

## TERMO DE USO

O presente Termo de Uso regula a utilização do aplicativo Celular Seguro, oferecido pelo Ministério da Justiça e Segurança Pública, localizado(a) na Esplanada dos Ministérios Bloco T - Bairro Zona Cívico Administrativa, Brasília/DF, CEP 70064-900.

O uso deste serviço está condicionado à **aceitação** destes Termos de Uso e ao Aviso de Privacidade. O usuário deverá ler estes Termos e Aviso de Privacidade, certificar-se de havê-los entendido, estar consciente de todas as condições estabelecidas e se comprometer a cumpri-los previamente ao primeiro acesso.

**Ao utilizar o serviço, o usuário manifesta estar ciente com relação ao conteúdo destes e estará legalmente vinculado a todas as condições, obrigações e responsabilidades aqui previstas.**

## DEFINIÇÕES DO TERMO DE USO

Para os fins deste instrumento, consideram-se:

- (i) **Aplicativo:** o aplicativo Celular Seguro, fornecido pelo Ministério da Justiça tanto em sua versão App quanto sua versão WEB;
- (ii) **Agente público:** Todo aquele que exerce, ainda que transitoriamente ou sem remuneração, por eleição, nomeação, designação, contratação ou qualquer outra forma de investidura ou vínculo, mandato, cargo, emprego ou função nos órgãos e entidades da Administração Pública, direta e indireta;
- (iii) **Agentes de Estado:** Inclui órgãos e entidades da Administração pública além dos seus agentes públicos;
- (iv) **Códigos maliciosos:** Qualquer programa de computador, ou parte de um programa, construído com a intenção de provocar danos, obter informações não autorizadas ou interromper o funcionamento de sistemas/serviços e/ou redes de computadores;
- (v) **Informação Restrita:** informação submetida à restrição de acesso público em razão de hipótese legal específica;
- (vi) **Sítios e aplicativos:** Sítios e aplicativos por meio dos quais o **Usuário** acessa os serviços e conteúdos disponibilizados;
- (vii) **Terceiro:** Pessoa ou entidade que não participa diretamente em um contrato, em um ato jurídico ou em um negócio, ou que, para além das partes envolvidas, pode ter interesse num processo jurídico;



- (viii) **Titular/usuário:** pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;
- (ix) **Internet:** Serviço constituído do conjunto de protocolos lógicos, estruturado em escala mundial para uso público e irrestrito, com a finalidade de possibilitar a comunicação de dados entre terminais por meio de diferentes redes;
- (x) **Usuário:** cidadão que aceita estes Termos de Uso e utiliza o aplicativo Celular Seguro;
- (xi) **Contatos/Pessoas de Confiança:** pessoa cadastrada pelo usuário como contato/pessoa de confiança que comunicar o furto, o roubo ou extravio do Dispositivo Móvel Cadastrado em nome do usuário que a cadastrou;
- (xii) **Telefone/Aparelho/Dispositivo Móvel Cadastrado:** aparelho dotado de tecnologias digitais, que permite a mobilidade, o acesso à Internet e a realização de ligações telefônicas, cujos dados sejam voluntariamente cadastrados pelo Usuário no Aplicativo ou plataforma web;
- (xiii) **Serviço Celular Seguro:** conjunto de ferramentas, incluído o Aplicativo e sua versão WEB, que permitem melhorar a segurança na utilização de Dispositivos Móveis Cadastrados, por meio de cadastro centralizado dos dispositivos, assim como inclusão de dados de contato de Pessoas de Confiança dos Usuários proprietários dos Dispositivos Móveis Cadastrados, de forma a garantir o acionamento imediato de medidas de segurança a partir da comunicação de eventos de furto, roubo ou extravio.
- (xiv) **Ocorrência/Evento/Incidente:** Evento de Roubo, furto ou extravio do Dispositivo Móvel cadastrado passível de acionamento de medidas de segurança ou alerta;

## ARCABOUÇO LEGAL

O arcabouço legal aplicável ao Serviço Celular Seguro compreende os seguintes atos legislativos e normativos:

[Lei nº 12.527, de 18 de novembro de 2011](#): Lei de Acesso à Informação (LAI), que regula o acesso a informações previsto na Constituição Federal;

[Lei nº 12.737, de 30 de novembro de 2012](#): Dispõe sobre a tipificação criminal de delitos informáticos;



[Lei nº 12.965, de 23 de abril de 2014](#): Marco Civil da Internet, que estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil;

[Lei nº 13.444, de 11 de maio de 2017](#): Dispõe sobre a Identificação Civil Nacional (ICN);

[Lei nº 13.460, de 26 de junho de 2017](#): que dispõe sobre participação, proteção e defesa dos direitos do usuário dos serviços públicos da administração pública.

[Lei nº 13.709, de 14 de agosto de 2018](#): Lei Geral de Proteção de Dados Pessoais (LGPD), que dispõe sobre a proteção de dados pessoais.

[Decreto nº 7.724, de 16 de maio de 2012](#): Regulamenta a Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação), que dispõe sobre o acesso a informações previsto na Constituição;

[Decreto nº 7.845, de 14 de novembro de 2012](#): Regulamenta procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo, e dispõe sobre o Núcleo de Segurança e Credenciamento;

[Decreto nº 8.777, de 11 de maio de 2016](#): Institui a Política de Dados Abertos do Poder Executivo federal;

[Decreto nº 9.637, de 26 de dezembro de 2018](#): Institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação, e altera o Decreto nº 2.295, de 4 de agosto de 1997, que regulamenta o disposto no art. 24, caput, inciso IX, da Lei nº 8.666, de 21 de junho de 1993, e dispõe sobre a dispensa de licitação nos casos que possam comprometer a segurança nacional;

[Decreto nº 10.046, de 09 de outubro de 2019](#): Dispõe sobre a governança no compartilhamento de dados no âmbito da administração pública federal e institui o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados; e

[Portaria MJSP nº 561, de 31 de dezembro de 2021](#): Institui a Política Geral de Proteção de Dados Pessoais no âmbito do Ministério da Justiça e Segurança Pública

[Portaria MJSP nº 260, de 28 de dezembro de 2022](#): aprova o Regimento Interno da Secretaria-Executiva.

## DESCRIÇÃO DO SERVIÇO

O Serviço Celular Seguro do Ministério da Justiça e Segurança Pública permite melhorar a segurança na utilização de dispositivos móveis por meio de cadastro centralizado dos Dispositivos Móveis Cadastrados, assim como dados de contato de Pessoas de Confiança dos proprietários dos Dispositivos Móveis Cadastrados, de forma a permitir o acionamento imediato de medidas de bloqueio dos Dispositivos Móveis Cadastrados a partir da comunicação de eventos de furto, roubo e perda.

Os interessados em utilizar a aplicação poderão fazer o *download* do Aplicativo nas lojas virtuais (App Store e Play Store) ou utilizar a plataforma web disponibilizada pelo Ministério da Justiça e Segurança Pública.

Serviços disponibilizados aos Usuários:

**Aplicativo para dispositivos móveis que estará disponível nas lojas virtuais da App Store (Apple) e da Play Store (Google).** Este Aplicativo proporcionará um processo de cadastro simplificado inicialmente, coletando informações como nome completo, número de telefone, número de série e marca/modelo do dispositivo.

Além disso, é implementado um Serviço de validação do cadastro, utilizando a plataforma **gov.br**, melhorando a precisão e segurança das informações registradas.

Inicialmente, o Aplicativo fará a integração com:

- (i) O Cadastro de Estações Móveis Impedidas, módulo Secretaria de Segurança Pública (CEMI SSP), mantido pela Associação Brasileira de Recursos em Telecomunicações (ABR Telecom), permitindo o compartilhamento de dados com operadoras de telefonia brasileiras participantes da solução para bloqueio do dispositivo, reduzindo potenciais danos fruto de roubos, furtos ou extravios de Dispositivos Móveis Cadastrados e subcontratados; e,
- (ii) instituições financeiras e instituições de pagamento, autorizadas pelo Banco Central do Brasil, aderentes ao Serviço Celular Seguro, permitindo o bloqueio de serviços financeiros ligados às suas instituições bancárias e financeiras dos Dispositivos Móveis Cadastrados roubados, furtados ou extravitados, cujo roubo, furto ou extravio tenha sido comunicado(a) por meio do Aplicativo ou plataforma web.

A critério do Ministério da Justiça e Segurança Pública, posteriormente poderão ocorrer integrações com outras empresas que possuem aplicações embarcadas em dispositivos móveis e que também têm preocupação com



possíveis fraudes e golpes em caso de ocorrências com os Dispositivos Móveis Cadastrados.

A comunicação via Aplicativo ou plataforma web não exige o Usuário de realizar as comunicações necessárias perante autoridades policiais, operadoras de telefonia e instituições financeiras e de pagamento .

## **DIREITOS DO USUÁRIO DO SERVIÇO**

De acordo com a Lei nº 13.460, de 26 de junho de 2017, são direitos básicos do Usuário:

- (i) Participação no acompanhamento da prestação e na avaliação dos serviços;
- (ii) Obtenção e utilização dos serviços com liberdade de escolha entre os meios oferecidos e sem discriminação;
- (iii) Acesso e obtenção de informações relativas à sua pessoa constantes de registros ou bancos de dados relacionados ao Aplicativo, observado o disposto no inciso X do caput do art. 5º da Constituição Federal e na Lei nº 12.527, de 18 de novembro de 2011;
- (iv) Proteção de suas informações pessoais, nos termos da Lei nº 12.527, de 18 de novembro de 2011, e da Lei nº 13.709, de 14 de agosto de 2018.

## **RESPONSABILIDADES DO USUÁRIO**

O Usuário se responsabiliza pela precisão e pela veracidade dos dados informados, bem como por mantê-los atualizados, e reconhece que a inconsistência deles poderá implicar a impossibilidade de se utilizar o Serviço Celular Seguro do Ministério da Justiça e Segurança Pública.

Durante a utilização do serviço, a fim de resguardar e de proteger os direitos de Terceiros e da Pessoa de Confiança, o Usuário se compromete a fornecer somente seus dados pessoais e os dados cadastrais da Pessoa de Confiança que tenha lhe autorizado a indicação.

O Usuário que vir a fornecer dados de Terceiros de maneira indevida será responsabilizado nos termos da lei pelos eventuais danos que causar. O Usuário responderá solidariamente caso o Ministério da Justiça e Segurança Pública, Instituições Financeiras participantes ou a ABR Telecom sofram qualquer tipo de dano em razão do fornecimento de dados de Terceiros e

da Pessoa de Confiança de maneira indevida, ou este, realize notificação não autorizado.

O login e senha só poderão ser utilizados pelo Usuário cadastrado, que se compromete a manter o sigilo da senha, que é pessoal e intransferível, não sendo possível, em qualquer hipótese, a alegação de uso indevido de sua conta após o ato de compartilhamento, negligência ou imperícia do **Usuário** em manter sua senha segura.

O Usuário do serviço é responsável pela atualização dos seus dados pessoais e da Pessoa de confiança, e pelas consequências em caso de omissão ou erros nos dados fornecidos.

O Usuário é responsável pela reparação de todos e quaisquer danos, diretos ou indiretos (inclusive decorrentes de violação de quaisquer direitos de outros usuários; de Terceiros, inclusive direitos de propriedade intelectual; de sigilo; e de personalidade), que sejam causados à Administração Pública, à ABR Telecom, as IF, e outros participantes, a qualquer outro Usuário, ou ainda a qualquer Terceiro, inclusive em decorrência do descumprimento do disposto nestes Termos de Uso ou de qualquer ato praticado a partir de seu acesso ao serviço.

O Ministério da Justiça e Segurança Pública não poderá ser responsabilizado pelos seguintes fatos:

- (i) Equipamento infectado (vírus, malwares e afins) ou invadido por atacantes (hackers) via Códigos maliciosos;
- (ii) Equipamento avariado no momento do uso de serviços;
- (iii) Monitoração clandestina do computador e do Dispositivo Móvel Cadastrado do Usuário; e
- (iv) Vulnerabilidades ou instabilidades existentes nos Serviços do Usuário;
- (v) Indisponibilidade do Sistema Celular Seguro em decorrência de problemas técnicos;

Em nenhuma hipótese, a Administração Pública Federal será responsável pela instalação, no equipamento do Usuário ou de Terceiros, de Códigos Maliciosos (vírus, *trojans*, *malware*, *worm*, *bot*, *backdoor*, *spyware*, *rootkit*, ou de quaisquer outros que venham a ser criados), em decorrência da navegação na Internet pelo Usuário.

O Aplicativo deverá ser baixado única e exclusivamente nas lojas App Store e Play Store oficiais. A Administração Pública não poderá ser responsabilizada por eventuais danos causados ao Usuário em caso de

instalação do aplicativo baixado de outra fonte, site ou link que não as lojas oficiais App Store e Play Store.

O usuário que tiver a emissão de alerta por meio do Serviço Celular Seguro fica ciente que para realizar o desbloqueio dos serviços deverá dirigir-se a sua prestadora de telefonia e as instituições financeiras para proceder com a solicitação de cancelamento dos bloqueios efetuados.”

## **RESPONSABILIDADE DA ADMINISTRAÇÃO PÚBLICA**

A Administração Pública se compromete a cumprir todas as legislações inerentes ao uso correto dos dados pessoais do Usuário e da Pessoa de Confiança de forma a preservar a privacidade dos dados utilizados no serviço, bem como a garantir todos os direitos e garantias legais. Também se obriga a promover, independentemente de requerimentos, a divulgação em local de fácil acesso, no âmbito de suas competências, de informações de interesse coletivo ou geral por eles produzidas ou custodiadas. É de responsabilidade da Administração Pública implementar controles de segurança para proteção dos dados pessoais dos Usuários.

A Administração Pública poderá, quanto às ordens judiciais de pedido das informações, compartilhar informações necessárias para investigações ou tomar medidas relacionadas a atividades ilegais, suspeitas de fraude ou ameaças potenciais contra pessoas, bens ou Serviços que sustentam o Serviço ou de outra forma necessárias para cumprir com obrigações legais. Caso ocorra, a Administração Pública notificará os Titulares dos dados, salvo quando o processo estiver em segredo de justiça.

## **AVISO DE PRIVACIDADE**

O Aviso de Privacidade informa ao Usuário a maneira como os seus dados pessoais são tratados no âmbito do fornecimento do Serviço do Aplicativo Celular Seguro.

Este Aviso de Privacidade acompanha o presente Termo de Uso, ressaltando-se que os dados pessoais mencionados serão tratados nos termos da legislação em vigor.

Para mais informações acesse nosso Aviso de Privacidade, anexo ao Termo de Uso.

Ao aceitar o presente Termo de Uso, o Usuário confirma ter ciência dos termos do Aviso de Privacidade do Serviço Celular Seguro.



## **MUDANÇAS NO TERMO DE USO**

A presente versão 1.1 deste Termo de Uso foi atualizada pela última vez em: 06/12/2023.

O Ministério da Justiça e Segurança Pública se reserva o direito de modificar ou descontinuar o Aplicativo e a plataforma web a qualquer momento, especialmente para adaptá-las às evoluções do Serviço Celular Seguro do Ministério da Justiça e Segurança Pública, seja pela disponibilização de novas funcionalidades, seja pela supressão ou modificação daquelas já existentes.

Qualquer alteração e/ou atualização do Termos de Uso e do Aviso de Privacidade passará a vigorar a partir da data de sua publicação no Aplicativo e na plataforma web, e deverá ser integralmente observada pelos Usuários.

## **INFORMAÇÕES PARA CONTATO**

Em caso de dúvidas relacionadas ao Serviço Celular Seguro do Ministério da Justiça e Segurança Pública, entre em contato através do Serviço de Informação ao Cidadão (SIC) e Ouvidoria-Geral (<https://falabr.cgu.gov.br/>).

## **FORO**

Este Termo será regido pela legislação brasileira. Qualquer reclamação ou controvérsia com base neste Termo será dirimida exclusivamente pela circunscrição de Brasília-DF.

Sem prejuízo de qualquer outra via administrativa ou judicial disponível, todos os titulares de dados pessoais têm direito a apresentar reclamação à Autoridade Nacional de Proteção de Dados (ANPD).



## AVISO DE PRIVACIDADE

### DEFINIÇÕES

Para melhor compreensão deste documento, neste Aviso de Privacidade são observados os conceitos da LGPD e consideram-se:

- (i) **Agentes de tratamento:** O controlador e o operador;
- (ii) **Anonimização:** Utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo;
- (iii) **Autoridade Nacional de Proteção de Dados:** Órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento da Lei 13.709/2018 em todo o território nacional;
- (iv) **Banco de Dados:** Conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico;
- (v) **Consentimento:** Manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;
- (vi) **Controlador:** Pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;
- (vii) **Dado Anonimizado:** Dado relativo a um titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;
- (viii) **Dado Pessoal:** Informação relacionada a uma pessoa natural identificada ou identificável;
- (ix) **Dado Pessoal Sensível:** Dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;
- (x) **Encarregado:** Pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD);
- (xi) **Operador:** Pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.

- (xii) **Órgão de Pesquisa:** Órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos, legalmente constituída sob as leis brasileiras e com sede e foro no País, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico;
- (xiii) **Titular:** Pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;
- (xiv) **Transferência Internacional de Dados:** Transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro;
- (xv) **Tratamento:** Toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração; e
- (xvi) **Uso Compartilhado de Dados:** Comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados.

## **BASE LEGAL PARA TRATAMENTO DE DADOS PESSOAIS**

Este Aviso de Privacidade foi elaborado em conformidade com a [Lei Federal nº 12.965 de 23 de abril de 2014](#) (Marco Civil da Internet) e com a [Lei Federal nº 13.709, de 14 de agosto de 2018](#) (Lei Geral de Proteção de Dados Pessoais - LGPD).

O Controlador se compromete a cumprir as normas previstas na LGPD e a respeitar os princípios dispostos no Art. 6º de tal norma:

- (i) **Finalidade:** realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
- (ii) **Adequação:** compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;



- (iii) **Necessidade:** limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;
- (iv) **Livre acesso:** garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;
- (v) **Qualidade dos dados:** garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;
- (vi) **Transparência:** garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;
- (vii) **Segurança:** utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;
- (viii) **Prevenção:** adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
- (ix) **Não discriminação:** impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;
- (x) **Responsabilização e prestação de contas:** demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

## QUAIS DADOS SÃO TRATADOS

Para o cumprimento dos objetivos do Serviço Celular Seguro, são necessários coletar os dados pessoais listados abaixo:

Do Usuário:

- Marca do Celular;
- Modelo do Celular;
- Número de Série do Celular;
- Operadora;

Telefone;  
IMEI;  
UF;  
Município;  
CPF;  
E-mail;  
Nome; e  
**Geolocalização\*.**

Da Pessoa de Confiança:

CPF;  
Telefone;  
E-mail; e  
Nome.

Caso novos dados pessoais passem a ser coletados, este Aviso de Privacidade será necessariamente alterado.

**\*Dado tratado apenas pelo login único GOV.BR, não pelo aplicativo Celular Seguro.**

### **COMO OS DADOS SÃO COLETADOS**

Os interessados em se tornar Usuários do Serviço **Celular Seguro** do Ministério da Justiça e Segurança Pública se cadastram utilizando o login único disponibilizado pelo aplicativo **Gov.br**, optando em utilizar o Aplicativo do Serviço ou por meio da plataforma web (**celularseguro.mj.gov.br**). O Usuário pode cadastrar previamente os dados de seu Dispositivo Móvel Cadastrado e posteriormente providenciar o acionamento do alerta.

### **QUAL O TRATAMENTO REALIZADO E PARA QUAL FINALIDADE**

Os Dados Pessoais coletados são armazenados e tratados pelo Ministério da Justiça e Segurança Pública, que atua como Controlador de Dados para as seguintes finalidades:

Para fornecimento de dados obrigatórios a serem entregues à ABR TELECOM, à ANATEL e às instituições financeiras e de pagamento aderentes ao Serviço Celular Seguro, com objetivo de bloquear os



Dispositivos Móveis Cadastrados pelas prestadoras participantes da solução Cadastro de Estações Móveis Impedidas, módulo Secretaria de Segurança Pública (CEMI SSP) e os aplicativos fornecidos por instituições financeiras e de pagamento aderentes ao Serviço Celular Seguro, que estejam instalados em tais Dispositivos Móveis Cadastrados objeto de extravio, roubo ou furto;

Para gestão do consentimento conferido pelos Usuários para tratamento dos Dados Pessoais e compartilhamento com os participantes do Serviço Celular Seguro, incluídas as instituições financeiras e de pagamento aderentes ao Serviço Celular Seguro.

## SEGURANÇA DOS DADOS

O Serviço **Celular Seguro** do Ministério da Justiça e Segurança Pública se compromete a aplicar as medidas técnicas e organizativas aptas a proteger os dados pessoais de acessos não autorizados e de situações de destruição, perda, alteração, comunicação ou difusão de tais dados.

Para a garantia da segurança, serão adotadas soluções que levem em consideração: as técnicas adequadas; os custos de aplicação; a natureza, o âmbito, o contexto e as finalidades do tratamento; e os riscos para os direitos e liberdades do usuário.

O serviço utiliza criptografia para que os dados sejam transmitidos de forma segura e confidencial, de maneira que a transmissão dos dados entre o servidor e o usuário, e em retroalimentação, ocorra de maneira totalmente cifrada ou encriptada.

No entanto, o serviço se exime de responsabilidade por culpa exclusiva de terceiros, como em caso de ataque de *hackers* ou *crackers*, ou culpa exclusiva do Usuário, como no caso em que ele mesmo transfere seus dados a terceiro. O Serviço Celular Seguro do Ministério da Justiça e Segurança Pública se compromete, ainda, a comunicar o Usuário em prazo adequado caso ocorra algum tipo de violação da segurança de seus dados pessoais que possa lhe causar um alto risco para seus direitos e liberdades pessoais, nos termos da LGPD.

## COMPARTILHAMENTO DE DADOS

O Ministério da Justiça e Segurança Pública poderá compartilhar suas informações pessoais com terceiros que sejam relevantes no âmbito do aplicativo Celular Seguro em base de dados única para fornecimento de dados obrigatórios a serem entregues à ABR TELECOM, à ANATEL e às

instituições financeiras e de pagamento aderentes ao Serviço Celular Seguro, subcontratados, ou ainda para cumprir requisitos legais. O compartilhamento de dados pessoais com a ABR TELECOM e respectivas prestadoras participantes da solução Cadastro de Estações Móveis Impedidas, módulo Secretaria de Segurança Pública (CEMI SSP), a ANATEL e às instituições financeiras e de pagamento aderentes ao Serviço Celular Seguro é realizado única e exclusivamente com a finalidade de prestação do serviço oferecido pelo aplicativo Celular Seguro.

O Compartilhamento de dados com a prestadoras de serviço de tecnologia da informação contratadas pelo Ministério da Justiça e Segurança Pública é estritamente necessário para desempenhar as atividades de prestação de serviço de forma adequada e eficiente. O acesso a base é garantido apenas a dados que sejam relevantes e essenciais para o cumprimento das responsabilidades atribuídas às prestadoras, que incluem, por exemplo, desenvolvimento, manutenção e atualização de softwares e geração de relatórios para elaboração de métricas. O Ministério da Justiça e Segurança Pública é controlador dos dados e as prestadoras desempenham o papel de operador, comprometendo-se a garantir sua confidencialidade, integridade e disponibilidade conforme previsto em contrato. Para isso, a equipe passa por treinamentos e atualizações sobre LGPD e segurança da informação.

O Compartilhamento de dados com as instituições financeiras e de pagamento aderentes ao Serviço Celular Seguro será realizado para fins de atendimento do bloqueio dos aplicativos de tais instituições financeiras e de pagamento eventualmente instalados no Dispositivo Móvel Cadastrado roubado, furtado ou extraviado.

## **TRANSFERÊNCIA INTERNACIONAL DE DADOS**

O Serviço Celular Seguro do Ministério da Justiça e Segurança Pública não realiza transferência internacional de dados.

## **COOKIES**

Cookies são pequenos arquivos salvos no computador ou celular do Usuário para ajudar a armazenar as preferências e outras informações usadas nas páginas da Web que ele visita.

As informações eventualmente armazenadas em cookies também são consideradas dados pessoais. Todas as regras previstas neste Aviso de Privacidade também são aplicáveis aos referidos cookies.

O Serviço Celular Seguro, em sua versão web, do Ministério da Justiça e Segurança Pública utiliza os seguintes cookies:



- LastMRH\_Session: Registrar o idioma em que o site deve ser exibido; e
- F5\_ST: O cookie F5\_ST é usado exclusivamente para manter o cliente informado sobre o tempo limite de sessão e tempo limite de inatividade através do uso de JavaScript específico baseado em navegador BIG-IP APM;
- TS?...: Mantém informações de política de segurança para garantir a validação da requisição e sessão do usuário. O Serviço BIG-IP ASM valida esses cookies retornando dos clientes para garantir que os cookies não sejam modificados.

## **TRATAMENTO POSTERIOR DOS DADOS PARA OUTRAS FINALIDADES**

Caso o titular de dados pessoais opte por excluir os seus dados, eles serão anonimizados. Os dados anonimizados poderão ser utilizados futuramente para geração de estatísticas, de forma a melhorar os procedimentos do Serviço Celular Seguro do Ministério da Justiça e Segurança Pública. Também podem ser utilizados para fins de pesquisa por órgãos especializados no assunto. Podem, igualmente, ser utilizados de maneira agregada para divulgação de informações através de meios de comunicação, e em publicações científicas e educacionais.

## **DIREITOS DO TITULAR DE DADOS PESSOAIS**

O titular de dados pessoais possui os seguintes direitos, conferidos pela Lei Geral de Proteção de Dados Pessoais (LGPD):

- (i) Direito de confirmação e acesso (Art. 18, incisos I e II): é o direito do titular de dados de obter do serviço a confirmação de que os dados pessoais que lhe digam respeito são ou não objeto de tratamento e, se for esse o caso, o direito de acessar os seus dados pessoais.
- (ii) Direito de retificação (Art. 18, inciso III): é o direito de solicitar a correção de dados incompletos, inexatos ou desatualizados.
- (iii) Direito à limitação do tratamento dos dados (Art. 18, inciso IV): é o direito do titular de dados de limitar o tratamento de seus dados pessoais, podendo exigir a eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto na Lei Geral de Proteção de Dados Pessoais.
- (iv) Direito de oposição (Art. 18, § 2º): é o direito do titular de dados de, a qualquer momento, opor-se ao tratamento de dados por motivos relacionados com a sua situação particular, com fundamento em uma das hipóteses de dispensa de consentimento ou em caso de

descumprimento ao disposto na Lei Geral de Proteção de Dados Pessoais.

- (v) Direito de portabilidade dos dados (Art. 18, inciso V): é o direito do titular de dados de realizar a portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial.
- (vi) Direito de não ser submetido a decisões automatizadas (Art. 20): o titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade.

## **RESPONSABILIDADE**

O Ministério da Justiça e Segurança Pública (MJSP) prevê a responsabilidade dos agentes que atuam nos processos de tratamento de dados, em conformidade com os artigos 42 a 45 da Lei Geral de Proteção de Dados.

O Ministério da Justiça e Segurança Pública (MJSP) se compromete em manter este Aviso de Privacidade atualizado, observando suas disposições e zelando por seu cumprimento.

Além disso, também assume o compromisso de buscar condições técnicas e organizativas seguramente aptas a proteger todo o processo de tratamento de dados.

## **MUDANÇAS NO AVISO DE PRIVACIDADE**

A presente versão 1.0 deste Aviso de Privacidade foi atualizada pela última vez em: 30/11/2023.

O Ministério da Justiça e Segurança Pública, na qualidade de Controlador, se reserva o direito de modificar, a qualquer momento, no Aplicativo e na plataforma web, as presentes normas, especialmente para adaptá-las às evoluções do Serviço Celular Seguro do Ministério da Justiça e Segurança Pública, seja pela disponibilização de novas funcionalidades, seja pela supressão ou modificação daquelas já existentes.

Este Aviso de Privacidade poderá ser atualizado em decorrência de eventual atualização normativa. Qualquer modificação neste Aviso de Privacidade será comunicada ao Usuário.



## **CONTROLADOR**

A Lei Geral de Proteção de Dados Pessoais define como controlador, em seu Art. 5º, inciso VI, a pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.

Para o Serviço **Celular Seguro**, o Ministério da Justiça e Segurança Pública será o Controlador dos dados pessoais que compartilhar, no que couber.

Endereço: Esplanada dos Ministérios - Bloco T - Térreo - Ouvidoria-Geral - CEP 70.064-900 – Brasília – DF.

E-mail: [encarregadolgpd@mj.gov.br](mailto:encarregadolgpd@mj.gov.br).

## **ENCARREGADO**

A Lei Geral de Proteção de Dados Pessoais define como encarregado, em seu Art. 5º, inciso VIII, a pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).

O usuário poderá entrar em contato por meio do e-mail [encarregadolgpd@mj.gov.br](mailto:encarregadolgpd@mj.gov.br), para sanar quaisquer dúvidas sobre este Aviso de Privacidade ou para obter mais informações sobre o tratamento dos dados realizado pelo Aplicativo Celular Seguro.

## PARTICIPANTES DO SERVIÇO CELULAR SEGURO

O Serviço Celular Seguro, do Ministério da Justiça e Segurança Pública, conta com a parceria das seguintes empresas/instituições que desempenharão os seguintes papéis:

Empresa/Instituição	Data de Início da parceria	Descrição das ações a serem tomadas
Ministério da Justiça e Segurança Pública	19/12/2023	Coleta de informações pertinentes ao aplicativo e comunicação aos participantes quando solicitado pelo usuário.
ANATEL	18/12/2023	Coordenação das operadoras de telefonia e ABR
FEBRABAN	18/12/2023	Coordenação das Instituições Financeiras
ABR TELECOM	18/12/2023	<ul style="list-style-type: none"><li>• <b>Recebimento e validações das informações de pedido de bloqueio de terminais telefônicos móveis para envio às prestadoras participantes (Algar Telecom, Claro, Sercomtel, Telefônica, Tim, Datora Telecom, Emnify Brasil e Surf Telecom) do serviço CEMI-Segurança Pública.</b></li><li>• Os prazos para validação sistêmica da ABR Telecom são contabilizados conforme manual operacional do CEMI, listado abaixo:</li><li>• <b>Validação Sistêmica:</b> Até 6 horas para encaminhamento do IMEI às Prestadoras MNOs visando o respectivo bloqueio nos seus EIRs;</li><li>• <b>Validação Prestadoras:</b> Até 1 dia útil a partir do encaminhamento para validação de Cadastro e/ou IMEI via CEMI SSP.</li></ul>
Banco Pan	19/12/2023	<ul style="list-style-type: none"><li>• O cliente passará pelo processo de validação de vida (liveness) para redefinir o acesso ao aplicativo.</li></ul>
Banco Inter	19/12/2023	<ul style="list-style-type: none"><li>• O cliente passará pelo processo de validação de vida (liveness) para redefinir a senha. Preventivamente, os serviços nas carteiras digitais (Google Pay e Apple Pay) também serão bloqueados.</li></ul>



		<ul style="list-style-type: none"> <li>O tempo máximo para suspensão temporária dos serviços Bancários realizados remotamente, será concluída no prazo de até 30 (trinta) minutos após a comunicação.</li> </ul>
Sicoob	19/12/2023	<ul style="list-style-type: none"> <li>Bloqueio do dispositivo no Sicoob para realizar transações no Sicoob em até 10 minutos.</li> </ul>
CAIXA	19/12/2023	<ul style="list-style-type: none"> <li>Suspensão temporária dos serviços Bancários executados de forma remota em até 30 minutos</li> </ul>
BANCO BTG PACTUAL	19/12/2023	<ul style="list-style-type: none"> <li>O cliente passará pelo processo de validação de vida (liveness) para redefinir a senha. Preventivamente, os serviços nas carteiras digitais (Google Pay e Apple Pay) também serão bloqueados em até 10 minutos após a comunicação da ocorrência.</li> </ul>
XP Investimentos	19/12/2023	<ul style="list-style-type: none"> <li>Bloqueio imediato de contas e cartões em todas as marcas do grupo XPInc, seguido do envio da comunicação para o cliente por e-mail sobre os bloqueios realizados e que a origem foi devida ação realizada no APP Celular Seguro - MJSP;</li> </ul>
Santander	19/12/2023	<ul style="list-style-type: none"> <li>Bloqueio imediato de acesso ao app do banco</li> </ul>
Banco Safra	19/12/2023	<ul style="list-style-type: none"> <li>Suspensão temporária aos acessos dos canais digitais, no prazo de até 10 minutos, após a comunicação.</li> </ul>
Banco do Brasil S.A	19/12/2023	<ul style="list-style-type: none"> <li>Bloqueio do canal Mobile em até 30 minutos após o recebimento da informação. Para realizar o desbloqueio será necessário o cliente entrar em contato com BB.</li> </ul>
Itaú-Unibanco	19/12/2023	<ul style="list-style-type: none"> <li>Bloqueio de acesso ao APP e bloqueio da carteira digital – em até 10 minutos</li> </ul>
Banco Cooperativo Sicredi S.A	19/12/2023	<ul style="list-style-type: none"> <li>Suspensão temporária dos serviços Bancários realizados remotamente, concluída no prazo de 30 minutos após a comunicação.</li> </ul>
Bradesco	19/12/2023	<ul style="list-style-type: none"> <li>Suspensão temporária dos serviços bancários realizados remotamente, concluída no prazo de 30 minutos após a comunicação</li> </ul>