MERC GROUP

THINK GROWTH. THINK MERC.

GUIA TÉCNICO MERC · REGULAÇÃO

Governança, riscos e continuidade nível banco em PSAVs *três linhas de defesa, risco cibernético e terceirização*

O regime eleva a PSAV ao nível banco em governança e riscos. Entenda três linhas de defesa, risco operacional e cibernético, continuidade e governança de terceirização.

NORMA BASE	PÚBLICO	EDIÇÃO	DATA
Regulação	Diretoria financeira, controladoria e governança	1ª edição	2026-08-10

ABERTURA

O que este material resolve

A frase que resume o novo regime é uma só: o mercado de ativos virtuais subiu para o nível banco. Não é retórica. Significa que a PSAV passa a ser cobrada por uma estrutura de governança, gestão de riscos e continuidade equivalente à das instituições autorizadas pelo Banco Central. Conselho e diretoria com responsabilidades definidas, três linhas de defesa funcionando de verdade, gestão de risco operacional e cibernético à altura de quem guarda ativo alheio em ambiente digital, plano de continuidade e governança sobre a terceirização. Para muitas plataformas nascidas com cultura de produto e velocidade, essa é a maior mudança de todas. Este artigo mapeia o que o nível banco cobra em governança. Não trata de nenhuma empresa específica.

SEÇÃO 01

Resumo

01 **O regime cobra da PSAV**

O regime cobra da PSAV uma **estrutura de governança** com papéis definidos: administração responsável, funções de controle independentes e prestação de contas ao regulador. Governança informal não sobrevive à supervisão.

02 **As **três linhas de defesa****

As **três linhas de defesa** organizam quem faz, quem controla e quem avalia de forma independente. A separação entre operação, compliance e auditoria interna é estrutural, não opcional.

03 **Risco operacional e cibernético**

ganham peso máximo, porque a PSAV guarda ativo de terceiros em ambiente digital. Segurança, continuidade e resposta a incidentes são parte do controle, não anexos técnicos.

04 **A **terceirização** de funções relevantes**

A **terceirização** de funções relevantes, comum no setor, precisa de governança formal: a responsabilidade perante o cliente e o regulador permanece com a sociedade, mesmo quando a execução é de um terceiro.

Linha de defesa	Quem é · Responsabilidade
Primeira linha	Áreas de negócio e operação · Executa e é dona do risco no dia a dia
Segunda linha	Riscos e compliance · Define política, monitora e desafia a operação
Terceira linha	Auditoria interna · Avalia de forma independente a eficácia dos controles

SEÇÃO 02

Governança deixa de ser informal

Plataformas de tecnologia costumam nascer com governança enxuta e decisão concentrada, o que faz sentido na fase de produto. O regime muda essa lógica. A administração passa a ter responsabilidades formais sobre riscos e controles, as funções de controle precisam existir com mandato claro e a sociedade precisa prestar contas ao regulador de forma estruturada. Isso não significa burocratizar a operação; significa que as decisões de risco deixam de depender da presença de uma pessoa e passam a depender de um arranjo que sobrevive à troca de gente.

O sinal mais claro dessa mudança é a exigência de independência das funções de controle. Compliance que responde à área comercial, ou auditoria interna que não tem independência do compliance, não cumprem o papel que o regime espera. A independência funcional é o que garante que a segunda e a terceira linha consigam desafiar a operação de verdade, e não apenas homologar o que a primeira linha decidiu.

SEÇÃO 03

Três linhas de defesa que funcionam

O modelo de três linhas de defesa é simples de enunciar e difícil de implementar bem. A primeira linha é a operação, dona do risco no dia a dia, que executa e convive com as consequências das próprias decisões. A segunda linha é a estrutura de riscos e compliance, que define política, monitora e desafia a operação, atuando como contrapeso. A terceira linha é a auditoria interna, que avalia de forma independente se os controles funcionam e reporta a quem tem autoridade para agir.

O erro frequente não é desconhecer o modelo, mas implementá-lo apenas no organograma. Ter uma caixa de compliance no organograma não é ter segunda linha se essa área não tem mandato, recurso e independência para desafiar. Ter auditoria interna no papel não é ter terceira linha se ela reporta a quem ela deveria avaliar. O que a supervisão examina é se as três linhas operam com a separação e a independência que o modelo pressupõe, e é aí que muitas estruturas descobrem que tinham apenas o desenho.

SEÇÃO 04

Risco operacional, cibernético e continuidade

Nenhum tipo de risco pesa mais em uma PSAV do que o operacional e o cibernético, e a razão é a natureza do negócio: a sociedade guarda ativo de terceiros em ambiente digital, onde uma falha técnica ou um ataque bem-sucedido pode significar perda direta e irreversível. Por isso segurança da informação, resiliência dos sistemas, gestão de acessos e resposta a incidentes deixam de ser assunto exclusivo de tecnologia e passam a ser componentes do controle interno que a governança precisa endereçar.

A continuidade de negócio completa o quadro. A sociedade precisa ter plano para operar e para se recuperar quando algo falha, com testes que comprovem que o plano funciona, e não apenas um documento guardado. Em um mercado que opera de forma contínua, a indisponibilidade prolongada não é só um problema técnico: é um problema de proteção ao cliente, porque impede acesso a recurso e ativo. A auditoria examina se esses planos existem, se são testados e se a resposta a incidentes deixa trilha.

SEÇÃO 05

A terceirização não terceiriza a responsabilidade

O setor de ativos virtuais é intensivo em terceirização: custódia, monitoramento on-chain, infraestrutura de nuvem, ferramentas de KYC. Isso é legítimo e muitas vezes recomendável, porque concentra funções especializadas em quem as faz melhor. Mas há um princípio que o regime não abre mão: a responsabilidade perante o cliente e o regulador permanece com a sociedade, mesmo quando a execução é de um terceiro.

Na prática, isso exige governança formal sobre os prestadores relevantes. A sociedade precisa avaliar o terceiro antes de contratar, monitorar o serviço durante a relação, ter trilha sobre o desempenho e manter capacidade de responder quando o terceiro falha. Terceirizar sem governança é transferir a execução mantendo o risco, sem manter o controle. Esse é um dos gaps mais comuns e mais subestimados, porque a plataforma assume que, ao contratar um provedor especializado, transferiu também o problema, quando na verdade continua respondendo por ele.

SEÇÃO 06

Um caso anonimizado

Considere uma plataforma que cresceu rápido, com governança concentrada na fundação e funções de controle montadas conforme a necessidade aparecia. No papel, existem compliance, gestão de risco e até auditoria interna. Quando a asseguração independente se aproxima, o exame revela que o compliance responde à área comercial, que a auditoria interna nunca teve independência real e que a resposta a incidentes cibernéticos nunca foi testada. A custódia e o monitoramento são terceirizados, mas não há governança formal sobre esses provedores: contratos existem, avaliação e monitoramento não. Nenhum desses pontos decorre de descuido deliberado. Decorre de montar controle por reação, e não por desenho. A lição é que governança de nível banco não se improvisa na véspera da autorização; ela precisa preceder o pedido.

SEÇÃO 07

Como a MERC pode ajudar

A MERC apoia PSAVs a elevar a governança ao nível que o regime exige. Ajudamos a formalizar responsabilidades da administração, a estruturar as três linhas de defesa com independência real entre operação, compliance e auditoria interna, e a organizar a gestão de risco operacional e cibernético como componente do controle interno. Apoiamos o desenho e o teste do plano de continuidade e da resposta a incidentes, e a construção de governança formal sobre a terceirização de funções relevantes. Conduzimos o trabalho de asseguração independente sobre esse ambiente de controle com a experiência de quem examina governança em instituições reguladas. O objetivo é que a estrutura de governança sobreviva à supervisão e à troca de pessoas, e não apenas ao organograma.

MERC GROUP

PRÓXIMO PASSO

Precisa de *apoio técnico?*

A MERC Group é firma de auditoria independente registrada na CVM, com atuação em auditoria, asseguração, consultoria regulatória e transações. Este material é de apoio e não substitui a análise do caso concreto.

SITE	www.mercgroup.com.br
CONTEÚDO	www.mercgroup.com.br/insights
E-MAIL	contato@mercgroup.com.br
TELEFONE	+55 11 98196 1447