	Versão	Data de criação	Data de atualização	Autor	Revisado por	Aprovado por /data	Descrição das alterações
moneria	1.0	24/07/2025		José Souza	Andrey Santos	David Santos	[inserir descrição]
	1.2		16/02/2026	José Souza	Compliance	David Santos	Atualização Padrão

Controle de acesso:

Cargo ou função	Acesso permitido (somente leitura, ler e editar/atualizar)
Diretoria, Andrey, Consultoria JS	Ler e editar/atualizar
Diretoria	Leitura e aprovação
Colaboradores	Leitura

Observações: [inserir quaisquer observações relevantes sobre a política]

POLÍTICA DE DUE DILIGENCE DE FORNECEDORES E TERCEIROS

Sumário

1. OBJETIVO

Estabelecer diretrizes, critérios, metodologia e controles para realização de Due Diligence de fornecedores e terceiros, assegurando que riscos operacionais, tecnológicos, regulatórios, reputacionais e de segurança da informação sejam devidamente avaliados antes e durante a contratação.

2. ABRANGÊNCIA

Esta política aplica-se a:

a. Todos os fornecedores e prestadores de serviço
b. Parceiros tecnológicos e operacionais
c. Provedores de serviços em nuvem (AWS, SaaS, etc.)
d. Terceiros com acesso a dados, sistemas ou infraestrutura
e. Fornecedores envolvidos com Pix, SPI, STR e CDE

3. REFERÊNCIAS NORMATIVAS

Regulação

a. Resolução CMN nº 4.658/2018
b. Resolução CMN nº 5.274/2025
c. Resolução BCB nº 538/2025
d. Lei nº 13.709/2018 (LGPD)

Padrões Técnicos

a. ISO/IEC 27001 e 27002
b. ISO/IEC 27701
c. PCI DSS v4.0.1
d. NIST SP 800-53 / 800-161 (Supply Chain Risk)

4. DEFINIÇÕES

Due Diligence: processo estruturado de avaliação prévia de riscos antes da contratação.

Fornecedor crítico: fornecedor cujo impacto afeta diretamente operações essenciais.

Risco de terceiros: risco decorrente da dependência de entidades externas.

5. PRINCÍPIOS

A Moneria adota:

a. Avaliação obrigatória antes da contratação

b. Abordagem baseada em risco (risk-based)

c. Responsabilidade indelegável

d. Avaliação contínua (não pontual)

e. Proporcionalidade ao nível de risco

f. Evidência auditável

6. CLASSIFICAÇÃO DE RISCO DO FORNECEDOR

Antes da due diligence, o fornecedor deve ser classificado:

6.1 Critérios de Classificação

a. Acesso a dados sensíveis

b. Impacto operacional

c. Integração com sistemas críticos

d. Dependência tecnológica

e. Relevância para continuidade do negócio

6.2 Níveis de Risco

Nível	Descrição
Crítico	Impacto direto em Pix, CDE, core ou operação
Alto	Acesso a dados sensíveis ou sistemas críticos
Médio	Impacto operacional moderado
Baixo	Impacto limitado

7. ETAPAS DA DUE DILIGENCE

7.1 Coleta de Informações

a. Dados cadastrais e societários

b. Estrutura organizacional

c. Histórico e reputação

d. Situação financeira

7.2 Avaliação de Segurança da Informação

a. Políticas de segurança implementadas

b. Certificações (ISO 27001, SOC 2, PCI DSS)

c. Controles de acesso e IAM

d. Criptografia e proteção de dados

e. Gestão de vulnerabilidades

7.3 Avaliação de Privacidade (LGPD)

a. Existência de DPO

b. Políticas de privacidade

c. Tratamento de dados pessoais

d. Transferência internacional de dados

7.4 Avaliação de Continuidade de Negócios

a. Existência de PCN/DRP

b. Testes de continuidade

c. Redundância de infraestrutura

7.5 Avaliação de Compliance e Regulação

a. Conformidade com BACEN (quando aplicável)

b. Conformidade com PCI DSS

c. Aderência a requisitos legais

7.6 Avaliação Técnica (quando aplicável)

a. Arquitetura tecnológica

b. Segurança de APIs

c. Configuração de cloud

d. Logs e monitoramento

8. QUESTIONÁRIO DE DUE DILIGENCE

A Moneria deve aplicar questionário estruturado contendo:

a. Segurança da informação

b. Privacidade de dados

c. Gestão de acessos

d. Resposta a incidentes

e. Continuidade de negócios

f. Governança e compliance

9. ANÁLISE E CLASSIFICAÇÃO DE RISCO

Após avaliação:

a. Atribuir score de risco

b. Identificar vulnerabilidades

c. Classificar fornecedor

d. Definir necessidade de mitigação

10. DECISÃO DE CONTRATAÇÃO

A contratação deve considerar:

a. Nível de risco identificado

b. Capacidade de mitigação

c. Controles existentes

d. Aprovação formal das áreas responsáveis

11. PLANOS DE MITIGAÇÃO

Quando necessário:

a. Definir controles adicionais

b. Exigir adequações do fornecedor

c. Estabelecer prazos

d. Monitorar implementação

12. REQUISITOS PARA FORNECEDORES CRÍTICOS

Devem atender a:

a. Avaliação completa e aprofundada

b. Evidências documentadas

c. Controles técnicos validados

d. Auditorias periódicas

e. Monitoramento contínuo

13. REAVALIAÇÃO PERIÓDICA

A Moneria deve:

a. Reavaliar fornecedores periodicamente

b. Atualizar classificação de risco

c. Revisar controles

d. Monitorar mudanças relevantes

14. MONITORAMENTO CONTÍNUO

Inclui:

a. Avaliação de performance

b. Monitoramento de incidentes

c. Revisão de SLA

d. Análise de risco contínua

15. EVENTOS DE REAVALIAÇÃO IMEDIATA

Deve ocorrer nova due diligence em caso de:

a. Incidente de segurança

b. Mudança relevante no fornecedor

c. Alteração contratual significativa

d. Aquisição ou fusão

16. DOCUMENTAÇÃO E EVIDÊNCIAS

Devem ser mantidos:

a. Questionários respondidos

b. Relatórios de avaliação

c. Classificação de risco

d. Planos de mitigação

e. Aprovações formais

17.INTEGRAÇÃO COM CONTRATOS

A due diligence deve resultar em:

a. Cláusulas contratuais específicas

b. Requisitos de segurança

c. SLA definidos

d. Direito de auditoria

18. AUDITORIA E CONFORMIDADE

O processo está sujeito a:

a. Auditorias internas

b. Auditorias externas (BACEN, PCI)

c. Revisões regulatórias

19. RESPONSABILIDADES

Segurança da Informação

a. Conduzir avaliação técnica

Compliance

a. Avaliar riscos regulatórios

Jurídico

a. Validar cláusulas contratuais

Área Demandante

a. Justificar contratação

20. RESPONSABILIZAÇÃO

A contratação sem due diligence adequada pode resultar em:

a. Risco operacional elevado

b. Não conformidade regulatória

c. Responsabilização interna

d. Sanções regulatórias

21. REVISÃO E ATUALIZAÇÃO

Esta política será:

a. Revisada anualmente

b. Atualizada conforme evolução regulatória

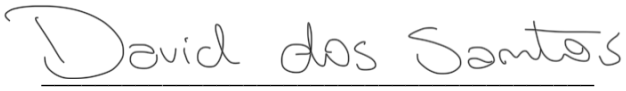
22. APROVAÇÃO E VIGÊNCIA

Aprovada pela Alta Administração da Moneria.

23. ANEXOS

a. ANEXO I - QUESTIONÁRIO DE DUE DILIGENCE DE FORNECEDORES
b. ANEXO II – MATRIZ DE RISCO DE FORNECEDORES (SCORE)
c. ANEXO II – MATRIZ DE RISCO DE FORNECEDORES (SCORE)
d. ANEXO IV – CHECKLIST BACEN PARA TERCEIRIZAÇÃO CRÍTICA

Aracaju/SE, 16 de fevereiro de 2026



David dos Santos
Diretoria

ANEXO I – QUESTIONÁRIO DE DUE DILIGENCE DE FORNECEDORES

1. INFORMAÇÕES GERAIS

a. Razão Social:

b. CNPJ:

c. País de operação:

d. Tempo de mercado:

e. Tipo de serviço prestado:

2. GOVERNANÇA E ESTRUTURA

a. Possui área formal de Segurança da Informação? ( ) Sim ( ) Não

b. Possui CISO ou responsável designado?

c. Possui políticas formais documentadas?

3. SEGURANÇA DA INFORMAÇÃO

a. Possui certificação ISO 27001? ( ) Sim ( ) Não

b. Possui SOC 2? ( ) Sim ( ) Não

c. Possui política de controle de acesso (IAM)?

d. MFA é obrigatório?

e. Possui gestão de logs (SIEM)?

4. PROTEÇÃO DE DADOS (LGPD)

a. Possui DPO?

b. Possui política de privacidade?

c. Realiza transferência internacional de dados?

d. Possui registro de tratamento de dados?

5. SEGURANÇA TÉCNICA

a. Dados são criptografados em repouso?

b. Dados são criptografados em trânsito?

c. Possui gestão de vulnerabilidades?

d. Realiza pentests?

6. CONTINUIDADE DE NEGÓCIOS

a. Possui PCN/DRP?

b. Frequência de testes de continuidade:

c. Possui redundância geográfica?

7. INCIDENTES DE SEGURANÇA

a. Possui plano de resposta a incidentes?

b. Já sofreu incidentes relevantes nos últimos 24 meses?

c. Tempo médio de resposta a incidentes:

8. CLOUD E INFRAESTRUTURA

a. Utiliza AWS/Azure/GCP?

b. Possui segregação de ambientes?

c. Logs estão habilitados (ex: CloudTrail)?

9. CONFORMIDADE PCI DSS (SE APLICÁVEL)

a. É certificado PCI DSS?

b. Escopo inclui CDE?

c. Possui tokenização?

10. DECLARAÇÃO

Declaro que as informações fornecidas são verdadeiras.

Assinatura: _____

ANEXO II – MATRIZ DE RISCO DE FORNECEDORES (SCORE)

Modelo de Avaliação

Critério	Peso	Score (1–5)	Resultado
Acesso a dados sensíveis	5		
Impacto operacional	5		
Integração com sistemas críticos	5		
Dependência do serviço	4		
Maturidade de segurança	4		
Conformidade regulatória	5		
Histórico de incidentes	4		

Cálculo

Score Final = Σ (Peso x Score)

Classificação

Score	Classificação
90–100	Crítico
70–89	Alto
40–69	Médio
<40	Baixo

Ação Recomendada

a. Crítico → Due diligence completa + auditoria contínua
b. Alto → Controles adicionais
c. Médio → Monitoramento periódico
d. Baixo → Controle básico

ANEXO III – MODELO DE RELATÓRIO DE AVALIAÇÃO DE FORNECEDOR

1. IDENTIFICAÇÃO

a. Fornecedor:

b. Serviço:

c. Data da avaliação:

2. CLASSIFICAÇÃO DE RISCO

a. Classificação: ( ) Crítico ( ) Alto ( ) Médio ( ) Baixo

b. Score: _____

3. PRINCIPAIS RISCOS IDENTIFICADOS

a. Risco 1:

b. Risco 2:

c. Risco 3:

4. CONTROLES EXISTENTES

a. Segurança da informação:

b. LGPD:

c. Continuidade:

d. Infraestrutura:

5. GAPs IDENTIFICADOS

a. Gap 1:

b. Gap 2:

c. Gap 3:

6. PLANO DE MITIGAÇÃO

Ação - Responsável - Prazo

7. DECISÃO FINAL

a. ( ) Aprovado

b. ( ) Aprovado com ressalvas

c. ( ) Reprovado

8. APROVAÇÕES

a. Segurança: _____

b. Compliance: _____

c. Jurídico: _____

ANEXO IV – CHECKLIST BACEN PARA TERCEIRIZAÇÃO CRÍTICA

1. GOVERNANÇA

a. Fornecedor classificado como crítico
b. Avaliação de risco formal realizada
c. Aprovação da alta administração

2. CONTRATO

a. Cláusula de confidencialidade
b. Cláusula LGPD
c. SLA definido
d. Direito de auditoria
e. Notificação de incidentes

3. SEGURANÇA

a. IAM implementado
b. Criptografia ativa
c. Logs e monitoramento
d. Gestão de vulnerabilidades

4. CONTINUIDADE

a. PCN validado
b. DRP testado
c. Redundância garantida

5. CLOUD (SE APLICÁVEL)

a. Modelo de responsabilidade compartilhada definido
b. Controles de segurança cloud avaliados
c. Logs ativos

6. MONITORAMENTO

a. SLA monitorado
b. Revisão periódica
c. Auditorias realizadas

7. INCIDENTES

a. Processo de notificação definido

b. Tempo de resposta acordado

c. Integração com resposta da Moneria

8. ENCERRAMENTO

a. Revogação de acessos

b. Exclusão de dados

c. Evidência documentada