MERC GROUP

THINK GROWTH. THINK MERC.

GUIA TÉCNICO MERC · REGULAÇÃO

Credenciamento de provedores de TI no sistema financeiro *o que a terceirização de tecnologia crítica cobra de controles gerais, cibersegurança e asseguração*

O credenciamento de provedores de serviços de TI para o sistema financeiro aperta a régua. Veja o que a terceirização de tecnologia crítica exige de controles, cibersegurança e trilha auditável.

NORMA BASE	PÚBLICO	EDIÇÃO	DATA

ABERTURA

O que este material resolve

Quase nenhuma instituição financeira opera hoje só com tecnologia própria. Processamento de dados, conectividade, nuvem e integrações críticas rodam, em boa parte, na infraestrutura de prestadores especializados. O regulador olhou para essa dependência e mudou a régua: para prestar serviços de tecnologia da informação que dão acesso à rede do sistema financeiro, o provedor passa a precisar de credenciamento formal, com patrimônio mínimo, governança específica de segurança e risco, e controles operacionais objetivamente verificáveis. Para as instituições contratantes, a novidade tem um efeito silencioso e profundo: aquilo que era um contrato de fornecedor de tecnologia passa a ser um elo da cadeia de controle que precisa ser avaliado, monitorado e comprovado. Este artigo não trata de nenhum provedor ou instituição específica. Trata do que a terceirização de tecnologia crítica exige de controles gerais, de cibersegurança e de evidência, e de como a MERC apoia instituições a operar essa dependência de forma auditável.

SEÇÃO 01

Resumo

Terceirizar tecnologia crítica deixa de ser uma decisão só de custo e vira uma decisão de controle. Quando parte relevante do processamento e da conectividade que sustentam a operação roda em um prestador, a instituição continua responsável pelos riscos daquilo que terceirizou. O credenciamento do provedor formaliza uma régua mínima de capacidade técnica, governança e segurança, mas não transfere para o fornecedor a responsabilidade da instituição pela integridade e pela continuidade dos seus processos.

Os controles gerais de tecnologia passam a incluir a fronteira com o terceiro. Acesso, mudança, operação, continuidade e segurança não param na porta da instituição: seguem para dentro do provedor. Avaliar esses controles gerais significa entender onde o dado trafega, quem tem acesso a quê, como as mudanças são controladas e como a segurança é monitorada ao longo de toda a cadeia, e não apenas dentro do próprio ambiente.

Cibersegurança e continuidade viram exigência verificável, não promessa contratual. A régua pede detecção de acessos indevidos, monitoramento de comportamento, resposta a incidentes e capacidade de recuperação. Do ponto de vista de quem examina, o que importa não é a cláusula do contrato, e sim a evidência de que o controle existe, opera e é testado com regularidade.

A dependência de terceiros aproxima o tema da asseguração de controles de organizações prestadoras de serviço. Quando processos relevantes rodam fora da instituição, a forma madura de dar conforto a auditores, ao supervisor e aos clientes é um trabalho de asseguração sobre o desenho e a operação dos controles do prestador, com nível de confiança definido e trilha de evidência.

Dimensão	Terceirização de TI sob a lógica antiga · Terceirização de TI crítica
Natureza do vínculo	Contrato de fornecedor, tratado como compra de serviço · Elo da cadeia de controle, com provedor credenciado e requisitos mínimos
Governança do provedor	Variável, sem exigência formal padronizada · Estrutura definida para segurança, risco, compliance e crise operacional
Controles gerais de tecnologia	Avaliados dentro da instituição, com fronteira difusa no terceiro · Estendidos à fronteira com o provedor, com acesso, mudança e operação mapeados
Cibersegurança	Tratada como cláusula e boa prática · Controle verificável, com detecção, monitoramento e resposta a incidentes
Evidência para exame	Dispersa entre áreas e fornecedores · Trilha reconstituível e, quando possível, asseguração de controles do prestador

SEÇÃO 02

Por que a terceirização de tecnologia crítica é, no fundo, um problema de controle

A lógica de credenciar quem presta serviços de tecnologia da informação para o sistema financeiro parte de uma constatação simples: a resiliência e a segurança do sistema como um todo dependem de uma cadeia de prestadores que, até então, era contratada sob critérios muito desiguais. Ao exigir do provedor patrimônio mínimo, governança específica para segurança da informação, riscos, compliance e gestão de crises, e controles operacionais objetivamente verificáveis, o regulador não está apenas elevando a barra de entrada. Está reconhecendo que a falha de um elo terceirizado se propaga para dentro das instituições que dele dependem, com efeito sobre a continuidade dos serviços, sobre a integridade dos dados e sobre a confiança do próprio sistema.

Para a instituição contratante, o ponto central é este: credenciar o provedor não terceiriza a responsabilidade. A instituição continua respondendo pela integridade e pela continuidade dos processos que dependem daquela tecnologia, ainda que o processamento ocorra fora dela. Isso muda a natureza da relação. O contrato deixa de ser um documento comercial guardado no jurídico e passa a ser parte da arquitetura de controle da instituição, com direitos de acesso à informação, obrigações de reporte, definição de responsabilidades e capacidade de demonstrar, quando questionada, que sabe onde o dado está, quem o acessa e como a segurança é mantida.

O segundo motivo pelo qual o tema é sensível está na fronteira. Controles gerais de tecnologia, aquilo que sustenta a confiança em todos os sistemas que produzem informação contábil e operacional, não param no perímetro da instituição. Gestão de acessos, controle de mudanças, operação de rotinas, continuidade e segurança seguem para dentro do provedor. Uma avaliação que só olha o ambiente interno e assume que o resto está coberto pelo contrato deixa um vão perigoso justamente onde hoje mora boa parte do risco tecnológico: na infraestrutura terceirizada de que a operação depende para funcionar.

SEÇÃO 03

Onde a régua encosta nos controles, na cibersegurança e na auditoria

O primeiro ponto é de controles gerais de tecnologia na fronteira com o terceiro. Sob a lógica da **NBC TA 315 (R2)** , que trata do entendimento da entidade e do seu ambiente, incluindo os controles relevantes, e da **NBC TA 330** , que trata das respostas aos riscos avaliados, os controles gerais de tecnologia são a base sobre a qual repousa a confiança nos sistemas que geram informação. Quando esses sistemas rodam, no todo ou em parte, em um provedor, a avaliação precisa alcançar a gestão de acessos, o controle de mudanças e a operação também nesse ambiente. A pergunta não é se existe um bom fornecedor, e sim se os controles gerais permanecem confiáveis ao longo de toda a cadeia.

O segundo ponto é de cibersegurança e continuidade como controle verificável. Detecção de acessos indevidos, monitoramento de comportamento nas interfaces, resposta a incidentes e capacidade de recuperação deixam de ser promessas e passam a ser controles que precisam ter desenho claro e operação testada. Do ponto de vista de quem examina, isso significa procurar evidência: registros de monitoramento, testes de recuperação, tratamento documentado de incidentes e trilha das ações de segurança. Um controle de segurança que não deixa rastro é, para efeito de exame, um controle que não se pode confirmar.

O terceiro ponto é de dependência de terceiros e asseguração. Quando processos relevantes ocorrem fora da instituição, a maneira madura de dar conforto a auditores, ao supervisor e aos clientes é um trabalho de asseguração sobre os controles da organização prestadora de serviço, sob a lógica da **NBC TO 3402** , complementado, quando o objeto pede, por trabalhos de asseguração de propósito mais amplo sob a **NBC TO 3000 (R1)** . Esses relatórios permitem que a instituição contratante e seus auditores confiem, com evidência e nível de confiança definido, nos controles operados pelo prestador, em vez de dependerem apenas de declarações contratuais. É a diferença entre acreditar que o terceiro controla e conseguir demonstrar que controla.

Frente	Pergunta que o auditor faz · Risco se não houver resposta
Controles gerais na fronteira	Acesso, mudança e operação estão controlados também no provedor? · Confiança nos sistemas quebra num elo fora do perímetro interno

Frente	Pergunta que o auditor faz · Risco se não houver resposta
Cibersegurança	Há detecção, monitoramento e resposta a incidentes com evidência? · Segurança tratada como cláusula, sem prova de que o controle opera
Continuidade	A recuperação foi testada e o resultado está registrado? · Plano existe no papel, mas não se sabe se funciona sob estresse
Dependência de terceiros	Há asseguração sobre os controles do prestador de serviço? · Confiança apoiada em contrato, sem evidência independente dos controles

SEÇÃO 04

Como a MERC pode ajudar: o que fazemos e o que você recebe

A MERC é a primeira e única auditoria especializada no mercado financeiro brasileiro, e a terceirização de tecnologia crítica é exatamente o tipo de tema em que a especialização pesa, porque exige ler ao mesmo tempo a arquitetura tecnológica da operação, a fronteira dos controles com o prestador e a evidência que sustenta a segurança e a continuidade. A abordagem cobre do diagnóstico da dependência à asseguração de controles, com profundidade ajustável ao porte da instituição, à criticidade dos serviços terceirizados e ao grau de dependência de terceiros. O escopo abaixo mostra, frente a frente, o que executamos e o que fica na sua mão como entregável.

Sobre esse ciclo, a especialização da MERC agrega a leitura da dependência tecnológica pela ótica de quem depois vai examinar a evidência. Quando a instituição trata a terceirização de tecnologia crítica já pensando nos controles gerais que atravessam a fronteira, na cibersegurança que precisa deixar rastro e na asseguração que dá conforto sobre os controles do prestador, ela não contrata apenas um bom fornecedor: constrói uma dependência que resiste ao exame. É a diferença entre confiar no terceiro e conseguir demonstrar que os controles de que a operação depende funcionam, mesmo quando rodam fora de casa.

Frente	O que fazemos · O que você recebe
1. Mapa de dependência	Identificação dos serviços de tecnologia críticos e dos processos que dependem deles · Inventário de dependências, criticidade e concentração de risco
2. Controles gerais de TI	Avaliação de acesso, mudança, operação e continuidade na instituição e na fronteira com o provedor · Relatório de lacunas e plano de adequação priorizado

Frente	O que fazemos · O que você recebe
3. Cibersegurança	Exame do desenho e da operação dos controles de detecção, monitoramento e resposta · Diagnóstico de segurança e recomendações de remediação
4. Governança do contrato	Avaliação de direitos de acesso à informação, reporte e responsabilidades na relação com o prestador · Matriz de responsabilidades e requisitos mínimos de governança
5. Asseguração de controles	Trabalho de asseguração sobre o desenho e a operação dos controles do prestador de serviço · Relatório de asseguração com nível de confiança definido e trilha de evidência
6. Prontidão para exame	Preparação da documentação, dos registros e da trilha para responder ao supervisor e aos auditores · Dossiê de prontidão, roteiro de resposta e manuais operacionais

SEÇÃO 05

Um caso ilustrativo (anonimizado)

Considere uma instituição de médio porte que migrou parte relevante do seu processamento para um prestador especializado e tratou a mudança como um projeto de custo e de eficiência, conduzido pela área de infraestrutura. A migração correu bem, os custos caíram e o assunto foi considerado resolvido. No diagnóstico, o problema real aparece: a gestão de acessos ao ambiente terceirizado seguia critérios diferentes dos internos, sem revisão periódica; os controles de mudança do provedor não tinham trilha compartilhada com a instituição; a resposta a incidentes dependia de um fluxo informal, sem registro consistente; e não havia qualquer relatório de asseguração sobre os controles do prestador. O que parecia uma terceirização bem-sucedida era, na verdade, uma dependência crítica sem cobertura de controle na fronteira.

O trabalho é reorganizado em frentes. Primeiro o mapa de dependência e a criticidade dos serviços, depois os controles gerais de tecnologia na instituição e na fronteira com o provedor, em seguida a cibersegurança e a continuidade com evidência, e por fim a governança do contrato e a asseguração dos controles do prestador. Nenhuma etapa exigiu trazer a tecnologia de volta para dentro: exigiu tratar o terceiro como parte da cadeia de controle, com acesso à informação, trilha e asseguração. O caso é ilustrativo e não se refere a nenhuma instituição ou provedor específico. O padrão, porém, é frequente: o risco quase nunca está em terceirizar, e sim em terceirizar sem estender os controles e a evidência para onde o processo passou a rodar.

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