

A Gestão do Conhecimento na Segurança Cibernética: *Framework* FISIC como Integrador entre a Governança do COBIT 2019 e a Operação da ISO/IEC 27001

Knowledge Management in Cybersecurity: the FISIC Framework as an Integrator between COBIT 2019 Governance and ISO/IEC 27001 Operation

Philipp Valim

Mestrando. Universidade Nove de Julho (UNINOVE) – Brasil.
philippvalim@gmail.com

Ivanir Costa

Doutor. Universidade Nove de Julho (UNINOVE) – Brasil.
icostal1@live.com

Marcos Antonio Gaspar

Doutor. Universidade Nove de Julho (UNINOVE) – Brasil.
marcos_gaspar@hotmail.com

Marco Antonio Norbiato

Mestrando. Universidade Nove de Julho (UNINOVE) – Brasil.
norbiato@msn.com

Guilherme de Toledo Costa

Mestrando. Universidade Nove de Julho (UNINOVE) – Brasil.
g.toledocosta@gmail.com

RESUMO

A necessidade de conformidade regulatória e proteção contra ameaças digitais tornou a segurança da informação uma prioridade nas organizações. Ainda assim, é comum observar uma separação estrutural entre as diretrizes de governança e a execução operacional, o que resulta na fragmentação do conhecimento crítico. Essa divisão gera retrabalho, perda de memória organizacional e ineficiência, especialmente durante as auditorias. Sob a perspectiva da Gestão do Conhecimento, esta pesquisa propõe um modelo conceitual para traduzir o conhecimento estratégico em práticas operacionais rastreáveis. Por meio do método *Design Science Research* (DSR), o estudo desenvolve o *framework* FISIC, uma matriz de correlação direta entre o objetivo de otimização de riscos (EDM03) do COBIT 2019 e os controles técnicos do Anexo A da ISO/IEC 27001:2022. O estudo concentra-se especificamente no objetivo de governança EDM03 (Assegurar a Otimização de Riscos), entre os 40 objetivos do COBIT 2019, como recorte metodológico para a demonstração do *framework*. O artefato atua como um mecanismo de externalização, combinação e internalização do conhecimento, viabilizando a geração de uma evidência única de auditoria. O resultado oferece um referencial teórico e prático que reduz a dependência do conhecimento tácito individual e apoia uma cultura de governança de TI baseada na troca contínua de informações.

PALAVRAS-CHAVE: Gestão do Conhecimento; Governança de TI; Segurança da Informação; COBIT 2019; ISO/IEC 27001:2022.

ABSTRACT

The need for regulatory compliance and protection against digital threats has made information security a priority in organizations. Still, it is common to observe a structural separation between governance guidelines and operational execution, which results in the fragmentation of critical knowledge. This division generates rework, loss of organizational memory and

inefficiency, especially during audits. From a Knowledge Management perspective, this research proposes a conceptual model to translate strategic knowledge into traceable operational practices. Using the Design Science Research (DSR) method, the study develops the FISIC framework, a direct correlation matrix between the risk optimization objective (EDM03) of COBIT 2019 and the technical controls of Annex A of ISO/IEC 27001:2022. The study focuses specifically on the governance objective EDM03 (Ensure Risk Optimization), among the 40 objectives of COBIT 2019, as a methodological scope for demonstrating the framework. The artifact acts as a mechanism for externalizing, combining and internalizing knowledge, enabling the generation of unique audit evidence. The result offers a theoretical and practical framework that reduces dependence on individual tacit knowledge and supports an IT governance culture based on the continuous exchange of information.

KEYWORDS: Knowledge Management; IT Governance; Information Security; COBIT 2019; ISO/IEC 27001:2022.

1 INTRODUÇÃO

A segurança da informação deixou de ser uma preocupação exclusivamente técnica para assumir um papel central nas decisões da alta gestão, impulsionada pela rápida digitalização dos negócios (Alshaikh *et al.*, 2025). Hoje, um dos maiores desafios enfrentados pela Governança de TI (GTI) é garantir que a proteção de dados atue em sinergia com a continuidade operacional (Rambau *et al.*, 2026). Apesar dos investimentos em certificações e tecnologias, nota-se, na prática, dificuldade de traduzir políticas abstratas de governança em rotinas de trabalho integradas (Dhillon *et al.*, 2021; Leego; Bider, 2023).

A principal dificuldade para essa fluidez está na gestão do conhecimento corporativo. As corporações precisam se adequar a múltiplos padrões de mercado, como o COBIT 2019 (ISACA, 2019), de caráter estratégico, e a ISO/IEC 27001 (2022), focada na operação técnica. O que ocorre no dia a dia é o trabalho em áreas isoladas: o conselho administrativo define o apetite ao risco e as regras, enquanto as equipes de TI executam configurações isoladas sem entender plenamente o contexto de negócio. Sem um canal formal de compartilhamento de informações, a inteligência crítica de segurança fica retida na mente de poucos especialistas como um conhecimento tácito (Nonaka; Takeuchi, 1997). Consequentemente, as corporações realizam retrabalho e duplicação de evidências em ciclos exaustivos de auditorias.

Nesse contexto, a Gestão do Conhecimento (GC) oferece uma base conceitual importante para enfrentar essa fragmentação. Para transformar esforços isolados de conformidade em um processo corporativo mais consistente, é necessário estabelecer fluxos de conversão do conhecimento (Nonaka; Takeuchi, 1997; Valim *et al.*, 2025).

A partir desse problema, este estudo propõe a seguinte questão de pesquisa: como correlacionar e materializar os objetivos de governança do COBIT 2019 com as exigências operacionais da ISO/IEC 27001:2022 sob a perspectiva da Gestão do Conhecimento?

Para responder a essa questão, a pesquisa apoia-se no método *Design Science Research* (DSR) e propõe o *framework* FISIC Integrado de Segurança da Informação e Cibernética. O modelo consiste em uma matriz de correlação que conecta o objetivo de otimização de riscos (EDM03) do COBIT 2019 às exigências do Anexo A da ISO/IEC 27001:2022. O intuito é criar um padrão aplicável para documentar o conhecimento estratégico e consolidá-lo na geração de Evidências Únicas de Auditoria.

2 REFERENCIAL TEÓRICO

A fundamentação deste artigo articula-se no cruzamento entre os preceitos da GC e os instrumentos de governança corporativa (GovC) e segurança da informação.

2.1 FUNDAMENTOS DA GESTÃO DO CONHECIMENTO NA SEGURANÇA DA INFORMAÇÃO

Para compreender o papel da GC na GTI, resgata-se a hierarquia DIKW (Dados, Informação, Conhecimento, Sabedoria) (Ackoff, 1989). Segundo Davenport e Prusak (1998), dados são registros brutos, que se transformam em informação ao ganharem significado e propósito. O conhecimento, no entanto, é mais denso sendo o resultado da fusão entre a experiência humana, os valores e o contexto organizacional, permitindo a tomada de decisão estruturada. Trabalhos recentes (Lima *et al.*, 2024; Valim *et al.*, 2025) evidenciam que, no cenário tecnológico atual, é a estruturação e a fluidez desse conhecimento que sustentam a tomada de decisão ágil, estabelecendo uma correlação direta e necessária entre as práticas de GC e a eficácia da GTI.

Na segurança cibernética, essa dinâmica é decisiva. Acumular *logs* de sistemas (dados) ou emitir relatórios de conformidade (informação) não reduz riscos por si só. A efetividade das defesas depende da interpretação humana dos cenários e da aplicação adequada dos controles.

O desafio organizacional reside em lidar com as dimensões desse conhecimento. O conhecimento explícito é aquele passível de formalização, como manuais e políticas normativas. O tácito, por sua vez, é subjetivo, difícil de articular e inerente à vivência do profissional, como apontam Nonaka e Takeuchi (1997). Quando a inteligência de segurança permanece apenas no plano tácito, as organizações tornam-se dependentes de poucos especialistas.

Para superar esse gargalo, o modelo SECI (Socialização, Externalização, Combinação e Internalização), de Nonaka e Takeuchi (1997), torna-se relevante. No escopo deste artigo, destaca-se o processo de externalização, que traduz a experiência das equipes em procedimentos formais, e a combinação, que integra conceitos dispersos em um sistema

estruturado. É por meio dessa dinâmica que normas aparentemente desconexas podem convergir.

A Figura 1 apresenta o fluxo contínuo de criação do conhecimento proposto por Nonaka e Takeuchi (1997), detalhando as interações necessárias para superar a fragmentação das informações nas organizações.

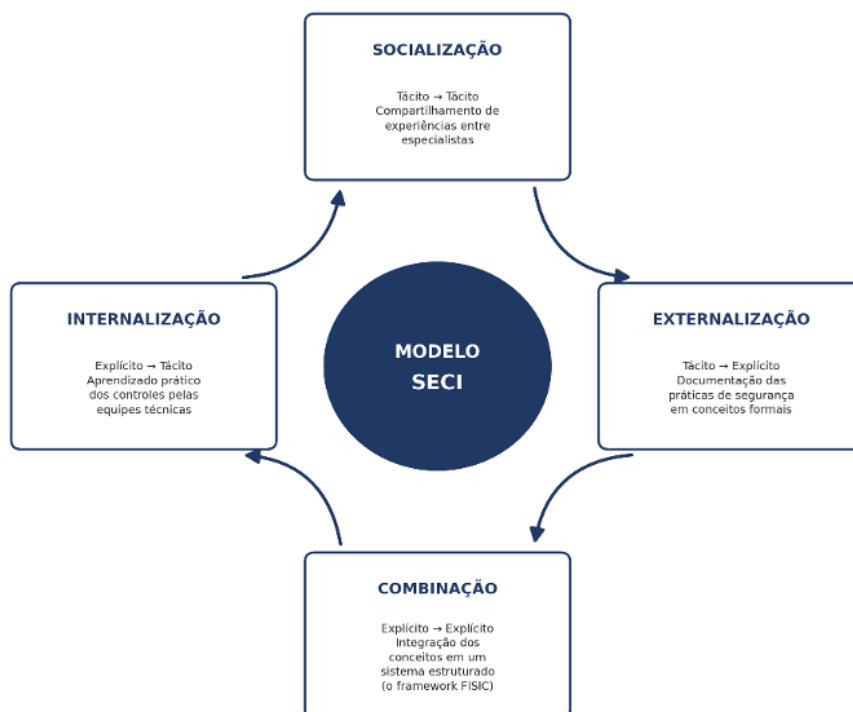


Figura 1 – Espiral de conversão do conhecimento (modelo SECI)

Fonte: Adaptado de Nonaka e Takeuchi (1997)

2.2 FRAMEWORKS DE GOVERNANÇA E SEGURANÇA: COBIT 2019 E ISO/IEC 27001

O mercado tem como referenciais consagrados o *framework* COBIT 2019 e a norma ISO/IEC 27001:2022, para ordenar seus processos tecnológicos. Contudo, a eficácia de ambos depende da fluidez com que a organização troca informações.

A ISO/IEC 27001:2022 fundamenta o Sistema de Gestão de Segurança da Informação (SGSI), adotando uma abordagem tática e operacional. Seu propósito é salvaguardar a confidencialidade, integridade e disponibilidade das informações, exigindo a formalização documental e a implementação de controles técnicos listados em seu Anexo A. Isso se alinha à retenção do conhecimento explícito. Em uma camada superior, o COBIT 2019 aborda a GTI com o olhar estratégico, buscando conectar a tecnologia aos fins do negócio (ISACA, 2019), separando claramente a governança da gestão.

A Figura 2 ilustra a separação estrutural entre as camadas de Governança e Gestão do COBIT 2019, destacando o domínio EDM, no qual se insere o objetivo EDM03, como a instância responsável por avaliar, direcionar e monitorar a otimização de riscos corporativos.

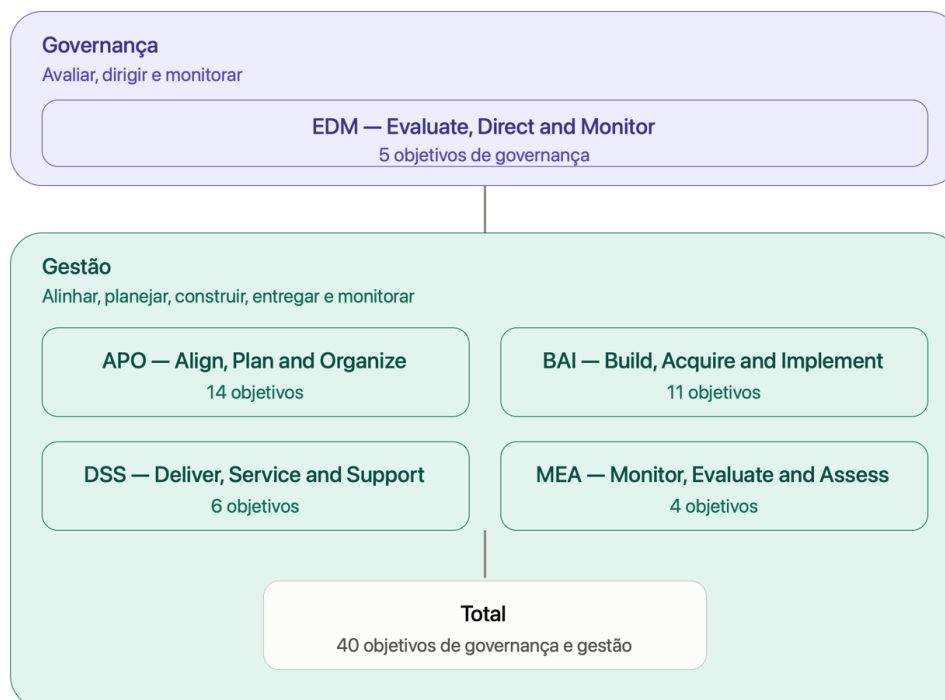


Figura 2 – Estrutura de Governança e Gestão do COBIT 2019

Fonte: Adaptado de ISACA (2019)

No domínio EDM (Avaliar, Direcionar e Monitorar), estão os interesses da alta administração. O objetivo EDM03 (Assegurar a Otimização de Riscos), por exemplo, dita como a diretoria deve entender e modular a tolerância ao risco corporativo. Outro ponto fundamental para o COBIT 2019 é a segregação de funções, que exige independência entre quem concebe as políticas (governança) e quem as executa ou audita (operação).

No contexto de monitoramento de governança, os indicadores de risco (*Key Risk Indicators* - KRIs) desempenham um papel fundamental. Conforme definido pela ISACA (2019), os KRIs são métricas quantitativas projetadas para monitorar a exposição ao risco e fornecer um alerta precoce sobre possíveis desvios no apetite ao risco estabelecido pela organização. Diferente de métricas operacionais isoladas, os KRIs traduzem indicadores técnicos em visões estratégicas de governança, permitindo que a alta direção identifique tendências adversas antes que estas se materializem em incidentes críticos.

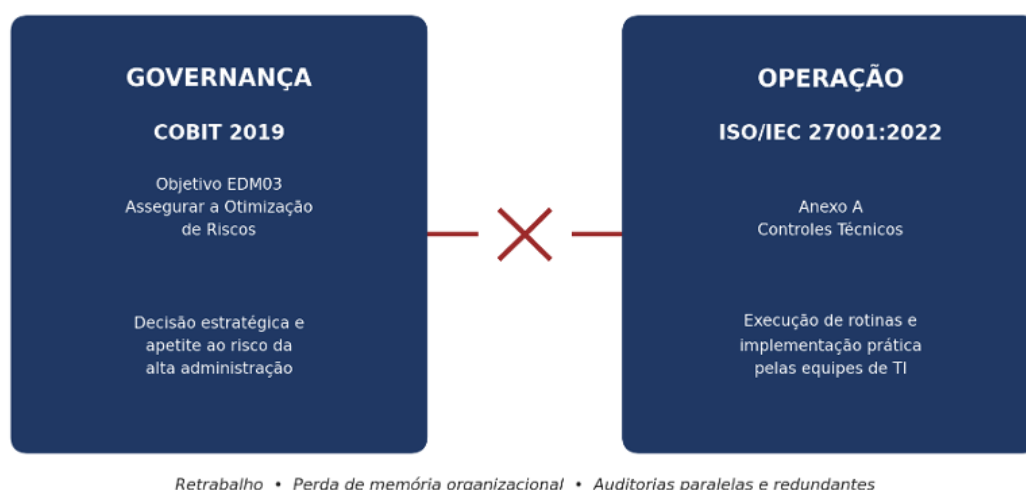
2.3 A FRAGMENTAÇÃO DO CONHECIMENTO NA PRÁTICA

O problema que motiva este trabalho decorre da ausência de integração prática entre os dois modelos de referência: o COBIT 2019, centrado na GTI, e a ISO/IEC 27001, focada nos requisitos técnicos de segurança da informação. Enquanto a alta cúpula debate a otimização de riscos, os administradores de redes configuram *firewalls* (barreiras de segurança) sem a visão macro do negócio.

A literatura indica que apenas adotar selos e certificações não garante proteção efetiva contra a sofisticação das ameaças modernas (Grigaliūnas *et al.*, 2024). A lacuna de integração se caracteriza no fato de que, enquanto o COBIT 2019 fornece a visão estratégica para a GTI do valor e do risco, a ISO/IEC 27001:2022 concentra-se na especificação granular dos controles de segurança; contudo, não há um protocolo formal que traduza o objetivo de governança (como o EDM03) diretamente para a execução técnica do Anexo A da norma.

A ausência de um elo de tradução leva as organizações a gerenciarem domínios isolados, resultando no isolamento de informações, em que o conhecimento de governança não alcança a operação e a execução técnica falha em espelhar as diretrizes de risco da alta gestão. A falta de uma forma clara de externalizar esse conhecimento perpetua a redundância de processos e o retrabalho. Portanto, torna-se necessário projetar um artefato que unifique esses domínios.

A Figura 3 sintetiza graficamente essa desconexão e a distância operacional entre a estratégia de governança e a prática de segurança.



Retrabalho • Perda de memória organizacional • Auditorias paralelas e redundantes

Figura 3 – Desconexão entre a Governança e a Operação de Segurança da Informação

Fonte: Elaborado pelos autores

3 METODOLOGIA

Esta pesquisa, de caráter exploratório e aplicado, busca estabelecer uma relação teórica e estrutural entre as diretrizes de governança da GTI e a operação da segurança da informação. Para isso, adotou-se o método *Design Science Research* (DSR), reconhecido por sua aplicação no desenvolvimento de artefatos voltados à solução de problemas organizacionais relevantes, gerando simultaneamente conhecimento científico generalizável (Hevner *et al.*, 2004).

Para a aplicação do método DSR, esta pesquisa fundamenta-se no modelo Ciclo de três níveis (*Three Cycle View*) proposto por Hevner (2007). A Figura 4 apresenta as etapas do Ciclo de três níveis do método DSR.

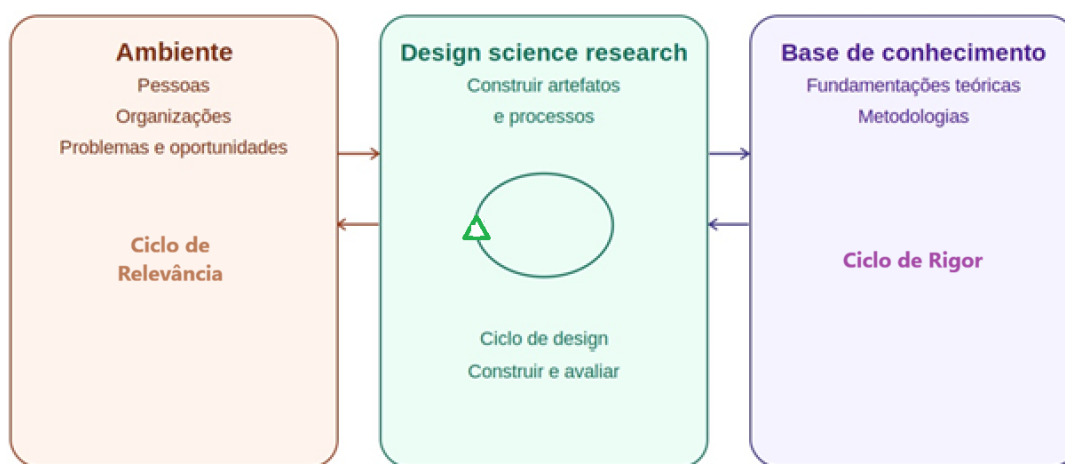


Figura 4 – Ciclo de três níveis do DSR

Fonte: Adaptado de Hevner (2007) - Desenvolvido pelos autores com apoio da IA generativa (Google Gemini)

Como mostra a Figura 4, a pesquisa é organizada em ciclos interligados: o Ciclo de Relevância, que ancora o problema no contexto real; o Ciclo de Design, que orienta a construção e avaliação do artefato; e o Ciclo de Rigor, que conecta a pesquisa à base científica consolidada.

Com base nessa estrutura teórica, o ciclo da pesquisa foi conduzido por meio de três etapas fundamentais:

- 1) Fundamentação e Diagnóstico (RSL):** O problema prático foi embasado por uma Revisão Sistemática da Literatura (RSL), conduzida de acordo com as diretrizes e o *checklist* do protocolo PRISMA 2020 (Page *et al.*, 2021), com o objetivo de garantir transparência e replicabilidade na seleção dos artigos. A busca foi realizada nas bases de dados acadêmicas Scopus e Web of Science, utilizando a *string* ("*Knowledge Management*" OR "*Knowledge Sharing*") AND ("*Cybersecurity*" OR "*Information Security*") AND ("*IT Governance*" OR "COBIT" OR "ISO 27001"), sem restrição de idioma, com

recorte temporal dos últimos cinco anos (2021–2026) e limitada a artigos científicos (excluindo-se livros, capítulos e anais de eventos). O processo de seleção seguiu as etapas do PRISMA, evidenciadas na Figura 5: identificação de 26 registros, dos quais 1 foi removido por duplicidade entre as bases ($n = 25$); triagem por título e resumo, com exclusão de 6 registros por não atenderem aos critérios de elegibilidade, sendo 3 por estarem fora do escopo temático (CE1: foco em áreas correlatas, como saúde, propriedade intelectual ou gestão de projetos de TI) e 3 por apresentarem foco estritamente técnico-matemático, sem abordagem do fator humano ou organizacional (CE2: modelagem via teoria dos jogos, protocolos criptográficos de usuário final e automação de dados sem interação humana), resultando em 19 artigos incluídos na revisão ($n = 19$). A análise detalhada desses 19 artigos ratificou a lacuna: a literatura selecionada mostra escassez de instrumentos que conectem diretamente o COBIT 2019 e a norma ISO/IEC 27001 no ambiente prático da TI.

2) Construção do Artefato (framework FISIC): A matriz de correlação foi projetada a partir dos princípios de externalização e combinação do conhecimento (Nonaka; Takeuchi, 1997), conectando a expectativa executiva de riscos aos controles técnicos exigidos.

3) Proposição do Artefato e Escopo de Validação: Como esta pesquisa tem o objetivo de estabelecer a base conceitual e estrutural do *framework* FISIC, ela se apoia no Ciclo de Relevância (identificação do problema) e no Ciclo de Rigor (fundamentação teórica em SECI, na hierarquia DIKW e na literatura de governança de TI e segurança da informação) para conduzir o Ciclo de *Design*, no qual o *framework* FISIC foi construído e proposto como uma contribuição teórica fundamentada. A etapa de avaliação empírica do artefato, ainda não realizada, constitui a etapa subsequente do Ciclo de *Design* e é proposta como trabalho futuro, a ser conduzida junto a profissionais de auditoria e *Chief Information Security Officers* (CISOs), com o objetivo de avaliar sua eficácia prática no mercado.

A Figura 5 apresenta os resultados obtidos com a pesquisa e seleção nas bases de dados, seguindo a estrutura do protocolo PRISMA 2020.



Figura 5 – Seleção de artigos usando protocolo PRISMA 2020 adaptado

Fonte: Adaptado do Protocolo PRISMA 2020

4 RESULTADOS E DISCUSSÃO

O artefato desenvolvido é o *Framework* FISIC, que funciona como um instrumento fundamental e formal de GC ao sistematizar a transição do conhecimento tácito para o explícito, como proposto por Nonaka e Takeuchi (1997). O *framework* opera por meio de dois pilares da GC: a externalização, que traduz os objetivos estratégicos da alta administração, que são frequentemente retidos como conhecimento tácito sobre apetite ao risco, em diretrizes normativas claras; e a combinação, que integra essas diretrizes aos controles técnicos do anexo A da ISO/IEC 27001:2022 em uma matriz estruturada.

Dessa forma, o FISIC assegura que cada atividade tática de segurança esteja vinculada a um propósito estratégico do negócio, transformando decisões de governança em evidências técnicas rastreáveis e auditáveis.

Sua aplicação dá-se pela conexão entre o objetivo EDM03 (Assegurar a Otimização de Riscos) do COBIT 2019 e o Anexo A da ISO/IEC 27001:2022. A estrutura do *framework* organiza-se em quatro componentes:

- **Eixo de Governança de TI (COBIT 2019):** Indica o alvo estratégico ditado pela alta gestão e seu apetite ao risco.
- **Eixo de Segurança (ISO/IEC 27001:2022):** Delimita qual controle ou cláusula normativa mitiga o risco apontado.

- **Ação de Correlação Prática:** Demonstra o movimento de externalização do conhecimento, explicando como a operação técnica atende à demanda da governança.
- **Evidência Única de Auditoria:** É o registro formal (entregável) que comprova a conformidade para ambos os referenciais ao mesmo tempo, reduzindo a duplicação de documentos.

O Quadro 1 detalha essa dinâmica. A matriz traduz as diretrizes do conselho em entregáveis claros para as equipes de proteção.

Quadro 1 – Matriz de correlação e externalização do conhecimento (FISIC)

Prática de Governança (COBIT 2019 – EDM03)	Eixo de Segurança (ISO/IEC 27001:2022)	Ação de Correlação Prática	Evidência Única de Auditoria (Entregável Esperado)
EDM03.01 – Avaliar a Gestão de Risco: avaliar o alinhamento da gestão de risco de TI com o apetite ao risco da organização.	Cláusulas 4.1, 4.2 e 6.1.2: contexto da organização, necessidades das partes interessadas e avaliação de riscos.	O Conselho avalia o cenário de ameaças e define o apetite ao risco de negócio. A operação de segurança técnica operacionaliza essa diretriz realizando o mapeamento de impactos sistêmicos.	Matriz Corporativa de Apetite ao Risco; Relatórios de Avaliação de Riscos e de Impacto nos Negócios (BIA).
EDM03.02 – Direcionar a Gestão de Risco: direcionar as práticas para garantir que as falhas não excedam a tolerância do negócio.	Cláusulas 5.1 e 6.1.3: liderança e comprometimento, tratamento de riscos de segurança da informação.	A alta direção patrocina os investimentos necessários e oficializa a adoção de controles técnicos, aprovando o plano formal de tratamento de riscos e delegando a implementação ao CISO.	Declaração de Aplicabilidade (SoA); Plano de Tratamento de Riscos; Política Global de Segurança da Informação.
EDM03.03 – Monitorar a Gestão de Risco: monitorar os principais objetivos e métricas do processo de gestão de risco e relatar desvios à alta direção.	Cláusulas 9.1 e 9.3: monitoramento, medição, análise, avaliação e análise crítica pela direção.	A governança corporativa exige reporte sistemático do perfil de risco. A equipe de segurança atende à demanda estruturando indicadores de eficácia dos controles e apresentando-os à avaliação executiva.	Indicadores-Chave de Risco (KRIs); Ata da Reunião de Análise Crítica pela Direção.

Fonte: Desenvolvido pelos autores com apoio da IA generativa (Google Gemini)

O Quadro 1 apresenta a correlação entre as práticas de GTI (COBIT 2019) e as cláusulas operacionais de segurança da informação da norma internacional ISO/IEC 27001:2022, propondo as ações práticas conjuntas entre o conselho de administração (estratégico) e os responsáveis pela segurança da informação na TI. Ele indica também as evidências de auditoria tanto para auditores de GTI como auditores da norma ISO.

Já o Quadro 2 explicita a dimensão da Gestão do Conhecimento dentro do *framework* FISIC, mapeando cada diretriz do EDM03 ao modo de conversão do conhecimento do modelo SECI (Nonaka; Takeuchi, 1997) que ela aciona. Essa abordagem demonstra que o FISIC não

apenas correlaciona normas, mas opera como um mecanismo formal de externalização e combinação do conhecimento organizacional.

Quadro 2 – Correlação entre EDM03 do COBIT 2019, ISO/IEC 27001:2022 e o Modelo SECI de Gestão de Conhecimento

Diretriz de Governança (COBIT 2019 – EDM03)	Conexão Operacional (ISO/IEC 27001:2022)	Modo SECI (GC)	Movimento de Conhecimento
Diretriz 1 (EDM03.01) Avaliar a Gestão de Risco	Cláusulas 4.1, 4.2 e 6.1.2: contexto organizacional, partes interessadas e avaliação de riscos.	Externalização (Tácito → Explícito)	O apetite ao risco do conhecimento tácito da alta direção é convertido em uma Matriz Corporativa de Riscos e um BIA (Análise de Impacto nos Negócios), formalizados, tornando-se conhecimento explícito rastreável e acessível à equipe técnica.
Diretriz 2 (EDM03.02) Direcionar a Gestão de Risco	Cláusulas 5.1 e 6.1.3: liderança e comprometimento, tratamento de riscos de segurança.	Combinação (Explícito → Explícito)	A SoA (Declaração de Aplicabilidade), o Plano de Tratamento de Riscos e a Política Global integram múltiplos documentos explícitos em um sistema unificado de governança, consolidando o conhecimento disperso em um único artefato rastreável.
Diretriz 3 (EDM03.03) Monitorar a Gestão de Risco	Cláusulas 9.1 e 9.3: monitoramento, medição, avaliação e análise crítica pela direção.	Internalização (Explícito → Tácito)	O ciclo de monitoramento e análise crítica transforma os KRIs e relatórios formais em aprendizado organizacional contínuo, incorporando o conhecimento de risco à cultura e à rotina da equipe de segurança.

Fonte: Elaborado pelos autores com apoio da IA generativa (Google Gemini)

A socialização (Tácito → Tácito) não foi incluída no mapeamento das diretrizes do EDM03, uma vez que o recorte deste estudo se concentra na formalização documental do conhecimento (externalização e combinação) e na sua incorporação à rotina técnica (internalização). A dimensão da socialização, compartilhamento de experiências entre especialistas de segurança, permanece como lacuna relevante a ser explorada em trabalhos futuros, sobretudo por sua relevância na transmissão do conhecimento tácito entre profissionais seniores e equipes técnicas.

O apoio de IA generativa (Google Gemini) na elaboração da Figura 4 e dos Quadros 1, 2 e 3 limitou-se à geração de layout visual e à sugestão inicial de redação das células descritivas. Todas as correlações normativas apresentadas entre as diretrizes do EDM03, as cláusulas da ISO/IEC 27001:2022 e os modos de conversão do modelo SECI foram integralmente verificadas pelos autores contra os textos originais do COBIT 2019 (ISACA, 2019) e da ISO/IEC 27001:2022, de modo a assegurar a exatidão técnica do conteúdo.

5 DISCUSSÃO E IMPACTOS

O *framework* FISIC propõe uma mudança na forma de gerir a conformidade. Em vez de tratar a GTI e a segurança como áreas isoladas, o *framework* usa a GC para aproximá-las, com efeitos organizacionais e financeiros.

5.1 IMPACTO ORGANIZACIONAL E RETENÇÃO DO CONHECIMENTO

No âmbito da cultura organizacional, a matriz funciona como um meio de externalização (Nonaka; Takeuchi, 1997). Registrar formalmente a relação entre o apetite de risco corporativo e o controle de TI reduz a dependência da memória isolada dos profissionais sêniores e incorpora a inteligência de segurança aos processos da organização. Além disso, ao contrário do que se poderia supor, consolidar as evidências não fere o princípio de Segregação de Funções exigido pelo COBIT 2019; pelo contrário, o modelo esclarece os papéis: o conselho define a tolerância ao risco e o *Chief Information Security Officer* (CISO) coordena a mitigação técnica, preservando a autonomia das instâncias.

5.2 IMPACTO ECONÔMICO PROJETADO E OTIMIZAÇÃO DE AUDITORIAS

Do ponto de vista operacional e econômico, a principal contribuição do *framework* FISIC conceitual está na Evidência Única de Auditoria. Em cenários corporativos tradicionais e fragmentados, é comum que um mesmo controle técnico exija a emissão de relatórios paralelos e desconexos para auditores distintos. O FISIC busca reduzir essa disfunção: ao gerar um documento cruzado que satisfaz tanto a auditoria de negócios quanto a de TI, por meio de *Key Risk Indicators* (KRI), a ferramenta tem o potencial de permitir que uma única evidência técnica sirva a múltiplos propósitos de controle. Dessa forma, espera-se que a organização economize tempo das equipes e reduza custos relevantes associados a longos ciclos de auditorias, embora tal ganho ainda não tenha sido mensurado empiricamente, constituindo uma expectativa a ser validada em aplicações futuras do *framework*.

O Quadro 3 detalha a evolução projetada das dimensões operacionais, evidenciando como a migração para uma estrutura de Evidência Única tem o potencial de promover maior eficiência e transparência na governança de TI.

Quadro 3 – Comparativo projetado de cenários organizacionais antes e após a adoção do framework FISIC

Dimensão	Cenário Fragmentado (Antes)	Cenário Projetado com o Framework FISIC (Depois)
Evidências de auditoria	Relatórios duplicados para governança e para segurança técnica, produzidos em ciclos separados.	Evidência Única de Auditoria, compartilhada simultaneamente entre os dois referenciais.
Conhecimento crítico	Concentrado de forma tácita em poucos especialistas seniores.	Externalizado e documentado na matriz, reduzindo a dependência individual.
Segregação de funções	Pouco clara entre quem define o risco e quem implementa o controle.	Explícita: o Conselho define o apetite ao risco; o CISO responde pela execução técnica.
Retrabalho operacional	Alto, com esforço redundante entre auditorias de governança e técnicas.	Reduzido, pela reutilização do mesmo entregável nas duas frentes de auditoria.
Rastreabilidade	Indireta; difícil demonstrar o vínculo entre decisão estratégica e controle técnico.	Direta; cada controle do Anexo A é correlacionado a um objetivo específico do EDM03.

Fonte: Elaborado pelos autores com apoio da IA generativa (Google Gemini)

6 CONSIDERAÇÕES FINAIS E IMPLICAÇÕES

6.1 CONTRIBUIÇÃO DO TRABALHO

Este estudo propôs uma solução conceitual para o distanciamento recorrente entre as políticas de GTI e a operação técnica de segurança da informação. A pesquisa demonstrou que a fragmentação na conformidade regulatória decorre, em grande parte, de dificuldades no compartilhamento e na GC corporativo.

A aplicação das etapas de Fundamentação (RSL), Diagnóstico (Ciclo de Relevância) e *Design* do Artefato (Ciclo de *Design*) do método DSR permitiu a estruturação do *Framework* FISIC, uma matriz teórica que correlaciona diretamente o objetivo de otimização de riscos (EDM03) do COBIT 2019 aos controles táticos do Anexo A da norma ISO/IEC 27001:2022.

O artefato cumpre o propósito de desenhar um caminho para transformar decisões estratégicas em práticas operacionais rastreáveis, utilizando mecanismos de externalização e combinação do conhecimento para garantir a integridade da memória organizacional. Ao converter diretrizes abstratas em evidências documentais estruturadas, o *framework* FISIC estabelece uma trilha de auditoria contínua, argumentando que a segurança da informação atinge seu potencial máximo quando o conhecimento gerencial é formalizado e integrado à execução técnica.

6.2 IMPLICAÇÕES TEÓRICAS, PRÁTICAS E GERENCIAIS

Como contribuição acadêmica e gerencial, o trabalho fornece um modelo de referência estruturado para líderes de tecnologia e auditores que buscam simplificar o cumprimento de normas sobrepostas. Ao consolidar as evidências, o *framework* atua como um mecanismo de GC que protege a memória técnica da organização, evitando a fragmentação do saber e

reduzindo a dependência do conhecimento tácito retido individualmente. Esse processo materializa-se por meio da Evidência Única de Auditoria, que atua como um registro permanente e formalizado das decisões de governança e das práticas técnicas correspondentes.

6.3 LIMITAÇÕES DA PESQUISA E ESTUDOS FUTUROS

Por se tratar de uma proposição teórica e conceitual, o estudo possui limitações metodológicas decorrentes da ausência de testes de campo empíricos. Adicionalmente, o *framework* FISIC foi demonstrado a partir de um único objetivo de governança do COBIT 2019 (EDM03), não abrangendo os demais 39 objetivos do *framework*, o que constitui um recorte metodológico e não uma limitação de aplicabilidade do modelo proposto. Para trabalhos futuros, recomenda-se buscar a aprovação do *framework* FISIC junto a especialistas do mercado e aplicá-lo em ambientes corporativos reais, com o objetivo de mensurar quantitativamente a redução de horas investidas em auditorias e avaliar a consistência e a usabilidade da matriz perante especialistas do setor de segurança cibernética.

7 REFERÊNCIAS

ACKOFF, R. L. From data to wisdom. **Journal of Applied Systems Analysis**, v. 16, n. 1, p. 3-9, 1989.

ALSHAIKH, A.; ZHU, L.; SUN, J. Adaptive governance for digital transformation: a framework for IT security. **Journal of Strategic Information Systems**, v. 34, n. 1, 2025.

DAVENPORT, T. H.; PRUSAK, L. **Working knowledge**: how organizations manage what they know. Boston: Harvard Business Review Press, 1998.

DHILLON, G.; SMITH, M.; SUN, L. Security governance and technical compliance: the reality of organizational practice. **Computers & Security**, v. 102, 2021.

GRIGALIŪNAS, Š.; JEGELEVIČIUS, D.; TUREVIČIUS, G.; VAIŠNORAS, M. Holistic information security management and compliance framework. **Electronics**, v. 13, n. 19, p. 3955, 2024.

HEVNER, A. R. A three cycle view of design science research. **Scandinavian Journal of Information Systems**, v. 19, n. 2, art. 4, p. 87-92, 2007.

HEVNER, A. R.; MARCH, S. T.; PARK, J.; RAM, S. Design science in information systems research. **MIS Quarterly**, v. 28, n. 1, p. 75-105, 2004.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. **ISO/IEC 27001: information security management systems**. Geneva, 2022.

ISACA. **COBIT 2019 framework**: governance and management objectives. Schaumburg: ISACA, 2019.

LEEGO, S.; BIDER, I. Improving IT governance, security and privacy using fractal enterprise modeling: a case of a highly regulated company. In: PERSPECTIVES IN BUSINESS INFORMATICS RESEARCH, 2023, Berlin. **Lecture Notes in Business Information Processing**. Berlin: Springer, 2023. v. 493, p. 199-213. Disponível em: https://doi.org/10.1007/978-3-031-43126-5_15. Acesso em: 29 ago. 2026.

LIMA, M. R.; GASPAR, M. A.; PINTO, L. F. R.; COSTA, I.; MONTEIRO, R. C. Gestão do conhecimento e governança de tecnologia da informação: análise de elementos correlacionáveis. **Perspectivas em Gestão & Conhecimento**, João Pessoa, v. 14, n. 1, 2024.

NONAKA, I.; TAKEUCHI, H. **Criação de conhecimento na empresa**: como as empresas japonesas geram a dinâmica da inovação. Rio de Janeiro: Campus, 1997.

PAGE, M. J. *et al.* The PRISMA 2020 statement: an updated guideline for reporting systematic reviews. **BMJ**, v. 372, art. n71, 2021. Disponível em: <https://doi.org/10.1136/bmj.n71>. Acesso em: 29 ago. 2026.

RAMBAU, T. M.; MUNYOKA, W.; PHAHLAMOHLAKA, L. J.; KADYAMATIMBA, A. Evaluating cyber resilience frameworks for e-government: applicability of NIST CSF, ISO/IEC 27001 and COBIT 2019 in developing country contexts. **Information and Computer Security**, ahead-of-print, 2026. Disponível em: <https://doi.org/10.1108/ICS-09-2025-0376>. Acesso em: 29 ago. 2026.

VALIM, P. C.; COSTA, I.; NORBIATO, M. A.; CASTILHO, R.; OLIVEIRA NETO, G. C. Diretrizes para a inovação segura: equilibrando gestão do conhecimento e cibersegurança. In: CONGRESSO BRASILEIRO DE GESTÃO DO CONHECIMENTO (KM BRASIL), 20., 2025, São Paulo. **Anais [...]**. São Paulo: SBGC, 2025. p. 1-19.