**UNIVERSIDADE SÃO JUDAS TADEU**

**Sistemas Computacionais e Segurança**

*Isabelle de Godoy Sanchez*

*Kathleen Lohanny de Souza*

*Kauã Santana Oliveira*

*Pedro Henrique Ferreira da Rocha*

*Pedro Henrique Ribeiro Baptista*

*Richard Rosa Galindo*

**Relatório Comparativo entre ISO/IEC 27001 e SOC 2**

**Introdução**

A segurança da informação é uma preocupação crescente no mundo corporativo, especialmente com o aumento de serviços digitais, computação em nuvem e requisitos de privacidade. Diversas certificações foram desenvolvidas para garantir boas práticas de segurança e conformidade. Este relatório apresenta um estudo comparativo entre duas das certificações mais relevantes: **ISO/IEC 27001** e **SOC 2**, analisando seus requisitos, áreas de atuação, benefícios e abordagem de gestão de riscos.

1. **Requisitos para certificação**

**ISO/IEC 27001**

* Baseada em uma norma internacional criada pela ISO e IEC.
* Exige a implementação de um **Sistema de Gestão da Segurança da Informação (SGSI)**.
* Requer documentação detalhada: política de segurança, avaliação de riscos, plano de tratamento de riscos, etc.
* Auditorias são realizadas por **organismos certificadores acreditados**.
* A certificação tem validade de 3 anos, com auditorias anuais de manutenção.

**SOC 2**

* Baseada nos **Trust Services Criteria**, definidos pelo **AICPA** (Instituto Americano de Contadores).
* Avalia os controles de uma organização com foco em: segurança, disponibilidade, integridade de processamento, confidencialidade e privacidade.
* Requer auditoria por uma firma independente (normalmente um CPA).
* Não é uma certificação formal, mas sim um **relatório de auditoria** (tipo 1 ou tipo 2).
* O tipo 1 avalia em um ponto no tempo; o tipo 2 avalia os controles ao longo de um período (geralmente 6–12 meses).

1. **Setores de atuação**

**ISO/IEC 27001**

* Aplicada em diversos setores: financeiro, saúde, tecnologia, governo, educação, entre outros.
* Altamente valorizada em empresas que operam globalmente e precisam atender regulamentações internacionais (ex: GDPR).
* Comum em empresas que lidam com grande volume de dados sensíveis ou críticos.

**SOC 2**

* Muito utilizada por empresas de **tecnologia e serviços digitais**, especialmente **SaaS**, **provedores de nuvem**, **startups**, e **B2B**.
* Predominantemente exigida por empresas nos **Estados Unidos**, sendo considerada um diferencial competitivo para negócios com parceiros norte-americanos.
* Adoção crescente em empresas que terceirizam operações ou prestam serviços digitais a outras empresas.

1. **Benefícios de obter a certificação**

**ISO/IEC 27001**

* Reconhecimento internacional da segurança da informação da empresa.
* Demonstra comprometimento com **boas práticas de governança e gestão de riscos**.
* Ajuda na conformidade com leis de proteção de dados (ex: GDPR, LGPD).
* Melhoria contínua com auditorias periódicas.
* Vantagem competitiva em processos de licitação e contratação pública ou privada.

**SOC 2**

* Aumenta a confiança dos clientes e parceiros em relação aos serviços oferecidos.
* Exigência comum para empresas que desejam atuar no mercado americano.
* Demonstra eficácia e confiabilidade dos controles operacionais.
* Relatório personalizável de acordo com os critérios relevantes ao negócio (ex: segurança + disponibilidade).
* Excelente ferramenta para **transparência** com stakeholders e investidores.

1. **Diferenças na abordagem de gestão de riscos**

**ISO/IEC 27001**

* Gestão de riscos é **parte central** do processo.
* Exige identificação, análise, avaliação e tratamento dos riscos de segurança da informação.
* Requer a implementação de políticas e procedimentos baseados na gestão de riscos.
* Usa o ciclo **PDCA (Plan, Do, Check, Act)** para melhoria contínua.
* Foco proativo e estratégico.

**SOC 2**

* Avalia se a empresa tem controles eficazes, mas **não exige um processo estruturado de gestão de riscos** como a ISO 27001.
* A gestão de riscos está presente, mas de forma menos formal e mais focada nos critérios de confiança.
* Foco reativo e operacional: verifica se os controles estão funcionando durante um período.
* Menos prescritivo: cada organização define seus próprios controles, desde que cumpram os critérios exigidos.

**Conclusão**

Tanto a **ISO/IEC 27001** quanto a **SOC 2** são ferramentas poderosas para demonstrar maturidade em segurança da informação, cada uma com seu foco, escopo e aplicabilidade.

A ISO 27001 é mais abrangente, estruturada e internacionalmente reconhecida, sendo ideal para empresas que buscam padronização global e uma abordagem estratégica da segurança.

A SOC 2, por outro lado, é muito valorizada no mercado norte-americano e focada na **confiabilidade operacional**, especialmente útil para empresas de tecnologia que fornecem serviços a terceiros.

A escolha entre elas (ou mesmo a adoção das duas) dependerá dos objetivos estratégicos da organização, exigências de mercado e perfil dos clientes atendidos.