



INSS – INSTITUTO NACIONAL DO SEGURO SOCIAL

---

# Guia Prático – Cadastramento de Usuários Externos

PAT Entidade | GERID (GID e GPA)

Gestão de Usuários Externos · Entidades Conveniadas

# Objetivo do Guia

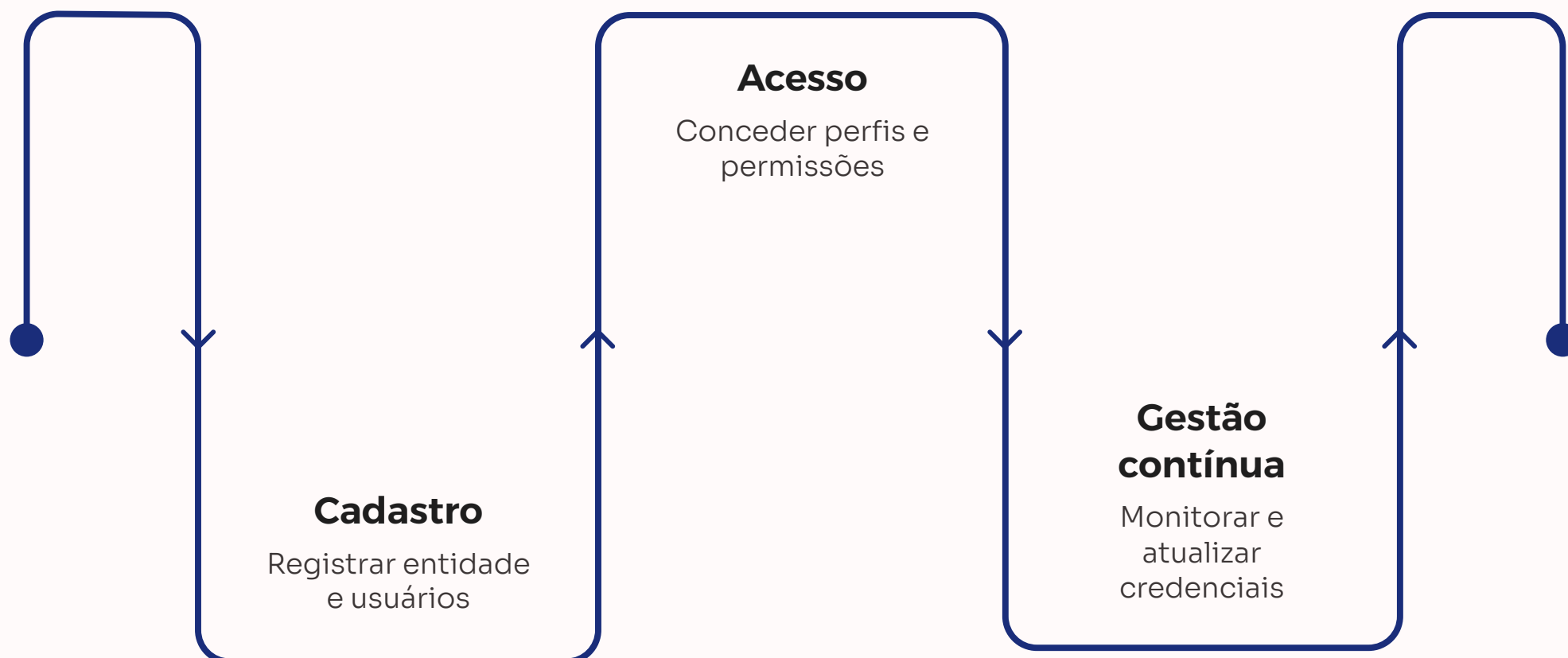
Este guia destina-se às entidades conveniadas do INSS e tem como objetivo apresentar, de forma clara e estruturada, as alterações decorrentes da implantação do novo modelo de gestão de identidades e acessos por meio do GERID (Dataprev), bem como orientar quanto aos procedimentos atualizados de cadastramento de usuários externos, concessão de acessos e gestão contínua para acessar o sistema PAT Entidade.

A atualização do GERID trouxe mudanças relevantes na forma de autenticação, na organização do fluxo de trabalho e na gestão dos usuários, com a centralização dos processos em um único ambiente e a adoção de maior controle e rastreabilidade das operações.

## Neste contexto, o presente guia tem como foco:

- Explicar o que mudou com o novo GERID
- Esclarecer como passa a funcionar o fluxo de cadastro e acesso
- Detalhar o papel do cadastrador externo no novo modelo
- Apresentar, de forma prática, o passo a passo atualizado para utilização do sistema

Ao longo do documento, são abordados os sistemas envolvidos — PAT Entidade e GERID —, as responsabilidades da entidade conveniada e os cuidados necessários para garantir a correta gestão dos acessos. Ao final, é apresentado um resumo consolidado do fluxo completo para facilitar a consulta rápida no dia a dia da entidade.



# Portal de Atendimento

## Portal de Atendimento – PAT Entidade

O **Portal de Atendimento – PAT Entidade** (<https://atendimento.inss.gov.br/>) é a plataforma oficial utilizada para o registro e a gestão dos requerimentos de benefícios e serviços no âmbito do INSS. Trata-se do mesmo sistema utilizado pela Central 135, pelo Meu INSS e pelas unidades de atendimento do Instituto, o que garante padronização, integração e uniformidade nos procedimentos.

Por meio do PAT, cada solicitação registrada dá origem a um **Processo Administrativo Previdenciário (PAP)**, conjunto de atos que formaliza o pedido e possibilita sua análise pelo INSS. Nesse contexto, o papel da entidade conveniada é fundamental: cabe a ela assegurar que o requerimento seja corretamente instruído, com dados consistentes e documentação completa, contribuindo diretamente para a agilidade e a qualidade da análise.

O PAT substituiu sistemas anteriores, como o **SAG/SEC**, representando um avanço significativo em termos de padronização, integração e segurança da informação. Atualmente, constitui o principal ambiente de atendimento previdenciário digital.

Ao operacionalizar o Acordo de Cooperação Técnica (ACT) por meio do PAT, a entidade conveniada desempenha papel relevante na ampliação do acesso aos serviços previdenciários, contribuindo para a redução de filas, a otimização de recursos institucionais e o fortalecimento da política de proteção social.

- Destaca-se que o êxito na análise dos requerimentos está diretamente relacionado à qualidade das informações prestadas. Dados incorretos, incompletos ou documentos ilegíveis podem ocasionar exigências, atrasos ou indeferimentos. Por outro lado, processos bem instruídos favorecem decisões mais céleres, seguras e efetivas.

**Cada requerimento corretamente instruído representa não apenas um procedimento administrativo bem executado, mas um passo concreto para que o direito do cidadão seja reconhecido com rapidez, segurança e dignidade.**

### Sistema anterior

**SAG/SEC** — plataforma anterior substituída pelo PAT, com ganhos em padronização, integração e segurança da informação.

### Sistema atual

**PAT Entidade** — plataforma oficial de atendimento previdenciário digital, integrada à Central 135, ao Meu INSS e às unidades do INSS.

### Processo gerado

**PAP (Processo Administrativo Previdenciário)** — conjunto de atos que formaliza cada requerimento registrado e possibilita sua análise pelo INSS.

# O que é o GERID

O **GERID** é o sistema desenvolvido e mantido pela **Dataprev** responsável pelo controle de identidades e acessos aos sistemas do INSS. Em termos práticos, o GERID atua como o "**porteiro digital**" dos sistemas institucionais: ele verifica quem está solicitando acesso, se essa pessoa está devidamente cadastrada e se possui as permissões necessárias para utilizar os recursos solicitados.

Para as entidades conveniadas, o GERID é o ambiente onde todas as operações relacionadas a usuários externos são registradas e gerenciadas. Isso inclui o cadastro inicial de novos usuários, a alteração de dados cadastrais, a concessão ou revogação de permissões de acesso e a exclusão de usuários que deixaram de ter vínculo com a entidade.

Toda ação realizada no GERID é registrada com data, hora e identificação do responsável, garantindo rastreabilidade e auditoria.

O INSS modernizou o controle de acessos com a implantação do **novo GERID (Gerenciador de Identidades da Dataprev)**, trazendo melhorias importantes para as entidades

O acesso ao GERID é feito por meio de **certificado digital**, o que confere segurança jurídica e técnica às operações realizadas. A entidade deve garantir que seus responsáveis possuam certificados digitais válidos e que estejam corretamente vinculados ao sistema antes de iniciar qualquer procedimento de cadastro ou gestão de acessos.



## Controle de identidades

Gerencia quem são os usuários autorizados a acessar os sistemas do INSS, com validação por certificado digital e registro completo de todas as operações.



## Rastreabilidade e auditoria

Todas as ações realizadas no sistema são registradas com data, hora e identificação do responsável, garantindo total transparência e conformidade.



## Gestão de acessos

Define quais recursos e funcionalidades cada usuário pode utilizar, com base nas permissões concedidas pela entidade e validadas pelo INSS.



## Infraestrutura Dataprev

Sistema desenvolvido e mantido pela Dataprev, garantindo alta disponibilidade, segurança e integração com os demais sistemas do INSS.

# Nova estrutura do sistema

Recentemente, o GERID passou por uma evolução tecnológica com a adoção de uma nova base de dados mais moderna e eficiente. Essa mudança tem como objetivo principal melhorar o desempenho, aumentar a capacidade de processamento e ampliar as funcionalidades de gestão, especialmente na geração de relatórios e no controle de usuários.

- ❏ Importante destacar que essa alteração ocorre de forma gradual e transparente para as entidades conveniadas. Na prática, não há mudança imediata na lógica de utilização, mas sim uma melhoria na infraestrutura que sustenta o sistema.

## Estrutura atual do GERID (fase de transição)

Atualmente, o ambiente do GERID encontra-se em processo de transição entre a estrutura antiga e a nova. Durante esse período, coexistem diferentes módulos:

<b>GID (cadastro de usuários)</b> Responsável pelo registro dos dados cadastrais dos usuários externos, como identificação, e-mail institucional e vínculo com a entidade.	<b>GPA (Gestão de Permissões de Acesso)</b> Responsável pela concessão, alteração e revogação das permissões de acesso aos sistemas do INSS.	<b>Novo GERID (base atualizada)</b> Nova estrutura que está gradualmente incorporando as funcionalidades dos módulos anteriores, com melhor desempenho e maior capacidade de gestão.
---	---	---

## Como funciona na prática

Neste momento, as entidades conveniadas continuam utilizando:

- o módulo de cadastro (GID) para inclusão e manutenção de usuários;
- o módulo de permissões (GPA) para concessão de acessos.

À medida que os sistemas forem sendo migrados para a nova estrutura, essas funcionalidades serão unificadas em um único ambiente, simplificando a operação.

# O que mudou com o novo GERID

## ANTES

- Controle de acesso mais limitado, com menos recursos para organizar, acompanhar e ajustar permissões conforme a necessidade operacional.
- Cadastro e permissões menos estruturados, o que dificultava a padronização dos procedimentos e tornava o processo mais sujeito a inconsistências.
- Menor rastreabilidade das ações, reduzindo a visibilidade sobre quem realizou cada operação e em que momento ela ocorreu.

## AGORA

- Traz mais organização ao fluxo de trabalho e torna cada etapa mais objetiva.
- Controle centralizado pelo GERID (Dataprev), permitindo uma gestão unificada das informações e maior consistência na administração dos usuários.
- Emissão de relatórios gerenciais dos usuários.
- Renovação em lote otimizada.
- Gestão mais organizada e segura, com processos mais claros para acompanhar, conceder e revisar acessos de forma controlada.

## Ganhos para os usuários externos

### Mais segurança

Acesso vinculado ao certificado digital, garantindo que apenas pessoas devidamente identificadas possam acessar os sistemas. Isso reduz riscos de fraudes, evita acessos indevidos e fortalece a proteção das informações.

### Mais controle

A entidade pode definir com precisão o sistema que cada usuário acessa, por quanto tempo o acesso permanece ativo e qual é o nível de permissão concedido. Isso torna a gestão mais precisa e alinhada às necessidades de cada perfil.

### Rastreabilidade

O histórico completo das ações fica registrado no GERID, permitindo acompanhar cada operação realizada e consultar registros quando necessário. Isso favorece auditorias, amplia a transparência e apoia a comprovação de conformidade.

### Menos risco de uso indevido

Os acessos podem ser revogados imediatamente em caso de desligamento, mudança de vínculo ou identificação de irregularidade. Dessa forma, a entidade mantém maior proteção e reduz a exposição a usos inadequados.

### Gestão mais eficiente

A entidade passa a ter autonomia para cadastrar, alterar e revogar acessos, o que agiliza os processos internos e melhora a resposta às necessidades operacionais do dia a dia.

## E para o usuário externo muda algo?

### Mesmo endereço de acesso

O Portal de Atendimento (PAT Entidade - <https://atendimento.inss.gov.br/>) continua sendo acessado pelo mesmo endereço de sempre. Nada muda para o usuário nesse ponto.

### Nova camada de autenticação

A validação do usuário e a autorização de acesso passam a ocorrer no novo ambiente do GERID, mais seguro e centralizado.

### Sem mudança nos requerimentos

Não há alteração no sistema de requerimentos. A mudança é exclusivamente na camada de autenticação e gestão de acessos, que foi modernizada e unificada.

# O papel do cadastrador externo

A entidade conveniada com mais de 20 usuários ativos deve indicar formalmente **dois responsáveis** para atuar na gestão dos usuários externos no sistema GERID: um **titular** e um **substituto**.

O cadastrador externo é uma figura central para garantir que a entidade conveniada funcione de maneira organizada e segura dentro do ACT INSS Digital. Seu papel vai além do simples acesso ao sistema: ele é responsável por habilitar os usuários externos da entidade no Portal de Atendimento (PAT Entidade), garantindo que todos tenham perfis corretos e segurança no uso da ferramenta.

- ☐ "É o representante da entidade conveniada responsável por cadastrar, atualizar e manter os acessos dos demais representantes no sistema."

Esses profissionais acumularão duas funções essenciais: a de **cadastrador externo** e a de **gestor de acesso**. A indicação deve ser formalizada junto ao INSS e os responsáveis devem possuir certificado digital válido para operar nos sistemas.

## Usuário externo

Somente entidades com mais de 20 representantes ativos podem indicar cadastradores externos.

## Titular

Cada entidade pode indicar um representante titular para essa função.

## Substituto

Cada entidade pode indicar um representante substituto para essa função.

## Quem pode ser cadastrador externo

Os responsáveis indicados pela entidade (titular e substituto), que atuarão como cadastrador externo e gestor de acesso, devem possuir vínculo formal com a entidade.

**Estar autorizado formalmente pela instituição**

**Possuir vínculo com a entidade**

**Curso Entidades Parceiras - ACT INSS Digital**

**Assinar o Termo de Compromisso e Manutenção de Sigilo (TCMS)**

A indicação de usuários sem vínculo direto com a entidade (como terceirizados, voluntários ou prestadores de serviço) deve ser feita com cautela. Nesses casos, a entidade assume integral responsabilidade pelo acesso concedido. Recomenda-se que exista formalização do vínculo (contrato, designação ou instrumento equivalente) e que haja controle e supervisão direta da atuação desse usuário.

- ☐ O acesso é pessoal, intransferível e vinculado à responsabilidade da entidade perante o INSS.

## Documentação e responsabilidade

Além das etapas operacionais no GERID, o cadastramento de usuários externos deve ser acompanhado da formalização documental pela entidade.

- TCMS – Termo de Compromisso e Manutenção de Sigilo
- Termo de Ciência de Boas Práticas de Segurança Cibernética
- Declaração de participação no Curso Entidades Parceiras – Escola PEP
- Documento de identificação

A entidade é responsável por manter os documentos atualizados e organizados, garantir que os usuários cadastrados estejam autorizados e apresentar a documentação sempre que solicitada pelo INSS.

- ☐ O GERID controla o acesso, mas a responsabilidade pela legitimidade do usuário é da entidade.

## Importância do cadastrador externo

**O cadastrador externo é o guardião da porta de entrada digital da entidade no ACT INSS Digital — responsável por garantir que apenas usuários habilitados e preparados utilizem o sistema, fortalecendo a parceria com o INSS e contribuindo para um atendimento mais ágil, seguro e transparente.**

## Responsabilidades do cadastrador externo

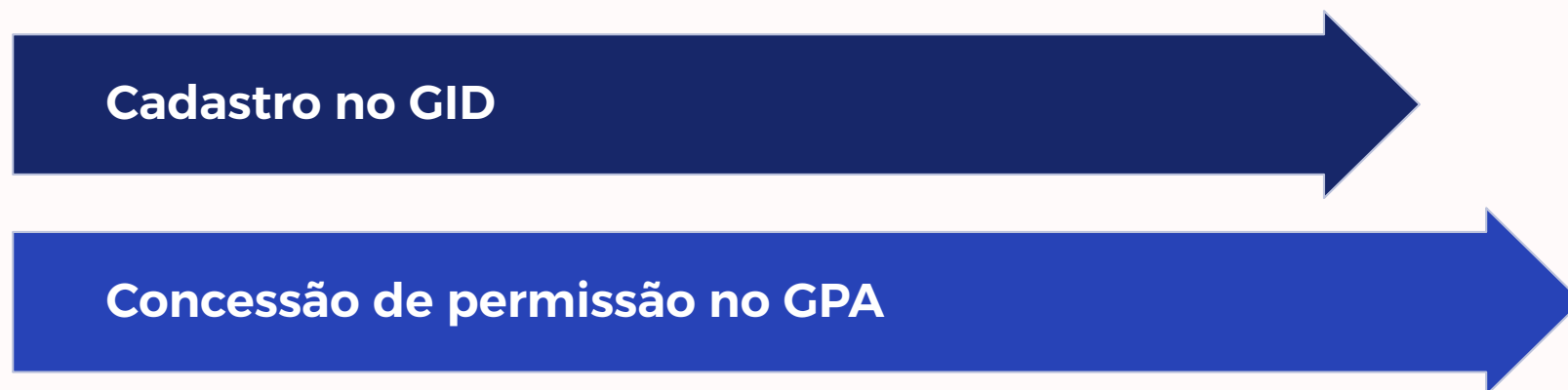
- Garantir que apenas pessoas autorizadas tenham acesso ao sistema.
- Manter atualizados os cadastros: exclusão de representantes desligados, prorrogação de acessos e atualização de contatos.
- Orientar os novos representantes sobre segurança da informação, uso correto do PAT e obrigações do ACT.
- Abrir chamados no Suporte INSS/ACT sempre que necessário para desbloqueios, ajustes ou inconsistências.
- Conferência dos documentos necessários para o cadastro do usuário externo.

# Etapas do processo de cadastramento

O cadastramento de usuários externos no **GERID** acontece dentro de um único sistema, mas em duas áreas diferentes: o **GID**, em que o usuário é cadastrado, e o **GPA**, em que o acesso é liberado. Essas duas etapas são feitas pelo **cadastrador externo** da entidade, com uso de certificado digital.

O processo é simples e precisa seguir a ordem certa. Primeiro, o usuário deve estar cadastrado e ativo no **GID**. Só depois disso é possível liberar o acesso no **GPA**. Se o cadastro não estiver pronto no GID, o acesso não pode ser concedido. E, se o acesso não for liberado no GPA, o usuário ainda não poderá usar os sistemas do INSS.

Por isso, o cadastrador externo deve liberar apenas as permissões necessárias para a função do usuário, sem excesso nem falta.



O diagrama acima mostra o caminho que deve ser seguido: primeiro, cadastrar as informações do usuário no **GID**; depois que o cadastro estiver ativo, liberar as permissões de acesso no **GPA**. A ordem é sempre essa, e as duas etapas ficam sob responsabilidade do cadastrador externo indicado pela entidade conveniada.

# Documentação e pré-requisitos para o cadastramento

Antes de efetuar o cadastramento, verifique se consta no processo:

## → Documentos necessários para o cadastro usuário externo

- Conferir os termos obrigatórios:
  - TCMS – Termo de Compromisso e Manutenção de Sigilo
  - Termo de Ciência de Boas Práticas de Segurança Cibernética
- Declaração de Participação no Curso Entidades Parceiras – Escola PEP
- Documento de identificação

## → Documentos necessários para o cadastro de advogado pelo ACT OAB

- Verificar regularidade cadastral do advogado
- Analisar se há incompatibilidade ou impedimento
- Conferir os termos obrigatórios:
  - Termo de Aceite (\* para advogados - ACT com a OAB)
  - TCMS – Termo de Compromisso e Manutenção de Sigilo
  - Termo de Ciência de Boas Práticas de Segurança Cibernética
- Declaração de Participação no Curso Entidades Parceiras – Escola PEP
- Documento de identificação

## Passo a passo – cadastramento no GERID - módulo GID

Ao incluir os dados do usuário externo no GERID no módulo GID, esta ação criará um banco de dados que permitirá conceder a permissão acesso com o vínculo ao CNPJ informado.

<p>01</p> <hr/> <p>Acesse o endereço: <a href="http://geridinss.dataprev.gov.br">geridinss.dataprev.gov.br</a></p>	<p>02</p> <hr/> <p>Clique em "Autenticar" e digite CPF e senha para fazer login.</p>
<p>03</p> <hr/> <p>Informe o código de verificação gerado pelo aplicativo de Autenticação de Multifatores (Google Authenticator, Microsoft Authenticator etc.) instalado em seu celular.</p>	<p>04</p> <hr/> <p>Clique no botão "Entrar".</p>
<p>05</p> <hr/> <p>Vá ao Menu "Cadastro" e clique em "Cadastradores Externos".</p>	<p>06</p> <hr/> <p>No campo "Grupo", selecione a opção "PJ".</p>
<p>07</p> <hr/> <p>Em "Unidade Organizacional", informe o número do CNPJ da entidade sem caracteres especiais.</p>	<p>08</p> <hr/> <p>Clique em "Buscar Unidades".</p>
<p>09</p> <hr/> <p>No campo "Unidade", clique sobre o número do CNPJ e nome da entidade e depois clique em "Filtrar". Serão listados todos os representantes já cadastrados.</p>	<p>10</p> <hr/> <p>Caso o representante não conste na lista, clique em "Novo Usuário" para realizar o cadastro.</p>
<p>11</p> <hr/> <p>Preencha os dados do representante. Verifique se o e-mail e o nome estão corretos. Informe também o telefone de contato e clique em "Confirmar".</p>	<p>12</p> <hr/> <p>Uma senha automática será enviada ao e-mail cadastrado.</p>

**ATENÇÃO:** É necessário que o usuário cadastrado altere a senha em 24h. Após concluir o cadastramento, altere a 'Situação de Acesso' para 'Ativo'. Estando o representante inativo, siga: Consulte o usuário → Clique em 'Alterar Situação' → Selecione 'Ativo' → Preencha o campo 'Motivo'.

Depois de incluir o representante, somente a Dataprev poderá alterar dados como nome e e-mail. Nesses casos, abra um ticket pelo Suporte INSS/ACT.

# Cadastramento de acesso no módulo - GPA

Após criar a identidade no GID, é hora de atribuir permissão de acesso nos sistemas. A concessão dessa autorização permite que o representante acesse o Portal de Atendimento (atendimento.inss.gov.br).

## Passo a passo – acesso no GPA

01	Acesse o endereço: geridinss.dataprev.gov.br	02	Fazer login com certificado digital
03	Informe o código de verificação gerado pelo aplicativo de Autenticação de Multifatores (Google Authenticator, Microsoft Authenticator etc.) instalado em seu celular.	04	Clique no botão "Entrar".
05	Clique em "Atribuições" e selecione "Autorizações de Acesso".	06	Escolha a forma de cadastro: clique em "Novo" para cadastrar um usuário por vez, ou em "Novo Múltiplos Usuários" para cadastrar vários representantes de uma só vez.

## Como preencher os campos

<b>Sistema</b> SAG	<b>Subsistema</b> SAG_EXTERNO (para entidades convencionais) / SAG_EXTERNO_OAB (para a OAB)	<b>Papel</b> ENTIDADE_CONVENIENDA_PROTOCOLO (na maioria dos casos) / ENTIDADE_CONVENIENDA_OAB (para a OAB)	<b>Tipo de domínio</b> CNPJ
<b>Data de validade</b> data fim da validade do acesso, limitada à data de acesso do cadastrador e não superior à vigência do ajuste	<b>Período de acesso</b> dias da semana conforme o plano de trabalho	<b>Hora de acesso/início</b> hora de início dos trabalhos conforme o plano de trabalho	<b>Hora de acesso/fim</b> hora de encerramento dos trabalhos conforme o plano de trabalho
<b>Domínio</b> CNPJ da entidade, sem pontos ou travessão	<b>Usuário</b> CPF do representante, sem pontos ou travessão		

Após preencher todos os campos, clique em 'Avançar', adicione os usuários com 'Incluir usuário' e finalize clicando em 'Concluir'.

# Atualização de dados cadastrais

A manutenção dos dados cadastrais dos usuários externos é uma responsabilidade contínua da entidade conveniada. Sempre que houver alteração em qualquer informação registrada no GID — como mudança de e-mail institucional, atualização de nome, alteração de CPF ou qualquer outro dado pessoal — o **cadastrador externo** deve proceder à atualização no sistema de forma tempestiva.

Dados desatualizados podem gerar problemas operacionais significativos, como o não recebimento de comunicações oficiais do INSS, falhas na autenticação com certificado digital (quando há divergência entre os dados do certificado e os dados cadastrados) e até mesmo o bloqueio preventivo do acesso por inconsistência de informações. Por isso, a atualização deve ser realizada tão logo a entidade tome conhecimento da alteração.

O processo de atualização é realizado integralmente no módulo **GID**, pelo cadastrador externo, mediante autenticação com certificado digital. Não é necessário abrir chamado ou solicitar autorização prévia do INSS para realizar alterações cadastrais de usuários vinculados à própria entidade. A entidade tem autonomia para gerir os dados de seus próprios usuários, dentro dos limites de sua competência.

## Dados que requerem atualização

Os principais dados que devem ser mantidos atualizados no GID incluem:

- Endereço de e-mail institucional
- Nome completo do usuário
- Correção de CPF em caso de erro de digitação no cadastro
- Vínculo com a entidade conveniada
- Situação

## Como realizar a atualização

O processo de atualização segue os passos abaixo:

1. Acessar o módulo GID com certificado digital válido
2. Localizar o usuário cujo dado será atualizado
3. Selecionar a opção de edição de cadastro
4. Alterar o campo necessário e confirmar a operação
5. Verificar se a alteração foi registrada corretamente
6. Comunicar ao usuário sobre a atualização realizada

📄 Em caso de dúvida sobre qual campo alterar, consulte o manual operacional do GERID ou entre em contato com o suporte técnico do INSS.

# Responsabilidades da entidade conveniada

A entidade conveniada do INSS assume responsabilidades específicas e intransferíveis no que tange à gestão dos usuários externos que operam em seu nome nos sistemas institucionais. Essas responsabilidades não se encerram com o cadastramento inicial — elas se estendem por todo o ciclo de vida do vínculo do usuário com a entidade, exigindo atenção contínua e processos internos bem definidos.

A legislação e as normas do INSS estabelecem que a entidade é corresponsável pela segurança e conformidade dos acessos concedidos a seus colaboradores. Isso significa que a entidade pode ser chamada a prestar esclarecimentos sobre acessos indevidos, usuários ativos sem vínculo atual ou permissões concedidas de forma inadequada. Manter uma gestão rigorosa dos acessos é, portanto, uma obrigação legal e institucional da entidade.

**1**

## Manter acessos atualizados

A entidade deve revisar periodicamente os acessos concedidos a seus usuários, garantindo que as permissões no GPA reflitam a realidade funcional de cada colaborador. Usuários que mudaram de função devem ter suas permissões ajustadas, e acessos que não são mais necessários devem ser revogados prontamente. Recomenda-se uma revisão semestral formal de todos os acessos ativos.

**2**

## Excluir usuários sem vínculo

Quando um usuário deixa de ter vínculo com a entidade — seja por desligamento, término de contrato, aposentadoria ou qualquer outra razão — a entidade tem a obrigação de **solicitar a exclusão ou bloqueio do cadastro** no GID imediatamente. Manter usuários desvinculados com acesso ativo aos sistemas do INSS constitui irregularidade grave e pode gerar responsabilização da entidade.

**3**

## Zelar pela segurança das credenciais

A entidade deve orientar seus usuários sobre a importância de proteger seus certificados digitais e credenciais de acesso. O compartilhamento de certificados, o uso de senhas fracas ou o acesso a partir de dispositivos não seguros são práticas que comprometem a segurança do sistema e podem resultar em bloqueio de acessos e abertura de processo administrativo.

**4**

## Comunicar alterações ao INSS

Alterações na estrutura da entidade — como mudança de responsáveis, alteração de endereço, fusão ou cisão — devem ser comunicadas formalmente ao INSS para que os registros no GERID sejam atualizados. A entidade deve manter seus dados institucionais sempre atualizados junto ao INSS, garantindo a continuidade dos serviços e a validade dos acessos concedidos.

# Fluxo completo: do cadastro à gestão contínua

Este guia percorreu todos os aspectos essenciais do processo de cadastramento e gestão de usuários externos no sistema PAT Entidade | GERID. Para facilitar a consulta rápida e a memorização do fluxo completo, apresentamos abaixo o resumo consolidado das etapas e responsabilidades que toda entidade conveniada deve dominar.

Lembre-se: o processo não termina com a concessão do acesso. A gestão contínua, incluindo atualização de dados, revisão de permissões e exclusão de usuários desvinculados, é parte integrante e obrigatória das responsabilidades da entidade. Um acesso bem gerido é um acesso seguro e que protege tanto a entidade quanto os cidadãos atendidos pelo INSS.


## Pontos de atenção

- O GID e o GPA são módulos complementares e sequenciais
- O certificado digital é obrigatório para todas as operações
- A entidade é responsável pela exclusão de usuários desvinculados
- Dados desatualizados podem gerar bloqueio de acesso
- O substituto possui as mesmas atribuições do titular

## Canais de suporte

Em caso de dúvidas sobre os procedimentos descritos neste guia, a entidade conveniada deve consultar:

- O manual operacional do sistema GERID
- As comunicações oficiais do INSS sobre o PAT Entidade
- O suporte técnico disponibilizado pela Dataprev
- A Portaria DTI/INSS nº 105/2023 (base legal do sistema)

 Este guia é um documento de referência prática. Para informações atualizadas, consulte sempre os canais oficiais do INSS.