WHITEPAPER

Entendendo a importância da Certificação SOC 2

segura® | Futureproof Identity Security | segura.security

Introdução

A Certificação SOC 2 é fundamental para garantir a segurança e a conformidade de uma organização. Ela aumenta a competitividade, já que os clientes preferem trabalhar com fornecedores seguros e confiáveis. Além disso, os critérios da SOC 2 facilitam a obtenção de outras certificações importantes, como ISO 27001 e HIPAA. Esta certificação oferece inúmeras vantagens para as organizações.

Com a digitalização crescente, a segurança da informação é cada vez mais importante para empresas de todos os portes e segmentos, incluindo aquelas que confiam em fornecedores especializados para conduzir suas operações principais. A falta de proteção adequada dos dados pode expor uma empresa a riscos, como ataques de malware, extorsão e roubo de informações.

A SOC 2 é uma norma de auditoria que garante a gestão segura dos dados por parte dos provedores de serviços, preservando a privacidade dos clientes e protegendo os interesses da empresa.

Este whitepaper fornecerá uma visão mais detalhada sobre o que é a SOC 2, seus princípios e benefícios, além de outras informações relevantes sobre o tema. Leia até o final para obter uma compreensão completa.

O que é a Certificação SOC 2

A SOC 2 é uma estrutura de conformidade de segurança cibernética criada pelo American Institute of Certified Public Accountants (AICPA) para garantir o armazenamento e processamento seguro de dados por parte de provedores terceirizados. Esta estrutura define requisitos para manter altos padrões de segurança de dados com base nos seguintes princípios:

- Segurança;
- Privacidade;
- Disponibilidade;
- Confidencialidade;
- Integridade de processamento.

Nem todos os países adotam a SOC 2 como uma forma de validar que a corporação armazena e processa de maneira segura os dados, porém, com a privacidade dos usuários se tornando um prioridade global, esse contexto deve ser revertido nos próximos anos.

Em todo caso, é importante saber que existem três relatórios de auditoria SOC diferentes (SOC 1, SOC 2 e SOC 3) e, dentro de cada um deles, dois tipos.

Relatórios de auditoria SOC

Conforme mencionamos anteriormente, existem três relatórios de auditoria SOC diferentes. São eles:

- **SOC 1:** examina os relatórios financeiros de uma organização.
- **SOC 2:** avalia como a empresa se compromete com controles internos associados a um ou mais critérios de serviços de confiança do AICPA — disponibilidade, segurança, integridade de processamento, confidencialidade e privacidade;
- **SOC 3:** é uma releitura da SOC 2, interpretada visando ampla distribuição, de modo a ser compreensível pelo público em geral.

Os relatórios de auditoria SOC 1 e SOC 2 ainda podem ser dos Tipos I e II. No Tipo I avalia-se os controles pontualmente e, no Tipo II, é analisada a eficiência desses controles dentro de um determinado período de tempo, que pode ser de seis meses até um ano. Por sua vez, o relatório de auditoria SOC 3 é fundamentado nos resultados de uma avaliação SOC 2 Tipo II.

Dentre todas estas alternativas, o relatório SOC 2 Tipo II é o mais criterioso. Sendo assim, uma auditoria SOC 2 Tipo II garante às organizações a validação perante um auditor externo sobre a adequação e eficácia de seus controles de dados, cobrindo aspectos como:

- Controles de acesso lógico e físico;
- Operações do sistema;
- Gerenciamento de mudanças;
- Mitigação de riscos.

Os 5 princípios da SOC 2

O American Institute of Certified Public Accountants define que a SOC 2 é uma estrutura que os provedores de serviço devem utilizar para auditar e relatar como funciona seu gerenciamento de dados confidenciais.

Na prática, a SOC 2 se refere a um conjunto de normas e diretrizes que descrevem como uma organização deve garantir cinco princípios, ou critérios de confiança. As empresas definem o escopo da certificação com base na seleção dos princípios, tendo a obrigatoriedade sobre o princípio de segurança. Confira, a seguir, os cinco princípios:

Princípio 1 — Segurança

Em uma abordagem de Confiança Zero, é necessário autenticar e autorizar usuários humanos e máquinas, sem exceção. O princípio de segurança SOC 2 engloba o design de segurança de aplicativos e o modo como é efetuado o controle e proteção de informações confidenciais, incluindo propriedade intelectual, dados financeiros e informações de identificação pessoal (PII).Nesta abordagem, SOC 2 valida os controles de acesso, uso de Múltiplo Fator de Autenticação (MFA) e detecção de intrusão, e proteção de ameaças.

Princípio 2 — Disponibilidade

A expectativa dos usuários é que serviços disponibilizados em nuvem possam ser utilizados a qualquer momento. Desse modo, o princípio da disponibilidade analisa se os provedores do serviço são capazes de manter a disponibilidade, monitorando a performance junto a processos necessários para responder a incidentes de segurança.

O princípio de segurança Zero Trust requer recursos de monitoramento que possibilitem às empresas analisar e identificar rapidamente ameaças respondendo a incidentes de segurança de forma adequada.

Princípio 3 — Integridade do Processamento

Este princípio se concentra em como os dados são processados. A qualidade e os controles de monitoramento permitem que as empresas validem a segurança dos processos de armazenamento, entrega, modificação e retenção de dados.

Porém, para lidar com os controles que garantem a proteção dos dados dos clientes, é necessário que a organização se prepare para isso.

Essa preparação é um aspecto essencial da abordagem Confiança Zero, pois permite à empresa manter-se pronta para detectar e responder ameaças, antes que os agentes maliciosos obtenham privilégios que, por consequência, causem grandes danos.

Princípio 4 — Confidencialidade

A confidencialidade é indispensável, especialmente no caso de sistemas SaaS distribuídos. É essencial que as organizações garantam que seus dados classificados como confidenciais ou sigilosos estejam efetivamente protegidos contra acesso indevido. A SOC 2 valida a forma de proteção por meio de controles de acesso, criptografia de dados e firewalls.

Na abordagem Zero Trust, as soluções de segurança validam as identidades individuais, protegendo o acesso a ambientes críticos. Para isso, é necessário autenticar essa identidade de modo preciso, autorizá-la e permitir seu acesso, restringindo o privilégio sobre os ativos considerados confidenciais e podendo auditar a qualquer momento.

Deste modo, provê transparência sobre a conformidade com as políticas de segurança e, por sua vez, do processo.

Princípio 5 — Privacidade

O princípio de privacidade analisa como o aplicativo ou serviço processa informação fornecida ou gerada por um indivíduo, tendo base na política de dados nos Princípios de Privacidade Geralmente Aceitos (GAPP) da AICPA.

Assim, controles de acesso adequados devem ser adotados a fim de evitar acesso e privilégios indevidos. Para isso, é imperativo verificar usuários, validar dispositivos, e limitar o acesso privilegiado por meio de uma abordagem Zero Trust.

Benefícios da conformidade com a SOC 2

Confira alguns benefícios de possuir a certificação SOC 2:

A conformidade com a SOC 2 comprova que sua empresa tomou todas as medidas necessárias para prevenir violações de dados e melhorar sua reputação no mercado, além de conquistar a confiança de seus clientes.

Essa certificação também pode lhe dar uma vantagem competitiva sobre outras organizações do mesmo setor, pois muitos clientes preferem fornecedores seguros e capazes de evitar violações de dados, e a conformidade com a SOC 2 é uma forma de demonstrar a segurança da sua empresa.

Ter um relatório SOC 2 também pode ser uma vantagem de marketing para sua organização, já que muitas empresas concorrentes não possuem essa certificação para comprovar sua segurança.

A adoção das melhores práticas de segurança e eficiência operacional, que permitem a obtenção da certificação SOC 2, pode otimizar os processos e controles de sua organização, baseados no conhecimento dos riscos de segurança digital enfrentados por seus clientes.

Os critérios da SOC 2 facilitam o processo de obtenção do ISO 27001 e do HIPAA, pois são estruturas complementares.

Estar em conformidade com a SOC 2 demonstra sua capacidade de proteger a segurança cibernética de seus clientes, evitando violações e preservando seus dados privilegiados, além de evidenciar o seu compromisso com a segurança geral de TI e sua conformidade com as melhores práticas do setor.

A certificação SOC 2 garante a eficácia do ambiente de controle e segurança da informação, já que os critérios de auditoria para o SOC 2 Tipo II exigem a comprovação da eficácia operacional dos controles em vigor por pelo menos seis meses.

Um relatório SOC 2 fornece informações valiosas sobre os riscos enfrentados pela sua organização e sua postura de segurança, incluindo aspectos como gestão de fornecedores, controles internos, governança e supervisão regulatória, entre outros.

A importância da certificação SOC 2 para a Segura®

Nós, da Segura®, buscamos trabalhar de acordo com as melhores práticas de segurança do mercado. Por isso, em 2022, conquistamos a certificação SOC 2 Tipo II para o SaaS 360o, nossa solução em nuvem. A análise para a conformidade com a SOC 2 foi realizada entre 1o de junho de 2022 e 30 de novembro de 2022, utilizando informações sobre os controles do sistema que a Segura® projetou.

Esta avaliação se baseou nos critérios de serviços de confiança relevantes para segurança, disponibilidade, integridade de processamento, confidencialidade e privacidade — requisitos estabelecidos pelo AICPA.

O relatório SOC 2 detalhou os seguintes aspectos:

- A natureza dos serviços prestados pela empresa;
- Como o sistema da empresa interage com usuários, parceiros comerciais, prestadores de serviços e outras partes;
- Controles internos e suas limitações;
- Controles complementares do usuário e da sua empresa, incluindo como esses controles trabalham em conjunto com os controles da empresa para atingir os compromissos de serviço e os requisitos do sistema;
- Responsabilidades do usuário e como elas podem afetar sua capacidade de usar efetivamente os serviços da empresa;
- Critérios de confiança de serviços aplicáveis;
- Riscos que ameaçam o cumprimento dos compromissos de serviço e requisitos do sistema da empresa, e como os controles lidam com esses riscos.

Conclusão

Neste WhitePaper, explicamos o que é o SOC 2 e a avaliação realizada durante uma auditoria, abordamos sua importância para os fornecedores terceirizados e clientes. Também mostramos que a Segura® recentemente alcançou essa certificação, que garante a operação seguindo os critérios de confiabilidade, traduzido nas políticas e no cotidiano, transmitindo confiança ao seu público.

Segura®: Futureproof Identity Security.

Líder em Privileged Access Management (PAM), a Segura® oferece segurança rápida, simples e poderosa. Reconhecida globalmente por Gartner, Frost & Sullivan e KuppingerCole, é a solução nº 1 no Gartner Peer Insights, ideal para equipes de TI que preferem resultados à burocracia.

Além disso, colocamos as organizações em conformidade com critérios de auditoria e com os maisexigentes padrões, como ISO 27001, PCI DSS, Sarbanes-Oxley e HIPAA.

WHITEPAPER

Entendendo a importância da Certificação SOC 2