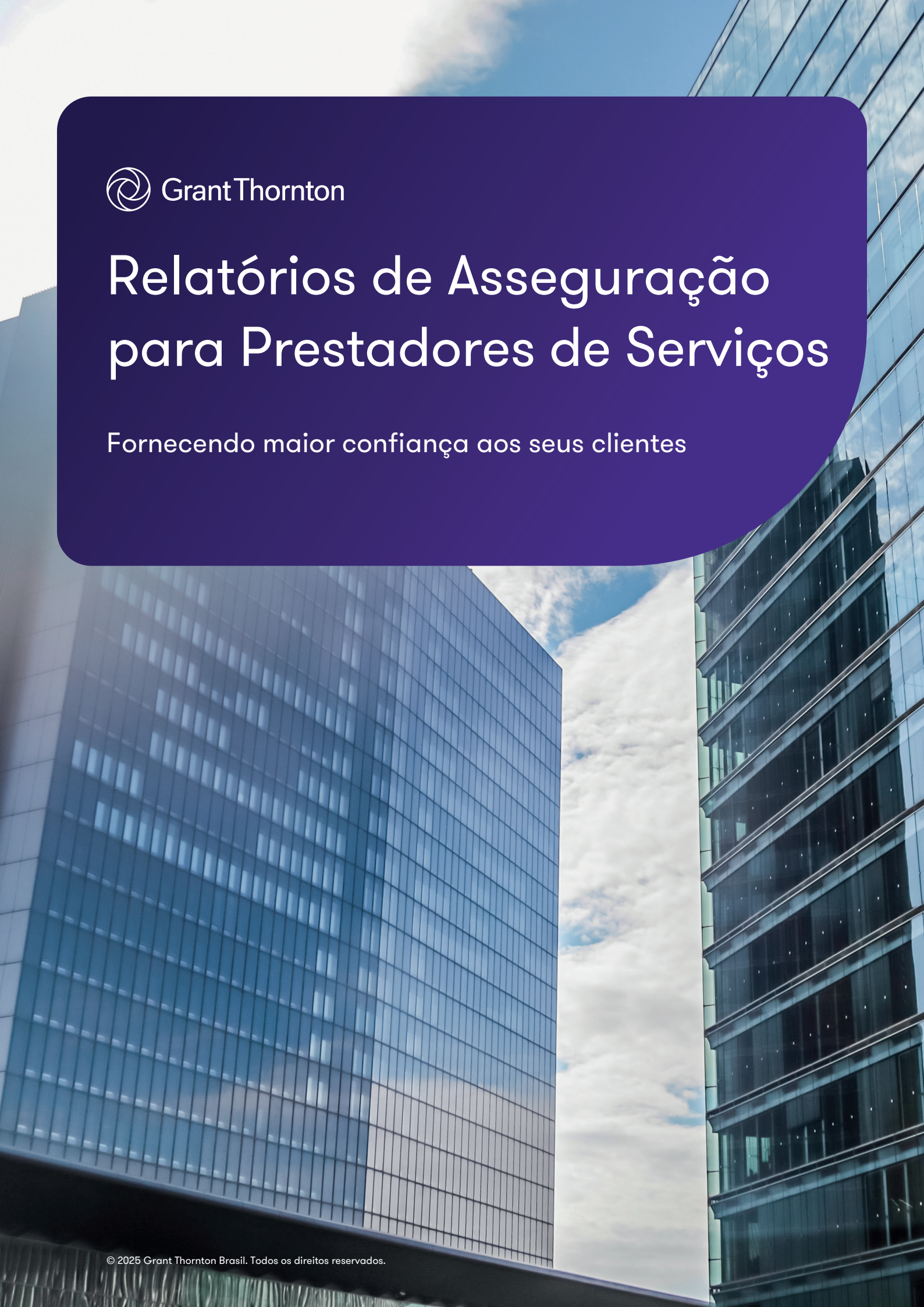


Grant Thornton

Relatórios de Asseguração para Prestadores de Serviços

Fornecendo maior confiança aos seus clientes

Conteúdo

Abordagem padronizada para asseguração

Os Relatórios de Asseguração para Prestadores de Serviço (*Service Auditor Reports* – SARs) ajudam as empresas prestadoras de serviços a construírem confiança com uma variedade de *stakeholders*, e podem eliminar a necessidade de auditorias anuais. No entanto, encontrar a solução ideal pode ser um desafio. Analisamos os diferentes tipos de relatórios disponíveis para ajudar sua organização a identificar a abordagem correta.

A terceirização tem se tornado uma prática comum para que as empresas expandam suas linhas de serviços e adotem novas tecnologias de maneira acessível e sustentável. Contudo, independentemente de uma atividade ser realizada internamente ou por um provedor terceirizado, ela deve atender às mesmas expectativas de qualidade, segurança e resiliência. Por isso, é essencial obter asseguração adequada dos provedores de serviços, garantindo que os usuários finais mantenham sua responsabilidade perante clientes, reguladores e outras partes interessadas.

Os relatórios SAR fornecem asseguração padronizada para demonstrar que as empresas prestadoras de serviços terceirizados operam controles eficazes. Esses relatórios são amplamente utilizados em setores como financeiro, tecnologia, hospedagem de *data centers*, gestão de ativos e processamento de pagamentos. No Brasil, as normas ISAE 3402 e ISAE 3000 (bem como as normas equivalentes NBC TO 3402 e 3000) e os relatórios SOC 1, SOC 2 e SOC 3 são amplamente reconhecidos como os padrões para avaliação e auditoria de controles internos de uma organização prestadora de serviço.

Navegando pelos diferentes tipos de relatórios

Para maximizar o valor dos relatórios SAR, é essencial escolher o tipo certo de relatório, considerando as necessidades de seus clientes e o contexto regulatório.

Relatórios para reportes financeiros

Os relatórios ISAE 3402 e SOC 1 podem ser úteis para empresas de todos os setores, incluindo bancos, fundos de pensão, administradores de propriedades, provedores de TI ou serviços de software. Todos os padrões se alinham a julgamentos específicos, então é importante considerar os territórios em que seus clientes estão baseados:

- ISAE 3402 é uma norma internacional
- SOC 1 é uma norma dos EUA/global
- NBC TO 3402 é uma norma para fins locais

ISAE 3402

Aplica-se globalmente e fornece asseguração sobre controles que impactam a demonstrações financeiras dos clientes das empresas prestadoras de serviço. É amplamente utilizado por empresas de tecnologia, processamento de folha de pagamento, administração de ativos e serviços financeiros.

SOC 1

Derivado dos padrões SSAE 18 nos EUA, é semelhante ao ISAE 3402, mas preferido por empresas americanas. Esses relatórios focam em controles relacionados à precisão e integridade das demonstrações financeiras dos clientes da empresa prestadora de serviço.

NBC TO 3402

Semelhante ao ISAE 3402, sendo este relatório de uso apenas local no Brasil, também com foco em controles relacionados à precisão das demonstrações financeiras.

Relatórios para propósitos não financeiros

SOC 2

Avalia categorias de segurança, disponibilidade, integridade de processamento, confidencialidade e privacidade. É amplamente usado por provedores de tecnologia, *Software as a Service* (SaaS), como empresas de computação em nuvem.

SOC 3

Semelhante ao SOC 2, mas com um nível menor de detalhamento. Pode ser compartilhado publicamente, tornando-o ideal para divulgação ao mercado.

Um exemplo de escopo para relatórios financeiros pode incluir:

- Processos de aceitação de novos clientes
- Procedimentos para processamento e relatórios de transações
- Registros contábeis do Sistema
- Tratamento de eventos e condições significativas além de transações
- Preparação de relatórios para usuários
- Suporte a controles gerais de TI

Guia rápido

Qual tipo de relatório?

Relatórios financeiros	Relatórios não financeiros
• ISAE 3402 (Global)	• SOC 2 (Global)
• SOC 1 (EUA/Global)	• SOC 3 (Global)
• NBC TO 3402 (BR/Local)	• ISAE 3000 (Global)
	• NBC TO 3000 (BR/Local)

Qual nível de asseguração?

Tipo 1	Tipo 2
Avaliação da adequação dos controles em um ponto específico no tempo (ou seja, adequação do projeto de controles)	Avaliação da adequação dos controles durante um período de tempo específico (ou seja, eficácia)

Qual período de asseguração?

6 meses ou **9 meses** ou **12 meses**

Quais são as categorias de serviços confiáveis?

As categorias de serviços confiáveis fornecem uma estrutura para o SAR.

Segurança

Assegura ao cliente que os dados estão protegidos contra acesso não autorizado

Disponibilidade

Atesta que os sistemas necessários para armazenar e processar dados estarão disponíveis para uso

Integridade de processamento

Exige que o processamento de dados seja preciso e completo

Confidencialidade

Garante que as informações rotuladas como sensíveis/confidenciais sejam protegidas como tal

Privacidade

Alinha as práticas de tratamento de dados com a política de privacidade da sua organização para assegurar que as informações pessoais sejam tratadas e armazenadas adequadamente

Qual nível de asseguração você precisa?

Para tornar ainda mais complexa a escolha da revisão mais adequada para o seu negócio, os relatórios de auditoria de serviços são categorizados em Tipo 1 e Tipo 2.

Conforme descrito nas páginas anteriores, esses relatórios diferem de acordo com o tópico em análise. Em contrapartida, o tipo 1 *versus* o tipo 2 é sobre o nível de asseguração e a profundidade do relatório.

Seus clientes frequentemente o aconselharão sobre o tipo de relatório de que precisam, geralmente um tipo 2, pois este fornece o maior nível de garantia. Mas se esta for sua primeira vez, seria melhor começar com um tipo 1, pois ele permite o desenvolvimento e a maturidade de controles relevantes. As principais diferenças a serem consideradas são descritas abaixo.

1

Relatório SAR - Tipo 1

Avalia a adequação do design dos controles em um momento específico. É recomendado para organizações que estão iniciando o processo de asseguração.

2

Relatório SAR - Tipo 2

Avalia a operação efetiva dos controles ao longo de um período específico (ex.: 6 ou 12 meses). Proporciona maior nível de confiança e é geralmente exigido por clientes mais maduros.

Readiness Assessment

Antes de iniciar um processo formal de asseguração, é recomendada uma etapa preparatória, conhecida como *Readiness Assessment*. Essa fase permite avaliar o *framework* de controles existente, identificando *gaps* ou fragilidades que possam comprometer o sucesso do relatório. É uma abordagem estratégica que auxilia na maturidade do ambiente de controles antes do exame formal.

Escolhendo o período de asseguração correto

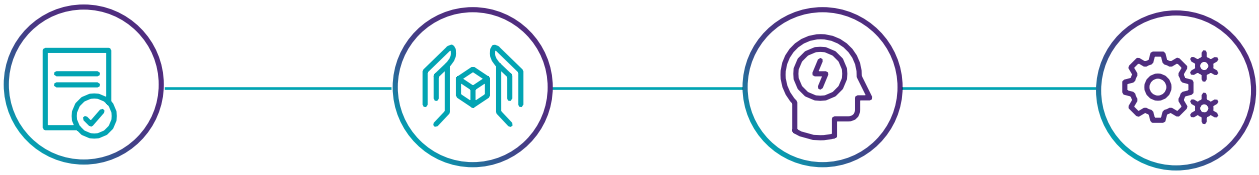
É comum que um SAR forneça uma asseguração razoável por um período de 12 meses, mas ocasionalmente eles podem ser projetados para cobrir períodos mais longos ou mais curtos, por exemplo, seis meses, se necessário, para atender a um prazo específico do cliente.

Esta decisão é influenciada pelo tipo de asseguração necessária para você ou seus clientes e quão maduro é o seu ambiente de controle. Comprometer-se a entregar um relatório de eficácia operacional tipo 2 cobrindo um período de seis meses quando seu ambiente de controle ainda está em desenvolvimento, ou não está operando efetivamente, pode ser uma abordagem arriscada. Neste caso, um relatório de asseguração somente de Desenho (Tipo 1) seria mais realista até que seu ambiente de controle tenha evoluído mais.

Os relatórios tipo 2 fornecem um nível mais alto de asseguração, mas você precisará estar confiante de que seus controles estão operando efetivamente por um período de tempo mais longo. Se seu ambiente de controle ainda não estiver pronto, o SAR pode identificar exceções de controle e resultar em uma opinião "modificada". Uma boa estratégia seria começar com um relatório do tipo 1 no primeiro ano, seguido por um tipo 2 nos anos subsequentes, quando você tiver evidências suficientes de que seus controles estão operando efetivamente.

Maximizando o valor do processo SAR

O processo SAR oferece uma série de benefícios, incluindo:



Impulsionar seu processo de vendas e desenvolvimento de negócios: oferece aos clientes potenciais um Relatório de Asseguração reconhecido no mercado

Redução da fadiga de auditoria: agiliza o processo, economizando tempo e recursos

Novos insights: ajuda a identificar soluções para fortalecer e adaptar controles em contextos de mudanças

Melhoria do ambiente de controle: identifica controles redundantes, promove eficiência e melhora a cultura de gerenciamento de riscos

Revisão de relatórios existentes

Mesmo para empresas que já emitem relatórios, é importante revisitar as práticas atuais. Na Grant Thornton Brasil, contamos com uma equipe experiente e podemos agregar valor ao:

1

Entender suas necessidades

Por onde começar

- Revisar relatórios e experiências do ano anterior
- Sugerir melhorias – formato, escopo, abordagens, controles
- Confirmar seus principais marcos
- **Valor que podemos agregar:** Garantir que suas partes interessadas estejam totalmente alinhadas com o direcionamento do projeto, marcos críticos de entrega e uma abordagem "sem surpresas".

2

Planejar

Fundamental para que todas as partes interessadas estejam consideradas

- Concordar com cronogramas, plano de projeto e protocolos de comunicação
- Reunião(ões) introdutória(s) com todos os proprietários de controle
- Concordar com os prazos para recebimento de evidências e respostas a consultas
- Orientações com os donos de controle
- Solicitações e rastreamento automatizados de evidências para melhorar a eficiência e responsabilizar os donos de controle pela entrega
- **Valor que podemos agregar:** Nossa abordagem transparente e colaborativa com os donos de controle ajuda a esclarecer sua compreensão do processo e dos requisitos.

3

Realizar trabalho de campo

Abordagem de entrega proativa

- Testes realizados de acordo com o padrão técnico aplicável por uma equipe qualificada e experiente
- As evidências são submetidas a triagem após o recebimento para garantir a validade em tempo hábil
- Revisão e controle de qualidade em tempo hábil para evitar surpresas
- Comunicação tempestiva e discussões de exceções com os donos de controle
- **Valor que podemos agregar:** equipe experiente para realizar testes de forma eficaz e eficiente, além de gerenciar eventuais deficiências/exceções de maneira tempestiva e objetiva.

4

Automatizar fluxos e relatórios

Documentando resultados

- Uso de ferramenta automatizada para fornecer eficiência nos procedimentos de auditoria
- Nossa ferramenta ajudará na documentação dos testes e elaboração do relatório de forma tempestiva.
- **Valor que podemos agregar:** iremos relatar quaisquer exceções assim que as identificarmos, permitindo a você o tempo máximo para investigar quaisquer controles de mitigação para possíveis exceções ou possíveis ressalvas na opinião do auditor.

5

Melhorar continuamente

- Realizar um exercício de lição aprendida bidirecional
- Discussões para identificar soluções para mitigar o risco de exceção na próxima vez
- Identificar potenciais eficiências para o próximo ano
- **Valor que podemos agregar:** Forneceremos uma lista de todas as oportunidades de melhoria em seus processos de negócios e TI que identificamos durante a execução do trabalho de campo.

Estudo de Caso

Desafio

Uma *fintech* brasileira especializada em soluções de pagamentos digitais enfrentava dificuldades em expandir suas operações para os Estados Unidos. Empresas americanas exigiam comprovação do relatório SOC 2 antes de fechar contratos, o que limitava a adoção do produto no mercado americano.

Solução

Colaboramos com a equipe para a emissão do relatório SOC 2, adotando uma abordagem ágil e adaptada às necessidades da fintech, garantindo conformidade com os padrões internacionais e americano.

Resultados

Com a obtenção do relatório SOC 2, a *fintech* conseguiu demonstrar credibilidade e segurança aos parceiros americanos. Como resultado, assinou seus primeiros contratos nos EUA, expandindo seu mercado e aumentando significativamente sua base de clientes internacionais.

Soluções Adicionais em Asseguração e Avaliação de Controles

Para ampliar nosso portfólio e atender às demandas crescentes do mercado, apresentamos outros serviços relacionados à asseguração e avaliação de controles:

1

Relatórios de Controles em Conformidade com Normas Específicas

- Avaliações e relatórios personalizados para conformidade com regulamentações como LGPD (Lei Geral de Proteção de Dados), ISO 27001, NIST e COBIT.
- **Benefícios:** Demonstração de conformidade com legislações locais e internacionais, promovendo confiança de clientes e reguladores.

2

Auditorias de Terceiros e Fornecedores (*Third-Party Risk Management*)

- Avaliação de riscos e controles de terceiros para garantir segurança e continuidade.
- **Benefícios:** Redução de riscos associados à terceirização e maior visibilidade sobre a cadeia de fornecimento.

3

Auditorias de Monitoramento Contínuo e Automática

- Implementação de ferramentas de monitoramento contínuo para avaliação de controles.
- **Benefícios:** Detecção proativa de falhas em controles e maior eficiência operacional.

4

Avaliação de Riscos em Implementação de Sistemas

- Análise de riscos durante implementações tecnológicas, como ERPs e sistemas em nuvem.
- **Benefícios:** Garantia de que os objetivos de controle sejam atendidos durante transições críticas.

5

Avaliação e Asseguração de Riscos Cibernéticos

- Auditorias de segurança cibernética, incluindo testes de invasão e asseguração contra *ransomware*.
- **Benefícios:** Mitigação de riscos digitais e fortalecimento da resiliência contra-ataques

6

Relatórios de Sustentabilidade e ESG

- Asseguração sobre informações de sustentabilidade e práticas ambientais, sociais e de governança.
- **Benefícios:** Transparência para investidores e *stakeholders* preocupados com ESG.

Com esses serviços, reforçamos nosso compromisso em fornecer soluções inovadoras e adaptadas às necessidades de nossos clientes, ajudando-os a superar desafios regulatórios e operacionais.

Trabalhando conosco

Na Grant Thornton, fornecemos serviços de asseguração SOC baseados nos padrões locais e internacionais, ajudando empresas a gerenciar riscos com eficiência e confiança.

A natureza global da nossa base de clientes significa que todas as nossas tarefas de garantia independentes são entregues de forma consistente em todo o mundo, com todas as firmas-membro entregando uma metodologia única, testada e aprovada. Isso fornece uma enorme base de qualidade e experiência para o benefício de nossos clientes.

Entre em contato conosco

Marcos Tondin
Líder de IT Risk
E marcos.tondin@br.gt.com
T +55 11 3886 5100

Maikon Silva
Sócio de IT Risk
E maikon.silva@br.gt.com
T +55 11 3886 5100

Grant Thornton

granthornton.com.br