Política de Acesso do CADASTRO ÚNICO

Gestão de Acesso e Responsabilidades de Operadores(as) do Sistema

SECRETARIA DE AVALIAÇÃO, GESTÃO DA INFORMAÇÃO E CADASTRO ÚNICO

MINISTÉRIO DO DESENVOLVIMENTO E ASSISTÊNCIA SOCIAL, FAMÍLIA E COMBATE À FOME

GOVERNO FEDERAL

VOCÊ JÁ OUVIU FALAR DA POLÍTICA DE CONTROLE DE ACESSO DO CADASTRO ÚNICO?

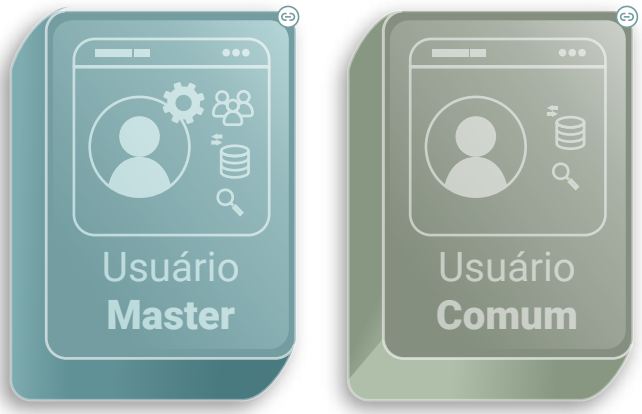
O MDS instituiu, em 2017, a Política de Acesso do Cadastro Único, que estabelece:

- As regras para controlar e monitorar o acesso aos dados identificados da base de dados do CadÚnico, vinculando sistemas de informação e outros meios de acesso direto a esses dados; e
- Os direitos e deveres dos usuários dos dados do Cadastro Único.

Se você trabalha com o Cadastro Único, essas informações são muito importantes para o seu dia a dia!

VAMOS COMEÇAR TE APRESENTANDO UMA NORMA:

A Portaria n° 502 de 2017 que estabeleceu a Política de Controle de Acesso aos Dados do Cadastro Único para Programas Socais, definiu dois tipos de usuários(as) do sistema que podem manipular a base de dados do Cadastro Único:



Vamos conhecer nesta cartilha um pouco mais sobre cada perfil de usuário(a)!

Usuário **Master**

A PESSOA INDICADA COMO USUÁRIA MASTER REALIZA A GESTÃO DAS PERMISSÕES E ACESSOS DOS(AS) USUÁRIOS(AS) COMUNS, ALÉM DE TODAS AS ATIVIDADES ATRIBUÍDAS NO SISTEMA A UMA PESSOA COM PERFIL DE USUÁRIA COMUM!

A pessoa com perfil de Usuária Master é responsável por:

- Cadastrar as pessoas que serão Usuárias Comuns do sistema, com perfil de acesso adequado às atribuições que serão desempenhadas;
- Realizar a gestão dos acessos ao sistema do Cadastro Único no Município;
- Reavaliar, **diariamente**, as permissões e retirar imediatamente o acesso ao sistema do Cadastro Único das pessoas usuárias que:
  - não trabalham mais na equipe; ou
  - estejam acessando indevidamente o sistema.
- Retirar o acesso do(a) Usuário(a) Comum que violar ou tentar violar o sigilo dos dados e realizar apuração e punição administrativa; e
- Reportar ao MDS qualquer fato que possa violar a segurança das informações do Sistema de Cadastro Único.

ATENÇÃO – Clique aqui e consulte o Manual Operacional do Sistema do Cadastro Único, na seção 16, e siga as orientações para realizar a permissão e o acesso dos(as) usuários(as)!

Usuário **Comum**

A PESSOA QUE TEM O PERFIL DE USUÁRIA COMUM PODE ACESSAR E OPERACIONALIZAR O SISTEMA DO CADASTRO ÚNICO, MAS SUA ATUAÇÃO É RESTRITA ÀS ATIVIDADES PREVIAMENTE AUTORIZADAS.

A pessoa com perfil de Usuária Comum é responsável por:

- Utilizar os dados apenas para as finalidades que foram autorizadas pelo(a) Usuário(a) Máster;
- Zelar pelo bom uso e sigilo dos dados;
- Reportar ao(à) Usuário(a) Master qualquer fato que possa violar a segurança da informação;
- Solicitar ao(à) Usuário(a) Master a exclusão do seu acesso ao sistema quando:
  - estiver afastado(a) de suas atribuições;
  - não tiver mais necessidade de acesso às informações cadastrais.

ATENÇÃO – O MDS pode verificar periodicamente, junto às pessoas Usuárias Master dos municípios, a regularidade da situação do perfil dos(as) usuários(as) do sistema de Cadastro Único.

AS PESSOAS QUE TRABALHAM COM A BASE DE DADOS DO CADASTRO ÚNICO DEVEM:

- Ter o **Termo de Compromisso e Manutenção de Sigilo (TCMS)** assinado e autorizado pelo(a) Coordenador(a) Municipal/Estadual do Cadastro Único, conforme previsto na Portaria n° 810/2022;
- Seguir as normas da Portaria MDS n° 810/2022.
- Adotar medidas que garantam o sigilo dos dados e a segurança quanto ao acesso indevido ao sistema de Cadastro Único de pessoas não autorizadas.

OLHO VIVO! – Os dados do Cadastro Único são sigilosos, então observe e siga todas as recomendações previstas na legislação, em especial a Lei Geral de Proteção de Dados Pessoais (LGPD) e o Decreto nº 11.016, de 29 de março de 2022.

SEGURANÇA E CONTROLE DOS DADOS

Para trabalhar de forma segura com os dados do Cadastro Único é importante observar os seguintes procedimentos:

- **NUNCA compartilhe seu acesso ou a sua senha! A autorização de acesso ao sistema do Cadastro Único é INDIVIDUAL;**
- **NÃO repasse a terceiros, sem autorização do(a) Coordenador(a) Municipal/Estadual do Cadastro Único, as informações acessadas;**
- NÃO armazene os arquivos em ambiente de rede aberto e compartilhado com pessoas não autorizadas;
- INSTALE dispositivos de proteção contra softwares maliciosos nos computadores utilizados para acesso ao sistema;
- Adote BOAS PRÁTICAS para preservar as informações do Cadastro Único, observando seu caráter de acesso restrito, como, por exemplo:
  - deletar o arquivo da base de dados quando concluir o uso ou após carregar em um banco de dados seguro;
  - criptografar as bases para evitar que, em eventuais ataques, as informações do Cadastro Único possam ter seu conteúdo facilmente acessado;
  - manter os dados nos bancos de dados e sistemas apenas pelo tempo necessário para o uso; e
  - seguir a Portaria n° 810/2023 e a Política de Controle de Acesso do Cadastro Único que estabelece uma cadeia de responsabilidade na gestão de acessos.

ATENÇÃO – Se as bases do Cadastro Único forem carregadas em um sistema gerenciador de bancos de dados ou em outro sistema do município, é preciso estabelecer um procedimento de controle de acesso que certifique que apenas pessoas usuárias, previamente autorizadas pelo(a) Coordenador(a) Municipal e que tenham o TCMS assinado, manipulem os dados do Cadastro Único.

COMO TRATAR CASOS DE SUSPEITA DE FRAUDES NO CADASTRO ÚNICO?

Ao identificar cadastramentos suspeitos, verifique se:

- os formulários ou folhas-resumo existem e se foram assinados pelo(a) Responsável Familiar; e
- as pessoas operadoras do sistema do Cadastro Único reconhecem a operação suspeita e se houve conduta indevida por erro ou má fé.

Identificada a má fé, a gestão municipal deve:

- retirar todos os perfis de acesso da pessoa;
- avaliar todos os cadastros que tenham sido manipulados por ela; e
- realizar um processo de apuração de responsabilidades no âmbito do município.

Realize a correção dos registros fraudados ou a exclusão do cadastro, quando você constatar que ele é inexistente.

OLHO VIVO! – Para mais orientações sobre o processo de suspeita de fraudes no Cadastro Único, consulte a Instrução Operacional nº 02/2019.

DICAS VALIOSAS:

- **NUNCA COMPATILHE SUA SENHA!** Todas as operações realizadas no Cadastro Único ficam registradas no CPF de quem logou no sistema;
- Fuja dos fraudadores! O MDS, a CAIXA, e a DATAPREV **NÃO entram em contato** para solicitar a sua senha!;
- **NUNCA** clique em um link para recadastrar senha que você não solicitou;
- Em caso de **DÚVIDAS**, ligue para o Suporte Operacional da CAIXA, no **4004-0104**;
- **NÃO** utilize aplicativos de terceiros, como jogos, testes de personalidade e edição de imagens, pois eles podem capturar suas informações pessoais e senhas;
- **EVITE** acessar sites desconhecidos ou programas não autorizados pela área de Tecnologia da Informação do seu município no computador utilizado para operação do Cadastro Único.

Proteger os dados do Cadastro Único é uma obrigação de todas as pessoas que operam o sistema!

VAMOS JUNTOS NESSA AÇÃO!