E-BOOK

guia de segurança

Lembrete

Segurança em primeiro lugar, a Xiaomi cuida de você

Tecnologia de qualidade
acessível para todos.

SEU CELULAR É SUA CARTEIRA: CUIDE DA SUA VIDA DIGITAL

Toda a praticidade que o celular traz pode rapidamente se tornar um pesadelo se ele cair nas mãos erradas. Veja aqui como se preparar antecipadamente para reduzir os danos e o que fazer se um furto ocorrer.

Tecnologia de qualidade
acessível para todos.

ÍNDICE

SEU CELULAR É A SUA CARTEIRA

Tecnologia de qualidade
acessível para todos.

COMO SE PREVENIR E REDUZIR PREJUÍZOS

Tecnologia de qualidade
acessível para todos.

1. BLOQUEIE SEMPRE A TELA DO CELULAR COM UMA SENHA FORTE

Se o ladrão pegar o celular desbloqueado ou se a senha de desbloqueio for fácil de adivinhar, ele consegue acessar aplicativos instalados, fazer buscas por senhas, alterar configurações e ler mensagens. Para evitar isso, siga estas dicas de segurança:

•Configure um método de autenticação para a tela inicial
•Defina uma senha longa, se possível alfanumérica.
•Se usar padrão de desbloqueio, utilize o maior número de pontos possíveis e evite desenhos simples, como letras.
•Ative o bloqueio de tela automático com o menor tempo disponível.

2. HABILITE A FUNÇÃO PIX SEGURO

Mesmo que seu smartphone possua uma senha de desbloqueio, é importante considerar situações em que você pode perder o dispositivo ou ser vítima de furto ou roubo. Nesses casos, a Xiaomi oferece dois recursos incríveis para aprimorar sua segurança: o ”Bloqueio de aplicativos" e o ”Ocultar aplicativos".
O bloqueio de aplicativos e o ocultamento de aplicativos são recursos disponíveis em dispositivos Xiaomi que proporcionam diversas vantagens em termos de segurança e privacidade.
O bloqueio de aplicativos permite adicionar uma camada adicional de proteção para aplicativos específicos, exigindo uma senha, impressão digital ou outro método de autenticação para acessá-los. Esse recurso é especialmente útil para aplicativos que contêm informações sensíveis, como aplicativos bancários, e-mails ou redes sociais. Com essa funcionalidade, é possível impedir que outras pessoas acessem esses aplicativos sem sua permissão, mesmo se o dispositivo estiver desbloqueado.
Já o ocultamento de aplicativos permite esconder determinados aplicativos da tela inicial e do menu de aplicativos visíveis. Além disso, você pode desativar as notificações dos aplicativos ocultos. Esses aplicativos ocultos geralmente requerem um gesto e uma senha específica para serem acessados. Essa opção é útil para preservar a privacidade de determinados aplicativos, evitando que outras pessoas tenham conhecimento ou acessem facilmente esses aplicativos em seu dispositivo.
Esses recursos adicionais fornecidos pela Xiaomi oferecem uma camada extra de segurança e privacidade aos usuários, permitindo um melhor controle de acesso aos aplicativos e a manutenção da proteção de suas informações pessoais.

Abaixo, segue o passo a passo:

Bloqueio de Aplicativos:

- Abra o aplicativo ”Segurança" no seu dispositivo Xiaomi.
- Role para baixo, e selecione o recurso ”Bloqueio de apps".
- Você será solicitado a definir um padrão de desbloqueio, senha ou usar a impressão digital, caso ainda não tenha configurado.
- Após configurar o método de desbloqueio, você verá uma lista de todos os aplicativos instalados no seu dispositivo.
- Selecione os aplicativos que deseja bloquear e ative o recurso de bloqueio.
- Agora, sempre que você ou alguém tentar abrir um aplicativo bloqueado, será solicitada a autenticação usando o método escolhido.

Ocultar Aplicativos:

- Abra o aplicativo ”Segurança" no seu dispositivo Xiaomi.
- Role para baixo, e selecione o recurso ”Bloqueio de apps".
- Nessa tela, você verá a lista de todos os aplicativos instalados no seu dispositivo.
- Selecione os aplicativos que deseja ocultar e eles serão removidos da tela inicial e do menu de aplicativos visíveis.
- Além disso, você pode ativar a opção "Ocultar notificações" para que as notificações desses aplicativos também sejam ocultadas.
- Para acessar os aplicativos ocultos posteriormente, geralmente é necessário fazer um gesto de pinça na tela.

Lembrando que os passos podem variar um pouco dependendo da versão do sistema operacional MIUI em seu dispositivo Xiaomi. Certifique-se de estar utilizando a versão mais recente e, se necessário, consulte o manual do usuário do seu dispositivo para obter instruções mais detalhadas.

1- Clique no app de segurança

2- Role a tela até o fim

3- Clique no recurso para ativar

3. PROTEJA O CHIP SIM COM UMA SENHA

Um chip SIM protegido por senha é uma medida eficaz para impedir que um ladrão ative o chip em outro aparelho. Isso ajuda a evitar que o ladrão receba mensagens SMS contendo códigos de verificação, que são frequentemente usados para acessar suas contas ou redefinir suas senhas.
Para ativar o bloqueio do chip SIM e alterar o código PIN padrão, siga estes passos:

1.Acesse as configurações do seu Xiaomi.
2.Procure a opção "Senhas e segurança" ou algo semelhante.
3.Em seguida, clique em "Privacidade" e procure pela opção referente à sua operadora de telefonia (por exemplo, "Vivo", "Claro", "Tim", etc.).
4.Dentro das configurações da sua operadora, você encontrará a opção para ativar o bloqueio do chip SIM.
5.Certifique-se de ativar essa opção para proteger o chip com uma senha.
6.Verifique com sua operadora qual é o código PIN padrão do chip SIM, pois pode variar de acordo com a operadora.
7.É altamente recomendável alterar o código PIN padrão para uma senha personalizada. Para fazer isso, siga as instruções fornecidas pela sua operadora.

Lembre-se de entrar em contato com a sua operadora de telefonia para obter informações específicas sobre como ativar o bloqueio do chip SIM e alterar o código PIN. Eles poderão fornecer as orientações adequadas e esclarecer qualquer dúvida sobre o processo.
Mantenha seu chip SIM protegido por senha e atualize-a regularmente para garantir uma camada adicional de segurança para o seu dispositivo móvel.

4. ANOTE O IMEI DO APARELHO CELULAR

Para solicitar o bloqueio do seu aparelho junto à operadora e registrar um boletim de ocorrência, é essencial fornecer o IMEI (International Mobile Equipment Identity), que é o código identificador exclusivo do dispositivo. Essa informação é fundamental para tomar as medidas necessárias e garantir a segurança do seu aparelho. Não se esqueça de ter o IMEI em mãos ao realizar essas solicitações.
O IMEI é um número único atribuído a cada aparelho móvel e pode ser encontrado de diversas maneiras:

1. Na nota fiscal
2. Na caixa do equipamento
3. Nas configurações do sistema. Para acessar as configurações do sistema e localizar rapidamente a opção do IMEI, siga estas etapas simples:

- Abra as configurações do seu dispositivo.
- Na parte superior da tela de configurações, você verá uma barra de pesquisa.
- Digite a palavra "IMEI" na barra de pesquisa e pressione enter ou toque no ícone de pesquisa.
- Em seguida, a opção relacionada ao IMEI será exibida nos resultados da pesquisa.
- Toque na opção do IMEI para visualizar ou copiar o código identificador do seu aparelho.
- Dessa forma, você poderá encontrar facilmente a opção do IMEI dentro das configurações do sistema e acessar as informações necessárias do seu dispositivo digitando *#06# diretamente no aparelho.

Imagem ilustrativa da caixa
do seu Xiaomi

Guarde a caixa do seu aparelho, pois assim você terá acesso rápido às informações importantes. A Caixa contém dados relevantes, como o número de série, o modelo do aparelho e o IMEI impresso. Essas informações podem ser úteis em casos de perda, roubo ou necessidade de suporte técnico. Manter a caixa do seu aparelho guardada em um local seguro é uma prática recomendada, pois além de facilitar o acesso às informações cruciais, também pode ajudar na revenda do dispositivo no futuro, já que ter a caixa original é um diferencial para muitos compradores. Portanto, lembre-se de guardar a caixa do seu aparelho em um local de fácil acesso e mantenha-a organizada junto com outros documentos importantes. Dessa forma, você estará preparado para qualquer eventualidade e terá todas as informações necessárias à mão quando precisar delas.

5. USE SENHAS FORTES PARA EVITAR FRAUDES

Sequências conhecidas ou baseadas em informações pessoais, como datas, são fáceis de adivinhar. Reutilizar senhas também facilita a vida do ladrão, pois dá acesso a todas as contas onde a mesma senha é usada.

- Não use informações pessoais ou sequências conhecidas.
- Não repita senhas.
- Ao criar uma senha, é importante considerar alguns aspectos para garantir sua segurança. Siga essas dicas para criar uma senha forte, clara, curta e que atenda aos requisitos de letras maiúsculas, minúsculas e caracteres especiais:

- Escolha uma frase curta e significativa para você.
- Selecione a primeira letra de cada palavra na frase e utilize letras maiúsculas e minúsculas de forma alternada.
- Inclua um ou mais caracteres especiais, como !, @, #, $, %, etc. Pode ser colocado no início, meio ou final da senha.
- Considere substituir algumas letras por números ou caracteres similares. Por exemplo, "S" pode ser substituído por "5" ou "a" por "@", mas evite padrões previsíveis.
- Certifique-se de que a senha tenha pelo menos 8 caracteres.
- Evite usar informações pessoais óbvias, como seu nome, data de nascimento ou palavras comuns.
- Evite sequências simples, como "123456" ou "abcdef".
- Evite repetir a mesma senha em diferentes contas.
- Aqui está um exemplo de senha que segue essas diretrizes:
- Frase: "Eu amo viajar!" Senha: “E@v1A#!”.
- Lembre-se de que é essencial criar uma senha forte e única para cada conta que você utiliza, e também de atualizá-las periodicamente para manter sua segurança online.

6. GUARDE SUAS SENHAS DE FORMA SEGURA

Senhas guardadas no celular podem ser encontradas pelos ladrões usando mecanismos de buscas. Não guarde senhas, especialmente de instituições financeiras, em aplicativos de e-mail, anotações, mensagens, contatos e fotos. Existem várias opções seguras para armazenar suas senhas e evitar esquecimentos. Aqui estão algumas sugestões:

- Bloco de notas criptografado: Você pode usar um bloco de notas criptografado em seu computador ou dispositivo móvel para armazenar suas senhas.
- Planilha protegida por senha: Utilize uma planilha eletrônica, como o Microsoft Excel ou o Google Sheets, para criar uma lista de senhas. Proteja a planilha com uma senha forte e salve-a em um local seguro.
- Armazenamento offline: Se preferir um método não digital, você pode escrever suas senhas em um caderno ou em cartões individuais e guardá-los em um local seguro, como uma gaveta trancada.

7. REDUZA OS LIMITES DE TRANSAÇÕES PARA MINIMIZAR PREJUÍZOS

Para evitar fraudes por meio de transferências bancárias, é importante adotar algumas medidas de segurança. Aqui estão algumas recomendações:

- Reduza os limites de transferências entre contas, DOC, PIX e TED: Verifique os limites de transferência estabelecidos em sua conta bancária e avalie a possibilidade de reduzi-los. Isso pode dificultar a ação de possíveis fraudadores, limitando o valor que eles podem transferir sem a sua autorização.
- Reavalie limites de créditos pré-aprovados: Caso possua créditos pré-aprovados, como empréstimos ou cartões de crédito com limites altos, avalie se é realmente necessário mantê-los no valor atual. Reduzir esses limites pode diminuir os riscos de possíveis fraudes.

Ao realizar essas ações, é importante encontrar um equilíbrio entre a segurança e a conveniência para suas necessidades financeiras. Portanto, converse com seu banco ou instituição financeira para obter informações mais detalhadas sobre como ajustar esses limites e quais opções estão disponíveis para garantir a segurança das suas transações bancárias.

8. PREPARE-SE PARA APAGAR O APARELHO REMOTAMENTE

Apagar o conteúdo do aparelho remotamente é uma tarefa fácil e simples, proporcionando segurança e tranquilidade. Com apenas alguns cliques, você pode garantir a proteção dos seus dados pessoais e evitar o acesso não autorizado. Através de um processo rápido e eficiente, todo o conteúdo do dispositivo será completamente apagado, sem deixar vestígios. Mantenha-se no controle total da sua privacidade com essa poderosa função de apagamento remoto.

- Ative a localização remota do aparelho.
- A fim de apagar um Xiaomi, é necessário acessar o site i.mi.com e realizar o login utilizando o seu email e senha da **conta Mi**. Após ter entrado na sua conta, você terá acesso às seguintes opções:

- Tocar som: Essa opção permite que você faça o seu dispositivo tocar um som, o que é útil caso você o tenha perdido em casa, na bolsa, ou em algum lugar próximo. O som pode ajudar a localizá-lo mais facilmente.
- Modo perdido: Se você acredita que ainda há uma chance de encontrar o dispositivo, mas não tem certeza de onde ele está, pode ativar o Modo Perdido. Esse modo bloqueará o dispositivo temporariamente, para evitar que outras pessoas tenham acesso a ele enquanto você tenta localizá-lo. Você também pode exibir uma mensagem na tela bloqueada com informações de contato para que alguém possa entrar em contato com você caso encontre o dispositivo.
- Apagar dados: Caso você tenha certeza de que o dispositivo foi perdido, furtado ou roubado, a opção de apagar dados permite que você remova todos os dados pessoais do dispositivo remotamente. Isso é útil para proteger suas informações pessoais e impedir o acesso não autorizado aos seus dados.

- Se você não souber o seu email, ID da conta ou mesmo o celular cadastrado na conta Mi, existe outro recurso que você pode utilizar para apagar seu smartphone Xiaomi. Basta digitar no Google "Encontre Meu Dispositivo" e acessar por meio da sua conta do Google (Gmail), que é a mesma que você usa no seu dispositivo. Através desse recurso, você poderá **localizar**, **bloquear** ou **apagar** os dados do seu smartphone Xiaomi.

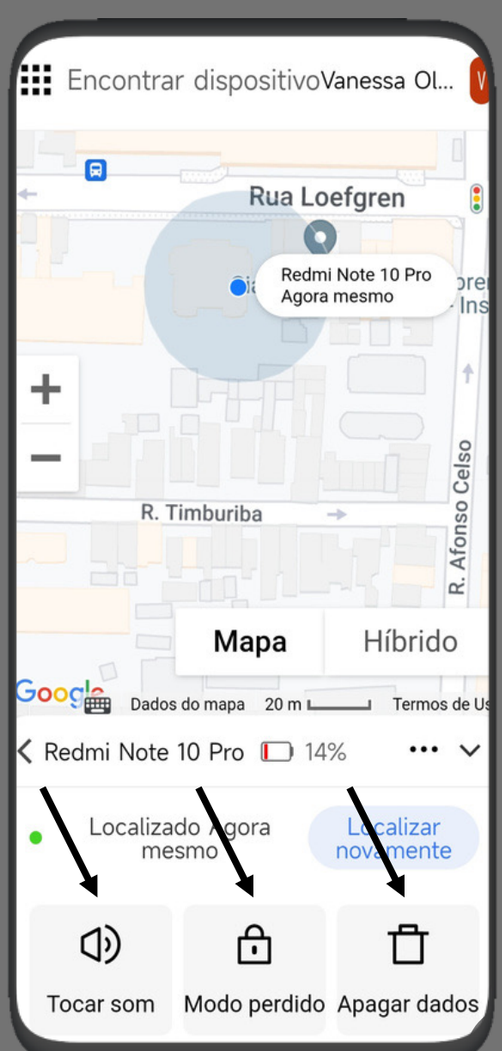
Lembre-se de que os procedimentos podem variar ligeiramente dependendo do modelo específico do Xiaomi ou de atualizações de software. Sempre verifique as instruções fornecidas pela Xiaomi ou pelo Google para obter orientações precisas sobre como apagar um dispositivo Xiaomi.

- Passo a passo de como acessar a sua conta Mi:

1)

2)

3)



9. PLANEJE-SE PARA RECUPERAR SUAS CONTAS E DADOS DEPOIS

Para recuperar suas contas e dados em outro aparelho, algumas ações e configurações devem ser feitas antes que o furto ocorra.

- Defina um número de celular alternativo para recuperação de contas.
- Gere e tenha em facil acesso codigos de backup para contas que usem verificaçao em duas etapas.
- Faça backups diariamente.

Lembre-se códigos de backup são gerados pela função de verificação em duas etapas para serem usados quando outros métodos de autenticação não estiverem disponíveis.

10. PROTEJA SEUS DADOS PARA NÃO SEREM USADOS EM FRAUDES

Proteger os dados armazenados é fundamental, pois informações desprotegidas podem ser facilmente acessadas por criminosos e usadas para fins fraudulentos.

- Evite armazenar fotos de documentos, cartões, senhas e até mesmo blocos de notas com seus dados e senhas pessoais. É importante tomar precauções para garantir a segurança dos seus dados e evitar o acesso não autorizado a informações sensíveis.

Lembre-se sempre de estar atento aos sinais de atividades suspeitas, como transações não autorizadas ou comunicações estranhas. Caso suspeite de qualquer atividade maliciosa, entre em contato com as autoridades e com os fornecedores de serviços relevantes para tomar as medidas necessárias.

II. O QUE FAZER CASO OCORRA O FURTO OU PERDA

Tecnologia de qualidade
acessível para todos.

1. NOTIFIQUE AS INSTITUIÇÕES FINANCEIRAS

É importante estar ciente de que ladrões podem utilizar aplicativos de instituições financeiras e de comércio eletrônico para cometer fraudes, tais como transferências bancárias, empréstimos, pagamentos de boletos e compras online. Para se proteger, recomenda-se notificar as instituições financeiras que você acessa por meio de aplicativos e solicitar as seguintes medidas:

- O bloqueio do acesso às contas por meio do aplicativo.
- O bloqueio dos cartões associados ao celular furtado.

Ao comunicar essas informações às instituições financeiras, você estará tomando medidas importantes para prevenir possíveis fraudes e minimizar os danos causados por ações não autorizadas.

2. CONTATE A OPERADORA DE CELULAR

À operadora de celular tem a capacidade de desativar o chip SIM e bloquear o IMEI do aparelho, o que impede a conexão à rede de telefonia móvel. Ao não poder fazer ou receber chamadas e mensagens SMS, as chances de fraudes, incluindo aquelas que poderiam afetar seus contatos, são significativamente reduzidas.

- É recomendado que você solicite à sua operadora a desativação do chip SIM e o bloqueio do código IMEI do aparelho. Essas ações ajudarão a garantir a segurança dos seus dados e a proteção contra possíveis usos indevidos do dispositivo.

Ao tomar essas medidas, você estará contribuindo para minimizar o risco de fraudes e salvaguardar tanto suas informações pessoais quanto as de seus contatos.

3. FAÇA UM BOLETIM DE OCORRÊNCIA

O boletim de ocorrência é um registro policial fundamental que auxilia na sua defesa, especialmente se o ladrão tentar se passar por você. É comumente exigido para contestar fraudes e acionar seguros.
Ao elaborar o boletim de ocorrência, é importante incluir informações essenciais, como o código IMEI e o número de série do aparelho. Esses dados ajudam à identificar de forma única o seu dispositivo e fornecem evidências importantes para investigações posteriores.

Certifique-se de declarar com precisão o código IMEI (International Mobile Equipment Identity) e o número de série do aparelho no boletim de ocorrência. Essas informações são cruciais para auxiliar as autoridades a rastrear o dispositivo e fornecer os recursos necessários para lidar com a situação.

Lembre-se de que a rapidez na elaboração do boletim de ocorrência é essencial para aumentar as chances de recuperação do aparelho e para fornecer as bases legais para tomar as medidas adequadas contra ações fraudulentas.

4. APAGUE REMOTAMENTE O APARELHO

Um celular furtado dificilmente é recuperado. Para evitar o uso indevido do seu celular e de seus dados, apague remotamente todo o conteúdo.

Para acessar o serviço de localização remota para dispositivos Android, você pode seguir as instruções fornecidas anteriormente em "PREPARE-SE PARA APAGAR O APARELHO REMOTAMENTE".
Acesse o site para localização remota: https://android.com/find/para Android conforme explicado anteriormente em "PREPARE-SE PARA APAGAR O APARELHO REMOTAMENTE".
Outra opção é utilizar a conta Mi, como mencionado anteriormente em "PREPARE-SE PARA APAGAR O APARELHO REMOTAMENTE". Para isso, acesse o site i.mi.com e faça o login usando o seu email e senha da conta Mi. Após ter acessado a sua conta, você encontrará a opção "apagar dados", que permitirá que você apague remotamente os dados do seu dispositivo.

Lembre-se de que essas medidas devem ser tomadas o mais rápido possível para aumentar as chances de proteger seus dados e minimizar qualquer risco de uso indevido do dispositivo.

5. DESCONECTE APLICATIVOS E TROQUE AS SENHAS DE SUAS CONTAS

É importante estar ciente de que vários aplicativos, como e-mail e redes sociais, podem permanecer autenticados no seu aparelho, permitindo o acesso sem a necessidade de digitar a senha a cada uso. No entanto, para evitar que um ladrão tenha acesso a esses aplicativos, é recomendado desconectar as contas e trocar as senhas regularmente.
Aqui estão algumas medidas que você pode tomar:

- Desconecte as contas dos aplicativos instalados no seu celular, realizando o logout. Isso garantirá que o ladrão não tenha acesso direto aos seus aplicativos autenticados.
- Troque as senhas das contas usadas no celular, principalmente do seu e-mail. Certifique-se de criar senhas fortes, combinações únicas de letras, números e caracteres especiais, para garantir uma camada adicional de segurança.
- Troque as senhas de login social, que são as contas de redes sociais usadas para autenticar em outros aplicativos. Isso impedirá que o ladrão acesse outros serviços e aplicativos através dessas credenciais.
- Não se esqueça de trocar as senhas das suas instituições financeiras, garantindo assim a segurança das suas transações e informações bancárias.
- Além disso, é recomendado atualizar as senhas do ID do sistema, para evitar qualquer acesso indesejado aos seus dispositivos e serviços.

Ao seguir essas medidas, você estará fortalecendo a segurança das suas contas e minimizando o risco de um ladrão ter acesso a informações sensíveis e realizar atividades fraudulentas.

6. CONTESTE FRAUDES E MONITORE SUA VIDA FINANCEIRA

Mesmo após o susto inicial, é importante estar atento, pois os problemas podem persistir se seus dados e contas forem utilizados indevidamente. Para lidar com essa situação, siga as seguintes orientações:

- Revise cuidadosamente os extratos de seus cartões e contas em instituições financeiras e de telefonia. Esteja atento a quaisquer transações suspeitas ou não autorizadas.
- Caso identifique transações fraudulentas, como transferências, empréstimos, pagamentos ou compras não realizadas por você, é fundamental contestá-las imediatamente. Entre em contato com as respectivas instituições financeiras ou fornecedores de serviços para relatar o ocorrido e buscar resolução.
- Se necessário, registre uma reclamação junto ao Banco Central. Eles podem fornecer orientações e assistência adicional na resolução de questões relacionadas a transações bancárias indevidas.

Agir prontamente e acompanhar de perto suas contas e transações é essencial para mitigar os impactos e minimizar quaisquer prejuízos causados por uso indevido de suas informações pessoais.

Lembre-se de manter-se atualizado sobre os procedimentos e políticas de segurança das instituições financeiras e seguir suas orientações específicas para lidar com casos de fraudes ou transações não autorizadas.

7. TROQUE AS SENHAS USADAS EM DISPOSITIVOS DE TERCEIROS

Agir rapidamente para conter prejuízos e evitar acessos indevidos é de extrema importância. Em situações de urgência, pode ser que você tenha utilizado suas senhas em um dispositivo emprestado, cuja segurança não pode ser garantida.
Para minimizar os riscos, é essencial redefinir as senhas usadas no dispositivo emprestado assim que você tiver acesso a um dispositivo confiável. Siga estes passos para fortalecer a segurança das suas contas:

- Assim que possível, procure um dispositivo de confiança, como o seu próprio smartphone ou computador.

- Acesse cada uma das contas em que você utilizou suas senhas no dispositivo emprestado.
- Utilize a opção de redefinição de senha disponibilizada por cada serviço ou aplicativo. Geralmente, isso envolve solicitar um link de redefinição por e-mail, responder a perguntas de segurança ou utilizar autenticação de dois fatores, se estiver disponível.
- Crie senhas novas e fortes para cada uma das contas, garantindo que sejam combinações únicas de letras, números e caracteres especiais. Evite utilizar informações pessoais óbvias nas senhas.

Ao redefinir as senhas em um dispositivo confiável, você estará aumentando a segurança das suas contas e reduzindo as chances de acesso não autorizado. Lembre-se de adotar boas práticas de segurança, como não compartilhar senhas, ativar a autenticação de dois fatores sempre que possível e manter-se atento a atividades suspeitas em suas contas.

8. PROGRAMA CELULAR SEGURO

8.1. O que é?

O Programa Celular Seguro, conduzido pelo Ministério da Justiça e Segurança Pública (MJSP), tem como objetivo primordial combater o roubo e o furto de aparelhos celulares em território nacional. Uma das estratégias propostas pelo MJSP para mitigar esse tipo de delito é a adoção de uma tecnologia que possibilite a comunicação do crime e, simultaneamente, ative bloqueios no próprio dispositivo, nos aplicativos bancários e em quaisquer outros acessos disponíveis no celular.

O Ministério da Justiça e Segurança Pública (MJSP) promoveu discussões com entidades setoriais, agências regulatórias, empresas de telefonia e de tecnologia para buscar soluções eficazes contra o roubo e o furto de celulares no país.

Uma das medidas propostas pelo MJSP para enfrentar esse problema é a implementação de uma tecnologia que permita a comunicação imediata do roubo ou furto, além de acionar bloqueios no dispositivo, nos aplicativos bancários e em possíveis acessos disponíveis no celular. A colaboração da Agência Nacional de Telecomunicações (Anatel), da Federação Brasileira de Bancos (Febraban), das instituições financeiras e das operadoras de telefonia foi fundamental para o desenvolvimento desse projeto.
Essa parceria resultou na criação da solução Celular Seguro, que possibilitará aos envolvidos serem alertados e tomarem as medidas necessárias para evitar danos maiores.

8.2. Quem pode utilizar?

O Programa Celular Seguro é destinado à todos os cidadãos brasileiros. Para registrar o aparelho celular é preciso estar cadastrado no Gov.br.

8.3. Etapas para realização deste serviço?

a) Instalar o Aplicativo: Abra a sua loja de aplicativos e busque por "Celular Seguro", acesse a página do app e clique para instalá-lo.
Após a instalação, o aplicativo estará disponível para o uso no seu aparelho celular.

Web: Acessar o site
Aplicativo móvel: Baixar o aplicativo

b) Logar no aplicativo por meio do Gov.br: Para utilizar o aplicativo, é essencial realizar o login. Basta tocar no botão "entrar com Gov.br"
Você será redirecionado para a página inicial do Gov.br, onde poderá fazer o login utilizando seu CPF e senha.

c) Concordar com os Termos de Uso: Ao entrar e iniciar o app, você será apresentado aos Termos de Uso e Privacidade de dados.
Nesse documento, também há a relação das instituições participantes do projeto.
Por favor, leia atentamente os termos e, para prosseguir, clique no botão CONCORDO.

d) Cadastrar pessoas de Confiança: Ao acessar o aplicativo pela primeira vez, você não terá nenhuma pessoa registrada. Para começar, clique na opção "Cadastrar Contrato". Quando você cadastra alguém como sua pessoa de confiança, ela passa a visualizar o seu aparelho no perfil dela para que, caso aconteça algo com o seu celular, por meio do aplicativo ela crie uma ocorrência em seu nome. Portanto, escolha com sabedoria.

e)Registrar Telefone: Ao acessar o aplicativo pela primeira vez você não encontrará nenhum aparelho registrado. Para começar, clique na opção “Cadastrar Telefone”.
Observação: Não existe quantidade limite para dispositivos, mas atenção! A linha do aparelho deve estar cadastrada no seu CPF.
Caso contrário, o alerta não será emitido.

f) Registrar Ocorrência: Caso ocorra alguma situação de roubo, perda ou furto do seu aparelho, você, ou a pessoa de confiança indicada, poderá criar uma ocorrência por meio do site ou aplicativo.

1. Selecione qual aparelho deseja fazer a ocorrência, seja "Meus telefones" ou "Telefones de Confiança"
2. Em seguida, você verá uma lista de todos os aparelhos cadastrados. Selecione aquele que teve o problema.
3. Clique em cima do botão "Alerta" para criar uma ocorrência

g) Atenção: Assim que a ocorrência for emitida, será exibido o NÚMERO DE PROTOCOLO. É necessário guardar esse número, pois para atendimentos posteriores com as instituições parceiras, o usuário precisará fornece-lo.

8.4. Outras informações

Para mais informações ou dúvidas sobre este serviço, entre em contato. O usuário poderá tirar dúvidas na página institucional do “Celular Seguro”, acessando o botão “Dúvidas Frequentes” no site gov.br/celularseguro. Este é um serviço do(a) Ministério da Justiça e Segurança Pública, em caso de dúvidas, reclamações ou sugestões favor contactá-lo.

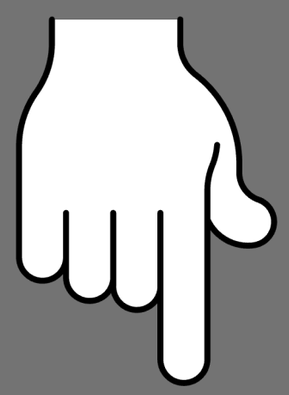
O usuário deverá receber, conforme os princípios expressos na lei nº 13.460/17, um atendimento pautado nas seguintes diretrizes:

•Urbanidade
•Respeito
•Acessibilidade
•Cortesia
•Presunção da boa-fé do usuário
•Igualdade
•Eficiência
•Segurança
•Ética

O usuário do serviço público, conforme estabelecido pela lei nº13.460/17, tem direito a atendimento presencial, quando necessário, em instalações salubres, seguras, sinalizadas, acessíveis e adequadas ao serviço e ao atendimento.

Tem direito a atendimento prioritário as pessoas com deficiência, os idosos com idade igual ou superior a 60 anos, as gestantes, as lactantes, as pessoas com crianças de colo e os obesos, conforme estabelecido pela lei 10.048, de 8 de novembro de 2000.

SAIBA MAIS



Para mais detalhes sobre este e outros assuntos relacionados com cuidados na Internet, consulte os demais Fascículos da Cartilha de Segurança para Internet, disponíveis em: https://cartilha.cert.br/
Procurando material para conversar sobre segurança com diferentes públicos? O Portal Internet Segura apresenta uma série de materiais focados em crianças, adolescentes, pais, responsáveis e educadores, confira em: https://internetsegura.br/.

A XIAOMI CUIDA DE VOCÊ

Tecnologia de qualidade
acessível para todos.