Universidade São Judas Tadeu

Sistemas Computacionais e Segurança

ATIVIDADADE 2

RELATÓRIO COMPARATIVO NIST CSF X COBIT 5

João Vitor Chioatto Serafim – 825133189

João Victor de Souza - 825135230

Professor: Robson Calvetti

São Paulo – SP

2025

Relatório Comparativo — NIST CSF x COBIT 5

Requisitos para Certificação

NIST CSF (National Institute of Standards and Technology Cybersecurity Framework):

Não é uma certificação formal, mas um conjunto de diretrizes e boas práticas que podem ser implementadas voluntariamente.

Organizações podem buscar auditorias ou avaliações baseadas no NIST CSF para demonstrar conformidade.

Requer uma análise interna de riscos, identificação de ativos críticos e adoção dos cinco pilares do framework: Identify, Protect, Detect, Respond, Recover.

COBIT 5 (Control Objectives for Information and Related Technologies):

Desenvolvido pela ISACA, o COBIT 5 possui certificações oficiais tanto para profissionais quanto para empresas.

Para implementação organizacional, exige mapeamento de processos de TI, definição de metas de governança e controles, e integração com frameworks como ITIL e ISO 27001.

Para profissionais, há níveis de certificação como COBIT 5 Foundation, Implementation e Assessor.

Setores de Atuação

NIST CSF:

Usado amplamente por empresas críticas de infraestrutura, como energia, saúde, finanças e telecomunicações

Muito aplicado em instituições governamentais e empresas dos EUA, mas também adotado internacionalmente.

COBIT 5:

Mais comum em empresas privadas de grande porte, especialmente nos setores financeiro, bancário, tecnologia e consultoria.

Muito usado por auditores e gestores de TI que precisam alinhar TI às metas de negócio.

Benefícios de Obter Cada Certificação

NIST CSF:

Melhora a resiliência cibernética e a maturidade de segurança da informação.

Facilita avaliações de risco e priorização de investimentos em segurança.

Aumenta a conformidade com leis e regulamentos, como LGPD e GDPR.

COBIT 5:

Promove governança efetiva de TI, garantindo que a tecnologia apoie os objetivos estratégicos da empresa.

Facilita auditorias internas e certificações integradas (como ISO 27001 e ITIL).

Melhora a eficiência operacional e o controle de processos de TI.

Diferenças na Abordagem de Gestão de Riscos

NIST CSF:

Foca diretamente no gerenciamento de riscos de segurança cibernética.

Baseia-se em uma abordagem contínua e adaptável, permitindo que cada organização personalize o framework conforme seus riscos específicos.

Utiliza um ciclo de vida de segurança (identificar → proteger → detectar → responder → recuperar).

COBIT 5:

Tem uma visão mais ampla de riscos corporativos, não só de segurança, mas também de processos, conformidade e governança de TI.

Enfatiza a integração entre negócios e TI, alinhando riscos tecnológicos às metas da organização.

Foca em controles e processos para assegurar que o valor da TI seja maximizado.

Conclusão:

O NIST CSF e o COBIT 5 servem pra coisas diferentes, então o “melhor” depende do que a empresa precisa.

O NIST CSF é ótimo pra quem trabalha com segurança da informação e cibersegurança, tipo empresas de tecnologia, saúde, governo ou energia. Ele ajuda a proteger sistemas, evitar ataques e saber o que fazer se algo der errado.
É mais usado por analistas de segurança, técnicos e profissionais que cuidam da parte prática da proteção de dados.

O COBIT 5 é melhor pra empresas que querem organizar a área de TI e deixá-la alinhada com o negócio, tipo bancos, consultorias e grandes empresas. Ele serve pra melhorar a gestão, auditoria e governança de TI. Normalmente é usado por gestores, consultores e quem cuida da parte estratégica da empresa.