



METODOLOGIA DE ATENDIMENTO PARA Certificação SOC

CONTROLE DE ORGANIZAÇÃO DE SERVIÇO

O que são relatórios SOC?

Relatórios SOC são uma forma de as empresas verificarem, por meio de garantia independente de terceiros, que prestadores de serviços têm controles apropriados em vigor e seguem os padrões da indústria antes terceirizar uma função de negócios para essa organização. Isto dá aos prestadores de serviços uma oportunidade para estabelecer credibilidade e construir confiança com clientes, investidores, parceiros de negócios e auditores ao mesmo tempo em que obtém uma vantagem competitiva no mercado. Todos os exames SOC são realizados conforme

AICPA guidelines :

Durante o processo de **Implementação SOC** uma equipe experiente de consultores de tecnologia e os auditores trabalharão em estreita colaboração com a liderança da sua organização para garantir que:

- O relatório SOC final é adaptado de forma completa e oportuna às necessidades exclusivas de uma organização.
- As operações comerciais e os processos de controle interno são simplificados.
- As obrigações contratuais e as preocupações do mercado são cumpridas.
- Os requisitos de relatórios do AICPA são atendidos.

Como determino o tipo de relatório SOC Minhas necessidades de negócios?

Existem duas razões principais para se submeter a uma avaliação e certificação SOC:

- Um cliente ou cliente potencial ou auditor solicita um relatório SOC.
- Sua organização decide obter conformidade social de forma proativa.

No primeiro cenário, o solicitante provavelmente poderá especificar o tipo de relatório SOC necessário. Em qualquer um cenário, uma organização deve primeiro considerar seus objetivos. Normalmente, o resultado desejado para qualquer organização é demonstrar seu compromisso com o design apropriado e operação eficaz do seu ambiente de controle interno.

Gráfico de comparação SOC 1, 2 e 3

Existem 3 tipos distintos de relatórios SOC - SOC 1, SOC 2 e SOC 3. Cada relatório varia, mas fornece informações valiosas que são necessárias para avaliar os riscos e controles internos associados com um prestador de serviços terceirizado. É necessário um auditor terceirizado e independente para examinar e afirmar vários aspectos de uma organização antes de produzir o relatório final.

SOC 1	SOC 2	SOC 3
Relatório sobre o seu interno controles relacionados a finanças informações ou declarações. Compartilhado principalmente para auditores Aplicável a empresas qual processo financeiro informações como médicos Processamento de reclamações, folha de pagamento Serviços, empréstimos etc.	Relatório sobre seus controles internos relacionado a cinco serviços de confiança princípios: segurança, disponibilidade, integridade, confidencialidade e privacidade. Compartilhado principalmente com clientes e partes interessadas Aplicável a qualquer empresa de tecnologia que está no processamento de informações. Baseado em produtos e serviços empresas.	Relatório sobre os resultados de SOC 2 de maneira adequada para audiência pública. Compartilhado para o público em geral Aplicável a qualquer público empreendimento que possui SOC 2 verificado e deseja para produzir um relatório SOC 3 para um público maior.

CERTIFICAÇÃO SOC 1



Um relatório SOC 2 concentra-se nos controles da sua organização relevantes para o desempenho financeiro de uma entidade usuária. É um exame hiperdetalhado que requer uma compreensão especializada da indústria e ambiente de controle relacionado. A organização de serviços normalmente especifica seus objetivos de controle e atividades de controle relacionadas com base nos serviços específicos que executam.

Um relatório SOC 1 geralmente inclui controles de processos de negócios envolvendo o desempenho. Um SOC 1 O relatório geralmente inclui controles de processos de negócios que envolvem a integridade e a precisão de transações, bem como controles gerais de tecnologia da informação, como segurança de rede e acesso lógico.

Dado o âmbito limitado, um relatório SOC 1 é mais adequado para organizações que devem incutir confiança em seus controles e seguranças sobre os dados financeiros de seus clientes. Muitas vezes é necessário quando uma entidade usuária é de capital aberto e deve cumprir a SOX 404 ou similar regulamentos. Aqui estão alguns exemplos:



**Manutenção de registros
Services**



**Reivindicações
médicas processa-
mento**



**Serviços de folha de
pagamento**



**Serviços de
empréstimo**

CERTIFICAÇÃO SOC 2



Um relatório SOC 2 é para organizações de serviços cujas entidades usuárias não respondem necessariamente controles para relatórios financeiros, permitindo que os provedores atendam às necessidades de uma gama mais ampla de entidades usuárias.

Um exame SOC 2 concentra-se principalmente em como os dados são armazenados e protegidos, especificamente controles relacionados aos compromissos de serviço e requisitos do sistema com base nos requisitos do AICPA critérios de serviços de confiança (definidos abaixo).

- **Segurança** – As informações e os sistemas são protegidos contra acesso não autorizado, divulgação de informação
- **Disponibilidade** – As informações e os sistemas estão disponíveis para operação e uso para atender às necessidades da entidade. objetivos
- **Integridade de Processamento** – O processamento do sistema é completo, válido, preciso, oportuno e autorizado a cumprir os objetivos da entidade
- **confidencialmente** – As informações designadas como confidenciais são protegidas para atender aos requisitos da entidade. objetivos
- **Privacidade** – As informações pessoais são coletadas, usadas, retidas, divulgadas e descartadas para atender os objetivos da entidade

Os relatórios SOC 2 podem ser disponibilizados por qualquer empresa de tecnologia que Você está interessado no processamento de informações. Embora os relatórios SOC 1 e SOC 2 tenham públicos restritos, os relatórios SOC 2 podem ser entregues a outras partes, como potenciais clientes, profissionais de gerenciamento de fornecedores, reguladores e outros parceiros comerciais importantes.

CERTIFICAÇÃO SOC 3



Tal como o SOC 2, os relatórios do SOC 3 centram-se nos controlos relevantes para os cinco serviços de confiança do AICPA categorias. No entanto, ao contrário do SOC 2, os relatórios do SOC 3 são certificados e podem ser tornados públicos disponíveis, tornando-os ferramentas valiosas para comercializar a eficácia do seu controle ambiente.

Caso você deseje um relatório SOC 3, sua organização deve primeiro preencher um relatório SOC 2, Tipo 2 exame (mais sobre os tipos de relatório abaixo). Os exames SOC 2 e SOC 3 podem ser realizados em uma ou mais categorias de serviços de confiança. Os relatórios SOC 3 contêm praticamente o mesmo informações incluídas nos relatórios SOC 2, exceto com uma descrição muito menos detalhada do seu controles relacionados à conformidade e operações. Eles também não incluem controle específico atividades, procedimentos de teste ou resultados detalhados sobre a eficácia operacional.

TIPO 1 vs. TIPO 2

Todos os relatórios SOC (exceto SOC 3) podem ser do Tipo 1 ou do Tipo 2. A diferença é com base principalmente no período no escopo

- **Relatório Tipo 1:** Um RELATÓRIO TIPO 1 descreve a adequação do serviço por parte de uma organização de serviços. projeto e implementação de controles em um momento específico.
- **Relatório Tipo 2:** UM RELATÓRIO TIPO 2 garante que as atividades de controle definidas sejam consistentemente operando efetivamente durante um período definido, que geralmente é de 6 meses a 1 ano, gerando assim melhor desempenho operacional.

Em muitos casos, uma organização de serviços começará com um relatório Tipo 1 para definir o controle atividades, a partir de um determinado momento. Uma vez projetados e implementados os controles, o Tipo 2, o relatório viria a seguir. Como o relatório Tipo 2 cobre um período (ou seja, 6 ou 12 meses), este relatório é mais valioso para os usuários porque garante que, durante um período, os controles estavam operando efetivamente. Uma organização normalmente contrata uma empresa de auditoria para preencher o relatório Tipo 2, anualmente.

Como me preparo para uma avaliação SOC?



Ao iniciar sua primeira avaliação SOC, é benéfico trabalhar com o fornecedor terceirizado selecionado ou consultor como nós para realizar uma avaliação inicial de lacunas, permitindo-lhe remediar quaisquer lacunas antes do início do processo de relatório do SOC. Seguir esse caminho ajuda você a preencher o espaço existente lacunas em seu sistema atual, produzindo assim um sistema muito mais compatível e muito próximo para cumprir os requisitos do SOC. Embora cada relatório SOC tenha escopo diferente, há certas áreas de foco essenciais para todas as avaliações SOC. Ao focar nas seguintes tarefas, uma organização pode começar a preparar seus funcionários para um ambiente de controle mais forte e portanto, uma avaliação SOC mais eficiente.

DOCUMENTAÇÃO

Do ponto de vista dos auditores, se não estiver documentado, então não existe. Embora possa haver fortes controles internos em vigor, a evidência da ocorrência poderá não ser registrada. Garantir documentação é mantida para apoiar todos os controles em vigor (por exemplo, aprovação para concessões de acesso, reconhecimentos de funcionários, manutenção de populações, etc.).

POLÍTICAS E PROCEDIMENTOS DEFINIDOS

Para garantir que todas as partes relevantes entendam suas responsabilidades para cumprir objetivos, garantir que os processos e procedimentos fundamentais sejam documentados. Isto fornece um recurso para que os funcionários e os auditores entendam a intenção da organização dentro do ambiente de controle. O âmbito das políticas deve incluir:

- » Procedimentos organizacionais para cumprir obrigações contratuais
- » Meios de cumprir os principais compromissos de serviço e requisitos do sistema
- » Abordagem de gestão de risco

AValiação DE RISCO

Um processo formalizado facilitado por uma discussão anual de avaliação de risco e aprovado pelo conselho de administração ou gestão executiva. Em vez de uma avaliação de risco anual formal, uma organização também pode optar por realizar reuniões trimestrais para discutir mudanças nas ameaças, operações comerciais, etc., e seu impacto na avaliação geral de riscos. A avaliação de risco deve incluir níveis de risco definidos (ou seja, ameaça baixa, média e alta) e a abordagem de remediação da empresa (ou seja, aceitar, mitigar ou eliminar) com detalhes sobre como a empresa respondeu ou planeja responder no futuro.

Roteiro de implementação do SOC

Embora cada relatório SOC tenha requisitos e objetivos diferentes, cada um é geralmente realizado seguindo sete etapas principais

ESTÁGIO DO PROCESSO		PRINCIPAIS PARTICIPANTES	MATERIAIS CHAVE
1	Escopo	Alta Administração Auditores, Consultores	Antecedentes organizacionais necessidades e exigência do cliente
2	Passo a passo e Projeto de controle	Consultor, Proprietários de Processos	Políticas e procedimentos existentes, materiais do tempo gasto com cada proprietário do processo
3	Avaliação de lacunas	Consultor, Proprietários de Processos	Documentação preliminar para roteiro de remediação de suporte
4	Correção	Consultor, Proprietários de Processos	Documentação para validação do ambiente de controle
5	Teste de exame	Auditor, Consultor, Processo Proprietárias	Documentação do processo, prova de exame
6	Relatório	Auditores CPA	Políticas e procedimentos, rascunho de feedback, resposta a feedback e exceções
7	Emissão	Auditores CPA	Relatório SOC

Mesmo com os exames do primeiro ano, a maioria das etapas pode ser concluída dentro de um período definido. O cronograma, embora o mais imprevisível dos estágios, é a remediação (estágio 4). O nível de esforço despendido na remediação é determinado com base nos resultados da lacuna avaliação (etapa 3). Durante a fase de avaliação, sua empresa de auditoria fornecerá um roteiro de remediação para garantir a conformidade com os critérios SOC aplicáveis. Ao criar um ambiente de controle forte antes do início do exame, você está definindo o base para uma auditoria organizada e minimamente perturbadora.

Serviços de auditoria SOC



Nossa equipe experiente aconselha organizações de serviços sobre os requisitos de relatórios SOC do AICPA. Fornecemos informações valiosas que clientes, clientes potenciais e auditores precisam para avaliar os riscos e controles internos associados a um prestador de serviços terceirizado.

Como empresa de consultoria qualificada neste espaço, tivemos inúmeras conversas sobre educação, valor e eficiência. Temos orgulho em trabalhar com organizações que possuem necessidades, prioridades concorrentes, restrições de tempo e outros objetivos exclusivos. Nós entendemos o valor do tempo, planejamento apropriado e educação que garantem um exame perfeito progredir.

Sobre TOPCertifier

TOPCertifier é uma empresa de consultoria de gestão reconhecida mundialmente e especializada em informações serviços de segurança e avaliações sociais.

Com sede em Bangalore (Índia), atuamos em mais de 20 países com destaque especial concentre-se nos EUA, Europa e países do Golfo. Também temos uma presença impressionante na Ásia-Regiões do Pacífico e África. Aconselhamos mais de 2.800 organizações, abrangendo numerosos indústrias, em soluções contábeis, fiscais, de lucratividade e de processos de negócios, desde o nosso início em janeiro de 2010. Com uma equipe de mais de 200 consultores especializados do setor, auditores líderes certificados e Especialistas no assunto, entregamos um histórico de 100% em termos de nossa certificação taxa de sucesso.



Obrigado

PARA SABER MAIS,
VISIT WWW.TOPCERTIFIER.COM