

## MAPEAMENTO E MANUALIZAÇÃO DOS PROCESSOS DE TI: Controle de Acesso Físico e Lógico

### 1. FUNDAMENTO LEGAL

Decreto Nº 014/2021, que Dispõe sobre a Política de Gestão e Segurança da Informação do Instituto de Gestão Previdenciária do Município de Petrolina – IGEPREV.

### 2. OBJETIVO

Controles físicos e controles lógicos são as aplicações, técnicas e estratégias criadas com o objetivo de barrar acessos não autorizados, seja em um local físico ou em um sistema virtual do Instituto de Gestão Previdenciária do Município de Petrolina – IGEPREV, sendo uma das principais ferramentas aplicadas por meio da Política de Gestão e Segurança da Informação.

### 3. SETORES ENVOLVIDOS NO PROCESSO

Gerência do Núcleo de Segurança e Tecnologia da Informação do IGEPREV, Diretoria de RH, Setores/servidores internos do IGEPREV, Segurados e Protocolo/Atendimento.

### 4. AÇÕES POR NÃO CUMPRIMENTO DAS OBRIGAÇÕES

No caso de não cumprimento com o disposto das legislações vigentes referente à temática, será necessário que a Política de Segurança da Informação seja retificada. Portanto, se o acesso virtual dos servidores não for cumprido de maneira correta, à concessão dos acessos devem ser revistas e inicializadas novamente.

### 5. FREQUÊNCIA DOS PROCESSOS

Sempre que alguns dos setores envolvidos precisarem, os fluxos desta atividade deverão ser feitas.

### 6. SISTEMAS UTILIZADOS PARA ACESSO

- 1DOC – Para acesso dos segurados e servidores internos do IGEPREV;
- SISPREVWEB – Para acesso dos servidores internos do IGEPREV;
- APLICATIVO MEU RPPS – Para acesso dos segurados.

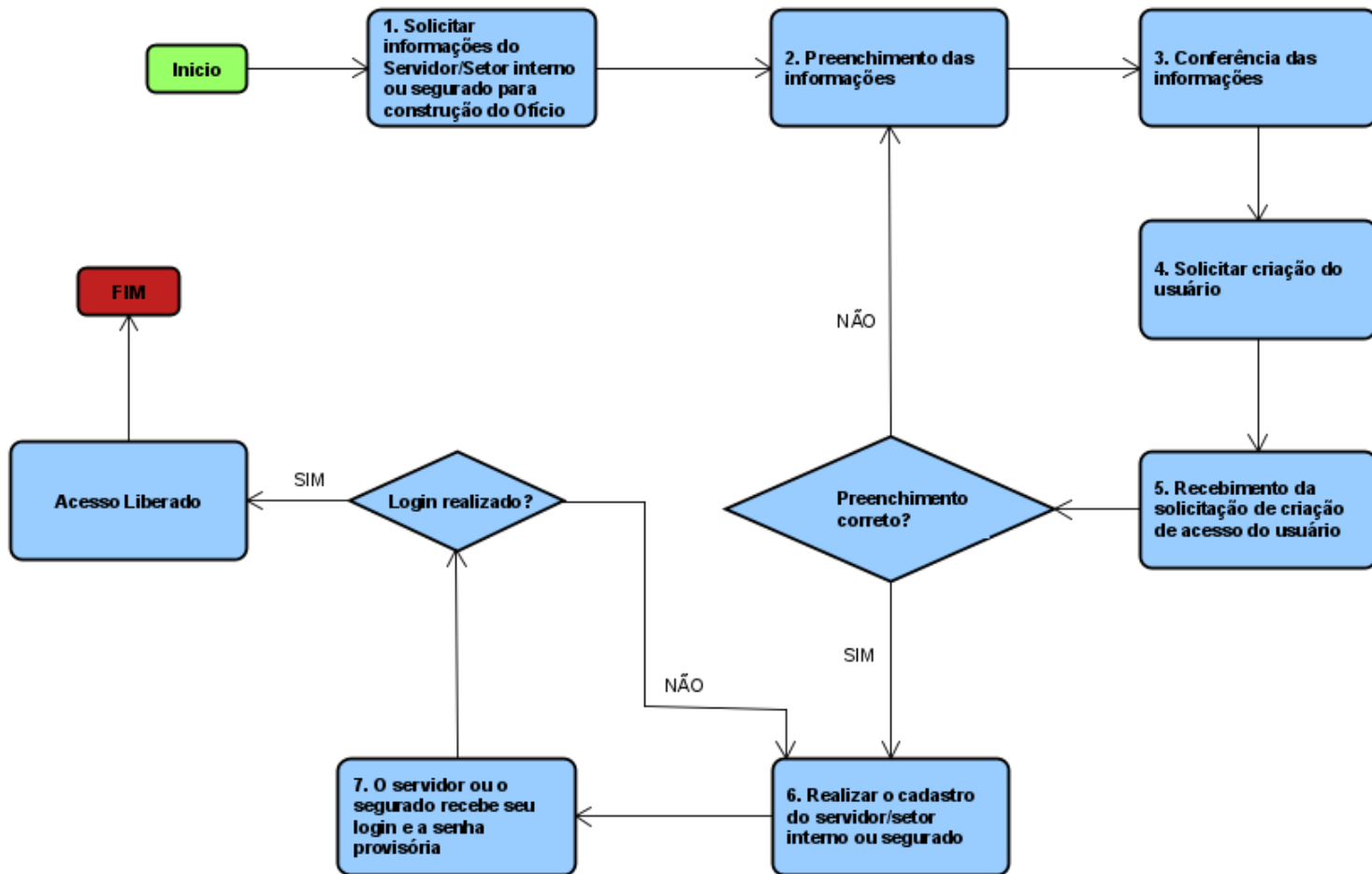
### 7. PROCEDIMENTOS DE CONTROLE DE ACESSO LÓGICO

Fase	Atividade	Responsáveis	Detalhamento
1	A Diretoria de RH do IGEPREV deverá informar ao setor de TI por meio de ofício enviado pelo sistema 1doc, as informações do servidor/setor interno do instituto a ser cadastrado o acesso. No caso dos segurados, fica a cargo	Gerência do Núcleo de Segurança e Tecnologia da Informação, Diretoria de RH, Setores/servidores internos, Segurados e Protocolo/Atendimento	O ofício com os principais dados deve ser solicitado pelo RH por meio do sistema 1doc ao setor de TI, seguindo o padrão do anexo I. Antes de enviar o ofício para o TI deve ser observada a Política de Segurança e as competências da mesma. O protocolo/atendimento deve se atentar a política de segurança da mesma forma, o que muda é que o cadastramento do segurado será feito pelo próprio sistema

Previdência do Servidor, Construindo Um Novo Tempo.

	do setor de Protocolo/Atendimento o cadastro por meio do próprio sistema.		na aba de cadastro, conforme anexo II.
2	Preenchimento das informações	Diretoria de RH, Setores/servidores internos, Segurados e Protocolo/Atendimento	O preenchimento ter que ser feito no modo correto e seguindo o padrão estabelecidos no anexo I e II.
3	Conferência das informações	Diretoria de RH e Protocolo/Atendimento	
4	Solicitar criação do usuário	Diretoria de RH e Protocolo/Atendimento	
5	Recebimento da solicitação de criação de acesso do usuário	Gerência do Núcleo de Segurança e Tecnologia da Informação	Realizar análise sobre a solicitação e verificar a liberação de acesso junto ao Diretor-Presidente do Instituto.
5.1	Se todas as informações estiverem corretas e no padrão estabelecido, pula para a fase 6	Gerência do Núcleo de Segurança e Tecnologia da Informação	
5.2	Se alguma informação estiver incorreta ou não seguir o padrão, volta-se à fase 2.	Gerência do Núcleo de Segurança e Tecnologia da Informação	
6	Realizar o cadastro do servidor/setor interno ou segurado.	Gerência do Núcleo de Segurança e Tecnologia da Informação	
7	O servidor ou o segurado recebe seu login e a senha provisória.	Setores/servidores internos e Segurados.	No primeiro acesso o usuário precisa cadastrar uma nova senha.
7.1	Se o acesso for concretizado com sucesso, processo finalizado.	Setores/servidores internos e Segurados.	
7.2	Se for verificado algum problema de login, volta-se à fase 5.	Setores/servidores internos e Segurados.	

## 8. FLUXOGRAMA DO PROCESSO



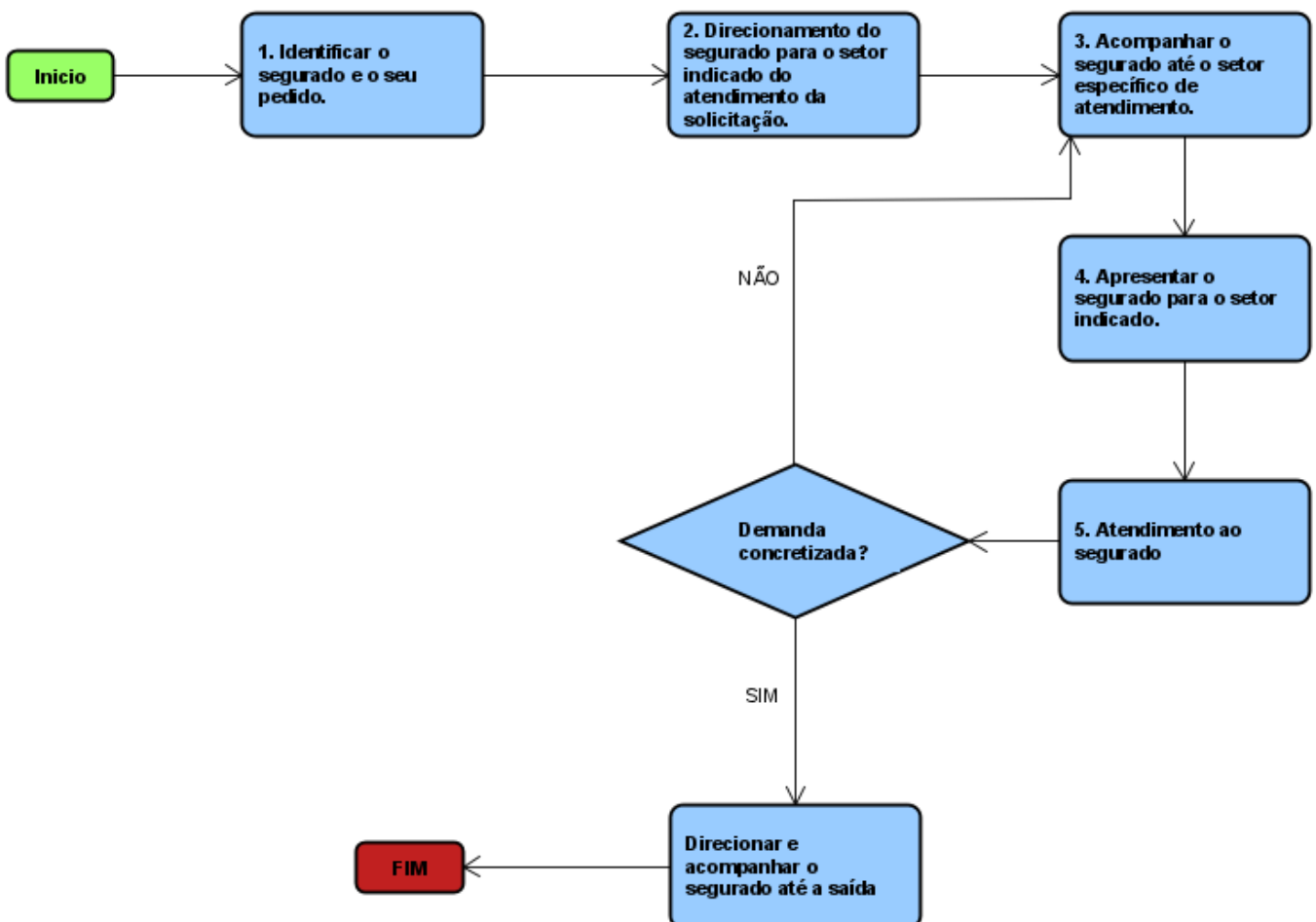
## 9. PROCEDIMENTOS DE CONTROLE DE ACESSO FÍSICO

Etapa	Atividade	Responsáveis	Detalhamento
1	Identificar o segurado e o seu pedido.	Protocolo/Atendimento do IGEPREV	O segurado deverá se apresentar na recepção do IGEPREV e explicar o assunto a ser tratado para o servidor responsável pelo atendimento.
2	Direcionamento do segurado para o setor indicado do atendimento da solicitação.	Protocolo/Atendimento do IGEPREV	
3	Acompanhar o segurado até o setor específico de atendimento.	Protocolo/Atendimento do IGEPREV	O servidor do IGEPREV antes de prosseguir com o atendimento do segurado realiza orientações sobre as responsabilidades do segurado perante a Política de Segurança da Informação e que após conclusão do atendimento poderá verificar o mesmo de forma online ou presencial junto a Ouvidoria do IGEPREV.
4	Apresentar o segurado para o setor indicado.	Servidor/setor interno, Protocolo/Atendimento e	Explicar o assunto a ser tratado para o setor/servidor.

Previdência do Servidor, Construindo Um Novo Tempo.

		segurado.	
5	Atendimento ao segurado.	Servidor/setor interno	O atendimento deve ser cordial, ético, seguir as diretrizes da Política de segurança e com empatia.
5.1	Se a demanda não for concretizada da forma correta, voltar para a fase 3.	Segurado	
5.2	Se a demanda for finalizada da forma correta, encerra-se o atendimento.	Servidor/setor do IGEPREV.	

## 10. FLUXOGRAMA DO PROCESSO



Previdência do Servidor, Construindo Um Novo Tempo.

## 11.ANEXOS

### ANEXO I

Ofício/Memorando padrão pelo 1doc, para ser enviada a solicitação de acesso aos sistemas. Deve conter no mínimo as seguintes informações:

#### Cadastro de Servidor/Setor Interno:

Setor:

Nome do Servidor:

Cargo:

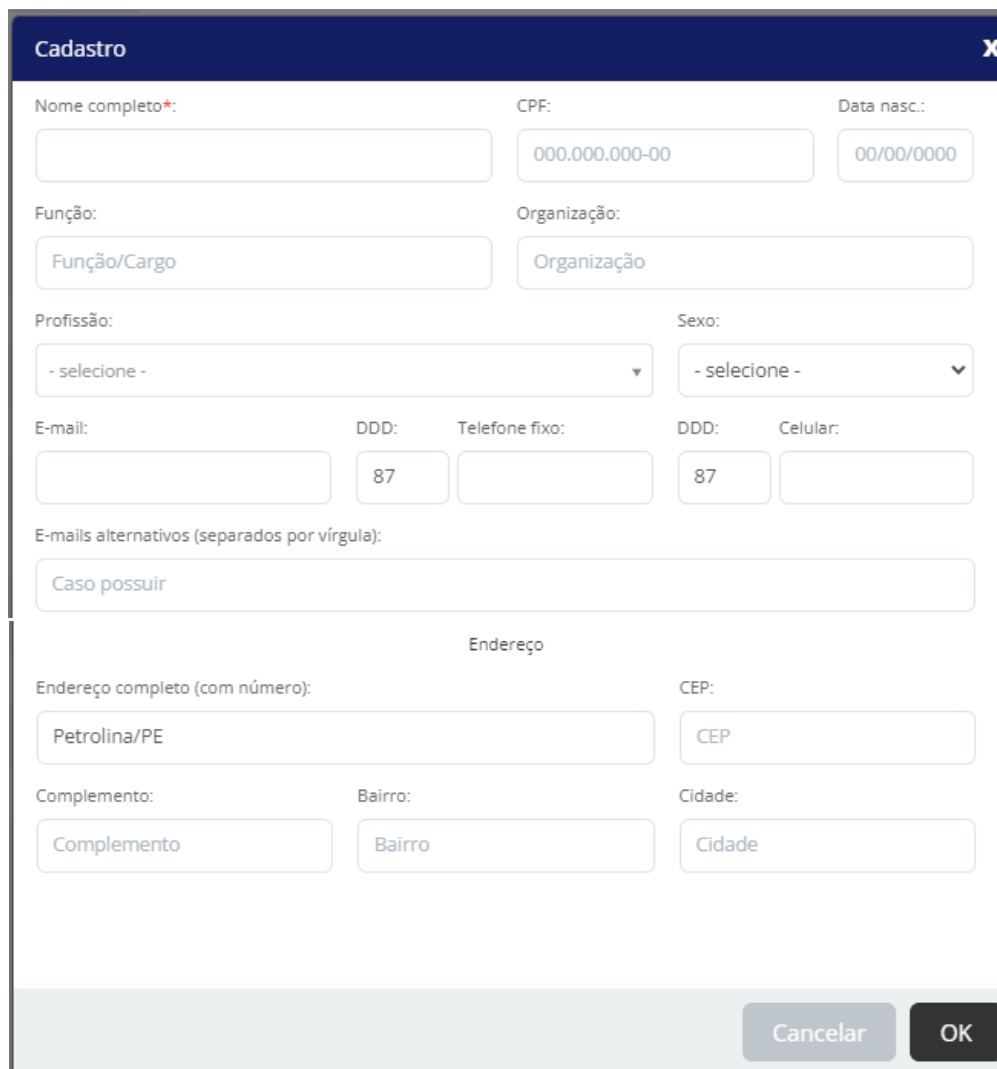
E-mail:

Telefone:

### ANEXO II

Cadastro feito por meio do próprio sistema 1doc, para que o segurado tenha acesso e possa solicitar qualquer tipo de demanda aos setores. Deve conter no mínimo as seguintes informações:

#### Cadastro de Segurado do IGEPREV:



**Cadastro** X

Nome completo\*:  CPF:  Data nasc.:

Função:  Organização:

Profissão:  Sexo:

E-mail:  DDD:  Telefone fixo:  DDD:  Celular:

E-mails alternativos (separados por vírgula):

Endereço

Endereço completo (com número):  CEP:

Complemento:  Bairro:  Cidade:

Cancelar OK