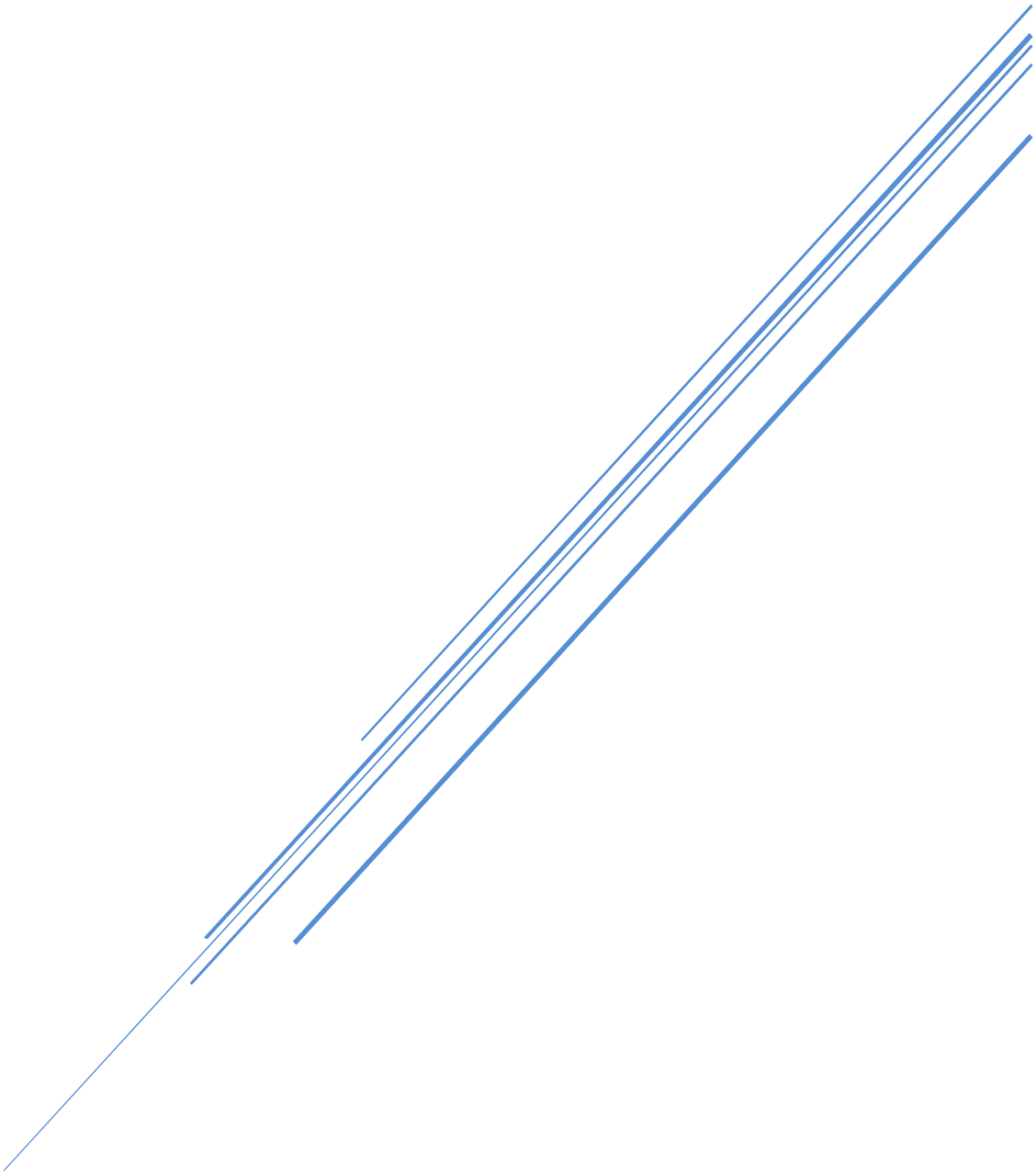
# POLÍTICA DE SEGURANÇA DA INFORMAÇÃO



Resolução 02/2021, de 14 de dezembro de 2021
Anexo Único

# Sumário

# 1. DEFINIÇÕES E TERMOS

**Administração:** Instituto de Previdência Social do Município de Navegantes – NAVEGANTESPREV;

**Credencial:** conta de usuário com senha para ingresso em domínio, entendido como um endereço de gerenciamento da rede de computadores do Ente;

**Diretoria:** diretor-presidente da Administração;

**Ente:** Prefeitura Municipal de Navegantes, suas secretarias, fundações, autarquias, e a Câmara de Vereadores de Navegantes;

**Estação de trabalho:** computador funcional com seus periféricos;

**Periféricos:** acessórios que atuam em conjunto com o computador, como mouse, teclado, scanner de mesa e coletor de digital;

**PSI:** Política de Segurança da Informação;

**Segurado:** servidor ativo do quadro funcional do Ente e segurado inativo ou pensionista da Administração;

**Servidor:** servidor do quadro funcional do Instituto de Previdência Social do Município de Navegantes – NAVEGANTESPREV, bem como o estagiário a serviço deste;

**Setor de TI:** Departamento de Tecnologia da Informação do Ente;

**Terceiro:** prestador de serviço contratado pelo Ente;

**TI:** servidor do Departamento de Tecnologia da Informação do Ente;

**TI Primário:** servidor da Administração que possua privilégios de acesso assemelhados ao do TI para pequenas ações.

# 2. INTRODUÇÃO

Diante da constante evolução tecnológica que vivemos na atualidade, há uma crescente necessidade de busca de mecanismos que ofereçam segurança e integridade àinformação gerada pelas organizações. Conforme definição da norma ABNT NBR ISO/IEC 27002:2005:

> ***A informação*** é um ativo que, como qualquer outro ativo importante, é essencial para os negócios de uma organização e, consequentemente, necessita ser adequadamente protegida. [...] A informação pode existir em diversas formas. Ela pode ser impressa ou escrita em papel, armazenada eletronicamente, transmitida pelo correio ou por meios eletrônicos, apresentada em filmes ou falada em conversas. Seja qual for a forma de apresentação ou o meio através do qual a informação é compartilhada ou armazenada, é recomendado que ela seja sempre protegida adequadamente.

Neste contexto, visando a proteção destes ativos e a modernização da Administração, que aderiu ao Programa de Certificação Institucional e Modernização da Gestão dos Regimes Próprios de Previdência Social da União, dos Estados, do Distrito Federal e dos Municípios (Portaria MPS nº 185/2015, alterada pela Portaria MF nº 577/2017) denominada de Pró-Gestão RPPS, moderniza-se, através deste documento, a PSI da Administração.

Portanto, esta PSI é uma declaração formal de compromisso da Administração com a proteção das informações sob sua guarda e a formalização das normas para segurança, devendo ser observado por todos os seus Segurados e Terceiros.

# 3. OBJETIVO

A política de segurança da informação é um conjunto de princípios que norteiam a gestão de segurança de informações e que deve ser observado pelo Setor de TI, Diretoria e Servidores, garantindo a integridade, confidencialidade, autenticidade e disponibilidade das informações processadas pela Administração, reduzindo os riscos de falhas, danos e prejuízos que possam comprometer os objetivos da Administração.

# 4. REGRAS DE UTILIZAÇÃO DE RECURSOS TECNOLÓGICOS

Neste contexto, diante da necessidade iminente de proteger as informações custodiadas e geradas pela Administração, apresenta-se neste tópico as principais regras de utilização dos recursos tecnológicos.

## 4.1. Proteção da Informação

Define-se como necessária a proteção das informações da Administração ou sob sua custódia como fator primordial nas atividades laborativas de cada Segurado e Terceiro da Administração, sendo que:

**a)** Os Servidores devem assumir uma postura proativa no que diz respeito à proteção das informações e devem estar atentos a ameaças externas, bem como fraudes,roubo de informações, e acesso indevido a sistemas de informação sob responsabilidade;

**b)** A produção, guarda, e tratamento de informações pessoais dos Segurados e Terceiros deverão ser preservados tão somente aqueles considerados essenciais para a correta execução das atividades da Administração;

**c)** Assuntos confidenciais não devem ser expostos publicamente;

**d)** Senhas, chaves e outros recursos de caráter pessoal são considerados intransferíveis e não podem ser compartilhados e divulgados;

**e)** Somente softwares homologados ou gratuitos podem ser utilizados no ambiente computacional;

**f)** Documentos impressos e arquivos contendo informações confidenciais devem ser armazenados e protegidos, devendo o descarte ser feito através do uso de desfragmentadora ou qualquer outra forma que a Administração assim promover;

**g)** Os computadores só podem ser acessados através de credencial criada pelo TI;

**h)** Será restrito o quanto possível o compartilhamento de pastas de rede dos Servidores da Administração para evitar acesso indevido ou desnecessário de conteúdos que não sejam pertinentes ao usuário.

**i)** Todos os dados considerados como imprescindíveis aos objetivos da Administração devem ser protegidos através de rotinas de cópia de segurança.

## 4.2. Regras gerais aos Servidores e Terceiros

Cabe aos Servidores e Terceiros da Administração cumprir com as seguintes obrigações:

**a)** Zelar continuamente pela proteção das informações da Administração contra acesso, modificação, destruição ou divulgação não autorizada;

**b)** Assegurar que os recursos (computacionais ou não) colocados à sua disposição sejam utilizados apenas para as finalidades da Administração;

**c)** Zelar para que os sistemas e informações sejam utilizados de acordo com as normas estabelecidas nesta PSI;

**d)** Os equipamentos devem ser manuseados com cuidado, considerando que oscomputadores e periféricos são patrimônio público. Em caso de o Servidor notar alguma anormalidade com o computador e seus periféricos, ou a ausências desses, deve comunicar imediatamente o TI Primário ou Setor de TI para que sejam tomadas as devidas providências;

**e)** Alimentos e/ou bebidas devem ser mantidos a distância dos equipamentos suficiente para garantir que se evite danos aos equipamentos;

**f)** Não é permitida a abertura física ou a desmontagem de equipamentos de informática sem supervisão do TI Primário ou TI;

**g)** As mudanças de local dos equipamentos tecnológicos devem ser realizadas com zelo que todo Servidor probo deve ter, ou supervisionadas pelo TI Primário com o objetivo de evitar danos ao patrimônio;

**h)** Comunicar imediatamente a Diretoria sobre qualquer descumprimento da PSI ou dos procedimentos manualizados para devidas providências cabíveis;

**i)** Não é permitido a instalação de softwares ou equipamentos nos computadores sem prévia autorização do TI Primário ou TI;

**j)** É proibido fazer download e/ou armazenar, em computador local ou unidade de rede, software comercial, música, fotos, filmes ou qualquer outro material cujo direito pertença a terceiros (copyright), sem ter um contrato de licenciamento, salvo se, disponibilizado gratuitamente (freeware) e para o desempenho de suas funções;

**k)** Os arquivos que estiverem em desconformidade com as normas desta PSI serão excluidos da rede sem prévio aviso.

## 4.3. Contas e Senhas de Acesso

**a)** Cada Servidor deve possuir uma credencial na estação de trabalho, sendo pessoal e intransferível, e de responsabilidade exclusiva do Servidor;

**b)** A criação e atualização da credencial, bem como a criação e atualização de acesso a softwares cujos acessos sejam gerenciados pelo Setor de TI, devem ser realizadas ao Setor de TI com permissão de acesso autorizado pela Diretoria, e terá somente o privilégio necessário para desempenhar suas

funções;

**c)** A criação e atualização de e-mail, bem como a criação e atualização de acesso a softwares cujos acessos sejam gerenciados pela Administração devem ser realizadas pelo TI Primário ou pela Diretoria, com permissão de acesso autorizado pela Diretoria, e terá somente o privilégio necessário para desempenhar suas funções;

**d)** É de responsabilidade do Servidor manter, sob sua guarda, as contas de e-mail e usuário, e de softwares necessários para desempenhar suas funções, sendo igualmente responsável pelas ações incorridas em decorrência do uso destas contas, sendo desaconselhado manter *login* e senhas salvos automaticamente;

**e)** É incentivado que todo usuário promova práticas de segurança como o bloqueio de sua estação de trabalho sempre que se ausentar do ambiente de trabalho, e renovação periódica de senhas fortes, assim caracterizada com o uso de caracteres alfanúmericas maiúsculas e minúsculas, e com caracteres especiais.

## 4.4. Acesso e Armazenamento de Arquivos na Rede Corporativa

Será disponibilizado em rede, um diretório exclusivo para cada Servidor da Administração com a pasta nomeada por sua credencial, além de um diretório compartilhado para uso da Administração contendo as permissões para os Servidores dos respectivos departamentos nomeada por "Público". É de responsabilidade exclusiva dos Servidores manter, nestes diretórios, as informações produzidas para o bom andamento da execução das atividades da Administração, e para que essas sejam preservadas através das rotinas de segurança e backup;

As definições das permissões dos diretórios da Rede é de responsabilidade do Setor de TI.

## 4.5. Uso do Antivírus

Todas as estações de trabalho devem ter um antivírus instalado, que em hipótese alguma, pode ser desabilitado pelo usuário;

Todo arquivo em mídia proveniente de entidade externa (cd, hd, *pendrive),* ou recebido/obtido através da rede mundial de computadores (internet), deve ser verificado por programa antivírus, executado pelo próprio usuário.

## 4.6. Uso do Correio Eletrônico

**a)** Cada Servidor receberá uma conta de e-mail corporativo com senha única, pessoal e

intransferível e de sua exclusiva responsabilidade, cuja conta deverá ser providenciada pelo TI Primário com base na solicitação da Diretoria;

**b)** O uso do e-mail corporativo deve ser apenas para assuntos profissionais, sendo, todas as mensagens de propriedade da Administração, podendo ser monitorados sem prévia notificação;

**c)** É terminantemente proibido enviar ou encaminhar qualquer mensagem, entre usuários da Administração ou não, com conteúdo difamatório, ofensivo, racista, especulativo, obsceno, *bullying*, *spams*, correntes ou de qualquer natureza similar, indução religiosa ou política, comércio, propaganda e incentivo a atos de terrorismo, ou que visem instigar, ameaças, invadir a privacidade ou prejudicar pessoas e/ou organizações;

**d)** É terminantemente proibido utilizar o e-mail corporativo e demais recursos de TI para executar quaisquer tipos de fraudes;

**e)** É desaconselhável a utilização de e-mail não institucional para tratamento de assuntos corporativos, visto que tal prática pode comprometer a segurança da informação, ficando o Servidor única e exclusivamente responsável por eventuais danos gerados à Administração;

## 4.7. Uso de Plataforma de mensagens e Aplicativos de videoconferência

O acesso a plataforma de mensagens como Skype, WhatsApp, bem como acesso a aplicativos de videoconferência como Google Meet, Microsoft Teams e Zoom será permitido para a facilitação da comunicação entre os Servidores, Terceiros e Segurados, no estrito exercício de suas funções.

**a)** O uso destas ferramentas devem ser apenas para assuntos profissionais, sendo todo seu conteúdo produzido de propriedade da Administração;

**b)** É terminantemente proibido enviar ou encaminhar qualquer conteúdo, entre usuários da Administração ou não, com conteúdo difamatório, ofensivo, racista, especulativo, obsceno, *bullying*, *spams*, correntes ou de qualquer natureza similar, indução religiosa ou política, comércio, propaganda e incentivo a atos de terrorismo, ou que visem instigar, ameaças, invadir a privacidade ou prejudicar pessoas e/ou organizações;

**c)** É terminantemente proibido utilizar as ferramentas, em conjunto ou isoladamente, para executar quaisquer tipos de fraudes;

**d)** A comunicação entre Servidores não deve ser usada como forma a substituir a comunicação formal necessária para a consecução das atividades da Administração;

**e)** O Servidor é responsável pela disponibilidade de informações pessoais de Segurados que vier a transmitir por estas ferramentas, devendo fornecer tais dados somente com solicitação ou consentimento prévio do titular da informação;

**f)** Será dada preferência de utilização de software cuja implementação seja custeada pela

Administração ou de conta criada pela Administração, em detrimento do uso de software de conta privada criada pelo Servidor;

**g)** A utilização de conta privada criada pelo Servidor sujeitará o Servidor ao atendimento das mesmas condições que as praticadas em conta criada pela Administração;

**h)** O monitoramento e registro poderão ser efetuados mesmo nas conexões com fins particulares autorizadas por esta PSI;

**i)** O uso destas ferramentas em desconformidade com as normas desta PSI poderá ensejar responsabilidade administrativa.

## 4.8. Acesso à Internet

O acesso à internet pela rede interna será disponibilizado em todos as estações detrabalho, devendo ser utilizado única e exclusivamente para atender os objetivos institucionais da Administração.

Será permitido o uso do acesso à internet disponibilizado para o uso com fins particulares pelos Servidores nas seguintes condições:

**a)** Seja utilizado para acesso a instituições financeiras e a sites cujo conteúdo proporcionem desenvolvimento pessoal aos Servidores;

**b)** O tempo de acesso e conteúdo acessado não interfiram no cumprimento das funções do agente público;

**c)** O acesso não interfira no bom funcionamento da rede e dos sistemas da Administração;

**d)** Não seja contabilizado para justificar a necessidade de aumento da capacidade de acesso;

**e)** Todas as conexões feitas e conteúdos transmitidos estão sujeitos à monitoramento, mesmo que para uso particular e de conteúdo privado;

**f)** O acesso não coloque em risco a segurança da rede e dos sistemas da Administração;

**g)** O acesso poderá ser bloqueado a qualquer momento devido a critérios técnicos pelo Setor de TI ou por requerimento da Diretoria, sem que seja responsabilizado por qualquer perda ou dano decorrente do bloqueio do acesso;

**h)** A Administração não será responsabilizada por qualquer perda ou dano decorrente de alguma falha na segurança durante o acesso de carater pessoal;

**i)** As conexões poderão ter seu conteúdo monitorado e registrado pelo Setor de TI, a qualquer momento, sem aviso prévio, independente de autorização superior, para fins de detecção de uso indevido, invasão ou de softwares maliciosos;

**j)** O monitoramento e registro poderão ser efetuados mesmo nas conexões com fins particulares autorizadas por esta PSI;

**k)** O uso da internet em desconformidade com as normas desta PSI poderá ensejar

responsabilidade administrativa.

### 4.9. Cópia de Segurança dos Arquivos

**a)** É responsabilidade dos Servidores o armazenamento de textos, planilhas, mensagens eletrônicas, desenhos e outros arquivos ou documentos na rede corporativa que será incluída na rotina de backup.

**b)** A rotina de backup de arquivos que não estão incluídos na rede corporativa será administrada pelo TI Primário, que promoverá meios para que cada estação de trabalho possa ter sua rotina de backup apartada.

## 5. PAPÉIS E RESPONSABILIDADES

### 5.1. Dos Servidores

**a)** Ter ciência do conteúdo do objetivo desta PSI;

**b)** Cumprir e fazer cumprir a PSI, as atividades manualizadas e outros procedimentos relativos a esta PSI.

### 5.2. Da Diretoria

**a)** Assegurar que seus Servidores possuam acesso e entendimento da PSI, das atividades manualizadas e de outros procedimentos relativos a esta PSI;

**b)** Emitir Termo de Resposabilidade e Sigilo (Anexo I), colher assinatura do Servidor e manter arquivo em processo administratvo de PSI, para consulta a qualquer tempo;

**c)** Comunicar imediatamente ao Setor de TI eventuais casos de violação da PSI, das atividades manualizadas e de outros procedimentos relativos a esta PSI.

**d)** Comunicar os casos de nomeação, exoneração, contratação ou rescisão de Servidor ao Setor de TI para que sejam feitas as adequações necessárias de acordo com as permissões concedidas em razão das atividades realizadas.

### 5.3. Do Setor de TI

**a)** Cadastrar Servidores, disponibilizando acesso necessário para o desenvolvimento de suas atribuições;

**b)** Assessorar os Servidores sobre dúvidas pertinentes a esta PSI;

**c)** Atender as demandas abertas pelos Servidores e Diretoria, levando em conta as medidas necessárias para o fiel cumprimento desta PSI e da continuidade das atividades da Administração;

**d)** Conceder permissão a Servidor que possua capacidade de intermediar as demandas na Administração como TI Primário, de modo a trazer maior celeridade às respostas do Setor de TI, e remover tal permissão quando pertinente;

**e)** Monitorar a utilização das ferramentas tecnológicas, inclusive acesso à internet e rede corporativa;

**f)** Eliminar arquivos e programas que estejam em desacordo com as normas desta política.

**g)** Definir procedimentos de contingência, que determinem a existência de cópias de segurança dos sistemas informatizados e dos bancos de dados, o controle de acesso (físico e lógico) e a área responsável por elas, estando estes procedimentos mapeados e manualizados;

**h)** Promover práticas que fomentam a segurança da informação.

## 5.4. Do TI Primário

**a)** Auxiliar a Diretoria, os Servidores e o Setor de TI, como canal intermediário para a solução de demandas de menor complexidade, entendida como aquelas que não há a necessidade de atuação direta do Setor de TI;

**b)** Atuar com o mesmo zelo necessário para a atuação das atividades correlatas ao Setor de TI, respondendo pelos atos praticados em desconformidade.

## 6. VIOLAÇÕES E SANÇÕES

São consideradas violações à PSI, às atividades manualizadas e a outros procedimentos relativos a esta PSI, não se limitando às mesmas:

**a)** Quaisquer ação ou situação que possa expor a Administração ou seus Segurados à perda financeira e de imagem, direta ou indiretamente, potenciais ou reais, comprometendo seus ativos de informação;

**b)** Utilização indevida de dados da Administração, divulgação não autorizada de informações, sem a permissão expressa da Diretoria;

**c)** Uso de dados, informações, equipamentos, software, sistemas ou outros recursos tecnológicos, para propósitos ilícitos, que possam incluir a violação de leis, de regulamentos internos e externos, da ética ou de exigências de organismos reguladores da área de atuação da Administração ou de seus Segurados;

**d)** A não comunicação imediata ao Setor de TI de quaisquer descumprimentos da PSI, das atividades manualizadas e de outros procedimentos relativos a esta PSI, que porventura um Servidor, Segurado ou Terceiro venha a tomar conhecimento ou chegue a presenciar.

## 7. DISPOSIÇÕES FINAIS

Os procedimentos de contingência, que determinem a existência de cópias de segurança dos sistemas informatizados e dos bancos de dados, o controle de acesso (físico e lógico) e a área responsável por elas, serão estabelecidas em manual de procedimentos internos.

A concessão de permissão ao TI Primário se dará a critério do Setor de TI, podendo tais permissões obedecer a critérios estabelecidos pelo Setor de TI a qualquer tempo, bem como a admissibilidade da manutenção do TI Primário.

Os casos não previstos nesta PSI deverão ser tratados diretamente pela Diretoria, que poderá, a critério, acionar o Setor de TI para dirimir tais casos.

# 8. LEGISLAÇÃO APLICÁVEL

Decreto-Lei 2848, de 7 de dezembro de 1940 (Institui o Código Penal);

Lei Federal 3129, de 14 de outubro de 1982 (Regula a Concessão de Patentes aos autores de invenção ou descoberta industrial);

Lei Federal 8159, de 08 de janeiro de 1991 (Dispõe sobre a Política Nacional de Arquivos Públicos e Privados);

Lei Federal 8429, de 02 de junho de 1992 (Dispõe sobre Ato de Improbidade Administrativa);

Lei Federal 9279, de 14 de maio de 1996 (Dispõe sobre Marcas ePatentes);

Lei Federal 9610, de 19 de fevereiro de 1998 (Dispõe sobre o Direito Autoral);

Lei Federal 9983, de 14 de julho de 2000 (Altera o Código Penal e dá outras providencias);

Lei Federal 10406, de 10 de janeiro de2002 (Institui o Código Civil);

Lei Federal 12527, de 18 de novembro de 2011 (Dispõe sobre Lei de Acesso à Informação);

Lei Federal 13460, de 26 de junho de 2017 (Dispõe sobre o Direito Autoral);

Lei Federal 13709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais).

# ANEXO I – TERMO DE RESPONSABILIDADE E SIGILO

Pelo presente instrumento, eu_____, CPF_____, Identidade_____, **DECLARO**, sob pena das sanções cabíveis, nos termos da legislação vigente, que conheço e estou comprometido com as práticas, responsabilidades e obrigações normativas referente a Política de Segurança da Informação (PSI) do Instituto de Previdência Social do Município de Navegantes – NAVEGANTESPREV.

Navegantes/SC, DD de MMM de AAAA.

_____

Nome do Servidor
Cargo do Servidor



Instituto de Previdência Social do Município de Navegantes
Endereço: Av. Conselheiro João Gaya, 295 – Centro, Navegantes – CEP 88.370.114
Fone: (47) 3342.3838 – WhatsApp: (47) 99244.4656 – E-mail: atendimento@navegantesprev.sc.gov.br