M A N U A L

Selo ABECS
de Conformidade

(Atualização de 04.03.2024)

Sumário

I. DAS DISPOSIÇÕES PRELIMINARES 3
II. DAS SÉRIES DO SELO 3
III. DOS REQUISITOS DE CONFORMIDADE 4
IV. DOS REQUISITOS DE CONFORMIDADE ESPECÍFICOS 5
V. DO PROCESSO DE AVALIACAO 12
VI. DOS CRITÉRIOS DE APROVAÇÃO 13
VII. DOS PRAZOS, CONDIÇÕES DE OBTENÇÃO E DE VALIDADE DO SELO 13
VIII. DA DIVULGAÇÃO 15
IX. DO CONTROLE DOS PRAZOS 15
X. DAS DISPOSIÇÕES FINAIS 15

I. DAS DISPOSIÇÕES PRELIMINARES

I.1. A Associação Brasileira das Empresas de Cartões de Crédito e Serviços – ABECS, associação civil sem fins lucrativos, que representa instituições e entidades atuantes no mercado de cartões de crédito e serviços, com base nas Políticas Institucionais aprovadas por seus associados, concebidas com o propósito de contribuir com o aperfeiçoamento das melhores práticas e o com o fortalecimento desse mercado, e objetivando o integral alinhamento às exigências previstas na Resolução n° 150, de 6 de outubro de 2021, do Banco Central do Brasil (BCB) – que consolida normas sobre os arranjos de pagamento e aprova o regulamento que disciplina a prestação de serviço de pagamento no âmbito dos arranjos de pagamento integrantes do Sistema de Pagamentos Brasileiro (SPB), instituiu o **Selo ABECS de Conformidade** (ou simplesmente **Selo**), para que as instituições autorizadas a operar nesse mercado, e seus agentes, possam comprovar a plena aderência a esses dispositivos. O processo de concessão do Selo será regido com base nas disposições do presente Manual.

II. DAS SÉRIES DO SELO

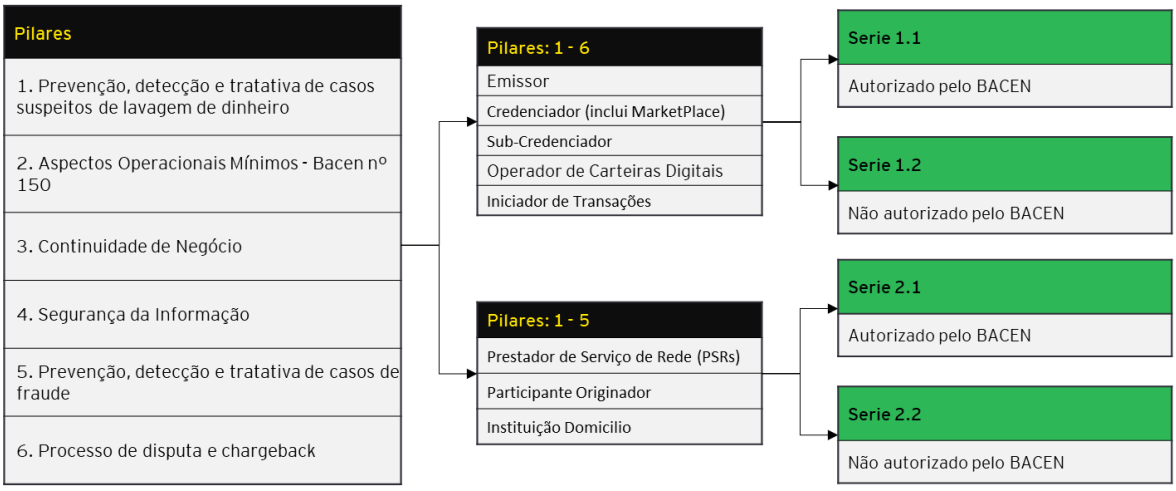
II.1. O Selo, destinado às instituições participantes de arranjos de pagamento e aos seus parceiros nas operações nos meios de pagamento, terá 4 séries principais, sem prejuízo da existência futura de outras:

- Série 1.1 destinada a Emissores, Credenciadores, Sub-Credenciadores, Operadores de Carteiras Digitais e Iniciador de Transações **autorizados** pelo BACEN;

- Série 1.2 destinada a Emissores, Credenciadores, Sub-Credenciadores, Operadores de Carteiras Digitais e Iniciador de Transações **não autorizados** pelo BACEN;

- Série 2.1 Prestador de Serviço de Rede (PSRs), Participantes Originadores e Instituições Domicílios **autorizados** pelo BACEN; e

- Série 2.2 Prestador de Serviço de Rede (PSRs), Participantes Originadores e Instituições Domicílios **não autorizados** pelo BACEN.



II.2. Os não autorizados serão sujeitos a menos requisitos devido à não obrigatoriedade de algumas exigências do BACEN direcionadas aos autorizados. Isso inclui aspectos como avaliação interna de riscos, comunicação ao COAF, acompanhamento de controles de participantes não autorizados pelo BACEN, relatório de efetividade, relatório de avaliação de limites máximos para risco de fraude, e avaliação de efetividade dos mecanismos de compartilhamento de dados e existência de auditoria interna.

II.3. Os prazos para a obtenção do respectivo Selo e as datas limites para que a instituição ou a entidade esteja em conformidade com os respectivos requisitos serão tratados no Capítulo VII deste Manual.

III. DOS REQUISITOS DE CONFORMIDADE

III.1. Para cada Série do Selo serão definidos requisitos de conformidade específicos, a serem aferidos de forma a comprovar a existência e a adequação dos procedimentos e requerimentos sobre os arranjos de pagamento do participante ou dos seus correspondentes, e o cumprimento das normas do Banco Central, estritamente aplicados às operações de meios de pagamento.

III.2. Esses requisitos serão divulgados previamente à data de implementação da respectiva Série, e refletidos no Capítulo a seguir.

IV. DOS REQUISITOS DE CONFORMIDADE ESPECÍFICOS

IV.1. Os temas de conformidade a serem aferidos para a obtenção do Selo, serão avaliados com base no seguinte Roteiro:

1. **Aspectos Operacionais Mínimos – Resolução BCB nº 150**: o instituidor deve avaliar e estabelecer procedimentos, bem como definir requerimentos para a atuação dos participantes no seu arranjo, conforme estipulado no Artigo 4º.

    a. Credenciamento por bandeira.

    b. Estrutura de avaliação de riscos.

    c. Aprovação e divulgação da Política de Gerenciamento de Riscos.

    d. Responsável pela avaliação de riscos e segregação da gestão de riscos.

    e. Acompanhamento de indicadores de risco.

    f. Processo de tratativa de riscos identificados.

    g. Mecanismo de fluxo de recursos entre Arranjos de Pagamento.

    h. Processo claro de iniciação de transações de pagamento.

    i. Oferta padronizada de pagamento via QR Code.

    j. Envio de propostas e sugestões ao instituidor.

    k. Colaboração na compensação e liquidação de ordens.

    l. Conformidade às regras estabelecidas.

    m. Procedimento de conciliação entre participantes e monitoramento dos processos de conciliação.

    n. Testes de integridade na mensageria e políticas para divergências nas informações.

    o. Treinamentos para conciliação de transações e atualização de informações para clientes.

    p. Treinamento para fornecimento claro de informações aos clientes e monitoramento de disponibilidade e desempenho dos sistemas.

    q. Mecanismos de alerta em falhas nos serviços e análise de riscos e medidas

preventivas.

r. Monitoramento da disponibilidade dos sistemas e acordos de nível de serviço com provedores.

s. Políticas de atualização e melhoria dos sistemas e revisões internas de garantia de disponibilidade.

t. Utilização de sistema de reconciliação e procedimentos para correção de erros.

u. Manutenção de registros e auditorias internas.

2. **Prevenção à Fraude**: Aplicação das Resoluções CMN 4.753, Conjunta nº 6 e CMN 4.859 é necessária para estabelecer procedimentos eficazes de acompanhamento e detecção de fraudes em cada instituição participante, garantindo a integridade do sistema

   a. Equipe estruturada de prevenção à fraude e sinergia na governança para prevenção de fraude.

   b. Treinamentos periódicos sobre prevenção a fraudes e divulgação da política de prevenção de fraudes.

   c. Política de monitoramento, controle e prevenção de fraudes e aprovação da política de prevenção de fraudes.

   d. Procedimento de abertura de conta/relacionamento e restrição inicial para qualificação simplificada.

   e. Procedimento de monitoramento de transações e procedimento de bloqueio de recursos.

   f. Canal dedicado para denúncias de fraudes e histórico de ocorrências de fraude.

   g. Consideração de indicadores de fraude nos riscos operacionais e revisão de ocorrências de fraude.

   h. Controles nos participantes para redução de fraudes e controles de fraudes de agentes e terceiros.

   i. Sistema de prevenção a fraudes e formalização de regras e parâmetros.

   j. Monitoramento de redes sociais e sites suspeitos e utilização de serviços de inteligência.

   k. Revisão periódica das regras de prevenção a fraudes e testes de integridade

do sistema de prevenção a fraudes.

l. Sistema eletrônico de acesso a dados compartilhados sobre fraudes e autenticação e criptografia dos dados compartilhados.

m. Testes de intrusão no sistema de compartilhamento de dados e trilha de auditoria no sistema de compartilhamento de dados.

n. Acordos de níveis de serviço do sistema de compartilhamento de dados e relatórios gerenciais de limites máximos para mitigação de riscos.

o. Avaliação de efetividade dos mecanismos de controle e avaliação do processo de prevenção a fraudes pela Auditoria Interna.

p. Armazenamento de informações sobre conformidade, documentações, resultados de testes, acordos de níveis de serviço e mecanismos de controle.

3. **Continuidade de Negócios**: Aplicação das Resoluções 4.893 e 4.557, juntamente com as normas ISO/IEC 22301 para estabelecer práticas eficazes de controle de continuidade de negócios, assegurando a resiliência operacional.

    a. Plano de Continuidade/Contingência de Negócios aprovado pela alta administração e testes periódicos.

    b. Frequência de revisão da Política de Continuidade dos Negócios e contratação de serviços em nuvem (Cloud).

    c. Realização de *backups* frequentes e testes de restauração das mídias produzidas.

    d. Testes independentes da operacionalidade do Processo de Continuidade dos Negócios e definição de papéis e responsabilidades.

    e. Comunicação ao Contratante em caso de acionamento da contingência e redundância nos links de comunicação.

    f. Implementação de Análise de Impacto nos Negócios (BIA) e periodicidade de atualização.

4. **PLD/FT**: Aplicação da Resolução 3.978 para avaliar procedimentos e controles eficazes na prevenção à lavagem de dinheiro e no combate ao financiamento do terrorismo

    a. Existência de políticas e procedimentos de prevenção à lavagem de dinheiro e ao financiamento do terrorismo (PLD/FT).

b. Aprovação da Política de PLD/FT pelo Conselho de Administração ou Diretoria.

c. Divulgação da Política de PLD/FT para todos os funcionários, parceiros e prestadores de serviços terceirizados.

d. Abrangência da política de PLD/FT, incluindo definição de papéis, procedimentos para novos produtos/serviços, avaliação interna de risco e promoção da cultura organizacional de PLD/FT.

e. Formalização das atribuições da área de PLD/FT em manual, com descrição detalhada da estrutura.

f. Indicação ao Banco Central do diretor responsável pelo PLD/FT no Sisbacen.

g. Funções adicionais do Diretor responsável pelo PLD/FT dentro da instituição.

h. Realização de treinamento em PLD/FT, sanções, anticorrupção e ética aos colaboradores.

i. Cobertura do treinamento de PLD/FT, anticorrupção e ética para todos os funcionários.

j. Treinamento de parceiros, prestadores de serviços e terceiros para cumprimento das políticas de PLD/FT.

k. Inclusão de cláusulas de PLD/CFT e anticorrupção nos contratos formalizados.

l. Realização da Avaliação Interna de Riscos nos últimos 24 meses.

m. Aprovação e encaminhamento da Avaliação Interna de Riscos.

n. Metodologia da Avaliação Interna de Riscos conforme Circular 3.

o. Definição de categorias de risco e controles correspondentes.

p. Possuir manual de procedimentos de KYC conforme Circular 3.

q. Atualização tempestiva do manual de procedimentos de KYC.

r. Aprovação do manual de procedimentos de KYC pela diretoria.

s. Detalhamento dos procedimentos diferenciados por categorias de risco.

t. Coleta de informações em operações envolvendo residentes ou empresas

no exterior.

u. Procedimentos de qualificação do cliente, incluindo verificação de PEP.

v. Procedimentos de identificação dos clientes, incluindo coleta de informações.

w. Procedimentos de qualificação e classificação dos clientes, incluindo verificação PEP.

x. Manutenção de registros e guarda de documentos comprobatórios.

y. Procedimentos para detecção de operações atípicas ou irregulares.

z. Possuir manual de procedimentos de MSAC conforme Circular 3.

aa. Atualização tempestiva do manual de procedimentos de MSAC.

bb. Considerar os requerimentos em relação aos procedimentos de monitoramento e seleção.

cc. Considerar os requerimentos em relação aos procedimentos de análise de operações suspeitas.

dd. Considerar os requerimentos em relação aos procedimentos de comunicação de operações em espécie.

ee. Considerar os requerimentos em relação aos procedimentos de comunicação de operações suspeitas.

ff. Aprovação do manual de procedimentos de MSAC pela diretoria.

gg. Estabelecimento de parâmetros para identificação de operações suspeitas.

hh. Controle das decisões de comunicação ao COAF.

ii. Quantidade de operações/situações alertadas e analisadas.

jj. Quantidade de operações/situações comunicadas ao COAF nos últimos 12 meses.

kk. Acompanhamento dos controles de participantes não autorizados pelo BACEN.

ll. Estabelecimento de indicadores de acompanhamento dos participantes não autorizados.

mm. Utilização de ferramentas para verificação contínua de clientes frente a

lista de sancionados.

nn. Testes de integridade periódicos das ferramentas de verificação contínua.

oo. Tratamento automático de alertas com base em critérios de risco.

pp. Possuir manual de procedimentos de KYE conforme Circular 3.

qq. Aprovação do manual de procedimentos de KYE pela diretoria.

rr. Procedimentos de identificação, qualificação e classificação da atividade do funcionário.

ss. Possuir manual de procedimentos de KYS conforme Circular 3.

tt. Aprovação do manual de procedimentos de KYS pela diretoria.

uu. Procedimentos de identificação, qualificação e classificação da atividade do fornecedor.

vv. Possuir manual de procedimentos de KYP conforme Circular 3.

ww. Aprovação do manual de procedimentos de KYP pela diretoria.

xx. Procedimentos de identificação, qualificação e classificação da atividade do parceiro.

yy. Parceiros em empresas de cripto, extração de minério ou localizados em regiões de fronteira.

zz. Possuir Plano Anual de Auditoria Interna ou revisão realizado nos últimos 12 meses.

aaa. Auditorias dos parceiros/terceiros no PI.

5. **Segurança da Informação**: Aplicação das normas ISO 27001:2013, NIST, Cobit, ITIL e as diretrizes do PCI Council é essencial para avaliar a segurança da informação, abrangendo desde a gestão de riscos até as melhores práticas operacionais.

    a. Existência e implementação de políticas abrangentes de segurança da informação, gestão de acesso, gestão de mudanças, *cybersecurity*, gestão de incidentes e operações de TI.

    b. Uso de criptografia em várias frentes, incluindo armazenamento de senhas, envio de e-mails e conexões HTTPS/TLS.

    c. Monitoramento contínuo de eventos críticos de segurança e detecção de

ataques em sistemas de rede.

d. Implementação de *firewalls*, soluções de proteção de e-mail e prevenção de perda de dados (DLP).

e. Gestão eficaz de incidentes de cibersegurança e procedimentos de comunicação.

f. Plano e testes regulares de invasão para identificar e tratar vulnerabilidades.

g. Controle rigoroso de acessos, com revisões periódicas e segregação de funções.

h. Utilização de trilhas de auditoria em sistemas e bancos de dados, além de parâmetros mínimos para senhas e perfis administrativos autorizados.

i. Procedimentos robustos para registro, validação e homologação de mudanças, *backup* e *restore* de dados.

j. Certificação PCI DSS para garantir a segurança de transações financeiras e presença de terminais de pagamento seguros.

k. Uso de criptografia e HSM para proteger chaves transacionais e dados sensíveis.

l. Treinamentos regulares em segurança da informação para conscientização dos colaboradores.

m. Varreduras periódicas de vulnerabilidades e definição de SLAs para correção.

n. Manutenção de inventário de ativos e controles de segurança para dispositivos móveis.

o. Implementação de duplo fator de autenticação e processos de desenvolvimento seguro de *software*.

6. **Disputas e *Chargeback***: Avaliação dos controles previstos nos regulamentos dos instituidores dos arranjos de pagamento.

a. Existência de uma equipe estruturada de disputas e *chargeback.*

b. Atualização dos colaboradores envolvidos por meio de treinamentos e comunicações.

c. Existência de uma política de Contestações.

d. Existência de procedimento de registro de disputas e *chargeback.*

e. Aprovação da política/procedimentos pelo Conselho de Administração ou Diretoria.

f. Divulgação da política de disputas e *chargeback* para todos os funcionários.

g. Divulgação dos procedimentos apenas aos colaboradores envolvidos.

h. Canal dedicado para o recebimento de contestações.

i. Existência de histórico de disputas e *chargeback.*

j. Processo de revisão de disputas e *chargeback.*

k. Consideração dos indicadores na avaliação de riscos e penalidades.

l. Geração de indicadores para avaliar eficiência no processo.

m. Utilização de sistema próprio automatizado.

n. Revisão e ajuste dos sistemas conforme as regras dos instituidores dos arranjos de pagamento.

V. DO PROCESSO DE AVALIAÇÃO

V.1. A avaliação dos requisitos de conformidade será feita por empresa de avaliação independente, selecionada e credenciada pela ABECS anualmente dentre aquelas de reconhecida capacidade técnica e experiência comprovada, de forma a garantir o menor custo, para a instituição de pagamento, a uniformidade e a isonomia no processo de coleta de informações e de avaliação.

V.2. As informações sobre as empresas credenciadas, para o processo de avaliação de cada Série, serão divulgadas pela ABECS, na página **www.certificacaoabecs.org.br.**

V.3. Para dar início ao processo de avaliação a instituição ou entidade deverá encaminhar previamente à ABECS manifestação formal de interesse na obtenção do Selo, por intermédio de link específico na página **www.certificacaoabecs.org.br**. A partir do exame inicial das informações, a ABECS enviará os contatos das empresas credenciadas para a instituição obter os custos do selo, assinar minuta de contrato com a empresa de avaliação, e após a assinatura do contrato, a empresa credenciada marcará com o interessado reunião para solicitar as informações e os documentos necessários, e informar o cronograma para o desenvolvimento dos trabalhos.

VI. DOS CRITÉRIOS DE APROVAÇÃO

VI.1. Com base nos resultados apresentados a partir da análise dos requisitos de conformidade, a empresa de avaliação independente atribuirá nota a cada requisito, de forma a aferir a existência e a adequação das políticas, procedimentos e controles da instituição ou do agente, e fará apontamentos de melhoria caso a nota fique abaixo do mínimo previamente estabelecido.

VI.2. Os critérios para a atribuição das notas foram desenvolvidos pela empresa de avaliação e validados pela ABECS.

VI.3. Para a obtenção do Selo, de qualquer Série, será necessário atingir nota final 90% ou superior. Para isso, o avaliado não poderá obter nota na escala mínima (ou seja, NA) em qualquer um dos requisitos, a partir do seguinte critério de pontuação:

- Não conforme: escala entre 0 e 44 %;
- Em atenção: escala entre 45 e 74 %;
- Parcialmente Conforme: escala entre 75 e 89 %; e
- Em conformidade: escala entre 90 e 100 %

VI.4. Para as notas entre as escalas de “Em atenção” ou “Parcialmente Conforme” a instituição ou entidade terá até 90 dias para remediação dos requisitos não atendidos para avaliar conformidade.

VI.5. Para as notas inferiores ao mínimo, o Selo não poderá ser emitido. Nesse caso, a instituição ou entidade precisará implementar as soluções para os apontamentos e se submeter a uma nova avaliação, que confirme os aperfeiçoamentos e a satisfação do padrão mínimo exigido.

VII. DOS PRAZOS, CONDIÇÕES DE OBTENÇÃO E DE VALIDADE DO SELO

VII.1. O selo tem validade de um ano a partir da conclusão da avaliação, junto com a emissão do relatório correspondente.

VII.2. A emissão do Selo se dará para as instituições cujo somatório das notas atinja o padrão mínimo requerido, e precisará ser renovada a cada ano pelo mesmo processo.

VII.3. As instituições devem observar as datas de vencimentos dos respectivos

Selos, para a renovação e manutenção deles. Será tomada como referência a data de conclusão do processo relativo à primeira renovação do Selo, ou seja, as instituições e entidades precisarão iniciar o novo processo do selo, para a renovação e manutenção do Selo, mediante a entrega de toda a documentação necessária, com no mínimo 60 dias de antecedência em relação à mencionada data e cumprir tempestivamente o cronograma apresentado pela avaliação.

VII.4. Nos casos em que se verifique a impossibilidade de conclusão do processo de avaliação até a data correspondente à conclusão do processo relativo à primeira renovação do Selo, poderá ser concedida, em caráter excepcional, uma dilação desse prazo, para cuja análise criteriosa, por parte da empresa de avaliação, serão considerados os motivos que provocaram a demora e o tempo ainda necessário para a finalização da avaliação. A manutenção do nome e da logomarca da instituição ou da entidade no site da ABECS, mesmo após a data de vencimento do Selo, pressupõe a dilação do prazo de validade.

VII.5. Após o vencimento, caso não tenha sido renovado ou não esteja em processo de renovação, nas condições dos incisos precedentes, o Selo perderá sua validade, implicando na retirada do nome e da logomarca da instituição ou da entidade do site da ABECS.

VII.6. As instituições que venham a ser autorizadas a operar em meios de pagamento pelo BCB, ou ainda os novos instituidores de serviços de pagamento e seus participantes, que venham a oferecer ou executar serviços de meios de pagamento, terão o prazo de até 180 dias após o início das suas operações nesse mercado para a obtenção do Selo.

VII.7. A obtenção do Selo não é uma imposição, mas, por uma ação de autorregulação do próprio mercado, o relacionamento com outros pares, no País ou no exterior, poderá ser prejudicado caso as instituições, as entidades ou os correspondentes não se interessem ou não consigam obtê-lo.

VII.8. O Selo poderá ser cancelado nos casos em que se verifique, após concluído o processo de avaliação, o descumprimento de quaisquer dos seus requisitos.

VII.9. Por se tratar de instrumento destinado exclusivamente à aferição de conformidade às normas, será também passível de cancelamento a utilização indevida do Selo ensejando insinuar vínculo com a qualidade dos serviços prestados pela instituição ou pela entidade que o tenha obtido.

VIII. DA DIVULGAÇÃO

VIII.1. A ABECS divulgará este Manual e suas atualizações na página **www.certificacaoabecs.org.br** e enviará cópia eletrônica a todos os associados. Os interessados poderão ainda encaminhar suas dúvidas pelo e-mail **certificacao@abecs.org.br.**

IX. DO CONTROLE DOS PRAZOS

IX.1. A ABECS manterá controle dos prazos para a renovação dos Selos, mas a responsabilidade pelo cumprimento desses prazos será da própria instituição ou do correspondente interessados, que poderão consultar a ABECS em caso de dúvida.

X. DAS DISPOSIÇÕES FINAIS

X.1. O presente Manual poderá sofrer modificações, atualizações ou acréscimos, que deverão ser observados, sobretudo para efeito dos requisitos de conformidade para a obtenção do Selo, caso não iniciado o processo de avaliação anual de quaisquer das Séries aqui tratadas.

---------- *** ----------