SEBRAE SP	**MANUAL DE PROCEDIMENTOS**	**MP – 04/2011**

POLÍTICA DE SEGURANÇA DA TECNOLOGIA DA INFORMAÇÃO – PSTI e PRIVACIDADE DO BANCO DE DADOS DOS CLIENTES DO SEBRAE-SP

Macro Processo:	**Suporte**
Processo:	**Tecnologia da Informação**
Subprocesso	**Política de Segurança da Tecnologia da Informação – PSTI e Privacidade do Banco de Dados de Clientes**
Origem:	**Unidade Tecnologia da Informação**
Publicação:	**11/01/2011**
Nº Revisão/Data:	**00 – 11/01/2011**

ÍNDICE

1. INTRODUÇÃO

As informações e o conhecimento possuem para as modernas corporações um valor inestimável. Estrategicamente, investimentos têm sido feitos para garantir que os sistemas de informação do SEBRAE-SP atendam as necessidades dos usuários de tecnologia da informação.

Entende-se que as informações armazenadas nos bancos de dados, seja de clientes do Sebrae-SP, seja o conhecimento interno da entidade em quaisquer tipos de armazenamentos como sendo valiosos e sua perda e/ou dano causam prejuízos imensuráveis às instituições, e em alguns casos os danos são irrecuperáveis.

Conscientes destas ameaças, os ativos de tecnologia da informação e outras informações armazenadas por outras áreas, representam investimentos que devem ser protegidos e, para garantir a, integridade, e disponibilidade das informações e conhecimentos, torna-se necessário o apoio e o comprometimento de todos os usuários e a garantia da correta utilização de todos os ativos de TI, bem como, a confidencialidade no que tange à informação e a disponibilização dos dados cadastrais dos clientes (Pessoa Física ou Jurídica) do SEBRAE-SP. Desta forma, incorpora-se à PSTI a política de banco de dados de clientes do SEBRAE-SP.

2. OBJETIVO

2.1. Orientar aos usuários do SEBRAE-SP sobre a política de segurança da informação, quanto à utilização de seus dados e o manuseio de software e hardware garantindo total segurança da informação;

2.2. Orientar aos usuários sobre as diretrizes que garantam o atendimento e o fornecimento de informações confidenciais dos clientes do SEBRAE-SP.

3. ABRANGÊNCIA

Todas as unidades do SEBRAE-SP, bem como, parceiros, fornecedores e empresas prestadoras de serviços que manuseiam sistemas e informações do SEBRAE-SP.

4. PREMISSAS PARA POLÍTICA DE SEGURANÇA DA TECNOLOGIA DA INFORMAÇÃO

4.1. A política de segurança é fundamental para proporcionar aos usuários dos ativos de tecnologia da informação um ambiente de trabalho que seja, ao mesmo tempo, harmonioso, colaborativo, produtivo, seguro e com alta disponibilidade, dentro do ambiente corporativo do SEBRAE-SP.

4.2. Neste documento são apresentados os elementos básicos da Política de Segurança da Tecnologia da Informação - PSTI, documento elaborado tendo como base as normas técnicas NBR ISO/IEC 27001.

5. DA CONFIDENCIALIDADE E PROPRIEDADE

Todas as informações contidas neste documento bem como nos bancos de dados pertencentes ao SEBRAE-SP são estritamente confidenciais e restritas. Dessa forma, as informações aqui dispostas são fornecidas para a finalidade exclusiva de descrever os padrões e as recomendações de utilização dos ativos de tecnologia da informação, já incluso os dados cadastrais dos clientes do SEBRAESP, sendo vedada sua divulgação ou cópia,

parcial ou total, por quaisquer meios ou métodos, sem a prévia autorização formal da CSTI - Comissão de Segurança de Tecnologia da Informação do SEBRAE-SP.

6. CONCEITOS

6.1. Política de Segurança da Tecnologia da Informação – PSTI

6.1.1. O termo Tecnologia da Informação é comumente utilizado para designar o conjunto de recursos não humanos dedicados ao armazenamento, processamento e comunicação da informação, bem como o modo de como esses recursos estão organizados num sistema capaz de executar um conjunto de tarefas.

6.1.2. Denomina-se Política de Segurança da Tecnologia da Informação - PSTI, o conjunto de normas, constituído por padrões, recomendações, estruturas organizacionais e/ou funções de software/hardware que garantam as premissas de segurança da tecnologia de informação.

6.1.3. Padrões e Recomendações:

Políticas de segurança são compostas por normas, padrões e recomendações:

a) Normas são princípios que seguem regras.

b) Padrões consistem em procedimentos que devem ser obrigatoriamente aplicados e cumpridos para que a segurança seja garantida.

c) Recomendações consistem em procedimentos, cujo cumprimento é altamente aconselhável.

6.1.4. Manuais de Padrões e Recomendações de Segurança:

São documentos integrantes da política de segurança que contêm as normas, os padrões e as recomendações de segurança.

6.1.5. Usuário dos Ativos de TI:

Denominam-se usuários todos os colaboradores: funcionários, estagiários, prestadores de serviço, terceirizados, conveniados, credenciados, fornecedores, clientes ou quaisquer outros que, por ventura, venham a utilizar os ativos de tecnologia da informação em questão.

6.1.6. Comissão de Segurança de Tecnologia da Informação – CSTI:

6.1.6.1. A Comissão de Segurança de Tecnologia da Informação - CSTI é responsável pelo gerenciamento da PSTI, sendo composta pelos responsáveis das seguintes áreas:

a) Gestão de Pessoas;
b) Auditoria;
c) Jurídico;
d) Tecnologia da Informação;
e) Marketing e Comunicação;
f) Planejamento.

6.1.6.2. Para deliberação faz-se necessária obrigatoriamente a presença de maioria plena (50% + 1) da CSTI, sendo recomendada a presença das unidades de Gestão de Pessoas e Tecnologia da Informação.

Nota: A critério da Diretoria Executiva do SEBRAE-SP, outros colaboradores poderão ser convidados a integrar a Comissão.

6.1.6.3. O coordenador da CSTI será designado pela própria comissão, tendo como responsabilidade coordenar os respectivos trabalhos.

6.1.6.4. A nomeação dos membros que comporão a CSTI deverá ser feita por meio de portaria da Diretoria Executiva.

6.1.6.5. A CSTI poderá convidar outros colaboradores para participar das reuniões, em função de necessidades específicas.

6.1.7. Gestor de Segurança

6.1.7.1 O gestor de segurança da tecnologia da informação do SEBRAE-SP deve ser designado pela gerência da unidade de Tecnologia da Informação e ratificado pela CSTI.

6.1.7.2 O gestor de segurança promoverá a administração e operacionalização da PSTI, além de promover a disseminação do tema para a comunidade SEBRAE-SP.

6.1.7.3 Os incidentes aferidos pelo gestor de segurança serão comunicados à CSTI para a deliberação de medidas de resposta(s) ao(s) incidente(s).

6.1.8. Informação

Entende-se por “informação” todo e qualquer dado passível de ser armazenado para posterior transmissão ou processamento.

6.1.9. Ativos de Tecnologia da Informação

6.1.9.1. Entende-se como ativos de tecnologia da informação os *hardwares, softwares*, dados e informações armazenadas em qualquer tipo de mídia digital, todas as informações geradas ou processadas por todo e qualquer usuário dos ativos da entidade, que possuem seus respectivos valores associados e, conseqüentemente, podem também ser chamadas de ativos de TI, já incluso os dados cadastrais dos clientes do SEBRAESP.

6.1.9.2. Para a política de segurança em questão, são considerados os seguintes ativos:

a) Físicos: equipamentos computacionais e periféricos, infraestrutura física e lógica de rede, dispositivos de armazenamento de dados, instalações físicas, ambiente, etc.

b) *Softwares*: bancos de dados, aplicativos, sistemas operacionais, navegador, ferramentas de desenvolvimento, linguagens de programação, *softwares* utilitários, sistemas corporativos, gerenciamento de rede, etc.;

c) Informacionais: bases de dados, arquivos, documentação de sistemas, manuais, material de treinamento, metodologias e procedimentos operacionais, plano de continuidade dos negócios, etc.;

d) Prestação de serviços interno e externo: infraestrutura computacional e desenvolvimento de sistemas.

6.1.10. Segurança da Informação

Para preservar a segurança da informação, premissas básicas são consideradas:

a) Confidencialidade: garantia de que a informação é acessível apenas a pessoas ou processos devidamente autorizados;

b) Integridade: garantia de que os dados inseridos no sistema não sejam alterados inadvertidamente, independentes do modo de processamento da informação;

c) Disponibilidade: garantia de que os usuários ou processos devidamente autorizados obtenham acesso à informação e aos ativos correspondentes sempre que for necessário.

6.1.11. Segurança de Tecnologia da Informação

A segurança de TI consiste na união das premissas básicas para a segurança da informação aplicadas no âmbito dos ativos de TI da entidade, juntamente com a seguinte premissa:

- Uso adequado dos ativos de TI: todos os ativos de TI deverão ser utilizados estritamente para os fins aos quais foram destinados e, sempre, atendendo à respectiva política de segurança da informação.

6.1.12. Incidentes de Segurança

Entende-se por incidentes de segurança a ocorrência pelo não-cumprimento de normas, padrões e/ou recomendações de utilização dos ativos de tecnologia da informação.

6.1.13. Medidas Disciplinares

Entende-se por medidas disciplinares a aplicação de sanções administrativas, podendo ensejar, inclusive, a rescisão de contrato e a aplicação de medidas judiciais ou outras medidas pertinentes.

6.2. Privacidade do Banco de Dados dos Clientes do SEBRAE-SP

6.2.1. Entende-se por dados cadastrais, toda e qualquer informação prestada pelo cliente SEBRAE-SP que dizem respeito a sua pessoa, seja ela física ou jurídica, tais como: nome, razão ou denominação social, endereço, CPF/MF, CNPJ, telefone, e-mail, ramo de atividade, etc.

6.2.2. A expressão “dados confidenciais” significa toda e qualquer informação pertencente ao banco de dados de clientes do SEBRAE-SP, de forma escrita ou magnética.

6.2.3. A informação poderá se revestir de qualquer forma, seja oral, por escrito, presencial ou de qualquer outra forma.

7. ORGANIZAÇÃO DA PSTI

7.1. Gerenciamento

Caberá ao gestor de segurança e a CSTI o gerenciamento da PSTI, que tem como atribuições:

7.1.1. Assessorar na manutenção e revisão da PSTI pela área de Tecnologia da Informação, durante as seguintes etapas:

a) Elaboração da documentação;

b) Classificação dos riscos de segurança;

c) Seleção dos riscos a serem gerenciados, segundo os aspectos de:

c1) impacto dos riscos para a organização;
c2) viabilidade para implantação de controles de segurança;
c3) avaliação do custo versus benefício para minimização dos riscos.

d) Manutenção da política de segurança;

e) Obter compromissos de colaboração com a PSTI:

d1) da Diretoria Executiva;
d2) de todos os usuários dos ativos de tecnologia da informação.

f) Sensibilizar e informar usuários sobre a PSTI:

f1) Propor aos membros da CSTI, juntamente com as unidades de Gestão de Pessoas e Marketing e Comunicação, estratégias de divulgações internas das normas que regulamentam a PSTI (exemplos – cartilhas, hotsites, palestras, etc.).

g) Disseminar periodicamente informações relativas aos princípios e valores da PSTI;

h) Analisar e responder aos incidentes e às violações de segurança, sugerindo formalmente medidas disciplinares às alçadas competentes.

7.2. Planejamento, definição e implementação dos Controles de Segurança

O planejamento e a definição dos controles de segurança devem ser elaborados pela equipe técnica interna da unidade de Tecnologia da Informação do SEBRAE-SP, podendo eventualmente ser assessorado por consultor ou empresa especializada. Após a definição, o gestor de segurança deverá ratificar os controles de segurança com a CSTI e acompanhar a sua implementação.

7.3. Responsabilidades de usuários dos ativos de Tecnologia da Informação

Todos os usuários devem:

7.3.1. Utilizar os ativos de TI mediante as "condições de uso" constantes no "Manual de Padrões e Recomendações de Usuários (Anexo I);

7.3.2. Respeitar o "código de práticas" constante no "Manual de Padrões e Recomendações de Usuários" (Anexo I);

7.3.3. Zelar pela manutenção da integridade, disponibilidade e confidencialidade das informações;

7.3.4. Utilizar os ativos de TI exclusivamente para os fins autorizados pelo SEBRAE-SP e em conformidade com a PSTI:

a) *hardware, software*;
b) banco de dados;
c) correio eletrônico;
d) sistema de armazenamento de arquivos;
e) antivírus;
f) Internet, Intranet e Extranet;
g) *chat*, fóruns, ferramentas de comunicação instantânea;
h) sistemas corporativos do próprio SEBRAE.

Nota: A utilização dos ativos de TI deverá respeitar o direito a privacidade dos usuários.

7.3.5. O conteúdo dos ativos devem estar alinhados com o código de conduta e ética do SEBRAE-SP.

7.4. Da Formalização de Contratos e Convênios

Todos os contratos, convênios e processos em que haja utilização de ativos de TI devem mencionar a obrigatoriedade do cumprimento e da observância dos padrões e recomendações de segurança desta política pelo contratado, partícipe ou licitante.

8. DOCUMENTAÇÃO

A PSTI do SEBRAE-SP é composta por esta Instrução Normativa e pelo Manual de Padrões e Recomendações de Segurança, cuja circulação e disponibilidade são restritas aos colaboradores do SEBRAE-SP. Quaisquer outros documentos que venham a integrar ou complementar a PSTI devem ter suas restrições de circulação e disponibilidade definidas pela CSTI.

9. POLÍTICAS GERAIS PARA UTILIZAÇÃO DO BANCO DE DADOS DE CLIENTES

9.1. As estipulações e obrigações constantes sobre a confidencialidade não serão aplicadas a nenhum dado que:

a) Seja de domínio público no momento da revelação;
b) Já esteja em poder da outra parte, como resultado de sua própria pesquisa, contanto que a outra parte possa comprovar esse fato;
c) Seja revelada em razão de uma ordem válida ou de uma ordem judicial, somente até a extensão de tais ordens, contanto que a outra parte tenha notificado a existência de tal ordem, previamente e por escrito, à outra parte, dando a esta tempo hábil para pleitear medidas de proteção quer julgar cabíveis.

9.2. Os dados dos clientes do SEBRAE-SP deverão ser manipulados pelo próprio SEBRAE-SP. Caso a manipulação tenha que ser realizada por uma empresa ou entidade parceira do SEBRAE-SP, essa deverá assinar um Contrato de Confidencialidade (Anexo IV do manual), se comprometendo a manter os dados e informações em absoluto sigilo, mesmo após finalizada a prestação de serviços, por constituírem objeto de

sigilo, sob pena de obrigar-se a indenizar o SEBRAE-SP, a qualquer tempo, por danos e/ou prejuízos sofridos em decorrência da falha de manutenção de sigilo.

Nota: Esse contrato deve ser assinado em papel timbrado do parceiro e encaminhado para a Unidade de Tecnologia da Informação.

9.3. As informações estatísticas geradas pela análise dos dados e agregadas sobre o uso do SEBRAE-SP poderão ser compartilhadas visando atender as necessidades dos clientes, e também para ajudar nossos parceiros a entender os dados sócio-demográficos do nosso publico.

9.4. Se, por qualquer motivo o SEBRAE-SP decidir reunir e utilizar dados que possam identificar seus clientes, para qualquer fim que não tenha sido descrito anteriormente, o SEBRAE-SP deve solicitar autorização a esses clientes sobre o uso de seus dados e que isso poderá identificá-los individualmente.

9.5. Não obstante qualquer outra disposição contrária a Política de Privacidade, o SEBRAE-SP poderá divulgar os dados dos seus clientes mediante exigência das leis gerais ou pelas autoridades regulamentárias ou legais.

9.6. Se o SEBRAE-SP decidir mudar a Política de Privacidade, deverá anunciá-las publicamente visando manter todos os clientes informados.

10. FORMA DE ATUAÇÃO PARA UTILIZAÇÃO DO BANCO DE DADOS DE CLIENTES

10.1. Mala Direta

a) Nas negociações com os parceiros, o SEBRAE-SP deve fazer o possível para que os dados dos seus Clientes sejam somente manipulados por seus próprios técnicos ou pela agência dos correios contratada pelo SEBRAE-SP para tal fim;

b) Caso a manipulação dos dados pelos Parceiros seja inevitável, este deverá assinar o Contrato de Confidencialidade (Anexo IV do manual), descrito no item 9.2 e encaminhar à Unidade de Tecnologia da Informação, que irá arquivá-lo para periódicas verificações;

c) As etiquetas para postagem de mala direta serão encaminhadas para a área solicitante, que deverá efetuar a postagem para os correios (agência com contrato assinado com o SEBRAE-SP).

Nota: Caso haja necessidade da Unidade de Tecnologia da Informação enviar as etiquetas diretamente para o Escritório Regional, devido à pequena quantidade a ser postada, o ER deverá se responsabilizar em acatar a Política de Privacidade assim como obedecer às diretrizes da PSTI.

d) Os materiais que serão postados deverão conter o logotipo do SEBRAE-SP, ou seja, não será permitida a postagem de materiais nos quais o SEBRAE-SP não participe como parceiro.

e) Caso o contrato de confidencialidade seja descumprido pelo parceiro, este deverá indenizar o SEBRAE-SP, a qualquer tempo, por danos e/ou prejuízos sofridos em decorrência da falha de manutenção de sigilo. Para tanto, o SEBRAE-SP conta com instrumentos de fiscalização inseridos em sua base de dados que tornam possíveis a identificação de bases corrompidas pelo parceiro.

10.2. Listagens em geral contendo dados dos Clientes do SEBRAE-SP

a) As listagens solicitadas para telemarketing, envio de mensagens eletrônicas ou qualquer outro tipo de contato com o Cliente do SEBRAE-SP deverão ser manipuladas pelo próprio corpo técnico do SEBRAE-SP;

b) Toda e qualquer listagem, visando contatar os clientes do SEBRAE-SP com a finalidade de realizar pesquisas em geral, deve ser solicitada pela UO Marketing e Comunicação e obedecer aos seguintes critérios;

b1) A UO Marketing e Comunicação do SEBRAE-SP, por sua vez, solicitará ao parceiro que assine o Contrato de Confidencialidade, visando garantir os requisitos descritos neste manual;
b2) A assinatura deste contrato não implicará na concessão de nenhuma licença ou de qualquer outro direito, explícito ou implícito, em relação a qualquer direito de patente, direito de edição ou qualquer outro direito à propriedade intelectual;
b3) Todas as informações confidenciais reveladas pelo SEBRAE-SP à prestadora de serviço serão consideradas como propriedade exclusiva, devendo esta retornar imediatamente para o SEBRAE-SP assim que requerido, bem como, todas e quaisquer cópias eventualmente existentes;
b4) Esse documento terá validade plena e obrigatória durante o período de 5 (cinco) anos.

11. PROCEDIMENTOS

Todas as solicitações de etiquetas e/ou listagens devem ser realizadas pelo formulário na Intranet - Solicitação de Informações e de Impressões de Etiquetas e Listagens ou via e-mail para uoti@sebraesp.com.br com cópia para o superior imediato e respectiva Diretoria Executiva contendo as seguintes informações:

a) Como e por quem será feita a postagem do material;
b) Quem irá manipular as listagens de telemarketing;
c) Finalidade da solicitação;
d) Data limite para preparação do material;
e) Critérios mínimos para seleção dos clientes:
   e1) Tipo de pessoa (Física ou Jurídica);
   e2) Localização geográfica;
   e3) Setor de atividade (indústria, comércio, serviço ou agropecuária);
   e4) CNAE (Código Nacional de Atividade Econômica);
   e5) Porte (micro, pequena, média ou grande).

12. VIOLAÇÃO DE SEGURANÇA

Toda e qualquer violação das instruções descritas neste manual, deverá ser analisada pela Comissão de Segurança da Tecnologia da Informação (CSTI), que também será responsável pela definição das respostas às violações.

Nota: O não cumprimento dos critérios estabelecidos acarretará na aplicação de medidas disciplinares que serão definidas pela Diretoria Executiva, após a análise pela CSTI, podendo inclusive tais medidas acarretarem demissão, quebra de contrato (terceiros), processos judiciais ou outras medidas pertinentes.

13. REFERÊNCIAS NORMATIVAS

As políticas aqui definidas têm como referências os seguintes documentos:

a) NBR ISO/IEC 27001:2005;
b) NBR ISSO/IEC 27002:2005;
c) Constituição Federal;
d) Lei nº 9.296/96 – Interceptação do fluxo de comunicação em sistemas de informática e telemática;
e) Consolidação das Leis do Trabalho – CLT;
f) Lei nº 9.279/96- Direitos e obrigações relativas à propriedade intelectual.

14. DISPOSIÇÕES COMPLEMENTARES

14.1 A PSTI deverá ser amplamente divulgada a todos os usuários pelo coordenador da CSTI, apoiado pelo Gestor de Segurança, por meio de campanhas de sensibilização, (exemplos: cartilhas, *hotsites*, palestras, etc.).

14.2. A PSTI será revisada anualmente pela CSTI, ou de acordo com as necessidades e interesses do SEBRAE-SP.

14.3. Todos os padrões e recomendações estabelecidos pela PSTI serão passíveis de monitoramento para garantir o seu cumprimento.

14.4. As situações não-previstas pela PSTI deverão ser analisadas pelo gestor de segurança e pela CSTI e submetidas à deliberação da Diretoria Executiva.

14.5. As situações não previstas neste manual devem ser submetidas à avaliação e aprovação da Diretoria Executiva.

14.6. Este manual de Procedimentos entra em vigor na data de sua publicação, revogadas as disposições em contrário.

15. GLOSSÁRIO

Antivírus

Programa utilizado para descontaminar um computador ou rede que estiver infectada com vírus, *worm* e códigos maliciosos, bem como fornecer proteção contra novas infestações. Esses programas precisam ser atualizados com freqüência para garantir sua eficácia.

Aplicativo/Software

Programa de computador desenvolvido para executar uma função específica, normalmente para o usuário. Em alguns casos, pode desempenhar funções para outros programas como para o sistema operacional.

Backup

Rotina de segurança utilizada para a armazenagem, normalmente em mídia removível, de toda ou parte das informações existentes nos discos rígidos ou na rede, permitindo a recuperação de dados eventualmente perdidos ou danificados por incidente.

Banco de Dados

Banco de Dados, (ou base de dados), são conjunto de dados com uma estrutura regular que organizam informações. Um banco de dados normalmente agrupa informações utilizadas para um mesmo fim.

Cavalo de tróia

Programa nocivo utilizado por *hackers* para invadir computadores. Ao contrário do vírus, ele não se dissemina automaticamente, mas geralmente vem em um arquivo anexado por e-mail.

CD-ROM

Substituto natural da unidade de disco flexível, a unidade de CD-ROM (*Compact Disc-Read Only Memory*) é utilizada para a leitura de discos CD (dados e som), cujo acesso é mais rápido e confiável e tem capacidade de armazenamento de até 700 MB.

Cartão de memória

Cartão com chip que permite o armazenamento de informações.

Chat

Software que permite diálogo em tempo real entre pessoas ligadas pela internet.

Correio eletrônico

Ferramenta utilizada para a troca de mensagens por meio eletrônico, seja dentro de uma rede privada ou pela internet. Podem-se utilizar programas de apoio como o *Microsoft Outlook* ou serviços de correio na internet (*web mail*), como o *Hotmail*.

Disco Flexível

Unidade de acesso para leitura e gravação de discos flexíveis (disquetes), que têm baixa capacidade de armazenagem (1,44 Mb), baixa segurança e velocidade de acesso.

Drive

1. Qualquer unidade de acesso (disco flexível, disco rígido, *CD-ROM*).
2. Pequenas unidades de código que contêm informações sobre o funcionamento de determinado dispositivo necessário para sua instalação e/ou configuração.

DVD-ROM

A unidade de *DVD-ROM* (*Digital Vídeo Disc-Read Only Memory*) é utilizada para a leitura de discos DVD (dados e som), cujo acesso é mais rápido e confiável e tem capacidade de armazenamento de até 4,7 GB. Como o *CD-ROM* só permite ler informações gravadas em DVD, a solução dessa limitação são os *drives* de *DVDR-ROM (Digital Vídeo Disc Recordable-Read Only Memory*).

Estação de trabalho

Designação dada ao computador de acesso do usuário. A estação de trabalho pode ser um *desktop* completo, com todos os dispositivos típicos de um PC ou ser uma máquina mais enxuta, deixando funções como armazenamento para serem executadas pelo servidor.

Extranet

Rede de computadores com tecnologia internet que mantém comunicação com a empresa, mas está situada fora dela. Em geral, usada para conectar a empresa com seus parceiros, fornecedores e clientes.

Hardware

Designação genérica de todo tipo de equipamento de informática, por exemplo, computador, discos rígidos, memória, impressora, *scanner*, entre outros.

Help Desk

Serviço de apoio aos usuários para resolver problemas técnicos.

Infravermelho

Componente de comunicação sem fio, por meio de luz infravermelha.

Ferramenta de comunicação instantânea

Mensagens enviadas por programas, como IM, ICQ e MSN, entre outros, que podem ser lidas instantaneamente por uma outra pessoa conectada à internet. Os programas de mensagens instantâneas diferem do correio eletrônico por serem mais simples e capazes de estabelecer diálogos *on-line* imediatos.

Internet

Rede mundial de computadores, conhecida também por *web* ou WWW.

Intranet

Rede de computadores interna de uma empresa ou instituição que usa a tecnologia da internet.

Login
Identificação para acesso a um determinado computador ou sistema.

Modem

Dispositivo utilizado para conexão do computador a uma rede remota por meio de uma conexão discada. A velocidade padrão atual desses dispositivos é 56 kbps.

Notebook

Computador portátil que traz como principal característica a integração e a miniaturização da maior parte dos componentes, tornando-o leve e de pequenas dimensões. Muitos *notebooks*, hoje, têm capacidade de processamento similar aos *desktops*.

PDA

Personal digital assistants (PDA ou *Handheld*), ou "Assistente Pessoal Digital", é um computador de dimensões reduzidas, dotado de grande capacidade computacional, operando como agenda eletrônica, editor de texto, planilha eletrônica e demais sistemas elementares de utilização em escritório, com possibilidade de interconexão com um computador pessoal e/ou com rede informática sem fios - *wi-fi* - para acesso à internet.

Periférico

Denominação dada a todo dispositivo utilizado para comunicação ou interface entre o computador e o usuário ou entre o computador e outro computador. Entram nesta categoria, por exemplo, *modem*, impressora, *scanner*, entre outros.

Porta

Uma expressão abstrata usada pelo protocolo TCP/IP, a fim de distinguir entre conexões simultâneas para um único *host* destino. O termo também é usado para denominar um canal físico de entrada ou de um dispositivo.

Rede

Genericamente, um conjunto de computadores interligados, que se comunicam entre si.

Rede sem fio

Permite a conexão de um conjunto de computadores ligados que se comunicam entre si sem cabeamento.

Servidor

Computador que provê recursos para outros computadores da rede, tais como: armazenamento de dados, impressão, acesso discado etc.

Spamming

Denominação dada a mensagens de correio eletrônico enviadas e não-solicitadas. Essas mensagens, na maior parte das vezes, têm o objetivo de vender um produto ou fazer propaganda de determinado produto ou serviço não homologado pela entidade.

Spammer

Pessoa, empresa ou organização responsável por enviar *e-mails* não-solicitados em grandes quantidades e para diversos destinatários, sem o consentimento deles.

Vírus

Denominação dada a pequenos programas desenvolvidos para causar danos em diversos níveis, podendo afetar a integridade de arquivos de dados (removendo partes ou arquivos por completo), prejudicarem um computador em particular ou toda a rede de uma empresa ou mesmo milhões de computadores por meio da internet. Propagam-se por meio do correio eletrônico e aplicativos ilegalmente distribuídos e, por causa das tecnologias que vêm sendo empregadas na criação dessas pragas virtuais, podem se espalhar por milhões de máquinas em poucas horas, causando prejuízos enormes para empresas e pessoas físicas.

Web

"Teia". Abreviatura de *World Wide Web* (teia de amplitude mundial). Conjunto de computadores que funcionam com o protocolo de comunicação HTTP e exibem arquivos em linguagem HTML.

Wireless

Wireless (sem fio), tecnologia que permite a conexão entre diferentes pontos sem a necessidade do uso de cabos – seja ele eletrônico, coaxial ou ótico – por meio de equipamentos que usam radiofreqüência (comunicação via ondas de rádio) ou comunicação via in.

16. ANEXOS

ANEXO I - PADRÕES E RECOMENDAÇÕES PARA USUÁRIOS

1. Das condições de uso

.1.1. As "condições de uso" definem os padrões e as recomendações de segurança que os usuários devem cumprir para obter acesso aos ativos de TI do SEBRAE-SP.

.1.2. Os ativos de TI são de propriedade do SEBRAE-SP e são de uso exclusivo para execução dos trabalhos.

.1.3. Para a utilização dos ativos de TI do SEBRAE-SP, todos os usuários devem admitir às seguintes condições:

.1.3.1. Responsabilidades:

É responsabilidade de todo usuário:

a) utilizar, de forma responsável, profissional, ética e legal os ativos de TI;
b) respeitar a integridade, a disponibilidade, a privacidade e a confidencialidade das informações do SEBRAE-SP e de seus usuários.
c) respeitar os direitos e as permissões de uso dos ativos da TI concedidos pelo SEBRAE-SP;
d) respeitar e seguir o "código de práticas" deste documento;
e) seguir as normas e os procedimentos de atendimento aos usuários dos ativos de TI (*helpdesk*), informando corretamente o problema e o nível de prioridade.

.1.3.2. Restrições de uso:

a) Ausência da assinatura do “Termo de Compromisso para Usuários de Ativos da Tecnologia da Informação” (Anexo II).
b) Os ativos da TI não podem ser utilizados para difusão ou armazenamento de propaganda pessoal ou comercial, aliciamentos, programas destrutivos (vírus e *spam*), material político ou qualquer outro uso inadequado.
c) É expressamente proibido o uso da infra-estrutura computacional por qualquer indivíduo que não mantenha contrato direto ou indireto com o SEBRAE-SP.
d) O uso da infra-estrutura computacional é um recurso que pode ser revogado ou restringido a qualquer momento, caso ocorra algum incidente relatado à CSTI.

.1.3.3. Restrições de conteúdo

É expressamente proibido o armazenamento ou transmissão, sob qualquer forma ou meio de comunicação, de conteúdo inapropriado que promova, incite ou instrua ações e atitudes, tais como: crime, roubo, violência, terrorismo, difamação, calúnia, preconceito de qualquer tipo ou classe, drogas e pornografia.

.1.3.4. Uso de hardware

É proibido aos usuários:

a) disponibilizar o acesso a pessoas não-autorizadas;
b) instalar ou alterar as configurações do *hardware* sem autorização formal da unidade de Tecnologia da Informação;

c) instalar servidores, computadores, periféricos e acessórios na infra-estrutura computacional, sem prévia autorização formal da unidade de Tecnologia da Informação;
d) promover qualquer manutenção ou tentativa de manutenção dos ativos de TI.

.1.3.5. Conexões a redes de terceiros e Internet

Aos usuários de notebooks é permitido o acesso às redes de terceiros, desde que respeitadas as demais regras desta PSTI.

.1.3.6. Uso de software

É proibido aos usuários:
a) copiar *softwares* do SEBRAE-SP;
b) disponibilizar cópias de *softwares* para terceiros ou clientes do SEBRAE-SP;
c) instalar qualquer tipo de *softwares*;
d) alterar configurações de *softwares* instalados;
e) utilizar técnicas de engenharia reversa ou decompilar *softwares* de propriedade do SEBRAE-SP;
f) utilizar licenças de *softwares* que infrinjam quaisquer patentes ou direitos autorais.

.1.3.7. Suporte aos usuários e manutenção dos ativos de TI homologados pelo SEBRAE-SP.

a) O suporte aos usuários dos ativos homologados pelo SEBRAE-SP são restritos à equipe técnica da área de TI.b) A manutenção dos ativos de TI homologados pelo SEBRAE-SP é restrita às empresas contratadas por meio da área de TI, e somente elas poderão promover qualquer intervenção técnica, sob pena de perda de garantia dos ativos.

.1.3.8. Contingência

É reservado ao SEBRAE-SP, através da unidade de TI, o direito à adoção de medidas emergenciais para preservar a segurança dos seus ativos, incluindo a suspensão, bloqueio e alteração de contas, senhas, cancelamento do processo em andamento, dentre outros, de quaisquer usuários.

.1.3.9. Alterações da política de segurança

Esta política será revisada e/ou atualizada anualmente pela CSTI, de acordo com as necessidades do SEBRAE-SP. Todos os usuários serão informados quando ocorrerem tais revisões / atualizações.

.2. Do código de práticas

O "código de práticas" estabelece os padrões e recomendações para a utilização dos ativos de TI.

Faz parte do escopo do código indicar quais são as praticas mais adequadas para a utilização dos ativos de TI, observando aspectos peculiares a cada tipo de aplicação ou serviço.

.2.1. *Hardware*

Os ativos de *hardware* de TI devem ter seu uso racional, observando os limites de utilização estabelecidos pelo SEBRAE-SP.

É dever de todos os usuários proteger os ativos de TI contra qualquer tipo de danos e perdas.

Somente a U. O. Tecnologia da Informação poderá efetuar e/ou autorizar qualquer tipo de alteração e reparo interno ou externo nos ativos.

Os usuários dos ativos da TI somente estão autorizados a utilizar os hardwares homologados pelo SEBRAE-SP.

Poderão ter acesso à rede corporativa, mediante autorização da unidade de TI e aceite da PSTI todos os ativos não pertencentes ao SEBRAE-SP (*pen drive*, disco rígido externo, câmera digital, *notebook*, agenda eletrônica, PDA etc.).

.2.1.1. **Das movimentações dos ativos de TI**

As movimentações dos equipamentos de TI devem ser efetuadas por meio de Guia de Movimentação de Material – GMM, conforme normativa respectiva, devendo ser encaminhado o arquivo da GMM para o email unidade de TI - Suporte.

.2.2. Software

Os ativos de *software* de TI devem ter seu uso racional, observando os limites de utilização estabelecidos pelo SEBRAE-SP.

É dever de todos os usuários proteger os ativos de TI contra qualquer tipo de danos e perdas.

Os usuários dos ativos da TI somente estão autorizados a utilizar os *softwares* homologados pelo SEBRAE-SP (conforme Anexo III). Os *softwares* gratuitos poderão ser utilizados apenas quando justificados, autorizados e instalados pela unidade de TI.

É expressamente proibido instalar qualquer tipo de *software*, principalmente os que infrinjam quaisquer patentes ou direitos autorais e a utilização de técnicas de engenharia reversa, objetivando decompilar os *softwares* de propriedade da entidade.

.2.3. Vírus

Os vírus podem causar danos em diversos níveis, podendo afetar a integridade de arquivos de dados, causando prejuízos imensuráveis e, em alguns casos, irrecuperáveis. Cada usuário é responsável por tomar precauções para evitar a contaminação dos computadores.

O SEBRAE-SP fornece as ferramentas necessárias para a detecção e a eliminação de vírus de computadores e programas do tipo: *trojan, blaster*, cavalos de tróia*, spamms,* etc.

11.2.3.1. Os usuários dos ativos de TI comprometem-se a:

a) não executar programas ou arquivos de fontes desconhecidas provenientes da internet;
b) verificar os arquivos recebidos quanto à existência de vírus (via internet, redes de terceiros, disquetes, CDs, DVDs, cartão de memória, unidades de disco removível) com as ferramentas fornecidas pelo SEBRAE-SP para esta finalidade;
c) comunicar à unidade de TI, quando percebido, qualquer incidente de vírus
d) caberá exclusivamente a unidade de TI informar os procedimentos a serem adotados sobre vírus.

.2.4. Banco de dados

.2.4.1. As informações contidas nos sistemas de banco de dados do SEBRAE-SP são de seu uso exclusivo.

2.4.2. O banco de dados com informações de clientes possui política de privacidade específica de utilização.

2.4.3. É vedada a cópia ou uso não-autorizado destes dados para outros fins, que não sejam de interesse do SEBRAE-SP.

2.4.4. Os usuários deverão zelar pela integridade, disponibilidade e confidencialidade destas informações.

.2.5. Correio eletrônico

O sistema de correio eletrônico deverá ser utilizado somente para atividades relacionadas à instituição e que contribuam positivamente para o SEBRAE-SP.

É expressamente proibido:

a) enviar ou ser conivente com conteúdo não-aderente a esta política de segurança;
b) enviar mensagens para listas de clientes, fornecedores e parceiros que não sejam de interesse da entidade, sem a devida autorização da área responsável;
c) enviar mensagens que configurem *spamming* para usuários internos e externos;
d) enviar mensagens com a identificação do remetente alterada ou falsificada;
e) enviar mensagens com o conteúdo alterado ou falsificado;
f) invadir a privacidade de usuários pelo acesso não-autorizado à sua caixa postal;
g) enviar informações confidenciais do SEBRAE-SP para redes públicas (Internet), sem autorização.

2.6. Rede de computadores

A rede de computadores da entidade deve ser utilizada de forma proficiente e produtiva, mantendo sua integridade, disponibilidade e confidencialidade das informações e conhecimento.

11.2.6.1. É expressamente proibido o uso, sem autorização, de *softwares* não-aderentes à política de segurança do SEBRAE-SP.
11.2.6.2. Seja localmente em seu computador ou por meio da rede, os usuários não podem alterar, copiar e/ou excluir arquivos pertencentes a outro usuário sem primeiro obter sua permissão.
11.2.6.3. A rede não deve ser utilizada para transmitir ou armazenar informações que não sejam do interesse ou não contribuam com os objetivos do SEBRAE-SP.
11.2.6.4. Ao se ausentar ou sair, o usuário deverá desconectar seu login aberto ou bloquear sua estação de trabalho, para que não haja utilização indevida dos ativos de TI.
11.2.6.5. Todo usuário deve fazer uso racional dos recursos, observando os limites de utilização estabelecidos pela política de segurança da entidade.
11.2.6.6. O horário de acesso à rede de computadores restringe-se às normas e aos procedimentos vigentes, podendo ser ampliado mediante autorização, conforme norma especifica.

.2.7. Internet

A internet é uma rede mundial de computadores. Por sua diversidade de plataformas e a quantidade de computadores e usuários esse ambiente é propício para o surgimento e a disseminação de vírus em variados formatos, conteúdo ilegal e outros incidentes de segurança.

.2.7.1. Devem ser adotadas as seguintes práticas:

a) Todo o tráfego de utilização da internet será monitorado. Mediante solicitação, relatórios de utilização poderão ser emitidos e divulgados de acordo com os critérios estabelecidos, em documento específico, pela CSTI.
b) Todo o conteúdo recebido ou enviado através da internet será automaticamente submetido a verificações de segurança para eliminação de vírus e tentativas de invasão do ambiente de rede corporativa.
c) O SEBRAE-SP não se responsabilizará por problemas ocasionados em virtude do fornecimento de informações pessoais dos seus usuários na internet, tais como: números de cartão de crédito ou contas correntes bancárias e senhas para acesso a sistemas de internet *banking*.
d) Novos recursos na internet, além do acesso à *web* e ao correio eletrônico, deverão ser liberados somente mediante prévia análise de riscos de segurança e comprovação da necessidade e/ou benefícios do serviço para o SEBRAE-SP.

2.8. Senhas

Senhas devem ser escolhidas criteriosamente. Estatísticas comprovam que são por meio de senhas malformadas que a maioria das invasões a sistemas ocorre.

As seguintes práticas devem ser observadas:

.2.8.1. Após efetuar o seu primeiro acesso à rede corporativa, por meio de uma senha padrão fornecida pela equipe técnica da área de TI, o usuário receberá um aviso automático solicitando a mudança para uma nova senha.
.2.8.2. Senhas devem ser memorizadas, nunca escritas e registradas em papel ou digitalmente.
2.8.3. Senhas são individuais e nunca poderão ser compartilhadas com outros usuários.
2.8.4. Senhas devem ser trocadas a cada 3 (três) meses, ou imediatamente se comprometidas.
.2.8.5. Administradores de sistema executarão procedimentos periódicos de verificação de vulnerabilidade de senhas, para identificar se a escolha foi inadequada e solicitar a respectiva alteração.
.2.8.6. O usuário deve adotar como regra de formação de senhas:

a) Escolher senhas com 8 (oito) ou mais caracteres, compostos sempre por letras e números em conjunto;
b) Mesmo estando os sistemas configurados para minimizar a ocorrência de senhas vulneráveis, nunca deverão ser escolhidas senhas óbvias baseadas em: datas de aniversário da pessoa ou parentes, nomes abreviados, nomes próprios, apelidos, nomes de parentes, números de telefone, dentre outros;
c) Nunca utilize como senha o *login* de acesso à rede ou ao sistema;
d) Nunca escolha senhas baseadas em palavras contidas em dicionários. Grande parte dos incidentes de segurança ocorre por meio de métodos de exploração de senhas por força bruta utilizando, por exemplo, todas as palavras de um dicionário armazenadas em um banco de dados como possíveis senhas;
e) Use símbolos do tipo "%", "-" ou "$" para formar a senha.

2.9. Suporte aos usuários dos ativos de TI

.2.9.1. O suporte aos ativos de TI é realizado de acordo com os horários de atendimentos estabelecidos pelo SEBRAE-SP por meio de abertura de chamado técnico.

.2.9.2. É de responsabilidade de TI certificar-se de que o atendimento e a solução proposta seguem os padrões e o tempo estabelecidos.

.2.10. Sistemas corporativos

.2.10.1. Os usuários não podem instalar ou utilizar qualquer tipo de sistema ou aplicativos para desenvolvimento de bases de informação, paralelas aos sistemas corporativos adotados e homologados pelo SEBRAE-SP.

2.10.2. São de responsabilidade do usuário todas as informações inseridas por ele nos sistemas corporativos do SEBRAE-SP.

.2.10.3. Os usuários devem comprometer-se a informar quaisquer problemas encontrados nos sistemas do SEBRAE-SP, podendo facultativamente dar sugestões para a sua melhoria, por meio do helpdesk.

3. Da formalização

3.1. Termo de compromisso para usuários de ativos de TI

Todos os usuários deverão previamente assinar o "Termo de Compromisso para Usuários de Ativos de TI", (Anexo II), que trata do "de acordo" aos padrões e às recomendações estabelecidas pela PSTI.

.3.2. Rescisão de contrato

O término e a rescisão dos contratos de trabalho, de prestação de serviços em geral ou quaisquer outros tipos de Convênios, Acordos e Termos com o SEBRAE-SP implicarão na extinção imediata de todos os direitos de uso e acesso aos ativos da TI que possuíam o indivíduo ou empresa.

a) Cabe a unidade de Gestão de Pessoas informar à unidade de Tecnologia da Informação sobre as contratações e as rescisões de funcionários em geral, garantindo a segurança contra acessos indevidos, após o término do período estabelecido para utilização dos ativos de TI.b) Cabe a área contratante informar à unidade de Tecnologia da Informação sobre as contratações e as rescisões de terceiros em geral, garantindo a segurança contra acessos indevidos, após o término do período estabelecido para utilização dos ativos de TI.

.3.3. A unidade de Tecnologia da Informação poderá providenciar backup (cópia) das informações do usuário que estiver em processo de rescisão contratual, quando solicitado pelo gestor da área pertinente, e encaminhará essas informações à unidade de Gestão de Pessoas.

.4. Do monitoramento de tráfego e segurança

Os ativos de TI e quaisquer informações e conteúdos neles armazenados pertencem ao SEBRAE-SP; sendo assim, serão submetidos a processos de monitoramento de tráfego e segurança, garantindo

estabilidade, integridade, disponibilidade e confidencialidade do ambiente. O SEBRAE-SP não necessitará de qualquer tipo de aviso ou autorização judicial para executar tais ações.

.5. Da auditoria de conteúdo

Os ativos de TI e quaisquer informações e conteúdos neles armazenados pertencem ao SEBRAE-SP; sendo assim, poderão ser submetidos a processos de auditoria, caso ocorram incidentes de segurança. Tal processo só poderá ser autorizado pela Diretoria Executiva.

.6. Da comunicação dos incidentes e medidas disciplinares

.6.1 Comunicação

Todos os incidentes de segurança deverão ser relatados à unidade de TI pelo e-mail indicado (seguranca@sp.sebrae.com.br), com cópia para o CSTI - Comitê de Segurança de Tecnologia da Informação ao SEBRAE-SP, por meio do e-mail indicado (csti@sp.sebrae.com.br).

.6.2 A conivência ou omissão por parte dos usuários perante os incidentes de segurança é considerada como grave incidente.

.6.3 Medidas Disciplinares

Os usuários estarão sujeitos à aplicação de medidas disciplinares, que poderão chegar à demissão ou à rescisão de contrato, nos casos de incidentes desta política de segurança.

.7. Das Disposições Finais

.7.1. Divulgação

O SEBRAE-SP, através das unidades de Gestão de Pessoas, Tecnologia da Informação, Marketing e Comunicação, compromete-se a empregar esforços para informar, sensibilizar e conscientizar todos os usuários dos ativos de TI dos termos desta política.

.7.2. Alterações da política de segurança

A PSTI deverá ser revisada/atualizada anualmente pelo CSTI, de acordo com as necessidades do SEBRAE-SP.

.7.3 Situações não-previstas pela PSTI

Encaminhar ao CSTI, por meio do e-mail: (csti@sp.sebrae.com.br), quaisquer situações não-previstas pela PSTI. O CSTI compromete-se a analisar e responder aos incidentes de segurança no prazo de até 5 (cinco) dias úteis.

ANEXO II - TERMO DE COMPROMISSO PARA USUÁRIOS DE ATIVOS DE TI

Este termo de compromisso aplica-se a todos os usuários de ativos de Tecnologia da Informação do SEBRAE-SP.

Termo de Compromisso

Declaro que li e estou de acordo com a Política de Segurança da Tecnologia da Informação do SEBRAE-SP e com o Manual de Padrões e Recomendações de Usuários, tendo ciência de todo o seu conteúdo.

Declaro, ainda, estar ciente de que incidentes contrários à política de segurança resultarão em medidas que poderão chegar inclusive ao meu desligamento do quadro efetivo do SEBRAE-SP, à rescisão do contrato e à aplicação de medidas judiciais ou outras medidas pertinentes.

Comprometo-me a preservar a integridade, a disponibilidade e a confidencialidade das informações obtidas durante a vigência do contrato com o SEBRAE-SP, mesmo após o seu encerramento.

Em sendo prestador de serviço terceirizado comprometo-me igualmente no cumprimento das regras e diretrizes previstas nesta PSTI.

_____,_____de_____de 20__

DADOS DO FUNCIONÁRIO

Nome: _____

CPF: _____**R.E:**_____

Unidade de ação: _____ **Tel/Ramal:** _____

DADOS DO PRESTADOR DE SERVIÇOS/PARCEIRO

Nome: _____

CPF: _____ **Unidade de ação:** _____

Nome da Empresa: _____ **CNPJ:** _____

Endereço Comercial: _____

Telefone Com: ( ) _____ _____**Fax: ( )** _____

e-mail: _____

Para uso da U.O.Tecnologia da Informação

Nome do *login* na rede: _____

Nome da conta de e-mail: _____

Data de início e término de utilização dos ativos de TI: de ___/___/____ a ___/___/____

Nome do gestor do usuário/ ramal/ contato:_____

ANEXO III – HARDWARE, SOFTWARE E SISTEMAS HOMOLOGADOS

Os *hardwares* abaixo relacionados são os únicos homologados para uso comum dos usuários pelo SEBRAE-SP. Entende-se por hardware homologado os equipamentos que pertencem ao ativo imobilizado do SEBRAE-SP.

Os *hardwares* que não estão listados e que não pertencem ao SEBRAE-SP somente poderão acessar a rede corporativa com previa autorização, conforme Termo de Condições de Uso (ANEXO I).

Os *softwares* que não estão listados e não foram autorizados pela unidade de TI serão removidos.

***Hardwares* homologados pela entidade:**

- Microcomputadores
- *Computadores Portáteis*
- Impressoras laser
- Impressoras jato de tinta
- Servidores
- *Switches*
- *Scanner*
- Câmera digital
- *Pen Drive*
- *Smartphone*
- *Equipamentos de rede sem fio*
- *Mini modem*

***Softwares* homologados pela entidade:**

- *Windows XP Professional/ Windows Vista / Windows 7*
- *Office 2003 Professional/ Office 2007*
- *Acrobat Reader*
- *Symantec Endpoint Protection*
- *7-Zip*
- *Power Archiver 2000*
- *PDF Creator*
- *Cyberlink PowerDVD*
- *Microsoft Office Communicator*
- *VNC Free Edition*
- *Nero 7 Essentials*
- *OCS Inventory Agent*
- *Just Print client*
- *Internet Explorer 7 e 8*
- *Microsoft Project Professional 2003 e 2007*
- *Microsoft Visio Professional 2003 e 2007*
- *Windows Media Player*

Sistemas corporativos homologados:

- **Jurídico** – Cadastro de processos jurídicos, que incluem convênios e compras/ contratações (licitação), além de integrar informações do Oracle.
- **Consultoria –** sistema de gerenciamento e agendamento dos atendimentos prestados.
- **Feiras –** sistema de gerenciamento e controle dos eventos do SEBRAE-SP.
- **Atendimento –** sistema de registro dos atendimentos através da Central de Relacionamento e Escritórios Regionais.
- **Incubadoras –** sistema de gerenciamento e cadastramento dos convênios entre o SEBRAE-SP e Gestores das incubadoras das empresas.
- **Ações e Resultados –** sistema de gerenciamento e acompanhamento dos projetos e atividades finalisticas do SEBRAE-SP e seus parceiros.
- **RM Sistemas –** sistema de gestão empresarial administrativa e financeira integrado, que permite ao SEBRAE-SP gerenciar melhor os processos.
- **Processos de RH –** Gerencia requisição de funcionários, solicitação de alteração salarial, solicitação de treinamento de funcionários, mantendo históricos das movimentações.
- **Ouvidoria –** sistema de registro e controle dos fluxos das ocorrências recebidas pela Ouvidoria.
- **Protocolo Central (GEDOC) –** registra e consulta o recebimento e distribuição de correspondências e documentos na sede do SEBRAE-SP, de forma estruturada e corporativa.
- **Bolsa de Negócios –** sistema de cadastramento de empresas e empreendedores nacionais e internacionais e suas oportunidades de negócios para divulgação impressa ou via e-mail.
- **Educação Corporativa –** é um sistema que oferece aos funcionários do SEBRAE-SP a visão antecipada das ações de desenvolvimento de pessoal, através da divulgação detalhada, possibilitando o planejamento dos desenvolvidos.
- **Fundo Fixo – controla** a liberação da Ordem de Pagamento e dos respectivos valores aos responsáveis pelo Fundo Fixo nos Escritórios Regionais.
- **Kayako –** gerenciador de chamados de help desk para o atendimento aos usuários do SEBRAE-SP e seus consultores técnicos na distribuição de áreas e funções e gerenciador de chamados de web desk para inclusão e atualização de conteúdos que se destina a intranet, internet e extranet.
- **Webconferência –** gerenciador de webconferências realizadas pelo SEBRAE-NA ou pelo SEBRAE-SP, ajudando a pesquisar e administrar todas as webconferências realizadas;
- **Videoconferência –** gerenciador de videoconferências realizadas pelo Sebrae-NA ou pelo SEBRAE-SP, ajudando a gerenciar todas as videoconferências realizadas e que são disponibilizadas na Intranet.
- **Sistema de Atendimento ao Cliente (SAC) –** sistema gerenciador de cadastro de clientes e produtos oferecidos pelo SEBRAE/SP.

ANEXO IV - CONTRATO DE CONFIDENCIALIDADE – Política de Privacidade do banco de Dados dos Clientes

Pelo presente instrumento particular, e na melhor forma de direito, (NOME DA EMPRESA) com sede (ENDEREÇO COMPLETO: CEP, CIDADE, ESTADO), inscrita no CNPJ sob o nº 00.000.000/0000-00, neste ato, representada na forma de seu Contrato Social (doravante simplesmente denominada "PRESTADORA"), por si, seus funcionários, dirigentes e qualquer outra pessoa a ela relacionada, assume o compromisso irrevogável e irretratável de manter o mais absoluto sigilo de toda informação que lhe for disponibilizada (as "Informações Confidenciais") pelo SEBRAE-SP.

A expressão "Informações Confidenciais" significa toda e qualquer informação que venha a ser divulgada à PRESTADORA pelo SEBRAE-SP, de forma escrita ou magnética, durante o desenvolvimento dos serviços a serem prestados pela PRESTADORA. As informações conferidas à PRESTADORA deverão ser mantidas em absoluto sigilo, mesmo após finalizada a prestação de serviços, por constituírem objeto de sigilo, sob pena de obrigar-se a PRESTADORA a indenizar o SEBRAE-SP, a qualquer tempo, por danos e/ou prejuízos sofridos em decorrência da falha de manutenção de sigilo ou sua quebra, por parte de seus funcionários, dirigentes ou outra qualquer pessoa à qual tenha dado acesso às Informações Confidenciais.

Para tanto, o SEBRAE-SP conta com instrumentos de fiscalização inseridos em sua Base de Dados que tornam possíveis a identificação de bases corrompidas pela PRESTADORA.

São Paulo-SP, _____de _____ de 2003

_____
(NOME DO RESPONSÁVEL)
(NOME DA EMPRESA)

Testemunhas:

1.

2.