RETTA

TECNOLOGIA DA INFORMAÇÃO

Relatório documental do aplicativo Mundo Invest

08/08/2025 - 13/08/2025

—

Ariel da Silva Calixto

- Desenvolvedora Web Full-stack e estudante de Engenharia de Software
- Vaga: Estágio de Qualidade de Software (QA) na Mundo Invest
- Empresa: Retta

SUMÁRIO

Introdução:

Visão geral:

Com o objetivo de ampliar minha visão geral a respeito do comportamento do aplicativo, de forma a avaliar o funcionamento do backend e do front-end do mesmo, a análise será feita com base no resultado obtido através de três dispositivos diferentes, sendo eles:

1. Samsung Galaxy A03 Core;
   1.1. **Sistema Operacional**: Android

2. IPad modelo 6ª geração;
   2.1. **Sistema Operacional**: iOS

3. Xiaomi Poco C75;
   3.1. **Sistema Operacional:** Android

Objetivos:

1. Encontrar e relatar possíveis falhas e bugs, incluindo os mais visíveis, como problemas de interface, até os menos visíveis à primeira vista, como respostas do servidor e erros de configuração, se houverem.
2. Incluir observações e, quando possível, sugestões de melhorias e possíveis implementações que possam agregar ao funcionamento e/ou a identidade visual do aplicativo.
3. Ao final da análise, mostrar de forma objetiva e breve os resultados obtidos por meio de um vídeo gravado e disponibilizado na plataforma Loom.

Observações adicionais:

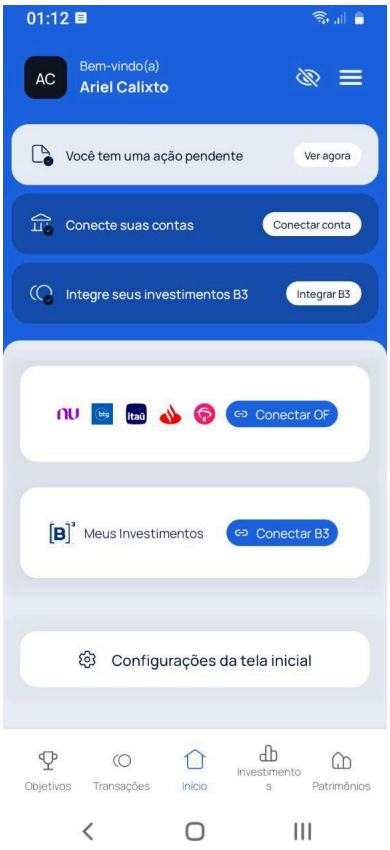
Após a finalização das etapas de avaliação, será possível chegar a uma conclusão de forma mais ampla, levando em consideração possíveis limitações, tudo será feito da melhor forma possível e - se necessário, com o uso de artigos para embasamento de análises e sugestões.

Primeiras impressões - Front-end:

A partir da tela de cadastro até a última tela que precede o acesso ao aplicativo, eu observei o layout, o uso das cores e até a hierarquia usada no layout. Usando os conceitos técnicos de UX e UI que eu utilizo nos meus projetos pessoais e profissionais, tomei a liberdade de fazer comentários a respeito do layout, como ele funciona ou pode funcionar pela perspectiva dos clientes e fazer sugestões, com o único objetivo de avaliar a efetividade da paleta de cores e a estrutura visual do aplicativo, afinal, a parte de cadastro é o que pode definir se o cliente vai continuar no aplicativo ou não, usando a minha experiência pessoal na etapa de cadastro como exemplo. Após a tela de cadastro, por último, vou avaliar visualmente de forma breve a tela de entrada no aplicativo.

Visão Geral:

1. O fundo cinza claro mantém a neutralidade, reduz uma possível fadiga visual e garante o contraste adequado entre elementos interativos.
2. O azul no CTA primário transmite segurança, profissionalismo e confiança e também ajuda a destacar a ação principal, o que é excelente para um aplicativo de finanças.
3. O texto em preto e cinza escuro, além de dar alta visualização do texto, também se encontra em conformidade com padrões de contraste (WCAG AA).
4. A cor verde para o feedback é muito importante, pois essas microinterações visuais reforçam a percepção de progresso, o que leva o usuário a se lembrar, por exemplo, da luz verde no trânsito, que passa a mensagem de “Siga em frente”, guiando o usuário visualmente.
5. A hierarquia visual foi respeitada. O foco primário no botão “Próximo passo”, por exemplo, no canto inferior direito está alinhado ao fluxo natural de leitura, ou seja, se encontra de acordo com o padrão F/Z.
6. Estruturalmente e visualmente, a área de cadastro está muito clara, e os campos e botões tem espaçamento adequado entre eles.
7. Além do alto contraste favorecendo uma leitura confortável, as áreas de toque são amplas (Fitts’s Law).
8. Padrões visuais consistentes, ajudando a diminuir a curva de aprendizado e facilitando a adaptação visual do cliente.
9. Durante o preenchimento do campo de número de telefone, os números se auto ajustaram, facilitando bastante a experiência de pessoas com dificuldade de digitação.



Tela de acesso:

Esse print foi tirado da tela do modelo **Samsung Galaxy A03 Core**, mais adiante neste documento durante os testes em outros dispositivos e em outro sistema operacional, houveram inconsistências visuais, mas por ora será usado este modelo do sistema operacional Android como referência. Descrição da tela de acesso:

1. A predominância do azul, ou #0066FF, reforça a ideia de confiança e profissionalismo mencionada anteriormente.
2. A consistência visual com a tela de cadastro foi mantida, dando a sensação de continuidade.
3. O contraste entre o azul de fundo e os elementos brancos é agradável visualmente, e o uso de branco e cinza claro nos cards ajuda a separar os conteúdos e evita a poluição visual.
4. No topo, a saudação e o ícone de privacidade criam a sensação de segurança.
5. A organização em blocos ajuda visualmente, mas funções excessivas podem aumentar a rolagem, levando ao cansaço visual.
6. O menu inferior fixo é perfeito para manter as principais funções sempre acessíveis, porém a palavra “Investimentos” foi cortada por falta de espaço, forçando o “s” para baixo, quebrando a consistência do menu e causando um certo desconforto visual.

Sugestões:

1. A opção de dark mode é sempre bem vinda, visto que algumas pessoas, incluindo eu, tem certa sensibilidade à luz, e a exposição prolongada a cores claras pode causar um certo desconforto visual.
2. Na área de menu, o azul sólido pode sobrecarregar visualmente depois de certo tempo, utilizar degradês ou alguma ilustração mais sutil pode suavizar visualmente.
3. O agrupamento visual de funções parecidas pode parecer um pouco redundante, por exemplo, “Conectar Conta” e “Integrar B3” poderiam ficar em um card separado com subtarefas.
4. Usar um indicador de progresso também é sempre interessante, como por exemplo, mostrar percentuais ou etapas concluídas no onboarding são recursos interessantes.

Primeiras impressões - Back-end:

1. Cadastro

Ao entrar na área de cadastro, percebi dois possíveis problemas:

1. No campo que solicita o nome completo, coloquei apenas o meu primeiro nome, para saber se o campo realmente aceita apenas nomes completos, e até mesmo se ele aceitaria qualquer nome que eu colocasse ali. De forma inesperada e infelizmente, ao colocar apenas o meu primeiro nome, o aplicativo me permitiu confirmar o campo "*Li e aceito os termos de uso e política de privacidade*", sem qualquer resistência do back-end.

2. No campo de criação de senha, como mostrado na foto a seguir, o campo considerou como sendo uma senha forte quando eu apenas incluí uma letra maiúscula e números, e também aceitou uma senha de apenas 8 caracteres

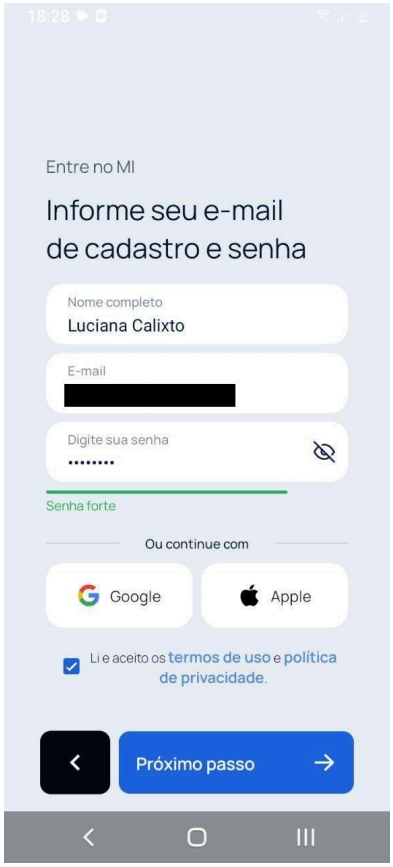
3. De acordo com um artigo da empresa Avast, uma senha considerada forte consiste em três características:

4. Longa:

4.1. De acordo com o artigo, quanto mais longa a senha, mais segura ela é, afirmando também que tais senhas devem conter pelo menos 10 caracteres para serem consideradas fortes, o que já confronta a afirmação do próprio campo de senha do aplicativo ao permitir uma senha de apenas 8 caracteres.

5. Complexa:

5.1. Também de acordo com o artigo, uma senha considerada forte é composta por uma combinação de letras, incluindo maiúsculas e minúsculas, números e símbolos, para formar uma linha de caracteres de difícil previsão, o que infelizmente, não se aplica ao campo de senha do aplicativo, que me permitiu criar uma senha sem nenhum caracter especial.



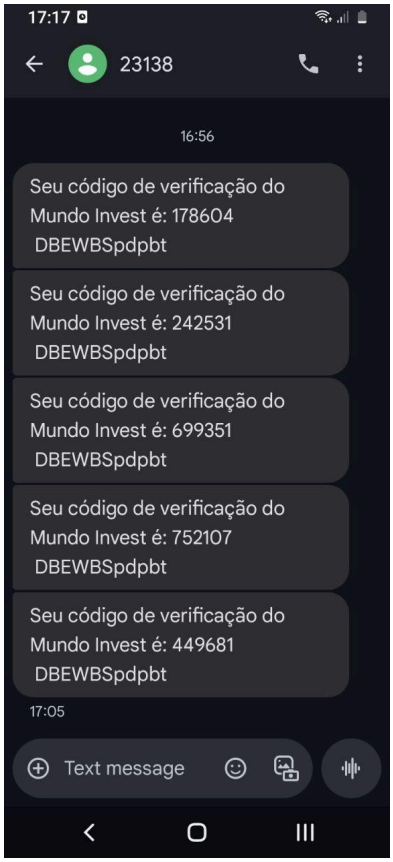
6. Exclusiva:

6.1. Uma senha forte só deve ser utilizada uma vez, para reduzir a vulnerabilidade em caso de vazamento de dados.

7. Como também pode ser visto neste print, o campo de cadastro não só me permitiu criar um cadastro com uma senha que não pode ser considerada forte, como também me permitiu seguir com o cadastro sem se certificar de que eu realmente li os termos (como por exemplo, permitir marcar a caixa de confirmação apenas após a barra de rolagem chegar ao final do termo de confirmação). Em resumo, não encontrei uma resistência mais rigorosa no campo de cadastro e nem na criação da senha.

8. O artigo da Avast pode ser encontrado neste link:

www.avast.com/pt-br/random-password-generator#pc

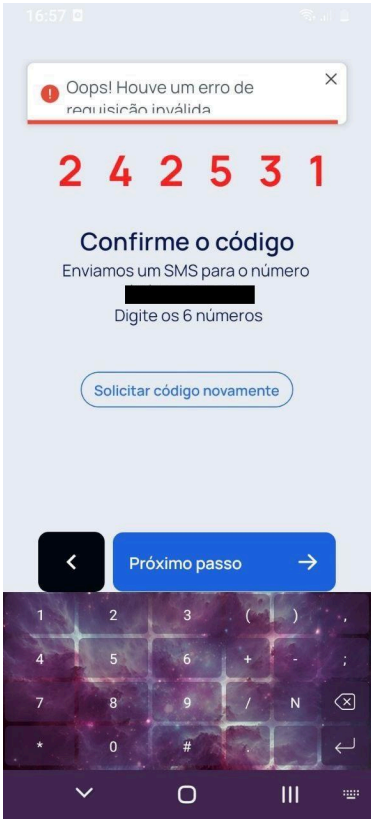


2. Autenticação

Ao concluir a etapa de cadastro, recebi a solicitação para inserir os seis dígitos enviados por SMS para o meu celular, para confirmar o meu número cadastrado, no entanto, após inserir os 6 dígitos, aparecia a mensagem: "*Oops! Houve um erro de requisição inválida*". A seguir, podemos ver nos prints a mensagem SMS com os 6 dígitos, a tentativa de inserir os dígitos e a mensagem, repare na quantidade de vezes que essa mensagem SMS foi enviada e o acesso foi negado pelo sistema, mesmo o código estando correto:

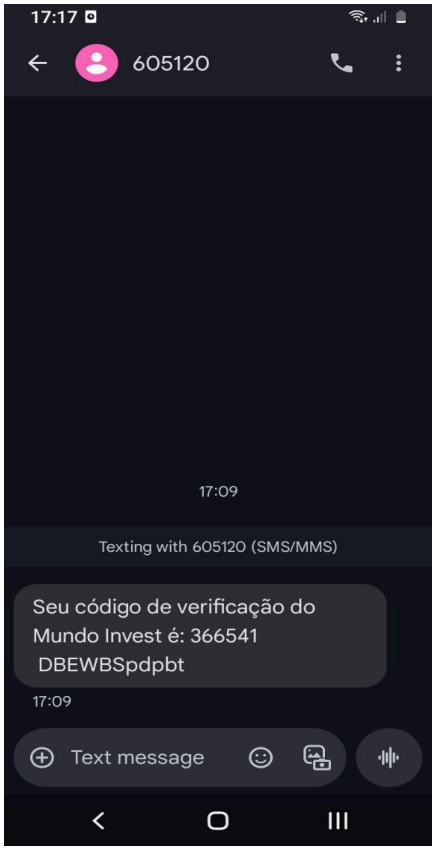
1. Neste primeiro print, vemos as primeiras tentativas, os SMSs foram enviados bem rapidamente, repare também no número de SMS do qual ele foi enviado: **23138**.

2. A seguir, temos um print da tela em que foram inseridos os 6 dígitos enviados por SMS, e também podemos ver a mensagem: "*Oops! Houve um erro de requisição inválida*", negando o acesso ao sistema e a continuidade do cadastro mesmo os números estando corretos.



3. Levando em consideração a User Experience (UX) e a User Interface (UI), considero esse vermelho um pouco agressivo e pode causar uma certa ansiedade e desconforto em pessoas mais sensíveis emocionalmente. Repare que os dígitos enviados por SMS e os digitados são idênticos, porém o sistema não me permitiu avançar, ou seja, não consegui passar da página de autenticação no modelo Samsung Galaxy A03 Core. Seguirei com os testes com os outros dois dispositivos, incluindo no sistema IOS.

4. Observe que muitas tentativas foram feitas, no print a seguir mostrarei exatamente mais 5 tentativas de inserir o código corretamente e todas as vezes, a mensagem apareceu novamente, até que por curiosidade, decidi sair e tentar novamente, e de forma curiosa e inesperada, uma nova mensagem com o número de autenticação foi enviado, porém agora de outro número: **605120**. Não sei se isso é esperado do sistema, mas achei válido comentar sobre isso, pois mostra uma certa inconsistência no sistema de envio de SMS.



5. Após esses testes, decidi mais uma vez me cadastrar para saber se talvez esse problema tinha algo a ver com o fato de eu não ter inserido o meu nome e um sobrenome, então fiz o teste: tentei me cadastrar de novo e dessa vez, só após a primeira tentativa, o sistema me solicitou o meu nome completo, porém isso levanta uma preocupação, pois isso pode ser considerada uma brecha na segurança, afinal, se existe essa brecha, quais outras brechas existem? Testei isso também e decidi colocar um nome que não é o meu nome de nascimento. O resultado foram os seguintes:

6. O sistema me permitiu seguir com o cadastro mesmo colocando um nome diferente, porém dessa vez me pediu o nome e o sobrenome. Infelizmente, mesmo colocando meu nome completo, o sistema continuou me impedindo de prosseguir com o cadastro mesmo inserindo os números corretos.

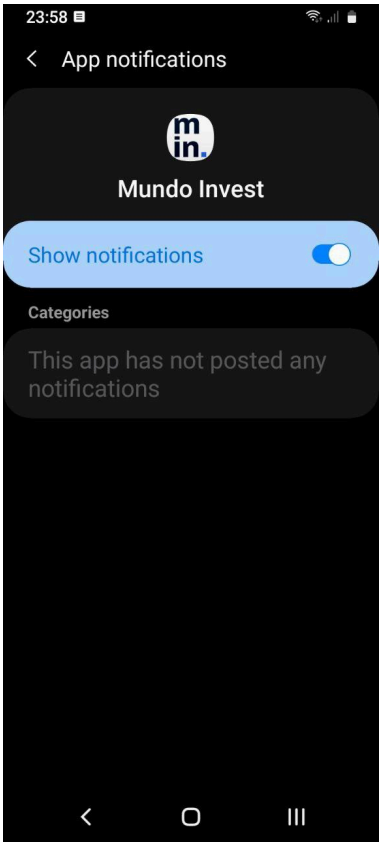
Conclusão:

Houve uma grande frustração no meu cadastro, não consegui concluir o cadastro e não consegui descobrir a causa do problema de autenticação de SMS. Após muitas tentativas, decidi continuar os testes em outros dispositivos.

Sugestões:

1. A inconsistência no número de envio por SMS é um pouco estranha à primeira vista. Seria interessante verificar isso, caso esse não seja um comportamento esperado.

2. Implementar uma verificação mais rigorosa e minuciosa no campo de cadastro para diminuir chances de falsidade ideológica, e implementar uma forma de forçar o cliente a ler os termos antes de concluir o cadastro, além de trocar o campo “Nome Completo” por dois campos: “Nome” e “Sobrenome”.



3. Implementar um sistema de criação de senha mais robusto, com o uso de senha com no mínimo 10 dígitos, letras maiúsculas e minúsculas e dígitos especiais.

Informações adicionais:

Estas são informações adicionais que precisam ser relatadas e acredito que mereçam atenção e futura correção. Ao final dessa conclusão adicional, serão apresentadas sugestões referentes ao que eu considero ser um bug, ou no mínimo, um equívoco de código que talvez não tenha sido levado em consideração ou simplesmente foi ignorado em alguma etapa do processo de desenvolvimento do aplicativo.

1. **O que aconteceu?**

1.1. Para contextualizar, como pode ser visto nos prints exibidos anteriormente, em primeiro lugar, não é exibida nenhuma forma de contato com alguém caso um erro ocorra - o que foi o meu caso. Durante todo o processo de tentativa de cadastro, em nenhum momento foi apresentado um número de telefone, whatsapp ou sequer um email para contato caso o cliente considerasse necessário em seu processo de cadastro, o que leva a dois possíveis problemas:

1.1.1. O cliente fica frustrado e desiste de concluir o cadastro. O cliente se sente desamparado e incapaz de encontrar uma ajuda que deveria estar a seu alcance, mas que infelizmente não está.

1.1.2. A empresa perde um potencial cliente por causa de uma falha de comunicação,

2. **A causa do problema foi encontrada?**
   2.1. A resposta é: acredito que sim. O que diferencia essa última tentativa de todas as outras tentativas foi um fator muito imprevisível e inusitado: nas tentativas anteriores eu rejeitei o pedido do aplicativo para que eu ativasse as notificações. Sendo uma pessoa que não gosta de notificações que não são estritamente necessárias no meu celular, não ativei as notificações e acreditei que não havia problema nenhum nisso. Para minha surpresa, sim, parece que houve um impacto disso no meu cadastro, são eles:

      2.1.1. Não consegui realizar o cadastro. Muitas tentativas foram feitas (como mostrado nos prints), porém o sistema não permitiu a conclusão do meu cadastro.

      2.1.2. Não houve nenhuma mensagem de orientação. Nada como: *"Você precisa ativar as notificações para proceder com o cadastro.*", ou um: "*Em caso de dúvidas ou problemas, nos envie um email.*". Nada que, infelizmente, pudesse servir de orientação para o cliente.

Sugestões finais:

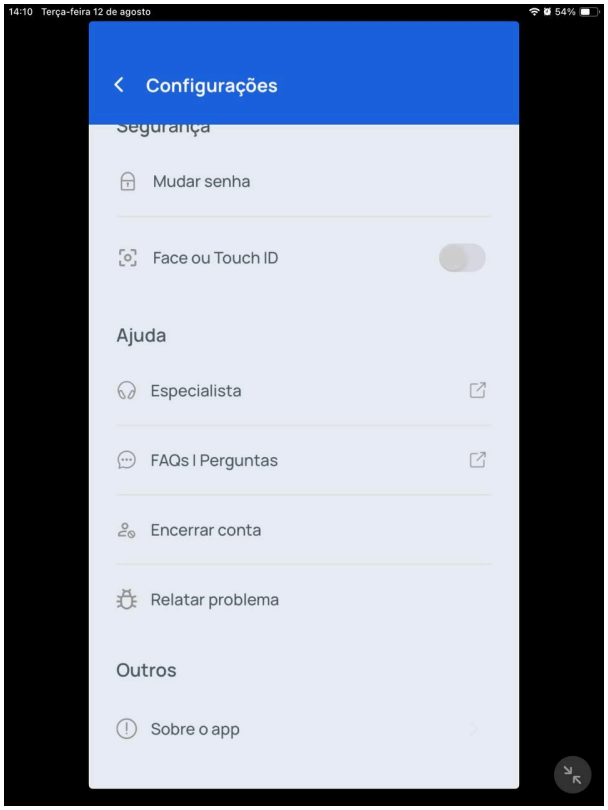
Eis uma lista de sugestões para essa etapa do processo de cadastro:

1. Foi sugerido forçar o cliente a ler os termos antes de concluir o cadastro e implementar um uso de senha mais robusto, então o próximo passo seria implementar uma forma de evitar fraudes e falsidade ideológica. Muitos aplicativos hoje em dia implementaram a necessidade de apresentação e autenticação de um documento com foto, como RG, passaporte ou carteira de trabalho. O uso de CPF não parece ser útil se usado sozinho, uma autenticação mais rígida em um aplicativo de finança soa altamente necessário. Não seria exagero implementar mais rigor nessa parte do cadastro.

2. Implementar mensagens de orientação durante todo o processo de cadastro. Como eu mencionei, não houve nenhuma mensagem de orientação, a única mensagem que apareceu foi: "*Oops! Houve um erro de requisição inválida*". Uma mensagem muito técnica, o que prejudica a comunicação com o cliente mais leigo que não entende do que se trata, uma mensagem em vermelho e levemente cortada pelo layout da autenticação dos 6 dígitos, o que pode levar a ansiedade em pessoas mais sensíveis emocionalmente e se tornar um pouco desagradável visualmente para pessoas detalhistas como eu, o que pode levar a acreditar que houve um pouco de desleixo ou não testaram as mensagens em telas de smartphone. Ou seja: remover ou simplificar a linguagem técnica, diminuir a intensidade do vermelho usado na mensagem ou até mesmo substituir por uma cor menos agressiva e por último, ajustar a mensagem para que ela não apareça cortada, melhorando visualmente o layout e facilitando a visualização da mensagem.

Utilizando outros aparelhos:

Por motivo de comparação, agora começaremos os testes e as comparações visuais e configuracionais dos aparelhos **Xiaomi Poco C75** e **IPad modelo 6ª geração**, ou seja, se encontrados, serão relatados bugs e/ou inconsistências na identidade visual e/ou layout do aplicativo através da experiência de usuário em um sistema operacional diferente, ou seja, iOS e também utilizando um modelo mais atual de um celular com sistema Android.



Este é o primeiro print mostrado da tela do Ipad. Repare que só após entrar no aplicativo a opção de relatar o problema apareceu no final das opções nas configurações, o que me levou a seguinte impressão:

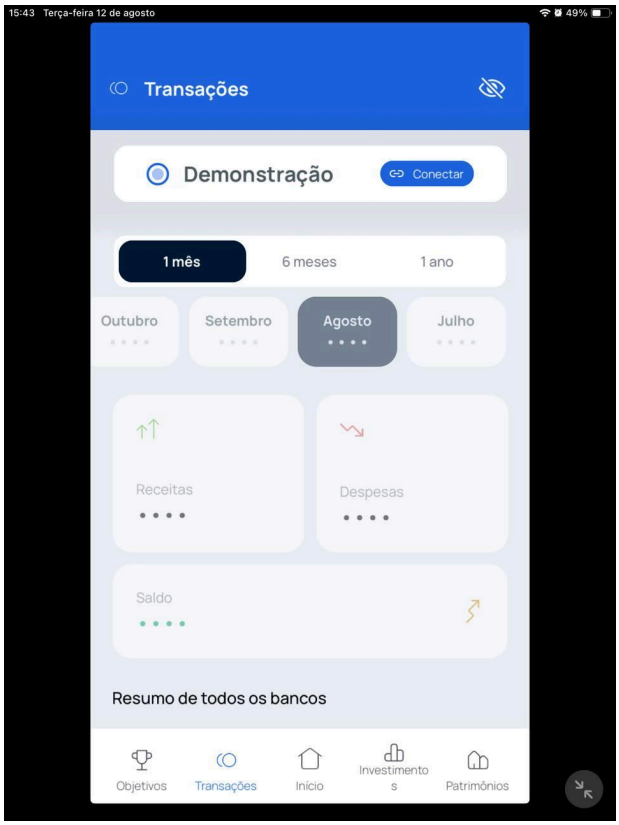
A opção de enviar feedback está presente, mas foi posicionada de forma discreta, o que pode dificultar que usuários a encontrem e utilizem.

É compreensível, porém, que isso tenha sido feito para não passar a ideia de um aplicativo defeituoso, afinal, uma opção de relatar bug bem na tela inicial não passaria uma boa impressão, soaria não-profissional e passaria uma sensação de insegurança. Um meio termo seria colocar essa opção não na tela principal, e também não escondido no fundo das configurações, mas sim colocá-lá na forma de “Fale conosco” durante todo o processo de cadastro e a opção “Relatar problema” poderia ser colocada em uma posição um pouco mais visível nas configurações, ou se preferirem uma opção mais elegante e sutil, poderiam renomear a opção para “Fale conosco” e remover o ícone de besouro, afinal nem todo mundo sabe o que isso significa e tornaria essa opção visualmente mais acessível.

Visualmente, o menu de configurações no IPad é agradável e nada foi cortado da tela, nenhuma palavra ou letra foi deformada por não caber no espaço determinado, o que não pode ser dito do menu de configurações no Xiaomi Poco C75 a seguir.

Observe a área “Outros” no fundo da seção de configurações. Nesta área encontra-se a opção “Sobre o app”. Nesta seção temos o endereço da Mundo Invest, os termos de uso, a política de privacidade, um email, as redes sociais da empresa e o CNPJ, porém como pode ser visto a opção está cortada pelo fundo do menu. Observe o esforço que o usuário precisa fazer ao tomar cuidado para não clicar no botão de visão geral dos apps abertos, ou seja, o usuário sairia do aplicativo e iria ver todos os outros aplicativos abertos apenas porque a opção “Sobre o app” está quase cortada pela metade. Imagine um usuário com limitações físicas, dificuldades motoras e até com problemas de visão. Em resumo: isso não é agradável visualmente, atrapalharia a experiência do usuário pelo motivo já mencionado e seria bem desagradável para pessoas com necessidades físicas especiais.

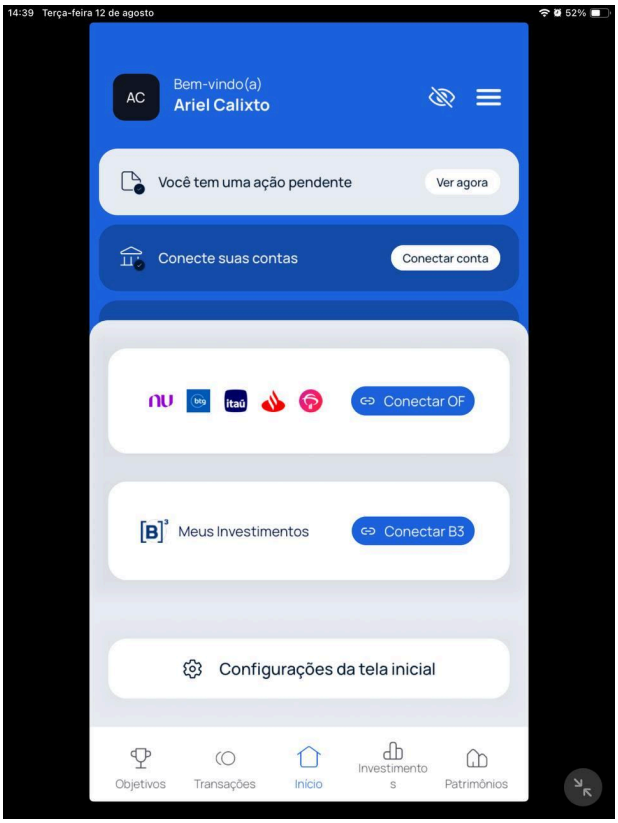
Saindo da área de configurações e entrando na opção “Recomendações”, logo abaixo da opção “Perfil”, encontra-se a área mostrada no print à direita. Neste print tirado da tela do Ipad que está sendo utilizado nos testes, observe os “cards” semicoloridos. Apenas o card da frente tem uma legenda e um breve resumo. Será que os usuários sabem que os cards de trás são interativos? Essa é uma pergunta que parece que não foi feita durante a concepção dessa área. As cores diferentes entre os cards são interessantes para mostrar ao usuário que são cards distintos, mas por que estão amontoados? Por que não estão dispostos um abaixo do outro ou lado a lado? Por que apenas o da frente tem legenda e uma breve apresentação - com ênfase no “breve”? Essa breve apresentação soa genérica, não explica muita coisa, o que me causou uma certa confusão e provavelmente causaria o mesmo a outros usuários, especialmente pessoas idosas que podem não compreender o que está escrito.



Agora estamos na área de “Transações”. Acredito que, até agora, esta é a única área do aplicativo onde eu não encontrei imperfeições visuais. O ícone de demonstração é altamente evidente, com um sutil efeito que guia o usuário sem precisar dizer nada. Como pode ser visto no print, o mês de agosto não foi selecionado por mim, assim que entrei ele já estava selecionado, guiando o usuário sem que ele precise se lembrar de qual mês ele está.

O ícone de ocultar os números também se encontra aqui, mostrando consistência visual e técnica entre as seções do aplicativo.

Neste print à direita tirado da tela “Início”, considerei necessário mostrar uma coisa: a opção de “Configurações da tela inicial” foi quase que completamente cortada, então após rolar a tela para baixo para ver essa opção, observei que os cards acima não se adaptaram para permanecerem visíveis ao usuário. No modelo Samsung Galaxy A03 Core e no modelo Xiaomi Poco C75 não houve sequer a necessidade de rolar para baixo, pois tudo estava bem visível à primeira vista, porém mais uma vez, acredito que não testaram adequadamente essa tela em um Ipad, ou não julgaram esse detalhe visual como sendo importante para uma boa experiência de usuário.



Testes de segurança:

Essa parte do relatório documental foi reservada para testes de segurança que julguei serem necessários.
Comecei por um teste simples: tentei criar uma nova conta usando o mesmo email, afinal isso seria uma falha grave de segurança, assim como os próximos testes que serão feitos, que também estarão sob o objetivo de explorar vulnerabilidades e, posteriormente, serão feitas sugestões de correção caso necessário.

1. Mesmo email para contas diferentes:

Essa falha de segurança seria incrivelmente grave, então desde o início do relatório este foi um dos primeiros testes que eu fiz. Felizmente, como mostrado no print, o sistema não me permitiu criar uma outra conta utilizando o mesmo email. A mensagem que apareceu foi: "*Email já cadastrado*!", frase curta e objetiva, porém não sei se vejo a necessidade de usar um ponto de exclamação ao final das mensagens ou se esse amarelo é a melhor opção de cor. Vou analisar essa parte pela ótica da UI e da UX:

1. Pela ótica da UX:

1.1. A mensagem é informativa e clara, porém muito técnica e pouco "humana".

1.2. A mensagem não necessariamente ajuda o usuário a saber qual é o próximo passo. De acordo com as regras de UX, não se pode apenas dizer o que deu errado, é necessário guiar o usuário para o próximo passo.

1.3. A mensagem soa brusca e quase como se fosse uma bronca do sistema, o que pode levar o usuário a ficar frustrado, e como já foi mencionado, a parte de cadastro é uma parte importante, pois é onde o usuário pode decidir se vai continuar o cadastro ou não.

1.4. A cor usada (amarelo) pode causar uma sensação de ambiguidade, por exemplo, o usuário pode se perguntar se essa mensagem se trata de algo grave, se é um lembrete ou um alerta de segurança.

2. Pela ótica da UI:

2.1. O amarelo é uma cor um pouco mais amena do que o vermelho, então não é inteiramente uma escolha ruim nessas situações, porém aqui como se trata de um bloqueio no fluxo de cadastro, ele parece mais um erro do que um aviso.

2.2. Claramente a intenção desta mensagem não é assustar o usuário, porém uma mensagem mais acolhedora e instrutiva seria mais apropriada, algo como: "*Email já cadastrado. Faça login para continuar.*" soaria mais amigável e mais instrutiva para o usuário, e claro, sem o ponto de exclamação.

2.3. O amarelo na hierarquia visual é usado para chamar a atenção do usuário, mas não quando se quebra um fluxo, como por exemplo: "*Sua senha vai expirar*." ou "*Complete o seu perfil*.", sendo essas mensagens que não quebram o fluxo.

2.4. No caso de uma quebra de fluxo, o padrão é geralmente usar um vermelho ou um vermelho mais leve e uma instrução.

2. Logins simultâneos em aparelhos diferentes:

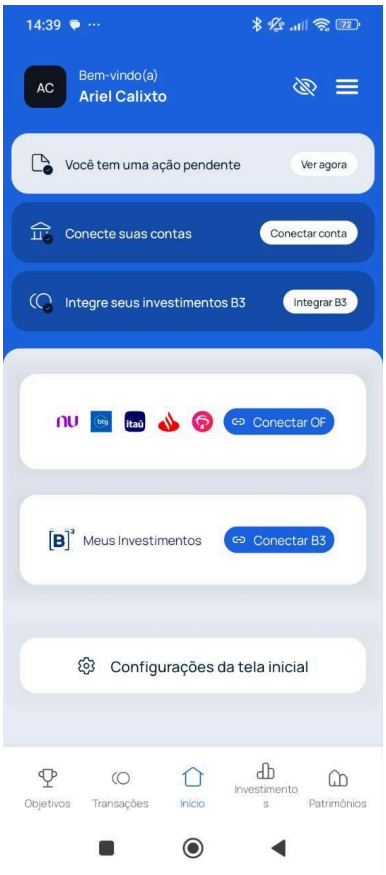
Infelizmente, é nesta parte do relatório que as informações ficam um pouco mais sérias e preocupantes, especialmente por se tratar de um app de finanças.
Antes de seguir para detalhes mais técnicos, gostaria de ressaltar alguns riscos de permitir que um app aceite uma mesma pessoa de logar em dois aparelhos diferentes ao mesmo tempo sem que o mesmo termine uma das sessões primeiro:

1. Em um eventual compartilhamento de contas, o usuário pode passar credenciais para outras pessoas e o sistema não poderia impedir, já que tecnicamente é o usuário quem está fazendo tal coisa, e isso dificultaria bastante rastrear essas atividades.

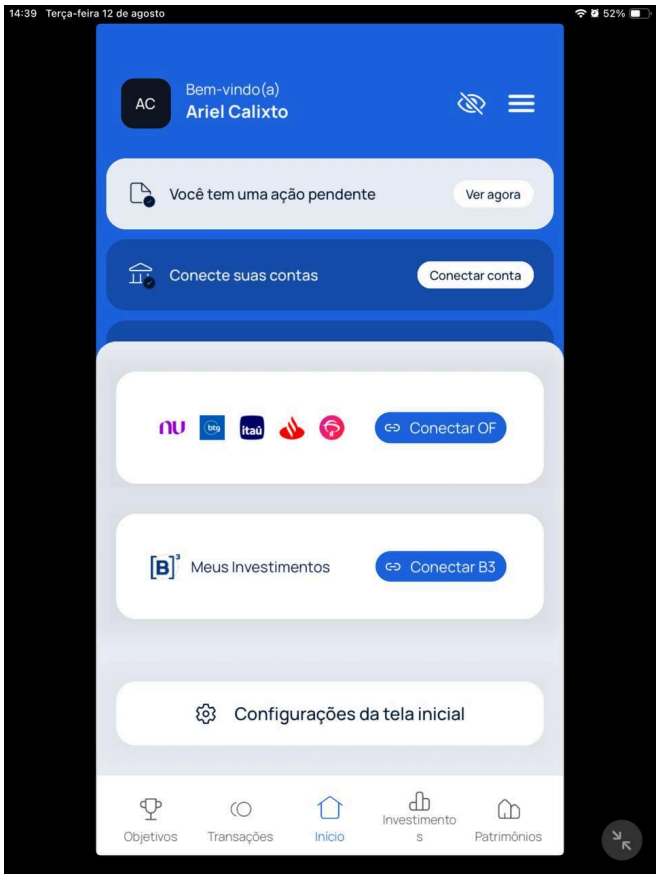
2. Em um eventual roubo de sessão, um hacker pode capturar o token de autenticação do usuário usando um dispositivo diferente sem ser detectado.

3. Ainda que o usuário faça logout ou troque de dispositivo, um hacker ainda teria acesso a conta do usuário.

4. E é necessário mencionar que dados sensíveis estarão expostos, como carteiras de investimentos, contas bancárias e informações pessoais como CPF.



Este print foi tirado da tela do modelo **Xiaomi Poco C75**. Observe o horário no canto superior esquerdo da tela, podemos ver que esse print foi tirado às 14:39 da tarde e a prova de que essa é a minha conta, é o meu nome visível abaixo da saudação “Bem-vindo(a)”.



No print a direita, tirado a partir da tela do **Ipad modelo 6ª geração**, ao dar um zoom na foto e observar também a parte superior esquerda da tela, também é possível ver o horário em que esse print foi tirado: 14:39 da tarde.
Observe também que assim como no print tirado do celular, o print do Ipad também está mostrando o meu nome, já que estava na minha conta. Acredito que agora que ambos os prints estão lado a lado, fica mais fácil ver aonde eu quero chegar com esse teste.

Conclusão:

O resultado deste teste foi preocupante, afinal eu não esperava ver o sistema de um app de finanças permitir esse tipo de ação. Como mencionado anteriormente, os riscos de se permitir algo assim são muito grandes, permitindo que hackers roubem dados pessoais de clientes sem serem incomodados e sem sequer serem identificados, prejudicando o cliente que pode ter seus dados e até seu dinheiro roubados e também prejudicando a empresa, que não será capaz de impedir que um hacker faça isso, já que nem sequer saberia que outra pessoa está usando a conta do cliente por outro dispositivo.

Sugestões:

1. Um dos passos que eu sugiro para evitar o login do usuário em dois dispositivos diferentes é um gerenciamento de sessões no servidor. Por exemplo, seria interessante armazenar o token de sessão no banco de dados junto com um identificador único de dispositivo, ou seja, ao fazer login seria possível verificar se já existe um token ativo, e se existe, a sessão anterior seria encerrada antes do usuário criar uma nova.
2. Um outro passo interessante seria invalidar tokens antigos automaticamente. Sempre que o usuário logar, gerar um novo token e invalidar todos os outros tokens relacionados àquela conta.
3. Uma outra forma de evitar logins simultâneos seria identificação do dispositivo por hash de informações, como: SO, IP, navegador ou até resolução, se o hash for diferente do último que foi registrado, então a reautenticação seria necessária e a sessão anterior seria encerrada.
4. Acredito que um campo “current_session_id” no banco de dados também poderia ajudar, por exemplo, toda requisição compararia o session_id enviado pelo usuário com o armazenado no banco de dados, se não bater então um novo login seria necessário.
5. Se estas sugestões não forem implementadas, ao menos sugiro que em caso de logins simultâneos, uma mensagem seja enviada ao usuário por email, por exemplo, para que o usuário possa tomar providências como mudar a senha em caso de login em dispositivos não identificados, exatamente como o Google e a Microsoft fazem.

Testes sugeridos:

1. Testes unitários podem ser utilizados para garantir que funções e middlewares que lidam com sessão, token e verificação de dispositivo funcionem de forma independente.

2. Um teste de integração, ou seja de fluxo ponta a ponta, poderia simular interações reais entre cliente, servidor e banco.

3. Um teste de segurança para simular um ataque também seria muito útil para verificar se existem falhas que podem ser exploradas no controle de sessão, como por exemplo um **Replay Attack** para tentar reutilizar um token antigo, ou um **Token Theft** para simular a clonagem de um token de um dispositivo e tentar usar em outro.

Conclusão:

Neste relatório documental foram relatados imperfeições em diversas áreas do aplicativo “Mundo Invest”, entre as áreas que foram exploradas e documentadas, foram citadas:

1. **Front-end:**
   - 1.1. identidade visual;
   - 1.2. imperfeições de layout;
   - 1.3. responsividade;
   - 1.4. experiência do usuário;
2. **Back-end:**
   - 2.1. respostas do sistema;
   - 2.2. falhas de autenticação;
   - 2.3. rigor no cadastro;
3. **Comparação:**
   - 3.1. entre modelos;
   - 3.2. entre dispositivos;
   - 3.3. entre sistemas operacionais;
4. **Segurança:**
   - 4.1. login simultâneo;
   - 4.2. uso do mesmo email para contas diferentes;

Após o detalhamento de todas estas áreas citadas, foram feitas sugestões de melhorias que acredito que acrescentariam ao funcionamento e uso do aplicativo de forma considerável, além de acreditar que as sugestões de segurança que foram feitas seriam as de maior necessidade em serem implementadas, já que se trata de um app de finanças contendo informações sensíveis de usuários.

No geral, o app é promissor e altamente funcional, a experiência foi agradável e foi com grande prazer que os testes foram feitos, pois um aplicativo de qualidade é aquele que funciona de forma satisfatória em todas as suas partes, e é para isso que os testes foram desenvolvidos e é por isso que são tão importantes.

Agradeço a oportunidade de poder avaliar o aplicativo e sugerir correções, pois esse é o tipo de experiência que acrescenta profissionalmente na vida de um desenvolvedor.

Espero que este documento possa ser útil de alguma forma e que o profissionalismo e dedicação que foram usados para escrever este relatório estejam visíveis à todos que estejam lendo este documento.

Referências:

- Avast. (2025). **Gerador de Senhas Aleatórias.** https://www.avast.com/pt-br/random-password-generator#pc

- Soegaard, Mads. (2021).**Hierarquia Visual: Organizando conteúdo para seguir padrões naturais de movimento ocular**. Interact Design Foundation. https://www.interaction-design.org/literature/article/visual-hierarchy-organizing-content-to-follow-natural-eye-movement-patterns

- Vizel, Moran. (2025). **WCAG: Diretrizes de acessibilidade padrão ouro**. Userway. https://userway.org/pt/blog/wcag-diretrizes-acessibilidade/

- msp4msps. (2024). **Como se proteger contra roubo de tokens**. Tminus365. https://tminus365.com/how-to-protect-against-token-theft-conditional-access/

- Budiu, Raluca. (2022). **Lei de Fitts e suas aplicações em UX.** NNGroup. https://www.nngroup.com/articles/fitts-law/

- Binance Academy. (2019). **O que é Replay Attack?** https://academy.binance.com/pt/articles/what-is-a-replay-attack