

SYSCREDI

Handbook Institucional e Operacional

Regras de negócio, perfis, escopo, controles e operação completa do sistema de microcrédito.

Edição 1.0
Versão de referência 1.0.2+3
27 de setembro de 2026
Uso interno e institucional

Sobre este documento

Este handbook constitui a referência institucional do Syscredi para formação, implantação, operação, supervisão e auditoria. Políticas aprovadas, configuração da instituição, legislação aplicável e autorização do backend prevalecem sobre exemplos deste documento.

Sumário executivo

1. Propósito do handbook
2. Visão executiva do Syscredi
3. Escopo funcional
4. Modelo institucional e conceitos
5. Perfis, responsabilidades e segregação
6. Acesso, sessão e segurança
7. Configuração inicial da instituição
8. Cadastro de clientes e partes relacionadas
9. Produtos de crédito e simulação
10. Ciclo completo do crédito
11. Regras de decisão e exceção
12. Contratos, carteira e prestações
13. Pagamentos, recibos e estornos
14. Cobranças e gestão de atraso
15. Reestruturação, refinanciamento e baixa
16. Tesouraria e caixa
17. Contabilidade
18. Risco, AML/KYC e garantias
19. Documentos e gestão de evidências
20. Relatórios e exportações
21. Pesquisa, interface e experiência operacional
22. Notificações, tarefas e prazos
23. Modo offline, pendências e sincronização
24. Auditoria e rastreabilidade
25. Privacidade e proteção de dados
26. Backups, continuidade e recuperação
27. Integrações
28. Administração do sistema
29. Rotinas operacionais recomendadas
30. Controles-chave
31. Indicadores de gestão
32. Gestão de incidentes
33. Resolução de problemas
34. Checklist de entrada em produção
35. Formação por perfil
36. Governança do handbook
37. Glossário
38. Regras de ouro
39. Referências técnicas internas

Este handbook é a referência funcional e operacional do Syscredi. Ele descreve o propósito do produto, escopo, perfis, regras de negócio, ciclo do crédito, controles, responsabilidades e práticas de operação. Configurações da instituição, políticas de crédito, legislação aplicável e autorizações do backend prevalecem sempre sobre exemplos deste documento.

1. Propósito do handbook

Este documento existe para:

- estabelecer uma visão comum sobre o funcionamento do Syscredi;
- definir responsabilidades e limites de cada perfil;
- documentar o ciclo completo do microcrédito;
- tornar explícitas as principais regras de negócio e controles;
- apoiar formação, implantação, operação, auditoria e suporte;
- reduzir decisões informais, duplicidade de dados e risco operacional;
- servir de base para procedimentos internos e critérios de aceitação.

O handbook deve ser revisto sempre que houver alteração relevante em perfis, políticas, estados, integrações, documentos, regras financeiras ou requisitos regulatórios.

2. Visão executiva do Syscredi

O Syscredi é uma plataforma de gestão de microcrédito orientada à operação institucional. Centraliza cadastro, originação, análise, decisão, autorização, desembolso, carteira, cobranças, tesouraria, contabilidade, risco, conformidade, documentos, relatórios e administração.

2.1. Resultados esperados

- fonte única e auditável para clientes, pedidos e créditos;
- maior disciplina no processo de concessão;
- separação entre preparação, análise, decisão e execução financeira;
- rastreabilidade de utilizadores, datas, alterações e movimentos;
- consistência entre condições aprovadas, contrato e plano de pagamento;
- melhor controle da carteira, atrasos, caixa e risco;
- continuidade operacional em ambientes de conectividade limitada;
- capacidade de operar em desktop, web e dispositivos móveis.

2.2. Princípios do produto

1. Isolamento institucional: cada organização opera dentro da sua própria fronteira de dados.
2. Menor privilégio: cada pessoa recebe apenas os acessos necessários.
3. Segregação de funções: atividades incompatíveis devem ser executadas ou revistas por pessoas distintas.
4. Rastreabilidade: decisões e movimentos relevantes devem possuir autor, data, contexto e histórico.
5. Integridade financeira: valores monetários não devem depender de arredondamentos imprecisos ou duplicação de pedidos.
6. Configuração institucional: produtos, marca, políticas e parâmetros pertencem à organização.

7. Defesa em profundidade: ocultar menus não substitui autorização no backend.
8. Exceção explícita: desvios de política exigem justificação e aprovação competente.
9. Documento coerente: contrato, aprovação, desembolso e plano de pagamento devem refletir a mesma decisão.
10. Operação verificável: nenhuma mensagem de sucesso substitui confirmação do estado final.

3. Escopo funcional

3.1. Incluído no sistema

Domínio	Capacidades principais
Identidade e acesso	Registo institucional, autenticação, recuperação, convites, perfis, estados e sessão.
Clientes	Pessoas singulares, empresas, contactos, documentos, situação profissional e contexto financeiro.
Partes relacionadas	Co-assinantes, fiadores, garantias e documentos associados.
Produtos	Limites, moedas, taxas, prazos, juros, comissões, periodicidade, carência e elegibilidade.
Originação	Criação, preparação e submissão de pedidos de crédito.
Análise	Capacidade financeira, risco, AML/KYC, visita, garantias e recomendação.
Decisão	Aprovação, rejeição, devolução, condições e registo de fundamento.
Formalização	Autorização, contrato, documentos e preparação de desembolso.
Carteira	Créditos, contratos, saldos, prestações, vencimentos e desempenho.
Pagamentos	Recebimentos, imputação, recibos, reversões e rastreabilidade.
Cobranças	Atrasos, promessas, contactos, ações e acompanhamento.
Financeiro	Contas, caixa, transferências, desembolsos, reembolsos, receitas e despesas.
Contabilidade	Plano de contas, lançamentos, diário, razão e demonstrações disponíveis.
Risco e conformidade	Alertas AML, indicadores, limites, exceções, garantias e auditoria.
Documentos e relatórios	Contratos, recibos, cartas, exportações e relatórios operacionais.
Administração	Utilizadores, definições, auditoria, sincronização, backups, planos e integrações.

3.2. Fora do escopo sem integração ou validação adicional

O Syscredi não deve ser presumido como substituto automático para:

- decisão jurídica, parecer de compliance ou aprovação regulatória;
- confirmação de identidade por autoridade pública;
- transferência bancária ou mobile money sem integração ativa;
- reconciliação bancária externa sem fonte confirmada;
- bureau de crédito sem conector contratado;
- assinatura digital qualificada sem provedor adequado;
- arquivo físico obrigatório;
- definição autónoma da política de crédito da instituição;
- cálculo fiscal ou regulamentar não validado para a jurisdição;
- recuperação judicial ou extrajudicial conduzida por profissionais habilitados.

4. Modelo institucional e conceitos

Conceito	Definição operacional
Organização/tenant	Instituição proprietária dos utilizadores, dados e configurações.
Utilizador	Identidade autenticada associada a uma organização, perfil e estado.
Perfil	Conjunto de capacidades atribuídas ao utilizador.
Cliente	Pessoa singular ou empresa candidata ou titular de crédito.
Fiador	Terceiro que oferece garantia pessoal; não se confunde com o perfil Avalista.
Avalista	Perfil interno de análise de crédito, tecnicamente compatível com a chave analyst.
Produto de crédito	Regras comerciais e financeiras aplicáveis a uma modalidade de financiamento.
Pedido	Dossiê de crédito antes do desembolso.
Decisão	Resultado formal da análise: aprovar, rejeitar, devolver ou condicionar.
Crédito/loan	Obrigação financeira ativa criada após desembolso.
Contrato	Registo documental das condições aceites e aprovadas.
Prestação	Parcela prevista no plano de pagamento.
Movimento	Entrada, saída, transferência, pagamento ou lançamento financeiro.
Garantia	Bem, valor, documento ou obrigação pessoal associado ao risco.
Exposição	Valor em risco de um cliente, grupo, produto ou carteira.
Idempotência	Garantia de que repetir a mesma solicitação não duplica o efeito.

4.1. Fonte de verdade

- dados de negócio confirmados no backend constituem a fonte operacional principal;
- documentos gerados são evidência, mas devem refletir o registo estruturado;
- conteúdo local pendente não deve ser tratado como confirmado até sincronizar;
- o histórico de auditoria não substitui o registo principal, mas explica a sua evolução;
- exportações são fotografias de um momento e podem ficar desatualizadas.

5. Perfis, responsabilidades e segregação

5.1. Gestor

Responsável pela governação institucional e supervisão da operação. Pode, conforme a configuração, administrar utilizadores, produtos, políticas, relatórios, finanças, risco, auditoria, subscrição, backups e integrações.

Responsabilidades mínimas:

- manter perfis e acessos adequados;
- aprovar políticas, limites e exceções;
- supervisionar carteira, caixa, risco e conformidade;
- garantir reconciliação, backups e continuidade;
- preservar pelo menos um segundo acesso gestor válido;
- investigar alertas, anomalias e operações sensíveis.

5.2. Operador

Executa o atendimento e a preparação operacional dos processos.

Pode incluir: cadastro de clientes e empresas, associação de fiadores, preparação do pedido, recolha documental, introdução de condições propostas e acompanhamento de pendências.

Não deve: aprovar exceções próprias, elevar o próprio perfil, executar controlos reservados ao gestor ou alterar movimentos financeiros sem competência expressa.

5.3. Avalista

Perfil interno de análise. Examina capacidade de pagamento, documentação, risco, AML/KYC, garantias, visita e condições propostas. Pode recomendar, devolver, aprovar ou rejeitar quando a política e a permissão atribuída o permitirem.

A designação visual Avalista não deve ser confundida com o fiador do cliente. A chave técnica pode permanecer `analyst` para compatibilidade.

5.4. Fiador

Parte relacionada ao crédito e, quando possuir conta de utilizador, perfil de acesso mínimo. Deve visualizar apenas dados, documentos, garantias e pendências que legitimamente lhe dizem respeito.

O fiador não deve receber métricas globais, carteira institucional, dados de outros clientes, tesouraria, administração ou configurações.

5.5. Equipa de suporte e administração técnica

Atua na resolução de incidentes, configuração e continuidade. O acesso técnico não implica autorização para decidir crédito, movimentar caixa ou alterar dados sem procedimento documentado.

5.6. Matriz funcional de referência

Área	Gestor	Operador	Avalista	Fiador
Início e indicadores	Completo	Operacional	Crédito/risco	Restrito
Clientes e empresas	Completo	Criar/editar	Consulta contextual	Próprios dados
Fiadores e co-assinantes	Completo	Preparar	Analisar	Próprios vínculos
Produtos de crédito	Administrar	Consultar	Consultar	Não
Simulação	Sim	Sim	Sim	Conforme política
Pedidos	Completo	Criar/preparar	Analisar/decidir	Restrito
Desembolso	Autorizar/executar	Não, salvo delegação	Não	Não
Carteira e cobranças	Completo	Operacional	Consulta	Próprias obrigações
Tesouraria/contabilidade	Completo	Não, salvo delegação	Não	Não
Risco e AML	Completo	Sinalizar	Analisar	Não
Relatórios	Completo	Operacionais	Analíticos	Não
Utilizadores/configurações	Administrar	Não	Não	Não
Auditoria/backups	Completo	Não	Consulta autorizada	Não

Esta matriz é uma referência de desenho. A autorização efetiva depende do perfil ativo, das políticas institucionais e das verificações do backend.

5.7. Regras de segregação recomendadas

- quem prepara um pedido não deve ser o único decisor;
- quem aprova não deve executar sozinho um desembolso sensível;
- quem recebe numerário não deve ser o único responsável pela reconciliação;
- estornos e alterações de condições devem exigir revisão superior;
- utilizadores não devem atribuir privilégios a si próprios;
- acessos de suporte devem ser temporários, justificados e auditáveis;
- exceções de política devem identificar proponente, aprovador e fundamento.

6. Acesso, sessão e segurança

6.1. Registo institucional

O primeiro gestor cria a instituição e a identidade inicial. O fluxo deve associar organização, utilizador e perfil numa operação coordenada. Dados incompletos ou credenciais inválidas devem impedir a conclusão.

6.2. Convites e ativação

1. O gestor cria ou convida o utilizador.
2. Define nome, e-mail, perfil e estado.
3. O destinatário conclui o convite e estabelece credencial.
4. O acesso somente é válido com identidade reconhecida, perfil existente e estado ativo.
5. Convites expirados devem ser renovados; não devem ser reutilizados indefinidamente.

6.3. Autenticação

- utilizar credenciais individuais; contas partilhadas são proibidas;
- não guardar palavras-passe em documentos, chats ou tickets;
- confirmar organização e perfil carregados após o login;
- aplicar MFA quando disponível e exigido pela política;
- bloquear ou rever tentativas suspeitas conforme procedimento institucional.

6.4. Recuperação e encerramento

A recuperação deve usar canal previamente validado. Ao terminar sessão, o aplicativo remove a sessão local com tolerância a falhas do armazenamento seguro. Em equipamentos partilhados, o utilizador deve confirmar o retorno à tela de login.

6.5. Gestão do ciclo de acesso

Evento	Ação obrigatória
Admissão	Criar conta nominal com menor privilégio.

Evento	Ação obrigatória
Mudança de função	Rever perfil e remover acessos anteriores.
Ausência prolongada	Suspender ou restringir conforme política.
Saída da instituição	Desativar imediatamente e revogar sessões.
Suspeita de comprometimento	Bloquear, redefinir credenciais e investigar auditoria.
Revisão periódica	Confirmar necessidade, perfil, atividade e proprietário.

7. Configuração inicial da instituição

Antes de operar crédito real, o gestor deve concluir e validar:

1. identidade institucional, logótipo, cor, contactos e rodapé;
2. moeda e formatos aplicáveis;
3. produtos, taxas, prazos, limites, comissões e carências;
4. perfis, utilizadores, aprovadores e alçadas;
5. contas financeiras, caixa e estrutura contabilística;
6. critérios de KYC, AML, garantias e documentação;
7. modelos de contrato, recibos, cartas e relatórios;
8. canais de pagamento e integrações;
9. política de backups, retenção e recuperação;
10. procedimento de incidentes, estornos e reconciliação;
11. testes de ponta a ponta com valores não produtivos;
12. aprovação jurídica, contabilística e regulatória.

Nenhuma configuração visual deve ser interpretada como validação jurídica das cláusulas ou conformidade regulatória.

8. Cadastro de clientes e partes relacionadas

8.1. Cliente individual

O cadastro deve conter informação suficiente para identificar, contactar e avaliar o cliente. Campos concretos dependem da política e do formulário ativo, mas normalmente incluem:

- nome completo e identificação;
- data de nascimento e contactos;
- morada e localização;
- profissão, empregador ou atividade económica;
- rendimento, despesas e outras obrigações;
- finalidade do crédito;
- documentos de identificação e comprovativos;
- consentimentos e declarações exigidas.

8.2. Empresa

Além da identificação legal, devem ser considerados representantes, beneficiários efetivos, atividade, localização, contactos, capacidade financeira, documentos societários e poderes de assinatura.

8.3. Fiadores e co-assinantes

- um co-assinante participa da obrigação;
- um fiador fornece garantia pessoal;
- a mesma pessoa não deve ser duplicada sem necessidade;
- vínculos devem indicar o cliente ou pedido correspondente;
- contactos, documentos, consentimento e capacidade devem estar atualizados;
- o perfil interno Avalista não é uma parte garantidora.

8.4. Qualidade e duplicidade

Antes de criar um cliente, pesquise por nome, contacto, documento ou referência disponível. A correção de duplicados deve preservar histórico e relacionamentos; não apague simplesmente um registo com operações associadas.

8.5. Arquivo e inativação

Registos com histórico financeiro devem ser inativados ou arquivados, não eliminados de forma destrutiva. A reativação deve respeitar nova verificação documental e de risco quando necessária.

9. Produtos de crédito e simulação

Um produto define a moldura dentro da qual pedidos podem ser propostos e aprovados.

9.1. Parâmetros típicos

- montante mínimo e máximo;
- moeda;
- taxa e método de cálculo de juros;
- prazo e periodicidade;
- método de amortização;
- comissões, impostos e encargos;
- carência e vencimento inicial;
- garantias e documentos exigidos;
- critérios de elegibilidade;
- limites de atraso, exposição e exceção;
- regras de renovação, reestruturação ou liquidação antecipada.

9.2. Regras de produto

- um pedido deve usar produto ativo e aplicável à organização;
- valores fora de limite devem ser bloqueados ou tratados como exceção formal;
- taxa, prazo e comissões devem ser capturados na decisão e no contrato;
- alterações posteriores não devem reescrever contratos existentes sem processo próprio;

- desativar um produto impede novas originações, mas não elimina créditos anteriores;
- a moeda do produto deve permanecer consistente no pedido, contrato e movimentos.

9.3. Simulação

A simulação é indicativa até existir aprovação e contrato. Deve apresentar, quando disponível, montante, prazo, taxa, prestação estimada, encargos e total previsto. Mudanças de data, arredondamento, impostos ou condições podem alterar o plano final.

10. Ciclo completo do crédito

10.1. Etapa 1 — Preparação

O operador seleciona o cliente e o produto, informa montante, prazo, finalidade e condições propostas. O sistema deve impedir submissão quando faltam elementos obrigatórios.

10.2. Etapa 2 — Documentação

Documentos devem ser legíveis, atuais, corretamente classificados e ligados ao titular apropriado. A existência de um ficheiro não prova autenticidade; a validação pertence ao procedimento KYC.

10.3. Etapa 3 — Análise financeira

A análise deve considerar rendimento, despesas, obrigações existentes, fluxo de caixa, estabilidade, sazonalidade, exposição e prestação proposta. O resultado deve explicar a capacidade de pagamento, e não apenas apresentar um número.

10.4. Etapa 4 — Risco, AML e visita

Quando aplicável, verificar:

- identidade e coerência dos dados;
- beneficiário efetivo e partes relacionadas;
- alertas AML/KYC e sinais atípicos;
- finalidade e origem de fundos;
- localização, atividade e evidências de visita;
- garantias, propriedade, valor e validade;
- conflitos de interesse e concentração de risco.

Um alerta não deve ser simplesmente ignorado: deve ser resolvido, escalado ou aceite por autoridade competente com fundamento.

10.5. Etapa 5 — Recomendação e decisão

A decisão deve indicar resultado, montante, prazo, taxa, condições, garantias, exceções e fundamento. Uma aprovação condicional permanece incompleta até cumprimento das condições.

10.6. Etapa 6 — Autorização

A autorização confirma que a decisão é válida, as condições foram cumpridas, a documentação está pronta e a pessoa possui alçada para avançar.

10.7. Etapa 7 — Formalização

O contrato e documentos associados devem refletir exatamente a aprovação. Divergências de montante, moeda, taxa, prazo, encargos, datas ou garantias devem interromper o processo.

10.8. Etapa 8 — Desembolso

Antes de desembolsar, confirmar:

- aprovação e autorização válidas;
- contrato aceite conforme o procedimento;
- conta financeira e canal corretos;
- beneficiário e dados de pagamento;
- ausência de bloqueios de conformidade;
- disponibilidade de fundos;
- chave de idempotência ou mecanismo equivalente.

Após confirmação, o desembolso cria ou ativa o crédito, gera o plano de pagamento e registra os movimentos correspondentes. Repetir a mesma solicitação não deve duplicar o desembolso.

10.9. Estados de referência

Estado	Significado	Próxima ação esperada
Rascunho	Pedido em preparação.	Completar dados e documentos.
Submetido	Pedido entregue para análise.	Validar completude e distribuir.
Em análise	Avaliação financeira, documental e de risco.	Emitir recomendação.
Devolvido/Pendente	Existem correções ou condições por cumprir.	Corrigir e voltar a submeter.
Aprovado	Decisão favorável registrada.	Cumprir condições e autorizar.
Rejeitado	Decisão desfavorável encerrada.	Comunicar e preservar fundamento.
Autorizado	Pronto para formalização/desembolso.	Validar contrato e executar.
Desembolsado/Ativo	Fundos entregues e obrigação vigente.	Acompanhar prestações.
Em atraso	Uma ou mais obrigações vencidas.	Cobrança e avaliação de risco.
Reestruturado	Condições alteradas por processo formal.	Cumprir novo plano e monitorizar.
Liquidado	Saldo elegível integralmente pago.	Encerrar e emitir comprovativos.
Anulado/Cancelado	Processo encerrado sem efeito futuro válido.	Preservar motivo e auditoria.

Nomes concretos podem variar na interface ou API. Transições devem seguir as ações disponíveis e nunca ser forçadas por edição direta de dados.

11. Regras de decisão e exceção

11.1. Aprovação

Uma aprovação deve ser reproduzível: outra pessoa autorizada deve conseguir entender quais dados, documentos, cálculos e critérios fundamentaram a decisão.

11.2. Rejeição

O motivo deve ser objetivo, permitido e documentado. A comunicação ao cliente deve seguir a política da instituição e a legislação, evitando exposição indevida de mecanismos internos de risco.

11.3. Devolução

Use devolução quando o processo pode prosseguir após correção. Não use rejeição apenas para sinalizar um documento em falta.

11.4. Exceção

Uma exceção deve conter:

- regra ultrapassada;
- motivo de negócio;
- impacto e risco;
- medidas compensatórias;
- proponente e aprovador;
- prazo ou condição de validade;
- evidência na auditoria.

Exceção recorrente indica que a política ou o produto precisa ser revisto.

12. Contratos, carteira e prestações

12.1. Snapshot contratual

Condições relevantes devem ser preservadas no crédito/contrato. Alterar um produto no futuro não deve alterar retroativamente a obrigação existente.

12.2. Plano de pagamento

Cada prestação deve possuir número ou referência, vencimento, componentes financeiros, valor previsto, valor pago e estado. A soma e os saldos devem ser reconciliáveis com o crédito.

12.3. Composição financeira

Conforme o produto, uma prestação pode incluir capital, juros, comissões, impostos, penalidades e outros encargos autorizados. A ordem de imputação deve ser definida pela instituição e implementada de forma consistente.

12.4. Arredondamento e moeda

- cálculos devem usar representação monetária segura;
- arredondamentos devem ser determinísticos;
- diferenças residuais devem ser tratadas segundo política;

- valores de moedas distintas não devem ser somados sem conversão explícita;
- taxa de câmbio, quando aplicável, deve possuir fonte e data.

12.5. Liquidação antecipada

O valor de liquidação deve ser calculado para uma data de referência e considerar capital, juros vencidos, encargos e descontos permitidos. A simulação não encerra o crédito; apenas um pagamento confirmado e a atualização correspondente o fazem.

13. Pagamentos, recibos e estornos

13.1. Registo de pagamento

Antes de confirmar:

- localizar o crédito correto;
- validar pagador, valor, moeda, data, canal e referência;
- verificar duplicidade;
- confirmar conta de destino;
- informar observação quando necessário.

O sistema deve aplicar o pagamento segundo a regra vigente e atualizar saldos/prestações de forma consistente.

13.2. Pagamentos parciais, excedentes e retroativos

- pagamento parcial reduz a obrigação conforme a ordem de imputação;
- excedente deve seguir política de crédito, crédito futuro, saldo a favor ou devolução;
- pagamento retroativo exige data efetiva, justificação e tratamento financeiro consistente;
- valores sem crédito identificado devem permanecer em conta transitória ou procedimento equivalente, nunca ser imputados arbitrariamente.

13.3. Recibos

O recibo deve ser emitido somente após confirmação. Deve permitir identificar instituição, cliente, crédito, valor, moeda, data, canal, referência e componentes relevantes.

13.4. Estorno

Estorno é uma operação compensatória, não apagamento. Deve exigir motivo, referência ao movimento original, autorização adequada e reflexo em caixa, carteira, contabilidade e auditoria.

13.5. Idempotência e concorrência

Pagamentos, desembolsos, transferências, estornos e outras operações financeiras devem ser protegidos contra repetição, duplo clique, reenvio por rede e atualizações concorrentes.

14. Cobranças e gestão de atraso

14.1. Objetivo

Recuperar valores de forma diligente, respeitosa, documentada e compatível com a legislação e a política de tratamento do cliente.

14.2. Fluxo recomendado

1. identificar prestação e dias de atraso;
2. confirmar contactos e circunstâncias;
3. registar tentativa, canal, resultado e responsável;
4. obter promessa de pagamento quando aplicável;
5. acompanhar a promessa na data acordada;
6. escalar por faixa de atraso, exposição ou risco;
7. avaliar reestruturação apenas por processo formal;
8. preservar todas as evidências.

14.3. Regras de cobrança

- não alterar contactos históricos sem preservar a atualização;
- não prometer descontos ou perdões sem autorização;
- não ocultar atraso por pagamento fictício ou mudança manual de data;
- respeitar horários, privacidade e conduta profissional;
- tratar garantias e vias legais somente por procedimento autorizado;
- medir promessas cumpridas, recuperação e reincidência.

15. Reestruturação, refinanciamento e baixa

15.1. Reestruturação

Deve ocorrer apenas quando existe análise atualizada, justificação, aprovação, novo plano e documentação. O histórico original deve permanecer visível.

15.2. Refinanciamento

Quando implementado, deve ser distinguido de mera edição do crédito. O sistema e a política devem explicar como o crédito anterior é liquidado, transferido ou relacionado ao novo.

15.3. Baixa/write-off

Baixa contabilística não significa perdão automático da dívida. Deve possuir autoridade, motivo, tratamento contabilístico, estado de cobrança e evidência de auditoria.

16. Tesouraria e caixa

16.1. Contas e saldos

Cada movimento deve identificar conta, tipo, valor, moeda, data, referência, origem e utilizador. Saldos apresentados dependem da integridade dos movimentos e da reconciliação.

16.2. Abertura e fecho

Quando houver operação de caixa:

- confirmar saldo inicial;
- registar cada entrada e saída no momento correto;
- manter comprovativos;
- contar fisicamente no fecho;
- comparar saldo esperado e realizado;
- justificar e escalar diferenças;
- impedir alteração retroativa sem autorização.

16.3. Transferências

Transferências internas devem possuir origem, destino, valor, moeda, referência e efeito equilibrado. Não devem ser representadas como receita ou despesa sem fundamento.

16.4. Reconciliação

A reconciliação compara sistema, comprovativos e extratos externos. Diferenças devem ser classificadas, atribuídas, corrigidas e encerradas por responsável autorizado.

17. Contabilidade

O módulo contabilístico organiza contas, lançamentos, diário, razão, balancete e demonstrações disponíveis.

17.1. Princípios operacionais

- um evento financeiro deve produzir lançamentos coerentes;
- débitos e créditos devem permanecer equilibrados;
- períodos fechados não devem ser alterados informalmente;
- correções devem usar lançamentos de ajuste ou reversão;
- contas transitórias devem ser reconciliadas;
- integração entre carteira e contabilidade deve ser verificada regularmente.

17.2. Responsabilidade institucional

A instituição deve validar plano de contas, reconhecimento de juros, imparidade/provisões, impostos, write-off e mapas regulamentares com profissionais competentes. O software não substitui essa validação.

18. Risco, AML/KYC e garantias

18.1. Risco de crédito

Acompanhar exposição, concentração, atrasos, deterioração, exceções, garantias, capacidade de pagamento e desempenho por produto, segmento e período.

18.2. AML/KYC

Alertas podem resultar de dados incompletos, padrões incomuns ou critérios externos. Cada alerta deve possuir estado, responsável, análise, decisão e evidência. Casos sensíveis devem seguir o procedimento de escalonamento e confidencialidade.

18.3. Garantias

Registrar tipo, proprietário, descrição, valor, moeda, data de avaliação, documentos, localização, estado e vínculo. Reavaliações não devem apagar valores anteriores.

18.4. Indicadores recomendados

- carteira bruta e saldo em risco;
- PAR por faixa de atraso;
- taxa de aprovação e rejeição;
- tempo médio de decisão e desembolso;
- concentração por cliente, produto ou setor;
- cobertura por garantias;
- recuperações, reestruturações e write-offs;
- exceções por regra e aprovador;
- alertas AML abertos e tempo de resolução.

19. Documentos e gestão de evidências

19.1. Tipos

Identificação, comprovativos, formulários, análises, visitas, garantias, decisões, contratos, recibos, cartas, relatórios e evidências de integração.

19.2. Regras documentais

- classificar corretamente o documento;
- associar ao titular e processo correto;
- verificar legibilidade, validade e completude;
- restringir dados sensíveis;
- preservar versão e data quando relevante;
- não substituir evidência histórica sem trilha;
- eliminar somente segundo política de retenção e base legal.

19.3. Geração de documentos

A geração local ou remota deve usar dados confirmados. Documentos finais devem possuir identidade institucional consistente e, quando aplicável, número, data, responsável e referência ao processo.

20. Relatórios e exportações

O sistema pode disponibilizar exportações, registos, cartas, carta para o Banco de Moçambique, relatórios de créditos, clientes, financeiros e diversos.

20.1. Uso responsável

- confirmar período, moeda, filtros e estado;
- distinguir data de extração de data de referência;
- reconciliar números críticos com a fonte operacional;
- limitar distribuição a pessoas autorizadas;
- proteger ficheiros exportados fora do sistema;
- não editar um relatório e apresentá-lo como extração original;
- documentar critérios para mapas regulatórios.

20.2. Relatório não é controlo isolado

Um relatório pode revelar uma anomalia, mas a correção deve ocorrer no processo e registo de origem, com autorização e auditoria.

21. Pesquisa, interface e experiência operacional

21.1. Navegação

O menu é organizado por áreas operacionais, gestão e controlo. Itens não autorizados podem ser ocultados, mas a proteção real deve continuar no backend.

21.2. Pesquisa global

Use termos suficientemente específicos e confirme o identificador antes de agir. Pessoas com nomes semelhantes ou referências próximas podem causar operação no registo errado.

21.3. Estados de interface

Cada área deve comunicar carregamento, conteúdo, vazio, erro e sucesso. Uma tela vazia por falha não deve ser confundida com ausência real de dados.

21.4. Mensagens de erro

- leia a mensagem completa;
- evite repetir operação financeira sem confirmar o resultado;
- registre horário, utilizador, área, referência e passos;
- não envie credenciais, tokens ou documentos sensíveis em capturas;
- acione suporte quando o estado final não puder ser determinado.

22. Notificações, tarefas e prazos

Notificações ajudam a acompanhar documentos, decisões, vencimentos, promessas, alertas e operações. Não substituem revisão diária das filas críticas.

Uma tarefa deve possuir responsável, prazo, estado, prioridade, contexto e conclusão verificável. Reatribuições e atrasos importantes devem ser visíveis à supervisão.

23. Modo offline, pendências e sincronização

O Syscredi pode preservar operações locais pendentes para continuidade controlada.

23.1. Regras

- pendente local não significa confirmado no servidor;
- não repita uma operação financeira sem verificar o estado remoto;
- sincronize em rede confiável;
- trate conflitos de versão conscientemente;
- não altere relógio do dispositivo para manipular datas;
- evite operar a mesma entidade simultaneamente em vários dispositivos;
- revise e encerre a fila de pendências diariamente.

23.2. Conflitos

Quando duas versões competem, deve prevalecer a política de concorrência definida. Operações sensíveis não devem ser fundidas silenciosamente; exigem rejeição, reaplicação ou revisão.

24. Auditoria e rastreabilidade

Eventos relevantes devem permitir identificar:

- quem realizou a ação;
- quando ocorreu;
- organização e contexto;
- entidade afetada;
- estado anterior e posterior quando disponível;
- motivo, referência e resultado;
- origem técnica suficiente para investigação.

Logs são protegidos contra uso casual. Correções no negócio não devem apagar o facto histórico de que um erro ocorreu.

25. Privacidade e proteção de dados

25.1. Princípios

- finalidade específica;
- minimização de dados;
- acesso por necessidade;

- qualidade e atualização;
- retenção limitada;
- confidencialidade e integridade;
- responsabilização.

25.2. Conduta obrigatória

- não exportar dados para dispositivos ou contas pessoais;
- não partilhar credenciais;
- bloquear o ecrã quando se ausentar;
- evitar dados reais em testes e demonstrações;
- usar canais autorizados;
- reportar perda, exposição ou acesso indevido imediatamente;
- observar direitos do titular e obrigações locais.

26. Backups, continuidade e recuperação

- definir frequência, retenção, cifragem e responsáveis;
- manter cópias isoladas conforme risco;
- testar restauração, não apenas criação do backup;
- documentar RPO e RTO institucionais;
- incluir configurações, documentos e dependências externas;
- executar recuperação em ambiente controlado;
- validar integridade financeira após restauração.

Um backup nunca testado não é garantia de recuperação.

27. Integrações

Integrações podem abranger autenticação, Supabase/API, Vercel, bancos, mobile money, e-mail, armazenamento, assinatura e serviços externos.

27.1. Regras de integração

- credenciais e chaves secretas nunca devem estar no cliente ou Git;
- ambientes de desenvolvimento, homologação e produção devem ser separados;
- chamadas financeiras devem ser idempotentes;
- timeouts não devem ser tratados automaticamente como falha final;
- webhooks devem ser autenticados, deduplicados e auditados;
- falhas devem entrar em fila de reconciliação;
- contrato, versão e proprietário da integração devem ser documentados;
- indisponibilidade externa deve degradar de forma segura.

28. Administração do sistema

28.1. Utilizadores

O gestor cria, ativa, desativa e atribui perfis. Uma identidade sem perfil ativo não deve acessar dados. Nunca remova o último gestor válido sem plano de recuperação.

28.2. Definições institucionais

Marca, logótipo, cor, marca de água, rodapé e outros parâmetros afetam documentos e apresentação. Alterações devem ser revistas antes de publicação.

28.3. Produtos e políticas

Mudanças devem possuir vigência clara e avaliação de impacto. Créditos existentes precisam manter as condições contratadas.

28.4. Planos, subscrição e limites

A disponibilidade de capacidades pode depender do plano contratado. Expiração ou limitação deve ser tratada antes de interromper a operação crítica.

28.5. Backups e sincronização

A administração deve monitorizar execução, falhas, última conclusão válida e capacidade de restauração.

29. Rotinas operacionais recomendadas

29.1. Início do dia

- verificar autenticação, perfil e organização;
- confirmar conectividade e sincronização;
- rever caixa/saldos iniciais;
- consultar tarefas, pedidos, vencimentos e alertas AML;
- verificar falhas de integração ou backup;
- distribuir pendências e prioridades.

29.2. Durante o dia

- pesquisar antes de criar;
- validar dados antes de confirmar;
- anexar evidências ao processo correto;
- usar observações objetivas;
- não partilhar sessão;
- confirmar estados finais das operações;
- escalar exceções e alertas.

29.3. Fim do dia

- reconciliar pagamentos, caixa e desembolsos;

- rever operações pendentes ou falhadas;
- confirmar promessas e tarefas críticas;
- verificar diferenças e exceções;
- sincronizar e encerrar sessão;
- registrar incidente não resolvido para continuidade.

29.4. Rotina mensal

- rever acessos e utilizadores inativos;
- analisar carteira, PAR, concentração e exceções;
- reconciliar carteira, tesouraria e contabilidade;
- validar backups e teste de recuperação programado;
- rever produtos, limites e documentação;
- encerrar período conforme procedimento;
- acompanhar incidentes e ações corretivas.

30. Controlos-chave

Risco	Controlo mínimo
Cliente duplicado	Pesquisa prévia e procedimento de consolidação.
Aprovação indevida	Alçada, segregação e fundamento obrigatório.
Desembolso duplicado	Idempotência, autorização e reconciliação.
Pagamento no crédito errado	Confirmação de identificadores e recibo.
Fraude interna	Menor privilégio, dupla revisão e auditoria.
Alteração retroativa	Bloqueio, autorização e trilho de ajuste.
Perda de dados	Backup cifrado e restauração testada.
Vazamento	RLS/autorização, minimização e canais seguros.
Falha de integração	Retry controlado, deduplicação e reconciliação.
Relatório incorreto	Filtros documentados e reconciliação com origem.
Crédito fora de política	Validação automática ou exceção formal.
Atraso não tratado	Filas, tarefas, escalonamento e métricas.

31. Indicadores de gestão

A instituição deve definir metas, responsáveis e frequência para:

- pedidos recebidos, aprovados, rejeitados e pendentes;
- tempo de preparação, análise, decisão e desembolso;
- carteira ativa, desembolsos e reembolsos;
- PAR e montante vencido por faixa;
- pagamentos e promessas cumpridas;
- reestruturações, write-offs e recuperações;
- exposição e concentração;

- exceções de política;
- alertas AML e tempo de resolução;
- diferenças de caixa e reconciliação;
- incidentes, disponibilidade e sincronizações falhadas;
- qualidade cadastral e documentação vencida.

Indicadores devem possuir definição única. Alterar fórmula ou população exige registo de vigência para manter comparabilidade.

32. Gestão de incidentes

32.1. Exemplos

Acesso indevido, pagamento duplicado, saldo incoerente, falha de integração, documento exposto, indisponibilidade, perda de dispositivo, resultado financeiro desconhecido ou suspeita de fraude.

32.2. Resposta

1. proteger pessoas, dados e fundos;
2. interromper propagação sem destruir evidência;
3. registar horário, impacto, utilizadores e referências;
4. escalar ao responsável adequado;
5. reconciliar o estado real;
6. corrigir por procedimento autorizado;
7. comunicar conforme obrigação;
8. realizar causa raiz e ação preventiva.

Não tente “limpar” logs ou apagar registos para ocultar o incidente.

33. Resolução de problemas

Sintoma	Verificação recomendada
Não entra	Credenciais, convite, recuperação, perfil ativo, organização e conectividade.
Menu ausente	Perfil, estado, subscrição e permissões.
Dados vazios	Filtros, organização, rede, erro de carregamento e sincronização.
Operação repetida	Pesquisar pelo identificador antes de reenviar.
Documento não abre	Permissão, ligação, origem e disponibilidade do ficheiro.
Valor divergente	Produto, data, moeda, taxa, arredondamento, movimentos e estornos.
Saldo não atualiza	Estado remoto, fila local, concorrência e reconciliação.
Relatório divergente	Data de referência, filtros, estado e fonte de verdade.
Sessão expira	Voltar a autenticar; não repetir operação sensível sem confirmar.

Ao contactar suporte, forneça área, referência, horário, ação, resultado esperado e observado. Remova palavras-passe, tokens e dados pessoais desnecessários.

34. Checklist de entrada em produção

34.1. Segurança e acesso

- ☐ perfis, menor privilégio e segregação validados;
- ☐ RLS/autorização remota testada por organização;
- ☐ MFA e recuperação avaliados;
- ☐ segredos fora do cliente e repositório;
- ☐ revisão de acessos e resposta a incidente documentadas.

34.2. Crédito e documentos

- ☐ produtos, limites, taxas e arredondamentos aprovados;
- ☐ ciclo operador → avalista → gestor testado;
- ☐ exceções e alçadas configuradas;
- ☐ contratos, recibos e cartas revistos juridicamente;
- ☐ casos de rejeição, devolução, reestruturação e liquidação testados.

34.3. Financeiro e contabilístico

- ☐ desembolso e pagamento protegidos contra duplicação;
- ☐ caixa, contas e reconciliação testados;
- ☐ estornos e ajustes exigem autorização;
- ☐ lançamentos e relatórios conciliados;
- ☐ plano de contas e tratamento regulatório aprovados.

34.4. Dados e continuidade

- ☐ migração e qualidade de dados validadas;
- ☐ backups cifrados e restauração testada;
- ☐ retenção e privacidade aprovadas;
- ☐ modo offline e conflitos testados;
- ☐ monitorização, suporte, RPO e RTO definidos.

34.5. Plataformas e operação

- ☐ builds assinados e associados ao commit correto;
- ☐ web, Android, iOS/macOS e Windows validados conforme escopo;
- ☐ formação concluída por perfil;
- ☐ procedimentos diários e mensais aprovados;
- ☐ piloto controlado concluído antes da escala.

35. Formação por perfil

Perfil	Formação obrigatória
Gestor	Governança, acessos, produtos, alçadas, risco, finanças, auditoria e continuidade.
Operador	Cadastro, documentação, pedido, qualidade de dados, privacidade e pendências.
Avalista	Análise financeira, risco, AML/KYC, garantias, decisão e exceções.
Fiador com acesso	Consulta própria, documentos, obrigações e segurança da conta.
Finanças/contabilidade	Caixa, pagamentos, estornos, reconciliação, lançamentos e fecho.
Suporte	Diagnóstico seguro, auditoria, privacidade, escalonamento e continuidade.

A formação deve incluir casos práticos e avaliação de competência, não apenas apresentação do menu.

36. Governança do handbook

- proprietário: gestão do produto/operação;
- revisores: crédito, risco, compliance, finanças, jurídico, tecnologia e suporte;
- periodicidade: pelo menos semestral ou a cada mudança material;
- mudanças: registrar versão, data, autor, resumo e aprovação;
- distribuição: disponibilizar edição vigente e arquivar edições anteriores;
- conflito: políticas aprovadas e legislação prevalecem sobre texto desatualizado.

37. Glossário

Termo	Significado
AML	Prevenção ao branqueamento de capitais.
KYC	Conhecimento e verificação do cliente.
PAR	Carteira em risco a partir de determinada faixa de atraso.
RLS	Segurança por linha no backend/base de dados.
RPO	Perda máxima de dados tolerada medida no tempo.
RTO	Tempo objetivo para recuperação do serviço.
Alçada	Limite de autoridade para aprovar ou executar.
Carência	Período definido antes de determinada cobrança.
Idempotência	Repetição segura sem duplicar o efeito.
Imputação	Aplicação do pagamento aos componentes da dívida.
Write-off	Baixa contabilística segundo política aprovada.
Reconciliação	Comparação de fontes para explicar e corrigir diferenças.
Tenant	Organização isolada logicamente no sistema.

38. Regras de ouro

1. Pesquise antes de criar.
2. Confirme antes de movimentar dinheiro.
3. Nunca partilhe credenciais.
4. Não contorne estados ou autorizações.

5. Documente decisões e exceções.
6. Não apague história financeira.
7. Trate um timeout como resultado desconhecido até reconciliar.
8. Mantenha contrato, crédito e movimentos coerentes.
9. Escale alertas de risco e privacidade.
10. Em dúvida, pare a operação sensível e peça revisão.

39. Referências técnicas internas

- README.md
- APP_ARCHITECTURE.md
- docs/CLEAN_ARCHITECTURE.md
- docs/INTEGRATION_E2E_CHECKLIST.md
- docs/INTERFACE.md
- docs/LOCALIZATION.md
- docs/PRODUCT_READINESS.md
- docs/SUPABASE.md
- lib/app/bootstrap/composition.dart
- lib/app/config/config.dart
- lib/features/api/domain/repository.dart
- lib/features/api/presentation/navigation.dart

Nota institucional final: antes de utilizar o Syscredi para operação financeira real, a instituição deve validar segurança, RLS, MFA, contratos, cálculos, contabilidade, relatórios regulamentares, integrações, backups, reconciliação e conformidade com a legislação aplicável em Moçambique e em qualquer outra jurisdição onde opere.