MERC GROUP

THINK GROWTH. THINK MERC.

Cibersegurança

Cibersegurança e *nuvem* o que a BCB 538 exige

A Resolução BCB 538 e a CMN 5.274 trocam política no papel por evidência técnica e teste de intrusão independente. Veja o que a auditoria passa a examinar.

NORMA BASE	PÚBLICO	EDIÇÃO	DATA
Resolucao BCB 538	Diretoria de TI, riscos e comite de auditoria	Setembro 2026	Agosto de 2026

A régua de segurança do sistema financeiro deixou de aceitar a política no papel como prova. A Resolução BCB nº 538 e a Resolução CMN nº 5.274, de dezembro de 2025, atualizaram a política de segurança cibernética e os requisitos de contratação de processamento, armazenamento de dados e computação em nuvem das instituições autorizadas pelo Banco Central, com prazo de adequação em março de 2026. A mudança de fundo é clara: o supervisor quer evidência técnica e efetividade operacional, não a descrição de um controle que ninguém testou.

Cibersegurança

Resumo

01 **As Resoluções BCB 538 e CMN 5.274 atualizam o ar**

As Resoluções BCB 538 e CMN 5.274 atualizam o arcabouço de segurança cibernética e de nuvem de 2021, com prazo de adequação em 1º de março de 2026, e valem para instituições autorizadas a funcionar pelo Banco Central.

02 **A virada central é de abordagem: sai a conformid**

A virada central é de abordagem: sai a conformidade baseada em política formal, entra o modelo orientado a evidência técnica, rastreabilidade e efetividade operacional dos controles.

03 **Passa a ser obrigatório o teste de intrusão anua**

Passa a ser obrigatório o teste de intrusão anual, conduzido por empresa ou profissional independente, com documentação, plano de ação corretivo e retenção das evidências.

04 **A contratação de nuvem e de serviços de tecnolog**

A contratação de nuvem e de serviços de tecnologia ganha exigências de diligência, localização de dados, continuidade e saída, o que amplia o exame de terceiros e da cadeia de subcontratação.

P	A
Abordagem	De política formal para evidência e efetividade operacional
Teste de intrusão	Anual e obrigatório, por parte independente
Nuvem e terceiros	Diligência, localização, continuidade e saída
Incidentes	Resposta, comunicação e rastreabilidade

As quatro frentes da Resolução BCB 538 e o que cada uma pede de evidência.

Nuvem

A virada que muda a natureza da conformidade

Por anos, a conformidade cibernética foi avaliada, na prática, pela existência de uma política aprovada e de um responsável designado. O novo arcabouço fecha essa brecha. O que a norma pede agora é prova de que o controle funciona: registros de que o monitoramento detecta, de que o acesso é revisado, de que o backup é testado e de que o incidente foi tratado no prazo. A pergunta deixou de ser existe a política e passou a ser onde está a evidência de que ela opera.

Essa mudança tem consequência direta para quem prepara e para quem audita. Um ambiente que só produz documentos, sem trilha do funcionamento, não sustenta mais a conformidade. A efetividade operacional vira o objeto do exame, e a ausência de evidência deixa de ser um detalhe formal para virar uma deficiência de controle. É a mesma lógica de evidência técnica que sustenta a homologação de ambientes regulados, tema que tratamos em a homologação da infraestrutura de duplicata escritural.

BCB 538

O teste de intrusão independente deixa de ser opcional

O ponto mais concreto da norma é a exigência de teste de intrusão anual, conduzido por empresa ou profissional independente. Não basta rodar uma varredura automática interna. O teste precisa ter escopo definido, ser executado por parte com independência em relação a quem construiu e opera o ambiente, gerar documentação formal, resultar em plano de ação corretivo para as falhas encontradas e ter suas evidências retidas.

Para a auditoria, o teste de intrusão vira um insumo e um objeto ao mesmo tempo. Como insumo, informa o risco tecnológico que afeta os controles gerais de tecnologia sobre os quais a auditoria das demonstrações se apoia. Como objeto, ele próprio é examinado: houve independência real, o escopo cobriu os sistemas críticos, as falhas de maior severidade viraram ação com prazo e responsável, e as correções foram verificadas. Um teste que aponta falhas e morre no relatório não reduz risco, apenas o documenta.

Ciberseguranca

Nuvem e terceiros: o risco que sai de casa

A segunda frente da norma trata da contratação de processamento, armazenamento de dados e computação em nuvem. Quando a instituição move sistemas críticos para um provedor, o risco não desaparece, muda de endereço. A norma reforça a diligência prévia do provedor, os requisitos de localização e acesso a dados, a continuidade do serviço e, um ponto que costuma faltar, a estratégia de saída: como a instituição recupera dados e operação se precisar trocar de provedor ou trazer o serviço de volta.

O exame de terceiros passa a ser inseparável do exame do ambiente próprio. A auditoria olha o contrato e os direitos de auditoria nele previstos, a cadeia de subcontratação do provedor, os relatórios de asseguração sobre os controles do prestador e o plano de reversão. Aqui a norma conversa com a avaliação de serviços terceirizados relevantes para o controle interno, que já tratamos em terceirização de tecnologia e a NBC TA 402: confiar no provedor exige evidência, não apenas contrato.

P	A
Política robusta sem registro de operação	Controle descrito, mas não efetivo
Teste de intrusão feito por equipe interna	Falta de independência exigida pela norma
Nuvem crítica sem estratégia de saída	Dependência do provedor e risco de continuidade
Incidente sem trilha de resposta	Impossível provar prazo e tratamento adequados

Sinais de alerta sob a Resolução BCB 538 e a resposta esperada da auditoria.

Nuvem

O elo com os controles gerais de tecnologia

A auditoria das demonstrações financeiras se apoia em controles gerais de tecnologia, os que governam acesso, mudança e operação dos sistemas que produzem os números. A norma de cibersegurança reforça exatamente essa base. Um ambiente com acesso mal controlado, mudanças sem trilha ou incidentes não tratados fragiliza a confiança nos relatórios que dele saem, mesmo que a contabilidade esteja correta.

Por isso a leitura da Resolução BCB 538 não é só de tecnologia. Ela define a qualidade da evidência que sustenta a auditoria financeira e a asseguração de controles. Quando o supervisor eleva a régua para efetividade e independência, ele eleva também o piso de confiança que qualquer trabalho de asseguração pode oferecer sobre aquele ambiente.

BCB 538

Caso anonimizado

Uma instituição de médio porte tinha uma política de segurança exemplar no papel e um comitê ativo, mas tratava o teste de intrusão como uma varredura interna anual sem escopo formal. Ao migrar o núcleo transacional para a nuvem, não desenhou estratégia de saída nem revisou os direitos de auditoria no contrato do provedor. No exame, faltava evidência de que os controles operavam e faltava independência no teste.

Na adequação, o teste de intrusão passou a ser contratado de parte independente, com escopo nos sistemas críticos e plano de ação com prazo, o contrato de nuvem incorporou direitos de auditoria e plano de reversão, e a instituição passou a reter a trilha de operação dos controles. O caso ilustra a virada da norma: a segurança deixou de ser um documento e virou um conjunto de evidências que alguém, de fora, consegue verificar.

Ciberseguranca

Como a MERC pode ajudar

A MERC é especializada no mercado financeiro brasileiro e trata a avaliação de controles de tecnologia como parte do trabalho de auditoria independente e de asseguração. Sob o novo arcabouço, isso significa examinar a efetividade operacional dos controles, avaliar o teste de intrusão quanto à independência e ao encerramento das falhas, e ler a contratação de nuvem pela ótica do risco de terceiros, da continuidade e da estratégia de saída.

Para bancos, fintechs, instituições de pagamento e prestadores de infraestrutura, o ganho é duplo: uma adequação que resiste à supervisão orientada a evidência e uma base de controles gerais de tecnologia que dá confiança às demonstrações e aos relatórios de asseguração. Se a sua instituição está fechando a adequação à Resolução BCB 538, o contato é o caminho para discutir o caso concreto.

Nuvem

Perguntas frequentes

MERC GROUP

PRÓXIMO PASSO

Do requisito ao *teste* que o sustenta.

A MERC e firma de auditoria independente registrada na CVM, especializada em mercado financeiro. Estruturamos o trabalho do diagnostico a evidencia: leitura do requisito, desenho dos testes, trilha de auditoria e o relatorio que sustenta a conclusao. Fale com a equipe pelo canal de contato.

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