de Informática | **DTI-001** | http://qualidade.sesisenaisp.org.br/Pages/File.aspx?f=iiMpp0x4GUWObZNLWhG9BA |
| Manual de Teste das mídias corporativas anuais | **DTI-IS-37-09** | http://qualidade.sesisenaisp.org.br/Pages/File.aspx?f=MoVijJLuvk-rMH5sT9u01g |
| Manual para Geração de Arquivo de Assinatura de Correio | **DTI-038** | http://qualidade.sesisenaisp.org.br/Pages/File.aspx?f=zEXAeCgHX0CRcJwlJi5LVw |
| Manual para utilização da Relação dos Serviços Críticos monitorados pela Central de Serviços | **DTI-044** | http://qualidade.sesisenaisp.org.br/Pages/File.aspx?f=Jw9PkFeXYUetjeADot0e9A |
| Manual para instalação e configuração do cliente VPN-IPSEC | **DTI-046** | http://qualidade.sesisenaisp.org.br/Pages/File.aspx?f=MgcZKh3Hk0eX0_1OQav8iw |
| Procedimento de Gestão de incidentes de segurança da informação | **DTI-082** | http://qualidade.sesisenaisp.org.br/Pages/File.aspx?f=uxGNemC6Nk6Cpt2a0YePiA |
| Procedimento de análise e risco em mudanças no ambiente de TI | **DTI-088** | http://qualidade.sesisenaisp.org.br/Pages/File.aspx?f=59SNNvRyc0ils7LsH56gGw |
| Procedimento de Auditoria dos serviços críticos de TI | **DTI-089** | http://qualidade.sesisenaisp.org.br/Pages/File.aspx?f=We3y9vrQi0yB9ShmKRk0WA |
| Procedimento de Auditoria nas aplicações do SESI-SP e SENAI-SP publicadas na internet | **DTI-099** | http://qualidade.sesisenaisp.org.br/Pages/File.aspx?f=AhqRj0fyrEOAQqH98B3fiA |
| Manual de como verificar se há vírus e se a lista de vírus está atualizada | **DTI-101** | http://qualidade.sesisenaisp.org.br/Pages/File.aspx?f=MslxboBAS06nJRraYsYlBg |
| Manual de critérios para logins e senhas | **DTI-102** | http://qualidade.sesisenaisp.org.br/Pages/File.aspx?f=8ylNjGKkTUiTit77zMDx1A |
| Manual de como bloquear e desbloquear o microcomputador | **DTI-104** | http://qualidade.sesisenaisp.org.br/Pages/File.aspx?f=dI19_S2fzE27Y8S0gW1lWw |
| Manual de utilização do Software Criptográfico TrueCrypt | **DTI-106** | http://qualidade.sesisenaisp.org.br/Pages/File.aspx?f=WYMi7VwtQUmFyJpWu78Q1Q |
| Manual de recomendações e orientações para uso de mídias sociais | **DTI-107** | http://qualidade.sesisenaisp.org.br/Pages/File.aspx?f=1xot8s8Ujkym9kr2qnsR1Q |
| Manual para uso dos celulares corporativos | **DTI-108** | http://qualidade.sesisenaisp.org.br/Pages/File.aspx?f=36bRwSp-3U2pSid0cnpeew |
| Manual para descarte de mídias utilizadas | **DTI-109** | http://qualidade.sesisenaisp.org.br/Pages/File.aspx?f=KNIHWLlbJky8QNJLcFnNOQ |
| Manual para envio de e-mails externos | **DTI-110** | http://qualidade.sesisenaisp.org.br/Pages/File.aspx?f=5dZIA_lOdEGSurc_WyP2vw |
| Manual de Exportação de lista de contatos do Lotus Notes 8.5 para o Outlook Office 365 | **DTI-116** | http://qualidade.sesisenaisp.org.br/Pages/File.aspx?f=L-WoGmHbLUKKytaWqqG8LQ |
| Manual de Exportação de lista de contatos do Lotus Notes 6 e 7 para o Outlook Office 365 | **DTI-117** | http://qualidade.sesisenaisp.org.br/Pages/File.aspx?f=42RyeqNJukKooHMVTScq_w |
| Manual de utilização do Office 365 – Correio Eletrônico | **DTI-118** | http://qualidade.sesisenaisp.org.br/Pages/File.aspx?f=9yHlojBoN0aTbGnf6OhcKA |
| Procedimento para Gestão de Incidentes detectados pelo DLP | **DTI-120** | http://qualidade.sesisenaisp.org.br/Pages/File.aspx?f=5pBBFHoffUCF3uOWKWPMGA |
| Orientações Relativas a meio ambiente | **DITEC-034** | http://qualidade.sesisenaisp.org.br/Pages/File.aspx?f=OqVCWuT8VEW0qdCGI_or8w |

# 5. GLOSSÁRIO

## A

**Acesso 3G:** tipo de acesso à Internet através do serviço de telefonia celular.

**Access Point:** equipamento que permite a montagem, configuração e funcionamento de uma rede wireless.

**Active Directory:** serviço de diretório responsável pelo armazenamento de informações sobre objetos da rede, como usuários, grupos, senhas, políticas, etc.

**ANS (Acordo de Nível de Serviço):** representa o tempo e as garantias de atendimento a um determinado serviço, podendo ser acordado internamente entre as áreas das instituições – por exemplo, o prazo de atendimento entre áreas – ou externamente entre as instituições e empresas contratadas – por exemplo, a disponibilidade mínima de um serviço.

**ASCII (American Standard Code for Information Interchange):** padronização dos códigos para caracteres alfanuméricos (letras, sinais, números e acentos), possibilitando aos computadores de diferentes fabricantes entender os códigos.

**Ataque XSS (Cross-Site Scripting):** os ataques XSS ocorrem sempre que uma aplicação obtém as informações fornecidas pelo usuário e as envia de volta ao navegador sem realizar validação ou codificação daquele conteúdo. O XSS permite aos atacantes executarem scripts no navegador da vítima, o qual pode roubar sessões de usuário, pichar sites Web, introduzir worms, etc.

**Ativo de informação:** é todo bem de valor pertencente ao SESI-SP e SENAI-SP, podendo ser, mas não se restringindo a um colaborador, documento, aplicação, mídia ou equipamento.

**Ativo de Tecnologia da Informação:** abrange sistemas, equipamentos e informações que fazem parte da infraestrutura de tecnologia da informação (TI).

**Ato ilícito:** é toda a ação que fere ou infringe a legislação brasileira.
**Auditor:** condutor da atividade de auditoria e que possui conhecimento suficiente para verificar a conformidade dos serviços e processos.

**Auditoria:** atividade que engloba o exame das operações, processos, sistemas e responsabilidades gerenciais, com o intuito de verificar sua conformidade com os objetivos e políticas institucionais, orçamentos, regras, normas ou padrões.

## B

**Backup:** cópias de dados eletrônicos para que possam ser restaurados em caso de perda dos dados originais.

**Blacklist:** listas que agrupam e-mails, domínios ou endereços de IP denunciados como disseminadores de spam na internet.

**Bluetooth:** provê uma maneira de conectar e trocar informações entre dispositivos como telefones celulares, notebooks, computadores, impressoras, câmeras digitais e consoles de videogames digitais através de uma frequência de rádio de curto alcance.

**Body:** corpo do e-mail, ou local onde a mensagem é digitada

## C

**Caixa de e-mail:** arquivo digital localizado no servidor, onde são armazenadas as mensagens recebidas e enviadas.

**Caixa de Entrada:** pasta no correio eletrônico que exibe todas as mensagens recebidas. As mensagens permanecem na Caixa de entrada até que o colaborador as mova para uma pasta diferente ou as exclua.

**Captcha:** técnica que exige ao usuário identificar as letras de uma imagem distorcida, às vezes com a adição de uma sequência obscurecida das letras ou dos dígitos que apareça na tela. Captcha são utilizados para impedir a execução de ações automatizadas que degradam a qualidade do serviço de um sistema.

**Cavalo de Tróia:** conhecido como Trojan Horse, é um programa que aparentemente realiza as funções esperadas pelo usuário, porém por trás dele são executadas ações maliciosas, sem o consentimento do usuário.

**Chamado técnico via Central de Serviços de TI:** ponto único de contato para solicitação de solução técnica, realizada junto à empresa prestadora de serviço contratada pela Diretoria de Tecnologia da Informação para esse fim. Para abrir chamado via intranet, utilize o site http://intranet.sesisenaisp.org.br, seção Catálogo de Serviços de TI. Por telefone na unidade corporativa, ligue no ramal 3333 e nas unidades operacionais, ligue no telefone (11) 0800-778-3003.

**Códigos maliciosos:** termo genérico que se refere a todos os tipos de programas desenvolvidos para executar ações maliciosas em recursos de Tecnologia da Informação (TI), tais como vírus, Cavalo de Tróia, Spyware, Worms, entre outros.

Colaboradores: todos os funcionários, terceiros ou contratados que estão autorizados a utilizar os recursos de Tecnologia da Informação do SESI-SP e SENAI-SP.

**Compartilhamento:** promove a disponibilidade de um recurso da rede para mais de um usuário.

**Confidencialidade:** consiste na garantia de que somente pessoas autorizadas tenham acesso às informações armazenadas nos equipamentos do SESI- SP e SENAI-SP ou que sejam transmitidas por meio de redes de comunicação.

**Contas funcionais**: endereço eletrônico de uso exclusivo de um único colaborador, referenciando a função, local ou área de lotação do mesmo. Ex.: convenioXXX@sesisenaisp.org.br.

**Contas nominais:** endereço eletrônico de uso exclusivo de um único colaborador, referenciando seu nome.

**Controle de acesso:** conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso.
**Correio eletrônico:** meio de comunicação utilizado para troca de mensagens internas e externas.

**Criptografia:** conjunto de técnicas que visa codificar uma informação de forma que somente o emissor e o receptor autorizados possam as acessar, evitando que um intruso consiga interpretá-la.

## D

**Datacenter:** ambiente projetado para abrigar servidores e outros componentes como sistemas de armazenamento (storages) e ativos de rede (switches, roteadores), visando garantir a disponibilidade dos serviços essenciais ao negócio de uma organização.

**Disclamer:** aviso ou declaração sobre um escopo especifico

**DLP (Data Loss Prevention):** O termo Data Loss Prevention (DLP) é utilizado na área de Segurança da Informação para se referir a sistemas e metodologias que possibilitam as empresas reduzir o risco ou identificar a perda de dados através da identificação do conteúdo, monitoramento e bloqueio de dados sensíveis.

**DMZ (DeMilitarized Zone):** situada entre a rede confiável e não confiável, a função da DMZ é manter todos os serviços que possuem acesso externo (tais como websites do SESI-SP e SENAI-SP) separados da rede interna, limitando assim o potencial dano em caso de comprometimento de algum destes serviços por um atacante.

**Disaster Recovery (Recuperação de desastres**): é um plano que visa garantir a operação da empresa com o mínimo de impacto ao negócio e aos seus clientes em situações de contingência.

**Disponibilidade:** consiste na garantia de que as informações estejam acessíveis às pessoas e aos processos necessários, sempre que forem requisitadas. Dispositivo móvel: qualquer equipamento eletrônico com atribuições de mobilidade, tais como notebooks, smartphones e tablets.

**Download:** é a transferência de arquivos de um computador remoto para um computador local.

## E

**Enviados:** pasta do correio eletrônico que exibe todas as mensagens enviadas. Ext3: sistema de arquivos para Linux.

## F

**Firewall:** sistema de segurança de computadores usado para restringir o acesso de/para uma rede, além de realizar a filtragem de pacotes com base em regras previamente configuradas.

**Freeware:** software de licenciamento gratuito, que não exige o pagamento de licenças de uso. Front-end: parte do sistema que interage diretamente com o usuário.
**FTP (File Transfer Protocol):** protocolo para transferência e acesso aos arquivos via internet.

## G

**GMT (Greenwich Mean Time):** marcador oficial de tempo. No Brasil, a referência é a hora de Brasília.

**Grupos de Usuários:** lista pré-definida de usuários com o objetivo de facilitar o envio coletivo de mensagens.

## H

**Hardware:** termo geral para equipamentos.

**Hash:** função criptográfica de mão única para proteção de senhas das aplicações.

**HDD (Hard Drive Disk):** unidade de armazenamento fixa do computador (C:), onde está instalado o sistema operacional do equipamento e os **arquivos locais.** HDD externo: unidade de armazenamento externo e móvel ligado através de cabo externo USB ao microcomputador.
**HTML (HyperText Markup Language):** é uma linguagem de marcação para páginas web. Ela provê meios para a criação de documentos estruturados através da definição de semântica estrutural para cabeçalhos, parágrafos, listas, links e assim por diante.
**Hypervisor:** é uma plataforma que permite aplicar diversas técnicas de controle de virtualização para utilizar, ao mesmo tempo, diferentes sistemas operacionais no mesmo computador.

## I

**IIS (Internet Information Services):** usado em servidores Windows, fornece vários componentes de serviço para internet, entre estes componentes citamos servidor web, de e-mail, de arquivos, entre outros.

**Informação:** toda informação de propriedade do SESI-SP e SENAI-SP, como documentos, planilhas, apresentações, dentre outros. O365: versão "webmail" do correio eletrônico.
**Integridade:** consiste na preservação das características dos dados armazenados.
**Internet:** são várias redes diferentes integradas entre si.

**Intranet:** é uma rede interna e exclusiva para os funcionários de uma determinada organização, utilizado para compartilhamento de informações restritas.
**IOS:** sistema operacional móvel da Apple usado no smartphone iPhone e no tablet iPad.
**IP:** é uma sequência numérica que identifica um dispositivo (computador, impressora, etc.) em uma rede local ou pública.

**IPS (Intrusion Prevention System**): sistema de prevenção de intrusão, cuja finalidade é detectar ataques na rede em tempo real e minimizar o impacto sem a necessidade de recursos humanos.

**IPSec (IP Security Protocol):** protocolo que visa garantir a conexão segura em comunicações pela Internet.

## J

**Junos Pulse:** softwares para dispositivos móveis (smartphones e tablets) para acesso à rede interna do SESI-SP e SENAI-SP via VPN SSL.

## L

**Lei 6.019/74:** Lei trabalhista que rege a contratação no regime temporário.
**Lei 12.965:** Lei que regulamento os aspectos de privacidade na internet brasileira e incentiva a disseminação da disciplina do uso de seguro da rede mundial de computadores.

**Lista de vírus:** lista com os vírus e vacinas conhecidas pelo antivírus.

**Log:** arquivo que registra eventos ocorridos em um sistema computacional, sendo utilizado para auditoria e diagnóstico de problemas.

**Login:** número de identificação do colaborador, sem o dígito de controle, iniciando por "SS" para SESI ou "SN" para SENAI, que juntamente com a digitação da senha, possibilita o acesso à rede do SESI-SP e SENAI-SP.

**Lync:** O Lync é um serviço hospedado que permite que uma pessoa/usuário se conecte com outras pessoas/usuários através de mensagens instantâneas (MI), chamadas de vídeo e reuniões online.

## M

**Maintenance Hook:** mecanismo de desvio do controle de acesso aos sistemas através de uma combinação de teclas para acesso direto ao banco de dados ou código fonte da aplicação.

**Mídias removíveis:** dispositivos de armazenamento móvel. Por exemplo: CD, CD-RW, DVD, DVD-RW, Disquetes e Fitas (DAT e AIT), Pendrive.

**Mídias sociais (Facebook, Orkut, dentre outros):** sites de relacionamento, cujo objetivo é ajudar os seus membros a criar amizades e manter relacionamentos.

**MSN Messenger:** programa de mensagens instantâneas criado pela Microsoft, permitindo comunicação entre os usuários em tempo real.

## N

**NAT (Network Address Translation):** protocolo responsável por realizar a tradução dos endereços IP da rede privada para a externa (Internet), e vice-versa. NIST (National Institute of Standard and Technology): agência governamental, cuja função é estabelecer padrões de uso de tecnologia para o governo dos Estados Unidos e usada como referência pelo mercado mundial.

**NIST (National Institute of Standard Technologie)** Orgão regulador do governo do EUA responsável por determinar os padrões de tecnologia usados nos órgãos governamentais desse pais. Suas publicações são de domínio público e são adotados como melhores práticas no mundo corporativo.

**NTP (Network Time Protocol):** protocolo de sincronização dos relógios, cujo objetivo é manter a hora correta em um conjunto de computadores conectados em uma rede.

**NTFS (New Technology File System):** sistema de arquivos desenvolvido pela Microsoft.

## O

**Office 365:** O Office 365 é o mesmo Office que usado diariamente. Como o Office 365 tem tecnologia da nuvem, pode se acessar aplicativos e arquivos de praticamente qualquer lugar (PC, Mac e tablets) e eles estão sempre atualizados. O mesmo vale para atualizações de recursos.

**OneDrive:** É um serviço de armazenamento online através de acesso com conta da Microsoft ou do Outlook.com. Pode ser usado para salvar documentos, fotos e outros arquivos na nuvem, compartilhá-los e até mesmo colaborar com conteúdo.

**Open source (código aberto):** um software open source é onde todos podem contribuir para melhorá-lo, e a sua distribuição é livre.

## P

**Patch de segurança:** executável disponibilizado pelo fabricante, cuja finalidade é corrigir problemas e vulnerabilidades identificadas em um determinado software ou hardware.

**Patch:** atualizar ou corrigir um sistema, incluindo vulnerabilidades de segurança.

## R

**RAID-1:** tipo de solução computacional que combina vários discos rígidos (HDs) para formar uma única unidade lógica de armazenamento de dados.

**Rainbow table**: ataque baseado em uma tabela pré calculada para comparação de resultado do hash e o seu texto claro correspondente.

**Rascunhos:** pasta no correio eletrônico que exibe todas as mensagens salvas, mas não enviadas. Recursos: todo e qualquer hardware ou software.
**Rede:** dois ou mais computadores e outros dispositivos interligados entre si de modo a poderem compartilhar recursos físicos e lógicos.
**Rede sem fio privada:** redes sem fio que exigem senha para acesso.
**Rede sem fio pública:** redes sem fio que não exigem senha para acesso. Possuem riscos de segurança maior do que a rede sem fio privada.
**Restauração:** recuperar as informações copiadas após um desastre ou falha computacional.

## S

**Service Pack:** pacote de correções para determinado sistema operacional.

**Servidores:** equipamentos com alta capacidade de armazenamento e processamento, que são utilizados como concentradores de dados e Usuários.

**Shareware:** software disponibilizado de forma gratuita, porém com recursos limitados. Para acessar a funcionalidade completa, o usuário deverá pagar para isso.

**Site de Web Free Mail:** serviço de e-mail gratuito através de ferramenta na web.

**Smartphone:** celular com funcionalidades avançadas, como acesso a e-mails, mensagens instantâneas, internet, GPS, entre outros.
**SMTP (Simple Mail Transfer** Protocol): protocolo padrão para envio de e-mails através da internet.

**Software:** programa de computador composto por funcionalidades para auxiliar os colaboradores em suas atividades. Solicitação automática: o próprio sistema de login solicita ao colaborador a troca da sua senha de acesso.
**Spam:** envio em massa de mensagens eletrônicas não solicitadas, com o objetivo de afetar a produtividade e degradar o desempenho de sistemas e de redes.

**Spyware:** programa espião, que monitora as atividades realizadas na máquina comprometida e as envia para terceiros.

**SQL Injection:** ameaça de segurança que se aproveita de falhas em sistemas que interagem com base de dados via SQL. O atacante consegue inserir uma série de instruções SQL dentro de uma consulta através da manipulação de entrada de dados de uma aplicação.

**SSL (Secure Socket Layer):** protocolo que fornece comunicação de dados segura através de criptografia.

**Super-usuário:** usuário com acesso irrestrito às informações e comandos. Normalmente, esse tipo de usuário é o responsável por tarefas administrativas dos serviços de TI.

**Subject:** Assunto do e-mail, digitado no campo assunto.

## T

**Tablet:** dispositivo móvel em formato de prancheta que pode ser usado para acesso à internet, organização pessoal, visualização de fotos, vídeos, leitura de livros, jornais e revistas e para entretenimento com jogos.

## U

**Upload:** transferência de dados de um computador local para outro computador ou para um servidor.

## V

**Vírus:** programa malicioso que faz cópias de si mesmo e se espalha para outros arquivos ou computadores, a fim de apagar ou modificar arquivos do computador.

**VPN (Virtual Private Network):** rede de comunicações privada construída em cima de uma rede de comunicações pública, como por exemplo, a Internet.

## W

**WAF:** Sigla para “Web Application Firewall”, dispositivo de rede que protege aplicações web contra-ataques específicos.

**Webmail:** interface de e-mail disponibilizada ao usuário através de um navegador de internet. Exemplos: Gmail, Hotmail, Yahoo!, dentre outros.

**Wireless:** tecnologia de rede que dispensa a utilização de cabos.
**Worm:** conhecido como verme, é um programa malicioso que propaga cópias de si mesmo pela rede, consumindo recursos, com o objetivo de degradar o desempenho da rede.

**WPA-2:** provê autenticação e criptografia, propondo a garantia de confidencialidade, autenticidade e integridade em redes sem fio.

**WSUS (Windows Server Update Services):** programa desenvolvido pela Microsoft, cuja finalidade é auxiliar os administradores de sistemas a gerenciar a distribuição de patchs lançados para serviços da Microsoft em todas as máquinas da rede.

## Y

**Yammer:** Rede social corporativa disponibilizada para os colaboradores trocarem conhecimento e noticiais pertinentes as atividades.

# 6. CONTROLE DE REVISÕES

| VER. | DATA | NATUREZA DA ALTERAÇÃO |
|---|---|---|
| 01 | 12/09/2013 | Primeira emissão. |
| 02 | 01/11/2014 | 1) Alteração do item 1.7.1, com inserção da RC-03/14;<br>2) Alteração do texto do item 2.4, removendo a palavra “pessoal”;<br>3) Inclusão do Item 3.5 “Revisões dos acessos” da norma 3.1;<br>4) Alteração do item 3.1 “figura 2” da norma 3.2;<br>5) Alteração do item 3.2 “de 90 dias para 45 dias “da norma 3.4;<br>6) Inclusão do item 3.3 “Processos DLP” da norma 3.4;<br>7) Inclusão do item de parágrafo do item 3 “Resultados das auditorias” da norma 3.4;<br>8) Inclusão do item 3.4 “Incidentes de Segurança da Informação” da norma 3.4<br>9) Alteração do item 3.1 “trocas da palavra CIC por CPF” da norma 3.7;<br>10) Alteração do item 3.3 “inserções do horário de expediente” da norma 3.7;<br>11) Inclusão do item 3.5 “Exclusões do Acesso” da norma 3.7;<br>12) Inclusão do item 3.6 “Horário de acesso” da norma 3.7<br>13) Alteração de utilização de ferramenta de correio, de Lotus para Office 365 da norma 3.9;<br>14) Inclusão do item 3.1 “Textos relacionado a testes de ambiente de desenvolvimento” da norma 3.11;<br>15) Remoção do Item 3.6 “Exclusões de Acesso” da norma 3.15;<br>16) Exclusão dos documentos de Referência do item 4, DTI-023, DTI-024, DTI-042 DTI-049, DTI-103 e DTI-105;<br>17) Inclusão dos documentos de Referência do item 4, RC 03/14, DTI-038, DTI-116, DTI-117, DTI-118, DTI-120;<br>18) Alteração do item 5 Glossários, com inclusão DLP, Lync, Office 365, OneDrive, com exclusão de AntiSpam, Skype, Webmail Corporativo;<br>Alteração do item 5 Glossários, o texto que citam “Contas Nominais e Contas Funcionais”. |
| 03 | 01/02/2016 | 1) Alteração em todo documento que citam: “Superintendência Operacional do SESI-SP” passa a ser “Superintendente do SESI-SP”;<br>2) Inclusão do item 6.19 “Envio de e-mail em massa” na norma 3.9;<br>3) Alteração “inclusão do 4G” na norma 3.15<br>4) Alteração do item 3.2 “inclusão do 4G” da norma 3.15<br>5) Alteração do item 3.3 “inserção do texto sobre compartilhamento local do computador” da norma 3.15;<br>6) Inclusão do item 3.6 “Documentos em papel” na norma 3.10; |

| | | |
|---|---|---|
| | | 7) Alteração do item 3.2 da Norma 3.7 “Norma de controle de acesso lógico”, incluindo apontamento sobre troca de senha de colaboradores do SESI-SP e SENAI-SP no retorno do período de férias e sobre troca de senha de colaboradores terceiros anualmente no vencimento do contrato;<br>8) Alteração na “Norma para Cópias de Segurança e Restauração” incluindo apontamento sobre cópias de segurança de sistemas hospedados em nuvem;<br>9) Alteração da “Norma para o Desenvolvimento de Sistemas de Informação”, recomendando o uso de base de dados fictícias em ambiente de desenvolvimento;<br>10) Alteração da “Norma de servidores de rede” dividindo o texto sobre tempo mínimo de armazenamento de arquivo de logs em dois tópicos;<br>11) Inclusão na “Norma de servidores de rede” os tópicos:<br>a. “3.3 Servidores virtuais”;<br>b. “3.4 Provedores de nuvens pública e privada que hospedam servidores do SESI-SP e SENAI-SP”;<br>c. “3.5 Provedores de nuvem privada que hospedam servidores do SESI-SP e SENAI-SP”;<br>d. “3.6 Provedor de nuvem pública que hospedam servidores do SESI-SP e SENAI-SP”;<br>e. “Perímetro da DMZ”.<br>12) Alteração da “Norma para uso de redes sociais” incluindo o tópico “3.1 Rede Social Yammer”;<br>13) Alteração da norma “Norma para Uso da Rede de Comunicação de Dados” alterando o apontamento de obrigação de desabilitar o Broadcast de SSID para recomendação de desabilitar o Broadcast de SSID;<br>14) Alteração da norma “Norma para Uso da Rede de Comunicação de Dados” Incluindo apontamento sobre a obrigação da troca de senhas padrão dos dispositivos wireless por senhas fortes;<br>15) Inclusão da definição da palavra “Hypervisor” no glossário;<br>16) Inclusão da definição da palavra “subject” no glossário;<br>17) Inclusão da palavra “body” no glossário;<br>18) Inclusão do documento DITEC-034 nas referências documento<br>19) Inclusão da palavra Yammer no glossário;<br>20) Inclusão da lei 6.019/74 no glossário;<br>21) Inclusão da palavra WAF no glossário<br>22) Inclusão da Sigla NIST no glossário;<br>23) Inclusão da Lei 12.965 no glossário;<br>24) Inclusão da palavra “Blacklist” no glossário.<br>25) Alterado norma 3.8, incluso descrição de normas de cópias de segurança usado nas nuvens pública e privada utilizada pelo SESI-SP e SENAI-SP<br>26) Inserida nota sobre aspectos legais no Item 3.6 da norma 3.10 |

| | | |
|---|---|---|
| | | 27) Retirada da norma de homologação de Software a referência ao manual DITEC-035, a pedido do supervisor de projetos e infraestrutura Sr. Heverton Luis Marino.<br>28) Inserido na “Norma para Cópias de Segurança e Restauração” o tópico “Os recursos tecnológicos do SESI-SP e SENAI-SP deverão ser utilizados exclusivamente para atividades das instituições, dados ou arquivos que forem armazenados sem atender a esse requisito, não terão garantias quanto a sua confidencialidade, integridade e disponibilidade, podendo inclusive ser excluídos sem aviso prévio. ”<br>29) Na Norma para Rede de Comunicação de Dados, alteradas as últimas linhas das tabelas, “Unidade Corporativa” e “Unidade operacional do SESI-SP e SENAI-SP”, na coluna “descrição”, substituindo a palavra “pessoais por individuais”<br>30) Na “Norma para Rede de Comunicação de Dados” item “3.5.2 Acesso a pasta e arquivos do local de rede de outro usuário”, substituída a palavra pessoais por individuais. |

Elaboração
Diretoria de Tecnologia da Informação

Documento
Política de Segurança da Informação

Vigência
01/02/2016

Versão
3.0

Classificação
Interna