



INSTITUTO NACIONAL DO SEGURO SOCIAL

Diretoria De Benefícios

**PORTARIA DIRBEN/INSS Nº 901, DE 20 DE MAIO DE 2021**

Dispõe sobre regras de condutas de acesso pelos Titulares e Substitutos de Cartórios de Registro Civil ao Sistema Nacional de Informações de Registros Cíveis - SIRC

**O DIRETOR DE BENEFÍCIOS DO INSTITUTO NACIONAL DO SEGURO SOCIAL - INSS** uso da competência que lhe confere o Decreto nº 9.746, de 8 de abril de 2019, e tendo em vista o que consta no Processo Administrativo nº 35014.105039/2021-81,

RESOLVE:

Art. 1º Comunicar as regras de condutas de acesso pelos Titulares e Substitutos de Cartórios de Registro Civil ao Sistema Nacional de Informações de Registros Cíveis - SIRC, conforme descrição constante do anexo.

Art. 2º Esta Portaria entra em vigor na data de sua publicação.

**ALESSANDRO ROOSEVELT SILVA RIBEIRO**

Diretor de Benefícios



Documento assinado eletronicamente por **ALESSANDRO ROOSEVELT SILVA RIBEIRO, Diretor(a)**, em 20/05/2021, às 17:56, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do [Decreto nº 8.539, de 8 de outubro de 2015](#).



A autenticidade deste documento pode ser conferida no site [https://sei.inss.gov.br/sei/controlador\\_externo.php?acao=documento\\_conferir&id\\_orgao\\_acesso\\_externo=0](https://sei.inss.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0), informando o código verificador **3735804** e o código CRC **3DBB0C5C**.

## ANEXO I

### **REGRAS DE CONDUTAS DE ACESSO AO SIRC**

1. Com o objetivo de evitar irregularidades quanto ao controle de autorização e gestão de acesso ao Sistema Nacional de Informações dos Registro Civil – SIRC, ratificamos que as credenciais externas de acesso devem ser concedidas somente aos Titulares de Cartórios de Registros Cíveis de Pessoas Naturais, o substituto oficial e funcionários da serventia.

2. Os acessos e gestões ao SIRC dos Titulares de Cartórios de Registros Cíveis de Pessoas Naturais e substitutos são concedidos pelos servidores do INSS representantes da Central Especializada de Serviço de Informações de Segurados-CES/AIS das Gerências-Executivas de abrangência do cartório.

3. Os acessos dos funcionários dos cartórios de registro civil serão concedidos pelos Titulares ou substituto do cartório ou quem seja delegado para esta competência na serventia. Neste último caso, o Titular deverá repassar a gestão do SIRC ao delegado para a função.

4. A renovação da gestão de acesso, bem como do acesso dos usuários, ocorre por meio do Gerenciamento de Permissões e Acesso - GPA, no Gerenciamento de Identidades – GERID, pelo endereço eletrônico [geridins.dataprev.gov.br/gpa](http://geridins.dataprev.gov.br/gpa).

5. Quanto à utilização das credenciais e perfis de acesso ao SIRC, o usuário:

I - deve manter sigilo das informações obtidas por meio do perfil concedido;

II - deve utilizar os serviços e as informações obtidas, por meio do perfil de acesso, única e exclusivamente em razão do cumprimento do disposto no artigo 68 da Lei nº 8.212/91, quanto à obrigatoriedade do Cartório de Registro Civil de Pessoas Naturais e para os fins que lhe foi designado, cumprindo os procedimentos dispostos neste normativo, sem prejuízo das demais normatizações vigentes na Administração Pública Federal;

III - não pode divulgar, nem mesmo compartilhar, os códigos de segurança que lhe forem atribuídos (credenciais de acesso), os quais são pessoais e intransferíveis;

IV - não pode utilizar as credenciais para acessar os recursos disponíveis em mais de uma estação de trabalho simultaneamente;

V - não pode fazer uso das credenciais de acesso de outros usuários;

VI - deve comunicar ao INSS quaisquer violações ou incidentes referentes à proteção do dado, do software ou de outros ativos da informação;

VII - deve, sempre que for necessário, afastar-se da estação de trabalho, certificar-se de que a sessão de acesso ao sistema corporativo esteja encerrada ou bloqueada;

VIII - deverá, obrigatoriamente, efetuar processo de alteração da sua senha em seu primeiro acesso à rede de dados corporativa; e

IX - no ato do primeiro acesso, o usuário deverá manifestar concordância com os termos dispostos na mesma e com o contido no item 11 do presente documento.

6. É vedado aos Gestores de Acesso ao SIRC atribuir perfil de acesso e/ou de gestão ao referido Sistema aos menores de 18 anos de idade, salvo os devidamente emancipados.

7. É obrigação dos Gestores de Acesso ao SIRC realizar a manutenção de credenciamentos dos usuários em decorrência da sua gestão, devendo para tanto:

I - excluir perfil de acesso e/ou de gestão ao SIRC de Titular, substituto ou funcionário que não esteja mais no quadro funcional do Cartório de registro Civil que possui credencial;

II - excluir perfil de acesso e/ou de gestão ao SIRC de Titular, substituto ou funcionário que tenha

vindo à óbito.

8. Em caso de alteração do emissor da credencial, para fins de captura do perfil de acesso ou gestão no GERID, o novo gestor de acesso deverá localizar no GPA, por meio do filtro de pesquisa, o usuário que deseja alterar, selecioná-lo, clicar em "Alterar" e em seguida não havendo necessidade de alteração da credencial, clicar em "Confirmar".

9. Compete aos Titulares e/ou substituto do cartório responsáveis pela atribuição de perfis de acesso ao SIRC efetuar o controle dos acessos, bem como orientar seus funcionários quanto ao uso responsável e adequado dos acessos concedidos, sendo que aqueles que fizerem mau uso desses acessos estarão sujeitos à responsabilização penal, civil e disciplinar.

10. Com relação às senhas de acesso, deve se observar que:

I - deverão ter no mínimo oito caracteres e conter, obrigatoriamente, caracteres alfanuméricos (combinação de letras e números). O usuário poderá acrescentar caracteres especiais (espaços em branco, símbolos, sinais de pontuação, etc.);

II - é vedada a reutilização das últimas quatro senhas utilizadas pelo usuário;

III - podem ser alteradas sempre que preciso ou quando o usuário achar necessário;

IV - o prazo de validade não deve ultrapassar 90 (noventa) dias; e

V - o usuário receberá, por meio de comunicado direto (via interface do sistema ou por mensagem no correio eletrônico), a informação do prazo próximo de vencimento da senha, quando esta estiver a 15 (quinze) dias da sua data de expiração.

11. O Termo de Responsabilidade de Compromisso e Sigilo - TCMS possui os seguintes termos, devendo o usuário comprometer-se à:

I - Manusear os dados identificados do SIRC apenas por necessidade de determinação expressa legal;

II - Manter a absoluta cautela quando da exibição de dados em tela, impressora, ou, ainda, na gravação em meios eletrônicos, afim de evitar que deles venham a tomar ciência pessoas não autorizadas;

III - Não se ausentar do terminal sem encerrar a sessão de uso do SIRC, garantindo assim a impossibilidade de acesso indevido por pessoas não autorizadas;

IV - Manter sigilo dos dados ou informações sigilosas obtidas por força de suas atribuições, abstendo-se de revelá-los ou divulgá-los, sob pena de incorrer nas sanções civis e penais decorrentes de eventual divulgação;

V - Realizar atividades de tratamento de dados observando a boa-fé e os princípios definidos na Lei nº 13.709, de 14 de Agosto de 2018, que dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet) e estar ciente das Sanções Administrativas previstas em seu Art. 52, § 3º;

VI - Estar ciente das restrições previstas no artigo 31, § 2º, da Lei Federal nº 12.527/2011 (Lei de Acesso à Informação) e do § 2º, do artigo 61 do Decreto nº 7.724/2012 (uso indevido da informação), no artigo 20 (divulgação autorizada ou necessária) da Lei nº 10.406/2002 (Código Civil) e nos artigos 138 a 145 (crimes contra a honra), 297, 299 e 304 (crimes de falsidade documental) do Decreto-Lei nº 2.848/1940 (Código Penal);

VII - Reconhecer que a utilização das informação do SIRC poderá ser monitorada;

VIII - Não utilizar e nem disponibilizar os dados para uso comercial; e

IX - Responder, em todas as instâncias devidas, pelas consequências decorrentes das ações ou omissões que possam pôr em risco ou comprometer a exclusividade de conhecimento de sua senha.

