Certificações ISO/IEC 27701 e SOC 2

Objetivo

Este estudo tem como objetivo realizar um comparativo entre duas certificações/referenciais de segurança da informação: ISO/IEC 27701 (focada em privacidade da informação) e SOC 2. O comparativo abordará requisitos para certificação, setores de atuação, benefícios e diferenças na abordagem de gestão de riscos.

1. Requisitos para Certificação

• ISO/IEC 27701:
- Extensão da ISO/IEC 27001, exige que a organização já tenha implementado o SGSI;
- Implementação de um Sistema de Gestão de Informações de Privacidade (SGIP);
- Conformidade com requisitos para operadores e controladores de dados pessoais;
- Auditoria realizada por organismo certificador acreditado.

• SOC 2:
- Auditoria conduzida por uma firma de contabilidade registrada (CPA);
- Avaliação com base nos princípios de confiança: segurança, disponibilidade, integridade de processamento, confidencialidade e privacidade;
- Relatório Tipo I (momento) ou Tipo II (período de operação).

2. Setores de Atuação

• ISO/IEC 27701:
- Adotada por empresas que tratam dados pessoais e desejam demonstrar conformidade com leis de privacidade como GDPR ou LGPD;
- Indicada para setores como saúde, tecnologia, finanças e governo.

• SOC 2:
- Comum em empresas de tecnologia, SaaS, serviços em nuvem, fintechs e consultorias de TI;
- Predominante nos Estados Unidos, mas com crescente adoção global.

3. Benefícios de Obter Cada Certificação

• ISO/IEC 27701:
- Demonstra conformidade com legislações de proteção de dados pessoais (como LGPD e GDPR);
- Integração com outros sistemas de gestão ISO;
- Melhoria na governança de dados e privacidade.

• SOC 2:
- Credibilidade de mercado com clientes corporativos;
- Evidência externa e independente da segurança dos serviços prestados;

- Diferencial competitivo em contratos e parcerias, especialmente no mercado norte-americano.

4. Diferenças na Abordagem de Gestão de Riscos

• ISO/IEC 27701:
- Enfatiza avaliação de riscos relacionados ao tratamento de dados pessoais;
- Apoiada na metodologia de riscos da ISO/IEC 27005;
- Estrutura voltada à melhoria contínua do sistema de gestão de privacidade.

• SOC 2:
- Baseado na avaliação de controles internos e sua eficácia em proteger os dados dos clientes;
- Foco na evidência de funcionamento dos controles ao longo do tempo (Tipo II);
- Permite adaptação dos critérios de confiança conforme o tipo de serviço oferecido.

Conclusão

A ISO/IEC 27701 e o SOC 2 oferecem abordagens complementares à proteção de dados e à privacidade. A ISO/IEC 27701 é mais voltada à governança de privacidade conforme legislações específicas, enquanto o SOC 2 fornece uma validação prática da segurança operacional de serviços digitais. A escolha entre elas depende do contexto regulatório e do tipo de mercado em que a organização atua.