



TRABALHO DE SISTEMAS COMPUTACIONAISE SEGURANÇA

ISABELLE DE GODOY SANCHEZ
KATHLEEN LOHANNY DE SOUZA
KAUÃ SANTANA OLIVEIRA
PEDRO HENRIQUE FERREIRA DA ROCHA
PEDRO HENRIQUE RIBEIRO BAPTISTA
RICHARD ROSA GALINDO

Sumário

ATIVIDADE 1

Slide 03 à 08

CONCLUSÃO

Slide 09

ATIVIDADE 2

Slide 10 à 19

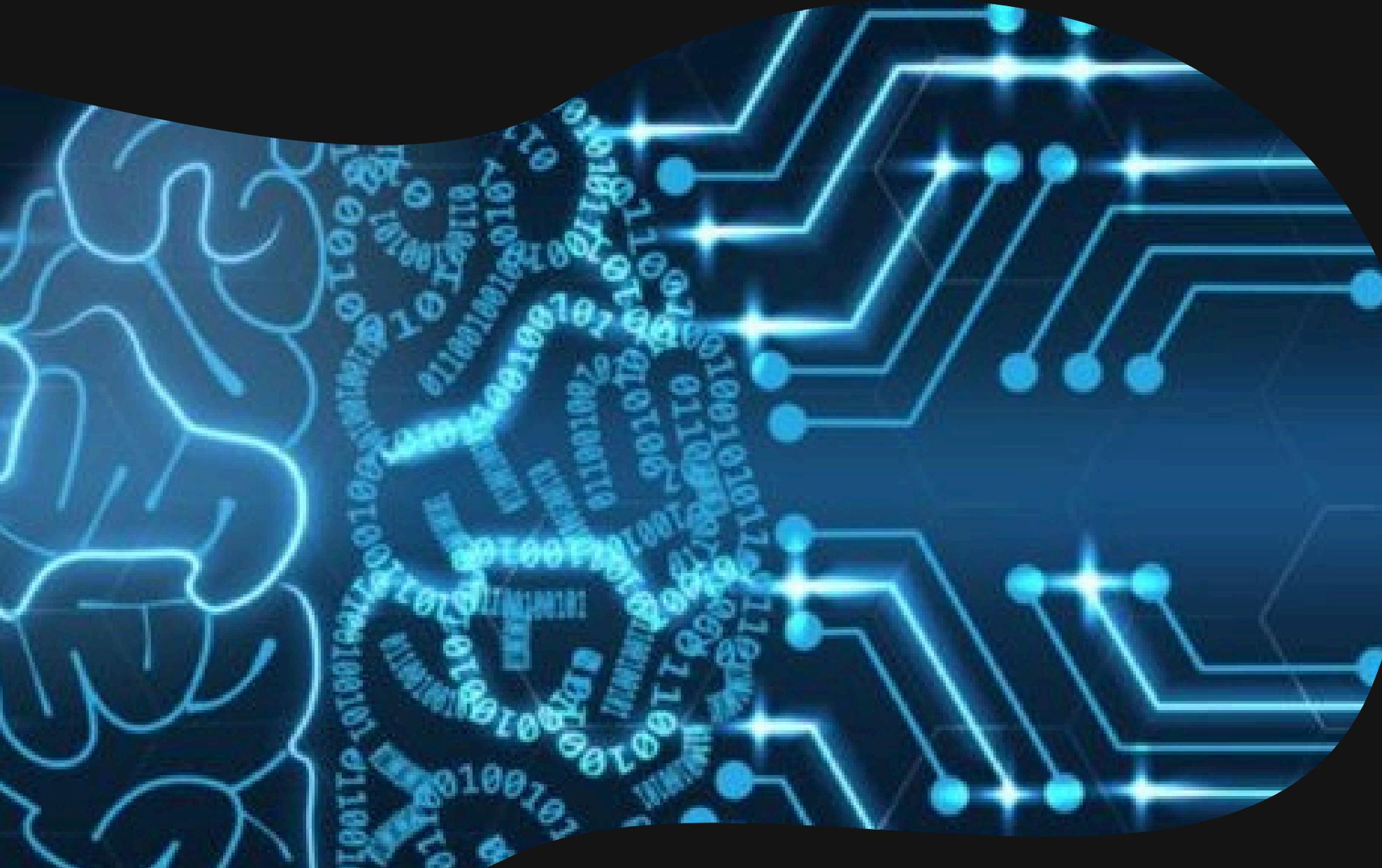
CONCLUSÃO

Slide 20

Atividade 1

Desenvolvimento de Políticas de Segurança Para uma Pequena Empresa

INTRODUÇÃO



Foram criadas políticas de segurança para a empresa fictícia TechSafe Soluções Digitais, com o objetivo de adotar boas práticas e evitar problemas de segurança.

As políticas foram elaboradas com base nos princípios de:

- Confidencialidade
- Integridade
- Disponibilidade da informação

POLÍTICA 1:

Acesso e Controle de Usuários



OBJETIVO:

Garantir acesso seguro e controlado aos sistemas corporativos.

- Criação de contas somente mediante solicitação formal e aprovação do gestor.
- Senhas devem conter letras maiúsculas, minúsculas, números e caracteres especiais.
- Contas inativas por mais de 30 dias serão bloqueadas.
- Autenticação de dois fatores obrigatória para acesso remoto.

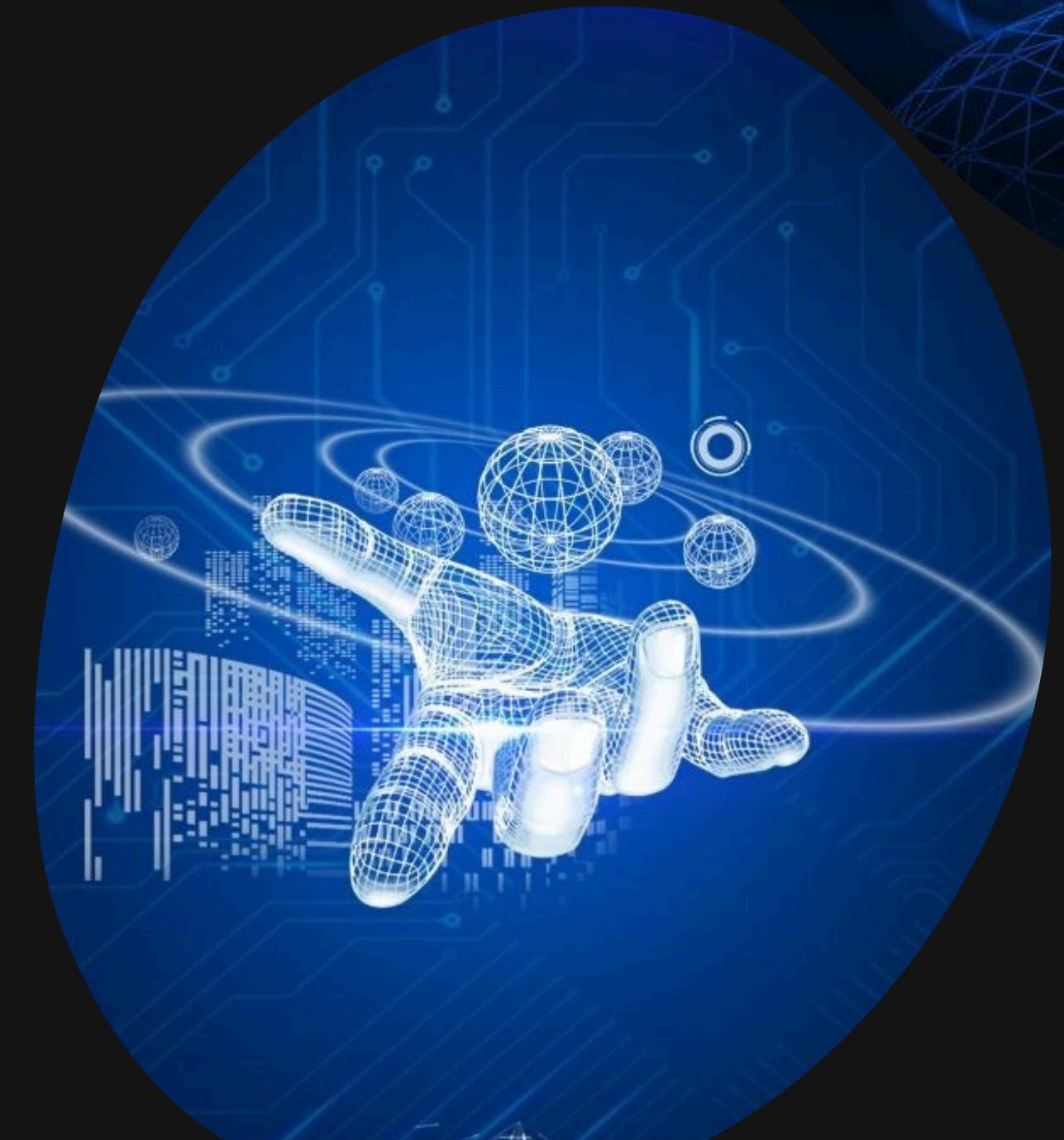
POLÍTICA 2:

Uso de Dispositivos Móveis e Redes

OBJETIVO:

Proteger os dados corporativos durante o uso de dispositivos móveis e conexões externas.

- É proibido conectar dispositivos pessoais a sistemas corporativos.
- Uso obrigatório de VPN ao acessar informações fora da empresa.
- Wi-Fi corporativo deve possuir senha forte e criptografia WPA3.
- Instalação de antivírus e bloqueio remoto em todos os dispositivos móveis.



POLÍTICA 3:

Uso de Dispositivos Móveis e Redes

OBJETIVO:

Estabelecer um processo eficaz de resposta a incidentes.

- Todos os colaboradores devem reportar incidentes imediatamente ao setor de TI.
- O time de resposta deve conter profissionais treinados para isolar sistemas comprometidos.
- Devem ser mantidos registros (logs) detalhados de cada incidente.
- Após a contenção, realizar análise de causa e plano de prevenção.



POLÍTICA 4:

Backup e Recuperação de Desastres

OBJETIVO:

Garantir a continuidade operacional da empresa.

- Backup diário automático em servidores locais e na nuvem.
- Testes mensais de restauração.
- Armazenamento de cópias em locais distintos.
- Criação de um plano de continuidade de negócios (BCP).

CONCLUSÃO

implementação dessas políticas estabelece uma base sólida de segurança, reforçando a cultura de proteção da informação e garantindo maior confiabilidade às operações da TechSafe Soluções Digitais.

Atividade 2

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.



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.

Auditórias são realizadas por organismos certificadores acreditados.

A certificação tem validade de 3 anos, com auditorias anuais de manutenção.

REQUISITOS PARA CERTIFICAÇÃO (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 (geralmente 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).

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.



SETORES DE ATUAÇÃO (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 um diferencial competitivo para negócios com parceiros norte-americanos.

Adoção crescente em empresas que terceirizam operações ou prestam serviços digitais a outras empresas.

BENEFÍCIOS DA CERTIFICAÇÃO (ISO/IEC 27001)

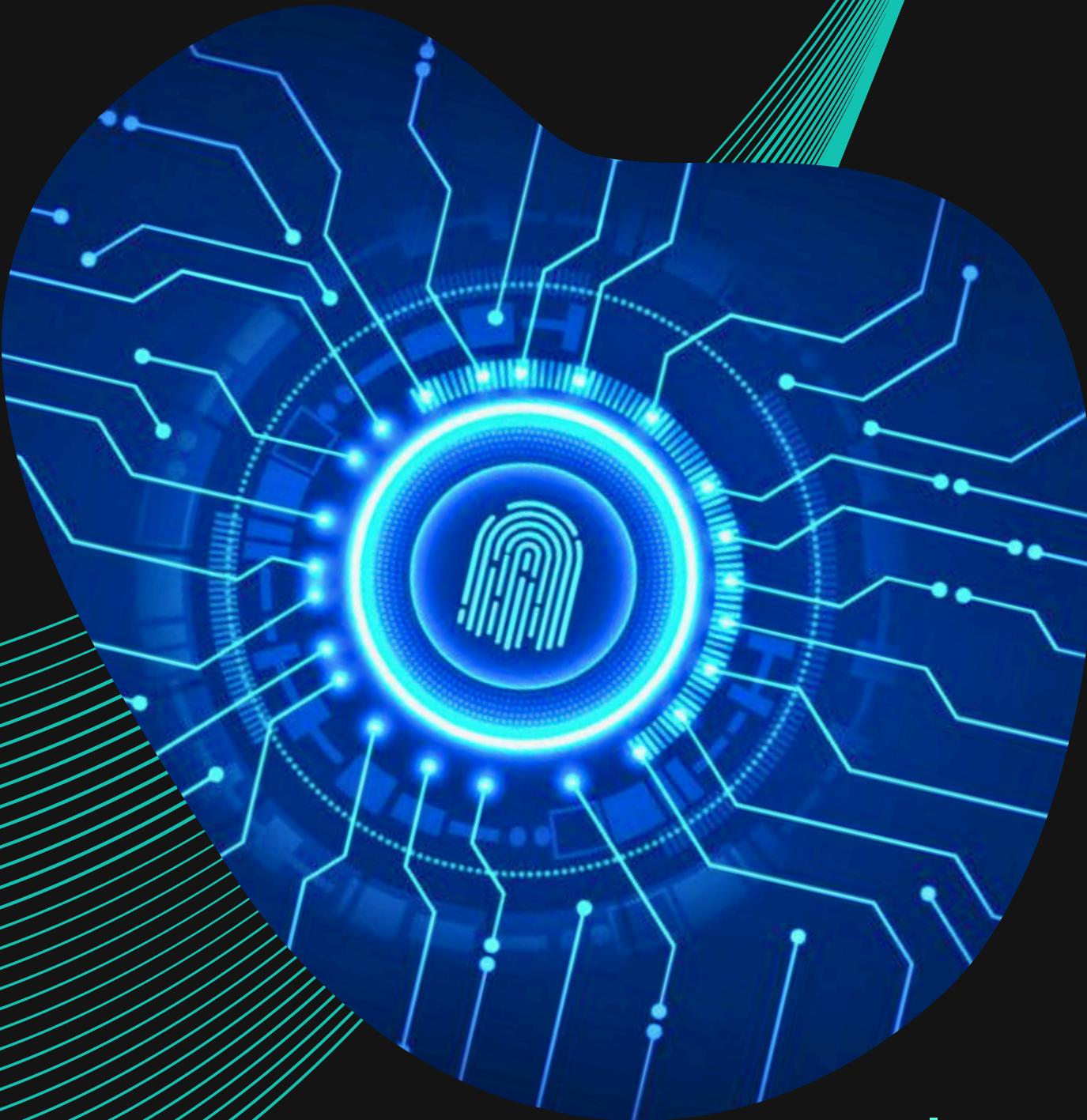
Reconhecimento internacional da segurança da informação da empresa.

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 licitações e contratações públicas ou privadas.



BENEFÍCIOS DA CERTIFICAÇÃO (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 conforme os critérios relevantes ao negócio (ex: segurança + disponibilidade).

Excelente ferramenta para transparência com stakeholders e investidores.



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 políticas e procedimentos baseados na gestão de riscos.

Utiliza o ciclo PDCA (Plan, Do, Check, Act) para melhoria contínua.

Foco proativo e estratégico.



ABORDAGEM DE GESTÃO DE RISCOS (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, porém de forma menos formal e mais focada nos critérios de confiança.

Foco reativo e operacional: verifica se os controles funcionam durante um período.

Menos prescritivo: cada organização define seus próprios controles, desde que atenda aos critérios exigidos.



CONCLUSÃO

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

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

SOC 2: valorizada no mercado norte-americano, com foco na confiabilidade operacional, especialmente útil para empresas de tecnologia que prestam serviços a terceiros.

A escolha entre elas (ou a adoção de ambas) depende dos objetivos estratégicos, exigências de mercado e perfil dos clientes atendidos.