

RESOLUÇÃO Nº 001/2016

DISPÕE SOBRE A POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DO INSTITUTO MUNICIPAL DE PREVIDÊNCIA SOCIAL – SANTAFÉPREV

1. INTRODUÇÃO

Segurança da Informação (SI) é a disciplina dedicada à proteção da informação de forma a garantir a continuidade dos serviços, minimizando os danos e maximizando o retorno dos investimentos e as oportunidades de atuação de uma instituição.

A Política de Segurança da Informação (PSI), por sua vez, é o documento formal que orienta e estabelece as diretrizes corporativas para a proteção dos ativos de informação e a gestão da segurança da informação.

“Política de Segurança da Informação e Comunicações: documento aprovado pela autoridade responsável pelo SANTAFÉPREV, com o objetivo de fornecer diretrizes, critérios e suporte administrativo suficientes à implementação da segurança da informação e comunicações”.

Os objetivos genéricos da Política de Segurança da Informação para o Santaféprev são:

- A. Eliminar a dependência externa em relação a sistemas, equipamentos, dispositivos e atividades vinculadas à segurança dos sistemas de informação;
- B. Promover a capacitação de recursos humanos para o desenvolvimento de competência em segurança da informação;
- C. Promover as ações necessárias à implementação e manutenção da segurança da informação;

2. CAMPO DE APLICAÇÃO

Os objetivos e diretrizes estabelecidos nesta Política de Segurança da Informação serão aplicados em toda a organização; deverão ser observados por todos servidores, colaboradores, fornecedores e prestadores de serviço e se aplicam à informação em qualquer meio ou suporte. Este documento, dentre outras diretrizes, dá ciência a cada envolvido de que os ambientes, sistemas, recursos computacionais e redes informacionais do órgão poderão ser monitorados e gravados, com prévia informação, conforme previsto na legislação brasileira.

3. SEGURANÇA DA INFORMAÇÃO INSTITUTO MUNICIPAL DE PREVIDÊNCIA SOCIAL – SANTAFÉPREV

3.1 PRINCÍPIOS E OBJETIVOS

Além de buscar preservar as informações e seus respectivos ativos quanto à confidencialidade, integridade, disponibilidade e autenticidade; são objetivos da Política de Segurança da Informação do SANTAFÉPREV:

- A. Estabelecer diretrizes para a disponibilização e utilização de recursos de informação, serviços de redes de dados, estações de trabalho, internet, telecomunicações e correio eletrônico institucional.
- B. Designar, definir ou alterar papéis e responsabilidades do grupo responsável pela Segurança da Informação.
- C. Apoiar a implantação das iniciativas relativas à Segurança da Informação.
- D. Possibilitar a criação de controles e promover a otimização dos recursos e investimentos em tecnologia da informação, contribuindo com a minimização dos riscos associados.

São princípios da Política de Segurança da Informação do SANTAFÉPREV:

- A. Toda informação produzida ou recebida pelos servidores, colaboradores, fornecedores e prestadores de serviço, em resultado da função exercida e/ou atividade profissional contratada, pertence ao SANTAFÉPREV. As exceções devem ser explícitas e formalizadas entre as partes.

e-mail: santafeprev@santafeprev.com.br

Rua Sete nº 1167 - Centro - Fone/Fax (17) 3631-3468
CEP 15775-000 - ESTÂNCIA TURÍSTICA DE SANTA FÉ DO SUL/SP

PREFEITURA ESTÂNCIA TURÍSTICA
SANTA FÉ DO SUL
Trabalhando hoje, por um futuro melhor

B. Todos os recursos de informação do SANTAFÉPREV devem ser projetados para que seu uso seja consciente e responsável. Os recursos comunicacionais e computacionais da instituição devem ser utilizados para a consecução de seus objetivos finalísticos.

C. Deverão ser criados e instituídos controles apropriados, trilhas de auditoria ou registros de atividades, em todos os pontos e sistemas em que a instituição julgar necessário, com vistas à redução dos riscos dos seus ativos de informação.

D. Os gestores, administradores e operadores dos sistemas computacionais poderão, pela característica de suas credenciais como usuários (privilegios diferenciados associados a cada perfil), acessar arquivos e dados de outros usuários. Tal operação só será permitida quando necessária para a execução de atividades operacionais sob sua responsabilidade. E. Todo o acesso a redes e sistemas do órgão deverá ser feito, preferencialmente, por meio de login de acesso único, pessoal e intransferível.

F. O SANTAFÉPREV pode utilizar tecnologias e ferramentas para monitorar e controlar o conteúdo e o acesso a quaisquer tipos de informação alocada na infraestrutura provida pelo instituto.

F. Cada usuário é responsável pela segurança das informações dentro do SANTAFÉPREV, principalmente daquelas que estão sob sua responsabilidade.

G. A gestão da segurança da informação no SANTAFÉPREV será realizada por comitê multidisciplinar, ora designado Comitê de Segurança da Informação.

H. Deverá constar em todos os contratos do SANTAFÉPREV, quando o objeto for pertinente, cláusula de confidencialidade e de obediência às normas de segurança da informação a ser observada por empresas fornecedoras e por todos os profissionais que desempenham suas atividades no SANTAFÉPREV.

I. Esta Política de Segurança da Informação será implementada no SANTAFÉPREV por meio de normas e procedimentos específicos, obrigatórios para todos os usuários, independentemente do nível hierárquico ou função, bem como de vínculo empregatício ou de prestação de serviço.

4. PAPÉIS E RESPONSABILIDADES

4.1 Descrição de papéis em Segurança da Informação.

PAPEL	PERFIL ASSOCIADO	DESCRIÇÃO
Usuário Interno	Servidores públicos e demais funcionários e colaboradores internos	Todos os servidores, gestores, técnicos, estagiários, consultores e colaboradores internos, que fazem uso dos recursos informacionais e computacionais do SantaFéprev
Usuário Externo	Prestadores de Serviços e demais colaboradores externos	Prestadores de serviços contratados direta ou indiretamente pelo SantaFéprev e demais colaboradores externos que fazem uso de seus recursos informacionais e computacionais.
Área de TI	Coordenação Geral de Tecnologia da Informação	Unidade organizacional responsável pela gestão e operação dos recursos de TI na organização e custodiante da informação.

e-mail: santafeprev@santafeprev.com.br

Rua Sete nº 1167 - Centro - Fone/Fax (17) 3631-3468
CEP 15775-000 - ESTÂNCIA TURÍSTICA DE SANTA FÉ DO SUL/SP

4.2 Responsabilidades Gerais

São responsabilidades gerais de todos os usuários e gestores de serviços de rede de dados, internet, telecomunicações, estações de trabalho, correio eletrônico e demais recursos computacionais do SANTAFÉPREV:

- A. Promover a segurança de seu usuário corporativo, departamental ou de rede local, bem como de seus respectivos dados e credenciais de acesso.
- B. Seguir, de forma colaborativa, as orientações fornecidas pelos setores competentes em relação ao uso dos recursos computacionais e informacionais do instituto.
- C. Utilizar de forma ética, legal e consciente os recursos computacionais e informacionais do SANTAFÉPREV.

Os modelos de declaração de compromisso e de ciência das normas de Segurança da Informação vigentes no SANTAFÉPREV estão presentes no ANEXO I e II.

4.3 Responsabilidades específicas

4.3.1 Usuários internos e externos.

Será de inteira responsabilidade de cada usuário (interno ou externo) todo prejuízo ou dano que vier a sofrer ou causar ao SANTAFÉPREV em decorrência da não obediência às diretrizes e normas referidas na Política de Segurança da Informação e nas normas e procedimentos específicos dela decorrentes. Os usuários externos devem entender os riscos associados à sua condição e cumprir rigorosamente as políticas, normas e procedimentos específicos vigentes. O SANTAFÉPREV poderá, a qualquer tempo, revogar credenciais de acesso concedidas a usuários em virtude do descumprimento da política de SI ou das normas e procedimentos específicos dela decorrentes.

4.3.2 Gestores de pessoas e processos.

Os gestores executivos do SANTAFÉPREV devem ter postura exemplar em relação à segurança da informação, diante, sobretudo, dos usuários sob sua gestão. Cada gestor deverá manter os processos sob sua responsabilidade aderentes às políticas, normas e procedimentos específicos de segurança da informação do SANTAFÉPREV, tomando as ações necessárias para cumprir tal responsabilidade.

4.3.3 Área de Tecnologia da Informação.

Quanto à gestão de segurança da informação, serão responsabilidades específicas da área de Tecnologia da Informação:

- A. Zelar pela eficácia dos controles de SI utilizados e informar aos gestores e demais interessados os riscos residuais.
- B. Negociar e acordar com os gestores níveis de serviço relacionados a SI, incluindo os procedimentos de resposta a incidentes.
- C. Configurar os recursos informacionais e computacionais concedidos aos usuários com todos os controles necessários para cumprir os requerimentos de segurança estabelecidos pelos procedimentos, normas e políticas de segurança da informação.
- D. Garantir segurança especial para sistemas com acesso público, fazendo guarda de evidências que permitam a rastreabilidade para fins de auditoria ou investigação.
- E. Administrar, proteger e testar cópias de segurança de sistemas e dados relacionados aos processos considerados críticos para o SANTAFÉPREV.
- F. Implantar controles que gerem registros auditáveis para retirada e transporte de mídias que contenham informações custodiadas pela TI, nos ambientes totalmente controlados por ela.

e-mail: santafeprev@santafeprev.com.br

Rua Sete nº 1167 - Centro - Fone/Fax (17) 3631-3468
CEP 15775-000 - ESTÂNCIA TURÍSTICA DE SANTA FÉ DO SUL/SP

PREFEITURA MUNICIPAL DE SANTA FÉ DO SUL
SANTA FÉ DO SUL
Trabalhando hoje, por um futuro melhor

G. Informar previamente o Gestor de SI sobre o fim do prazo de retenção de informações, para que este tenha a alternativa de alterá-lo ou postergá-lo, antes que a informação seja definitivamente descartada pelo custodiante.

H. Atribuir cada conta ou dispositivo de acesso a computadores, sistemas, bases de dados e qualquer outro ativo de informação a um responsável identificável como pessoa física, responsável pelo uso da conta (a responsabilidade pela gestão dos "logins" de usuários externos é do gestor do contrato de prestação de serviços ou do gestor do setor em que o usuário externo desempenha suas atividades).

5. DIRETRIZES GERAIS.

5.1 Tratamento da informação.

Diretrizes específicas e procedimentos próprios de tratamento da informação corporativa deverão ser fixados em norma complementar, considerando as seguintes diretrizes gerais:

A. Documentos imprescindíveis para as atividades dos usuários da instituição deverão ser salvos em drives de rede. Tais arquivos, se gravados apenas localmente nos computadores, não terão garantia de backup e poderão ser perdidos caso ocorra uma falha no computador, sendo, portanto, de responsabilidade do próprio usuário.

B. Arquivos pessoais e/ou não pertinentes às atividades institucionais do SANTAFÉPREV (fotos, músicas, vídeos, etc..) não deverão ser copiados ou movidos para os drives de rede, pois podem sobrecarregar o armazenamento nos servidores. Caso identificados, os arquivos poderão ser excluídos definitivamente sem necessidade de comunicação prévia ao usuário.

5.2 Controles de Acesso.

Diretrizes específicas e procedimentos próprios de controles de acesso lógico e físico deverão ser fixados em norma complementar, considerando as seguintes diretrizes gerais:

A. O controle de acesso deverá considerar e respeitar o princípio do menor privilégio para configurar as credenciais ou contas de acesso dos usuários aos ativos de informação do SANTAFÉPREV.

B. A criação e administração de contas será realizada de acordo com procedimento específico para todo e qualquer usuário. Para o usuário que não exerce funções de administração de rede será privilegiada a criação de uma única conta institucional de acesso, pessoal e intransferível. Contas com perfil de administrador somente serão criadas para usuários cadastrados para execução de tarefas específicas na administração de ativos de informação.

C. O acesso à rede corporativa deve dar-se de forma a permitir a rastreabilidade e a identificação do usuário por período mínimo a ser definido em norma específica.

5.3 Correio Eletrônico.

Diretrizes específicas e procedimentos próprios ao serviço de correio eletrônico (e-mail) deverão ser fixadas em norma complementar, considerando as seguintes diretrizes gerais:

A. O correio eletrônico é uma ferramenta disponível e obrigatória para todos os usuários do SANTAFÉPREV, independentemente de seu vínculo funcional.

B. O uso do correio eletrônico do SANTAFÉPREV é para fins corporativos e relacionados às atividades do usuário no âmbito da autarquia.

5.4 Serviço de Backup.

Os procedimentos próprios ao serviço de backup (cópia de segurança) deverão ser fixados em norma complementar, considerando as seguintes diretrizes gerais:

e-mail: santafeprev@santafeprev.com.br

Rua Sete nº 1167 - Centro - Fone/Fax (17) 3631-3468
CEP 15775-000 - ESTÂNCIA TURÍSTICA DE SANTA FÉ DO SUL/SP

PREFEITURA DA ESPERANÇA TURÍSTICA
SANTA FÉ DO SUL
Trabalhando hoje por um futuro melhor

A. O serviço de backup deve ser automatizado por sistemas informacionais próprios considerando, inclusive, a execução agendada fora do horário de expediente normal do órgão, nas chamadas "janelas de backup" – períodos em que não há nenhum ou pouco acesso de usuários ou processos automatizados aos sistemas de informática.

B. A solução de backup deverá ser mantida atualizada, considerando suas diversas características (atualizações de correção, novas versões, ciclo de vida, garantia, melhorias, entre outros).

C. A administração das mídias de backup deverá ser contemplada nas normas complementares sobre o serviço, objetivando manter sua segurança e integridade.

5.5 Data Center.

Os procedimentos para administração do centro de processamento de dados (data center) deverão ser fixados em norma própria, considerando as seguintes diretrizes gerais:

A. A administração de dados e de serviços de data center é tarefa tecnicamente complexa e sua realização deve balizar-se nas melhores práticas de mercado e na alocação de profissionais com perfil técnico adequado.

B. O acesso físico ao data center deverá ser feito por sistema forte de autenticação, mediante uso de solução de TI própria. O acesso físico por meio de chave apenas poderá ocorrer em situações de emergência, quando a segurança física do data center estiver comprometida, como por incêndio, inundação, abalo da estrutura predial ou quando o sistema de autenticação forte não estiver funcionando.

C. O acesso ao data center por visitantes ou terceiros somente poderá ser realizado com acompanhamento de um servidor autorizado.

5.6 Monitoramento e Auditoria do Ambiente.

Para garantir a aplicação das diretrizes mencionadas nesta PSI, além de fixar normas e procedimentos complementares sobre o tema, o SANTAFÉPREV poderá:

A. Implantar sistemas de monitoramento nas estações de trabalho, servidores, correio eletrônico, conexões com a internet, dispositivos móveis ou wireless e outros componentes da rede, de modo que a informação gerada por esses sistemas possa ser usada para identificar usuários e respectivos acessos efetuados, bem como material manipulado;

B. Tornar públicas as informações obtidas pelos sistemas de monitoramento e auditoria, no caso de exigência judicial;

C. Realizar, a qualquer tempo, inspeção física nas equipamentos de sua propriedade;

D. Instalar sistemas de proteção, preventivos e detectáveis, para garantir segurança das informações e dos perímetros de acesso.

E. Desinstalar, a qualquer tempo, qualquer software ou sistema que represente risco ou esteja em desconformidade com as políticas, normas e procedimentos vigentes.

5.7 Uso e acesso a Internet.

Diretrizes específicas e procedimentos próprios de controles de uso e acesso a Internet deverão ser fixadas em norma complementar, considerando as seguintes diretrizes gerais:

A. Todas as regras corporativas sobre uso de Internet visam basicamente ao desenvolvimento de um comportamento eminentemente ético e profissional. Embora a conexão direta e permanente da rede corporativa da Instituição com a internet ofereça um grande potencial de benefícios, a proteção dos ativos de informação do SANTAFÉPREV deverá sempre ser privilegiada.

B. Perfis institucionais mantidos nas redes sociais devem, preferencialmente, ser administrados e gerenciados por equipes compostas exclusivamente por servidores públicos ocupantes de cargo efetivo.

e-mail: santafeprev@santafeprev.com.br

Rua Sete nº 1167 - Centro - Fone/Fax (17) 3631-3468
CEP 15775-000 - ESTÂNCIA TURÍSTICA DE SANTA FÉ DO SUL/SP

PREVIDÊNCIA ESTÂNCIA TURÍSTICA
SANTA FÉ DO SUL
Trabalhando hoje, por um futuro melhor

Quando não for possível, a equipe pode ser mista, desde que sob a coordenação e responsabilidade de um servidor do quadro permanente do órgão.

C. Qualquer informação que seja acessada, transmitida, recebida ou produzida na internet está sujeita à divulgação e auditoria. Portanto, o SANTAFÉPREV, em total conformidade legal, reserva-se o direito de monitorar e registrar os acessos à rede mundial de computadores.

5.8 Gestão de Riscos.

A "Gestão de Riscos de Segurança da Informação e Comunicações é o conjunto de processos que permitem identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os seus ativos de informação, e equilibrá-los com os custos operacionais e financeiros envolvidos". As diretrizes gerais do processo de Gestão de Riscos de Segurança da Informação e Comunicações do SANTAFÉPREV deverão considerar, prioritariamente, os objetivos estratégicos, os processos, os requisitos legais e a estrutura do órgão, direta e indireta, além de estarem alinhadas a esta Política de Segurança da Informação.

6. PENALIDADES.

O SANTAFÉPREV, ao gerir e monitorar seus ativos de informação, pretende garantir a integridade destes, juntamente com suas informações e recursos. O descumprimento ou inobservância de quaisquer regras ou diretrizes definidas nesse instrumento e em suas normas complementares constituem falta grave, às quais o SANTAFÉPREV responderá com a aplicação de todas as medidas administrativas, cíveis e judiciais cabíveis. Toda tentativa de alteração dos parâmetros de segurança, por qualquer usuário, sem o devido credenciamento e a autorização para tal, será considerada inadequada e os riscos relacionados serão informados ao usuário e ao respectivo gestor. O uso de qualquer recurso em inobservância das normas vigentes ou para prática de atividades ilícitas poderá acarretar ações administrativas e penalidades decorrentes de processos administrativo, civil e criminal, em que a instituição cooperará ativamente com as autoridades competentes. Os dispositivos de identificação e senhas protegem a identidade do colaborador usuário, evitando e prevenindo que uma pessoa se faça passar por outra perante o SANTAFÉPREV e/ou terceiros.

7. ESTRUTURA NORMATIVA DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO.

Os documentos que comporão a estrutura normativa de gestão de segurança da informação serão divididos em três categorias:

A. Política – nível estratégico: constituída do presente documento, define as regras de alto nível que representam os princípios básicos que o SANTAFÉPREV decidiu incorporar à sua gestão de acordo com a visão estratégica da alta direção. Serve como base para que as normas e os procedimentos sejam criados e detalhados.

B. Normas – nível tático: especificam, no plano tático, as escolhas tecnológicas e os controles que deverão ser implementados para alcançar o cenário definido estrategicamente nas diretrizes da política.

C. Procedimentos – nível operacional: instrumentalizam o disposto nas normas e na política, permitindo sua direta aplicação nas atividades do SANTAFÉPREV.

7.1 Divulgação e acesso à estrutura normativa.

Os documentos integrantes da estrutura normativa de gestão de segurança da informação deverão ser divulgados a todos os servidores, colaboradores, estagiários, aprendizes e prestadores de serviços do SANTAFÉPREV quando de sua admissão, e também publicadas na Intranet corporativa, de maneira que seu conteúdo possa ser consultado a qualquer momento.

e-mail: santafeprev@santafeprev.com.br

Rua Sete nº 1167 - Centro - Fone/Fax (17) 3631-3468
CEP 15775-000 - ESTÂNCIA TURÍSTICA DE SANTA FÉ DO SUL/SP

PREFEITURA MUNICIPAL DE SANTA FÉ DO SUL
SANTA FÉ DO SUL
Desafinando hoje, por um futuro melhor

7.2 Aprovação e revisão.

Os documentos integrantes da estrutura normativa de gestão de segurança da informação do SANTAFÉPREV deverão ser aprovados pelos Conselhos Administrativo e Fiscal.

8. REFERÊNCIAS LEGAIS E NORMATIVAS.

Referências legais e normativas:

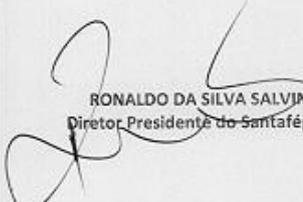
- Lei Federal 8.159/1991, de 08/01/1991 - Dispõe sobre a política nacional de arquivos públicos e privados.
- Lei Federal 9.610/1998, de 19/02/1998 - Dispõe sobre o direito autoral.
- Lei Federal 9.279/1996, de 14/05/1996 - Dispõe sobre marcas e patentes.
- Lei Federal 10.406/2002, de 10/01/2002 - Institui o Código Civil brasileiro.
- Decreto-Lei 2.848/1940, de 07/12/1940 - Institui o Código Penal brasileiro.

9. DISPOSIÇÕES FINAIS.

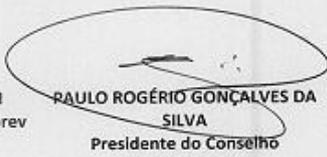
Para a uniformização da informação organizacional, esta Política de Segurança da Informação deverá ser comunicada a todos os gestores, servidores, colaboradores e prestadores de serviço do SANTAFÉPREV – a fim de que seja cumprida dentro e fora da autarquia.

O não cumprimento dos requisitos previstos nesta política, nas normas complementares e nos procedimentos de Segurança da Informação acarretará violação às regras internas da instituição e sujeitará o usuário às medidas administrativas e legais cabíveis.

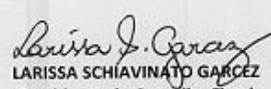
Estância Turística de Santa Fé do Sul, 10 de Agosto de 2016.
Aprovado pelos Conselhos Administrativo e Fiscal em 10/08/2016



RONALDO DA SILVA SALVINI
Diretor Presidente do SantaFéprev



PAULO ROGÉRIO GONÇALVES DA
SILVA
Presidente do Conselho
Administrativo



LARISSA SCHIAVINATO GARCEZ
Presidente do Conselho Fiscal

ANEXO I

TERMO DE COMPROMISSO CONFIDENCIALIDADE E SEGURANÇA DA INFORMAÇÃO	
IDENTIFICAÇÃO DO CONTRATO:	
Nº DO CONTRATO	
NOME DA EMPRESA CONTRATADA	
CNPJ DA CONTRATADA	
OBJETO RESUMIDO	
VIGÊNCIA CONTRATUAL	
TERMO:	
O <Contratante>, sediado em <Endereço Contratante>, CNPJ n.º <CNPJ Contratante>, doravante denominado CONTRATANTE , e, de outro lado, a <Contratada>, sediada em <Endereço Contratada>, CNPJ n.º <CNPJ Contratada>, doravante denominada CONTRATADA ;	
CONSIDERANDO que, em razão do CONTRATO N.º <nº contrato / ano> doravante denominado CONTRATO PRINCIPAL , a CONTRATADA poderá ter acesso a informações sigilosas do CONTRATANTE ;	
CONSIDERANDO a necessidade de ajustar as condições de revelação destas informações sigilosas, bem como definir as regras para o seu uso e proteção;	
CONSIDERANDO o disposto na Política de Segurança da Informação da CONTRATANTE ;	
Resolvem celebrar o presente TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO E CONFIDENCIALIDADE DAS INFORMAÇÕES , doravante TERMO , vinculado ao CONTRATO PRINCIPAL , mediante as seguintes cláusulas e condições:	
Cláusula Primeira – DO OBJETO	
Constitui objeto deste TERMO o estabelecimento de condições específicas para regulamentar as obrigações a serem observadas pela CONTRATADA , no que diz respeito ao trato de informações sensíveis e sigilosas, disponibilizadas pela CONTRATANTE - por força dos procedimentos necessários para a execução do objeto do CONTRATO PRINCIPAL celebrado entre as partes - segundo Resolução nº 001/2016, de 10 de Agosto de 2016, que regulamenta procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo, e dispõe sobre o Núcleo de Segurança e Credenciamento.	
Cláusula Segunda – DOS CONCEITOS E DEFINIÇÕES	
Para os efeitos deste TERMO , são estabelecidos os seguintes conceitos e definições:	
I. Informação: é o conjunto de dados organizados de acordo com procedimentos executados por meios eletrônicos ou não, que possibilitam a realização de atividades específicas e/ou tomada de decisão.	
II. Informação Pública ou Ostensiva: são aquelas cujo acesso é irrestrito, obtida por divulgação pública ou por meio de canais autorizados pela CONTRATANTE .	
III. Informações Sensíveis: são todos os conhecimentos estratégicos que, em função de seu potencial no aproveitamento de oportunidades ou desenvolvimento nos ramos econômico, político, científico, tecnológico, militar e social, possam beneficiar a Sociedade e o Estado brasileiros.	
IV. Informações Sigilosas: são aquelas cujo conhecimento irrestrito ou divulgação possam acarretar qualquer risco à segurança da sociedade e do Estado, bem como aquelas necessárias ao resguardo da inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas.	
V. Contrato Principal: contrato celebrado entre as partes, ao qual este TERMO DE COMPROMISSO se vincula.	
Cláusula Terceira – DAS INFORMAÇÕES SIGILOSAS	
Serão consideradas como informação sigilosa, toda e qualquer informação escrita ou oral, revelada a outra parte, contendo ou não a expressão confidencial e/ou reservada. O termo INFORMAÇÃO abrangerá toda informação escrita, verbal, ou em linguagem computacional em qualquer nível, ou de qualquer outro modo apresentada, tangível ou intangível, podendo incluir, mas não se limitando a: know-how, técnicas, especificações, relatórios, publicações, compilações, código fonte de programas de computador na íntegra ou em partes, fórmulas, desenhos, projetos, cópias, modelos, amostras de ideias, aspectos financeiros e econômicos, definições, informações sobre as atividades da CONTRATANTE e/ou quaisquer informações técnicas/comerciais relacionadas/resultantes ou não ao CONTRATO PRINCIPAL , doravante denominados INFORMAÇÕES , a que, diretamente ou pelos seus empregados, a CONTRATADA venha a ter acesso, conhecimento ou que venha a lhe ser confiada durante e em razão das atuações de execução do CONTRATO PRINCIPAL celebrado entre as partes.	
§1º – Comprometem-se as partes a não revelar, copiar, transmitir, reproduzir, utilizar, transportar ou dar conhecimento, em hipótese alguma, a terceiros, bem como a não permitir que qualquer empregado envolvido direta ou indiretamente na execução do CONTRATO PRINCIPAL , em qualquer nível hierárquico de sua estrutura organizacional e sob quaisquer alegações, faça uso dessas informações, que se restringem estritamente ao cumprimento do CONTRATO PRINCIPAL .	
§2º – As partes deverão cuidar para que as informações sigilosas fiquem restritas ao conhecimento das pessoas que estejam diretamente envolvidas nas atividades relacionadas à execução do objeto do CONTRATO PRINCIPAL .	
Parágrafo Terceiro – As obrigações constantes deste TERMO DE COMPROMISSO não serão aplicadas àquelas informações que:	

e-mail: santafeprev@santafeprev.com.br

Rua Sete nº 1167 - Centro - Fone/Fax (17) 3631-3468
CEP 15775-000 - ESTÂNCIA TURÍSTICA DE SANTA FÉ DO SUL/SP

PROFESSORIA GERENCIAL TURÍSTICA
SANTA FÉ DO SUL
"Município do Futuro Melhor"

- I. Sejam comprovadamente de domínio público no momento da revelação;
- II. Tenham sido comprovada e legitimamente recebidas de terceiros, estranhos ao presente TERMO DE COMPROMISSO;
- III. Sejam reveladas em razão de requisição judicial ou outra determinação válida do Governo, somente até a extensão de tais ordens, desde que as partes cumpram qualquer medida de proteção pertinente e tenham sido notificadas sobre a existência de tal ordem, previamente e por escrito, dando a esta, na medida do possível, tempo hábil para pleitear medidas de proteção que julgar cabíveis.

Cláusula Quarta – DOS DIREITOS E OBRIGAÇÕES

As partes se comprometem e se obrigam a utilizar a informação sigilosa revelada pela outra parte exclusivamente para os propósitos da execução do CONTRATO PRINCIPAL, em conformidade com o disposto neste TERMO DE COMPROMISSO.

§1º – A CONTRATADA se compromete a não efetuar qualquer tipo de cópia da informação sigilosa sem o consentimento expresso e prévio da CONTRATANTE.

§2º – A CONTRATADA compromete-se a dar ciência e obter o aceite formal da direção e empregados que atuarão direta ou indiretamente na execução do CONTRATO PRINCIPAL sobre a existência deste TERMO DE COMPROMISSO bem como da natureza sigilosa das informações.

I. A CONTRATADA deverá firmar acordos por escrito com seus empregados visando a garantir o cumprimento de todas as disposições do presente TERMO DE COMPROMISSO e dará ciência à CONTRATANTE dos documentos comprobatórios.

§3º – A CONTRATADA obriga-se a tomar todas as medidas necessárias à proteção da informação sigilosa da CONTRATANTE, bem como evitar e prevenir a revelação a terceiros, exceto se devidamente autorizado por escrito pela CONTRATANTE.

§4º – Cada parte permanecerá como fiel depositária das informações reveladas à outra parte em função deste

TERMO DE COMPROMISSO.

I. Quando requeridas, as informações deverão retornar imediatamente ao proprietário, bem como todas e quaisquer cópias eventualmente existentes.

§5º – A CONTRATADA obriga-se por si, sua controladora, suas controladas, coligadas, representantes, procuradores, sócios, prepostos, acionistas e cotistas, por terceiros eventualmente consultados, seus empregados, contratados e subcontratados, assim como por quaisquer outras pessoas vinculadas à CONTRATADA, direta ou indiretamente, a manter sigilo, bem como a limitar a utilização das informações disponibilizadas em face da execução do CONTRATO PRINCIPAL.

§6º – A CONTRATADA, na forma disposta no parágrafo primeiro, acima, também se obriga a:

I. Não discutir perante terceiros, usar, divulgar, revelar, ceder a qualquer título ou dispor das informações, no território brasileiro ou no exterior, para nenhuma pessoa, física ou jurídica, e para nenhuma outra finalidade que não seja exclusivamente relacionada ao objetivo aqui referido, cumprindo-lhe adotar cautelas e precauções adequadas no sentido de impedir o uso indevido por qualquer pessoa que, por qualquer razão, tenha acesso a elas;

II. Responsabilizar-se por impedir, por qualquer meio em direito admitido, arcando com todos os custos do impedimento, mesmo judiciais, inclusive as despesas processuais e outras despesas derivadas, a divulgação ou utilização das informações Proprietárias por seus agentes, representantes ou por terceiros;

III. Comunicar à CONTRATANTE, de imediato, de forma expressa e antes de qualquer divulgação, caso tenha que revelar qualquer uma das informações, por determinação judicial ou ordem de atendimento obrigatório determinado por órgão competente; e

IV. Identificar as pessoas que, em nome da CONTRATADA, terão acesso às informações sigilosas.

Cláusula Quinta – DA VIGÊNCIA

O presente TERMO DE COMPROMISSO tem natureza irrevogável e irretroatível, permanecendo em vigor desde a data de sua assinatura até expirar o prazo de classificação da informação a que a CONTRATADA teve acesso em razão do CONTRATO PRINCIPAL.

Cláusula Sexta – DAS PENALIDADES

A quebra do sigilo e/ou da confidencialidade das informações, devidamente comprovada, possibilitará a imediata aplicação de penalidades previstas conforme disposições contratuais e legislação em vigor que trata desse assunto, podendo culminar na rescisão do CONTRATO PRINCIPAL firmado entre as PARTES. Neste caso, a CONTRATADA, estará sujeita, por ação ou omissão, ao pagamento ou recomposição de todas as perdas e danos sofridos pela CONTRATANTE, inclusive as de ordem moral, bem como as de responsabilidades civil e criminal, as quais serão apuradas em regular processo administrativo ou judicial, sem prejuízo das demais sanções legais cabíveis, conforme Art. 87 da Lei nº. 8.666/93.

Cláusula Sétima – DISPOSIÇÕES GERAIS

Este TERMO DE COMPROMISSO é parte integrante e inseparável do CONTRATO PRINCIPAL. §1º – Surgindo divergências quanto à interpretação do disposto neste instrumento, ou quanto à execução das obrigações dele decorrentes, ou constatando-se casos omissos, as partes buscarão solucionar as divergências de acordo com os princípios de boa fé, da equidade, da razoabilidade, da economicidade e da moralidade.

§2º – O disposto no presente TERMO DE COMPROMISSO prevalecerá sempre em caso de dúvida e, salvo expressa determinação em contrário, sobre eventuais disposições constantes de outros instrumentos conexos firmados entre as partes quanto ao sigilo de informações, tais como aqui definidas.

Parágrafo Terceiro – Ao assinar o presente instrumento, a CONTRATADA manifesta sua concordância no sentido de que:

I. A CONTRATANTE terá o direito de, a qualquer tempo e sob qualquer motivo, auditar e monitorar as atividades da CONTRATADA;

e-mail: santafeprev@santafeprev.com.br

Rua Sete nº 1167 - Centro - Fone/Fax (17) 3631-3468
CEP 15775-000 - ESTÂNCIA TURÍSTICA DE SANTA FÉ DO SUL/SP

PREVIDÊNCIA MUNICIPAL DE SANTA FÉ DO SUL
SANTA FÉ DO SUL
Instituto Municipal de Previdência Social

II. A CONTRATADA deverá disponibilizar, sempre que solicitadas formalmente pela CONTRATANTE, todas as informações requeridas pertinentes ao CONTRATO PRINCIPAL;

III. A omissão ou tolerância das partes, em exigir o estrito cumprimento das condições estabelecidas neste instrumento, não constituirá novação ou renúncia, nem afetará os direitos, que poderão ser exercidos a qualquer tempo;

IV. Todas as condições, termos e obrigações ora constituídos serão regidos pela legislação e regulamentação brasileiras pertinentes;

V. O presente TERMO DE COMPROMISSO somente poderá ser alterado mediante TERMO ADITIVO firmado pelas partes;

VI. Alterações do número, natureza e quantidade das informações disponibilizadas para a CONTRATADA não descaracterizarão ou reduzirão o compromisso e as obrigações pactuadas neste TERMO DE COMPROMISSO, que permanecerá válido e com todos seus efeitos legais em qualquer uma das situações tipificadas neste instrumento;

VII. O acréscimo, complementação, substituição ou esclarecimento de qualquer uma das informações disponibilizadas para a CONTRATADA, serão incorporados a este TERMO, passando a fazer dele parte integrante, para todos os fins e efeitos, recebendo também a mesma proteção descrita para as informações iniciais disponibilizadas, sendo necessário a formalização de TERMO ADITIVO ao CONTRATO PRINCIPAL;

VIII. Este TERMO DE COMPROMISSO não deve ser interpretado como criação ou envolvimento das Partes, ou suas filiadas, nem em obrigação de divulgar informações sigilosas para a outra Parte, nem como obrigação de celebrarem qualquer outro acordo entre si.

Cláusula Oitava – DO FORO

A CONTRATANTE elege o foro da cidade de CIDADE (UF), onde está localizada a sede da CONTRATANTE, para dirimir quaisquer dúvidas originadas do presente TERMO, com renúncia expressa a qualquer outro, por mais privilegiado que seja.

DE ACORDO

E, por assim estarem justas e estabelecidas as condições, o presente TERMO DE COMPROMISSO é assinado pelas partes em 02 (duas) vias de igual teor e um só efeito.

CONTRATANTE	CONTRATADA
Local, dia/mês/ano.	Local, dia/mês/ano.
Nome do Responsável pelo Contratante Cargo	Nome do Responsável pelo Contratada Cargo/ CPF



ANEXO II

TERMO DE CIÊNCIA INDIVIDUAL CONFIDENCIALIDADE E SEGURANÇA DA INFORMAÇÃO	
IDENTIFICAÇÃO DO CONTRATO:	
Nº DO CONTRATO	
NOME DA EMPRESA CONTRATADA	
CNPJ DA CONTRATADA	
OBJETO RESUMIDO	
VIGÊNCIA CONTRATUAL	
TERMOS:	
O(s) funcionário(s) abaixo qualificado(s) declara(m) ter pleno conhecimento de sua(s) responsabilidade(s) no que concerne ao sigilo a ser mantido sobre as atividades desenvolvidas ou as ações realizadas no âmbito do Contrato Administrativo nº ____/____, bem como sobre todas as informações que eventualmente ou por força de sua(s) função(ões) venha(m) a tomar conhecimento, comprometendo-se a guardar o sigilo necessário nos termos da legislação vigente e a prestar total obediência às normas de segurança da informação vigentes no ambiente do CONTRATANTE ou que venham a ser implantadas a qualquer tempo por este; em conformidade com o TERMO DE COMPROMISSO DE SEGURANÇA DA INFORMAÇÃO firmado entre as partes.	
OBSERVAÇÕES:	
DE ACORDO	
E, por assim estarem justas e estabelecidas as condições, o presente TERMO DE CIÊNCIA é assinado pelas partes em 02 (duas) vias de igual teor e um só efeito.	
LOCAL, dia/mês/ano	
IDENTIFICAÇÃO E ASSINATURA DO(S) DECLARANTE(S):	
NOME: IDENTIDADE: CPF: CARGO/FUNÇÃO:	ASSINATURA:

e-mail: santafeprev@santafeprev.com.br

Rua Sete nº 1167 - Centro - Fone/Fax (17) 3631-3468
CEP 15775-000 - ESTÂNCIA TURÍSTICA DE SANTA FÉ DO SUL/SP