PROFIAP
MESTRADO PROFISSIONAL EM ADMINISTRAÇÃO PÚBLICA

UNIVERSIDADE FEDERAL DE SERGIPE

PLANEJAMENTO ESTRATÉGICO COM BSC E OKR APLICADOS À SEGURANÇA DA INFORMAÇÃO: UMA PROPOSTA DE INDICADORES ESTRATÉGICOS PARA A COSEG/IFS

PLANEJAMENTO ESTRATÉGICO COM BSC E OKR APLICADOS À SEGURANÇA DA INFORMAÇÃO: UMA PROPOSTA DE INDICADORES ESTRATÉGICOS PARA A COSEG/IFS

Relatório técnico apresentado pelo mestrando **João Silvio Ribeiro dos Santos** ao Mestrado Profissional em Administração Pública em Rede, sob orientação do docente **Prof. Dr. Cláudio Márcio Campos de Mendonça**, como parte dos requisitos para obtenção do título de Mestre em Administração Pública.

FICHA CATALOGRÁFICA ELABORADA PELA BIBLIOTECA CENTRAL
UNIVERSIDADE FEDERAL DE SERGIPE

S237p	Santos, João Silvio Ribeiro dos Planejamento estratégico com BSC e OKR aplicados à segurança da informação : uma proposta de indicadores estratégicos para a COSEG/IFS / João Silvio Ribeiro dos Santos ; orientador Claudio Márcio Campos de Mendonça. – São Cristóvão, SE, 2025. 24 p. : il. Relatório técnico conclusivo (mestrado profissional em Administração Pública em Rede Nacional) – Universidade Federal de Sergipe, 2025.
	1. Administração pública. 2. Planejamento estratégico – Metodologia. 3. Governança pública. 4. Sistemas de informação gerencial – Medidas de segurança. I. Instituto Federal de Educação, Ciência e Tecnologia de Sergipe. II. Mendonça, Claudio Márcio Campos de, orient. III. Título.
	CDU 35.08:005.21(813.7)

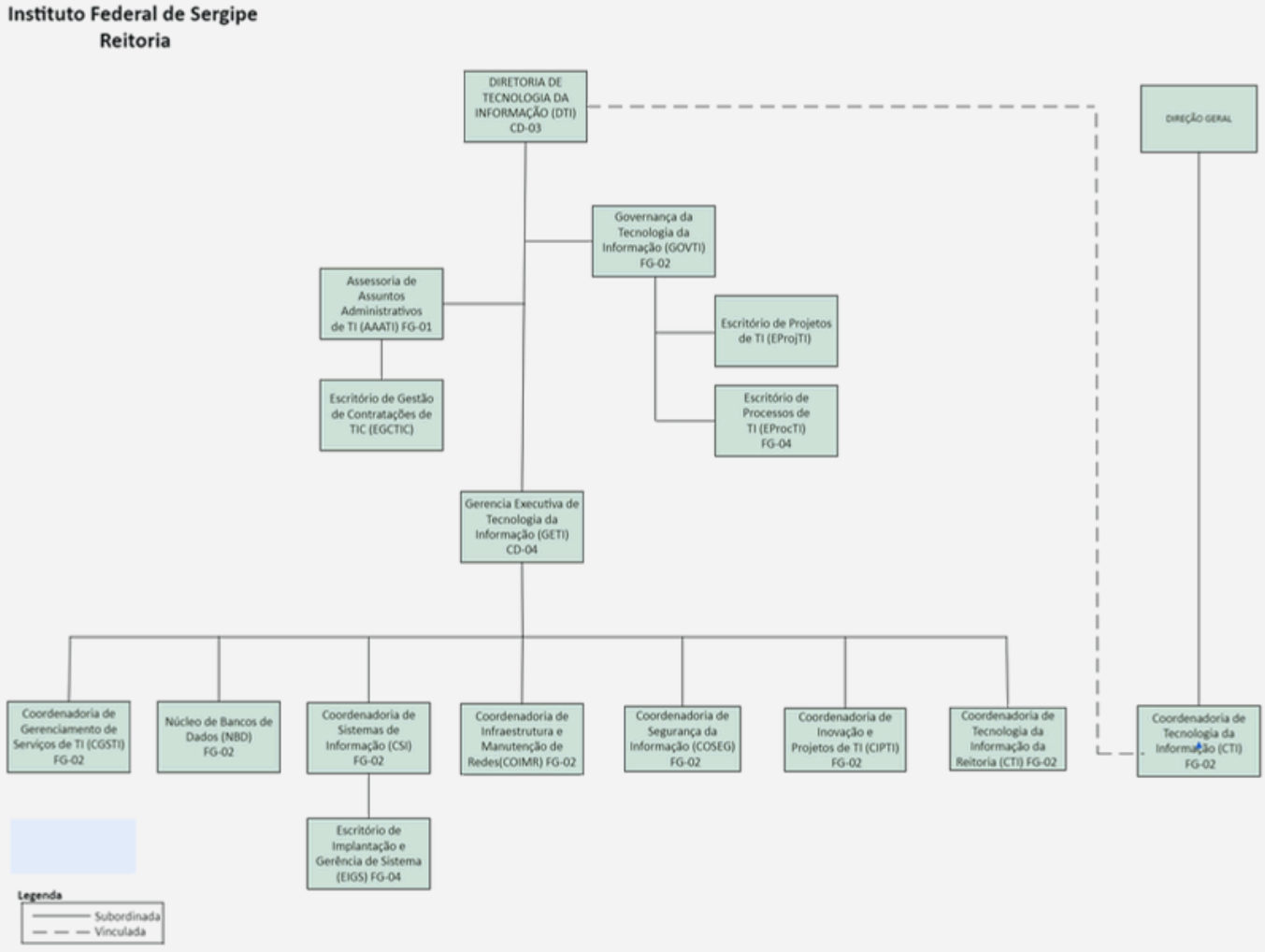
SUMÁRIO

RESUMO

Este trabalho tem como objetivo apresentar uma proposta de elaboração do planejamento estratégico no setor público, com base em uma abordagem integrada dos modelos Balanced Scorecard (BSC) e Objectives and Key Results (OKR). O estudo foi desenvolvido na Coordenadoria de Segurança da Informação (COSEG) do Instituto Federal de Sergipe (IFS), sendo estruturado como um Produto Técnico Tecnológico (PTT), requisito final da disciplina Planejamento e Administração Estratégica, vinculada ao Programa de Pós-graduação em Administração Pública (PROFIAP), em parceria com a Universidade Federal de Sergipe (UFS).

A análise evidenciou que, embora os servidores da COSEG possuam domínio técnico sobre segurança da informação, o setor enfrenta limitações significativas decorrentes da ausência de uma metodologia estruturada para orientar suas ações estratégicas. Diante desse cenário, propõe-se a aplicação de um modelo de planejamento estratégico que integra os frameworks BSC e OKR, visando melhorar os processos, alinhar objetivos institucionais e aprimorar os resultados da coordenação.

A possível replicação desta proposta de planejamento em outras unidades administrativas do IFS demandará adequações de natureza legal, estrutural e operacional, considerando as especificidades e realidades de cada ambiente institucional. A seguir, apresenta-se o organograma da Diretoria de tecnologia da Informação (DTI), que está diretamente vinculada à Reitoria.



APRESENTAÇÃO DA ORGANIZAÇÃO

O Instituto Federal de Sergipe (IFS) é uma instituição pública de ensino vinculada à Rede Federal de Educação Profissional, Científica e Tecnológica, cuja missão é promover educação de qualidade, articulando ensino, pesquisa e extensão em diversos níveis e modalidades. Com atuação multicampi no estado de Sergipe, o IFS é reconhecido pela sua contribuição ao desenvolvimento social e econômico da região, oferecendo formação técnica, tecnológica e superior alinhada às demandas contemporâneas da sociedade brasileira.

A estrutura administrativa do IFS é organizada para garantir a governança institucional e a excelência operacional dos seus serviços educacionais. Seus campi, departamentos, coordenadorias e setores técnicos trabalham de forma integrada, sob orientação das políticas públicas educacionais e diretrizes estratégicas definidas em seu Plano de Desenvolvimento Institucional (PDI).

Atualmente, o IFS tem expandido sua atuação no estado de Sergipe, promovendo educação profissional, científica e tecnológica de qualidade. Presente em vários municípios sergipanos, como Aracaju, São Cristóvão, Lagarto, Estância, Itabaiana, Socorro, Glória, Poço Redondo, Tobias Barreto e Propriá. Com um compromisso firme com a inclusão, inovação e excelência acadêmica, o Instituto Federal de Sergipe se consolidou como referência na educação pública de qualidade, contribuindo para a formação de profissionais qualificados e para a promoção da pesquisa e da extensão em diversas áreas do conhecimento. Em seu quadro de pessoal conta aproximadamente 1175 servidores, sendo 663 TAEs e 512 professores. dados do Plano Desenvolvimento Institucional (PDI) 2024.

A Coordenadoria de Segurança da Informação (COSEG) é o setor responsável pela gestão dos ativos informacionais do Instituto, atuando de forma preventiva e corretiva na mitigação de riscos digitais e na garantia da proteção dos dados institucionais. Vinculada diretamente à Gerência Executiva de Tecnologia da Informação (GETI), a COSEG desempenha papel fundamental na consolidação das práticas de governança digital, integrando esforços entre os setores acadêmicos, técnicos e administrativos para assegurar a integridade, confidencialidade e disponibilidade das informações. Sua atuação está alinhada às diretrizes estratégicas do IFS, sendo composta por profissionais especializados em segurança cibernética e infraestrutura tecnológica.

Imagem das futuras instalações do IFS Campus Aracaju.

PÚBLICO-ALVO DA PROPOSTA

Vinculada à Diretoria de Tecnologia da Informação (DTI) , a COSEG desempenha papel estratégico na preservação da integridade, confidencialidade e disponibilidade dos ativos informacionais da instituição. Sua atuação é guiada pela Política de Segurança da Informação e Comunicação (POSIC), instituída em 2011, que estabelece um conjunto de diretrizes para padronizar os procedimentos técnicos, administrativos e operacionais voltados à proteção de dados e ao controle de riscos digitais.

Em novembro de 2020, a relevância da COSEG foi amplamente reconhecida em âmbito nacional quando, em conjunto com a Coordenadoria de Infraestrutura e Manutenção de Redes (COIMR), o setor implementou 15 das 17 estratégias indicadas pela Secretaria de Governo Digital (SGD) do Governo Federal. Essa ação posicionou o IFS entre os órgãos públicos mais eficientes em segurança da informação, alcançando a terceira colocação entre os integrantes do Sistema de Administração de Tecnologia da Informação (SISP) e o primeiro lugar entre os Institutos e Universidades Federais vinculados ao Ministério da Educação (MEC). Esse desempenho destaca o comprometimento institucional na mitigação de vulnerabilidades, com ênfase na prevenção de ataques como o ransomware, que visam à criptografia e sequestro de dados mediante extorsão (IFS, 2020).

A atuação da COSEG no âmbito educacional representa um modelo de governança digital e boas práticas em segurança cibernética, contribuindo para a estabilidade das operações acadêmicas, administrativas e científicas. Ao garantir um ambiente virtual seguro e resiliente, a Coordenadoria fortalece a confiança na infraestrutura tecnológica do IFS e reafirma o papel da instituição como referência em inovação, eficiência pública e responsabilidade informacional.

DESCRIÇÃO DA SITUAÇÃO PROBLEMA

A atuação da COSEG no âmbito educacional representa um modelo de governança digital e boas práticas em segurança cibernética, contribuindo para a estabilidade das operações acadêmicas, administrativas e científicas. Ela desempenha um papel essencial na proteção dos ativos informacionais da instituição, alinhado aos principais pilares da segurança da informação: integridade, confidencialidade e disponibilidade. No entanto, apesar do relevante conhecimento técnico dos servidores alocados no setor, observa-se a ausência de um modelo estruturado de planejamento estratégico que possibilite o alinhamento das ações da coordenação aos objetivos institucionais mais amplos.

Essa lacuna metodológica compromete a definição de prioridades, a mensuração de resultados e o acompanhamento do desempenho da COSEG, além de dificultar a integração com outras áreas administrativa e acadêmica do IFS. A inexistência de diretrizes claras e sistematizadas torna os processos internos mais reativos do que proativos, o que é especialmente crítico em um setor que demanda respostas rápidas e alinhamento contínuo com padrões de segurança da informação e governança pública.

Diante desse cenário, torna-se necessário propor uma solução que ofereça estrutura, foco estratégico e instrumentos de monitoramento e avaliação. A escolha por uma abordagem integrada baseada no Balanced Scorecard (BSC) e nos Objectives and Key Results (OKR) visa preencher essa lacuna, promovendo uma gestão mais eficaz, com metas definidas, indicadores claros e alinhamento organizacional.

OBJETIVOS DA PROPOSTA

O objetivo geral deste PTT é Elaborar uma proposta de planejamento estratégico para a Coordenadoria de Segurança da Informação (COSEG) do Instituto Federal de Sergipe (IFS), utilizando uma abordagem integrada dos modelos Balanced Scorecard (BSC) e Objectives and Key Results (OKR), com foco no alinhamento institucional, na melhoria da gestão e no fortalecimento da segurança da informação.

Nos objetivos específicos, propõem-se:

1. Diagnosticar o cenário atual da COSEG quanto à gestão estratégica e à condução das ações de segurança da informação;
2. Utilizar a análise PESTEL e a matriz SWOT para identificar os fatores internos e externos — incluindo forças, fraquezas, oportunidades e ameaças — relacionados à ausência de um modelo estruturado de planejamento estratégico;
3. Construir uma matriz de priorizações unificada com a matriz Eisenhower;
4. Aplicar os princípios do BSC para definir objetivos estratégicos e indicadores de desempenho alinhados à missão institucional do IFS;
5. Integrar o framework OKR ao planejamento proposto, promovendo clareza de metas, acompanhamento de resultados e engajamento da equipe;
6. Contribuir para o fortalecimento da governança institucional por meio de práticas de planejamento, avaliação e melhoria contínua.

DIAGNÓSTICO E ANÁLISE

1. ANÁLISE AMBIENTAL - SETOR COSEG

A Coordenadoria de Segurança da Informação (COSEG) do Instituto Federal de Sergipe (IFS) é responsável por garantir a proteção dos ativos digitais institucionais, promovendo políticas, normas e ações voltadas à segurança da informação. Apesar da relevância estratégica do setor, o diagnóstico realizado revelou a inexistência de um planejamento estruturado que norteie suas ações, metas e indicadores. Essa ausência tem gerado lacunas na priorização das atividades, no monitoramento dos resultados e na articulação com os objetivos institucionais do IFS.

Observou-se que, embora os servidores da COSEG possuam conhecimento técnico adequado e atuem com comprometimento, as atividades do setor são, em grande parte, reativas, limitadas a demandas pontuais ou a ocorrências de incidentes. A falta de metodologias sistematizadas compromete o uso eficiente de recursos, a gestão de riscos e a definição de estratégias de médio e longo prazo. Também foi identificada uma carência de instrumentos formais que possibilitem o alinhamento do setor com o Plano de Desenvolvimento Institucional (PDI) e demais diretrizes de governança.

Diante desse cenário, é necessário realizar uma análise qualitativa baseada em entrevistas com os servidores da coordenação e revisão de documentos institucionais. Essa análise justificará a necessidade de adoção um modelo de gestão estratégica que possibilite a definição de objetivos claros, indicadores de desempenho e metas mensuráveis. A escolha por integrar os frameworks Balanced Scorecard (BSC) e Objectives and Key Results (OKR) fundamenta-se na complementaridade entre essas abordagens: enquanto o BSC fornece uma visão ampla e estruturada dos objetivos institucionais, o OKR favorece a definição de metas ágeis e orientadas por resultados.

Essa abordagem integrada busca promover maior coerência estratégica, engajamento da equipe, clareza de papéis e foco em resultados, criando as bases para uma gestão mais eficiente e alinhada aos princípios da administração pública. Como poderá ser visto nos próximos tópicos.

2. ANÁLISE AMBIENTAL – ANÁLISE PESTEL

A análise PESTEL é uma ferramenta de gestão baseada nos fatores que afetam o ambiente externo de uma operação. O acrônimo representa os seis principais fatores macroambientais que impactam os negócios: Políticos, Econômicos, Sociais, Tecnológicos, Ecológicos e Legais.

Segundo Johnson, Scholes e Whittington (2011), essa abordagem amplia a visão dos gestores ao considerar elementos externos que podem representar oportunidades ou ameaças, sendo fundamental para antecipar mudanças e adaptar estratégias de forma proativa. A análise sistemática desses fatores contribui para decisões mais alinhadas com o contexto em que a organização está inserida.

Além disso, os autores destacam que o modelo PESTEL é particularmente útil na identificação de indutores-chave de mudança, como alterações regulatórias, avanços tecnológicos ou transformações sociais, que podem redefinir o posicionamento competitivo das empresas. Ao integrar essa análise ao processo estratégico, os gestores conseguem desenvolver cenários mais realistas e robustos, favorecendo a construção de estratégias sustentáveis e resilientes.

Quadro 1 - Análise PESTEL

PESTEL
Análise dos fatores

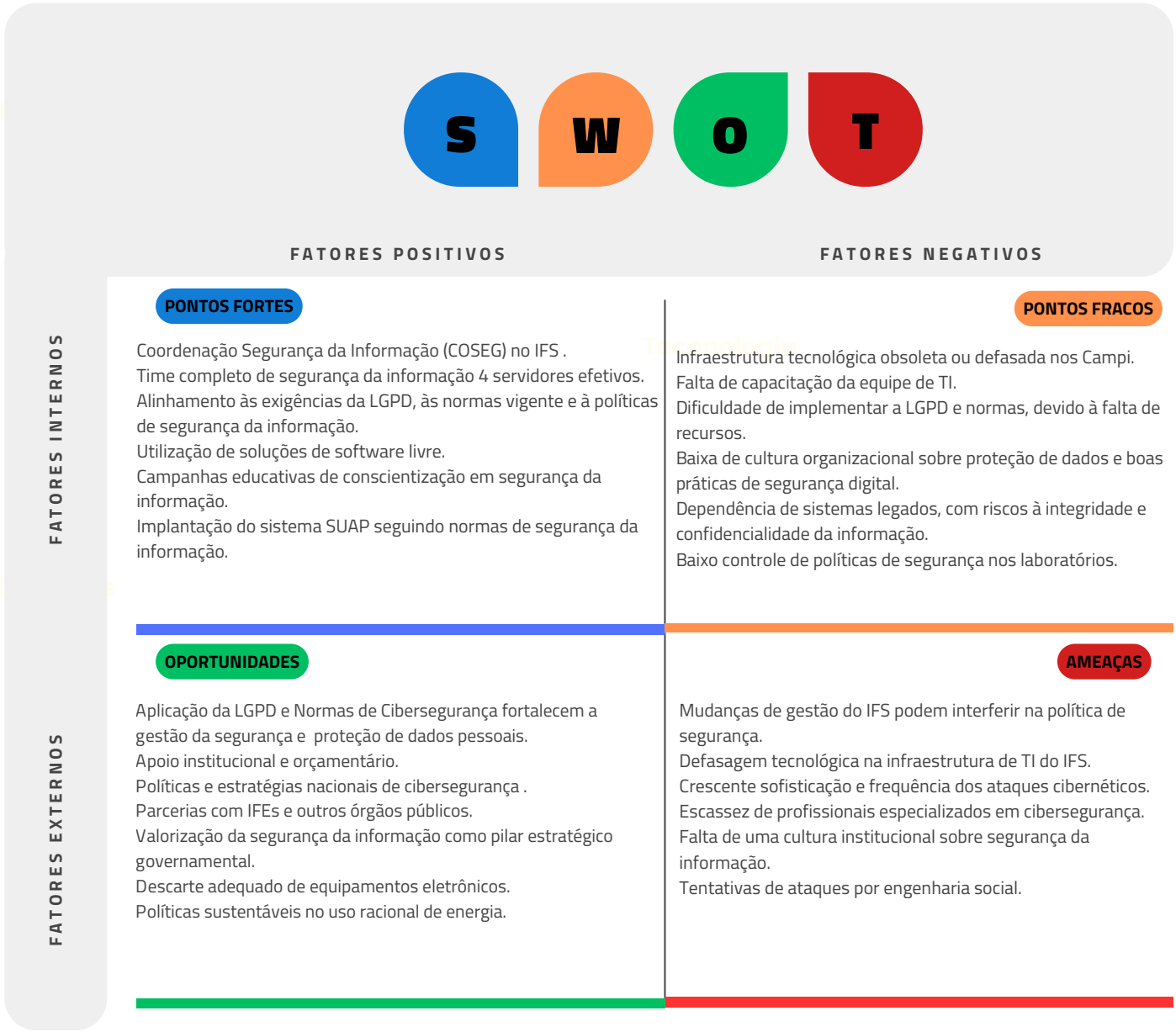
POLÍTICOS	ECONÔMICOS	SOCIAIS	TECNOLÓGICOS	ECOLÓGICOS	LEGAIS
# Legislação, regulamentação e normas do governo. # Políticas e estratégias nacionais de cibersegurança. # Apoio institucional e orçamentário. # Mudanças de gestão do IFS. # Parcerias com IFEs e outros órgãos públicos.	# Alto custo com investimentos em infraestrutura de segurança de TI. # Contratação de profissionais especializados em cibersegurança. # Custos com capacitação da equipe de TI. # Soluções de softwares livres.	# A cultura organizacional na Instituição # Conscientização sobre segurança da informação	# Novas tecnologias. # Evolução constante das ameaças cibernéticas. # A transformação digital na educação. # Crescente sofisticação e frequência dos ataques cibernéticos. # Defasagem tecnológica da infraestrutura de TI	# Políticas sustentáveis no uso racional de energia. # Descarte adequado de equipamentos eletrônicos. # O uso de tecnologias em nuvem reduzindo infraestrutura física de TI.	# Decreto nº 9.637/2018, a Política Nacional de Segurança da Informação (PNSI). # Lei nº 13.709/2018, Lei Geral de Proteção de Dados . # Lei nº 12.965/2014, Marco Civil da Internet. # Lei nº 12.527/2011, Lei de Acesso à Informação (LAI).
					

Fonte: Modelo Canva elaborado pelo autor (2025)

3. DIAGNÓSTICO ESTRATÉGICO - ANÁLISE SWOT

A análise SWOT constitui uma ferramenta estratégica relevante para a identificação de competências e habilidades internas, revelando os principais pontos fortes e fracos do indivíduo ou setor avaliado. Complementarmente, por meio da análise PESTEL, foram extraídas informações do ambiente externo, como oportunidades e ameaças, que contribuem significativamente para o planejamento dos objetivos estratégicos da COSEG. Assim, considera-se a estrutura clássica da matriz SWOT — Strengths (forças), Weaknesses (fraquezas), Opportunities (oportunidades) e Threats (ameaças) — como fundamento para integrar os aspectos internos e externos ao processo decisório.

Quadro 2- Análise SWOT



Fonte: Modelo Canva adaptado pelo autor (2025)

4. DIAGNÓSTICO ESTRATÉGICO - MATRIZ DE EISENHOWER

A Matriz de Eisenhower surgiu a partir das práticas do ex-presidente norte-americano Dwight D. Eisenhower, reconhecido por sua capacidade de tomar decisões com base na priorização eficiente de tarefas. Essa matriz organiza as atividades em quatro quadrantes conforme dois critérios principais — urgência e importância — e orienta as ações em direções estratégicas: realizar de imediato, planejar, delegar ou eliminar. A proposta oferece uma estrutura clara para a gestão do tempo, permitindo distinguir o que realmente merece atenção do que pode ser adiado ou descartado.

Covey (2015), popularizou esse modelo, adaptando-o à sua abordagem sobre eficácia pessoal. A chamada Matriz de Covey reforça que concentrar-se em atividades importantes, mesmo que não urgentes, é essencial para alcançar resultados duradouros. No contexto do planejamento estratégico da COSEG, esse modelo torna-se ainda mais relevante ao favorecer a integração com métodos analíticos como SWOT e PESTEL, ampliando a capacidade decisória e alinhando ações aos objetivos institucionais de forma mais consciente e assertiva.

Quadro 3- Matriz Eisenhower unificada

MATRIZ DE EISENHOWER UNIFICADA

	URGENTE	NÃO URGENTE
MAIS IMPORTANTE	***Oportunidades*** *Aplicação da LGPD e normas de cibersegurança.* ***Ameaças*** *Apoio institucional e orçamentário.* *Crescente sofisticação de ataques cibernéticos.* *Defasagem tecnológica na infraestrutura de TI do IFS.* ***Pontos Fortes*** *Fortalecer a COSEG como estrutura especializada no IFS.* ***Pontos Fracos*** *Melhorar infraestrutura tecnológica nos Campi.* *Solicitar capacitação para equipe de TI.*	***Oportunidades*** *Parcerias com IFEs e outros órgãos públicos.* *Políticas e estratégias nacionais de cibersegurança (CISC GOV.BR).* *Valorização da segurança da informação como pilar estratégico governamental.* ***Pontos Fortes*** *Utilizar de soluções de software livre.* *Criar Campanhas educativas de conscientização em segurança da informação.* *Implantar do sistema SUAP seguindo normas de segurança da informação.*
MENOS IMPORTANTE	***Ameaças*** *Mudanças de gestão do IFS podem interferir na política de segurança.* *Escassez de profissionais especializados em cibersegurança.* ***Pontos Fracos*** *Melhorar controle de políticas de segurança nos laboratórios.*	***Ameaças*** *Falta de uma cultura institucional sobre segurança da informação.* ***Pontos Fracos*** *Melhorar cultura organizacional sobre proteção de dados e boas práticas de segurança digital.* Dependência de sistemas legados.

Fonte: Modelo Canva adaptado pelo autor (2025)

4.1. DIAGNÓSTICO ESTRATÉGICO - MATRIZ DE EISENHOWER (PRIORIZAÇÕES)

Após montar a Matriz de Eisenhower unificada foram identificadas as priorizações que estão vinculadas às oportunidades, ameaças, pontos fortes e pontos fracos, conforme quadro 4 abaixo:

Quadro 4- Priorização Oportunidades, Ameaças, Pontos Force e Pontos fracos

Oportunidades	
1	Aplicação da LGPD e normas de cibersegurança
2	Apoio institucional e orçamentário
3	Parcerias com IFEs e outros órgãos públicos
4	Valorização da segurança da informação como pilar estratégico governamental.
Ameaças	
1	Mudanças de gestão do IFS podem interferir na política de segurança.
2	Defasagem tecnológica na infraestrutura de TI do IFS.
3	Crescente sofisticação dos ataques cibernéticos
4	Escassez de profissionais especializados em cibersegurança.
Pontos Fortes	
1	Fortalecer a COSEG como estrutura especializada no IFS.
2	Utilizar de soluções de software livre.
3	Solicitar capacitação para equipe de TI.
4	Criar Campanhas educativas de conscientização em segurança da informação.
Pontos Fracos	
1	Melhorar infraestrutura tecnológica nos Campi.
2	Melhorar cultura organizacional sobre proteção de dados e boas práticas de segurança digital.
3	Melhorar controle de políticas de segurança nos laboratórios.
4	Dependência de sistemas legados.

Fonte: Modelo Canva adaptado pelo autor (2025)

5. DIAGNÓSTICO ESTRATÉGICO - MATRIZ SWOT QUANTITATIVA

Do quadro 4, foram selecionadas 4 oportunidades e ameaças mais relevantes, e os 4 principais pontos fortes e pontos fracos, ambos mais importantes.
Para cada relação entre os fatores, foram feitas correlações entre o par de fatores externos x internos com a seguinte metodologia:

0: para os casos em que não existe correlação
1: para os casos em que existe correlação fraca
3: para os casos em que existe correlação média
6: para os casos em que existe correlação forte

O somatório de cada quadrante, identifica os principais pontos críticos da Matriz. Esse passo será importante para as definições das diretrizes estratégicas (missão, visão e valores) além dos objetivos estratégicos.

Quadro 5- Matriz SWOT Quantitativa

		Oportunidades				Ameaças				Total
Fatores externos → / Fatores internos ↓		Aplicação da LGPD	Apoio institucional e orçamentário	Parcerias com IFs e órgão públicos	Valorização da S.I governamental	Mudanças de gestão do IFS	Sofisticação dos ataques	Defasagem tecnológica do IFS.	Escassez de Pessoal	
Pontos Fortes	COSEG como estrutura especializada	6	6	1	3	6	6	3	6	37
	Utilizar de soluções de software livre	0	6	3	6	1	1	3	3	23
	Solicitar capacitação para equipe de TI	3	6	0	3	3	1	1	3	20
	Campanhas educativas de conscientização de SI.	6	1	1	3	3	6	0	1	21
	Totais	15	19	5	15	13	14	7	13	101
Pontos Fracos	Infraestrutura tecnológica obsoleta	3	6	1	3	6	3	6	3	31
	Baixo engajamento da comunidade	1	0	0	1	3	3	0	0	8
	Melhorar controle de políticas de segurança nos	3	6	0	3	3	6	6	3	30
	Dependência de sistemas legados	1	1	0	0	6	3	1	3	15
	Totais	8	13	1	7	18	15	13	9	84

Fonte: Modelo Canva adaptado pelo autor (2025)

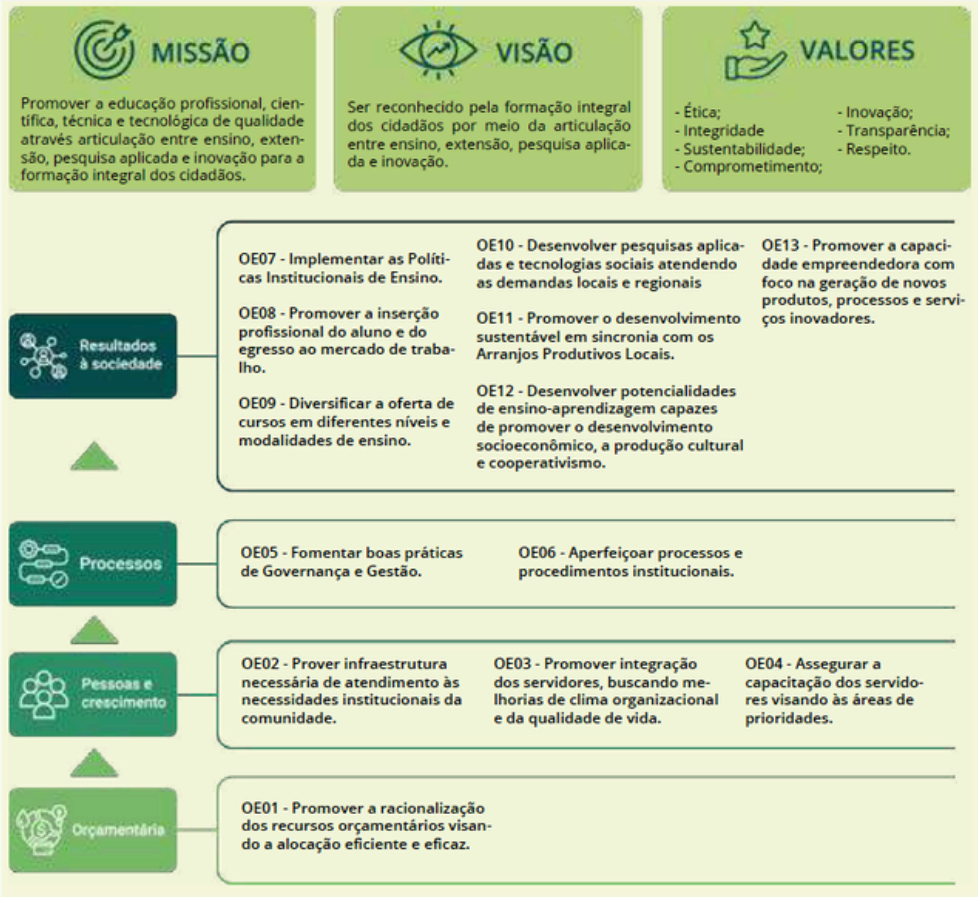
6. DIRETRIZES ESTRATÉGICAS - NEGÓCIOS E MISSÃO DA ORGANIZAÇÃO

A Coordenadoria de Segurança da Informação (COSEG) tem como missão institucional assegurar a confidencialidade, integridade e disponibilidade das informações, pilares fundamentais da segurança da informação. O negócio da COSEG está centrado na proteção dos ativos informacionais, tanto no ambiente digital quanto físico, garantindo que os dados institucionais estejam resguardados contra ameaças internas e externas.

Para cumprir esse propósito, a COSEG oferece políticas eficazes de segurança da informação, serviços de prevenção e resposta a incidentes, além de ações contínuas de conscientização e orientação aos usuários.Essas iniciativas estão alinhadas à norma ABNT NBR ISO/IEC 27002:2022, que estabelece diretrizes para práticas organizacionais em segurança da informação.

O desafio central da COSEG consiste em fomentar uma cultura organizacional voltada à segurança da informação, promovendo o engajamento dos usuários e acompanhando a evolução das ameaças e das tecnologias. Conforme destacado por Dos Anjos Oliveira (2024), a competência essencial da coordenadoria reside na aplicação de políticas, gestão de riscos, respostas a incidentes e ações educativas que asseguram a proteção dos dados, a continuidade dos serviços e o cumprimento das exigências legais.

Por fim, essas práticas são reforçadas no contexto institucional do Instituto Federal de Sergipe (IFS), onde a COSEG desempenha papel estratégico na governança da segurança da informação, conforme orientações da ABNT (2022) e dos princípios de gestão moderna.



Fonte: Mapa estratégico IFS, (PDI, 2024)

7. DIRETRIZES ESTRATÉGICAS (MISSÃO, VISÃO E VALORES)

A definição de diretrizes estratégicas — missão, visão e valores — constitui a base para o alinhamento institucional e a sustentabilidade de longo prazo das organizações. Segundo Drucker (2007), a missão representa a razão de ser da organização, seu propósito fundamental no ambiente social e econômico em que atua. Complementarmente, Chiavenato (2014) reforça que a missão deve refletir o papel central da organização na sociedade, enquanto a visão projeta o futuro desejado e os valores estabelecem os princípios éticos e comportamentais que orientam decisões e condutas. Maximiano (2017) destaca que esses três elementos formam o núcleo da cultura organizacional, influenciando diretamente a identidade e a forma como a instituição se relaciona com seus públicos

Quadro 6- diretrizes Estratégicas (Missão, visão e Valores)

DIRETRIZES ESTRATÉGICAS		
MISSÃO	**VISÃO**	**VALORES**
Contribuir para a segurança da informação institucional, por meio de políticas, processos e ações educativas eficazes, atendendo aos servidores, alunos e setores do Instituto Federal de Sergipe, com o desafio de promover uma cultura organizacional de proteção de dados e enfrentamento às ameaças digitais crescentes.	Ser referência entre os Institutos Federais em segurança da informação no âmbito da educação pública.	Ética; Responsabilidade; Transparência; Colaboração; Inovação; Cultura de Aprendizado; Agilidade; Foco no Usuário; Proatividade; Segurança Digital.
LEMA		
"Segurança com propósito: proteger, educar e transformar."		

Fonte: Modelo Canva adaptado pelo autor (2025)

8. MAPA ESTRATÉGICO - BALANCED SCORECARD (BSC)

O mapa estratégico, elemento central do modelo Balanced Scorecard (BSC), é uma representação gráfica que traduz a missão, visão e objetivos estratégicos de uma organização em indicadores tangíveis distribuídos em quatro perspectivas: financeira, clientes, processos internos e aprendizado e crescimento. Kaplan e Norton (2004) destacam que o mapa estratégico permite visualizar as relações de causa e efeito entre os objetivos, promovendo alinhamento e coerência na execução da estratégia.

Quadro 7- Balanced Scorecard (BSC)

B S C

CIDADÃO SOCIEDADE	PROCESSOS INTERNOS
1. Contribuir para a proteção dos dados pessoais da comunidade acadêmica 2. Promover a confiança institucional por meio da transparência e segurança digital	3. Padronizar processos de segurança da informação 4. Monitorar e responder a incidentes com agilidade 5. Ampliar a integração da COSEG com os demais setores institucionais
APRENDIZADO E CRESCIMENTO	**ORÇAMENTÁRIO FINANCEIRO**
6. Capacitar continuamente os servidores da COSEG e das áreas correlatas 7. Promover campanhas educativas sobre segurança da informação 8. Fomentar a cultura institucional de segurança da informação 9. Fortalecer o uso de tecnologias seguras e inovadoras	10. Maximizar o uso de soluções de software livre 11. Priorizar recursos orçamentários para segurança da informação conforme diretrizes do PDTIC.

Fonte: Modelo Canva adaptado pelo autor (2025)

Através do Mapa Estatégico - ME, foram elaborados 11 objetivos estratégicos, sendo (2) Cidadão / Sociedade, (3) Processos Internos, (4) Aprendizado e Crescimento e (2) Orçamentário e Financeiro. Com metas anuais para o período de 4 anos.

Quadro 7.1- Mapa Estratégico, indicadores e metas

MAPA ESTRATÉGICO					
CIDADÃO SOCIEDADE					
Objetivo Estratégico	**Indicador**	**META**			
		2025	**2026**	**2027**	**2028**
1. Contribuir para a proteção dos dados pessoais da comunidade acadêmica	• Percentual de cumprimento da LGPD dos sistemas e processos	75%	80%	90%	95%
2. Promover a confiança institucional por meio da transparência e segurança digital	• Notas indicadores de satisfação do Sistema de Chamados GLPI.	8,6	8,9	9,2	9,5
PROCESSOS INTERNOS					
Objetivo Estratégico	**Indicador**	**META**			
		2025	**2026**	**2027**	**2028**
3. Padronizar processos de segurança da informação	• Quantidade de normativos revisados.	2	3	4	5
4. Monitorar e responder a incidentes com agilidade	• Percentual dos sistemas monitorados.	45%	60%	80%	100%
5. Ampliar a integração da COSEG com os demais setores institucionais	• Quantidade de reuniões estratégicas entre setores com a COSEG.	1	2	3	4

MAPA ESTRATÉGICO					
APRENDIZADO E CRESCIMENTO					
Objetivos Estratégicos	**Indicador**	**META**			
		2025	**2026**	**2027**	**2028**
6. Capacitar continuamente os servidores da COSEG e das áreas correlatas	• Aumento do número de capacitações internas por servidor. horas/ano .	8h	16h	16h	20h
7. Promover campanhas educativas sobre segurança da informação	• Quantidade de campanhas educativas por ano.	2	2	3	3
8. Fomentar a cultura institucional de segurança da informação	• Aumento do índice de maturidade institucional em Segurança da informação (escala de 1 a 5)	2	3	4	4
9. Fortalecer o uso de tecnologias seguras e inovadoras	• Quantidade de adoção de novas tecnologias seguras.	0	1	2	3
ORÇAMENTÁRIO/FINANCEIRO					
Objetivos Estratégicos	**Indicador**	**META**			
		2025	**2026**	**2027**	**2028**
10. Maximizar o uso de soluções de software livre	• Percentual de uso de soluções de software livre.	30%	35%	40%	50%
11. Priorizar recursos orçamentários para segurança da informação conforme diretrizes do PDTIC.	• Reuniões estratégicas com a Diretoria sobre o impactos na segurança da informação. Realizar 4 reuniões por ano.	2	2	3	4

Fonte: Modelo Canva adaptado pelo autor (2025)

9. OBEJECTIVE KEY-RESULTS (OKR) ESTRATÉGICO DA COSEG

A metodologia Objective and Key Results (OKR) tem se consolidado como uma ferramenta estratégica de gestão por resultados, utilizada para alinhar objetivos organizacionais e mensurar o progresso de metas de forma transparente e participativa. Criada por Andy Grove na Intel, e popularizada por John Doerr, OKR é uma estrutura que "define o que se quer alcançar (Objective) e como saber se está sendo alcançado (Key Results)" (DOERR, 2019).

Quadro 8- Objective Key-Results (OKR)

Objectives, Key Activities and Results (OKR)			
01	OBJECTIVES	KEY ACTIVITIES	RESULTS
	1. Fortalecer a governança e os processos de segurança da informação no IFS	• 1.1. Revisão de pelo menos 5 normativos internos de segurança da informação até o 4° ano.	20%
		• 1.2. Reuniões com comitê ativo de segurança da informação da ETIRs, realizando ao menos 4 reuniões por ano.	60%
		• 1.3. Monitoramento de 100% dos sistemas críticos da instituição até o 4° ano.	70%
02	OBJECTIVES	KEY ACTIVITIES	RESULTS
	2. Aumentar a capacidade de resposta e mitigação de incidentes de segurança	• 2.1. Redução do tempo médio de resposta a incidentes de 36h para 12h até o 3° ano.	50%
		• *2.2. Realização de ao menos 2 simulações de incidentes cibernéticos por ano.*	40%
		• 2.3. Capacitação de 100% da equipe de TI / COSEG em resposta a incidentes e gestão de riscos até o 3° ano.	35%

03	OBJECTIVES	KEY ACTIVITIES	RESULTS
	3. Consolidar a cultura de segurança da informação na comunidade acadêmica e administrativa	• 3.1. Realização no mínimo 3 campanhas educativas de segurança da informação por ano.	30%
		• 3.2. Elevação até o nível 4 no índice de maturidade institucional em segurança da informação até o 4° ano.	35%
		• 3.3. Garantia de que 80% da comunidade interna conheça as boas práticas de segurança da informação, conforme avaliação anual.	35%

04	OBJECTIVES	KEY ACTIVITIES	RESULTS
	4. Otimizar recursos financeiros e tecnológicos com foco em sustentabilidade	• 4.1. Substituição de ao menos 50% das soluções comerciais por softwares livres até o 4° ano.	35%
		• 4.2. Reuniões estratégicas com a Diretoria sobre o impactos na segurança da informação. Realizar 4 reuniões por ano.	50%
		• 4.3. Implantação no mínimo 3 novas soluções tecnológicas seguras e inovadoras até o 4° ano.	35%

Fonte: Modelo Canva adaptado pelo autor (2025)

Quadro 9- SWOT + Objective and Key Results (OKR)

SWOT	OBJETIVOS	RESULTADOS CHAVES	INICIATIVA ESTRATÉGIA
Baixo controle de políticas de segurança nos laboratórios.	1. Fortalecer a governança e os processos de segurança da informação no IFS	1.1. Revisão de pelo menos 5 normativos internos de segurança da informação até o 4º ano. 1.2. Reunões com comitê ativo de segurança da informação da ETIRs, realizando ao menos 4 reuniões por ano. 1.3. Monitoramento de 100% dos sistemas críticos da instituição até o 4º ano.	• Criar um cronograma anual de revisão dos normativos, envolvendo a COSEG, setores de TI para garantir alinhamento à LGPD e às melhores práticas. • Instituir formalmente o comitê com representantes da COSEG, TI, gestão e usuários-chave, com atas e pautas de ações. • *Implementar ferramentas de monitoramento contínuo e estabelecer rotinas de análise de logs e eventos críticos.*
SWOT	**OBJETIVOS**	**RESULTADOS CHAVES**	**INICIATIVA ESTRATÉGIA**
Infraestrutura tecnológica obsoleta ou defasada nos Campi.	2. Aumentar a capacidade de resposta e mitigação de incidentes de segurança	2.1. Redução do tempo médio de resposta a incidentes de 36h para 12h até o 3º ano. 2.2. Realização de ao menos 2 simulações de incidentes cibernéticos por ano. 2.3. Capacitação de 100% da equipe de TI / COSEG em resposta a incidentes e gestão de riscos até o 3º ano.	• *Estabelecer equipe de resposta a incidentes níveis de acordo de serviço (SLAs) e protocolos padronizados.* • *Criar cenários simulados de ataques para treinar equipes técnicas e administrativas, com relatórios e planos de melhoria.* • *Promover treinamentos presenciais e EAD com parceiros como a RNP e o CISC GOV.BR.*
SWOT	**OBJETIVOS**	**RESULTADOS CHAVES**	**INICIATIVA ESTRATÉGIA**
Baixa de cultura organizacional sobre proteção de dados e boas práticas de segurança digital.	3. Consolidar a cultura de segurança da informação na comunidade acadêmica e administrativa	3.1. Realização de no mínimo 3 campanhas educativas de segurança da informação por ano. 3.2. Elevação até o nível 4 no índice de maturidade institucional em segurança da informação até o 4º ano. 3.3. Garantia de que 80% da comunidade interna conheça as boas práticas de segurança da informação, conforme avaliação anual.	• Criar um cronograma anual de revisão dos normativos, envolvendo a COSEG, setores de TI para garantir alinhamento à LGPD e às melhores práticas. • Instituir formalmente o comitê com representantes da COSEG, TI, gestão e usuários-chave, com atas e pautas de ações. • *Implementar ferramentas de monitoramento contínuo e estabelecer rotinas de análise de logs e eventos críticos.*
SWOT	**OBJETIVOS**	**RESULTADOS CHAVES**	**INICIATIVA ESTRATÉGIA**
Fortalecer a COSEG como estrutura especializada no IFS.	4. Otimizar recursos financeiros e tecnológicos com foco em sustentabilidade	4.1. Substituição de ao menos 50% das soluções comerciais por softwares livres até o 4º ano. 4.2. Priorização de Orçamento para segurança de TI de acordo com o Plano Diretor de Tecnologia da Informação - PDTIC. 4.3. Implantação no mínimo 3 novas soluções tecnológicas seguras e inovadoras até o 4º ano.	• *Levantar soluções comerciais passíveis de substituição e realizar projetos-piloto com alternativas de software livre.* • *Elaborar projetos de segurança da informação e escrever editais de licitações federais para aquisições planejadas.* • *Buscar soluções inovadoras no mercado, priorizando novas tecnologias e com suporte à continuidade de serviços.*

PROPOSTA DE INTERVENÇÃO

Este Projeto Técnico Tecnológico tem como proposta a elaboração do planejamento estratégico no serviço público, adotando uma abordagem integrada que contempla as ferramentas SWOT, Matriz Eisenhower, Balanced Scorecard (BSC) e Objective and Key Results (OKR).

Nesse contexto, foram analisados os seguintes elementos: diagnóstico organizacional; priorização de fatores que podem influenciar o alcance dos objetivos; diretrizes estratégicas (missão, visão e valores); definição dos objetivos estratégicos; indicadores de desempenho; metas; estruturação dos OKRs; e elaboração do plano de ação, com as iniciativas estratégicas e a designação dos responsáveis pela execução.

Com bases nos resultados obtidos sugere-se, a construção do planejamento estratégico na COSEG adotando as seguintes etapas:

1. Estabelecimento das diretrizes estratégicas;
2. Desenvolvimento do diagnóstico organizacional;
3. Identificação e priorização dos fatores que influenciam o alcance dos objetivos;
4. Determinação dos objetivos estratégicos;
5. Definição dos indicadores de desempenho e metas correspondentes;
6. Estruturação dos OKRs (Objectives and Key Results);
7. Formulação do plano de ação, com as iniciativas estratégicas e a atribuição de responsabilidades pela execução

RESPONSÁVEIS PELA PROPOSTA DE INTERVENÇÃO E DATA

João Silvio Ribeiro dos Santos

Mestrando no Programa de Pós-graduação em Administração Pública da Universidade Federal de Sergipe (PROFIAP/UFS). Especialista em Gestçao de Redes pela Escola Aberta do Brasil (2012), graduação em Gestão de Sistemas de Informação pela Faculdade de Administração e Negócios de Sergipe (2008). Atualmente é técnico de tecnologia de informação do Instituto Federal de Sergipe. Experiência na área de Gestão de Redes de Computadores e Segurança da Informação.
(joaosilvio@academico.ufs.br)

Prof. Dr. Cláudio Márcio Campos de Mendonça

Pós-Doutorado em Gestão na Católica Porto Business School (2018) na área de Transformação Digital e Capacidades Dinâmicas, Doutorado em Administração pelo PPGA/UFRN na área de Governança de TI e Computação em Nuvem, Mestrado em administração, Especializações: MBA em Gestão da Tecnologia da Informação e Gestão Universitária. Graduações em Processamento de Dados (1996) e Administração (2012) pela Universidade Potiguar - UnP. Atualmente Professor com Dedicação Exclusiva na Universidade Federal de Sergipe (UFS), Experiência nas áreas de Governança de TI, tecnologia da informação, banco de dados, Business Intelligence, Big Data, Inteligência Artificial, metodologias ágeis (OKR e Kanban), estratégia, gestão de projetos ágeis (SCRUM, Life Cycle Canvas, PMC), gestão por processo, educação a distância e gestão de ensino superior. Possui Certificações LCC Associate e LCC Professional - Life Cycle Canvas para Gestão de Projetos Ágeis. Professor Universitário desde 1997, lecionando disciplinas principalmente nos cursos de Sistemas de Informação e Administração, além de disciplinas de Pós-Graduação lato sensu e stricto sensu. Também atuado como Diretor de TI, Pró-Reitor de Graduação e Diretor de Qualidade Acadêmica da Universidade Potiguar-UnP/RN. Atualmente Coordenador Adjunto do Mestrado Profissional em Administração Pública - PROFIAP/UFS.
(claudiomendonca@academico.ufs.br)

REFERÊNCIAS

CHIAVENATO, Idalberto. **Introdução à teoria geral da administração**. Elsevier, 2014.

COVEY, Stephen R. **Os 7 hábitos das pessoas altamente eficazes**. Editora Best Seller, 2015.

DOERR, J. **Avalie o que importa: como o Google, Bono Vox e a Fundação Gates sacudiram o mundo com os OKRs**. Alta Books, 2019.

DRUCKER, Peter F. **Administração, tarefas, responsabilidades, práticas**. Pioneira, 1975.

KAPLAN, Robert S.; NORTON, David P. **Mapas estratégicos: balanced scorecard**. Alta Books, 2018.

JOHNSON, Gerry; SCHOLES, Kevan; WHITTINGTON, Richard. **Fundamentos de estrategia**. Bookman Editora, 2011.

MAXIMIANO, Antônio César Amaru. **Teoria geral da administração**: da revolução urbana à revolução digital. Atlas, 2017.

DOS ANJOS OLIVEIRA, Thaís Cristine. Governança em Segurança da Informação: por que ela é tão importante para os negócios?. **Advances in Knowledge Representation**, v. . 2, p. 142-159, 2024. Disponível em: https://periodicos.ufmg.br/index.php/advances-kr/article/view/52933. Acesso em: 08 jul. 2025.

IFS - Instituto Federal de Educação, Ciência e Tecnologia de Sergipe. Levantamentos de GovTIC / IFS. Aracaju: IFS, 2024. Disponível em: https://www.ifs.edu.br/noticias-dti/6865-levantamentos-de-govtic-ifs-2.html. Acesso em: 07 jul. 2025

IFS - Instituto Federal de Educação, Ciência e Tecnologia de Sergipe. IFS fica em 1º lugar entre órgãos do MEC em medidas de proteção contra ataques cibernéticos. IFS, 2020. Disponível em: https://ifs.edu.br/ultimas-noticias/9036-ifs-fica-em-1-lugar-entre-orgaos-do-mec-em-medidas-de-protecao-contra-ataques-ciberneticos. Acesso em: 07 jul. 2025

Protocolo de recebimento do produto técnico-tecnológico

À Diretoria de Tecnologia da Informação (DTI) do Instituto Federal de Sergipe (IFS)

Pelo presente, encaminhamos o produto técnico-tecnológico intitulado **"Planejamento Estratégico com BSC e OKR aplicados à Segurança da Informação: Uma Proposta de indicadores estratégicos para a COSEG/IFS"**, derivado do trabalho final da disciplina Planejamento e Administração Estratégica do Programa de Pós-graduação em Administração e Pública em Rede PROFIAP/UFS, de autoria de **João Silvio Ribeiro dos Santos.**

Os documentos citados foram desenvolvidos no âmbito do Mestrado Profissional em Administração Pública em Rede Nacional (Profiap), instituição associada **"Universidade Federal de Sergipe"**.

A solução técnico-tecnológica é apresentada sob a forma de um Produto Técnico Tecnologico - PTT e seu propósito é propor uma metodologia de elaboração de um planjenamento estratégico para a Coordenadoria de Segurança da Informação (COSEG).

Solicitamos, por gentileza, que ações voltadas à implementação desta proposição sejam informadas à Coordenação Local do Profiap, por meio do endereço "profiap@academico.ufs.br".

Aracaju, SE de de 2025.

Registro de recebimento

Profª. Msc. Marcos Pereira dos Santos
Diretor de Tecnologia da Informação (DTI/IFS)

Discente: João Silvio Ribeiro dos Santos

Orientador: prof. Dr. Cláudio Márcio Campos Mendonça

Universidade Federalde Sergipe (UFS)

julho de 2025.

PROFIAP

MESTRADO PROFISSIONAL EM ADMINISTRAÇÃO PÚBLICA