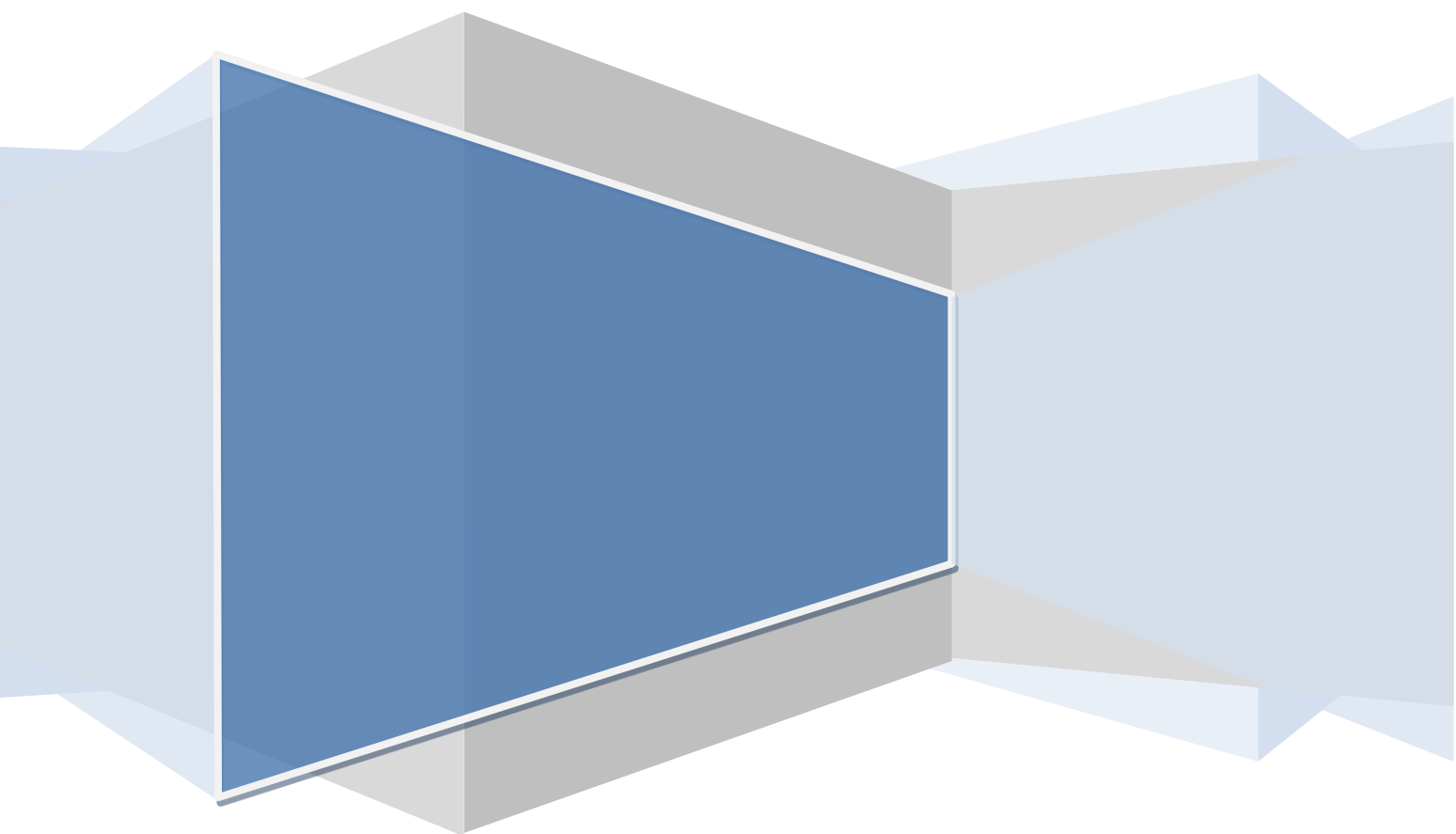


# **POLÍTICA DE SEGURANÇA DA INFORMAÇÃO**

## **PSI**



**AGOSTO DE 2016**

# POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

## Sumário

<b>1. INTRODUÇÃO</b>	<b>3</b>
<b>2. OBJETIVOS</b>	<b>3</b>
<b>3. APLICAÇÕES DA PSI</b>	<b>4</b>
<b>4. PRINCÍPIOS DA PSI</b>	<b>5</b>
<b>5. DIRETRIZES GERAIS DE SEGURANÇA DA INFORMAÇÃO</b>	<b>5</b>
<b>6. DIRETRIZES PARA INFORMAÇÕES CONFIDENCIAIS</b>	<b>7</b>
<b>7. DIRETRIZES PARA UTILIZAÇÃO DA REDE</b>	<b>8</b>
<b>8. DIRETRIZES PARA INSTALAÇÃO E REMOÇÃO DE SOFTWARES</b>	<b>9</b>
<b>9. DIRETRIZES PARA UTILIZAÇÃO DOS SISTEMAS CORPORATIVOS</b>	<b>10</b>
<b>10. DIRETRIZES PARA UTILIZAÇÃO DA INTERNET</b>	<b>11</b>
<b>11. DIRETRIZES PARA UTILIZAÇÃO DE CORREIO ELETRÔNICO (E-MAIL)</b>	<b>12</b>
<b>12. DIRETRIZES PARA UTILIZAÇÃO DE DISPOSITIVOS MÓVEIS (CONSUMERIZAÇÃO)</b>	<b>14</b>
<b>13. DIRETRIZES PARA UTILIZAÇÃO DE ACESSO REMOTO À REDE DO SEBRAE PREVIDÊNCIA</b>	<b>15</b>
<b>14. DIRETRIZES PARA UTILIZAÇÃO DE ACESSO REMOTO AO HOSTING</b>	<b>16</b>
<b>15. DIRETRIZES PARA UTILIZAÇÃO DE CONTAS E SENHAS DE ACESSO</b>	<b>17</b>
<b>16. CONDIÇÕES GERAIS</b>	<b>18</b>
<b>17. PENALIDADES</b>	<b>19</b>
<b>18. MEMBROS DA EQUIPE DE SEGURANÇA DA INFORMAÇÃO</b>	<b>20</b>
<b>19. VIGÊNCIA, VALIDADE E ATUALIZAÇÕES</b>	<b>20</b>
<b>GLOSSÁRIO</b>	<b>21</b>

## **1. INTRODUÇÃO**

A informação utilizada pelo SEBRAE PREVIDÊNCIA é um bem que tem valor. A informação deve ser protegida, cuidada e gerenciada adequadamente com o objetivo de garantir sua disponibilidade, integridade, confidencialidade, legalidade e auditabilidade, independentemente do meio de armazenamento, processamento ou transmissão que esteja sendo utilizado.

O desenvolvimento e a implantação da Política de Segurança da Informação - PSI é uma importante ferramenta para combater ameaças aos ativos do Instituto. Esta PSI é um conjunto de diretrizes e orientações de procedimentos que visam conscientizar e orientar os empregados, clientes, parceiros, colaboradores e fornecedores para o uso seguro dos ativos do Instituto.

A Gestão de Continuidade de Negócios, disposta em norma específica, tem por objetivo, em relação à segurança da informação, garantir níveis adequados de disponibilidade, integridade, confidencialidade e autenticidade das informações essenciais ao funcionamento dos processos críticos do SEBRAE PREVIDÊNCIA.

## **2. OBJETIVOS**

A Política de Segurança da Informação – PSI tem como objetivos:

I) Registrar os princípios e as diretrizes de segurança adotados pelo Instituto, a serem observados por todos os seus integrantes e colaboradores e aplicados a todos os sistemas de informação e processos corporativos.

II) Definir o tratamento que deve ser dado às informações armazenadas, processadas ou transmitidas no ambiente convencional ou no ambiente tecnológico.

III) Preservar as informações do SEBRAE PREVIDÊNCIA quanto a:

- a. **Confidencialidade:** propriedade que garante que a informação seja acessada somente pelas pessoas ou processos que tenham autorização para tal;
- b. **Integridade:** propriedade que garante a não violação das informações com intuito de protegê-las contra alteração, gravação ou exclusão indevida, acidental ou proposital;
- c. **Disponibilidade:** propriedade que garante que as informações estejam acessíveis às pessoas e aos processos autorizados, no momento requerido;
- d. **Autenticidade:** propriedade que assegura a correspondência entre o autor de determinada informação e a pessoa, processo ou sistema a quem se atribui a autoria;

As orientações aqui apresentadas são os princípios fundamentais e representam como o SEBRAE PREVIDÊNCIA exige que a informação seja utilizada.

### 3. APLICAÇÕES DA PSI

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

Esta política dá ciência a cada colaborador de que os ambientes, sistemas, computadores e redes da empresa poderão ser monitorados e gravados, com prévia informação, conforme previsto nas leis brasileiras.

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

## **4. PRINCÍPIOS DA PSI**

Toda informação produzida ou recebida pelos colaboradores como resultado da atividade profissional pertence ao SEBRAE PREVIDÊNCIA. As exceções devem ser explícitas e formalizadas.

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

Deverá constar em todos os contratos do SEBRAE PREVIDÊNCIA Cláusula de Confidencialidade, como condição imprescindível para que possa ser concedido o acesso aos ativos de informação disponibilizados pela instituição.

A responsabilidade em relação à segurança da informação deve ser comunicada na fase de contratação dos colaboradores. Todos os colaboradores devem ser orientados sobre os procedimentos de segurança, bem como o uso correto dos ativos, a fim de reduzir possíveis riscos. Eles devem assinar um termo de responsabilidade e de conhecimento desta PSI, bem como de suas atualizações.

## **5. DIRETRIZES GERAIS DE SEGURANÇA DA INFORMAÇÃO**

- a. Esta Política define as Diretrizes para a Segurança da Informação, visando preservar a integridade, confidencialidade e disponibilidade das informações sob gestão do SEBRAE PREVIDÊNCIA. Descreve a conduta considerada adequada para o manuseio, controle e proteção das informações contra destruição, modificação, divulgação indevida e acessos não autorizados, sejam acidentalmente ou intencionalmente, em consonância com o Código de Ética do Instituto.
- b. Somente atividades lícitas, éticas e administrativamente admitidas devem ser realizadas, pelos usuários quando na utilização dos recursos de processamento da informação do SEBRAE PREVIDÊNCIA.

- c. É vedado o acesso de pessoas não autorizadas ao CPD do SEBRAE PREVIDÊNCIA.
- d. O acesso de visitantes à Área Técnica ou às áreas internas do SEBRAE PREVIDÊNCIA deverá ser supervisionado ou por Diretor ou colaborador.
- e. A identificação do usuário por meio de senha é pessoal e intransferível, qualificando-o como responsável por todas as atividades desenvolvidas através dela.
- f. O cumprimento da Política de Segurança, pelos usuários, poderá ser auditado pelo SEBRAE PREVIDÊNCIA.
- g. O SEBRAE PREVIDÊNCIA se reserva o direito de monitorar, automaticamente, o tráfego efetuado através das suas redes de comunicação, incluindo o acesso à Internet e o uso do Correio Eletrônico.
- h. O SEBRAE PREVIDÊNCIA possui uma rede integrada de computadores com servidores e um microcomputador para cada usuário.
- i. Os acessos aos diretórios dos servidores e aos sistemas corporativos possuem senha de entrada com registro de “log” e sistema de back-up automático.
- j. Os usuários deverão proteger o acesso a seus computadores através de tela de bloqueio a ser liberada mediante senha, quando os mesmos não estiverem em uso.
- k. Além das cópias de segurança “backup” normalmente realizadas no servidor, será feita cópia de segurança adicional mantida em dispositivo externo com as informações codificadas (encriptografadas) em ambiente seguro para armazenagem fora do SEBRAE PREVIDÊNCIA.
- l. O acesso à internet é feito com tecnologia fornecida por operadora especializada.

m. As informações em formato físico devem ser acondicionadas em armários específicos ou destruídas em triturador de papel, quando se tratar de documentos confidenciais a serem inutilizados.

## **6. DIRETRIZES PARA INFORMAÇÕES CONFIDENCIAIS**

### **Objetivo:**

Estabelecer responsabilidades e requisitos básicos de utilização dos dados do SEBRAE PREVIDÊNCIA.

### **Abrangência:**

Aplicada aos ativos de informação e comunicação do SEBRAE PREVIDÊNCIA.

### **Conceito:**

São consideradas informações confidenciais, para os fins desta Política, quaisquer informações das partes consideradas não disponíveis ao público ou reservadas.

- a. É expressamente proibida a divulgação de informações dos Participantes;
- b. Informações confidenciais, quando impressas, deverão ser retiradas imediatamente das impressoras;
- c. Informações confidenciais impressas, quando não estiverem sendo utilizadas, deverão ser armazenadas em local fechado e seguro;
- d. Nenhuma das informações confidenciais podem ser repassadas para terceiros sem consentimento por escrito da Diretoria Executiva do SEBRAE PREVIDÊNCIA.

## 7. DIRETRIZES PARA UTILIZAÇÃO DA REDE

### **Objetivo:**

Estabelecer responsabilidades e requisitos básicos de utilização da rede do SEBRAE PREVIDÊNCIA.

### **Abrangência:**

Aplicada a todos os usuários que utilizam a rede do SEBRAE PREVIDÊNCIA.

### **Conceito:**

O acesso à rede permite aos usuários trafegar informações de internet, correio eletrônico e sistemas disponibilizados pelo SEBRAE PREVIDÊNCIA. Uma rede é definida como um conjunto de computadores interligados com o objetivo de permitir a transmissão das informações. Quanto à acessibilidade, podem ser públicas ou privadas. As redes privadas possibilitam a transmissão restrita de informações dentro do domínio de uma instituição pública ou privada; esta rede privada denomina-se intranet. As redes públicas permitem ao usuário a interconexão entre redes privadas. Quanto aos meios de transmissão, a informação pode ser enviada por conexões sem fio (Ex.: rádio e infravermelho) ou por conexões que utilizem cabeamento (Ex.: fibra ótica, cabo coaxial e par trançado).

- a. O usuário é responsável pela própria e devida autenticação nos sistemas de redes disponibilizados pelo SEBRAE PREVIDÊNCIA, não podendo fornecer e/ou compartilhar seu usuário, senha e/ou acesso à rede com outros usuários;
- b. O usuário está comprometido a utilizar as redes públicas e ou privadas do SEBRAE PREVIDÊNCIA para uso exclusivo de atividades relacionadas ao setor no qual o usuário pertence;
- c. É proibida a utilização de *proxies* não autorizados que permitam o tráfego de informações a redes privadas externas;



- d. É proibido o acesso a redes que disponibilizem conteúdos obscenos, pornográficos, eróticos, racistas, nazistas e de qualquer outro conteúdo que viole a lei;
- e. O usuário deve garantir que as senhas de acesso à rede não sejam enviadas a outras pessoas, pois a senha é de uso pessoal, intransferível e sigilosa.

## **8. DIRETRIZES PARA INSTALAÇÃO E REMOÇÃO DE SOFTWARES**

### **Objetivo:**

Estabelecer um conjunto de diretrizes e recomendações aos diferentes usuários sobre os procedimentos de instalação e/ou remoção de programas nos equipamentos do SEBRAE PREVIDÊNCIA.

### **Abrangência:**

Aplicada a todos os usuários do SEBRAE PREVIDÊNCIA que necessitam instalar e/ou remover programas dos computadores.

### **Conceito:**

Todo e qualquer programa (software) são ferramentas e/ou instrumentos que auxiliam civis, empresas, governos, instituições de pesquisa, instituições de ensino, entre outros a realizar suas respectivas atividades. Os softwares podem ser executados em desktops, estações de trabalho, servidores, mainframes, roteadores, celulares, e em qualquer outro dispositivo computacional. Quanto aos tipos de programas eles podem ser: software de sistema e software de aplicativo. Os softwares de sistema são responsáveis pela integração entre máquina, periféricos e software de aplicativo. Os softwares de aplicativo são responsáveis pela interação entre o usuário e suas atividades. Alguns exemplos de software são: sistemas operacionais, planilhas eletrônicas, editores de texto, editores de imagens, visualizadores de arquivos, mensageiros instantâneos, correio eletrônico, dentre outros. O acesso de um aplicativo pode ser realizado localmente (quando acessados fisicamente na máquina utilizada) e/ou

remotamente (quando os aplicativos são providos por outros equipamentos diferentes da máquina utilizada fisicamente).

- a. O usuário é proibido de instalar todo e qualquer programa não autorizado no computador e qualquer outro dispositivo computacional pertencente ao SEBRAE PREVIDÊNCIA, salvo as instalações de programas que contenham prévia autorização da Diretoria Executiva. Este item também é aplicado a programas com conteúdo de atualização conhecidos como *patches*;
- b. O usuário é proibido de remover toda e qualquer versão de software obsoleto, mesmo em casos onde exista uma versão atualizada da aplicação utilizada;
- c. Caso o usuário necessite instalar ou remover qualquer software, deverá entrar em contato com o gestor responsável.

## **9. DIRETRIZES PARA UTILIZAÇÃO DOS SISTEMAS CORPORATIVOS**

### **Objetivo:**

Estabelecer responsabilidades e requisitos básicos de utilização dos Sistemas Corporativos no ambiente de Tecnologia da Informação e Comunicação do SEBRAE PREVIDÊNCIA.

### **Abrangência:**

Aplicada a todos os usuários que utilizam os Sistemas Corporativos do SEBRAE PREVIDÊNCIA.

### **Conceito:**

Os Sistemas Corporativos são os sistemas utilizados na gestão do SEBRAE PREVIDÊNCIA de forma integrada, trazendo maior transparência, rapidez e confiabilidade para as informações, abrangendo todos os seguimentos da administração e permitindo o gerenciamento isolado de cada parte e a

interligação desta com o todo, produzindo relatórios analíticos, sintéticos e estatísticos, sendo acessados através de uma rede interna ou externa.

- a. É expressamente proibida a divulgação e/ou o compartilhamento indevido das informações contidas nos Sistemas Corporativos.
- b. Todos os Usuários dos ativos de informação de propriedade do SEBRAE PREVIDÊNCIA, ao utilizarem esse serviço, deverão fazê-lo no estrito interesse do SEBRAE PREVIDÊNCIA, mantendo uma conduta profissional.
- c. O acesso às informações contidas nos Sistemas Corporativos deve ser efetuado sempre através de identificação segura (chave e senha).
- d. Para cada usuário serão atribuídas permissões específicas, por módulo ou operação.
- e. O usuário é pessoalmente responsável por todas as atividades realizadas por intermédio de sua chave de acesso.

## **10. DIRETRIZES PARA UTILIZAÇÃO DA INTERNET**

### **Objetivo:**

Estabelecer responsabilidades e requisitos básicos de utilização da Internet no ambiente de Tecnologia da Informação e Comunicação do SEBRAE PREVIDÊNCIA.

### **Abrangência:**

Aplicada a todos os usuários que utilizam os recursos disponibilizados pelo SEBRAE PREVIDÊNCIA para acesso à Internet.

### **Conceito:**

Sob o aspecto de proteção e integridade dos sistemas de informação, a Internet é classificada como conexão de alto risco. Os Usuários devem estar cientes, portanto, das peculiaridades da navegação na Internet, antes de acessá-la e de utilizar os seus recursos.

- a. É expressamente proibida a divulgação e/ou o compartilhamento indevido de informações sigilosas em listas de discussão ou bate-papo.
- b. Os usuários poderão fazer download de arquivos da Internet que sejam necessários ao desempenho de suas atividades desde que observado os termos de licença de uso e registro desses programas.
- c. O usuário deve utilizar a Internet de forma adequada e diligente.
- d. O usuário deve utilizar a Internet observando a conformidade com a lei, a moral, os bons costumes aceitos e a ordem pública.
- e. O usuário deve se abster de utilizar a Internet com objetivos ou meio para a prática de atos ilícitos, proibidos pela lei ou pela presente Política, lesivos aos direitos e interesses da Entidade ou de terceiros, ou que, de qualquer forma, possam danificar, inutilizar, sobrecarregar ou deteriorar os recursos tecnológicos (hardware e software), bem como os documentos e arquivos de qualquer tipo, de seu uso ou de uso de terceiros.
- f. O usuário é pessoalmente responsável por todas as atividades realizadas por intermédio de sua chave de acesso.
- g. Não é permitida a utilização de software de peer-to-peer (P2P), tais como Torrent, Kazaa, Emule e afins.
- h. Não é permitido acesso a sites de Proxy.

## **11. DIRETRIZES PARA UTILIZAÇÃO DE CORREIO ELETRÔNICO (E-MAIL)**

### **Objetivo:**

Estabelecer responsabilidades e requisitos básicos de uso dos serviços de Correio Eletrônico, no ambiente de Tecnologia da Informação e Comunicação (TIC) do SEBRAE PREVIDÊNCIA.

### **Abrangência:**

Aplicada aos ativos de informação e comunicação do SEBRAE PREVIDÊNCIA.

### **Conceito:**

Prover a comunicação é, sem dúvida, a essência das redes. As pessoas sempre procuraram se corresponder da maneira mais rápida e fácil possível. O correio eletrônico (e-mail) é a aplicação que mais ilustra esta procura, pois reúne, entre outros, estes atributos. Entretanto, a facilidade de correio eletrônico fornecido pelo SEBRAE PREVIDÊNCIA deve ser usada no interesse do serviço, podendo ser, ocasionalmente, utilizada para mensagens pessoais curtas e pouco frequentes.

- a. Todos os Usuários dos ativos de informação de propriedade do SEBRAE PREVIDÊNCIA, ao utilizarem esse serviço, deverão fazê-lo no estrito interesse do SEBRAE PREVIDÊNCIA, mantendo uma conduta profissional.
- b. Todas as contas de correio eletrônico terão uma titularidade, determinando a responsabilidade sobre a sua utilização.
- c. Os usuários poderão ser titulares de uma única caixa postal individual no Servidor de Correio Eletrônico, com direitos de envio/recebimento de mensagens, via Intranet e Internet.
- d. Contas com inatividade por um período igual ou superior a 60 (sessenta) dias serão bloqueadas, a fim de evitar o recebimento de novas mensagens.
- e. O usuário é o responsável direto pelas mensagens enviadas por intermédio do seu endereço de correio eletrônico;
- f. O usuário deve utilizar o Correio Eletrônico de forma adequada e diligente;
- g. É vedada a utilização do Correio Eletrônico, nas situações abaixo:
  - acesso não autorizado à caixa postal de outro usuário;
  - envio, armazenamento e manuseio de material que contrarie o disposto na legislação vigente, a moral e os bons costumes e a ordem pública;

- envio, armazenamento e manuseio de material que caracterize a divulgação, incentivo ou prática de atos ilícitos, proibidos pela lei ou pela presente Política, lesivos aos direitos e interesses do SEBRAE PREVIDÊNCIA ou de terceiros, ou que, de qualquer forma, possam danificar, inutilizar, sobrecarregar ou deteriorar os recursos tecnológicos (hardware e software), bem como os documentos e arquivos de qualquer tipo, do usuário ou de terceiros;
- envio, armazenamento e manuseio de material que caracterize: promoção, divulgação ou incentivo a ameaças, difamação ou assédio a outras pessoas; assuntos de caráter obsceno; prática de qualquer tipo de discriminação relativa a raça, sexo ou credo religioso; distribuição de qualquer material que caracterize violação de direito autoral garantido por lei; uso para atividades com fins comerciais e o uso extensivo para assuntos pessoais ou privados;
- envio de mensagens do tipo “corrente” e “spam” ;
- envio intencional de mensagens que contenham vírus eletrônico ou qualquer forma de rotinas de programação de computador, prejudiciais ou danosas;
- utilização de listas e/ou caderno de endereços do SEBRAE PREVIDÊNCIA para a distribuição de mensagens que não sejam de estrito interesse funcional e sem a devida permissão do responsável pelas listas e/ou caderno de endereços em questão.

## **12. DIRETRIZES PARA UTILIZAÇÃO DE DISPOSITIVOS MÓVEIS (CONSUMERIZAÇÃO)**

### **Objetivo:**

Estabelecer responsabilidades e requisitos básicos de utilização de dispositivos móveis no ambiente de Tecnologia da Informação e Comunicação do SEBRAE PREVIDÊNCIA.

**Abrangência:**

Aplicada a todos os usuários que utilizam os recursos disponibilizados pelo SEBRAE PREVIDÊNCIA.

**Conceito:**

Dispositivos móveis são equipamentos portáteis dotados de capacidade computacional, e dispositivos removíveis de memória para armazenamento, entre os quais se incluem, não se limitando a estes: notebooks, netbooks, smartphones, tablets, pen drives, USB drives, HD externos e cartões de memória;

- a. É expressamente proibida a divulgação e/ou o compartilhamento indevido de informações sigilosas através de dispositivos móveis.
- b. O usuário deve utilizar os dispositivos móveis de forma adequada e diligente, de forma a prevenir ações que possam danificar, inutilizar, sobrecarregar ou deteriorar os recursos tecnológicos (hardware e software), bem como os documentos e arquivos de qualquer tipo, de seu uso ou de uso de terceiros;
- c. O usuário é pessoalmente responsável por todas as atividades realizadas por intermédio de dispositivos móveis, tanto por sua guarda quanto pelos conteúdos nele instalados.

### **13. DIRETRIZES PARA UTILIZAÇÃO DE ACESSO REMOTO À REDE DO SEBRAE PREVIDÊNCIA**

**Objetivo:**

Estabelecer responsabilidades e requisitos básicos de utilização da rede do SEBRAE PREVIDÊNCIA através de acesso remoto.

**Abrangência:**

Aplicada a todos os usuários que utilizam a rede do SEBRAE PREVIDÊNCIA e/ou terceiros que utilizam serviços de acesso remoto.

**Conceito:**

A interconexão entre redes privadas a distância permite ao usuário utilizar de redes e serviços de redes disponibilizados por terceiros. O acesso a redes remotas disponibilizados por redes privadas externas permitem ao usuário acessar, utilizar e executar aplicações e sistemas operacionais disponibilizados naquele ambiente, desde que tenham acesso autorizado para isto. Por se tratar de um acesso entre redes privadas, a segurança e integridade da informação trafegada dependem das configurações da rede. Logo, este tópico tem como objetivo estipular um conjunto de diretrizes e recomendações aos diferentes usuários do SEBRAE PREVIDÊNCIA. A boa utilização destes serviços é de responsabilidade de cada usuário com seus respectivos privilégios. Cabe ressaltar que os serviços estão disponibilizados para o uso estritamente profissional e de interesse do SEBRAE PREVIDÊNCIA.

- a. O usuário somente pode realizar acesso interativo entre redes onde a permissão esteja autorizada. A autorização depende das atividades profissionais relacionadas a função exercida;
- b. O usuário deve utilizar somente o local e o ambiente físico aprovado pelo SEBRAE PREVIDÊNCIA;
- c. O usuário externo deve configurar de forma adequada o firewall e a proteção antivírus na rede externa à rede do SEBRAE PREVIDÊNCIA;
- d. O usuário somente poderá realizar as atividades em período estipulado pelo SEBRAE PREVIDÊNCIA.

## **14. DIRETRIZES PARA UTILIZAÇÃO DE ACESSO REMOTO AO HOSTING**

**Objetivo:**

Estabelecer responsabilidades e requisitos básicos de utilização do Hosting Externo do SEBRAE PREVIDÊNCIA através de acesso remoto.



**Abrangência:**

Aplicada a todos os usuários que utilizam a rede do SEBRAE PREVIDÊNCIA e/ou terceiros que utilizam serviços de acesso remoto.

**Conceito:**

Para garantia da integridade dos dados do SEBRAE PREVIDÊNCIA e utilização em caso de contingência, as informações armazenadas na rede interna estão replicadas em servidores virtuais externos (nuvem). O acesso a redes remotas permite ao usuário acessar, utilizar e executar aplicações e sistemas operacionais disponibilizados naquele ambiente, desde que tenham acesso autorizado para isto. Este tópico tem como objetivo estipular um conjunto de diretrizes e recomendações aos diferentes usuários do SEBRAE PREVIDÊNCIA. A boa utilização destes serviços é de responsabilidade de cada usuário com seus respectivos privilégios. Cabe ressaltar que os serviços estão disponibilizados para o uso estritamente profissional e de interesse do SEBRAE PREVIDÊNCIA.

- a. Por se tratar de solução de contingência devem utilizados de acordo com o estabelecido nos normativos específicos ;
- b. O usuário somente poderá realizar as atividades em período estipulado pelo SEBRAE PREVIDÊNCIA.

## **15. DIRETRIZES PARA UTILIZAÇÃO DE CONTAS E SENHAS DE ACESSO**

**Objetivo:**

Estabelecer requisitos básicos de utilização dos recursos computacionais que requerem autenticação por senhas.

**Abrangência:**

Aplicada a todos os usuários do SEBRAE PREVIDÊNCIA que utilizem recursos computacionais que requerem autenticação por senhas.

**Conceito:**

Todo o usuário do SEBRAE PREVIDÊNCIA possui para cada recurso computacional (estações de trabalho, sistemas, etc.) um identificador único provido pela Instituto, sendo que para cada identificador é associada uma senha que permite o acesso ao recurso com seus devidos privilégios.

- a. O usuário não deve armazenar as senhas anotadas em papel ou em arquivos, seja no computador ou em dispositivos móveis, de forma desprotegida ou seja, sem utilizar um meio de proteção, como, por exemplo, criptografia;
- b. As senhas de acesso tem caráter pessoal, e é intransferível, cabendo ao seu titular total responsabilidade quanto ao seu sigilo;
- c. O usuário está proibido de utilizar contas e senhas de acesso pertencentes a outros usuários;
- d. O usuário deverá realizar a troca de suas senhas de acesso, pelo menos, semestralmente.

## **16. CONDIÇÕES GERAIS**

- a. Somente poderão acessar os Sistemas Corporativos e/ou a Internet usuários que tenham sido credenciados com suas senhas de acesso.
- b. Cada Diretoria deverá, através de e-mail, solicitar à Equipe de Segurança a liberação de acesso a novos usuários, definindo os serviços que deverão ser credenciados, justificando quanto a necessidade do referido usuário utilizar-se deste recurso.
- c. A senha de acesso tem caráter pessoal, e é intransferível, cabendo ao seu titular total responsabilidade quanto seu sigilo.
- d. A prática de compartilhamento de senhas de acesso é terminantemente proibida e o titular que fornecer sua senha a outrem responderá pelas

infrações por este cometidas, estando passível das penalidades aqui previstas.

- e. Caso o usuário desconfie que sua senha não é mais segura, ou de seu domínio exclusivo, poderá solicitar à Equipe de Segurança da Informação a alteração desta.
- f. Os usuários deverão tomar conhecimento formal desta Política, além de ser concedido treinamento para facilitar o entendimento e a comunicação.
- g. Todos os usuários (empregados e fornecedores) mesmo que em caráter temporário, deverão assinar termo de ciência e concordância desta Política, declarando ter conhecimento de suas responsabilidades no manuseio de hardware, software e acesso à internet.
- h. A Equipe de Segurança da Informação deverá, pelo menos semestralmente, efetuar testes de verificação de acesso ao sistema e bloqueio automático de senha.
- i. Deverão ser observados os princípios constantes do Estatuto Social e do Código de Ética do Instituto.
- j. Por ocasião do desligamento de qualquer empregado, a Equipe de Segurança da Informação deverá providenciar o imediato cancelamento de todas as senhas de acesso aos sistemas corporativos bem como do correio eletrônico.

## **17. PENALIDADES**

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

- a. Descredenciamento da senha de acesso à Internet;
- b. Cancelamento da caixa de e-mail;
- c. Desativação do ponto de rede do usuário;

- d. O(s) usuário(s) infrator deverá(ão) ser notificado(s) e a ocorrência da transgressão imediatamente comunicada, pela Equipe de Segurança da Informação, à Diretoria correspondente e à Presidência, para aplicação das penalidades previstas no Código de Ética do SEBRAE PREVIDÊNCIA.

## **18. MEMBROS DA EQUIPE DE SEGURANÇA DA INFORMAÇÃO**

A Equipe de Segurança da Informação será diretamente responsável pela implantação e implementação da presente política, devendo reportar-se à referida Equipe todo e qualquer usuário e/ou área para tratar de assuntos pertinentes à segurança da informação de que trata este instrumento.

A Equipe de Segurança da Informação será composta por três membros, devidamente indicados pela Diretoria Executiva, por meio de Portaria.

## **19. VIGÊNCIA, VALIDADE E ATUALIZAÇÕES**

A presente política passa a vigorar a partir da data de sua aprovação pelo Conselho Deliberativo, sendo válida por tempo indeterminado.

Após a implantação desta Política, para que ela continue sendo satisfatória para o Instituto, ou melhor, para que com o tempo ela não se torne desatualizada, serão implantados controles de melhoria continua, ou seja, deverão ser realizadas revisões periódicas ou sempre que acontecer uma falha de segurança de nível médio ou grave.

## **GLOSSÁRIO**

**BACK-UP** - Cópia de dados de um dispositivo de armazenamento a outro.

**FIREWALL** - Dispositivo de uma rede de computadores que tem por objetivo aplicar uma política de segurança a um determinado ponto da rede.

**LOG** - Registro de eventos em um sistema de computadores.

**PATCHES** - Programas criados para atualizar ou corrigir um software.

**PEER-TO-PEER (P2P)** - Arquitetura de redes de computadores onde cada um dos pontos ou nós da rede funciona tanto como cliente quanto como servidor, permitindo compartilhamentos de serviços e dados sem a necessidade de um servidor central.

**PROXIES** - Servidor intermediário que atende a requisições repassando os dados do cliente à frente.

**SERVIDOR** - Sistema de computação centralizada que fornece serviços a uma rede de computadores.

**SPAN** - Mensagem de correio eletrônico publicada em massa com fins publicitários.