MERC GROUP

THINK GROWTH. THINK MERC.

TECNOLOGIA

Controles gerais de *TI* o que a auditoria examina

Sem controles gerais de TI confiáveis, nenhum relatório ou controle automatizado é confiável. Veja o que a auditoria examina em ITGC no fechamento de 2026.

NORMA BASE	PÚBLICO	EDIÇÃO	DATA
NBC TA 315 · NBC TA 330	Instituições financeiras e fintechs	Guia técnico	Novembro de 2026

Quando quase toda a contabilidade de uma instituição nasce dentro de sistemas, a confiança do auditor em qualquer número depende de confiar nos sistemas que o produziram. Os controles gerais de tecnologia da informação, conhecidos pela sigla ITGC, são exatamente a camada que sustenta essa confiança. Eles não calculam a provisão nem conciliam a conta: garantem que o cálculo e a conciliação feitos pelo sistema não foram alterados sem autorização, que só quem deve acessa, que mudanças de programa passam por aprovação e teste, e que falhas de operação são detectadas e corrigidas. Se essa camada é frágil, nenhum relatório extraído do sistema e nenhum controle automatizado sobre ele podem ser considerados confiáveis, por mais bem desenhados que pareçam.

Para uma instituição financeira, uma fintech ou uma empresa que migrou o core para a nuvem, essa dependência cresceu a ponto de os controles gerais de TI deixarem de ser assunto da área técnica e virarem premissa da auditoria das demonstrações. A auditoria independente avalia esses controles antes de confiar em relatórios de sistema e em controles automatizados, e a densidade regulatória e tecnológica de 2026, com mais automação, mais integrações com terceiros e mais exigência sobre dados, elevou a barra desse exame. Para discutir como o seu ambiente de TI se sustenta diante do auditor, o caminho é o contato.

TECNOLOGIA

Resumo

Controles gerais de TI são a camada que garante a integridade dos sistemas onde a contabilidade é processada: acesso, mudanças, operações e segregação de funções. Eles não geram o número, mas garantem que o número não foi adulterado.

Quando os controles gerais são frágeis, o auditor não pode confiar em relatórios extraídos do sistema nem em controles automatizados, e precisa ampliar os testes substantivos, o que encarece e alonga o trabalho.

A norma de auditoria trata a confiança em controles automatizados e em informação produzida pela entidade como condicionada à robustez dos controles gerais de TI que os cercam, o que torna o ITGC uma base, não um detalhe.

A digitalização do core, a migração para a nuvem e a dependência de prestadores de serviço em 2026 ampliaram a superfície desses controles e trouxeram a fronteira com o terceiro para dentro do exame da auditoria.

P	A
Gestão de acessos	Só quem deve acessa cada sistema e função?
Gestão de mudanças	Toda alteração de programa é aprovada e testada antes de produção?

P	A
Operações de TI	Rotinas, cargas e interfaces rodam e falhas são detectadas?
Segregação de funções	Quem desenvolve é diferente de quem aprova e de quem opera?

CONTROLES

Por que a auditoria começa pelos sistemas

A lógica é de dependência. O auditor planeja confiar em certos controles para reduzir o volume de testes diretos sobre saldos e transações. Muitos desses controles são automatizados, como uma regra que bloqueia um lançamento fora de parâmetro, ou dependem de informação gerada pelo próprio sistema, como um relatório de vencidos que alimenta a provisão. Mas confiar em um controle automatizado só faz sentido se houver garantia de que o programa que o executa não foi alterado sem autorização, e confiar em um relatório de sistema só faz sentido se houver garantia de que ninguém manipulou os dados ou a consulta que o gerou. Essa garantia é dada pelos controles gerais de TI. Por isso eles vêm antes: são a fundação sobre a qual o auditor decide se pode ou não apoiar-se na tecnologia da entidade.

Quando os controles gerais são sólidos, o auditor testa o controle automatizado uma vez e confia que ele operou de forma consistente no período, porque sabe que o programa não mudou sem rastro. Quando são frágeis, essa confiança desaparece: mesmo um controle automatizado bem desenhado pode ter sido contornado, e o auditor precisa voltar a testar diretamente as transações, em volume maior. A fragilidade de ITGC não aparece como um achado isolado, portanto. Ela se espalha, porque derruba a confiança em tudo que se apoiava na tecnologia.

AUDITORIA

Acesso, mudança, operação e a fronteira com o terceiro

O domínio de acessos é onde mora o achado mais frequente. Usuários que mudaram de função e mantiveram permissões antigas, contas genéricas compartilhadas, acessos privilegiados sem revisão periódica, ex-colaboradores ativos no sistema: cada um desses é um caminho para que um lançamento contábil seja feito ou alterado por quem não deveria, sem responsabilidade clara. A segregação de funções, que separa quem desenvolve, quem aprova e quem opera, é o controle que impede que uma única pessoa consiga alterar um programa e esconder o efeito. Quando essa separação não existe de fato, o controle que depende dela perde valor.

A gestão de mudanças responde por outra ponta do risco. Toda alteração no sistema que processa a contabilidade precisa ser solicitada, aprovada, testada e colocada em produção com registro, de modo que nenhuma mudança relevante entre sem rastro. As operações de TI garantem que as rotinas rodem, que as cargas e interfaces entre sistemas completem o processamento e que falhas sejam detectadas e tratadas. E há a fronteira com o prestador de serviço: quando o processamento ou a infraestrutura estão em um terceiro, parte dos controles gerais vive fora da entidade, e o auditor precisa de evidência sobre esses controles, seja por um relatório de asseguração sobre a organização prestadora, seja por controles compensatórios na própria entidade. Em 2026, com mais core bancário e mais dados na nuvem, essa fronteira passou a ser parte rotineira do exame.

P	A
Acessos	Concessão, revisão periódica e remoção tempestiva de permissões
Segregação de funções	Separação real entre desenvolver, aprovar e operar
Mudanças	Aprovação e teste antes de produção, sem atalhos emergenciais sem registro
Operações	Execução de rotinas, integridade das interfaces e tratamento de falhas
Terceiros	Controles que vivem no prestador de serviço

ITGC

Quando o controle geral falha, o custo da auditoria sobe

A consequência prática de um ambiente de ITGC frágil não é apenas um parágrafo de recomendação no relatório. É mais trabalho. Sem confiança nos controles automatizados e nos relatórios de sistema, o auditor precisa provar cada número por outro caminho, testando diretamente volumes maiores de transações, reexecutando cálculos à margem do sistema e conciliando bases de forma manual. Isso consome mais horas, alonga o cronograma e aumenta o custo do trabalho, além de elevar a chance de que algo passe. A entidade que investe na camada de controles gerais, portanto, não gasta só com conformidade: reduz o esforço substantivo da auditoria e torna o próprio fechamento mais rápido e mais barato.

Há também um efeito sobre os controles de negócio. Muitos controles que a administração considera manuais dependem, na verdade, de um relatório de sistema para funcionar. O analista que revisa vencidos age sobre uma lista que o sistema produz; se a integridade dessa lista não está garantida pelos controles gerais, o controle manual revisa dados que podem estar incompletos. Esse é o ponto que costuma surpreender: um controle aparentemente humano herda a fragilidade da tecnologia que o alimenta, e só o exame dos controles gerais revela essa dependência.

TECNOLOGIA

Um caso anonimizado

Uma instituição havia migrado o processamento para a nuvem e mantinha uma rotina automatizada que classificava operações por faixa de risco, alimentando diretamente a provisão. O controle automatizado era bem desenhado e a administração confiava nele. Ao examinar os controles gerais, porém, o auditor encontrou acessos de desenvolvimento ativos no ambiente de produção e um fluxo de mudança que admitia alterações emergenciais sem aprovação posterior registrada. Não havia evidência de que o programa de classificação não tivesse sido alterado durante o período. O controle automatizado, por si, estava correto, mas a camada que deveria garantir sua integridade não estava, e a confiança nele caiu. A instituição precisou fechar os acessos de desenvolvimento em produção, formalizar o fluxo de mudança e obter o relatório de asseguração do prestador de nuvem. O caso é genérico e ilustra o padrão, sem corresponder a qualquer entidade específica.

CONTROLES

Como a MERC pode ajudar

A MERC atua na auditoria independente de instituições e empresas cuja contabilidade é processada em sistemas, avaliando os controles gerais de TI que sustentam a confiança nesses sistemas: gestão de acessos, segregação de funções, gestão de mudanças, operações e a fronteira com prestadores de serviço. O trabalho define onde o auditor pode apoiar-se em controles automatizados e em relatórios de sistema e onde a fragilidade dos controles gerais obriga a ampliar os testes diretos, e aponta, de forma objetiva, o que precisa ser corrigido para que a tecnologia da entidade seja uma aliada do fechamento, e não uma fonte de retrabalho. Para tratar do seu caso, fale com a equipe pelo contato.

AUDITORIA

Perguntas frequentes

Qual a diferença entre controle geral de TI e controle automatizado de negócio?

O controle automatizado de negócio é uma regra dentro do sistema que executa uma função contábil, como bloquear um lançamento fora de parâmetro. O controle geral de TI é a camada que garante que esse sistema é confiável: que o programa não muda sem autorização, que só quem deve acessa e que as rotinas rodam. O controle automatizado só é confiável se os controles gerais que o cercam forem sólidos.

Por que a auditoria examina acessos e mudanças se o foco é a contabilidade?

Porque a contabilidade é processada nos sistemas, e um acesso indevido ou uma mudança não autorizada podem alterar um número contábil sem deixar rastro. Testar acessos e mudanças é a forma de o auditor garantir que os lançamentos e cálculos produzidos pelo sistema refletem o que a administração autorizou, e não uma alteração à margem do controle.

O que acontece com a auditoria quando os controles gerais de TI são fracos?

O auditor perde a confiança nos controles automatizados e nos relatórios de sistema e precisa provar os números por testes diretos, em volume maior. Isso aumenta as horas de trabalho, alonga o cronograma e eleva o custo, além de aumentar o risco de distorção não detectada. Um ambiente de controles gerais sólido reduz esse esforço substantivo.

Como a auditoria trata o que está na nuvem ou em um prestador de serviço?

Parte dos controles gerais passa a viver fora da entidade. O auditor precisa de evidência sobre esses controles, geralmente por meio de um relatório de asseguração sobre a organização prestadora de serviço, que descreve e testa os controles do terceiro, ou por controles compensatórios mantidos pela própria entidade. Sem uma coisa nem outra, há uma lacuna de evidência sobre o ambiente.

Investir em controles de TI reduz o custo da auditoria?

Tende a reduzir. Quando os controles gerais são sólidos, o auditor pode apoiar-se em controles automatizados e relatórios de sistema e testar menos transações diretamente, o que diminui horas e prazo. Quando são frágeis, ocorre o inverso. O investimento na camada de controles gerais, portanto, paga-se também em eficiência do próprio fechamento, além da conformidade.

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

Material técnico de apoio da MERC Group. Conteúdo de caráter informativo, sem constituir oferta de serviços a entidades para as quais a independência seja vedada. Exemplos genéricos, sem referência a instituição específica.