UNIVERSIDADE ESTADUAL DE CAMPINAS
Faculdade de Engenharia Mecânica

REGINALDO DA SILVA LEME

Análise dos novos controles de segurança da informação evidenciados na ISO/IEC 27001:2022 com o uso do Método *Fuzzy* Dematel

CAMPINAS
2025

REGINALDO DA SILVA LEME

Análise dos novos controles de segurança da informação evidenciados na ISO/IEC 27001:2022 com o uso do Método Fuzzy Dematel

Dissertação apresentada à Faculdade de Engenharia Mecânica da Universidade Estadual de Campinas como parte dos requisitos exigidos para a obtenção do título de Mestre em Engenharia Mecânica, na Área de Materiais e Processo de Fabricação.

Orientador: Prof. Dr. Jefferson de Souza Pinto

Coorientador: Prof. Dr. Rosley Anholon

ESTE TRABALHO CORRESPONDE À VERSÃO FINAL DA DISSERTAÇÃO DEFENDIDA PELO ALUNO REGINALDO DA SILVA LEME E ORIENTADO PELO PROF. DR. JEFFERSON DE SOUZA PINTO.

CAMPINAS
2025

Ficha catalográfica
Universidade Estadual de Campinas (UNICAMP)
Biblioteca da Área de Engenharia e Arquitetura
Rose Meire da Silva - CRB 8/5974

L542a Leme, Reginaldo da Silva, 1987-
Análise dos novos controles de segurança da informação evidenciados na ISO/IEC 27001:2022 com o uso do método fuzzy dematel / Reginaldo da Silva Leme. – Campinas, SP : [s.n.], 2025.

Orientador: Jefferson de Souza Pinto.
Coorientador: Rosley Anholon.
Dissertação (mestrado) – Universidade Estadual de Campinas (UNICAMP), Faculdade de Engenharia Mecânica.

1. Tecnologia da informação - Sistemas de segurança. 2. Gerenciamento de riscos. 3. Conjuntos fuzzy. 4. Lógica Fuzzy. 5. Teoria da decisão. 6. Sistemas de informação - Medidas de segurança. 7. Gerenciamento de recursos de informação - Medidas de segurança. I. Pinto, Jefferson de Souza, 1978-. II. Anholon, Rosley, 1979-. III. Universidade Estadual de Campinas (UNICAMP). Faculdade de Engenharia Mecânica. IV. Título.

Informações complementares

Título em outro idioma: Analysis of the new information security controls highlighted in ISO/IEC 27001:2022 using the fuzzy DEMATEL method
Palavras-chave em inglês:
Information technology – Security systems
Risk management
Fuzzy sets
Fuzzy logic
Decision theory
Information systems – Security measures
Information resource management – Security measures
Área de concentração: Materiais e Processos de Fabricação
Titulação: Mestre em Engenharia Mecânica
Banca examinadora:
Jefferson de Souza Pinto [Orientador]
Suzana Regina Moro
Lucas Veiga Ávila
Data de defesa: 17-02-2025
Programa de Pós-Graduação: Engenharia Mecânica

Objetivos de Desenvolvimento Sustentável (ODS)
Não se aplica

Identificação e informações acadêmicas do(a) aluno(a)
- ORCID do autor: https://orcid.org/0000-0001-5566-7513
- Currículo Lattes do autor: http://lattes.cnpq.br/3156595495203818

UNIVERSIDADE ESTADUAL DE CAMPINAS
FACULDADE DE ENGENHARIA MECÂNICA

DISSERTAÇÃO DE MESTRADO ACADÊMICO

Análise dos novos controles de segurança da informação evidenciados na ISO/IEC 27001:2022 com o uso do Método Fuzzy Dematel

Autor: Reginaldo da Silva Leme

Orientador: Prof. Dr. Jefferson de Souza Pinto

Coorientador: Prof. Dr. Rosley Anholon

A Banca Examinadora composta pelos membros abaixo aprovou esta Dissertação:

Prof. Dr. Jefferson de Souza Pinto, Presidente
DEMM/FEM/UNICAMP/Campinas/SP

Profa. Dra. Suzana Regina Moro
DEMM/FEM/UNICAMP/Campinas/SP

Prof. Dr. Lucas Veiga Ávila
CS/UFSM/Cachoeira do Sul/RS

A Ata de Defesa com as respectivas assinaturas dos membros encontra-se no SIGA/Sistema de Fluxo de Dissertação/Tese e na Secretaria do Programa da Unidade.

Campinas, 17 de fevereiro de 2025.

Dedicatória

Dedico este trabalho à minha esposa, Flávia, companheira em todas as horas, que me apoiou incondicionalmente e esteve sempre ao meu lado nos momentos mais desafiadores, compartilhando cada passo dessa jornada. O seu carinho, paciência, compreensão e suporte foram essenciais para que este momento se concretizasse. Sem o seu apoio, nada disso seria possível. À minha filha, Yasmin, que me ensina diariamente o verdadeiro significado do amor. Seu sorriso constante ilumina meus dias e me inspira a ser uma pessoa melhor, a buscar novos conhecimentos e a enfrentar desafios com coragem, determinação e alegria. Vocês são o meu porto seguro e a minha maior fonte de inspiração, amo vocês.

Agradecimentos

Primeiramente agradeço a Deus por me dar força, saúde e sabedoria ao longo dessa jornada, renovando minha fé nos momentos difíceis e fortalecendo minha determinação para alcançar este objetivo.

Ao meu orientador, Prof. Dr. Jefferson de Souza Pinto, externo minha mais profunda gratidão pela confiança, suporte, dedicação e orientação ao longo dessa jornada. Agradeço por cada conselho, palavra de incentivo e generosidade na condução deste trabalho, o que foi fundamental para a sua concretização. A forma como compartilha suas experiências e paixão pelo ensino inspira todos ao seu redor, e sou grato por ter tido a oportunidade de ser orientado por uma pessoa tão humana e comprometida com o crescimento intelectual de seus alunos.

Ao meu coorientador, Prof. Dr. Rosley Anholon, pela parceria e pelos ensinamentos que enriqueceram imensamente minha trajetória acadêmica. Sua coorientação precisa, aliada a uma imensa capacidade de inspirar e motivar, foi crucial para o meu desenvolvimento. A clareza com que transmite seu conhecimento, além de sua dedicação e paciência, são qualidades que sempre me impulsionaram a conquistar meus objetivos ao longo de toda essa jornada.

À Profa. Dra. Suzana Regina Moro e ao Prof. Dr. Lucas Veiga Ávila, que compuseram a banca e, com sua vasta experiência e conhecimento, forneceram valiosas contribuições que enriqueceram este estudo. Sua análise criteriosa e *feedback* construtivo não só aprimoraram o conteúdo apresentado, mas também contribuíram significativamente para o meu desenvolvimento acadêmico e profissional.

A minha esposa, Flávia, pelo apoio incondicional e pela paciência ao longo de toda essa jornada. Sua compreensão, amor e incentivo foram essenciais para que eu pudesse me dedicar a este estudo. Sou eternamente grato por tê-la ao meu lado.

A minha filha, Yasmin, que me ensina todos os dias o verdadeiro significado de persistência e alegria. Sua energia e entusiasmo me lembram constantemente da importância de seguir em frente, sempre com um sorriso no rosto. Este trabalho é, de alguma forma, um reflexo da minha dedicação a você e do meu desejo de ser um exemplo de esforço, persistência e superação.

A minha Mãe Lourdes e meu Pai Antonio (*in memoriam*), que sempre foram minha fonte de inspiração e força. Sua sabedoria, amor e dedicação ao longo dos anos desempenharam um papel essencial na minha formação. Sou eternamente grato por tudo que fizeram por mim.

Aos meus colegas que, com seu apoio e colaboração, contribuíram para o sucesso deste trabalho. O suporte mútuo e o compartilhamento de ideias foram fundamentais para meu crescimento acadêmico e pessoal. A parceria e amizade de todos foram essenciais para superar os desafios e tornar esta jornada mais leve e enriquecedora.

"A persistência é o caminho do êxito."

Charles Chaplin

Resumo

Em um mundo de constante evolução tecnológica, os crimes cibernéticos têm aumentado cada vez mais, surgindo novas ameaças a todo momento, o que coloca em risco os dados e informações de diversas organizações. Diante de tal cenário, é de suma importância que as organizações implementem um Sistema de Gestão de Segurança da Informação para garantir que as ações de salvaguarda sejam tomadas, assegurando que as informações e dados permaneçam seguros e protegidos. Nesse sentido, a ISO/IEC 27001 provê um modelo para estabelecer, implementar, manter e melhorar continuamente um Sistema de Gestão de Segurança da Informação. A referida norma possui em seu Anexo A um conjunto de medidas de segurança intituladas controles, os quais abarcam práticas que devem ser adotadas pelas organizações com o objetivo de proteger suas informações contra ameaças e garantir a confidencialidade, a integridade e a disponibilidade dos dados. Em 2022, a ISO/IEC 27001 passou por uma revisão na qual 11 novos controles de segurança da informação foram evidenciados. Isto posto, o objetivo deste trabalho foi avaliar esses novos controles e identificar as relações de causa e efeito e o nível de influência entre cada um deles. Para alcançar esse objetivo, foi conduzida uma pesquisa de natureza exploratória, em que foi realizada uma *survey* com vinte e dois especialistas, todos Diretores de Tecnologia de empresas brasileiras. Com base nas respostas adquiridas, foi aplicado o método multicritério *Fuzzy Dematel*, a fim de analisar a causa e efeito e o nível de influência entre esses novos controles. Como resultados, foram identificadas essas relações e influências entre cada um deles, o que foi explicitado por meio do Diagrama Causal e o Mapa de Relações de Influência. A análise permitiu identificar os controles centrais, os quais pertencem ao grupo de controles organizacionais, destacando a preocupação com a governança da segurança da informação no cenário atual. Esses controles abrangem aspectos estratégicos essenciais para a proteção e gestão eficaz dos riscos, impactando diretamente a estrutura e a eficácia do SGSI. Foram identificados ainda os controles direcionadores, os independentes e os de impacto, o que revela sua influência e prioridade dentro do sistema, facilitando sua integração, gerenciamento e manutenibilidade de forma estratégica junto ao SGSI. Destaca-se ainda que o estudo identificou e caracterizou a prioridade na alocação de recursos para cada controle dentro do sistema, o que provê *insights* estratégicos e fornece informações valiosas aos tomadores de decisão para sua incorporação e gerenciamento em seu Sistema de Gestão de Segurança da Informação. Assim, com base nos resultados alcançados, conclui-se que o estudo oferece um nível de detalhamento claro e conciso sobre as relações de causa e efeito e o nível de influência entre cada um dos novos controles de segurança da informação evidenciados pela ISO/IEC 27001:2022, tratando-se de um estudo inovador realizado no Brasil nesse período.

Palavras Chave: Segurança da Informação, Sistema de Gestão de Segurança da Informação, ISO/IEC 27001:2022, Gerenciamento de Risco, *Fuzzy* Dematel.

Abstract

In a world of constant technological evolution, cybercrimes have been increasing, with new threats emerging at every moment, putting the data and information of various organizations at risk. Given this scenario, it is of utmost importance that organizations implement an Information Security Management System to ensure that safeguarding actions are taken, guaranteeing that information and data remain secure and protected. In this regard, ISO/IEC 27001 provides a model for establishing, implementing, maintaining, and continuously improving an Information Security Management System. This standard includes in its Annex A a set of security measures called controls, which encompass practices that organizations must adopt to protect their information against threats and ensure the confidentiality, integrity, and availability of data. In 2022, ISO/IEC 27001 underwent a revision in which 11 new information security controls were introduced. Therefore, the objective of this study was to evaluate these new controls and identify the cause-and-effect relationships and the level of influence among them. To achieve this objective, an exploratory study was conducted, involving a survey with twenty-two experts, all Technology Directors from Brazilian companies. Based on the collected responses, the Fuzzy Dematel multi-criteria method was applied to analyze the cause-and-effect relationships and the level of influence among these new controls. As a result, these relationships and influences were identified and explicitly represented through the Causal Diagram and the Influence Relationship Map. The analysis allowed the identification of central controls, which belong to the group of organizational controls, highlighting the concern with information security governance in the current scenario. These controls encompass essential strategic aspects for risk protection and effective management, directly impacting the structure and effectiveness of the ISMS. Additionally, guiding, independent, and impact controls were identified, revealing their influence and priority within the system, facilitating their strategic integration, management, and maintainability within the ISMS. The study also identified and characterized the priority of resource allocation for each control within the system, providing strategic insights and valuable information to decision-makers for their incorporation and management within their Information Security Management System. Thus, based on the achieved results, it is concluded that the study offers a clear and concise level of detail regarding the cause-and-effect relationships and the level of influence among each of the new information security controls introduced by ISO/IEC 27001:2022, constituting an innovative study conducted in Brazil during this period.

Key Word: Information Security, Information Security Management System, ISO/IEC 27001:2022, Risk Management, Fuzzy DEMATEL.

Lista de Figuras

Figura 3.1: Etapas do procedimento metodológico.....34
Figura 3.2: Passos para aplicação do Método Fuzzy DEMATEL.....40
Figura 3.3: Números fuzzy triangular para as variáveis linguísticas.....41
Figura 4.1: Diagrama Causal e seus Quadrantes.....51
Figura 4.2: Mapa Relacional de Influência.....54

Lista de Tabelas

Tabela 3.1: Avaliação linguística para o critério C1 – Inteligência de ameaças.....41
Tabela 3.2: Números *fuzzy* triangular correspondente a avaliação linguística do fator C1.....43
Tabela 3.3: Matriz de relações agregada por meio da Média Simples.....44
Tabela 3.4: Matriz Z desfuzzyficada 45
Tabela 3.5: Cálculo do valor máximo da Matriz Z.....46
Tabela 3.6: Matriz X normalizada.....46
Tabela 3.7: Matriz Identidade.....47
Tabela 3.8: Matriz de influência total T.....47
Tabela 3.9: Matriz T com os cálculos dos vetores R e C.....47
Tabela 4.1: Valores de R+C e R-C calculados.....49
Tabela 4.2: Influência dos critérios em relação à média da Matriz T.....54

Lista de Quadros

Quadro 2.1: Novos controles de segurança da informação da ISO/IEC 27001:2022.....24
Quadro 3.1: Classificação da pesquisa do trabalho.....34
Quadro 3.2: Fatores de Influência dos novos controles de segurança da informação da ISO/IEC 27001:2022.....35
Quadro 3.3: Perfil dos respondentes da pesquisa.....38
Quadro 3.4: Termos linguísticos e números triangular *fuzzy*.....41

Lista de Equações

Equação 3.1: Cálculo para agregação da Matriz Z.....44
Equação 3.2: Cálculo para obter a Matriz Z desfuzzyficada.....45
Equação 3.3: Cálculo para obter o valor máximo da Matriz Z.....45
Equação 3.4: Cálculo para obter a Matriz X normalizada.....46
Equação 3.5: Cálculo para obter a Matriz X normalizada.....46
Equação 3.6: Cálculo para obter os vetores *R* e *C*.....47
Equação 4.1: Cálculo para obter a média da Matriz T.....53

Lista de Siglas e Nomenclaturas

ABNT	Associação Brasileira de Normas Técnicas
AHP	*Analytic Hierarchy Process*
APA	*American Psychological Association*
BS	*British Standard*
CAAE	Certificado de Apresentação para Apreciação Ética
CCTV	*Closed-Circuit Television*
CEP	Comitê de Ética em Pesquisa
COA	*Center of Area*
CTO	*Chief Technology Officer*
DC	Diagrama Causal
DEMATEL	*Decision making trial and evaluation laboratory*
DLP	*Data Leakage Prevention*
IDS	*Intrusion Detection System*
ISO	*International Organization for Standardization*
LGPD	Lei Geral de Proteção de Dados
MRI	Mapa de Relação e Influência
NBR	Norma Brasileira Registrada
QP	Questão de Pesquisa
RGPD	Regulamento Geral de Proteção de Dados
SGSI	Sistema de Gestão de Segurança da Informação
TCLE	Termo de Consentimento Livre e Esclarecido
TI	Tecnologia da Informação
TIC	Tecnologia da Informação e Comunicação
UEBA	*User and Entity Behavior Analytic*

Sumário

1 INTRODUÇÃO 17
1.1 Contexto e Justificativa 17
1.2 Problema de Pesquisa 19
1.3 Objetivo Geral 19
1.4 Objetivos Específicos 19
1.5 Originalidade e Relevância 20
1.6 Apresentação da Estrutura do Trabalho 20
2 FUNDAMENTAÇÃO TEÓRICA 21
2.1 Sistema de Gestão da Segurança da Informação (SGSI) 21
2.2 ISO/IEC 27000, 27001 e 27002 22
2.3 Novos controles de segurança da informação 25
2.3.1 Inteligência de Ameaças 26
2.3.2 Segurança da informação para o uso de serviços em nuvem 26
2.3.3 Prontidão de TIC para a continuidade de negócios 27
2.3.4 Monitoramento de segurança física 27
2.3.5 Gestão de configuração 28
2.3.6 Descarte ou exclusão de informações 28
2.3.7 Mascaramento de Dados 28
2.3.8 Prevenção de vazamento de dados 29
2.3.9 Atividades de monitoramento 29
2.3.10 Filtragem da Web 30
2.3.11 Desenvolvimento Seguro 30
2.4 Breve resumo do Capítulo 31
3 PROCEDIMENTOS METODOLÓGICOS 32
3.1 Caracterização da Pesquisa 32
3.2 Procedimentos Metodológicos 34
3.2.1 Etapa 1 – Análise sobre as alterações da norma ISO/IEC 27001 – Variáveis, lacuna e objetivos 34
3.2.2 Etapa 2 – Estruturação da pesquisa – Protocolo e coleta de dados 36
3.2.3 Coleta de dados – Pesquisa com especialistas 37
3.2.4. Etapa 4 – Análise de dados – aplicação do Método *Fuzzy* Dematel 39
3.3 Resumo do Capítulo 48
4 APRESENTAÇÃO E DISCUSSÃO DOS RESULTADOS 49
4.1 Relação e Proeminência 49
4.1.1. Controles de causa 50
4.1.2. Controles de efeito 50
4.2. Diagrama Relacional Causal 51
4.3. Mapa Relacional de Influência 53
4.4. Discussões 55

5 CONCLUSÕES E CONSIDERAÇÕES FINAIS.....59
5.1 Conclusões.....59
5.2 Considerações Finais.....60
5.3 Limitações da Pesquisa.....61
5.4 Propostas de Trabalhos Futuros.....61
REFERÊNCIAS 63
APÊNDICE A - QUESTIONÁRIO DA PESQUISA.....66
ANEXO A - RESULTADOS DA AVALIAÇÃO LINGUÍSTICA DOS CRITÉRIOS 80
ANEXO B - NÚMEROS *FUZZY* TRIANGULAR CORRESPONDENTES AS AVALIAÇÕES LINGUÍSTICAS 84
ANEXO C - AUTORIZAÇÃO DO COMITÊ DE ÉTICA EM PESQUISA.....89
ANEXO D – TERMO DE CONSENTIMENTO LIVRE E ESCLARECIDO (TCLE).....96
ANEXO E – COMPROVAÇÃO DE SUBMISSÃO EM PERIÓDICO 101
ANEXO F – ARTIGO SUBMETIDO.....102

1 INTRODUÇÃO

O capítulo apresenta o contexto e o problema de pesquisa, além de definir o objetivo geral e os objetivos específicos, destacando a originalidade e a relevância do estudo. Em seguida, são apresentados a caracterização da pesquisa, os procedimentos metodológicos adotados e a estrutura do trabalho.

1.1 Contexto e Justificativa

A proteção de dados e informações é uma decisão estratégica adotada pela organização (ISO, 2018), a qual visa garantir a continuidade dos negócios, assegurar a conformidade com requisitos legais e regulamentares, além de fortalecer a confiança de clientes e parceiros ao demonstrar um compromisso sólido com a segurança da informação. Apesar de parecer algo intangível, existem algumas formas de garantir que as organizações se protejam e gerenciem tais riscos. Uma delas é por meio do uso da norma ISO/IEC 27001, a qual fornece uma diretriz para operacionalização de um Sistemas de Gerenciamento de Segurança da Informação (SGSI).

A referida norma define um conjunto de controles de segurança da informação em seu Anexo A, os quais são agrupados em seções e possuem como função principal prover ferramentas para a garantia da proteção e a integridade das informações. Esses controles permitem, dentre outras aplicações, que as organizações realizem uma avaliação para determinar o nível de maturidade do seu SGSI, sua conformidade de domínio e o seu valor de risco básico (Legowo e Jhartoyo, 2022). Além disso, eles promovem maior previsibilidade e controle sobre os processos de segurança, essenciais para ambientes corporativos cada vez mais complexos.

Legowo e Jhartoyo (2022) investigaram a aplicação dos controles de segurança da ISO/IEC 27001 para avaliar a maturidade do SGSI em uma organização. Esses controles, utilizados como ferramentas de auditoria, identificaram lacunas nas práticas de segurança e orientaram ajustes estratégicos para fortalecer a proteção e garantir a continuidade do negócio.

Os resultados reforçaram a importância de uma avaliação sistemática e alinhada aos requisitos normativos para otimizar a gestão da segurança. Os autores concluíram que a adoção dos controles promove maior transparência nos processos e amplia a visão das práticas organizacionais, contribuindo para um modelo de gestão mais seguro e resiliente.

Topa e Karyda (2019) analisaram o impacto dos controles de segurança da informação na conformidade dos funcionários com as políticas de segurança em Provedores de Serviços de Internet. O estudo destacou que avaliar atitudes e práticas dos usuários finais é essencial para a eficácia das iniciativas de segurança, especialmente em organizações de serviços intensivos.

A aplicação dos controles permitiu implementar políticas mais eficazes, identificar lacunas comportamentais e desenvolver estratégias para aumentar a adesão às diretrizes organizacionais.

Os autores concluíram que essa abordagem fortalece a cultura de segurança, oferecendo diretrizes claras aos funcionários e mitigando riscos operacionais.

Ho *et al*. (2015) destacaram que os controles mais críticos para a segurança da informação incluem política de segurança, controle de acesso e segurança de recursos humanos. Utilizando o método *Fuzzy* DEMATEL, analisaram as relações de causa e efeito entre esses controles, permitindo a priorização eficiente de recursos e a redução de custos operacionais.

Os resultados demonstraram que a priorização estratégica desses controles reduz riscos e aprimora a segurança organizacional. A análise das interações permitiu direcionar recursos para os controles com maior impacto, fortalecendo a resiliência do SGSI.

Tariq *et al.* (2020) utilizaram o método *Fuzzy Analytic Hierarchy Process* (AHP) para priorizar controles de segurança em redes de sensores sem fio integradas à computação em nuvem. O estudo demonstrou que abordagens sistemáticas permitem identificar e implementar controles eficazes considerando requisitos organizacionais, orçamento e tempo de implementação.

Os resultados evidenciaram que a priorização estratégica fortalece a resiliência das redes e reduz riscos de ataques cibernéticos. O método *Fuzzy* AHP classificou os controles mais eficazes na mitigação de vulnerabilidades, otimizando recursos e alinhando estratégias de segurança às necessidades operacionais.

Khajouei, Kazemi e Moosavirad (2017) aplicaram o método *Fuzzy* AHP para priorizar controles de segurança da informação, destacando o gerenciamento de acesso como prioridade principal, enquanto a continuidade de negócios teve menor relevância. O estudo reforça a importância de abordagens sistemáticas na seleção de controles conforme o contexto organizacional.

Foram analisados controles como gerenciamento de acesso, continuidade de negócios e gestão de ativos em uma empresa do setor petrolífero. Os resultados indicaram que controles prioritários fortalecem áreas críticas, enquanto os de menor prioridade pode ser ajustados a restrições orçamentárias sem comprometer a eficácia do SGSI.

Boonkrong e Nuansomsri (2018) desenvolveram um modelo *Fuzzy* baseado em regras para avaliação de riscos conforme a ISO/IEC 27001:2013, abordando incertezas na gestão de riscos. A lógica fuzzy auxiliou na definição de estratégias mais assertivas para mitigar riscos em ambientes complexos.

O modelo utilizou controles da ISO/IEC 27001:2013 para construir uma matriz de risco que combinava variáveis qualitativas e quantitativas na priorização de controles. Os autores demonstraram que essa abordagem aumenta a confiabilidade do gerenciamento de riscos, permitindo decisões informadas e alinhadas às necessidades organizacionais.

Conforme exposto, diversas pesquisas tiveram como foco avaliar a aplicação dos controles de segurança da informação contidos no Anexo A da norma ISO/IEC 27001, demonstrando sua relevância para fortalecer a proteção de dados e mitigar riscos organizacionais, tratando-se de um tema de suma importância para o cenário de análise de risco da segurança da informação.

Em relação à estrutura desses controles, no ano de 2022, houve uma revisão em seu conteúdo, apresentando alterações significativas, em detrimento a versão publicada em 2013. Apesar de nenhum controle ter sido removido, 57 controles foram mesclados em 24; vinte e três foram renomeados; um controle foi dividido em dois; 35 foram mantidos inalterados na sua essência,

embora tenha ocorrido pequenas atualizações na sua redação ou clareza e 11 novos foram evidenciados.

Dentre as alterações descritas a que mais se destaca foi o surgimento de 11 novos controles que foram evidenciados na versão de 2022, os quais não eram contemplados em sua versão anterior. Esses novos controles não foram analisados em pesquisas anteriores, o que revelou se tratar de uma importante lacuna de pesquisa a ser explorada. Desta forma, o objetivo desse estudo foi avaliar as relações de causa e efeito e o nível de influência entre cada um desses novos controles, o que permitiu fornecer informações de suma importância para que os gestores integrem e gerenciem esses novos controles junto ao SGSI de suas organizações.

1.2 Problema de Pesquisa

A partir do contexto apresentado, este trabalho teve como premissa responder às seguintes Questões de Pesquisa (QP):

QP1: Quais são as relações de causa e efeito entre os 11 novos controles de segurança da informação no contexto do Sistema de Gestão de Segurança da Informação?

QP2: Qual o nível de influência entre esses 11 novos controles no contexto do Sistema de Gestão de Segurança da Informação?

1.3 Objetivo Geral

O trabalho tem por objetivo geral identificar e mapear, por meio de um estudo exploratório, as relações de causa e efeito e o nível de influência entre cada um dos 11 novos controles de segurança da informação evidenciados pela ISO/IEC 27001:2022.

1.4 Objetivos Específicos

Decorre do objetivo geral, os seguintes objetivos específicos:

a) Identificar os 11 novos controles de segurança da informação evidenciados pela ISO/IEC 27001:2022, avaliando sua definição, propósitos, orientações e outras informações em consonância com outras informações provenientes da ISO/IEC 27002:2022, definindo-os como variáveis para pesquisa;
b) Identificar a relação de causa e efeito entre cada um dos 11 novos controles de segurança da informação;
c) Identificar o nível de influência entre cada um dos 11 novos controles de segurança da informação.

1.5 Originalidade e Relevância

Este estudo se insere na linha de pesquisa de “Sistemas de Engenharia da Produção” na Faculdade de Engenharia Mecânica da Unicamp com temática de “Segurança da Informação e Gestão de Riscos” na área de Engenharia da Qualidade e Confiabilidade. A lacuna de pesquisa para o trabalho consiste na análise da relação de causa e efeito e o nível de influência entre cada um dos 11 novos controles de segurança da informação que foram evidenciados, o que permite obter uma relação estruturada dessas relações em um sistema complexo, fornecendo informações claras, concisas e precisas para uma tomada de decisão assertiva, frente a sua incorporação e gerenciamento no SGSI.

Com base no exposto, a principal contribuição e relevância desta pesquisa consiste em prover uma base sólida para auxiliar os gestores das organizações na incorporação desses novos controles junto ao seu SGSI, fornecendo uma visão estruturada sobre sua relação de causa e efeito e o nível de influência entre cada um deles, o que permite o direcionamento de recursos e esforços para controles de maior impacto sistêmico, otimizando o uso de tempo, equipe e orçamento, facilitando e operacionalizando sua integração e gerenciamento no SGSI.

1.6 Apresentação da Estrutura do Trabalho

A estrutura do trabalho abrange, além deste capítulo, cujo objetivo foi esclarecer as motivações e a relevância deste estudo por meio da contextualização, os seguintes capítulos:

Capítulo 2: Fundamentação teórica, com o propósito de abarcar o contexto sobre os Sistema de Gestão da Segurança da Informação e a família ISO/IEC 27000 que contempla a ISO/IEC 27001 e 27002;

Capítulo 3 – Classificação e procedimentos metodológicos da pesquisa;

Capítulo 4 – Discussão dos resultados obtidos;

Capítulo 5 – Conclusões do trabalho, considerações finais, limitações e recomendações para trabalhos futuros.

Ao final, encontram-se as referências utilizadas, apêndice e anexos.

2 FUNDAMENTAÇÃO TEÓRICA

Este capítulo apresenta a base conceitual necessária para a compreensão do estudo, abordando os principais aspectos relacionados à segurança da informação e à gestão de riscos no contexto organizacional. Inicialmente, discute-se o Sistema de Gestão da Segurança da Informação, destacando sua importância para a proteção de dados e a mitigação de ameaças.

Em seguida, são exploradas as normas ISO/IEC 27000, 27001 e 27002, que estabelecem diretrizes e boas práticas para a implementação e aprimoramento de um sistema de gestão da segurança da informação. Por fim, são detalhados os novos controles de segurança introduzidos na ISO/IEC 27001:2022, os quais abrangem medidas essenciais para mitigar riscos emergentes, fortalecer a resiliência cibernética e garantir a proteção de dados em ambientes corporativos e digitais, alinhando-se às necessidades de segurança da informação diante das novas ameaças tecnológicas.

2.1 Sistema de Gestão da Segurança da Informação (SGSI)

Um Sistema de Gestão da Segurança da Informação abarca políticas, procedimentos, diretrizes e recursos e atividades associadas, as quais são gerenciadas coletivamente para se atingir os objetivos do negócio da organização (ISO, 2018).

Sua estrutura se baseia numa avaliação de riscos e nos seus níveis de aceitação junto às organizações, os quais são avaliados por meio de controles apropriados que garantem a proteção desses ativos, tratando-se de uma decisão estratégica para uma organização (ISO, 2018).

A implementação de um SGSI exige uma abordagem integrada, onde cada aspecto organizacional deve ser analisado para identificar vulnerabilidades e implementar mecanismos que minimizem riscos. De acordo com Chagas e Rodrigues (2025), a implementação de um SGSI alinhado à norma ISO/IEC 27001 é fundamental para garantir que as iniciativas de segurança estejam em sintonia com os objetivos estratégicos da organização. Este alinhamento assegura que as medidas de segurança reforcem o desempenho organizacional, em vez de atuarem como obstáculos. A ISO/IEC 27001 oferece uma estrutura metodológica robusta para o estabelecimento, operação, monitoramento e melhoria contínua do sistema, facilitando essa integração.

Ademais, um dos principais pilares de um SGSI é a gestão de riscos. Este processo não se limita apenas à identificação de ameaças externas, mas também inclui a análise de fatores internos, como o comportamento dos colaboradores e a adequação das políticas organizacionais (Hannigan *et al*., 2019). A análise de riscos permite priorizar investimentos e recursos para proteção das informações mais críticas, reduzindo a probabilidade de incidentes e seus impactos.

A gestão de riscos se torna ainda mais desafiadora em um ambiente em constante evolução tecnológica, onde novas ameaças e vulnerabilidades surgem rapidamente. Ao mesmo tempo, a implementação de um SGSI promove maior confiança entre os *stakeholders* internos e externos,

uma vez que demonstra o compromisso da organização com a proteção de dados e a conformidade regulatória (Kitsios, Chatzidimitriou e Kamariotou, 2022).

Nesse sentido, Raković (2021) aponta que o sucesso do SGSI depende, em grande parte, de sua capacidade de se adaptar às demandas dos clientes e às exigências legais, em que se pode citar a Lei Geral de Proteção de Dados (LGPD) e o Regulamento Geral de Proteção de Dados (RGPD) como exemplo de requisitos legais a serem cumpridos. Assim, a manutenção de um SGSI eficaz requer esforços contínuos de monitoramento, auditoria e atualização dos controles implementados.

Outra vantagem significativa de um Sistema de Gestão de Segurança da Informação está relacionada à sua capacidade de aumentar a resiliência organizacional frente a ataques cibernéticos. Conforme evidenciado por Ferreira, Nunes e Santos (2020), organizações que adotam sistemas de gestão bem estruturados conseguem não apenas evitar incidentes, mas também recuperar-se de forma mais rápida e eficiente, minimizando prejuízos financeiros e danos à reputação.

Hannigan *et al*. (2019) reforçam que a resiliência cibernética se tornou um diferencial competitivo, principalmente em setores altamente regulados, como o financeiro e o de saúde.

Além disso, o SGSI auxilia na padronização de processos e na criação de uma cultura organizacional voltada para a segurança da informação. Siponen e Baskerville (2018) afirmam que a conscientização dos colaboradores é um dos fatores mais críticos para o sucesso do sistema, visto que as ameaças internas, muitas vezes não intencionais, representam uma parcela significativa dos incidentes de segurança. Nesse contexto, programas de treinamento regulares e campanhas de conscientização são indispensáveis para garantir que todos os membros da organização compreendam seu papel na proteção dos ativos de informação.

Com a evolução tecnológica e o aumento da complexidade das ameaças cibernéticas no cenário de segurança da informação, é extremamente necessário que o SGSI seja continuamente aprimorado para acompanhar as transformações do ambiente digital. Segundo Kitsios, Chatzidimitriou e Kamariotou (2023), a adoção de tecnologias emergentes, como inteligência artificial e blockchain, pode complementar as estratégias tradicionais de segurança, oferecendo soluções mais robustas e escaláveis. Além disso, a revisão periódica do SGSI é necessária para que se identifique lacunas e oportunidades de melhoria, garantindo sua eficácia ao longo do tempo.

Desta forma, a implementação e manutenção de um SGSI não se limita à aplicação de controles técnicos, mas envolvem uma abordagem estratégica integrada que alia gestão de riscos, conformidade regulatória, conscientização organizacional e adoção de tecnologias emergentes.

Somente por meio de esforços contínuos de monitoramento, adaptação e aprimoramento, é possível garantir que o SGSI acompanhe a evolução tecnológica, atendendo às demandas do mercado e protegendo os ativos de informação de maneira eficaz.

2.2 ISO/IEC 27000, 27001 e 27002

A norma ISO/IEC 27000 teve como fonte de origem o Padrão Britânico (*British Standard*) BS 7799ª, que foi publicado em 1995, o qual foi escrito pelo Departamento de Indústria e Comércio

do Governo do Reino Unido, e abordava, na sua primeira parte, as melhores práticas para o Gerenciamento de Segurança da Informação (Calder e Watkins, 2005).

Sua estrutura fornece uma introdução e visão geral sobre a família ISO/IEC 27000, com definições e vocabulários claros sobre o SGSI, a qual traz em seu arcabouço as normas ISO/IEC 27001 e ISO/IEC 27002, dentre outras.

A família de normas ISO/IEC 27000 é amplamente reconhecida como uma referência global para a segurança da informação, fornecendo diretrizes específicas para a implementação, operação e manutenção de um Sistema de Gestão da Segurança da Informação. Além disso, essa norma desempenha um papel fundamental ao alinhar as práticas de segurança com as necessidades organizacionais e os requisitos regulatórios, promovendo uma abordagem integrada e coerente.

De acordo com Calder e Watkins (2005), a norma não apenas estabelece os fundamentos do SGSI, mas também facilita a harmonização das práticas de segurança em diferentes indústrias, garantindo uma linguagem comum e compreensível globalmente.

Ademais, a norma ISO/IEC 27000 se destaca por fornecer uma base para a certificação das organizações que implementam um SGSI em conformidade com os requisitos da ISO/IEC 27001. Essa certificação representa um diferencial estratégico, demonstrando aos *stakeholders* o compromisso da organização com a proteção de dados e a conformidade regulatória.

A ISO/IEC 27000 tem por objetivo fornecer as definições e conceitos que fundamentam a gestão da segurança da informação, enquanto que a ISO/IEC 27001 estabelece os requisitos mínimos obrigatórios para um implementar um SGSI eficaz.

A ISO 27001 é o padrão mais conhecido do mundo para Sistemas de Gerenciamento de Segurança da Informação (ISO, 2022) e tem por objetivo mitigar os riscos relacionados à segurança cibernética. Publicada pela primeira vez em 2005, a referida norma passou por duas revisões, em que a primeira foi realizada no ano de 2013 e a última no ano de 2022, a qual apresentou mudanças expressivas em relação a sua versão anterior.

A primeira mudança ocorrida foi no título da referida norma, o qual passou a ser denominado “Segurança da Informação, Cibersegurança e Proteção da Privacidade - Sistemas de Gestão da Segurança da Informação – Requisitos”, se alinhando ao contido na ISO/IEC 27002:2022.

Além disso, novas cláusulas foram introduzidas em sua estrutura, com o fito de harmonizar o documento frente a outras normas de sistema de gestão, tal como a ISO/IEC 22301:2019.

Outra mudança expressiva foi no Anexo A da ISO/IEC 27001:2022, que traz o referencial de controles de segurança da informação. A sua estrutura foi consolidada de 14 áreas na versão de 2013 para 4 áreas principais na versão de 2022, que são: Controles Organizacionais, Controles de Pessoas, Controles Físicos e Controles Tecnológicos.

Outrossim, alguns desses controles foram fundidos entre si, vinte e três foram renomeados, cinquenta e sete mesclados em vinte e quatro, um controle dividido em dois e trinta e cinco mantidos em sua essência, embora possam ter sofrido pequenas atualizações na sua redação ou clareza e 11 novos foram evidenciados.

Os 23 controles renomeados tiveram seus títulos alterados para refletir melhor a sua aplicabilidade prática e alinhar-se às terminologias mais modernas e amplamente reconhecidas. Por exemplo, o controle relacionado à "gestão de senhas" foi revisado para abordar a "gestão de informações de autenticação", reconhecendo a diversidade de métodos de autenticação atualmente

disponíveis, como biometria e autenticação multifator. Essa mudança visa trazer clareza e ampliar o escopo de aplicação do controle.

Os 57 controles mesclados em 24 foram resultado de uma simplificação estrutural, com o objetivo de reduzir redundâncias e facilitar a implementação por organizações de diferentes tamanhos e segmentos. Por exemplo, os controles relacionados à "segurança de rede" e "segregação de redes" foram agrupados em um único controle abrangente que trata da gestão de redes de forma holística. Essa abordagem permite que as organizações implementem medidas de segurança mais integradas e eficazes.

A divisão de um controle em dois ocorreu para refletir necessidades distintas de aplicação. Um exemplo disso é o controle relacionado à gestão de incidentes, que agora abrange separadamente o planejamento e a resposta a incidentes, reconhecendo que essas atividades requerem abordagens específicas e recursos dedicados.

Os 35 controles mantidos em sua essência representam aspectos fundamentais de segurança da informação que continuam relevantes e inalterados em sua funcionalidade principal. Contudo, pequenas alterações foram feitas em sua redação para torná-los mais claros e objetivos, alinhando-se à evolução das boas práticas.

Quanto aos 11 novos controles evidenciados, estes foram dispostos em três dos quatro grupos de atuação mencionados, conforme Quadro 2.1.

Com a ocorrência dessas mudanças, os controles que antes eram 114 no total, passaram a ter 93 na versão atual, os quais se reestruturam em: Controles organizacionais, perfazendo (37) controles, Controle de Pessoas (8), Controles físicos (14) e Controles tecnológicos (34).

Quadro 2.1: Novos controles de segurança da informação da ISO/IEC 27001:2022.

Grupos	Controles
Organizacional	I) Inteligência de ameaças; II) Segurança da informação para o uso de serviços em nuvem; III) Prontidão de TIC para a continuidade de negócios.
Físico	I) Monitoramento de segurança física.
Tecnológicos	I) Gestão de configuração; II) Descarte ou exclusão de informações; III) Mascaramento de dados; IV) Prevenção de vazamento de dados; V) Atividades de monitoramento; VI) Filtragem da *web*; VII) Desenvolvimento Seguro.

Fonte: Elaborado pelo autor (2025).

Em relação à ISO/IEC 27002:2022, sua estrutura tem como premissa o provimento de diretrizes sobre a implementação de controles genéricos de segurança da informação, incluindo orientação de implementação no contexto de um SGSI, baseado na ISO/IEC 27001:2022 (ISO, 2022a).

Alguns controles existentes na referida norma modificam o seu risco, enquanto que outros o mantêm (ISO, 2022a), como é o caso, por exemplo, de uma política de segurança. Os controles de segurança listados na Tabela A.1 do Anexo A da ISO/IEC 27001:2022 são diretamente derivados e alinhados com os listados na ISO/IEC 27002:2022, seções de 5 a 8, os quais devem ser utilizados em consonância com o subitem 6.1.3 da ISO/IEC 27001:2022.

Deste modo, a ISO/IEC 27002 se integra à ISO/IEC 27001, fornecendo uma estrutura para as melhores práticas internacionais em gestão da segurança da informação, além de prover dados para que um auditor externo possa examinar a implementação de um SGSI certificável (Calder e Watkins, 2008).

A relação entre a ISO/IEC 27002:2022 e a ISO/IEC 27001:2022 é de complementaridade direta. Enquanto a ISO/IEC 27001:2022 define os requisitos obrigatórios para um SGSI, incluindo o gerenciamento de riscos e a estrutura de controles, a ISO/IEC 27002:2022 fornece uma base detalhada para a implementação desses controles. Para exemplificar, a ISO/IEC 27001 exige que as organizações identifiquem e implementem controles para tratar riscos identificados, mas não detalha como fazê-lo. É a ISO/IEC 27002 que orienta a aplicação prática de cada controle, fornecendo explicações, objetivos e exemplos de como implementá-los no contexto de uma organização.

Outra característica essencial é que a ISO/IEC 27002:2022 reflete as mudanças introduzidas na ISO/IEC 27001:2022, como a estrutura revisada do Anexo A, que agora organiza os controles em quatro categorias principais. Essa reestruturação alinhou ambas as normas, garantindo que a aplicação dos controles siga uma lógica mais clara e prática. Assim, a ISO/IEC 27002 torna-se uma ferramenta indispensável para cumprir os requisitos de certificação da ISO/IEC 27001, oferecendo uma interpretação prática e detalhada dos controles definidos.

A ISO/IEC 27002:2022 também promove a adaptação dos controles às necessidades específicas das organizações, permitindo personalizações baseadas no tipo de negócio, porte e ambiente regulatório. Essa flexibilidade está alinhada à ISO/IEC 27001:2022, que incentiva um SGSI dinâmico, capaz de evoluir com as mudanças nos riscos e nas exigências legais. A conexão entre as duas normas não se limita ao conteúdo, mas também à forma como elas incentivam o uso de um ciclo contínuo de melhoria, onde os controles são revisados e otimizados para manter a eficácia diante de novas ameaças e tecnologias emergentes.

Em suma, a relação entre as normas reforça a importância de um gerenciamento de segurança da informação integrado e eficaz. A ISO/IEC 27001 estabelece a base para um SGSI certificado, enquanto a ISO/IEC 27002 atua como um guia técnico para garantir que as implementações atendam aos objetivos estratégicos e operacionais. Juntas, elas oferecem uma abordagem abrangente para proteger os ativos de informação, garantir a conformidade e aumentar a resiliência organizacional em um cenário de ameaças cada vez mais complexo.

2.3 Novos controles de segurança da informação

Conforme exposto, a versão de 2022 da ISO/IEC 27001 introduziu 11 novos controles de segurança da informação em seu Anexo A, os quais refletem a evolução das ameaças cibernéticas, tecnologias emergentes e práticas modernas de segurança da informação. Esses controles foram adicionados para atender às necessidades crescentes de proteção em áreas como computação em nuvem, inteligência de ameaças e privacidade.

Para proporcionar um entendimento mais claro sobre o conceito e a aplicação de cada controle de segurança, são apresentadas, a seguir, seus fundamentos, objetivos, orientações, conceitos e práticas, tomando por base a Norma Brasileira Registrada (NBR) ISO/IEC 27001 e 27002 versões 2022, que são as versões em português das ISO, as quais são fornecidas no Brasil pela Associação Brasileira de Normas Técnicas (ABNT).

2.3.1 Inteligência de Ameaças

A inteligência de ameaças consiste na coleta, análise e uso de informações sobre ameaças à segurança da informação, com o objetivo de compreender o ambiente de ameaças e adotar ações de mitigação eficazes (ISO, 2022a). Conforme seção 5.7, essa prática é organizada em três camadas: estratégica, com foco em tendências e mudanças gerais; tática, detalhando metodologias e ferramentas de atacantes; e operacional, fornecendo indicadores técnicos sobre ataques específicos. A norma destaca que a inteligência deve ser relevante, contextual e acionável, permitindo respostas rápidas e eficazes aos riscos identificados (ISO, 2022a).

De acordo com a seção 4.1 da ISO (2022), é imprescindível que as organizações integrem a gestão de ameaças à segurança da informação dentro do contexto de seus sistemas de gestão, considerando necessidades estratégicas e operacionais (ISO, 2022). As atividades incluem a definição de objetivos, a seleção de fontes confiáveis, a análise de dados e a comunicação clara dos resultados. Essa abordagem fortalece a capacidade de prevenção e resposta a incidentes, assegurando a proteção de ativos e a continuidade dos negócios em um ambiente de riscos em constante evolução.

2.3.2 Segurança da informação para o uso de serviços em nuvem

A segurança da informação no uso de serviços em nuvem requer que as organizações garantam que os riscos associados à contratação e utilização desses serviços sejam devidamente identificados e tratados. De acordo com a ISO (2022a), as organizações devem implementar controles específicos para proteger dados e serviços em nuvem, assegurando a confidencialidade, integridade e disponibilidade das informações armazenadas ou processadas nesses ambientes. A Seção 5.23 enfatiza que é essencial avaliar a segurança do provedor de serviços, estabelecer requisitos contratuais claros e monitorar continuamente os riscos e o desempenho (ISO,2022a).

A seção 6.1 da ISO (2022), ressalta que as organizações devem integrar a gestão de riscos de segurança da informação relacionados aos serviços em nuvem dentro do escopo do SGSI, alinhando-os às necessidades organizacionais e aos requisitos legais, regulatórios e contratuais (ISO,2022). As práticas incluem a verificação da conformidade do provedor com normas reconhecidas, a definição de políticas de acesso e proteção de dados, além de planos para gerenciar incidentes de segurança específicos para o ambiente em nuvem. Tais medidas fortalecem a

resiliência organizacional e garantem que os benefícios da computação em nuvem sejam aproveitados sem comprometer a segurança das informações.

2.3.3 Prontidão de TIC para a continuidade de negócios

A prontidão de tecnologia da informação e comunicação (TIC) para a continuidade de negócios busca assegurar que os serviços estejam preparados para manter a operação durante interrupções ou crises. Segundo a seção 5.30 da ISO (2022a), as organizações devem implementar medidas para garantir que os sistemas críticos de TIC sejam resilientes, incluindo planos de recuperação, redundância de recursos e testes periódicos. Essas medidas devem estar alinhadas com os objetivos de continuidade de negócios da organização, considerando os riscos e os impactos potenciais de falhas no ambiente operacional (ISO, 2022a).

De acordo com seção 8.3 da ISO (2022), é necessário que a continuidade dos serviços de TIC esteja integrada ao SGSI considerando tanto os riscos identificados quanto os requisitos regulatórios e contratuais. A norma reforça a importância de avaliar os requisitos de recuperação e estabelecer processos claros para resposta e restauração em caso de incidentes. Essa abordagem, que une planejamento, testes e aprimoramento contínuo, permite à organização garantir a disponibilidade de seus serviços críticos mesmo em cenários adversos (ISO, 2022).

2.3.4 Monitoramento de segurança física

O monitoramento de segurança física tem como objetivo garantir que os perímetros físicos e os ambientes sensíveis sejam protegidos contra acessos não autorizados ou ameaças físicas. De acordo com a seção 7.4 da ISO (2022a), as organizações devem implementar sistemas de monitoramento adequados, como circuitos de TV fechados (*Closed-Circuit Television* - CCTV), alarmes e sensores de movimento, para detectar atividades suspeitas em tempo real. Além disso, os registros gerados por esses sistemas devem ser revisados regularmente para identificar potenciais falhas de segurança e eventos suspeitos, garantindo que medidas corretivas possam ser tomadas prontamente (ISO, 2022a).

A ISO (2022) reforça que o monitoramento deve ser integrado à gestão de riscos e aos processos organizacionais, alinhando-se aos objetivos estratégicos de segurança da informação. A norma destaca a importância de estabelecer responsabilidades claras para a gestão e a revisão dos sistemas de monitoramento, bem como de garantir a conformidade com os requisitos legais e regulatórios aplicáveis. Essas medidas fortalecem a resiliência física e ajudam a proteger os ativos organizacionais contra ameaças externas e internas.

2.3.5 Gestão de configuração

A gestão de configuração tem como objetivo assegurar que os ativos de TIC sejam configurados e gerenciados de forma consistente para manter a segurança da informação. Segundo a Seção 8.9 da ISO (2022a), as organizações devem estabelecer e manter processos documentados para controlar as configurações de *hardware*, *software* e redes, garantindo que mudanças sejam realizadas de forma controlada e rastreável. Esse controle ajuda a evitar vulnerabilidades decorrentes de configurações inadequadas ou não autorizadas, promovendo a integridade e a estabilidade dos sistemas (ISO, 2022a).

A ISO (2022) reforça que a gestão de configuração deve estar alinhada ao SGSI, incorporando avaliações de risco e requisitos organizacionais. A norma destaca a importância de implementar controles que garantam que apenas configurações aprovadas sejam aplicadas e que as alterações sejam avaliadas quanto ao seu impacto na segurança. Essas práticas fortalecem a resiliência dos sistemas, minimizam o risco de interrupções operacionais e asseguram conformidade com requisitos legais e normativos aplicáveis.

2.3.6 Descarte ou exclusão de informações

O controle de descarte ou exclusão de informações visa garantir que dados sensíveis sejam removidos de maneira segura e irreversível ao final de seu ciclo de vida. De acordo com a seção 8.10 da ISO (2022a), as organizações devem implementar processos e ferramentas apropriados para excluir informações de forma que elas não possam ser recuperadas. Isso inclui o uso de métodos de exclusão segura para mídias digitais e a destruição física de mídias físicas, como papel e dispositivos de armazenamento, sempre alinhados às classificações de segurança da informação da organização (ABNT, 2022a).

Conforme a ISO (2022), o descarte de informações deve estar integrado ao SGSI, considerando riscos, requisitos legais e normativos, e necessidades contratuais. É essencial manter registros das exclusões realizadas e garantir que os processos atendam aos padrões de auditoria e conformidade. Essa abordagem reduz o risco de acesso não autorizado a informações descartadas, protegendo a confidencialidade e a integridade dos dados sensíveis.

2.3.7 Mascaramento de Dados

O mascaramento de dados é uma técnica de segurança utilizada para proteger informações sensíveis ao ocultar ou substituir seus valores reais por dados fictícios ou anonimizados. De acordo com a ISO (2022a), o objetivo do mascaramento de dados é limitar o acesso a informações

confidenciais, garantindo que apenas os dados necessários para a atividade em questão sejam acessados ou exibidos. A seção 8.11 enfatiza que essa prática é especialmente relevante em ambientes de desenvolvimento, testes ou análises, onde dados reais podem ser expostos a usuários não autorizados (ISO, 2022a).

A ISO (2022) reforça que o mascaramento de dados deve ser parte integrante do SGSI, considerando os riscos associados à exposição de informações sensíveis. A implementação dessa técnica deve ser planejada com base em critérios organizacionais e normativos, garantindo que os métodos utilizados preservem a integridade das operações e estejam em conformidade com os requisitos legais, regulatórios e contratuais. O mascaramento adequado ajuda a mitigar riscos de vazamento de dados e promove a proteção de informações críticas, mesmo em ambientes acessíveis a múltiplas partes.

2.3.8 Prevenção de vazamento de dados

A prevenção de vazamento de dados (*Data Leakage Prevention* - DLP) é um conjunto de práticas e tecnologias destinadas a proteger informações sensíveis contra acessos não autorizados, transmissão inadequada ou exposição acidental. De acordo com a ISO (2022a), as organizações devem implementar medidas técnicas e administrativas, como ferramentas de monitoramento e bloqueio de transferência de dados, além de políticas de uso aceitável. A seção 8.12 da ISO (2022a) pontua que essas práticas ajudam a identificar e prevenir o vazamento de informações confidenciais, assegurando a confidencialidade e a integridade dos dados corporativos.

A ISO (2022) destaca que a prevenção de vazamento de dados deve estar alinhada ao Sistema de Gestão de Segurança da Informação, considerando os riscos associados à manipulação e transferência de informações sensíveis. A norma também reforça a importância de educar os colaboradores sobre práticas seguras, implementar controles que monitorem o tráfego de dados em tempo real e realizar auditorias regulares para identificar possíveis falhas. Essa abordagem reduz os riscos de exposição acidental ou maliciosa de informações críticas, fortalecendo a resiliência organizacional e garantindo conformidade com requisitos legais e normativos.

2.3.9 Atividades de monitoramento

As atividades de monitoramento visam garantir a supervisão contínua de sistemas, redes e processos para detectar, registrar e responder a eventos de segurança em tempo hábil. De acordo com a ISO (2022a), as organizações devem implementar mecanismos de monitoramento proativos que permitam identificar atividades anômalas ou potenciais incidentes de segurança. Isso inclui o uso de ferramentas de registro e análise de logs, sistemas de detecção de intrusão (*Intrusion Detection System* - IDS) e monitoramento de comportamento de usuários e entidades (*User and*

Entity Behavior Analytics - UEBA). Conforme a seção 8.16 da ISO (2022ª), tais atividades devem estar alinhadas às necessidades de segurança organizacional e ser revisadas regularmente para assegurar sua eficácia.

A ISO (2022) reforça que o monitoramento deve ser uma prática contínua e integrada ao SGSI, permitindo uma visão abrangente dos riscos e ameaças. Além disso, a norma destaca a necessidade de estabelecer responsabilidades claras para a análise de eventos e o uso de tecnologias apropriadas para correlacionar dados e identificar padrões de ameaça. A implementação adequada dessas atividades fortalece a postura de segurança da organização, garantindo resposta eficiente a incidentes e conformidade com requisitos regulatórios e contratuais.

2.3.10 Filtragem da Web

A filtragem da web é um mecanismo de segurança projetado para controlar e restringir o acesso a recursos da internet com base em políticas organizacionais. Segundo a ISO (2022a), essa prática ajuda a prevenir acessos não autorizados ou inseguros a conteúdos e serviços na web que possam comprometer a segurança das informações ou o ambiente de Tecnologia da Informação (TI) da organização. A seção 8,23 da ISO (2022a) destaca que as organizações devem implementar ferramentas de filtragem que permitam bloquear ou monitorar atividades na web com base em categorias, reputação de sites, palavras-chave ou outros critérios, promovendo a proteção contra *malware* e atividades maliciosas.

De acordo com a ISO (2022), a filtragem da web deve ser integrada ao SGSI, alinhada às políticas de uso aceitável e aos requisitos de conformidade regulatória. A norma enfatiza a importância de equilibrar a proteção com a produtividade, garantindo que os controles de acesso não interfiram nas operações legítimas. Essa abordagem não apenas reduz o risco de exposição a ameaças cibernéticas, mas também contribui para a gestão de acessos apropriados, promovendo um ambiente de trabalho mais seguro e eficiente.

2.3.11 Desenvolvimento Seguro

O desenvolvimento seguro é um conjunto de práticas e controles destinados a integrar a segurança ao longo de todo o ciclo de vida de desenvolvimento de sistemas e aplicações. De acordo com a ISO (2022a), as organizações devem adotar princípios de segurança desde as etapas iniciais de design, garantindo que vulnerabilidades sejam identificadas e tratadas antes da implementação. Isso inclui o uso de métodos de codificação segura, ferramentas de análise estática e dinâmica de código e testes rigorosos de segurança. De acordo com a Seção 8.28 da ISO (2022a), tais práticas ajudam a reduzir riscos relacionados a falhas de *software* e a proteger os dados e sistemas organizacionais.

A ISO (2022) ressalta que o desenvolvimento seguro deve ser incorporado ao Sistema de Gestão de Segurança da Informação, alinhando-se aos requisitos organizacionais, legais e contratuais. A norma enfatiza a necessidade de estabelecer controles que promovam o treinamento de desenvolvedores em práticas seguras, bem como a implementação de processos formais para gerenciar mudanças e vulnerabilidades ao longo do desenvolvimento. Essa abordagem fortalece a resiliência das aplicações contra ataques cibernéticos e assegura que a segurança seja um componente central nas entregas de TI.

2.4 Breve resumo do Capítulo

O capítulo apresentou a fundamentação teórica sobre os pilares da segurança da informação e a gestão de riscos organizacionais. Inicialmente, a discussão sobre o SGSI enfatiza sua importância para a proteção de dados e a mitigação de ameaças, criando uma base sólida para a compreensão do tema. A exploração das normas ISO/IEC 27000, 27001 e 27002 reforça a necessidade de diretrizes estruturadas e boas práticas para a implementação de uma segurança eficaz, enquanto que a análise dos novos controles da ISO/IEC 27001:2022 evidencia a evolução das medidas de segurança, incorporando aspectos críticos importantes para a aplicação da nova versão da norma.

3 PROCEDIMENTOS METODOLÓGICOS

O capítulo aborda a classificação da pesquisa e detalha os procedimentos metodológicos adotados no estudo.

3.1 Caracterização da Pesquisa

Em relação à natureza da pesquisa, esta foi realizada de forma aplicada, uma vez que se buscou solucionar problemas práticos e específicos por meio de métodos direcionados, caracterizando-se como um estudo voltado para resultados concretos e úteis (Punch, 2016).

Por atuar sobre problemas práticos, a natureza aplicada pode conduzir a uma melhor compreensão do assunto estudado e, consequentemente, a descobertas de princípios científicos (Gil, 2002), o que é o objetivo do estudo, pois visa fornecer resultados diretamente utilizáveis para organizações em relação aos novos controles que foram evidenciados.

Segundo Creswell (2017), às pesquisas aplicadas são fundamentais para conectar o conhecimento acadêmico às necessidades reais das organizações, promovendo inovações que impactam positivamente os processos. Corroborando essa perspectiva, Lakatos e Marconi (2010) enfatizam que a pesquisa aplicada auxilia na transformação da teoria em prática, sendo essencial em contextos organizacionais para a resolução de problemas específicos.

Como objetivo de pesquisa, foi desenvolvido um estudo exploratório, o que é essencial para investigar campos relativamente novos e pouco explorados (Gil, 2008), como é o caso dos novos controles que foram introduzidos na ISO/IEC 27001:2022.

O caráter exploratório justifica-se pela necessidade de compreender melhor as interdependências e a importância relativa desses novos controles no contexto da segurança da informação, permitindo obter familiaridade com o problema e torná-lo mais explícito, para construir hipóteses acerca de seus resultados (Nascimento, 2016).

Segundo Yin (2015), a pesquisa exploratória é particularmente útil em estudos que envolvem tópicos emergentes, onde ainda não há consenso acadêmico ou modelos consolidados, pois fornece uma base inicial para futuras investigações mais aprofundadas. Complementando essa visão, Sampieri, Collado e Lucio (2013) destacam que esse tipo de pesquisa é um meio valioso para descobrir padrões e relacionamentos em áreas onde o conhecimento é escasso, contribuindo para a construção de bases teóricas mais sólidas.

Quanto ao método, esse estudo está pautado no processo amplo indutivo, vez que sua execução buscou analisar alguns fenômenos particulares, em que se estabelece uma conclusão geral sobre a temática apresentada (Gil, 2008). Os argumentos indutivos permitem levar a conclusões cujo conteúdo é mais amplo do que as premissas que os baseiam, em que, partindo desses dados, infere-se uma verdade geral ou universal (Marconi e Lakatos, 2017).

Segundo Bryman (2016), a abordagem indutiva é fundamental para a construção de teorias a partir de evidências empíricas, sendo amplamente utilizada em estudos exploratórios que visam desenvolver novas perspectivas teóricas. Complementarmente, Flick (2015) reforça que o método indutivo é indispensável em pesquisas qualitativas, permitindo a identificação de padrões e significados que emergem diretamente dos dados coletados.

A estratégia utilizada na pesquisa foi inicialmente uma revisão bibliográfica das normas ISO/IEC 27001 e 27002, com o fito de analisar sua estrutura, controles, objetivos e práticas sobre um Sistema de Gestão da Segurança da Informação.

A pesquisa bibliográfica é fundamental no desenvolvimento de pesquisas científicas, pois permite ao pesquisador compreender o estado atual do conhecimento em sua área de estudo, identificar lacunas e direcionar adequadamente sua investigação. Segundo Brito, Oliveira e Silva (2021), a pesquisa bibliográfica coloca o pesquisador em contato direto com toda a produção escrita sobre a temática estudada, sendo essencial para a fundamentação teórica e metodológica do trabalho científico.

Em seguida, após a identificação das informações necessárias para pesquisa, foi realizado um levantamento de dados via *survey,* em que o questionário foi aplicado por meio da ferramenta *Google Forms,* de forma online.

As pesquisas desse tipo têm por características a interrogação direta de pessoas acerca do problema estudado, com o objetivo de obter conclusões baseadas nos dados coletados (Creswell, 2017).

No estudo, o objetivo foi utilizar a *survey* para coletar as percepções de especialistas sobre o nível de influência de cada controle em relação aos demais, o que permite que se obtenha o conhecimento direto da realidade para a qual se procura uma resposta (Gil, 2008), com o propósito de descobrir novos fenômenos ou relação entre eles (Marconi e Lakatos, 2017).

A abordagem desta pesquisa foi qualitativa, a qual provê ao pesquisador o como (processo) e o porquê (significado) dos acontecimentos, a fim de atingir o entendimento profundo sobre uma situação (Cooper e Schindler, 2016).

A abordagem qualitativa se aplica em estudos que utilizaram a coleta de dados, a qual comumente é de natureza predominantemente qualitativa (Gil, 2008), o que é o caso do estudo em foco, o qual se vale de termos linguísticos para identificar as influências entre os controles que foram explicitados pela nova versão da norma ISO/IEC 27001:2022.

Em relação ao tempo da pesquisa, sua aplicação foi desenvolvida de forma transversal, visto estar pautada em um único momento do tempo em que houve a coleta de dados, a qual é útil quando se quer descrever variáveis e seus padrões de distribuição, indicando a prevalência de um fenômeno de interesse (Rouquayrol, 2018).

Segundo Setia (2016), o delineamento transversal é amplamente utilizado para analisar fenômenos em contextos específicos, sendo especialmente relevante para estudos que buscam identificar associações entre variáveis em um determinado momento. Complementarmente, Levin (2006) destaca que essa abordagem é eficaz para fornecer uma visão instantânea e detalhada de padrões e tendências sem a necessidade de acompanhamento longitudinal, tornando-a prática e acessível.

A seguir é apresentado o Quadro síntese sobre a classificação deste trabalho:

Quadro 3.1: Classificação da pesquisa do trabalho.

Pesquisa	Classificação
Natureza da pesquisa	Aplicada
Objetivo	Exploratório
Método Amplo	Indutivo
Estratégia	Pesquisa Bibliográfica
	Levantamento (*Survey*)
Abordagem	Qualitativa
Tempo (corte)	Transversal

Fonte: Elaborado pelo autor (2025).

3.2 Procedimentos Metodológicos

Este trabalho foi estruturado em quatro etapas, as quais são apresentadas no fluxo da pesquisa na Figura 3.1.

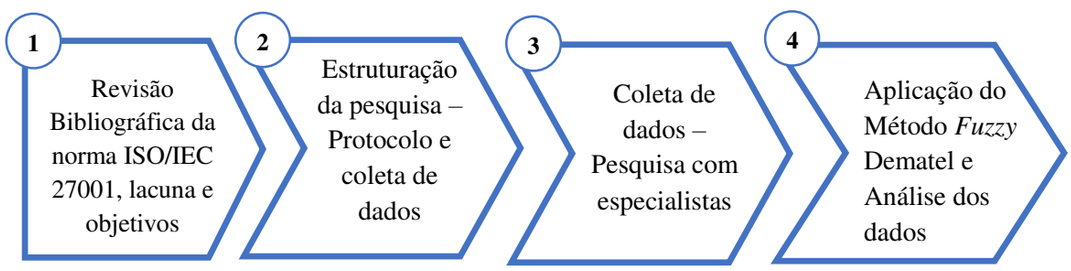


Figura 3.1: Etapas do procedimento metodológico.
Fonte: Elaborado pelo autor (2025).

As etapas descritas na figura 3.1 são apresentadas nas próximas seções.

3.2.1 Etapa 1 – Análise sobre as alterações da norma ISO/IEC 27001 – Variáveis, lacuna e objetivos

Tomando por base a norma ISO 27001:2022, foi realizada uma revisão bibliográfica, a fim de identificar as mudanças que ocorreram com o lançamento da sua nova versão. A primeira mudança constatada foi no título da referida norma, a qual passou a ser denominada “Segurança da Informação, Cibersegurança e Proteção da Privacidade – Sistemas de Gestão da Segurança da Informação – Requisitos”, se alinhando ao contido na ISO/IEC 27002:2022.

A segunda mudança observada foi a incorporação da cláusula 6.3 – Planejamento de Mudanças e novas exigências na cláusula 7.4 – Comunicação. A cláusula 8.1 – processos operacionais teve novos critérios estabelecidos, bem como, houve ainda a reestruturação e atualização de algumas terminologias.

A inclusão da cláusula 6.3, reforça a importância de um planejamento cuidadoso e detalhado para qualquer alteração no Sistema de Gestão de Segurança da Informação. Esse processo exige que as organizações considerem o impacto das mudanças em seus controles e processos existentes, alinhando as atualizações aos objetivos de segurança da informação e

mitigando potenciais riscos associados a alterações não planejadas. Com isso, busca-se garantir a continuidade operacional e o alinhamento estratégico das iniciativas de segurança.

Entretanto, a cláusula 7.4 foi expandida com novas exigências relacionadas à comunicação, destacando a necessidade de transmitir informações sobre segurança de maneira estruturada e eficiente. Isso inclui adaptar a comunicação ao público-alvo, sejam partes internas ou externas, e documentar adequadamente os processos para garantir clareza e rastreabilidade. Essas alterações visam melhorar a conscientização sobre a segurança da informação e assegurar que os objetivos organizacionais sejam comunicados de forma eficaz, promovendo alinhamento e engajamento entre as partes interessadas.

Quanto à cláusula 8.1, foram introduzidos novos critérios que priorizam a avaliação e o monitoramento contínuo das operações. Isso inclui a implementação de processos mais robustos para gerenciar riscos e assegurar a eficácia dos controles aplicados no dia a dia. Complementando essas mudanças, a atualização terminológica e a reorganização geral do texto das normas visam facilitar a interpretação e adoção dos requisitos, tornando-as mais acessíveis e práticas para organizações de diferentes portes e setores.

Outra mudança expressiva foi no Anexo A da ISO/IEC 27001:2022, que traz o referencial de controles de segurança da informação. A estrutura desses controles foi consolidada de 14 áreas na versão de 2013 para 4 áreas principais na versão de 2022.

Além disso, a quantidade total de controles foi reduzida de 114 para 93 e 11 novos controles foram evidenciados, os quais não eram contemplados na versão de 2013.

Uma vez identificado cada um dos 11 novos controles de segurança da informação, realizou-se uma análise sobre a definição, propósitos, orientações e outras informações de cada controle, para elaboração das variáveis a serem utilizadas na pesquisa.

Para atingir esse objetivo, recorreu-se ao conteúdo das normas ISO/IEC 27001 e ISO/IEC 27002, as quais serviram como base para a identificação de diretrizes e boas práticas voltadas à implementação dos controles de segurança da informação descritas no Anexo A da ISO/IEC 27001:2022.

A análise do conteúdo dessas normas, em especial seus conceitos e definições, propiciaram uma avaliação mais clara em relação ao significado de cada um dos novos controles evidenciados, fornecendo informações precisas sobre a aplicabilidade de cada um deles, chegando-se à definição dos fatores (variáveis) que foram utilizadas na pesquisa, conforme explicitado no Quadro 3.2.

Quadro 3.2: Fatores de Influência dos novos controles de segurança da informação da ISO/IEC 27001:2022.

Fator	Controle	Descrição
C1	Inteligência de Ameaça	Coleta e análise das informações relacionadas a ameaças à segurança da informação, produzindo inteligência de ameaças, para que ações de mitigação adequadas possam ser tomadas.
C2	Segurança da informação para o uso de serviços em nuvem	Especificação e gerenciamento da segurança da informação para uso de serviços em nuvem, avaliando processos de aquisição, uso, gestão e saída de serviços.
C3	Prontidão de TIC para a continuidade de negócios	Planejar, implementar, manter e testar a prontidão de TIC, com base nos objetivos de continuidade dos negócios, assegurando a disponibilidade das

		informações da organização e outros ativos associados durante a disrupção.
C4	Monitoramento de segurança física	Monitoramento contínuo das instalações para detectar e impedir o acesso físico não autorizado.
C5	Gestão de configuração	Configurações de segurança, hardware, software, serviços e redes, com o fito de que elas sejam estabelecidas, documentadas, implementadas, monitoradas e analisadas criticamente, para que não sejam modificadas por alterações não autorizadas ou incorretas.
C6	Atividades de monitoramento	Monitoramento de comportamentos anômalos e execução de ações apropriadas para avaliar possíveis incidentes de segurança da informação em redes, sistemas e aplicações.
C7	Prevenção de vazamento de dados	Detecção e prevenção da divulgação e extração não autorizadas de informações por indivíduos ou sistemas, prevenindo o vazamento de dados sejam por sistemas, redes, ou quaisquer outros dispositivos que tratam, armazenam ou transmitem informações sensíveis.
C8	Filtragem da web	Proteção dos sistemas para que não sejam comprometidos por *malware* e impedir o acesso a recursos da web não autorizados, reduzindo a exposição a conteúdos maliciosos.
C9	Desenvolvimento seguro	Escrita do software com segurança, abordando princípios de codificação segura ao desenvolvimento do software, para reduzir o número de potenciais vulnerabilidades de segurança da informação.
C10	Descarte ou exclusão de informações	Não exposição desnecessária de informações sensíveis, estando em *compliance* com requisitos legais, estatutários, regulamentares e contratuais, excluindo informações armazenadas em sistemas de informação, dispositivos ou qualquer outra mídia de armazenamento quando não forem mais necessárias.
C11	Mascaramento de dados	Mascaramento de dados para que seja usado de acordo com a política específica para o tema da organização, limitando a exposição de dados confidenciais, incluindo dados pessoais, cumprindo os requisitos legais, estatutários, regulamentares e contratuais.

Fonte: Elaborado pelo autor (2025) com base nas Normas ISO/IEC 27001:2022 e ISO/IEC 27002:2022.

3.2.2 Etapa 2 – Estruturação da pesquisa – Protocolo e coleta de dados

Neste passo foi delineada a construção do instrumento de pesquisa e obtenção de autorização para levantamento de dados via *survey*. Conforme exposto na etapa 1, as variáveis utilizadas neste estudo são oriundas do Anexo A da ISO/IEC 27001:2022, em conjunto com as informações delineadas na ISO/IEC 27001:2022, nos termos do que foi elencado no Quadro 3.2.

Com base nestas variáveis foi elaborado um questionário, conforme Apêndice A. O questionário é composto inicialmente por uma descrição do tema de pesquisa, *link* para acesso ao Termo de Consentimento Livre e Esclarecido (TCLE), conforme Anexo D, número do Certificado de Apresentação para Apreciação Ética (CAAE) e nome dos responsáveis pela pesquisa. Em seguida consta o campo para o aceite dos participantes em colaborar com a pesquisa, de acordo com as especificações descritas no TCLE.

Por conseguinte, são apresentadas 14 perguntas estruturadas, onde as três primeiras são destinadas à caracterização da amostra, sendo elas: nome, experiência profissional em anos e contato da rede social do *LinkedIn.*

As 11 perguntas subsequentes são relacionadas ao objeto de pesquisa e foram estruturadas com base no método *Fuzzy* DEMATEL. Para isso, ele foi composto por 11 perguntas subsequentes, cada uma direcionada a avaliar o nível de influência que um fator exerce sobre os demais, utilizando uma abordagem de comparações em pares (Lin e Wu, 2008). Esse formato permite uma análise detalhada das relações entre os fatores, considerando não apenas a presença, mas também a intensidade da influência.

A fim de garantir consistência e precisão na coleta dos dados, o critério "influência" foi representado por termos linguísticos que traduzem diferentes graus de intensidade. Os especialistas avaliaram cada relação com base nos seguintes níveis: Nulo, Baixíssima, Baixa, Média, Alta e Altíssima.

Esses termos foram escolhidos por sua clareza e facilidade de interpretação, permitindo que os participantes atribuíssem valores qualitativos de maneira intuitiva, enquanto o método *Fuzzy* converte essas avaliações em valores numéricos para posterior análise.

3.2.3 Coleta de dados – Pesquisa com especialistas

Na etapa 3, com a construção do questionário descrito na seção 3.2.2, foram seguidas as orientações para obtenção de autorização para a coleta de dados, a qual foi aprovada com a atribuição do CAAE sob o código 74829723.3.0000.5404, emitido pelo Comitê de Ética em Pesquisa (CEP) da Universidade de Campinas (UNICAMP), conforme Anexo C.

Para determinar o nível de influência entre os fatores de análise, foi definido como grupo de especialistas qualificados para responderem a pesquisa os Diretores de Tecnologia, também conhecidos como *Chief Technology Officer (CTO)* de empresas brasileiras de tecnologia, os quais possuem uma visão estratégica e abrangente do panorama tecnológico da organização, além de uma ampla experiência em gerenciar e implementar soluções tecnológicas complexas, o que os torna aptos a fornecer contribuições precisas, claras e relevantes para o estudo.

Neste contexto, a amostra composta por tais profissionais, compõem-se de Diretores de Tecnologia, os quais desempenham um papel fundamental na definição e execução da estratégia tecnológica das organizações, possuindo um conhecimento aprofundado sobre infraestrutura, inovação e tendências emergentes no setor. Com formação acadêmica robusta, em áreas como Ciência da Computação, Engenharia de Software ou Sistemas de Informação, esses profissionais também acumulam experiência prática na liderança de equipes de desenvolvimento e na gestão de projetos de tecnologia de ponta. Além disso, sua atuação envolve a avaliação e implementação de arquiteturas escaláveis e seguras, garantindo que os sistemas da empresa operem de maneira eficiente e resiliente diante dos desafios tecnológicos.

Complementarmente, o perfil dos profissionais da amostra, além das competências técnicas, os Diretores de Tecnologia também possuem um entendimento aprofundado sobre governança e

conformidade digital, o que os capacita a tomar decisões alinhadas com padrões regulatórios e boas práticas de mercado. Sua atuação exige a aplicação de *frameworks* de segurança da informação, como a ISO/IEC 27001, garantindo que os sistemas empresariais estejam protegidos contra ameaças cibernéticas. Esses profissionais lideram iniciativas de proteção de dados e prevenção de ataques, assegurando que as políticas internas e os protocolos de segurança sejam eficazes e continuamente aprimorados para mitigar riscos.

O conhecimento estratégico destes profissionais sobre segurança da informação também advém de sua responsabilidade na definição da cultura organizacional em relação à cibersegurança. Eles promovem treinamentos, implementam diretrizes de segurança e supervisionam auditorias internas para fortalecer a postura defensiva da empresa. Assim, sua expertise técnica e estratégica os qualifica como fontes confiáveis para análises das relações de influência entre os novos controles evidenciados pela norma.

Uma vez definido o perfil dos respondentes (especialistas), o questionário foi enviado via *Google Forms* individualmente para cada participante, entre dezembro de 2023 e maio de 2024, em que se obteve o total de 22 (vinte e duas) respostas.

O número de respondentes pode ser considerado expressivo, frente ao nível dos especialistas que contribuíram para o estudo, tratando-se de uma amostra que possui em média 25 anos de experiência, dentre os mais variados segmentos de mercado, conforme disposto no Quadro 3.3, além do contexto acadêmico brasileiro em relação ao óbice enfrentado na obtenção de dados via pesquisa.

Os respondentes que participaram da pesquisa possuem formação em Engenharia da Computação, Ciência da Computação, Tecnologia, Análise e Sistemas da Informação, Gestão Estratégica de Tecnologia e MBA Executivo, além de diversas certificações e licenças sobre os mais variados temas voltados a tecnologia como Gestão de TI, Processamento de Dados e Inteligência Artificial, dentre outros, o que demonstra o alto grau de conhecimento sobre a temática alvo do estudo, o que corrobora com a robustez dos dados que foram utilizados para análise dos novos controles evidenciados.

Quadro 3.3: Perfil dos respondentes da pesquisa.

Respondente	**Segmento de mercado**
1	Pesquisa em Energia e Materiais
2	Gestão de Segurança Pública e Privada
3	Química
4	Automação Comercial
5	Gestão de Inteligência de Crédito
6	Gestão de Segurança, *compliance* e produtividade
7	Arquitetura e Engenharia
8	Higiene e Limpeza
9	Soluções Tecnológicas
10	Instituição Financeira
11	Infraestrutura de TI
12	Tecnologia Industrial

13	Segurança Pública
14	Intercâmbio Cultural
15	Máquinas e Equipamentos Industriais
16	Consultorias especializadas
17	Hospedagem Inteligente
18	Soluções Tecnológicas
19	Produtos Digitais
20	Serviços Digitais
21	Restaurantes
22	Química Farmacêutica

Fonte: Elaborado pelo autor (2025).

Os dados obtidos após a aplicação do questionário formaram a base de dados para uma análise multicritério via método *Fuzzy* Dematel, apresentado na etapa 4.

3.2.4. Etapa 4 – Análise de dados – aplicação do Método *Fuzzy* Dematel

Na etapa 4, foi realizada a análise multicritério dos dados obtidos com o emprego do método *Fuzzy* Dematel. O Método *Decision making trial and evaluation laboratory* (DEMATEL) foi desenvolvida pelo Centro de Pesquisa de Genebra do *Battelle Memorial Institute* com o objetivo de se visualizar a estrutura das relações causais complexas por meio de matrizes ou dígrafos (Si *et al*., 2018).

Sua aplicabilidade é extremamente útil para análise da causa e efeito entre componentes de um sistema, além de apresentar um mapa que reflete as relações relativas entre eles, fornecendo informações para investigar e resolver problemas complexos interligados (Si *et al*., 2018).

Cabe salientar que o método Dematel clássico utiliza valores *crisp* para avaliar as relações dos fatores de decisão, todavia, em aplicações do mundo real, os julgamentos humanos são muitas vezes pouco claros (Si *et al*., 2018) e inadequados para estimar tais relações, por não refletirem a imprecisão do mundo real (Zadeh, 1965).

Como observado, ao utilizar dados sobre julgamento humanos, as preferências podem não ser claras, assim, é necessário que se utilize a lógica *Fuzzy*, a qual permite lidar com as questões de problemas relacionados a imprecisão (Chang, Yeh e Cheng, 1998) para que se obtenha resultados mais robustos e fidedignos para uma tomada de decisão assertiva.

Cabe ressaltar que o referido método é reconhecido e amplamente utilizado na literatura para a análise pretendida nesse estudo, em que se destaca, por exemplo, o estudo de Ho *et al*. (2015) que aplicou o *fuzzy* DEMATEL para identificar os controles considerados centrais para eficácia dos sistemas de segurança, tratando-se de um método muito eficiente para o objetivo proposto.

Com base no exposto, o método *Fuzzy* Dematel foi escolhido para ser aplicado no estudo, tomando por base a abordagem de Chien, Wu e Huang (2014), conforme Figura 3.2.

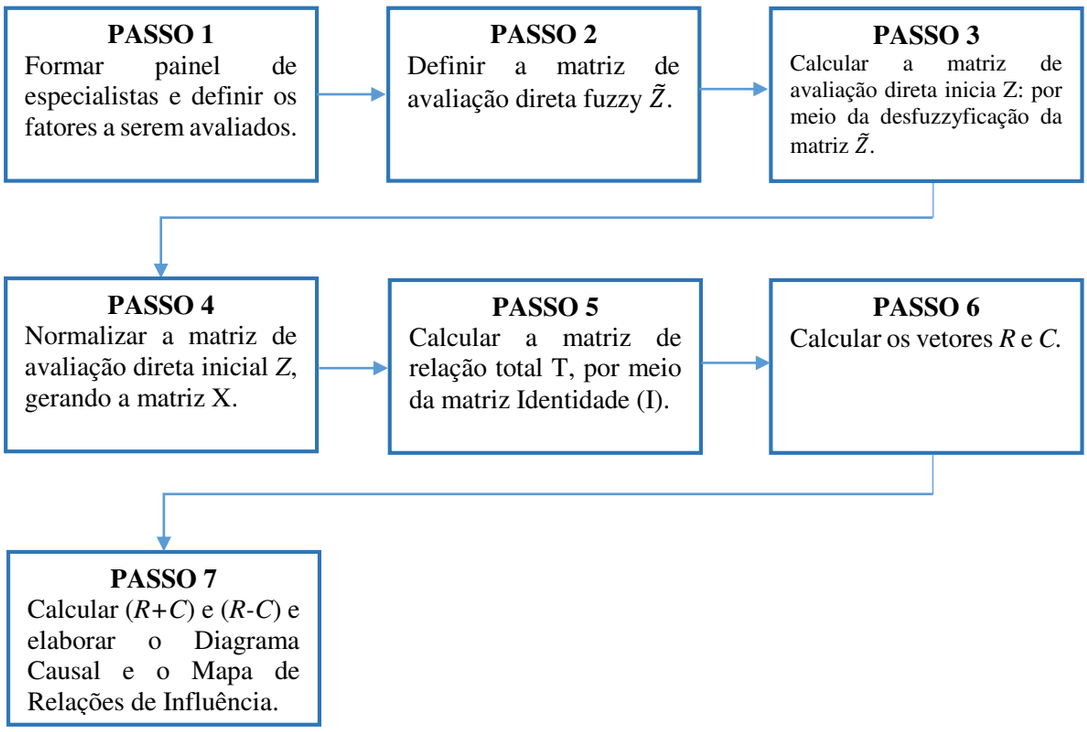


Figura 3.2: Passos para aplicação do Método *Fuzzy* DEMATEL.
Fonte: Elaborado pelo autor (2025).

A seguir os passos citados na Figura 3.2: são abordados para demonstrar todo o processo realizado:

Passo 1 – A definição dos especialistas é demonstrada na subseção 3.2.3 deste capítulo, tratando-se de Diretores de Tecnologia de organizações brasileiras. Quanto à definição dos fatores, essa ocorreu na subseção 3.2.2, após a revisão bibliográfica das normas ISO/IEC 27001 e 27002, em que se chegou a melhor definição para os fatores (Quadro 3.2) a serem avaliados pelos especialistas.

Passo 2 – Para definir a Matriz direta $\tilde{Z}$, é necessário realizar a avaliação das influências mútuas entre os fatores explicitados por cada um dos especialistas, tomando como base o uso da escala linguística definida.

Conforme disposto na subseção 3.2.2, os termos linguísticos utilizados para representar a variável influência foram: Nulo (N), Baixíssima (Z), Baixa (LI), Média (M), Alta (HI) e Altíssima (VH).

Com base nos termos linguísticos definidos foi construído a escala correspondente para os números *fuzzy,* conforme Figura 3.3. Neste estudo, utilizou-se os números triangulares *fuzzy*, os quais são comumente utilizados em estudos com o método Dematel (Si *et al*., 2018) onde cada termo é representado por três valores: o menor valor, o valor mais provável e o maior valor, podendo variar de 0 a 1 (Zadeh, 1965).

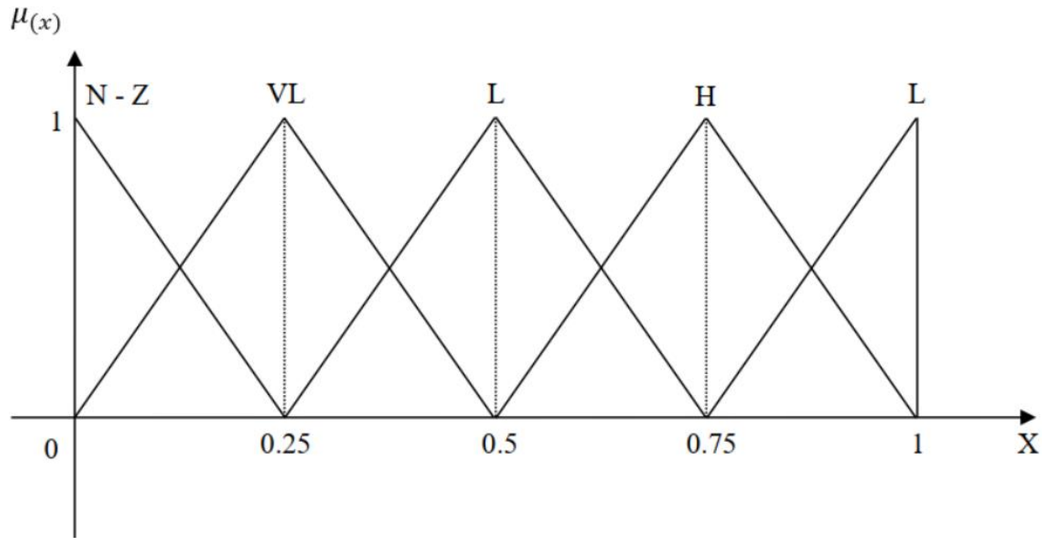


Figura 3.3: Números *fuzzy* triangular para as variáveis linguísticas.
Fonte: Elaborado pelo autor (2025).

▲

O Quadro 3.4 apresenta os termos linguísticos e seus números triangular *fuzzy* correspondentes, de acordo com o seu menor valor, mais provável e o maior valor.

Quadro 3.4: Termos linguísticos e números triangular *fuzzy*.

Termos Linguísticos	**Números triangular *fuzzy***
Altíssima (VH)	(0.75, 1, 1)
Alta (HI)	(0.5, 0.75, 1)
Média (M)	(0.25, 0.5, 0.75)
Baixa (LI)	(0, 0.25, 0.5)
Baixíssima (Z)	(0, 0, 0.25)
Nula (0)	(0, 0, 0.25)

Fonte: Elaborado pelo autor (2025).

Com os termos linguísticos definidos foi aplicado o questionário, conforme disposto na subseção 3.2.2, em que vinte e dois especialistas avaliaram as relações mútuas de influências entre cada par de critérios.

A partir desses dados coletados foi possível calcular a Matriz de influência direta individual $\tilde{Z}_k = [\tilde{Z}_{ij}^k]_{nxn}$ para cada um dos respondentes E = $\{E_{1,}E_{2,\ldots,}E_l\}$, em que $\tilde{Z}_{ij}^k = (\tilde{Z}_{ij1}^k, \tilde{Z}_{ij2}^k, \tilde{Z}_{ij3}^k)$ consiste na avaliação dos especialistas E_k, quanto ao grau de influência entre os fatores F_i e F_j (Si *et al*., 2018).

A Tabela 3.1 demonstra o resultado obtido para o Critério C1 – Inteligência de ameaças. Os demais resultados estão contidos no Anexo A.

Tabela 3.1: Avaliação linguística para o critério C1 – Inteligência de ameaças.

		C2	**C3**	**C4**	**C5**	**C6**	**C7**	**C8**	**C9**	**C10**	**C11**
		VH	VH	VH	VH	VH	VH	VH	VH	VH	VH
		HI	VH	VH	HI	VH	VH	VH	HI	VH	HI
		VH	VH	VH	VH	VH	VH	VH	VH	VH	VH
		HI	HI	VH	VH	VH	HI	HI	HI	HI	M
		HI	0	0	HI	0	0	M	HI	0	0
Z1	**C1**	VH	HI	VH	VH	HI	HI	VH	HI	M	LI
		VH	HI	HI	VH	HI	VH	VH	HI	HI	HI
		VH	VH	VH	VH	VH	VH	VH	VH	VH	VH
		M	LI	LI	M	HI	HI	HI	LI	Z	0
		VH	VH	VH	M	VH	HI	VH	M	Z	Z
		VH	HI	HI	VH	VH	HI	VH	M	M	M
		M	HI	M	HI	M	VH	HI	M	HI	HI

		VH	VH	HI	HI	VH	HI	HI	HI	HI	M
		HI	LI	LI	M	LI	LI	HI	M	M	HI
		HI	HI	VH	VH	HI	VH	VH	HI	VH	VH
		VH	VH	VH	VH	VH	VH	VH	VH	HI	HI
		VH	HI	VH	VH	VH	VH	VH	VH	HI	HI
		VH	HI	VH	HI	VH	VH	VH	VH	VH	VH
		VH	VH	0	VH	VH	VH	VH	VH	HI	M
		HI	HI	HI	VH	HI	HI	VH	VH	VH	HI
		HI	M	M	HI	HI	M	VH	M	LI	LI
		HI	VH	M	VH	M	VH	VH	VH	VH	VH

Fonte: Elaborado pelo autor (2025).

Em seguida, cada avaliação linguística foi substituída pelos seus números triangulares *fuzzy* correspondentes, a exemplo da Tabela 3.2, que traz os valores *fuzzy* relacionados ao C1 – Inteligência de ameaças. A substituição dos demais critérios são apresentadas no Anexo B.

Tabela 3.2: Números *fuzzy* triangular correspondentes a avaliação linguística do fator C1.

		C2			C3			C4			C5			C6			C7			C8			C9			C10			C11		
		l	**m**	**u**	**l**	**m**	**u**	**l**	**M**	**u**	**l**	**m**	**u**	**l**	**m**	**u**	**l**	**m**	**u**	**l**	**m**	**u**	**l**	**m**	**u**	**l**	**m**	**u**	**l**	**m**	**u**
		0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1
		0.5	0.75	1	0.75	1	1	0.75	1	1	0.5	0.75	1	0.75	1	1	0.75	1	1	0.75	1	1	0.5	0.75	1	0.75	1	1	0.5	0.75	1
		0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1
		0.5	0.75	1	0.5	0.75	1	0.75	1	1	0.75	1	1	0.75	1	1	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.25	0.5	0.75
		0.5	0.75	1	0	0	0.25	0	0	0.25	0.5	0.75	1	0	0	0.25	0	0	0.25	0.25	0.5	0.75	0.5	0.75	1	0	0	0.25	0	0	0.25
		0.75	1	1	0.5	0.75	1	0.75	1	1	0.75	1	1	0.5	0.75	1	0.5	0.75	1	0.75	1	1	0.5	0.75	1	0.25	0.5	0.75	0	0.25	0.5
		0.75	1	1	0.5	0.75	1	0.5	0.75	1	0.75	1	1	0.5	0.75	1	0.75	1	1	0.75	1	1	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1
		0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1
		0.25	0.5	0.75	0	0.25	0.5	0	0.25	0.5	0.25	0.5	0.75	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0	0.25	0.5	0	0	0.25	0	0	0.25
		0.75	1	1	0.75	1	1	0.75	1	1	0.25	0.5	0.75	0.75	1	1	0.5	0.75	1	0.75	1	1	0.25	0.5	0.75	0	0	0.25	0	0	0.25
Z1	**C1**	0.75	1	1	0.5	0.75	1	0.5	0.75	1	0.75	1	1	0.75	1	1	0.5	0.75	1	0.75	1	1	0.25	0.5	0.75	0.25	0.5	0.75	0.25	0.5	0.75
		0.25	0.5	0.75	0.5	0.75	1	0.25	0.5	0.75	0.5	0.75	1	0.25	0.5	0.75	0.75	1	1	0.5	0.75	1	0.25	0.5	0.75	0.5	0.75	1	0.5	0.75	1
		0.75	1	1	0.75	1	1	0.5	0.75	1	0.5	0.75	1	0.75	1	1	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.25	0.5	0.75
		0.5	0.75	1	0	0.25	0.5	0	0.25	0.5	0.25	0.5	0.75	0	0.25	0.5	0	0.25	0.5	0.5	0.75	1	0.25	0.5	0.75	0.25	0.5	0.75	0.5	0.75	1
		0.5	0.75	1	0.5	0.75	1	0.75	1	1	0.75	1	1	0.5	0.75	1	0.75	1	1	0.75	1	1	0.5	0.75	1	0.75	1	1	0.75	1	1
		0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.5	0.75	1	0.5	0.75	1
		0.75	1	1	0.5	0.75	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.5	0.75	1	0.5	0.75	1
		0.75	1	1	0.5	0.75	1	0.75	1	1	0.5	0.75	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1
		0.75	1	1	0.75	1	1	0	0	0.25	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.5	0.75	1	0.25	0.5	0.75
		0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.75	1	1	0.5	0.75	1	0.5	0.75	1	0.75	1	1	0.75	1	1	0.75	1	1	0.5	0.75	1
		0.5	0.75	1	0.25	0.5	0.75	0.25	0.5	0.75	0.5	0.75	1	0.5	0.75	1	0.25	0.5	0.75	0.75	1	1	0.25	0.5	0.75	0	0.25	0.5	0	0.25	0.5
		0.5	0.75	1	0.75	1	1	0.25	0.5	0.75	0.75	1	1	0.25	0.5	0.75	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1

Fonte: Elaborado pelo autor (2025).

Na sequência, foram agregadas as avaliações dos especialistas, por meio das Matrizes individuais $\tilde{Z}_k$ obtidas, tomando por base os números *fuzzy* correspondentes.

Nesse estudo a agregação se deu pela média simples (Si *et al*., 2018) entre cada um dos vértices, conforme Eq. 3.1, em que se obteve ao final a Matriz agregada, conforme Tabela 3.3.

$$\tilde{Z}_{ij} = \left(Z_{ij1}, Z_{ij2}, Z_{ij3}\right) = \frac{1}{l}\sum_{k=1}^{l} \tilde{z}_{ij}^{k} = \frac{1}{l}\sum_{k=1}^{l} \tilde{z}_{ij1}^{k}, \frac{1}{l}\sum_{k=1}^{l} \tilde{z}_{ij2}^{k}, \frac{1}{l}\sum_{k=1}^{l} \tilde{z}_{ij3}^{k} \tag{3.1}$$

Tabela 3.3: Matriz de relações agregada por meio da Média Simples.

	C1			**C2**			**C3**		
	L	**m**	**u**	**l**	**m**	**u**	**l**	**m**	**u**
C1	0.0000	0.0000	0.0000	0.6136	0.8636	0.9773	0.5227	0.7614	0.9091
C2	0.5568	0.7955	0.9091	0.0000	0.0000	0.0000	0.6250	0.8750	0.9886
C3	0.4886	0.7273	0.8864	0.5114	0.7500	0.8977	0.0000	0.0000	0.0000
C4	0.4432	0.6477	0.7841	0.4205	0.6136	0.7727	0.4318	0.6477	0.7955
C5	0.4318	0.6591	0.8295	0.5227	0.7614	0.9091	0.5795	0.8182	0.9318
C6	0.5682	0.8068	0.9091	0.5455	0.7841	0.8977	0.5227	0.7727	0.8864
C7	0.4545	0.6705	0.8409	0.5227	0.7500	0.8864	0.4205	0.6364	0.7955
C8	0.5455	0.7955	0.9091	0.5227	0.7500	0.8750	0.5114	0.7500	0.8750
C9	0.5114	0.7273	0.8295	0.5000	0.7273	0.8409	0.4773	0.6932	0.8182
C10	0.5000	0.7273	0.8636	0.5227	0.7614	0.9091	0.4545	0.6818	0.8409
C11	0.4205	0.6136	0.7727	0.5000	0.7273	0.8750	0.4091	0.6136	0.7955
	C4			**C5**			**C6**		
	l	**m**	**u**	**l**	**m**	**u**	**l**	**m**	**u**
C1	0.5000	0.7273	0.8523	0.6136	0.8636	0.9659	0.5682	0.8068	0.9205
C2	0.4886	0.7159	0.8636	0.5568	0.7955	0.9432	0.5227	0.7727	0.9205
C3	0.5227	0.7614	0.9205	0.5227	0.7727	0.9091	0.5909	0.8409	0.9659
C4	0.0000	0.0000	0.0000	0.4659	0.6932	0.8409	0.5227	0.7500	0.8523
C5	0.4886	0.6932	0.8182	0.0000	0.0000	0.0000	0.5568	0.7955	0.9205
C6	0.5000	0.7273	0.8636	0.5795	0.8295	0.9318	0.0000	0.0000	0.0000
C7	0.4659	0.6705	0.8068	0.5455	0.7727	0.8977	0.5682	0.7955	0.8977
C8	0.4545	0.6818	0.8523	0.5795	0.8295	0.9432	0.5568	0.8068	0.9091
C9	0.4432	0.6364	0.7955	0.5341	0.7727	0.8864	0.5000	0.7273	0.8636
C10	0.4091	0.6136	0.7841	0.4318	0.6591	0.8295	0.4886	0.7273	0.8636
C11	0.3523	0.5227	0.7045	0.3977	0.5909	0.7614	0.4091	0.6023	0.7500
	C7			**C8**			**C9**		
	l	**m**	**u**	**l**	**m**	**u**	**l**	**m**	**u**
C1	0.5795	0.8182	0.9318	0.6705	0.9205	0.9886	0.5227	0.7727	0.9205
C2	0.5682	0.8182	0.9659	0.5909	0.8295	0.9318	0.4318	0.6705	0.8523
C3	0.5227	0.7614	0.8977	0.5227	0.7500	0.9091	0.4545	0.6818	0.8523
C4	0.4659	0.6818	0.8182	0.5227	0.7500	0.8523	0.3182	0.5000	0.6818
C5	0.5455	0.7841	0.9091	0.5795	0.8182	0.9432	0.4432	0.6591	0.8295
C6	0.6023	0.8523	0.9318	0.5795	0.8295	0.9318	0.4545	0.6932	0.8523
C7	0.0000	0.0000	0.0000	0.5114	0.7273	0.8636	0.4318	0.6477	0.8068
C8	0.5227	0.7614	0.8750	0.0000	0.0000	0.0000	0.4773	0.6932	0.8523
C9	0.5568	0.7955	0.9205	0.5909	0.8295	0.9432	0.0000	0.0000	0.0000
C10	0.5227	0.7614	0.8977	0.4886	0.7045	0.8523	0.4886	0.7159	0.8523

C11	0.5682	0.7955	0.9091	0.4091	0.6023	0.7727	0.4773	0.6932	0.8409

	C10			**C11**		
	l	**m**	**u**	**l**	**m**	**u**
C1	0.4659	0.6818	0.8409	0.4091	0.6250	0.8068
C2	0.5000	0.7386	0.8977	0.4545	0.6932	0.8636
C3	0.3977	0.6250	0.8409	0.3864	0.6136	0.8182
C4	0.3636	0.5455	0.7273	0.3295	0.5000	0.6591
C5	0.4318	0.6477	0.8182	0.3864	0.6023	0.7955
C6	0.5341	0.7727	0.8864	0.3750	0.6023	0.7614
C7	0.5114	0.7386	0.8750	0.4318	0.6591	0.8409
C8	0.4659	0.6932	0.8523	0.4205	0.6364	0.8068
C9	0.6136	0.8636	0.9773	0.5455	0.7955	0.9318
C10	0.0000	0.0000	0.0000	0.4659	0.7045	0.8409
C11	0.5568	0.7841	0.8977	0.0000	0.0000	0.0000

Fonte: Elaborado pelo autor (2025).

Passo 3 – No terceiro passo foi utilizado um método de desfuzzyficação para se obter a Matriz *fuzzy* de influência direta do grupo (Si *et al*., 2018).

Existem diversas formas para se realizar a desfuzzyficação de uma Matriz. No estudo em epígrafe foi escolhido o método de *Center of Area* (COA), demonstrado por Si *et al*. (2018, p.20), em que, por meio da aplicação da Eq. 3.2, calcula-se a média entre os valores inferiores, médios e superiores, em que se obtêm ao final a Matriz Z desfuzzyficada, conforme Tabela 3.4.

$$y = l + \frac{(m-l)+(u-l)}{3}, \quad or \quad y = \frac{l+m+u}{3} \tag{3.2}$$

Tabela 3.4: Matriz Z desfuzzyficada.

	C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	C11
C1	0.000	0.818	0.731	0.693	0.814	0.765	0.777	0.860	0.739	0.663	0.614
C2	0.754	0.000	0.830	0.689	0.765	0.739	0.784	0.784	0.652	0.712	0.670
C3	0.701	0.720	0.000	0.735	0.735	0.799	0.727	0.727	0.663	0.621	0.606
C4	0.625	0.602	0.625	0.000	0.667	0.708	0.655	0.708	0.500	0.545	0.496
C5	0.640	0.731	0.777	0.667	0.000	0.758	0.746	0.780	0.644	0.633	0.595
C6	0.761	0.742	0.727	0.697	0.780	0.000	0.795	0.780	0.667	0.731	0.580
C7	0.655	0.720	0.617	0.648	0.739	0.754	0.000	0.701	0.629	0.708	0.644
C8	0.750	0.716	0.712	0.663	0.784	0.758	0.720	0.000	0.674	0.670	0.621
C9	0.689	0.689	0.663	0.625	0.731	0.697	0.758	0.788	0.000	0.818	0.758
C10	0.697	0.731	0.659	0.602	0.640	0.693	0.727	0.682	0.686	0.000	0.670
C11	0.602	0.701	0.606	0.527	0.583	0.587	0.758	0.595	0.670	0.746	0.000

Fonte: Elaborado pelo autor (2025).

Passo 4 – Uma vez obtida a Matriz Z desfuzzyficada, o próximo passo é realizar a normalização da Matriz, o que foi concretizado por meio da Eq. 3.3, a qual divide os valores da Matriz Z pelo valor de S, o qual corresponde ao valor máximo encontrado pela soma das linhas da Matriz Z, conforme Tabela 3.5.

$$S = \frac{max}{1 \le i \le n} \sum_{j=1}^{n} z_{ij} \tag{3.3}$$

Tabela 3.5: Cálculo do valor máximo da Matriz Z.

C1	7.473
C2	7.379
C3	7.034
C4	6.133
C5	6.970
C6	7.261
C7	6.814
C8	7.068
C9	7.216
C10	6.788
C11	6.375
Máximo (S)	7.473

Fonte: Elaborado pelo autor (2025).

Uma vez obtido o valor máximo S, aplicou-se a Eq. 3.4, para se obter a Matriz X normalizada. Para tanto, cada linha de cada coluna da Matriz Z é dividida pelo valor de S, resultando na Matriz X normalizada, conforme Tabela 3.6.

$$X = \frac{Z}{S} \tag{3.4}$$

Tabela 3.6: Matriz X normalizada.

	C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	C11
C1	0.000	0.109	0.098	0.093	0.109	0.102	0.104	0.115	0.099	0.089	0.082
C2	0.101	0.000	0.111	0.092	0.102	0.099	0.105	0.105	0.087	0.095	0.090
C3	0.094	0.096	0.000	0.098	0.098	0.107	0.097	0.097	0.089	0.083	0.081
C4	0.084	0.081	0.084	0.000	0.089	0.095	0.088	0.095	0.067	0.073	0.066
C5	0.086	0.098	0.104	0.089	0.000	0.101	0.100	0.104	0.086	0.085	0.080
C6	0.102	0.099	0.097	0.093	0.104	0.000	0.106	0.104	0.089	0.098	0.078
C7	0.088	0.096	0.083	0.087	0.099	0.101	0.000	0.094	0.084	0.095	0.086
C8	0.100	0.096	0.095	0.089	0.105	0.101	0.096	0.000	0.090	0.090	0.083
C9	0.092	0.092	0.089	0.084	0.098	0.093	0.101	0.105	0.000	0.109	0.101
C10	0.093	0.098	0.088	0.081	0.086	0.093	0.097	0.091	0.092	0.000	0.090
C11	0.081	0.094	0.081	0.070	0.078	0.079	0.101	0.080	0.090	0.100	0.000

Fonte: Elaborado pelo autor (2025).

Passo 5 – No passo 5 é calculado a Matriz T (Tabela 3.8) que corresponde a influência total, direta e indireta, entre os fatores analisados (Si *et al.*, 2018). A Matriz T é derivada a partir da matriz de avaliação direta normalizada X, e é obtida com a aplicação da Eq. 3.5, em que se realiza a multiplicação da Matriz X pela inversa da Matriz I – X, onde I corresponde a Matriz Identidade (Tabela 3.7).

$$T = X \,.\, (I - X)^{-1} \tag{3.5}$$

Tabela 3.7: Matriz Identidade.

	C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	C11
IT1	1.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000
IT2	0.000	1.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000
IT3	0.000	0.000	1.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000
IT4	0.000	0.000	0.000	1.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000
IT5	0.000	0.000	0.000	0.000	1.000	0.000	0.000	0.000	0.000	0.000	0.000
IT6	0.000	0.000	0.000	0.000	0.000	1.000	0.000	0.000	0.000	0.000	0.000
IT7	0.000	0.000	0.000	0.000	0.000	0.000	1.000	0.000	0.000	0.000	0.000
IT8	0.000	0.000	0.000	0.000	0.000	0.000	0.000	1.000	0.000	0.000	0.000
IT9	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	1.000	0.000	0.000
IT10	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	1.000	0.000
IT11	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	1.000

Fonte: Elaborado pelo autor (2025).

Tabela 3.8: Matriz de influência total T.

	C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	C11
C1	1.235	1.381	1.336	1.266	1.394	1.391	1.420	1.425	1.265	1.309	1.205
C2	1.310	1.266	1.331	1.250	1.372	1.371	1.404	1.399	1.240	1.298	1.197
C3	1.252	1.299	1.178	1.205	1.314	1.323	1.342	1.337	1.191	1.236	1.142
C4	1.106	1.143	1.117	0.984	1.162	1.169	1.186	1.188	1.042	1.090	1.003
C5	1.236	1.291	1.263	1.189	1.214	1.309	1.334	1.333	1.181	1.228	1.132
C6	1.294	1.338	1.303	1.235	1.356	1.264	1.387	1.381	1.226	1.283	1.171
C7	1.214	1.264	1.221	1.163	1.279	1.283	1.217	1.298	1.156	1.213	1.115
C8	1.264	1.305	1.272	1.203	1.326	1.325	1.348	1.255	1.199	1.248	1.149
C9	1.277	1.323	1.286	1.217	1.340	1.339	1.373	1.371	1.135	1.285	1.183
C10	1.215	1.262	1.222	1.155	1.264	1.272	1.302	1.292	1.159	1.123	1.116
C11	1.140	1.192	1.151	1.085	1.190	1.193	1.237	1.214	1.097	1.150	0.975

Fonte: Elaborado pelo autor (2025).

Passo 6 – Uma vez obtida a Matriz T, é possível realizar os cálculos dos vetores *Receiver* (R) e *Cause (C)* (Si *et al*., 2018), o que foi realizado com base na Eq. 3.6, obtendo os resultados contidos na Tabela 3.9.

$$R = \left[\sum_{j=1}^{n} \quad t_{ij} \right]_{nx1}, \qquad C = \left[\sum_{j=1}^{n} \quad t_{ij} \right]_{1xn} \tag{3.6}$$

Tabela 3.9: Matriz T com os cálculos dos vetores R e C.

	C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	C11	R
C1	1.235	1.381	1.336	1.266	1.394	1.391	1.420	1.425	1.265	1.309	1.205	14.628
C2	1.310	1.266	1.331	1.250	1.372	1.371	1.404	1.399	1.240	1.298	1.197	14.437
C3	1.252	1.299	1.178	1.205	1.314	1.323	1.342	1.337	1.191	1.236	1.142	13.820
C4	1.106	1.143	1.117	0.984	1.162	1.169	1.186	1.188	1.042	1.090	1.003	12.189
C5	1.236	1.291	1.263	1.189	1.214	1.309	1.334	1.333	1.181	1.228	1.132	13.710
C6	1.294	1.338	1.303	1.235	1.356	1.264	1.387	1.381	1.226	1.283	1.171	14.237
C7	1.214	1.264	1.221	1.163	1.279	1.283	1.217	1.298	1.156	1.213	1.115	13.422
C8	1.264	1.305	1.272	1.203	1.326	1.325	1.348	1.255	1.199	1.248	1.149	13.894
C9	1.277	1.323	1.286	1.217	1.340	1.339	1.373	1.371	1.135	1.285	1.183	14.131
C10	1.215	1.262	1.222	1.155	1.264	1.272	1.302	1.292	1.159	1.123	1.116	13.383
C11	1.140	1.192	1.151	1.085	1.190	1.193	1.237	1.214	1.097	1.150	0.975	12.624
C	13.545	14.065	13.679	12.952	14.211	14.240	14.549	14.491	12.890	13.463	12.388	

Fonte: Elaborado pelo autor (2025).

O Vetor R consiste na soma das linhas da Matriz T enquanto que o vetor C corresponde a soma das colunas. Com base nos valores obtidos (*R* e *C*), é possível calcular a Proeminência e

Relação dos fatores, bem como produzir o Diagrama de causa e efeito, também chamado de Diagrama Causal (DC), e o Mapa de Relação e Influência (MRI) (*Si et al*., 2018), os quais correspondem ao **passo 7** e será apresentado no Capítulo 4, seção 4.1, 4.2 e 4.3.

3.3 Resumo do Capítulo

Este capítulo apresentou os procedimentos metodológicos utilizados na pesquisa, destacando sua classificação, abordagem e métodos aplicados. A pesquisa foi estruturada em quatro etapas: (i) análise das alterações na norma e identificação das variáveis relevantes, (ii) estruturação da pesquisa e definição do protocolo de coleta de dados, (iii) levantamento de informações junto a especialistas do setor de tecnologia e segurança da informação e (iv) análise dos dados utilizando o método Fuzzy DEMATEL.

O levantamento de dados foi realizado por meio de um questionário aplicado a Diretores de Tecnologia, com o objetivo de avaliar a influência dos novos controles da ISO/IEC 27001:2022. As respostas foram analisadas com o método Fuzzy DEMATEL, com a demonstração de todos os passos para sua aplicação, permitindo mapear as relações de influência entre os controles e identificar aqueles que desempenham um papel central na estrutura de segurança da informação.

A seguir, são apresentados os resultados e as discussões sobre os achados da pesquisa.

4 APRESENTAÇÃO E DISCUSSÃO DOS RESULTADOS

Este capítulo apresenta os resultados alcançados por meio das análises com o *Fuzzy Dematel* e suas discussões.

4.1 Relação e Proeminência

Uma vez obtidos os vetores *R* e C, foi possível calcular a Proeminência e Relação dos fatores (Tabela 4.1), em que o eixo horizontal (*R+C*) ilustra a força das influências que são dadas e recebidas enquanto que o eixo vertical (*R-C*) mostra o efeito para o qual o fator contribui no sistema (Si *et al*., 2018). Além disso, quando positivo significa que ele influencia os outros fatores, podendo ser agrupado como fator de Causa, enquanto que, se for negativo, então o fator é influenciado e deve ser agrupado como Efeito (Si *et al*., 2018).

Tabela 4.1: Valores de R+C e R-C calculados.

Fator	R	C	R+C	R-C	**Causa ou Efeito**
Inteligência de Ameaça (C1)	14.628	13.545	28.173	1.083	**Causa**
Segurança da informação para o uso de serviços em nuvem (C2)	14.437	14.065	28.502	0.372	**Causa**
Prontidão de TIC para a continuidade de negócios (C3)	13.820	13.679	27.499	0.141	**Causa**
Monitoramento de segurança física (C4)	12.189	12.952	25.142	-0.763	**Efeito**
Gestão de configuração (C5)	13.710	14.211	27.921	-0.501	**Efeito**
Atividades de monitoramento (C6)	14.237	14.240	28.477	-0.003	**Efeito**
Prevenção de vazamento de dados (C7)	13.422	14.549	27.971	-1.127	**Efeito**
Filtragem da web (C8)	13.894	14.491	28.385	-0.598	**Efeito**
Desenvolvimento seguro (C9)	14.131	12.890	27.021	1.241	**Causa**
Descarte ou exclusão de informações (C10)	13.383	13.463	26.846	-0.080	**Efeito**
Mascaramento de dados (C11)	12.624	12.388	25.011	0.236	**Causa**

Fonte: Elaborado pelo autor (2025).

A Tabela 4.1. permite identificar, dentre os 11 controles de segurança da informação, quais são os controles de Causa (C1, C2, C3, C9 e C11) que são aqueles fatores que possuem mais influência, enquanto que os demais (C4, C5, C6, C7, C8 e C10) são considerados controles de Efeito, ou seja, são mais afetados pelos outros controles do que os afetam, o que se traduz em informações importantes para uma melhor compreensão desses novos controles, frente a sua incorporação junto ao SGSI.

4.1.1. Controles de causa

Os controles C1 – Inteligência de Ameaça, C2 – Segurança da Informação para o Uso de Serviços em Nuvem, C3 – Prontidão de TIC para a Continuidade de Negócios, C9 – Desenvolvimento Seguro e C11 – Mascaramento de Dados foram identificados como controles de causa, ou seja, aqueles que possuem maior influência sobre os demais. Esses controles desempenham um papel estruturante na segurança da informação, criando a base necessária para que os controles de efeito operem de forma eficiente.

A Inteligência de Ameaça (C1) antecipa riscos, permitindo ações proativas e fortalecendo medidas de proteção. A segurança em nuvem (C2) estabelece diretrizes fundamentais para proteger dados em ambientes externos, enquanto a prontidão de TIC (C3) assegura a continuidade das operações em cenários de interrupção. O desenvolvimento seguro (C9) influencia todo o ciclo de vida de sistemas e aplicações, reduzindo vulnerabilidades desde a concepção, enquanto que o mascaramento de dados (C11) protege informações sensíveis e complementa os esforços de segurança em diversos contextos. Esses controles, portanto, devem ser priorizados, pois sua implementação adequada potencializa a eficácia de todo o ecossistema de segurança.

4.1.2. Controles de efeito

Por outro lado, os controles classificados como de efeito, C4 – Monitoramento de Segurança Física, C5 – Gestão de Configuração, C6 – Atividades de Monitoramento, C7 – Prevenção de Vazamento de Dados, C8 – Filtragem da Web e C10 – Descarte ou Exclusão de Informações, são diretamente impactados pelas ações e diretrizes estabelecidas pelos fatores de causa. Esses controles operam como respostas ou consequências da estrutura estratégica definida pelos controles de influência.

O monitoramento de segurança física (C4) depende de informações precisas e de infraestrutura bem planejada, garantindo que riscos físicos sejam detectados e tratados. A gestão de configuração (C5) assegura a estabilidade e segurança do ambiente de TI, refletindo a efetividade de políticas previamente definidas.

As atividades de monitoramento (C6) atuam como uma extensão prática dos controles de causa, garantindo a supervisão contínua e detectando irregularidades. Enquanto a prevenção de vazamento de dados (C7) é fortemente influenciada por medidas estratégicas, como o desenvolvimento seguro, e age como uma barreira final para proteger informações sensíveis.

A filtragem da web (C8), por sua vez, contribui para restringir acessos não autorizados, alinhando-se às diretrizes de segurança organizacional. Ademais, o descarte ou exclusão de informações (C10) assegura o tratamento adequado de dados sensíveis, refletindo a maturidade das políticas de segurança.

Esses controles dependem diretamente da efetividade dos controles de causa e, portanto, devem ser gerenciados de forma a maximizar os benefícios resultantes da implementação estratégica dos controles prioritários.

4.2. Diagrama Relacional Causal

Com os valores (*R+C* e *R-C*) definidos, outro passo importante é construir o Diagrama Causal (DC), apresentado na Figura 4.2, que representa graficamente as relações de causa e efeito entre os fatores (Si *et al*., 2018).

O vetor *R+C* é denominado "Proeminência" por revelar a importância do peso do critério, enquanto que o vetor *R-C* é chamado de "Relação" por dividir os critérios em um grupo de causa e efeito, em que se positivo o critério geralmente pertence ao grupo de Causa, enquanto que, se negativo, pertence ao grupo de Efeito (Chien, Wu e Huang, 2014).

Com o diagrama construído, é possível fazer uma análise por quadrantes, tomando por base o cálculo da média de *R+C* (Si *et al*., 2018), em que se divide o diagrama em quatro quadrantes, conforme Figura 4.1, o que permite obter informações valiosas sobre cada um deles de acordo com a sua posição.

O quadrante I é denominado de Fatores Centrais; os contidos no quadrante II são os Fatores de Direcionadores ou Autônomos; os do Quadrantes III são identificados como Fatores Independentes e os fatores do Quadrante IV de Fatores de Impacto (Si *et al.,* 2018).

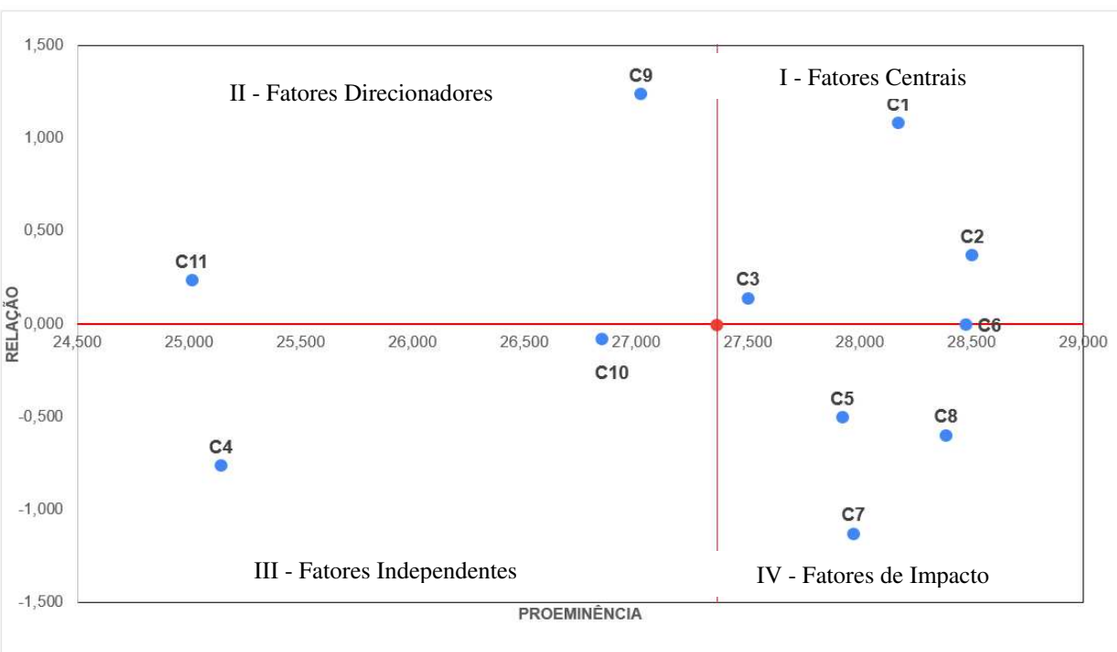


Figura 4.1: Diagrama Causal e seus Quadrantes.
Fonte: Elaborado pelo autor (2025).

Com base na distribuição disposta na Figura 4.2, pode-se observar que, no primeiro quadrante estão dispostos os controles de Inteligência de ameaças (C1), Segurança da informação para o uso de serviços em nuvem (C2) e Prontidão de TIC para a continuidade de negócios (C3) como Fatores Centrais do sistema, os quais possuem alta proeminência e alta relação, tratando-se de fatores chave

que são classificados como alvo prioritário no uso de recursos para o seu gerenciamento (Chien, Wu e Huang, 2014).

Esses controles desempenham um papel central na estrutura do sistema, pois não apenas orientam os outros controles (fatores de causa), mas também dependem de interações entre si para funcionarem de forma eficiente. Eles devem ser priorizados em estratégias de implementação, pois afetam diretamente a eficácia de todo o sistema.

No segundo quadrante estão os controles que fazem parte dos fatores Direcionadores, tratando-se de Desenvolvimento Seguro (C9) e Mascaramento de dados (C11), os quais possuem baixa proeminência e alta relação em que, ou seja, influenciam fortemente os demais controles, mas não são tão impactados por eles, os quais são classificados em segundo lugar no uso de recursos de gerenciamento (Chien, Wu e Huang, 2014).

No terceiro quadrante, estão delineados os fatores definidos como Independentes, tratando-se do Descarte ou exclusão de informações (C10) e Monitoramento de segurança física (C4). Neste quadrante estão localizados os fatores que possuem baixa proeminência e alta relação, os quais possuem baixa interação com outros fatores, qualificando-se em terceiro lugar para uso de recursos de gerenciamento (Chien, Wu e Huang, 2014).

Estes são fatores que operam de forma mais isolada, impactando pouco os outros controles e sendo pouco impactados por eles. Apesar de sua independência relativa, esses controles são importantes para cenários específicos, como o descarte adequado de dados sensíveis e a proteção física de ativos. Sua eficácia depende mais da qualidade de sua implementação do que de interações com outros fatores.

No quarto quadrante, tipificado como Fator de Impacto, estão localizados os controles de Atividades de monitoramento (C6), Gestão de configuração (C5), Filtragem da web (C8) e Prevenção de vazamento de dados (C7), os quais possuem alta proeminência e baixa relação, e devem ser gerenciados, mas não podem ser melhorados diretamente, ficando em último lugar em relação ao uso de recursos de gerenciamento (Chien, Wu e Huang, 2014).

Esses fatores operam como respostas às diretrizes estabelecidas e, embora devam ser cuidadosamente gerenciados para garantir sua eficácia, não podem ser diretamente melhorados sem mudanças nos controles estratégicos que os orientam. A filtragem da web (C8) e a prevenção de vazamento de dados (C7) dependem da qualidade das políticas e estruturas implementadas, funcionando como medidas práticas para executar as diretrizes de segurança. Por isso, seu aprimoramento está intrinsecamente ligado à melhoria dos controles de causa que lhes fornecem suporte.

Com as informações obtidas na análise dos quadrantes, os tomadores de decisão podem detectar visualmente as relações complexas causais entre os fatores (*Si et al.*, 2018), identificando facilmente aqueles que são considerados fatores chave no sistema e que devem ser prioritários na alocação de recursos, bem como os direcionadores, os independentes e os que não podem ser melhorados diretamente.

Essa abordagem oferece aos tomadores de decisão uma avaliação estratégica e assertiva na integração, gerenciamento e manutenção dos controles junto ao SGSI, o que permite que as organizações otimizem suas estratégias e alinhem as medidas de segurança aos seus objetivos

corporativos, promovendo uma gestão proativa e adaptativa diante das constantes mudanças no cenário de ameaças.

4.3. Mapa Relacional de Influência

O Mapa Relacional de Influência (MRI) é construído com base nas informações obtidas da Matriz T e fornece uma representação gráfica das interações entre os fatores (Si *et al*., 2018) o que provê informações valiosas para os tomadores de decisão.

Essa estrutura facilita a compreensão das dinâmicas de influência entre os fatores, permitindo que os tomadores de decisão priorizem ações nos pontos mais estratégicos. Ao visualizar as interações entre os fatores, os tomadores de decisão podem identificar claramente qual a relação entre eles e o seu nível de dependência com outros controles, o que é essencial para planejar intervenções mais eficazes, focando em melhorar controles estratégicos e fortalecendo o alinhamento entre os diferentes componentes.

É importante destacar que, em algumas situações, quando há muitos fatores a serem analisados, a representação pode se tornar excessivamente complexa, dependendo do número total de elementos. Se todas as relações forem consideradas, o mapa resultante pode ficar confuso, dificultando uma avaliação clara e precisa das interações entre os elementos (Sara, Stikkelman e Herder, 2015). Para mitigar esse problema, é necessário que se aplique um filtro para eliminar as influências que tem menor impacto no sistema, o que provê um mapa mais compreensível e claro para a tomada de decisão.

Para isso, antes da construção do MRI foi definido um valor limite de filtro, conforme é proposto por Si *et al*. (2018), a fim de que apenas os controles que tenham valor igual ou acima desse valor limite sejam considerados para ilustração no MRI. Para obter o valor limite foi aplicado a Eq. 4.1, que calcula uma média entre todos os elementos da Matriz T (Tabela 3.8).

$$\propto = \sum_{i=1}^{n} \sum_{j=1}^{n} [tij]/N \tag{4.1}$$

Considerando o valor limite obtido, tratando-se de 1,244, foram definidos os controles que serviram de base para a construção do Mapa Relacional de Influência apresentado na Figura 4.2, os quais estão destacados na cor verde na Matriz T, conforme Tabela 4.2, em que apenas as relações que possuem valor igual ou a acima do valor limite foram consideradas para exibição no MRI.

Tabela 4.2: Influência dos critérios em relação à média da Matriz T.

	C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	C11
C1	1.235	**1.381**	**1.336**	**1.266**	**1.394**	**1.391**	**1.420**	**1.425**	**1.265**	**1.309**	1.205
C2	**1.310**	**1.266**	**1.331**	**1.250**	**1.372**	**1.371**	**1.404**	**1.399**	1.240	**1.298**	1.197
C3	**1.252**	**1.299**	1.178	1.205	**1.314**	**1.323**	**1.342**	**1.337**	1.191	1.236	1.142
C4	1.106	1.143	1.117	0.984	1.162	1.169	1.186	1.188	1.042	1.090	1.003
C5	1.236	**1.291**	**1.263**	1.189	1.214	**1.309**	**1.334**	**1.333**	1.181	1.228	1.132
C6	**1.294**	**1.338**	**1.303**	1.235	**1.356**	**1.264**	**1.387**	**1.381**	1.226	**1.283**	1.171
C7	1.214	**1.264**	1.221	1.163	**1.279**	**1.283**	1.217	**1.298**	1.156	1.213	1.115
C8	**1.264**	**1.305**	**1.272**	1.203	**1.326**	**1.325**	**1.348**	**1.255**	1.199	**1.248**	1.149
C9	**1.277**	**1.323**	**1.286**	1.217	**1.340**	**1.339**	**1.373**	**1.371**	1.135	**1.285**	1.183
C10	1.215	**1.262**	1.222	1.155	**1.264**	**1.272**	**1.302**	**1.292**	1.159	1.123	1.116
C11	1.140	1.192	1.151	1.085	1.190	1.193	1.237	1.214	1.097	1.150	0.975

Fonte: Elaborado pelo autor (2025).

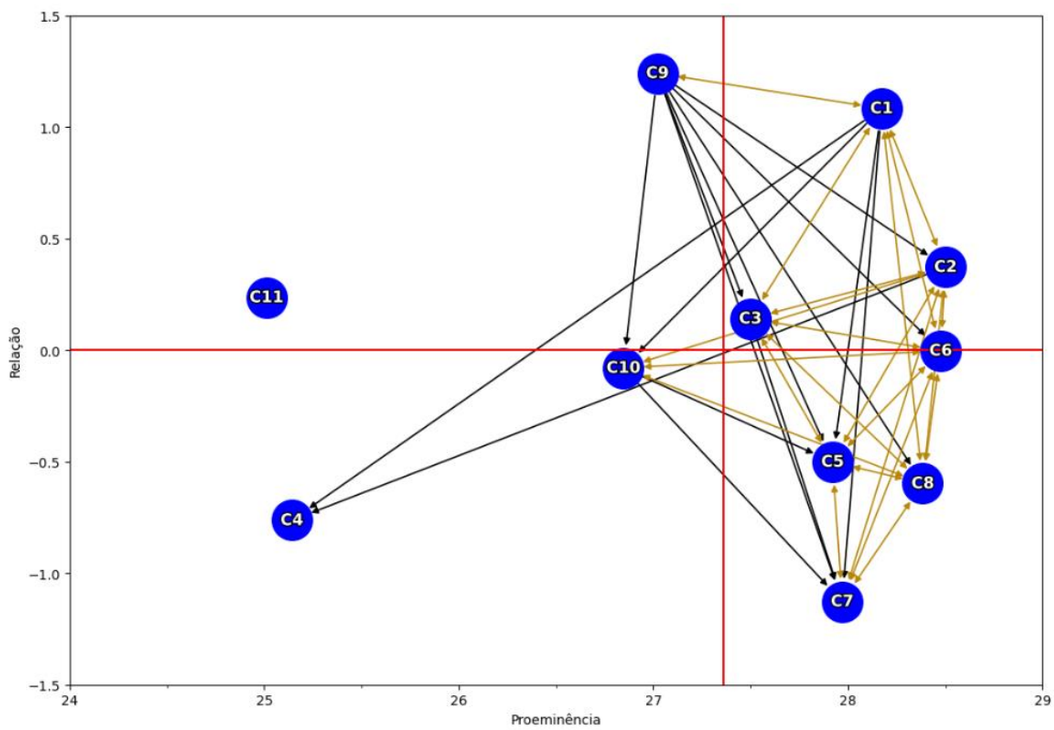


Figura 4.2: Mapa Relacional de Influência.
Fonte: Elaborado pelo autor (2025).

O MRI construído revela as interações críticas entre os fatores do sistema, destacando conexões bidirecionais e unidirecionais. As setas amarelas representam relações de interdependência, ou seja, o controle influência e também é influenciado pelo controle, enquanto que as pretas indicam uma relação de influência direta, não recíproca. Essa distinção permite identificar como os controles se relacionam e estruturam o sistema de segurança analisado.

Os controles C1 (Inteligência de Ameaça), C2 (Segurança da Informação para Uso de Serviços em Nuvem), C6 (Atividades de Monitoramento) e C8 (Filtragem da Web) possuem alta conectividade, relacionando-se com todos os outros controles, exceto C9 (Desenvolvimento Seguro), C4 (Monitoramento de Segurança Física) e C11 (Mascaramento de Dados).

Apesar de C9 não ser afetado pelos controles C1, C2, C3 (Prontidão de TIC para a continuidade de negócios), C6 (Atividades de monitoramento) e C8, ele influencia todos esses controles, indicando a sua importância ao gerenciá-los.

Por outro lado, os controles C4 (Monitoramento de Segurança Física) e C11 (Mascaramento de Dados) apresentam baixa conectividade no MRI, operando de forma mais independente. C4 possui um impacto localizado, relacionado principalmente à proteção de ativos físicos, enquanto

C11 aparece isolado, refletindo sua aplicação em cenários específicos e menos integrado às dinâmicas dos demais fatores.

Como base no MRI obtido, os tomadores de decisão podem avaliar, de forma gráfica, as principais influências entre os controles do sistema, obtendo informações valiosas para tomada de decisão em relação à incorporação e gerenciamento desses novos controles junto ao SGSI da organização.

4.4. Discussões

Os resultados obtidos neste estudo apresentam convergências significativas com pesquisas anteriores que utilizaram métodos baseados em lógica *fuzzy* para a priorização e análise de controles de segurança da informação. Estudos como o de Ho *et al*. (2015) empregaram o método Fuzzy DEMATEL para avaliar as relações de causa e efeito entre controles do Sistema de Gestão de Segurança da Informação, identificando os controles mais influentes dentro da norma ISO/IEC 27001 na sua versão de 2013. Da mesma forma, Tariq *et al.* (2020) aplicaram o *Fuzzy* AHP para priorizar controles em redes em nuvem e sensores sem fio, destacando a importância de direcionar recursos para os controles com maior impacto sistêmico. Os resultados deste estudo corroboram essas abordagens, identificando, de forma detalhada, a relação de causa e efeito as influências entre os 11 novos controles que foram evidenciados pela norma ISO/IEC 27001:2022, além de explicitar a hierarquia na gestão de investimentos dos recursos para cada um deles.

Entretanto, este estudo avança ao focar exclusivamente nos 11 novos controles introduzidos pela ISO/IEC 27001:2022, o que representa uma contribuição inédita para a literatura. Até o momento, as pesquisas revisadas analisaram controles da norma em versões anteriores, sem uma avaliação detalhada do impacto e das interações desses novos controles. Os achados indicam que "Inteligência de Ameaças" e "Desenvolvimento Seguro" emergem como fatores primários de influência, atuando como fatores centrais dentro do sistema avaliado. Esse resultado é consistente com a crescente ênfase na proteção de dados que estão dispostos em serviços de nuvem, e o surgimento de novas ameaças a todo momento, o que denota a sua importância para o Sistema de Gestão e Segurança da Informação.

Outro ponto de destaque é a obtenção de duas saídas ao aplicar o método Fuzzy DEMATEL, que englobam o Diagrama Causal e o Mapa Relacional de Influências, os quais fornecem uma representação visual das relações de causa e efeito, além das influências diretas e indiretas entre os controles analisados. A representação visual permite observar claramente as relações entre diferentes controles, o que é crucial para entender como mudanças em um controle podem impactar outros dentro do sistema. Além disso, estes suportam a tomada de decisões, permitindo que os gestores entendam melhor as implicações de suas escolhas e então planejem estratégias mais eficazes para sua implementação.

A análise do Diagrama Causal, pode-se observar que o controle Inteligência de Ameaça (C1) tem uma importância crítica na cadeia de dependência do sistema. Ao ser acionado, este impacta diretamente os controles de causa, gerando efeitos significativos. Entre esses controles, destaca-se

a Prevenção de Vazamento de Dados (C7), que recebe o maior impacto, tornando-se diretamente dependente das ações promovidas por este controle, bem como, é afetado fortemente pelo controle Segurança da Informação para uso de Serviços em Nuvem (C2) o qual também possui uma forte influência na sua eficácia. Além disso, o controle C7 não pode ser melhorado diretamente, assim, caso uma organização identifique a necessidade de sua melhoria, deve na verdade melhorar os controles citados para que ele possa ser melhorado.

Da mesma forma, os controles de Gestão da Configuração (C5) e Filtragem de Web (C8) também são fatores de impacto no sistema e assim, somente podem ser melhorados por meio de outros controles que os afetam.

Outro aspecto a ser considerado é que, o controle Monitoramento de Segurança Física (C4) é relativamente isolado no sistema e tem pouco impacto sobre os demais controles. Por isso, pode ser tratado de forma mais segmentada e, embora seja relevante no contexto geral da segurança da informação, não precisa ser priorizado ao modelar as dependências entre os controles.

No que se refere ao Mapa Relacional de Influência (Figura 4.2) observa-se que o controle C1 (Inteligência de Ameaça) está conectado aos controles C9 (Desenvolvimento Seguro), C2 (Segurança da Informação para o Uso de Serviços em Nuvem), C3 (Prontidão de TIC para a Continuidade de Negócios) e C6 (Atividades de Monitoramento), estabelecendo uma relação bidirecional entre eles. Essa interconexão indica que as influências não ocorrem de maneira unilateral, mas sim em um fluxo contínuo de troca de informações e impacto mútuo, reforçando a interdependência entre os controles e sua relevância na segurança do sistema.

Além disso, o controle de Atividade de Monitoramento (C6), apesar de ser considerado um controle de efeito, está no limiar do quadrante para ser considerado um fator chave na relação de causa ou de efeito. Sua posição intermediária na cadeia de influência e suas múltiplas conexões com outros controles indicam que seu impacto pode variar conforme o tipo de atividade monitorada. Dessa forma, é fundamental considerar a natureza específica desse monitoramento ao avaliar sua relevância e priorizar melhorias, garantindo que ele atue de maneira eficaz dentro do sistema de segurança da informação.

Enquanto o controle Mascaramento de Dados (C11) não apresenta uma relação forte com nenhum outro controle do sistema, o que sugere uma atuação mais isolada dentro da rede de influências. Sua posição no diagrama indica que, embora seja um controle relevante para a proteção de informações sensíveis, ele não exerce impacto significativo sobre outros fatores e depende diretamente deles para sua efetividade. Isso significa que sua implementação pode ser tratada de forma mais independente, sem a necessidade de ajustes em outros controles para garantir seu funcionamento adequado. No entanto, sua eficácia pode ser potencializada quando alinhada a estratégias mais amplas de proteção de dados, especialmente em conjunto com políticas de desenvolvimento seguro e prevenção de vazamento de informações.

Ao avaliar os grupos em que cada controle está alicerçado (Quadro 2.1), foi possível identificar que os três controles que fazem parte do grupo organizacionais - Inteligência de Ameaça (C1), Segurança da Informação, para uso de Serviço em Nuvem (C2) e Prontidão de TIC para a continuidade de negócios (C3) – foram identificados como Fatores Centrais do sistema, o que denota a preocupação em estabelecer diretrizes robustas para a governança e a gestão de riscos no cenário atual da segurança de informação. Esses controles organizacionais refletem a necessidade

de uma estrutura bem definida, garantindo a conformidade com normas e regulamentos, além de fortalecer a segurança e a eficiência operacional, demostrando sua importância e foco para o cenário atual da segurança da informação.

Dessa forma, a presença de controles organizacionais bem estabelecidos não apenas reforça a segurança, mas também demonstra um compromisso estratégico da instituição com a melhoria contínua e a adaptação às mudanças do ambiente interno e externo.

Em relação a implicações práticas, os resultados obtidos neste estudo proveem os seguintes ganhos para os gestores responsáveis pelo gerenciamento dos SGSI:

a) Priorização eficiente de controles: Ao identificar os controles de causa e efeito, os gestores podem concentrar recursos e esforços nos controles com maior impacto sistêmico, identificando quais são mais estratégicos e quais demandam de uma atenção especial para sua execução;
b) Otimização de recursos: Ao entender quais controles são mais influentes, é possível otimizar o direcionamento dos recursos, em que se obtém um ganho significativo no uso de tempo, equipe e orçamento, evitando esforços desnecessários em controles que não podem ser melhorados diretamente;
c) Tomada de decisão baseada em evidências: A análise fornece dados objetivos e estruturados, ajudando gestores a justificar decisões para seus *stakeholders*, com base nas influências claras entre os controles;
d) Melhoria contínua do SGSI: O mapeamento dinâmico permite identificar áreas para aprimoramento contínuo, especialmente em cenários onde mudanças no ambiente de risco exigem ajustes no SGSI;
e) Mitigação de riscos mais eficiente: Saber quais controles têm maior influência no sistema auxilia na implementação de medidas preventivas e corretivas, reduzindo vulnerabilidades de forma mais robusta e eficaz;
f) Facilidade na comunicação estratégica: O Diagrama de Causa e Efeito facilita o entendimento e a comunicação com equipes técnicas e não técnicas, além de ser útil em auditorias e apresentações gerenciais.

Em relação a implicações teóricas, este estudo contribui significativamente para a literatura sobre a gestão de segurança da informação, ao demonstrar as influências entre os 11 novos controles evidenciados na ISO/IEC 27001:2022, os quais até então ainda não haviam sido abordados no campo acadêmico e são essenciais para uma gestão efetiva do SGSI.

Nesse sentido, a ISO/IEC 27001:2022 abarca três grandes fatores de impacto que são: o aumento de ataques cibernéticos e ameaças avançadas; a expansão do ambiente digital, impulsionada pela computação em nuvem e pelo trabalho remoto; e a intensificação das regulamentações. Esses elementos configuram um novo cenário contemporâneo para a segurança da informação, exigindo abordagens mais dinâmicas e estratégicas.

Dessa forma, a ISO/IEC 27001:2022 representa uma evolução significativa na proteção digital, tornando-a mais alinhada aos desafios do mundo atual. Suas diretrizes aprimoradas fortalecem as organizações contra ameaças emergentes, proporcionando maior controle sobre segurança na nuvem, inteligência contra ameaças, mascaramento de dados e monitoramento contínuo. Assim, as empresas podem se adaptar melhor ao novo panorama, mitigando riscos e

garantindo conformidade frente a ataques cibernéticos, exigências regulatórias e transformações digitais constantes.

5 CONCLUSÕES E CONSIDERAÇÕES FINAIS

Este capítulo apresenta as conclusões, as considerações finais, as limitações da pesquisa e as propostas de trabalhos futuros.

5.1 Conclusões

A pergunta de pesquisa proposta foi respondida de maneira satisfatória e, com base nas discussões apresentadas, conclui-se que o objetivo geral do trabalho foi atingido. Com isso, identificou-se a relação de causa e efeito e o nível de influência entre cada um dos 11 novos controles de segurança da informação evidenciados pela norma ISO/IEC 27001:2022, o que representa uma resposta às demandas e lacuna de conhecimento identificados, propondo-se a solucionar o problema mediante as limitações do trabalho.

A contribuição deste trabalho consiste em apresentar um recorte das relações entre os novos controles de segurança da informação, em que, por meio de uma pesquisa estruturada e aplicada à especialistas do setor tecnológico, obteve-se a base de dados para sua análise mediante a aplicação de um método multicritério, o que se findou em um resultado que abarca uma base de conhecimento para os tomadores de decisão que gerenciam o Sistema de Gestão de Segurança da Informação de suas organizações.

Em relação às questões de pesquisa, o Capítulo 4, subseção 4.1 e 4.2, apresentam as relações de causa e efeito entre os controles, os quais foram obtidos por meio da aplicação do método *Fuzzy* DEMATEL, enquanto que a subseção 4.3 demonstra as influências e dependências entre cada um dos controles de forma gráfica, o que denota que as Questões de Pesquisa foram devidamente atendidas.

Os objetivos específicos oriundos do objetivo geral também foram atingidos**,** vez que:

a) Os fatores de análise foram definidos, conforme disposto na subseções 3.2.1, os quais suportaram a realização da pesquisa com especialistas, tornando-se as variáveis para análise do nível de influência entre cada um dos controles;
b) Identificou-se as relações de causa e efeito entre cada um dos novos controles o que é disposto nas subseções 4.1 e 4.2, demonstrando a relação de proeminência e relação entre cada um deles, bem como, sua distribuição em quadrantes que permitem a alocação de recursos em controles chave;
c) Identificou-se o nível de influência entre os controles, de acordo com o exposto na subseção 4.3, demonstra as interações críticas entre os fatores do sistema, em que se destacou as relações direcionais e bidirecionais entre os controles de maior importância para uma tomada de decisão.

De acordo com Gil (2008) e Cooper e Schindler (2016) a validade refere-se à precisão com que um instrumento de pesquisa mede aquilo que se propõe a medir. Ele enfatiza a importância de assegurar que os dados coletados sejam representativos e precisos, de modo a garantir a validade interna e externa do estudo, o que também é corroborado por Marconi e Lakatos (2017) que enfatizam que a validade de um estudo é crucial para garantir a qualidade e a precisão dos resultados.

Eles definem a validade interna como a capacidade de um estudo medir o que realmente se propõe a medir, enquanto a validade externa refere-se à generalização dos resultados para outros contextos, populações e tempos. Além disso, eles destacam a importância da validade de conteúdo, que assegura que o instrumento de pesquisa cobre de forma abrangente o tema investigado.

A validade de critério e a validade de constructo também são mencionadas como fundamentais para verificar a precisão e a adequação dos instrumentos de medida utilizados na pesquisa.

Portanto, conclui-se que a pesquisa atinge a validade interna e externa dos seus constructos, garantindo que o estudo mede o que se propõe a medir (validade interna) e que os resultados podem ser generalizados entre diferentes populações, ambientes e tempos (validade externa). Essas definições reforçam a relevância da validade como um pilar essencial na metodologia de pesquisa, assegurando que os instrumentos utilizados no estudo são adequados e precisos para as questões investigativas que foram levadas a efeito.

5.2 Considerações Finais

Este estudo apresentou uma análise detalhada dos 11 novos controles de segurança da informação evidenciados pela ISO/IEC 27001:2022, utilizando o método *Fuzzy* DEMATEL para avaliar as influências e relações de causa e efeito entre cada um deles.

A aplicação do método *Fuzzy* DEMATEL permitiu identificar os controles mais influentes e aqueles mais impactados, além de fornecer um mapa gráfico das relações que destaca as conexões de causa e efeito, mostrando-se adequado para aplicações nesse contexto, considerando o tamanho da amostra e as possíveis imprecisões nas avaliações.

Além disso, cada novo controle foi identificado de acordo com a sua localização nos quadrantes do Diagrama Causal, o que permitiu obter informações importantes sobre o papel que cada controle desempenha no sistema e o grau de influência ou dependência em relação aos demais fatores. Essa classificação permitiu identificar quais controles atuam como direcionadores estratégicos, quais são mais centrais para a estrutura do sistema e quais possuem impacto localizado ou operam de forma mais independente, o que permite demonstrar onde esforços e recursos devem ser alocados para priorizar e maximizar a eficácia do sistema.

Destarte, a análise desses novos controles da segurança da informação propicia uma nova perspectiva sobre a sua importância e relação, facilitando a priorização de esforços na sua implementação e gerenciamento, ao realizar a sua incorporação no SGSI.

Cabe salientar que o nível dos especialistas participantes da pesquisa confere uma robustez aos dados obtidos, considerando a média em anos de experiência e sua formação, o que denota um vasto conhecimento em relação ao gerenciamento de projetos complexos, o que é corroborado pelo seu nível na hierarquia da organização.

Destaca-se ainda a importância desses novos controles para fortalecer o SGSI das organizações uma vez que estes foram desenvolvidos para responder às crescentes e diversificadas ameaças cibernéticas, bem como para acompanhar as inovações tecnológicas e as novas regulamentações globais.

Outro ponto de atenção é que ao lançar a nova versão da norma em 2022, foi estabelecido um período de transição de 03 anos para incorporação desses novos controles, o que se finda em 31 de outubro de 2025. Dessa forma, todos os certificados ISO/IEC 27001:2013 devem ser atualizados para nova versão da norma, o que enseja a incorporação desses novos controles, sob pena das organizações não mais estarem certificadas a partir de então, o que expõe ainda mais a importância de uma gestão assertiva para que se integre estes novos controles de forma adequada e sistemática, para que se mantenha a garantia e a confiança dos clientes em relação a gestão do risco a segurança da informação de suas organizações.

Por derradeiro, espera-se que este trabalho contribua para a implementação, gerenciamento e manutenibilidade desses novos controles junto ao SGSI, fornecendo aos tomadores de decisão informações claras e precisas sobre as suas relações, propiciando que esforços e recursos sejam direcionados de forma estratégica e eficaz, garantindo que suas organizações estão em *compliance* com a gestão da segurança da informação.

5.3 Limitações da Pesquisa

São limitações da pesquisa desenvolvida no trabalho:

a) O estudo foca em empresas do setor de tecnologia no Brasil, o que pode restringir a generalização dos resultados para organizações de outros setores;
b) Por se tratar de um estudo de corte transversal, a análise realizada no estudo está restrita a um único ponto de corte no tempo, o que limita a capacidade de se capturar a dinâmica e a evolução das mudanças organizacionais ao longo do tempo.

5.4 Propostas de Trabalhos Futuros

A partir das discussões estabelecidas no trabalho, são propostos os seguintes trabalhos futuros:

a) Desenvolver um estudo com uma base de amostra de respondentes de outros países, como objetivo aplicar o Método *Fuzzy* Dematel e avaliar os resultados obtidos em detrimento com os alcançados nesse estudo;

b) Avaliar o impacto de causa e efeito entre os controles evidenciados e os controles existentes no Sistema de Segurança da Informação na versão anterior da norma, tomando por base o grupo atual a que cada controle está inserido;
c) Avaliar o impacto dos novos controles da Norma ISO/IEC 27001:2022 quando de sua implementação nos Sistemas de Gestão da Segurança da Informação das organizações.

Referências

BOONKRONG, P; NUANSOMSRI, C. *Fuzzy rule-based risk management under ISO/IEC27001: 2013 standard for information security.* ***JCST***, v. 8, n. 1, p. 33-40, 2018.

BRITO, A. P. G.; OLIVEIRA, G. S.; SILVA, B. A. A importância da pesquisa bibliográfica no desenvolvimento de pesquisas qualitativas na área de educação. **Cadernos da FUCAMP**, v. 20, n. 44, 2021.

BRYMAN, A. ***Social research methods***. *5th ed. Oxford: Oxford University Press*, 2016.

CALDER, A.; WATKINS, S. ***IT governance:*** *A manager's guide to data security and BS 7799/ISO 17799. Kogan Page Publishers*, *3th ed. London*, 2005.

CALDER, A; WATKINS, S. ***IT governance:*** *A manager's guide to data security and ISO 27001/ISO 27002. Kogan Page Ltd. 4th ed. United Kingdom,* 2008.

CHAGAS, C. H. L.; RODRIGUES, A. H. G. Análise do processo de implementação de um sistema de gestão da segurança da informação com base na ISO/IEC 27001. **Revista F&T**, v. 29, n. 142, 2025.

CHANG, Y. H.; YEH, C. H.; CHENG, J. H. *Decision support for bus operations under uncertainty: a fuzzy expert system approach.* ***Omega***, v. 26, n. 3, p. 367–380, 1998.

CHIEN, K. F.; WU, Z. H.; HUANG, S. C. *Identifying and assessing critical risk factors for BIM projects: Empirical study.* ***Automation in Construction***, v. 45, p. 1–15, 2014.

COOPER, D. R.; SCHINDLER, P. S. **Métodos de pesquisa em administração**. 12. Ed. Porto Alegre: McGraw Hill Brasil, 2016.

CRESWELL, J. W. ***Research design****: qualitative, quantitative, and mixed methods approaches. 2th ed. Thousand Oaks: Sage Publications*, 2017.

FERREIRA, N.; NUNES, P.; SANTOS, A. Gestão de crises e resiliência organizacional. **Revista Caderno Pedagógico**, v. 21, n. 6, p. 1-21, 2024.

FLICK, U. ***Introducing research methodology****: A beginner's guide to doing a research project. 2th ed. Thousand Oaks: Sage Publications*, 2015.

GIL, A. C. **Como elaborar projetos de pesquisa**. São Paulo: Atlas, 2002.

GIL, A. C. **Métodos e técnicas de pesquisa social**. 6. Ed. São Paulo: Atlas, 2008.

HANNIGAN, L.; DEYAB, G.; AL THANI, A.; AL MARRI, A.; AFIFI, N. *The implementation of an integrated management system at Katar biobank.* ***Biopreservation and Biobanking***, v. 17, n. 6, p. 506–511, 2019.

HO, L. H.; HSU, M. T.; YEN, T. M. *Identifying core control items of information security management and improvement strategies by applying fuzzy DEMATEL.* ***Information and Computer Security***, v. 23, n. 2, p. 161–177, 2015.

ISO**.** NBR ISO/IEC 27001:2022. **Segurança da informação, segurança cibernética e proteção à privacidade – Sistemas de gestão da segurança da informação – Requisitos**. 3. ed. Rio de Janeiro: ABNT, 2022.

ISO**.** NBR ISO/IEC 27002:2022a. **Segurança da informação, segurança cibernética e proteção à privacidade - Controles de segurança da informação**. 3. ed. Rio de Janeiro: ABNT, 2022.

ISO**.** ISO/IEC 27001:2022b. ***Information technology – Security techniques – Information security management systems – Requirements***. *Geneva*: ISO, 2022. Disponível em: < https://www.iso.org/standard/27001>. Acesso em: 20 dez. 2024.

ISO**.** ISO/IEC 27002:2022c. ***Information security, cybersecurity and privacy protection — Information security controls***. *Geneva*: ISO, 2022. Disponível em: < https://www.iso.org/standard/75652.html/>. Acesso em: 20 dez. 2024.

ISO**.** ISO/IEC 27000:2018. ***Information technology — Security techniques — Information security management systems — Overview and vocabulary***. *Geneva*: ISO, 2018. Disponível em: < https://www.iso.org/standard/73906.html>. Acesso em: 20 dez. 2024.

KITSIOS, F.; CHATZIDIMITRIOU, E.; KAMARIOTOU, M. *Developing a risk analysis strategy framework for impact assessment in information security management systems: a case study in IT consulting industry.* ***Sustainability***, v. 14, n. 3, p. 1269, 2022.

KITSIOS, F.; CHATZIDIMITRIOU, E.; KAMARIOTOU, M. The ISO/IEC 27001 *Information security management standard: how to extract value from data in the IT sector.* ***Sustainability***, v. 15, n. 7, p. 5828, 2023.

KHAJOUEI, H.; KAZEMI, M.; MOOSAVIRAD, S; H. *Ranking information security controls by using fuzzy analytic hierarchy process.* ***Information Systems and e-Business Management***, v. 15, p. 1-19, 2017.

LEGOWO, N.; JUHARTOYO, Y. *Risk management; risk assessment of information technology security system at bank using ISO 27001.* ***Journal of System and Management Sciences***, v. 12, n. 3, p. 181-199, 2022.

LEVIN, K. A. *Study design III: Cross-sectional studies.* ***Evidence-based dentistry***, v. 7, n. 1, p. 24-25, 2006.

LIN, C. J.; WU, W. W. *A causal analytical method for group decision-making under fuzzy environment.* ***Expert Systems with Applications***, v. 34, n. 1, p. 205–213, 2008.

MARCONI, M. de A.; LAKATOS, E. M. **Fundamentos de metodologia científica**. 7. ed. São Paulo: Atlas, 2010.

MARCONI, M. de A.; LAKATOS, E. M. **Metodologia do trabalho científico**: projetos de pesquisa/pesquisa bibliográfica/teses de doutorado, dissertações de mestrado, trabalhos de conclusão de curso. São Paulo: Atlas, 2017.

NASCIMENTO, F. P. **Metodologia da Pesquisa Científica:** teoria e prática – como elaborar TCC. 1. ed. São Paulo: Atlas, 2016.

PUNCH, K. F. ***Developing effective research proposals***. *3th ed. London*: *SAGE Publications*, 2016.

RAKOVIĆ, R. *Project of ISMS implementation in organization–aspects and practical experiences.* ***European project management journal***, v. 11, p. 20–30, 2021.

ROUQUAYROL, M. Z. **Epidemiologia & Saúde**. 8. ed. Rio de Janeiro: Medbook, 2018.

SAMPIERI, R. H.; COLLADO, C. F.; LUCIO, P. B. **Metodologia de pesquisa**. Porto Alegre: Penso, 2013.

SARA, J.; STIKKELMAN, R. M.; HERDER, P. M. *Assessing relative importance and mutual influence of barriers for CCS deployment of the ROAD project using AHP and DEMATEL methods.* ***International Journal of Greenhouse Gas Control,*** v. 41, p. 336-357, 2015.

SETIA, M. S. *Methodology series module 3: cross-sectional studies.* ***Indian Journal of Dermatology,*** v. 61, n. 3, p. 261-264, 2016.

SI, S. L.; YOU, X. Y.; LIU, H. C.; ZHANG, P. *DEMATEL technique: a systematic review of the state-of-the-art literature on methodologies and applications.* ***Mathematical Problems in Engineering,*** v. 2018, n. 1, 3696457, 33 *pages*, 2018.

SIPONEN, M.; BASKERVILLE, R. *Intervention effect rates as a path to research relevance: Information systems security example.* ***Journal of the Association for information Systems****, v. 19, n. 4, 2018.*

TARIQ, M. I., AHMED, S., MEMON, N. A., TAYYABA, S., ASHRAF, M. W., NAZIR, M., BALAS, M. M. *Prioritization of information security controls through fuzzy AHP for cloud computing networks and wireless sensor networks*. ***Sensors,*** v. 20, n. 5, p. 1310, 2020.

YIN, R. K. **Estudo de caso:** planejamento e métodos. 5. ed. Porto Alegre: Bookman, 2015.

ZADEH, L. *A. Information and control.* ***Fuzzy sets,*** v. 8, n. 3, p. 338-353, 1965.

APÊNDICE A - Questionário da Pesquisa

Pesquisa de Mestrado – Unicamp

TERMO DE CONSENTIMENTO LIVRE E ESCLARECIDO

https://drive.google.com/file/d/1sLb5We78pVL3jX4Ua9-Pa-rY85sjwDGp/view?usp=drive_link

CAAE: 74829723.3.0000.5404

Nome dos responsáveis:

Reginaldo da Silva Leme

Prof. Dr. Jefferson de Souza Pinto

Prof. Dr. Rosley Anholon

1 - CONCORDÂNCIA EM PARTICIPAR DA PESQUISA

Declaro que li o TCLE, tenho mais de 18 anos e estou disposto a participar desta pesquisa como participante.

2 – Nome do responsável pelo preenchimento do questionário:

_____

3 - Experiência em anos:

_____

4 - Por gentileza, nos informe o *link* de seu CV Lattes ou LinkedIn para melhor conhecer sua experiência.:

_____

5 - Indique a influência da "**Coleta e análise das informações relacionadas a ameaças à segurança da informação, produzindo inteligência de ameaças, para que ações de mitigação adequadas possam ser tomadas**", nos demais elementos:

1. Influência na Especificação e gerenciamento da segurança da informação para uso de serviços em nuvem, avaliando processos de aquisição, uso, gestão e saída de serviços.	○ Nulo	○ Baixíssima	○ Baixa	○ Média	○ Alta	○ Altíssima
2. Influência em Planejar, implementar, manter e testar a prontidão de TIC, com base nos objetivos de continuidade dos negócios, assegurando a disponibilidade das informações da organização e outros ativos associados durante a disrupção.	○ Nulo	○ Baixíssima	○ Baixa	○ Média	○ Alta	○ Altíssima
3. Influência no Monitoramento contínuo das instalações para detectar e impedir o acesso físico não autorizado.	○ Nulo	○ Baixíssima	○ Baixa	○ Média	○ Alta	○ Altíssima
4. Influência nas configurações de segurança,						

hardware, software, serviços e redes, com o fito de que elas sejam estabelecidas, documentadas, implementadas, monitoradas e analisadas criticamente, para que não sejam modificadas por alterações não autorizadas ou incorretas.	○ Nulo	○ Baixíssima	○ Baixa	○ Média	○ Alta	○ Altíssima
5. Influência no monitoramento de comportamentos anômalos e execução de ações apropriadas para avaliar possíveis incidentes de segurança da informação em redes, sistemas e aplicações.	○ Nulo	○ Baixíssima	○ Baixa	○ Média	○ Alta	○ Altíssima
6. Influência na detecção e prevenção da divulgação e extração não autorizadas de informações por indivíduos ou sistemas, prevenindo o vazamento de dados sejam por sistemas, redes, ou quaisquer outros dispositivos que tratem, armazenem ou transmitam informações sensíveis.	○ Nulo	○ Baixíssima	○ Baixa	○ Média	○ Alta	○ Altíssima
7. Influência na proteção dos sistemas para que não sejam comprometidos por malware e impedir o acesso a recursos da web não autorizados, reduzindo a exposição a conteúdos maliciosos.	○ Nulo	○ Baixíssima	○ Baixa	○ Média	○ Alta	○ Altíssima
8. Influência para que o software seja escrito com segurança, reduzindo o número de potenciais vulnerabilidades de segurança da informação, aplicando princípios de codificação segura ao desenvolvimento do software.	○ Nulo	○ Baixíssima	○ Baixa	○ Média	○ Alta	○ Altíssima
9. Influência no quesito de exposição desnecessária de informações sensíveis, estando em compliance com requisitos legais, estatutários, regulamentares e contratuais, excluindo informações armazenadas em sistemas de informação, dispositivos ou qualquer outra mídia de armazenamento quando não forem mais necessárias.	○ Nulo	○ Baixíssima	○ Baixa	○ Média	○ Alta	○ Altíssima
10. Influência no mascaramento de dados para que seja usado de acordo com a política específica para o tema da organização, limitando a exposição de dados confidenciais, incluindo dados pessoais, cumprindo os requisitos legais, estatutários, regulamentares e contratuais.	○ Nulo	○ Baixíssima	○ Baixa	○ Média	○ Alta	○ Altíssima

6 - Indique a influência da "**Especificação e gerenciamento da segurança da informação para uso de serviços em nuvem, avaliando processos de aquisição, uso, gestão e saída de serviços**", nos demais elementos:

1. Influência na coleta e análise das informações relacionadas a ameaças à segurança da informação, produzindo inteligência de ameaças, para que ações de mitigação adequadas possam ser tomadas.	○ Nulo	○ Baixíssima	○ Baixa	○ Média	○ Alta	○ Altíssima
2. Influência em Planejar, implementar, manter e testar a prontidão de TIC, com base nos objetivos de continuidade dos negócios, assegurando a disponibilidade das informações da organização e outros ativos associados durante a disrupção.	○ Nulo	○ Baixíssima	○ Baixa	○ Média	○ Alta	○ Altíssima
3. Influência no Monitoramento contínuo das instalações para detectar e impedir o acesso físico não autorizado.	○ Nulo	○ Baixíssima	○ Baixa	○ Média	○ Alta	○ Altíssima
4. Influência nas configurações de segurança, hardware, software, serviços e redes, com o fito de que elas sejam estabelecidas, documentadas, implementadas, monitoradas e analisadas criticamente, para que não sejam modificadas por alterações não autorizadas ou incorretas.	○ Nulo	○ Baixíssima	○ Baixa	○ Média	○ Alta	○ Altíssima
5. Influência no monitoramento de comportamentos anômalos e execução de ações apropriadas para avaliar possíveis incidentes de segurança da informação em redes, sistemas e aplicações.	○ Nulo	○ Baixíssima	○ Baixa	○ Média	○ Alta	○ Altíssima
6. Influência na detecção e prevenção da divulgação e extração não autorizadas de informações por indivíduos ou sistemas, prevenindo o vazamento de dados sejam por sistemas, redes, ou quaisquer outros dispositivos que tratem, armazenem ou transmitam informações sensíveis.	○ Nulo	○ Baixíssima	○ Baixa	○ Média	○ Alta	○ Altíssima
7. Influência na proteção dos sistemas para que não sejam comprometidos por malware e impedir o acesso a recursos da web não autorizados, reduzindo a exposição a conteúdos maliciosos.	○ Nulo	○ Baixíssima	○ Baixa	○ Média	○ Alta	○ Altíssima
8. Influência para que o software seja escrito com segurança, reduzindo o número de potenciais vulnerabilidades de segurança da informação, aplicando princípios de codificação segura ao desenvolvimento do software.	○ Nulo	○ Baixíssima	○ Baixa	○ Média	○ Alta	○ Altíssima
9. Influência no quesito de exposição desnecessária de informações sensíveis, estando em compliance com requisitos legais, estatutários, regulamentares e contratuais, excluindo informações armazenadas em sistemas de informação, dispositivos ou qualquer outra mídia de	○ Nulo	○ Baixíssima	○ Baixa	○ Média	○ Alta	○ Altíssima

armazenamento quando não forem mais necessárias.						
10. Influência no mascaramento de dados para que seja usado de acordo com a política específica para o tema da organização, limitando a exposição de dados confidenciais, incluindo dados pessoais, cumprindo os requisitos legais, estatutários, regulamentares e contratuais.	○ Nulo	○ Baixíssima	○ Baixa	○ Média	○ Alta	○ Altíssima

7 - Indique a influência em "**Planejar, implementar, manter e testar a prontidão de TIC, com base nos objetivos de continuidade dos negócios, assegurando a disponibilidade das informações da organização e outros ativos associados durante a disrupção**", nos demais elementos:

1. Influência na coleta e análise das informações relacionadas a ameaças à segurança da informação, produzindo inteligência de ameaças, para que ações de mitigação adequadas possam ser tomadas.	○ Nulo	○ Baixíssima	○ Baixa	○ Média	○ Alta	○ Altíssima
2. Influência na Especificação e gerenciamento da segurança da informação para uso de serviços em nuvem, avaliando processos de aquisição, uso, gestão e saída de serviços.	○ Nulo	○ Baixíssima	○ Baixa	○ Média	○ Alta	○ Altíssima
3. Influência no Monitoramento contínuo das instalações para detectar e impedir o acesso físico não autorizado.	○ Nulo	○ Baixíssima	○ Baixa	○ Média	○ Alta	○ Altíssima
4. Influência nas configurações de segurança, hardware, software, serviços e redes, com o fito de que elas sejam estabelecidas, documentadas, implementadas, monitoradas e analisadas criticamente, para que não sejam modificadas por alterações não autorizadas ou incorretas.	○ Nulo	○ Baixíssima	○ Baixa	○ Média	○ Alta	○ Altíssima
5. Influência no monitoramento de comportamentos anômalos e execução de ações apropriadas para avaliar possíveis incidentes de segurança da informação em redes, sistemas e aplicações.	○ Nulo	○ Baixíssima	○ Baixa	○ Média	○ Alta	○ Altíssima
6. Influência na detecção e prevenção da divulgação e extração não autorizadas de informações por indivíduos ou sistemas, prevenindo o vazamento de dados sejam por sistemas, redes, ou quaisquer outros dispositivos que tratem, armazenem ou transmitam informações sensíveis.	○ Nulo	○ Baixíssima	○ Baixa	○ Média	○ Alta	○ Altíssima
7. Influência na proteção dos sistemas para que não sejam comprometidos por malware e impedir o acesso a recursos da web não autorizados, reduzindo a exposição a conteúdos maliciosos.	○ Nulo	○ Baixíssima	○ Baixa	○ Média	○ Alta	○ Altíssima
8. Influência para que o software seja escrito com segurança, reduzindo o número de potenciais	○ Nulo	○ Baixíssima	○ Baixa	○ Média	○ Alta	○ Altíssima

vulnerabilidades de segurança da informação, aplicando princípios de codificação segura ao desenvolvimento do software.						
9. Influência no quesito de exposição desnecessária de informações sensíveis, estando em compliance com requisitos legais, estatutários, regulamentares e contratuais, excluindo informações armazenadas em sistemas de informação, dispositivos ou qualquer outra mídia de armazenamento quando não forem mais necessárias.	○ Nulo	○ Baixíssima	○ Baixa	○ Média	○ Alta	○ Altíssima
10. Influência no mascaramento de dados para que seja usado de acordo com a política específica para o tema da organização, limitando a exposição de dados confidenciais, incluindo dados pessoais, cumprindo os requisitos legais, estatutários, regulamentares e contratuais.	○ Nulo	○ Baixíssima	○ Baixa	○ Média	○ Alta	○ Altíssima

8 - Indique a influência do "**Monitoramento contínuo das instalações para detectar e impedir o acesso físico não autorizado**", nos demais elementos:

1. Influência na coleta e análise das informações relacionadas a ameaças à segurança da informação, produzindo inteligência de ameaças, para que ações de mitigação adequadas possam ser tomadas.	○ Nulo	○ Baixíssima	○ Baixa	○ Média	○ Alta	○ Altíssima
2. Influência na Especificação e gerenciamento da segurança da informação para uso de serviços em nuvem, avaliando processos de aquisição, uso, gestão e saída de serviços.	○ Nulo	○ Baixíssima	○ Baixa	○ Média	○ Alta	○ Altíssima
3. Influência em Planejar, implementar, manter e testar a prontidão de TIC, com base nos objetivos de continuidade dos negócios, assegurando a disponibilidade das informações da organização e outros ativos associados durante a disrupção.	○ Nulo	○ Baixíssima	○ Baixa	○ Média	○ Alta	○ Altíssima
4. Influência nas configurações de segurança, hardware, software, serviços e redes, com o fito de que elas sejam estabelecidas, documentadas, implementadas, monitoradas e analisadas criticamente, para que não sejam modificadas por alterações não autorizadas ou incorretas.	○ Nulo	○ Baixíssima	○ Baixa	○ Média	○ Alta	○ Altíssima
5. Influência no monitoramento de comportamentos anômalos e execução de ações apropriadas para avaliar possíveis incidentes de segurança da informação em redes, sistemas e aplicações.	○ Nulo	○ Baixíssima	○ Baixa	○ Média	○ Alta	○ Altíssima
6. Influência na detecção e prevenção da divulgação e extração não autorizadas de informações por indivíduos ou sistemas, prevenindo o	○ Nulo	○ Baixíssima	○ Baixa	○ Média	○ Alta	○ Altíssima

vazamento de dados sejam por sistemas, redes, ou quaisquer outros dispositivos que tratem, armazenem ou transmitam informações sensíveis.						
7. Influência na proteção dos sistemas para que não sejam comprometidos por malware e impedir o acesso a recursos da web não autorizados, reduzindo a exposição a conteúdos maliciosos.	○ Nulo	○ Baixíssima	○ Baixa	○ Média	○ Alta	○ Altíssima
8. Influência para que o software seja escrito com segurança, reduzindo o número de potenciais vulnerabilidades de segurança da informação, aplicando princípios de codificação segura ao desenvolvimento do software.	○ Nulo	○ Baixíssima	○ Baixa	○ Média	○ Alta	○ Altíssima
9. Influência no quesito de exposição desnecessária de informações sensíveis, estando em compliance com requisitos legais, estatutários, regulamentares e contratuais, excluindo informações armazenadas em sistemas de informação, dispositivos ou qualquer outra mídia de armazenamento quando não forem mais necessárias.	○ Nulo	○ Baixíssima	○ Baixa	○ Média	○ Alta	○ Altíssima
10. Influência no mascaramento de dados para que seja usado de acordo com a política específica para o tema da organização, limitando a exposição de dados confidenciais, incluindo dados pessoais, cumprindo os requisitos legais, estatutários, regulamentares e contratuais.	○ Nulo	○ Baixíssima	○ Baixa	○ Média	○ Alta	○ Altíssima

9 - Indique a influência de "**Configurações de segurança, hardware, software, serviços e redes, com o fito de que elas sejam estabelecidas, documentadas, implementadas, monitoradas e analisadas criticamente, para que não sejam modificadas por alterações não autorizadas ou incorretas**", nos demais elementos:

1. Influência na coleta e análise das informações relacionadas a ameaças à segurança da informação, produzindo inteligência de ameaças, para que ações de mitigação adequadas possam ser tomadas.	○ Nulo	○ Baixíssima	○ Baixa	○ Média	○ Alta	○ Altíssima
2. Influência na Especificação e gerenciamento da segurança da informação para uso de serviços em nuvem, avaliando processos de aquisição, uso, gestão e saída de serviços.	○ Nulo	○ Baixíssima	○ Baixa	○ Média	○ Alta	○ Altíssima
3. Influência em Planejar, implementar, manter e testar a prontidão de TIC, com base nos objetivos de continuidade dos negócios, assegurando a disponibilidade das informações da organização e outros ativos associados durante a disrupção.	○ Nulo	○ Baixíssima	○ Baixa	○ Média	○ Alta	○ Altíssima
4. Influência no Monitoramento contínuo das instalações para	○ Nulo	○ Baixíssima	○ Baixa	○ Média	○ Alta	○ Altíssima

detectar e impedir o acesso físico não autorizado.						
5. Influência no monitoramento de comportamentos anômalos e execução de ações apropriadas para avaliar possíveis incidentes de segurança da informação em redes, sistemas e aplicações.	○ Nulo	○ Baixíssima	○ Baixa	○ Média	○ Alta	○ Altíssima
6. Influência na detecção e prevenção da divulgação e extração não autorizadas de informações por indivíduos ou sistemas, prevenindo o vazamento de dados sejam por sistemas, redes, ou quaisquer outros dispositivos que tratem, armazenem ou transmitam informações sensíveis.	○ Nulo	○ Baixíssima	○ Baixa	○ Média	○ Alta	○ Altíssima
7. Influência na proteção dos sistemas para que não sejam comprometidos por malware e impedir o acesso a recursos da web não autorizados, reduzindo a exposição a conteúdos maliciosos.	○ Nulo	○ Baixíssima	○ Baixa	○ Média	○ Alta	○ Altíssima
8. Influência para que o software seja escrito com segurança, reduzindo o número de potenciais vulnerabilidades de segurança da informação, aplicando princípios de codificação segura ao desenvolvimento do software.	○ Nulo	○ Baixíssima	○ Baixa	○ Média	○ Alta	○ Altíssima
9. Influência no quesito de exposição desnecessária de informações sensíveis, estando em compliance com requisitos legais, estatutários, regulamentares e contratuais, excluindo informações armazenadas em sistemas de informação, dispositivos ou qualquer outra mídia de armazenamento quando não forem mais necessárias.	○ Nulo	○ Baixíssima	○ Baixa	○ Média	○ Alta	○ Altíssima
10. Influência no mascaramento de dados para que seja usado de acordo com a política específica para o tema da organização, limitando a exposição de dados confidenciais, incluindo dados pessoais, cumprindo os requisitos legais, estatutários, regulamentares e contratuais.	○ Nulo	○ Baixíssima	○ Baixa	○ Média	○ Alta	○ Altíssima

10 - Indique a influência no "**Monitoramento de comportamentos anômalos e execução de ações apropriadas para avaliar possíveis incidentes de segurança da informação em redes, sistemas e aplicações**", nos demais elementos:

1. Influência na coleta e análise das informações relacionadas a ameaças à segurança da informação, produzindo inteligência de ameaças, para que ações de mitigação adequadas possam ser tomadas.	○ Nulo	○ Baixíssima	○ Baixa	○ Média	○ Alta	○ Altíssima
2. Influência na Especificação e gerenciamento da segurança da informação para uso de serviços em nuvem, avaliando processos de aquisição, uso, gestão e saída	○ Nulo	○ Baixíssima	○ Baixa	○ Média	○ Alta	○ Altíssima

de serviços.						
3. Influência em Planejar, implementar, manter e testar a prontidão de TIC, com base nos objetivos de continuidade dos negócios, assegurando a disponibilidade das informações da organização e outros ativos associados durante a disrupção.	○ Nulo	○ Baixíssima	○ Baixa	○ Média	○ Alta	○ Altíssima
4. Influência no Monitoramento contínuo das instalações para detectar e impedir o acesso físico não autorizado.	○ Nulo	○ Baixíssima	○ Baixa	○ Média	○ Alta	○ Altíssima
5. Influência nas configurações de segurança, hardware, software, serviços e redes, com o fito de que elas sejam estabelecidas, documentadas, implementadas, monitoradas e analisadas criticamente, para que não sejam modificadas por alterações não autorizadas ou incorretas.	○ Nulo	○ Baixíssima	○ Baixa	○ Média	○ Alta	○ Altíssima
6. Influência na detecção e prevenção da divulgação e extração não autorizadas de informações por indivíduos ou sistemas, prevenindo o vazamento de dados sejam por sistemas, redes, ou quaisquer outros dispositivos que tratem, armazenem ou transmitam informações sensíveis.	○ Nulo	○ Baixíssima	○ Baixa	○ Média	○ Alta	○ Altíssima
7. Influência na proteção dos sistemas para que não sejam comprometidos por malware e impedir o acesso a recursos da web não autorizados, reduzindo a exposição a conteúdos maliciosos.	○ Nulo	○ Baixíssima	○ Baixa	○ Média	○ Alta	○ Altíssima
8. Influência para que o software seja escrito com segurança, reduzindo o número de potenciais vulnerabilidades de segurança da informação, aplicando princípios de codificação segura ao desenvolvimento do software.	○ Nulo	○ Baixíssima	○ Baixa	○ Média	○ Alta	○ Altíssima
9. Influência no quesito de exposição desnecessária de informações sensíveis, estando em compliance com requisitos legais, estatutários, regulamentares e contratuais, excluindo informações armazenadas em sistemas de informação, dispositivos ou qualquer outra mídia de armazenamento quando não forem mais necessárias.	○ Nulo	○ Baixíssima	○ Baixa	○ Média	○ Alta	○ Altíssima
10. Influência no mascaramento de dados para que seja usado de acordo com a política específica para o tema da organização, limitando a exposição de dados confidenciais, incluindo dados pessoais, cumprindo os requisitos legais, estatutários, regulamentares e contratuais.	○ Nulo	○ Baixíssima	○ Baixa	○ Média	○ Alta	○ Altíssima

11 - Indique a influência da "**Detectação e prevenção da divulgação e extração não autorizadas de informações por indivíduos ou sistemas, prevenindo o vazamento de dados sejam por**

sistemas, redes, ou quaisquer outros dispositivos que tratem, armazenem ou transmitam informações sensíveis", nos demais elementos:

1. Influência na coleta e análise das informações relacionadas a ameaças à segurança da informação, produzindo inteligência de ameaças, para que ações de mitigação adequadas possam ser tomadas.	○ Nulo	○ Baixíssima	○ Baixa	○ Média	○ Alta	○ Altíssima
2. Influência na Especificação e gerenciamento da segurança da informação para uso de serviços em nuvem, avaliando processos de aquisição, uso, gestão e saída de serviços.	○ Nulo	○ Baixíssima	○ Baixa	○ Média	○ Alta	○ Altíssima
3. Influência em Planejar, implementar, manter e testar a prontidão de TIC, com base nos objetivos de continuidade dos negócios, assegurando a disponibilidade das informações da organização e outros ativos associados durante a disrupção.	○ Nulo	○ Baixíssima	○ Baixa	○ Média	○ Alta	○ Altíssima
4. Influência no Monitoramento contínuo das instalações para detectar e impedir o acesso físico não autorizado.	○ Nulo	○ Baixíssima	○ Baixa	○ Média	○ Alta	○ Altíssima
5. Influência nas configurações de segurança, hardware, software, serviços e redes, com o fito de que elas sejam estabelecidas, documentadas, implementadas, monitoradas e analisadas criticamente, para que não sejam modificadas por alterações não autorizadas ou incorretas.	○ Nulo	○ Baixíssima	○ Baixa	○ Média	○ Alta	○ Altíssima
6. Influência no monitoramento de comportamentos anômalos e execução de ações apropriadas para avaliar possíveis incidentes de segurança da informação em redes, sistemas e aplicações.	○ Nulo	○ Baixíssima	○ Baixa	○ Média	○ Alta	○ Altíssima
7. Influência na proteção dos sistemas para que não sejam comprometidos por malware e impedir o acesso a recursos da web não autorizados, reduzindo a exposição a conteúdos maliciosos.	○ Nulo	○ Baixíssima	○ Baixa	○ Média	○ Alta	○ Altíssima
8. Influência para que o software seja escrito com segurança, reduzindo o número de potenciais vulnerabilidades de segurança da informação, aplicando princípios de codificação segura ao desenvolvimento do software.	○ Nulo	○ Baixíssima	○ Baixa	○ Média	○ Alta	○ Altíssima
9. Influência no quesito de exposição desnecessária de informações sensíveis, estando em compliance com requisitos legais, estatutários, regulamentares e contratuais, excluindo informações armazenadas em sistemas de informação, dispositivos ou qualquer outra mídia de armazenamento quando não forem mais necessárias.	○ Nulo	○ Baixíssima	○ Baixa	○ Média	○ Alta	○ Altíssima
10. Influência no mascaramento de dados para que seja usado de						

acordo com a política específica para o tema da organização, limitando a exposição de dados confidenciais, incluindo dados pessoais, cumprindo os requisitos legais, estatutários, regulamentares e contratuais.	○ Nulo	○ Baixíssima	○ Baixa	○ Média	○ Alta	○ Altíssima

12 - Indique a influência da "**Proteção dos sistemas para que não sejam comprometidos por malware e impedir o acesso a recursos da web não autorizados, reduzindo a exposição a conteúdos maliciosos**", nos demais elementos:

1. Influência na coleta e análise das informações relacionadas a ameaças à segurança da informação, produzindo inteligência de ameaças, para que ações de mitigação adequadas possam ser tomadas.	○ Nulo	○ Baixíssima	○ Baixa	○ Média	○ Alta	○ Altíssima
2. Influência na Especificação e gerenciamento da segurança da informação para uso de serviços em nuvem, avaliando processos de aquisição, uso, gestão e saída de serviços.	○ Nulo	○ Baixíssima	○ Baixa	○ Média	○ Alta	○ Altíssima
3. Influência em Planejar, implementar, manter e testar a prontidão de TIC, com base nos objetivos de continuidade dos negócios, assegurando a disponibilidade das informações da organização e outros ativos associados durante a disrupção.	○ Nulo	○ Baixíssima	○ Baixa	○ Média	○ Alta	○ Altíssima
4. Influência no Monitoramento contínuo das instalações para detectar e impedir o acesso físico não autorizado.	○ Nulo	○ Baixíssima	○ Baixa	○ Média	○ Alta	○ Altíssima
5. Influência nas configurações de segurança, hardware, software, serviços e redes, com o fito de que elas sejam estabelecidas, documentadas, implementadas, monitoradas e analisadas criticamente, para que não sejam modificadas por alterações não autorizadas ou incorretas.	○ Nulo	○ Baixíssima	○ Baixa	○ Média	○ Alta	○ Altíssima
6. Influência no monitoramento de comportamentos anômalos e execução de ações apropriadas para avaliar possíveis incidentes de segurança da informação em redes, sistemas e aplicações.	○ Nulo	○ Baixíssima	○ Baixa	○ Média	○ Alta	○ Altíssima
7. Influência na detecção e prevenção da divulgação e extração não autorizadas de informações por indivíduos ou sistemas, prevenindo o vazamento de dados sejam por sistemas, redes, ou quaisquer outros dispositivos que tratem, armazenem ou transmitam informações sensíveis.	○ Nulo	○ Baixíssima	○ Baixa	○ Média	○ Alta	○ Altíssima
8. Influência para que o software seja escrito com segurança, reduzindo o número de potenciais vulnerabilidades de segurança da informação, aplicando princípios de codificação segura ao desenvolvimento do software.	○ Nulo	○ Baixíssima	○ Baixa	○ Média	○ Alta	○ Altíssima

9. Influência no quesito de exposição desnecessária de informações sensíveis, estando em compliance com requisitos legais, estatutários, regulamentares e contratuais, excluindo informações armazenadas em sistemas de informação, dispositivos ou qualquer outra mídia de armazenamento quando não forem mais necessárias.	○ Nulo	○ Baixíssima	○ Baixa	○ Média	○ Alta	○ Altíssima
10. Influência no mascaramento de dados para que seja usado de acordo com a política específica para o tema da organização, limitando a exposição de dados confidenciais, incluindo dados pessoais, cumprindo os requisitos legais, estatutários, regulamentares e contratuais.	○ Nulo	○ Baixíssima	○ Baixa	○ Média	○ Alta	○ Altíssima

13 - Indique a influência da "**Escrita do software com segurança, abordando princípios de codificação segura ao desenvolvimento do software, para reduzir o número de potenciais vulnerabilidades de segurança da informação**", nos demais elementos:

1. Influência na coleta e análise das informações relacionadas a ameaças à segurança da informação, produzindo inteligência de ameaças, para que ações de mitigação adequadas possam ser tomadas.	○ Nulo	○ Baixíssima	○ Baixa	○ Média	○ Alta	○ Altíssima
2. Influência na Especificação e gerenciamento da segurança da informação para uso de serviços em nuvem, avaliando processos de aquisição, uso, gestão e saída de serviços.	○ Nulo	○ Baixíssima	○ Baixa	○ Média	○ Alta	○ Altíssima
3. Influência em Planejar, implementar, manter e testar a prontidão de TIC, com base nos objetivos de continuidade dos negócios, assegurando a disponibilidade das informações da organização e outros ativos associados durante a disrupção.	○ Nulo	○ Baixíssima	○ Baixa	○ Média	○ Alta	○ Altíssima
4. Influência no Monitoramento contínuo das instalações para detectar e impedir o acesso físico não autorizado.	○ Nulo	○ Baixíssima	○ Baixa	○ Média	○ Alta	○ Altíssima
5. Influência nas configurações de segurança, hardware, software, serviços e redes, com o fito de que elas sejam estabelecidas, documentadas, implementadas, monitoradas e analisadas criticamente, para que não sejam modificadas por alterações não autorizadas ou incorretas.	○ Nulo	○ Baixíssima	○ Baixa	○ Média	○ Alta	○ Altíssima
6. Influência no monitoramento de comportamentos anômalos e execução de ações apropriadas para avaliar possíveis incidentes de segurança da informação em redes, sistemas e aplicações.	○ Nulo	○ Baixíssima	○ Baixa	○ Média	○ Alta	○ Altíssima
7. Influência na detecção e prevenção da divulgação e extração não autorizadas de						

informações por indivíduos ou sistemas, prevenindo o vazamento de dados sejam por sistemas, redes, ou quaisquer outros dispositivos que tratem, armazenem ou transmitam informações sensíveis.	○ Nulo	○ Baixíssima	○ Baixa	○ Média	○ Alta	○ Altíssima
8. Influência na proteção dos sistemas para que não sejam comprometidos por malware e impedir o acesso a recursos da web não autorizados, reduzindo a exposição a conteúdos maliciosos.	○ Nulo	○ Baixíssima	○ Baixa	○ Média	○ Alta	○ Altíssima
9. Influência no quesito de exposição desnecessária de informações sensíveis, estando em compliance com requisitos legais, estatutários, regulamentares e contratuais, excluindo informações armazenadas em sistemas de informação, dispositivos ou qualquer outra mídia de armazenamento quando não forem mais necessárias.	○ Nulo	○ Baixíssima	○ Baixa	○ Média	○ Alta	○ Altíssima
10. Influência no mascaramento de dados para que seja usado de acordo com a política específica para o tema da organização, limitando a exposição de dados confidenciais, incluindo dados pessoais, cumprindo os requisitos legais, estatutários, regulamentares e contratuais.	○ Nulo	○ Baixíssima	○ Baixa	○ Média	○ Alta	○ Altíssima

14 - Indique a influência da "**Não exposição desnecessária de informações sensíveis, estando em *compliance* com requisitos legais, estatutários, regulamentares e contratuais, excluindo informações armazenadas em sistemas de informação, dispositivos ou qualquer outra mídia de armazenamento quando não forem mais necessárias.**", nos demais elementos:

1. Influência na coleta e análise das informações relacionadas a ameaças à segurança da informação, produzindo inteligência de ameaças, para que ações de mitigação adequadas possam ser tomadas.	○ Nulo	○ Baixíssima	○ Baixa	○ Média	○ Alta	○ Altíssima
2. Influência na Especificação e gerenciamento da segurança da informação para uso de serviços em nuvem, avaliando processos de aquisição, uso, gestão e saída de serviços.	○ Nulo	○ Baixíssima	○ Baixa	○ Média	○ Alta	○ Altíssima
3. Influência em Planejar, implementar, manter e testar a prontidão de TIC, com base nos objetivos de continuidade dos negócios, assegurando a disponibilidade das informações da organização e outros ativos associados durante a disrupção.	○ Nulo	○ Baixíssima	○ Baixa	○ Média	○ Alta	○ Altíssima
4. Influência no Monitoramento contínuo das instalações para detectar e impedir o acesso físico não autorizado.	○ Nulo	○ Baixíssima	○ Baixa	○ Média	○ Alta	○ Altíssima
5. Influência nas configurações de segurança, hardware, software, serviços e redes, com o fito de						

que elas sejam estabelecidas, documentadas, implementadas, monitoradas e analisadas criticamente, para que não sejam modificadas por alterações não autorizadas ou incorretas.	○ Nulo	○ Baixíssima	○ Baixa	○ Média	○ Alta	○ Altíssima
6. Influência no monitoramento de comportamentos anômalos e execução de ações apropriadas para avaliar possíveis incidentes de segurança da informação em redes, sistemas e aplicações.	○ Nulo	○ Baixíssima	○ Baixa	○ Média	○ Alta	○ Altíssima
7. Influência na detecção e prevenção da divulgação e extração não autorizadas de informações por indivíduos ou sistemas, prevenindo o vazamento de dados sejam por sistemas, redes, ou quaisquer outros dispositivos que tratem, armazenem ou transmitam informações sensíveis.	○ Nulo	○ Baixíssima	○ Baixa	○ Média	○ Alta	○ Altíssima
8. Influência na proteção dos sistemas para que não sejam comprometidos por malware e impedir o acesso a recursos da web não autorizados, reduzindo a exposição a conteúdos maliciosos.	○ Nulo	○ Baixíssima	○ Baixa	○ Média	○ Alta	○ Altíssima
9. Influência para que o software seja escrito com segurança, reduzindo o número de potenciais vulnerabilidades de segurança da informação, aplicando princípios de codificação segura ao desenvolvimento do software.	○ Nulo	○ Baixíssima	○ Baixa	○ Média	○ Alta	○ Altíssima
10. Influência no mascaramento de dados para que seja usado de acordo com a política específica para o tema da organização, limitando a exposição de dados confidenciais, incluindo dados pessoais, cumprindo os requisitos legais, estatutários, regulamentares e contratuais.	○ Nulo	○ Baixíssima	○ Baixa	○ Média	○ Alta	○ Altíssima

15 - Indique a influência da "**Mascaramento de dados para que seja usado de acordo com a política específica para o tema da organização, limitando a exposição de dados confidenciais, incluindo dados pessoais, cumprindo os requisitos legais, estatutários, regulamentares e contratuais.**", nos demais elementos:

1. Influência na coleta e análise das informações relacionadas a ameaças à segurança da informação, produzindo inteligência de ameaças, para que ações de mitigação adequadas possam ser tomadas.	○ Nulo	○ Baixíssima	○ Baixa	○ Média	○ Alta	○ Altíssima
2. Influência na Especificação e gerenciamento da segurança da informação para uso de serviços em nuvem, avaliando processos de aquisição, uso, gestão e saída de serviços.	○ Nulo	○ Baixíssima	○ Baixa	○ Média	○ Alta	○ Altíssima
3. Influência em Planejar, implementar, manter e testar a prontidão de TIC, com base nos objetivos de continuidade dos negócios, assegurando a	○ Nulo	○ Baixíssima	○ Baixa	○ Média	○ Alta	○ Altíssima

disponibilidade das informações da organização e outros ativos associados durante a disrupção.						
4. Influência no Monitoramento contínuo das instalações para detectar e impedir o acesso físico não autorizado.	○ Nulo	○ Baixíssima	○ Baixa	○ Média	○ Alta	○ Altíssima
5. Influência nas configurações de segurança, hardware, software, serviços e redes, com o fito de que elas sejam estabelecidas, documentadas, implementadas, monitoradas e analisadas criticamente, para que não sejam modificadas por alterações não autorizadas ou incorretas.	○ Nulo	○ Baixíssima	○ Baixa	○ Média	○ Alta	○ Altíssima
6. Influência no monitoramento de comportamentos anômalos e execução de ações apropriadas para avaliar possíveis incidentes de segurança da informação em redes, sistemas e aplicações.	○ Nulo	○ Baixíssima	○ Baixa	○ Média	○ Alta	○ Altíssima
7. Influência na detecção e prevenção da divulgação e extração não autorizadas de informações por indivíduos ou sistemas, prevenindo o vazamento de dados sejam por sistemas, redes, ou quaisquer outros dispositivos que tratem, armazenem ou transmitam informações sensíveis.	○ Nulo	○ Baixíssima	○ Baixa	○ Média	○ Alta	○ Altíssima
8. Influência na proteção dos sistemas para que não sejam comprometidos por malware e impedir o acesso a recursos da web não autorizados, reduzindo a exposição a conteúdos maliciosos.	○ Nulo	○ Baixíssima	○ Baixa	○ Média	○ Alta	○ Altíssima
9. Influência para que o software seja escrito com segurança, reduzindo o número de potenciais vulnerabilidades de segurança da informação, aplicando princípios de codificação segura ao desenvolvimento do software.	○ Nulo	○ Baixíssima	○ Baixa	○ Média	○ Alta	○ Altíssima
10. Influência no quesito de exposição desnecessária de informações sensíveis, estando em compliance com requisitos legais, estatutários, regulamentares e contratuais, excluindo informações armazenadas em sistemas de informação, dispositivos ou qualquer outra mídia de armazenamento quando não forem mais necessárias.	○ Nulo	○ Baixíssima	○ Baixa	○ Média	○ Alta	○ Altíssima

ANEXO A - Resultados da avaliação linguística dos critérios

		C1	C3	C4	C5	C6	C7	C8	C9	C10	C11
		VH	VH	VH	VH	VH	VH	VH	VH	VH	VH
		HI	HI	VH	VH	VH	VH	VH	HI	VH	HI
		VH	VH	HI	VH	VH	VH	VH	VH	VH	VH
		HI	HI	VH	HI	VH	HI	HI	HI	HI	HI
		0	M	M	HI	HI	HI	0	LI	0	0
		VH	VH	VH	HI	HI	HI	VH	M	LI	LI
		HI	HI	HI	HI	HI	HI	HI	HI	HI	HI
		VH	VH	VH	VH	VH	VH	VH	VH	VH	VH
		LI	VH	HI	HI	HI	VH	VH	Z	VH	VH
		VH	VH	VH	VH	VH	HI	VH	M	HI	LI
Z2	**C2**	VH	HI	HI	VH	VH	HI	VH	M	M	M
		VH	HI	M	HI	M	HI	HI	HI	HI	HI
		M	HI	M	HI	M	HI	HI	HI	M	M
		LI	HI	LI	M	LI	LI	LI	M	HI	HI
		HI	HI	Z	Z	LI	VH	VH	HI	VH	VH
		VH	VH	VH	VH	VH	VH	VH	VH	HI	HI
		VH	VH	VH	HI	VH	M	M	LI	LI	LI
		VH	VH	VH	VH	HI	HI	VH	VH	VH	VH
		VH	VH	0	M	HI	HI	HI	M	HI	M
		HI	VH	HI	HI	HI	VH	HI	HI	VH	HI
		HI	HI	HI	HI	HI	HI	VH	M	HI	HI
		VH	VH	M	VH	M	VH	VH	VH	HI	VH

		C1	C2	C4	C5	C6	C7	C8	C9	C10	C11
		HI	HI	HI	HI	HI	HI	HI	HI	HI	HI
		HI	HI	VH	VH	VH	VH	VH	HI	HI	HI
		VH	VH	VH	VH	VH	VH	VH	VH	VH	VH
		HI	HI	VH	VH	VH	VH	HI	HI	HI	HI
		0	0	0	HI	HI	0	0	0	0	0
		VH	VH	VH	HI	HI	VH	VH	HI	HI	LI
		HI	VH	HI	VH	HI	VH	HI	HI	HI	HI
		VH	VH	VH	VH	VH	VH	VH	VH	VH	VH
		LI	VH	HI	HI	HI	LI	HI	M	LI	LI
		HI	HI	HI	M	VH	LI	Z	Z	HI	Z
Z3	**C3**	HI	HI	HI	VH	VH	HI	HI	M	M	M
		VH	VH	HI	HI	HI	HI	HI	VH	HI	HI
		M	LI	M	LI	HI	HI	M	LI	LI	LI
		LI	M	LI	LI	LI	M	M	M	LI	M
		LI	LI	HI	HI	HI	HI	HI	VH	Z	HI
		VH	VH	VH	VH	VH	VH	VH	VH	HI	HI
		VH	HI	VH	VH	VH	HI	HI	HI	HI	HI
		HI	VH	VH	VH	VH	VH	VH	VH	HI	VH
		VH	M	HI	LI	VH	VH	HI	M	HI	M
		HI	HI	HI	HI	HI	HI	HI	HI	HI	HI
		HI	HI	HI	M	M	M	VH	M	M	M
		VH	VH	M	VH	VH	VH	VH	VH	VH	VH

		C1	C2	C3	C5	C6	C7	C8	C9	C10	C11
		Z	Z	Z	Z	Z	Z	Z	Z	Z	Z
		HI	HI	HI	HI	VH	VH	VH	HI	HI	VH
		VH	HI	VH	HI	VH	VH	VH	M	VH	M
		VH	VH	VH	VH	VH	VH	VH	VH	VH	VH
		0	0	0	0	0	0	0	0	0	0
		VH	VH	VH	HI	HI	VH	VH	HI	HI	M
		M	M	M	M	LI	VH	LI	Z	HI	LI
		VH	VH	VH	VH	VH	VH	VH	VH	VH	VH
		HI	HI	HI	HI	HI	LI	HI	Z	Z	Z
		VH	VH	VH	VH	VH	VH	VH	LI	Z	Z
Z4	**C4**	HI	VH	HI	VH	VH	HI	HI	M	HI	M
		VH	HI	VH	VH	VH	VH	VH	VH	VH	VH
		LI	Z	Z	LI	M	HI	LI	0	Z	0
		LI	HI	M	M	LI	LI	M	M	LI	M
		0	0	LI	HI	VH	HI	VH	HI	HI	VH
		VH	VH	VH	VH	VH	VH	VH	VH	VH	VH
		VH	HI	VH	VH	VH	HI	VH	M	M	M
		VH	VH	HI	VH	VH	HI	VH	VH	HI	VH
		0	0	LI	LI	VH	0	VH	0	0	0
		HI	LI	M	HI	HI	M	HI	LI	M	0
		LI	LI	LI	LI	LI	LI	LI	LI	LI	LI
		VH	VH	VH	VH	VH	VH	VH	VH	VH	VH

		C1	C2	C3	C4	C6	C7	C8	C9	C10	C11
		Z	Z	Z	Z	Z	Z	Z	Z	Z	Z
		HI	HI	VH	VH	VH	VH	VH	HI	HI	HI
		VH	VH	VH	VH	VH	VH	VH	VH	VH	VH
		HI	HI	HI	HI	HI	HI	HI	HI	HI	HI
		M	HI	HI	0	HI	HI	HI	M	0	0
		VH	VH	VH	HI	HI	VH	VH	HI	HI	M
		LI	M	M	LI	LI	HI	HI	Z	M	M
		VH	VH	VH	VH	VH	VH	VH	VH	VH	VH
		LI	LI	M	HI	HI	LI	HI	Z	Z	Z
		VH	VH	VH	VH	VH	HI	HI	VH	M	M
Z5	**C5**	HI	VH	VH	HI	VH	VH	HI	M	HI	M
		HI	HI	VH	VH	HI	VH	VH	HI	VH	VH
		LI	M	M	Z	HI	HI	HI	LI	HI	M
		LI	M	HI	LI	LI	LI	M	M	LI	M
		HI	HI	VH	VH	VH	VH	VH	HI	LI	HI
		VH	VH	VH	VH	VH	VH	VH	VH	VH	VH
		VH	VH	VH	VH	VH	M	M	M	M	M
		HI	VH	VH	VH	VH	HI	VH	VH	VH	VH
		0	HI	HI	0	VH	VH	VH	VH	VH	HI
		HI	HI	HI	VH	HI	VH	VH	HI	HI	HI
		HI	HI	HI	HI	HI	HI	HI	HI	HI	HI
		VH	VH	VH	VH	VH	VH	VH	VH	VH	LI

		C1	C2	C3	C4	C5	C7	C8	C9	C10	C11
		M	M	M	M	M	M	M	M	M	M
		HI	VH	VH	HI	VH	VH	VH	HI	VH	HI
		VH	VH	VH	VH	VH	VH	VH	VH	VH	VH
		VH	VH	VH	VH	VH	VH	VH	VH	VH	VH
		0	0	LI	0	HI	VH	VH	M	0	0
		VH	VH	VH	HI	HI	VH	VH	HI	HI	M
		HI	M	M	HI	VH	VH	HI	HI	HI	M
		VH	VH	VH	VH	VH	VH	VH	VH	VH	VH
		HI	HI	HI	HI	HI	HI	HI	Z	HI	Z
		VH	VH	VH	VH	VH	VH	VH	VH	VH	M
Z6	**C6**	HI	VH	M	HI	HI	M	M	M	M	M
		VH	VH	VH	VH	VH	VH	VH	VH	VH	VH
		VH	HI	HI	M	M	HI	HI	M	M	LI
		LI	LI	LI	LI	M	LI	LI	M	LI	LI
		HI	HI	M	VH	VH	VH	HI	M	VH	VH
		VH	VH	VH	VH	VH	VH	VH	VH	VH	VH
		VH	HI	VH	VH	VH	HI	HI	HI	VH	M
		VH	VH	VH	HI	VH	VH	VH	VH	VH	VH
		VH	VH	VH	0	M	VH	VH	M	VH	VH
		VH	HI	HI	VH	VH	VH	VH	M	HI	M
		LI	LI	LI	LI	LI	LI	LI	LI	LI	LI
		VH	VH	VH	VH	VH	VH	VH	VH	VH	LI

		C1	C2	C3	C4	C5	C6	C8	C9	C10	C11
		Z	Z	Z	Z	Z	Z	Z	Z	Z	Z
		HI	VH	VH	HI	VH	VH	VH	HI	VH	HI
		VH	VH	VH	VH	VH	VH	VH	VH	VH	VH
		HI	HI	HI	HI	HI	HI	HI	HI	HI	HI
		0	LI	LI	0	HI	HI	0	LI	M	M
		VH	VH	VH	HI	HI	VH	VH	HI	HI	M
		M	HI	M	M	HI	M	HI	LI	HI	M
		VH	VH	VH	VH	VH	VH	VH	VH	VH	VH
		M	VH	LI	HI	HI	HI	HI	Z	VH	HI
		HI	VH	VH	VH	VH	VH	VH	VH	VH	VH
Z7	**C7**	M	HI	M	HI	HI	HI	HI	M	HI	M
		HI	HI	M	VH	VH	VH	VH	VH	VH	HI
		HI	HI	M	LI	M	HI	HI	M	M	M
		LI	LI	M	LI	M	LI	LI	M	LI	LI
		HI	HI	Z	VH	VH	VH	HI	HI	VH	VH
		VH	VH	VH	VH	VH	VH	VH	VH	HI	HI
		VH	VH	HI	VH	M	VH	M	M	M	M
		HI	HI	HI	VH	VH	VH	VH	VH	VH	VH
		VH	VH	VH	0	VH	VH	VH	VH	VH	HI
		HI	HI	HI	VH	VH	VH	HI	HI	HI	HI
		Z	Z	Z	Z	Z	Z	Z	Z	Z	Z
		VH	VH	VH	VH	VH	VH	VH	VH	VH	VH

		C1	C2	C3	C4	C5	C6	C7	C9	C10	C11
		M	M	M	M	M	M	M	M	M	M
		HI	VH	VH	HI	VH	VH	VH	HI	VH	HI
		VH	VH	VH	HI	VH	VH	VH	VH	VH	VH
		HI	HI	HI	HI	HI	HI	HI	HI	HI	HI
		LI	0	0	0	LI	LI	0	0	0	0
		VH	VH	VH	HI	HI	VH	VH	HI	HI	M
		M	VH	HI	HI	VH	M	M	M	HI	M
		VH	VH	VH	VH	VH	VH	VH	VH	VH	VH
		HI	HI	LI	HI	HI	VH	LI	HI	LI	LI
		VH	VH	VH	VH	VH	VH	VH	VH	VH	VH
Z8	**C8**	M	VH	M	HI	HI	HI	HI	M	M	M
		VH	HI	VH	HI	VH	VH	VH	VH	VH	VH
		M	HI	HI	LI	M	M	M	Z	M	Z
		LI	LI	M	LI	M	LI	LI	M	LI	M
		VH	Z	M	0	HI	M	M	HI	HI	Z
		VH	VH	VH	VH	VH	VH	VH	VH	HI	HI
		VH	HI	VH	VH	VH	VH	VH	VH	VH	VH
		VH	VH	VH	VH	VH	HI	HI	HI	HI	HI
		VH	VH	VH	LI	HI	VH	VH	VH	VH	HI
		HI	HI	HI	VH	VH	VH	VH	HI	HI	M
		VH	LI	LI	HI	VH	VH	VH	Z	Z	VH
		VH	VH	VH	VH	VH	VH	VH	VH	VH	VH

		C1	C2	C3	C4	C5	C6	C7	C8	C10	C11
		VH	VH	VH	VH	VH	VH	VH	VH	VH	VH
		HI	VH	VH	HI	VH	VH	VH	HI	VH	HI
		VH	VH	VH	HI	VH	VH	VH	VH	VH	VH
		HI	HI	HI	HI	HI	HI	HI	HI	HI	HI
		Z	M	0	0	M	0	0	0	VH	VH
		VH	VH	VH	HI	HI	VH	VH	HI	HI	M
		HI	HI	VH	VH	VH	HI	M	VH	VH	HI
		VH	VH	VH	VH	VH	VH	VH	VH	VH	VH
		Z	LI	LI	M	LI	LI	HI	HI	HI	LI
		VH	VH	HI	HI	HI	HI	HI	VH	VH	VH
Z9	**C9**	LI	M	M	M	HI	HI	HI	M	M	M
		VH	VH	VH	HI	VH	HI	M	HI	HI	HI
		LI	LI	LI	0	LI	LI	M	HI	HI	M
		LI	M	M	M	M	M	M	M	M	M
		VH	Z	Z	0	M	M	HI	VH	HI	VH
		VH	VH	VH	VH	VH	VH	VH	VH	HI	HI
		VH	VH	HI	VH	VH	HI	VH	VH	VH	VH
		VH	VH	VH	VH	VH	VH	VH	VH	VH	VH
		VH	M	M	0	VH	VH	VH	VH	VH	HI
		VH	VH	VH	VH	VH	VH	VH	VH	VH	VH
		Z	Z	Z	Z	Z	Z	HI	HI	HI	HI
		VH	VH	VH	VH	VH	VH	VH	VH	VH	VH

		C1	C2	C3	C4	C5	C6	C7	C8	C9	C11
		M	M	M	M	M	M	M	M	M	M
		HI	VH	VH	HI	VH	VH	VH	HI	VH	HI
		VH	VH	VH	VH	VH	VH	VH	VH	VH	VH
		HI	HI	HI	HI	HI	HI	HI	HI	HI	HI
		0	HI	0	0	HI	HI	HI	0	VH	VH
		VH	VH	VH	HI	HI	VH	VH	HI	HI	M
		VH	HI	HI	M	LI	LI	M	VH	LI	LI
		VH	VH	VH	VH	VH	VH	VH	VH	VH	VH
		M	HI	LI	HI	HI	HI	HI	HI	HI	VH
		HI	HI	HI	VH	VH	VH	VH	HI	VH	VH
Z10	**C10**	LI	M	M	LI	M	M	M	HI	HI	M
		VH	VH	HI	VH	HI	VH	VH	VH	VH	VH
		HI	M	M	Z	LI	M	M	M	M	LI
		LI	LI	LI	LI	LI	LI	LI	LI	LI	LI
		HI	HI	HI	HI	Z	M	HI	0	0	VH
		HI	HI	HI	HI	HI	HI	HI	HI	HI	HI
		VH	VH	M	M	M	M	VH	VH	VH	M
		VH	VH	VH	VH	VH	VH	VH	VH	VH	VH
		VH	VH	VH	0	HI	VH	VH	VH	VH	VH
		VH	HI	VH	VH	VH	VH	HI	VH	M	M
		Z	Z	Z	Z	Z	Z	Z	Z	Z	Z
		VH	VH	VH	VH	VH	VH	VH	VH	VH	VH

		C1	C2	C3	C4	C5	C6	C7	C8	C9	C10
		HI	HI	HI	HI	HI	HI	HI	HI	HI	HI
		HI	VH	VH	HI	VH	VH	VH	HI	VH	HI
		VH	VH	VH	VH	VH	VH	VH	VH	VH	VH
		HI	HI	HI	HI	HI	HI	HI	HI	HI	HI
		0	0	0	0	0	0	VH	0	VH	VH
		VH	VH	VH	HI	HI	VH	VH	HI	HI	M
		HI	M	M	LI	M	LI	VH	M	LI	VH
		VH	VH	VH	VH	VH	VH	VH	VH	VH	VH
		Z	HI	LI	Z	Z	Z	HI	Z	Z	VH
		0	HI	HI	Z	Z	Z	Z	Z	Z	Z
Z11	**C11**	M	HI	HI	HI	HI	HI	HI	M	HI	VH
		VH	HI	HI	VH	VH	VH	VH	VH	VH	VH
		LI	M	Z	Z	LI	LI	HI	HI	M	HI
		LI	LI	M	LI	M	LI	LI	LI	M	LI
		VH	M	0	0	0	0	HI	0	HI	VH
		HI	HI	HI	HI	HI	HI	HI	HI	HI	HI
		VH	VH	M	M	M	M	VH	M	M	VH
		HI	VH	VH	VH	VH	VH	VH	VH	VH	HI
		0	VH	M	0	M	VH	VH	VH	VH	VH
		VH	VH	HI	VH	VH	VH	VH	VH	VH	VH
		Z	Z	Z	Z	Z	Z	Z	Z	Z	Z
		VH	VH	VH	VH	VH	VH	VH	VH	VH	VH

ANEXO B - Números *fuzzy* triangular correspondentes as avaliações linguísticas

		C1			C3			C4			C5			C6			C7			C8			C9			C10			C11		
		l	m	u	l	m	u	l	m	u	l	m	u	l	m	u	l	m	u	l	m	u	l	m	u	l	m	u	l	m	u
Z2	C2	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1
		0.5	0.75	1	0.5	0.75	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.5	0.75	1	0.75	1	1	0.5	0.75	1
		0.75	1	1	0.75	1	1	0.5	0.75	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1
		0.5	0.75	1	0.5	0.75	1	0.75	1	1	0.5	0.75	1	0.75	1	1	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1
		0	0	0.25	0.25	0.5	0.75	0.25	0.5	0.75	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0	0	0.25	0	0.25	0.5	0	0	0.25	0	0	0.25
		0.75	1	1	0.75	1	1	0.75	1	1	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.75	1	1	0.25	0.5	0.75	0	0.25	0.5	0	0.25	0.5
		0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1
		0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1
		0	0.25	0.5	0.75	1	1	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.75	1	1	0.75	1	1	0	0	0.25	0.75	1	1	0.75	1	1
		0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.5	0.75	1	0.75	1	1	0.25	0.5	0.75	0.5	0.75	1	0	0.25	0.5
		0.75	1	1	0.5	0.75	1	0.5	0.75	1	0.75	1	1	0.75	1	1	0.5	0.75	1	0.75	1	1	0.25	0.5	0.75	0.25	0.5	0.75	0.25	0.5	0.75
		0.75	1	1	0.5	0.75	1	0.25	0.5	0.75	0.5	0.75	1	0.25	0.5	0.75	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1
		0.25	0.5	0.75	0.5	0.75	1	0.25	0.5	0.75	0.5	0.75	1	0.25	0.5	0.75	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.25	0.5	0.75	0.25	0.5	0.75
		0	0.25	0.5	0.5	0.75	1	0	0.25	0.5	0.25	0.5	0.75	0	0.25	0.5	0	0.25	0.5	0	0.25	0.5	0.25	0.5	0.75	0.5	0.75	1	0.5	0.75	1
		0.5	0.75	1	0.5	0.75	1	0	0	0.25	0	0	0.25	0	0.25	0.5	0.75	1	1	0.75	1	1	0.5	0.75	1	0.75	1	1	0.75	1	1
		0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.5	0.75	1	0.5	0.75	1
		0.75	1	1	0.75	1	1	0.75	1	1	0.5	0.75	1	0.75	1	1	0.25	0.5	0.75	0.25	0.5	0.75	0	0.25	0.5	0	0.25	0.5	0	0.25	0.5
		0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.5	0.75	1	0.5	0.75	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1
		0.75	1	1	0.75	1	1	0	0	0.25	0.25	0.5	0.75	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.25	0.5	0.75	0.5	0.75	1	0.25	0.5	0.75
		0.5	0.75	1	0.75	1	1	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.75	1	1	0.5	0.75	1	0.5	0.75	1	0.75	1	1	0.5	0.75	1
		0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.75	1	1	0.25	0.5	0.75	0.5	0.75	1	0.5	0.75	1
		0.75	1	1	0.75	1	1	0.25	0.5	0.75	0.75	1	1	0.25	0.5	0.75	0.75	1	1	0.75	1	1	0.75	1	1	0.5	0.75	1	0.75	1	1

		C2			C3			C4			C5			C6			C7			C8			C9			C10			C11		
		l	m	u	l	m	u	l	m	u	l	m	u	l	m	u	l	m	u	l	m	u	l	m	u	l	m	u	l	m	u
Z3	C3	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1
		0.5	0.75	1	0.5	0.75	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1
		0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1
		0.5	0.75	1	0.5	0.75	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1
		0	0	0.25	0	0	0.25	0	0	0.25	0.5	0.75	1	0.5	0.75	1	0	0	0.25	0	0	0.25	0	0	0.25	0	0	0.25	0	0	0.25
		0.75	1	1	0.75	1	1	0.75	1	1	0.5	0.75	1	0.5	0.75	1	0.75	1	1	0.75	1	1	0.5	0.75	1	0.5	0.75	1	0	0.25	0.5
		0.5	0.75	1	0.75	1	1	0.5	0.75	1	0.75	1	1	0.5	0.75	1	0.75	1	1	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1
		0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1
		0	0.25	0.5	0.75	1	1	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0	0.25	0.5	0.5	0.75	1	0.25	0.5	0.75	0	0.25	0.5	0	0.25	0.5
		0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.25	0.5	0.75	0.75	1	1	0	0.25	0.5	0	0	0.25	0	0	0.25	0.5	0.75	1	0	0	0.25
		0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.75	1	1	0.75	1	1	0.5	0.75	1	0.5	0.75	1	0.25	0.5	0.75	0.25	0.5	0.75	0.25	0.5	0.75
		0.75	1	1	0.75	1	1	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.75	1	1	0.5	0.75	1	0.5	0.75	1
		0.25	0.5	0.75	0	0.25	0.5	0.25	0.5	0.75	0	0.25	0.5	0.5	0.75	1	0.5	0.75	1	0.25	0.5	0.75	0	0.25	0.5	0	0.25	0.5	0	0.25	0.5
		0	0.25	0.5	0.25	0.5	0.75	0	0.25	0.5	0	0.25	0.5	0	0.25	0.5	0.25	0.5	0.75	0.25	0.5	0.75	0.25	0.5	0.75	0	0.25	0.5	0.25	0.5	0.75
		0	0.25	0.5	0	0.25	0.5	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.75	1	1	0	0	0.25	0.5	0.75	1
		0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.5	0.75	1	0.5	0.75	1
		0.75	1	1	0.5	0.75	1	0.75	1	1	0.75	1	1	0.75	1	1	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1
		0.5	0.75	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.5	0.75	1	0.75	1	1
		0.75	1	1	0.25	0.5	0.75	0.5	0.75	1	0	0.25	0.5	0.75	1	1	0.75	1	1	0.5	0.75	1	0.25	0.5	0.75	0.5	0.75	1	0.25	0.5	0.75
		0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1
		0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.25	0.5	0.75	0.25	0.5	0.75	0.25	0.5	0.75	0.75	1	1	0.25	0.5	0.75	0.25	0.5	0.75	0.25	0.5	0.75
		0.75	1	1	0.75	1	1	0.25	0.5	0.75	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1

		C2			C3			C4			C5			C6			C7			C8			C9			C10			C11		
		l	m	u	l	m	u	l	m	u	l	m	u	l	m	u	l	m	u	l	m	u	l	m	u	l	m	u	l	m	u
		0	0	0.25	0	0	0.25	0	0	0.25	0	0	0.25	0	0	0.25	0	0	0.25	0	0	0.25	0	0	0.25	0	0	0.25	0	0	0.25
		0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.75	1	1	0.75	1	1	0.75	1	1	0.5	0.75	1	0.5	0.75	1	0.75	1	1
		0.75	1	1	0.5	0.75	1	0.75	1	1	0.5	0.75	1	0.75	1	1	0.75	1	1	0.75	1	1	0.25	0.5	0.75	0.75	1	1	0.25	0.5	0.75
		0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1
		0	0	0.25	0	0	0.25	0	0	0.25	0	0	0.25	0	0	0.25	0	0	0.25	0	0	0.25	0	0	0.25	0	0	0.25	0	0	0.25
		0.75	1	1	0.75	1	1	0.75	1	1	0.5	0.75	1	0.5	0.75	1	0.75	1	1	0.75	1	1	0.5	0.75	1	0.5	0.75	1	0.25	0.5	0.75
		0.25	0.5	0.75	0.25	0.5	0.75	0.25	0.5	0.75	0.25	0.5	0.75	0	0.25	0.5	0.75	1	1	0	0.25	0.5	0	0	0.25	0.5	0.75	1	0	0.25	0.5
		0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1
		0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0	0.25	0.5	0.5	0.75	1	0	0	0.25	0	0	0.25	0	0	0.25
Z4	C4	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0	0.25	0.5	0	0	0.25	0	0	0.25
		0.5	0.75	1	0.75	1	1	0.5	0.75	1	0.75	1	1	0.75	1	1	0.5	0.75	1	0.5	0.75	1	0.25	0.5	0.75	0.5	0.75	1	0.25	0.5	0.75
		0.75	1	1	0.5	0.75	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1
		0	0.25	0.5	0	0	0.25	0	0	0.25	0	0.25	0.5	0.25	0.5	0.75	0.5	0.75	1	0	0.25	0.5	0	0	0.25	0	0	0.25	0	0	0.25
		0	0.25	0.5	0.5	0.75	1	0.25	0.5	0.75	0.25	0.5	0.75	0	0.25	0.5	0	0.25	0.5	0.25	0.5	0.75	0.25	0.5	0.75	0	0.25	0.5	0.25	0.5	0.75
		0	0	0.25	0	0	0.25	0	0.25	0.5	0.5	0.75	1	0.75	1	1	0.5	0.75	1	0.75	1	1	0.5	0.75	1	0.5	0.75	1	0.75	1	1
		0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1
		0.75	1	1	0.5	0.75	1	0.75	1	1	0.75	1	1	0.75	1	1	0.5	0.75	1	0.75	1	1	0.25	0.5	0.75	0.25	0.5	0.75	0.25	0.5	0.75
		0.75	1	1	0.75	1	1	0.5	0.75	1	0.75	1	1	0.75	1	1	0.5	0.75	1	0.75	1	1	0.75	1	1	0.5	0.75	1	0.75	1	1
		0	0	0.25	0	0	0.25	0	0.25	0.5	0	0.25	0.5	0.75	1	1	0	0	0.25	0.75	1	1	0	0	0.25	0	0	0.25	0	0	0.25
		0.5	0.75	1	0	0.25	0.5	0.25	0.5	0.75	0.5	0.75	1	0.5	0.75	1	0.25	0.5	0.75	0.5	0.75	1	0	0.25	0.5	0.25	0.5	0.75	0	0	0.25
		0	0.25	0.5	0	0.25	0.5	0	0.25	0.5	0	0.25	0.5	0	0.25	0.5	0	0.25	0.5	0	0.25	0.5	0	0.25	0.5	0	0.25	0.5	0	0.25	0.5
		0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1

		C2			C3			C4			C5			C6			C7			C8			C9			C10			C11		
		l	m	u	l	m	u	l	m	u	l	m	u	l	m	u	l	m	u	l	m	u	l	m	u	l	m	u	l	m	u
		0	0	0.25	0	0	0.25	0	0	0.25	0	0	0.25	0	0	0.25	0	0	0.25	0	0	0.25	0	0	0.25	0	0	0.25	0	0	0.25
		0.5	0.75	1	0.5	0.75	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1
		0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1
		0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1
		0.25	0.5	0.75	0.5	0.75	1	0.5	0.75	1	0	0	0.25	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.25	0.5	0.75	0	0	0.25	0	0	0.25
		0.75	1	1	0.75	1	1	0.75	1	1	0.5	0.75	1	0.5	0.75	1	0.75	1	1	0.75	1	1	0.5	0.75	1	0.5	0.75	1	0.25	0.5	0.75
		0	0.25	0.5	0.25	0.5	0.75	0.25	0.5	0.75	0	0.25	0.5	0	0.25	0.5	0.5	0.75	1	0.5	0.75	1	0	0	0.25	0.25	0.5	0.75	0.25	0.5	0.75
		0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1
		0	0.25	0.5	0	0.25	0.5	0.25	0.5	0.75	0.5	0.75	1	0.5	0.75	1	0	0.25	0.5	0.5	0.75	1	0	0	0.25	0	0	0.25	0	0	0.25
		0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.5	0.75	1	0.5	0.75	1	0.75	1	1	0.25	0.5	0.75	0.25	0.5	0.75
Z5	C5	0.5	0.75	1	0.75	1	1	0.75	1	1	0.5	0.75	1	0.75	1	1	0.75	1	1	0.5	0.75	1	0.25	0.5	0.75	0.5	0.75	1	0.25	0.5	0.75
		0.5	0.75	1	0.5	0.75	1	0.75	1	1	0.75	1	1	0.5	0.75	1	0.75	1	1	0.75	1	1	0.5	0.75	1	0.75	1	1	0.75	1	1
		0	0.25	0.5	0.25	0.5	0.75	0.25	0.5	0.75	0	0	0.25	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0	0.25	0.5	0.5	0.75	1	0.25	0.5	0.75
		0	0.25	0.5	0.25	0.5	0.75	0.5	0.75	1	0	0.25	0.5	0	0.25	0.5	0	0.25	0.5	0.25	0.5	0.75	0.25	0.5	0.75	0	0.25	0.5	0.25	0.5	0.75
		0.5	0.75	1	0.5	0.75	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.5	0.75	1	0	0.25	0.5	0.5	0.75	1
		0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1
		0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.25	0.5	0.75	0.25	0.5	0.75	0.25	0.5	0.75	0.25	0.5	0.75	0.25	0.5	0.75
		0.5	0.75	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.5	0.75	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1
		0	0	0.25	0.5	0.75	1	0.5	0.75	1	0	0	0.25	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.5	0.75	1
		0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.75	1	1	0.5	0.75	1	0.75	1	1	0.75	1	1	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1
		0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1
		0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0	0.25	0.5

		C2			C3			C4			C5			C6			C7			C8			C9			C10			C11		
		l	m	u	l	m	u	l	m	u	l	m	u	l	m	u	l	m	u	l	m	u	l	m	u	l	m	u	l	m	u
Z6	C6	0.25	0.5	0.75	0.25	0.5	0.75	0.25	0.5	0.75	0.25	0.5	0.75	0.25	0.5	0.75	0.25	0.5	0.75	0.25	0.5	0.75	0.25	0.5	0.75	0.25	0.5	0.75	0.25	0.5	0.75
		0.5	0.75	1	0.75	1	1	0.75	1	1	0.5	0.75	1	0.75	1	1	0.75	1	1	0.75	1	1	0.5	0.75	1	0.75	1	1	0.5	0.75	1
		0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1
		0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1
		0	0	0.25	0	0	0.25	0	0.25	0.5	0	0	0.25	0.5	0.75	1	0.75	1	1	0.75	1	1	0.25	0.5	0.75	0	0	0.25	0	0	0.25
		0.75	1	1	0.75	1	1	0.75	1	1	0.5	0.75	1	0.5	0.75	1	0.75	1	1	0.75	1	1	0.5	0.75	1	0.5	0.75	1	0.25	0.5	0.75
		0.5	0.75	1	0.25	0.5	0.75	0.25	0.5	0.75	0.5	0.75	1	0.75	1	1	0.75	1	1	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.25	0.5	0.75
		0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1
		0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0	0	0.25	0.5	0.75	1	0	0	0.25
		0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.25	0.5	0.75
		0.5	0.75	1	0.75	1	1	0.25	0.5	0.75	0.5	0.75	1	0.5	0.75	1	0.25	0.5	0.75	0.25	0.5	0.75	0.25	0.5	0.75	0.25	0.5	0.75	0.25	0.5	0.75
		0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1
		0.75	1	1	0.5	0.75	1	0.5	0.75	1	0.25	0.5	0.75	0.25	0.5	0.75	0.5	0.75	1	0.5	0.75	1	0.25	0.5	0.75	0.25	0.5	0.75	0	0.25	0.5
		0	0.25	0.5	0	0.25	0.5	0	0.25	0.5	0	0.25	0.5	0.25	0.5	0.75	0	0.25	0.5	0	0.25	0.5	0.25	0.5	0.75	0	0.25	0.5	0	0.25	0.5
		0.5	0.75	1	0.5	0.75	1	0.25	0.5	0.75	0.75	1	1	0.75	1	1	0.75	1	1	0.5	0.75	1	0.25	0.5	0.75	0.75	1	1	0.75	1	1
		0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1
		0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.75	1	1	0.25	0.5	0.75
		0.75	1	1	0.75	1	1	0.75	1	1	0.5	0.75	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1
		0.75	1	1	0.75	1	1	0.75	1	1	0	0	0.25	0.25	0.5	0.75	0.75	1	1	0.75	1	1	0.25	0.5	0.75	0.75	1	1	0.75	1	1
		0.75	1	1	0.5	0.75	1	0.5	0.75	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.25	0.5	0.75	0.5	0.75	1	0.25	0.5	0.75
		0	0.25	0.5	0	0.25	0.5	0	0.25	0.5	0	0.25	0.5	0	0.25	0.5	0	0.25	0.5	0	0.25	0.5	0	0.25	0.5	0	0.25	0.5	0	0.25	0.5
		0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0	0.25	0.5

		C2			C3			C4			C5			C6			C7			C8			C9			C10			C11		
		l	m	u	l	m	u	l	m	u	l	m	u	l	m	u	l	m	u	l	m	u	l	m	u	l	m	u	l	m	u
Z7	C7	0	0	0.25	0	0	0.25	0	0	0.25	0	0	0.25	0	0	0.25	0	0	0.25	0	0	0.25	0	0	0.25	0	0	0.25	0	0	0.25
		0.5	0.75	1	0.75	1	1	0.75	1	1	0.5	0.75	1	0.75	1	1	0.75	1	1	0.75	1	1	0.5	0.75	1	0.75	1	1	0.5	0.75	1
		0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1
		0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1
		0	0	0.25	0	0.25	0.5	0	0.25	0.5	0	0	0.25	0.5	0.75	1	0.5	0.75	1	0	0	0.25	0	0.25	0.5	0.25	0.5	0.75	0.25	0.5	0.75
		0.75	1	1	0.75	1	1	0.75	1	1	0.5	0.75	1	0.5	0.75	1	0.75	1	1	0.75	1	1	0.5	0.75	1	0.5	0.75	1	0.25	0.5	0.75
		0.25	0.5	0.75	0.5	0.75	1	0.25	0.5	0.75	0.25	0.5	0.75	0.5	0.75	1	0.25	0.5	0.75	0.5	0.75	1	0	0.25	0.5	0.5	0.75	1	0.25	0.5	0.75
		0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1
		0.25	0.5	0.75	0.75	1	1	0	0.25	0.5	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0	0	0.25	0.75	1	1	0.5	0.75	1
		0.5	0.75	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1
		0.25	0.5	0.75	0.5	0.75	1	0.25	0.5	0.75	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.25	0.5	0.75	0.5	0.75	1	0.25	0.5	0.75
		0.5	0.75	1	0.5	0.75	1	0.25	0.5	0.75	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.5	0.75	1
		0.5	0.75	1	0.5	0.75	1	0.25	0.5	0.75	0	0.25	0.5	0.25	0.5	0.75	0.5	0.75	1	0.5	0.75	1	0.25	0.5	0.75	0.25	0.5	0.75	0.25	0.5	0.75
		0	0.25	0.5	0	0.25	0.5	0.25	0.5	0.75	0	0.25	0.5	0.25	0.5	0.75	0	0.25	0.5	0	0.25	0.5	0.25	0.5	0.75	0	0.25	0.5	0	0.25	0.5
		0.5	0.75	1	0.5	0.75	1	0	0	0.25	0.75	1	1	0.75	1	1	0.75	1	1	0.5	0.75	1	0.5	0.75	1	0.75	1	1	0.75	1	1
		0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.5	0.75	1	0.5	0.75	1
		0.75	1	1	0.75	1	1	0.5	0.75	1	0.75	1	1	0.25	0.5	0.75	0.75	1	1	0.25	0.5	0.75	0.25	0.5	0.75	0.25	0.5	0.75	0.25	0.5	0.75
		0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1
		0.75	1	1	0.75	1	1	0.75	1	1	0	0	0.25	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.5	0.75	1
		0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.75	1	1	0.75	1	1	0.75	1	1	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1
		0	0	0.25	0	0	0.25	0	0	0.25	0	0	0.25	0	0	0.25	0	0	0.25	0	0	0.25	0	0	0.25	0	0	0.25	0	0	0.25
		0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1

		C2			C3			C4			C5			C6			C7			C8			C9			C10			C11		
		l	m	u	l	m	u	l	m	u	l	m	u	l	m	u	l	m	u	l	m	u	l	m	u	l	m	u	l	m	u
Z8	C8	0.25	0.5	0.75	0.25	0.5	0.75	0.25	0.5	0.75	0.25	0.5	0.75	0.25	0.5	0.75	0.25	0.5	0.75	0.25	0.5	0.75	0.25	0.5	0.75	0.25	0.5	0.75	0.25	0.5	0.75
		0.5	0.75	1	0.75	1	1	0.75	1	1	0.5	0.75	1	0.75	1	1	0.75	1	1	0.75	1	1	0.5	0.75	1	0.75	1	1	0.5	0.75	1
		0.75	1	1	0.75	1	1	0.75	1	1	0.5	0.75	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1
		0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1
		0	0.25	0.5	0	0	0.25	0	0	0.25	0	0	0.25	0	0.25	0.5	0	0.25	0.5	0	0	0.25	0	0	0.25	0	0	0.25	0	0	0.25
		0.75	1	1	0.75	1	1	0.75	1	1	0.5	0.75	1	0.5	0.75	1	0.75	1	1	0.75	1	1	0.5	0.75	1	0.5	0.75	1	0.25	0.5	0.75
		0.25	0.5	0.75	0.75	1	1	0.5	0.75	1	0.5	0.75	1	0.75	1	1	0.25	0.5	0.75	0.25	0.5	0.75	0.25	0.5	0.75	0.5	0.75	1	0.25	0.5	0.75
		0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1
		0.5	0.75	1	0.5	0.75	1	0	0.25	0.5	0.5	0.75	1	0.5	0.75	1	0.75	1	1	0	0.25	0.5	0.5	0.75	1	0	0.25	0.5	0	0.25	0.5
		0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1
		0.25	0.5	0.75	0.75	1	1	0.25	0.5	0.75	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.25	0.5	0.75	0.25	0.5	0.75	0.25	0.5	0.75
		0.75	1	1	0.5	0.75	1	0.75	1	1	0.5	0.75	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1
		0.25	0.5	0.75	0.5	0.75	1	0.5	0.75	1	0	0.25	0.5	0.25	0.5	0.75	0.25	0.5	0.75	0.25	0.5	0.75	0	0	0.25	0.25	0.5	0.75	0	0	0.25
		0	0.25	0.5	0	0.25	0.5	0.25	0.5	0.75	0	0.25	0.5	0.25	0.5	0.75	0	0.25	0.5	0	0.25	0.5	0.25	0.5	0.75	0	0.25	0.5	0.25	0.5	0.75
		0.75	1	1	0	0	0.25	0.25	0.5	0.75	0	0	0.25	0.5	0.75	1	0.25	0.5	0.75	0.25	0.5	0.75	0.5	0.75	1	0.5	0.75	1	0	0	0.25
		0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.5	0.75	1	0.5	0.75	1
		0.75	1	1	0.5	0.75	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1
		0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1
		0.75	1	1	0.75	1	1	0.75	1	1	0	0.25	0.5	0.5	0.75	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.5	0.75	1
		0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.5	0.75	1	0.5	0.75	1	0.25	0.5	0.75
		0.75	1	1	0	0.25	0.5	0	0.25	0.5	0.5	0.75	1	0.75	1	1	0.75	1	1	0.75	1	1	0	0	0.25	0	0	0.25	0.75	1	1
		0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1

		C2			C3			C4			C5			C6			C7			C8			C9			C10			C11		
		l	m	u	l	m	u	l	m	u	l	m	u	l	m	u	l	m	u	l	m	u	l	m	u	l	m	u	l	m	u
Z9	C9	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1
		0.5	0.75	1	0.75	1	1	0.75	1	1	0.5	0.75	1	0.75	1	1	0.75	1	1	0.75	1	1	0.5	0.75	1	0.75	1	1	0.5	0.75	1
		0.75	1	1	0.75	1	1	0.75	1	1	0.5	0.75	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1
		0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1
		0	0	0.25	0.25	0.5	0.75	0	0	0.25	0	0	0.25	0.25	0.5	0.75	0	0	0.25	0	0	0.25	0	0	0.25	0.75	1	1	0.75	1	1
		0.75	1	1	0.75	1	1	0.75	1	1	0.5	0.75	1	0.5	0.75	1	0.75	1	1	0.75	1	1	0.5	0.75	1	0.5	0.75	1	0.25	0.5	0.75
		0.5	0.75	1	0.5	0.75	1	0.75	1	1	0.75	1	1	0.75	1	1	0.5	0.75	1	0.25	0.5	0.75	0.75	1	1	0.75	1	1	0.5	0.75	1
		0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1
		0	0	0.25	0	0.25	0.5	0	0.25	0.5	0.25	0.5	0.75	0	0.25	0.5	0	0.25	0.5	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0	0.25	0.5
		0.75	1	1	0.75	1	1	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.75	1	1	0.75	1	1	0.75	1	1
		0	0.25	0.5	0.25	0.5	0.75	0.25	0.5	0.75	0.25	0.5	0.75	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.25	0.5	0.75	0.25	0.5	0.75	0.25	0.5	0.75
		0.75	1	1	0.75	1	1	0.75	1	1	0.5	0.75	1	0.75	1	1	0.5	0.75	1	0.25	0.5	0.75	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1
		0	0.25	0.5	0	0.25	0.5	0	0.25	0.5	0	0	0.25	0	0.25	0.5	0	0.25	0.5	0.25	0.5	0.75	0.5	0.75	1	0.5	0.75	1	0.25	0.5	0.75
		0	0.25	0.5	0.25	0.5	0.75	0.25	0.5	0.75	0.25	0.5	0.75	0.25	0.5	0.75	0.25	0.5	0.75	0.25	0.5	0.75	0.25	0.5	0.75	0.25	0.5	0.75	0.25	0.5	0.75
		0.75	1	1	0	0	0.25	0	0	0.25	0	0	0.25	0.25	0.5	0.75	0.25	0.5	0.75	0.5	0.75	1	0.75	1	1	0.5	0.75	1	0.75	1	1
		0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.5	0.75	1	0.5	0.75	1
		0.75	1	1	0.75	1	1	0.5	0.75	1	0.75	1	1	0.75	1	1	0.5	0.75	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1
		0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1
		0.75	1	1	0.25	0.5	0.75	0.25	0.5	0.75	0	0	0.25	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.5	0.75	1
		0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1
		0	0	0.25	0	0	0.25	0	0	0.25	0	0	0.25	0	0	0.25	0	0	0.25	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1
		0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1

		C2			C3			C4			C5			C6			C7			C8			C9			C10			C11		
		l	m	u	l	m	u	l	m	u	l	m	u	l	m	u	l	m	u	l	m	u	l	m	u	l	m	u	l	m	u
Z10	C10	0.25	0.5	0.75	0.25	0.5	0.75	0.25	0.5	0.75	0.25	0.5	0.75	0.25	0.5	0.75	0.25	0.5	0.75	0.25	0.5	0.75	0.25	0.5	0.75	0.25	0.5	0.75	0.25	0.5	0.75
		0.5	0.75	1	0.75	1	1	0.75	1	1	0.5	0.75	1	0.75	1	1	0.75	1	1	0.75	1	1	0.5	0.75	1	0.75	1	1	0.5	0.75	1
		0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1
		0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1
		0	0	0.25	0.5	0.75	1	0	0	0.25	0	0	0.25	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0	0	0.25	0.75	1	1	0.75	1	1
		0.75	1	1	0.75	1	1	0.75	1	1	0.5	0.75	1	0.5	0.75	1	0.75	1	1	0.75	1	1	0.5	0.75	1	0.5	0.75	1	0.25	0.5	0.75
		0.75	1	1	0.5	0.75	1	0.5	0.75	1	0.25	0.5	0.75	0	0.25	0.5	0	0.25	0.5	0.25	0.5	0.75	0.75	1	1	0	0.25	0.5	0	0.25	0.5
		0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1
		0.25	0.5	0.75	0.5	0.75	1	0	0.25	0.5	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.75	1	1
		0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.5	0.75	1	0.75	1	1	0.75	1	1
		0	0.25	0.5	0.25	0.5	0.75	0.25	0.5	0.75	0	0.25	0.5	0.25	0.5	0.75	0.25	0.5	0.75	0.25	0.5	0.75	0.5	0.75	1	0.5	0.75	1	0.25	0.5	0.75
		0.75	1	1	0.75	1	1	0.5	0.75	1	0.75	1	1	0.5	0.75	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1
		0.5	0.75	1	0.25	0.5	0.75	0.25	0.5	0.75	0	0	0.25	0	0.25	0.5	0.25	0.5	0.75	0.25	0.5	0.75	0.25	0.5	0.75	0.25	0.5	0.75	0	0.25	0.5
		0	0.25	0.5	0	0.25	0.5	0	0.25	0.5	0	0.25	0.5	0	0.25	0.5	0	0.25	0.5	0	0.25	0.5	0	0.25	0.5	0	0.25	0.5	0	0.25	0.5
		0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0	0	0.25	0.25	0.5	0.75	0.5	0.75	1	0	0	0.25	0	0	0.25	0.75	1	1
		0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1
		0.75	1	1	0.75	1	1	0.25	0.5	0.75	0.25	0.5	0.75	0.25	0.5	0.75	0.25	0.5	0.75	0.75	1	1	0.75	1	1	0.75	1	1	0.25	0.5	0.75
		0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1
		0.75	1	1	0.75	1	1	0.75	1	1	0	0	0.25	0.5	0.75	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1
		0.75	1	1	0.5	0.75	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.5	0.75	1	0.75	1	1	0.25	0.5	0.75	0.25	0.5	0.75
		0	0	0.25	0	0	0.25	0	0	0.25	0	0	0.25	0	0	0.25	0	0	0.25	0	0	0.25	0	0	0.25	0	0	0.25	0	0	0.25
		0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1

		C2			C3			C4			C5			C6			C7			C8			C9			C10			C11		
		l	m	u	l	m	u	l	m	u	l	m	u	l	m	u	l	m	u	l	m	u	l	m	u	l	m	u	l	m	u
Z11	C11	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1
		0.5	0.75	1	0.75	1	1	0.75	1	1	0.5	0.75	1	0.75	1	1	0.75	1	1	0.75	1	1	0.5	0.75	1	0.75	1	1	0.5	0.75	1
		0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1
		0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1
		0	0	0.25	0	0	0.25	0	0	0.25	0	0	0.25	0	0	0.25	0	0	0.25	0.75	1	1	0	0	0.25	0.75	1	1	0.75	1	1
		0.75	1	1	0.75	1	1	0.75	1	1	0.5	0.75	1	0.5	0.75	1	0.75	1	1	0.75	1	1	0.5	0.75	1	0.5	0.75	1	0.25	0.5	0.75
		0.5	0.75	1	0.25	0.5	0.75	0.25	0.5	0.75	0	0.25	0.5	0.25	0.5	0.75	0	0.25	0.5	0.75	1	1	0.25	0.5	0.75	0	0.25	0.5	0.75	1	1
		0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1
		0	0	0.25	0.5	0.75	1	0	0.25	0.5	0	0	0.25	0	0	0.25	0	0	0.25	0.5	0.75	1	0	0	0.25	0	0	0.25	0.75	1	1
		0	0	0.25	0.5	0.75	1	0.5	0.75	1	0	0	0.25	0	0	0.25	0	0	0.25	0	0	0.25	0	0	0.25	0	0	0.25	0	0	0.25
		0.25	0.5	0.75	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.25	0.5	0.75	0.5	0.75	1	0.75	1	1
		0.75	1	1	0.5	0.75	1	0.5	0.75	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1
		0	0.25	0.5	0.25	0.5	0.75	0	0	0.25	0	0	0.25	0	0.25	0.5	0	0.25	0.5	0.5	0.75	1	0.5	0.75	1	0.25	0.5	0.75	0.5	0.75	1
		0	0.25	0.5	0	0.25	0.5	0.25	0.5	0.75	0	0.25	0.5	0.25	0.5	0.75	0	0.25	0.5	0	0.25	0.5	0	0.25	0.5	0.25	0.5	0.75	0	0.25	0.5
		0.75	1	1	0.25	0.5	0.75	0	0	0.25	0	0	0.25	0	0	0.25	0	0	0.25	0.5	0.75	1	0	0	0.25	0.5	0.75	1	0.75	1	1
		0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1	0.5	0.75	1
		0.75	1	1	0.75	1	1	0.25	0.5	0.75	0.25	0.5	0.75	0.25	0.5	0.75	0.25	0.5	0.75	0.75	1	1	0.25	0.5	0.75	0.25	0.5	0.75	0.75	1	1
		0.5	0.75	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.5	0.75	1
		0	0	0.25	0.75	1	1	0.25	0.5	0.75	0	0	0.25	0.25	0.5	0.75	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1
		0.75	1	1	0.75	1	1	0.5	0.75	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1
		0	0	0.25	0	0	0.25	0	0	0.25	0	0	0.25	0	0	0.25	0	0	0.25	0	0	0.25	0	0	0.25	0	0	0.25	0	0	0.25
		0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1	0.75	1	1

ANEXO C - Autorização do Comitê de Ética em Pesquisa

UNIVERSIDADE ESTADUAL DE CAMPINAS - UNICAMP/CAMPUS CAMPINAS

PARECER CONSUBSTANCIADO DO CEP

DADOS DO PROJETO DE PESQUISA

Título da Pesquisa: Análise dos novos controles evidenciados pela ISO 27001:2022 com uso do Fuzzy Cognitive Maps
Pesquisador: JEFFERSON DE SOUZA PINTO
Área Temática:
Versão: 1
CAAE: 74829723.3.0000.5404
Instituição Proponente: Faculdade de Engenharia Mecânica
Patrocinador Principal: Financiamento Próprio

DADOS DO PARECER

Número do Parecer: 6.477.629

Apresentação do Projeto:
As informações contidas nos campos "Apresentação do Projeto", "Objetivo da Pesquisa" e "Avaliação dos Riscos e Benefícios" foram obtidas dos documentos apresentados para apreciação ética e das informações inseridas pelo Pesquisador Responsável do estudo na Plataforma Brasil.

Introdução:
A norma ISO/IEC 27000 teve como origem o Padrão Britânico (British Standard) BS 7799ª, que foi publicado em 1995, o qual foi escrito pelo Departamento de Indústria e Comércio do Governo do Reino Unido, e abordava, na sua primeira parte, as melhores práticas para o Gerenciamento de Segurança da Informação (CALDER e WATKINS, 2005, p. 35). Sua estrutura ISO/IEC 27000 fornece uma introdução e visão geral sobre a família ISO 27000, com definições e vocabulários claros sobre o Sistema de Gestão de Segurança da Informação (SGSI), a qual contempla em seu arcabouço as normas ABNT ISO/IEC 27001 e ABNT ISO/IEC 27002, dentre outras.A ISO/IEC 27001 é o padrão mais conhecido do mundo para Sistemas de Gerenciamento de Segurança da Informação (ISO 27001,2022), a qual define requisitos que um SGSI deve atender para mitigar os riscos relacionados à segurança cibernética.Publicada pela primeira vez em 2005, a referida norma passou por duas revisões, em que a primeira foi realizada no ano de 2013 e a segunda no ano de 2022, esta última abrangendo mudanças expressivas em relação a sua versão anterior.A primeira mudança ocorrida foi no título da referida norma, o qual passou a ser denominado "Segurança da

Endereço: Rua Tessália Vieira de Camargo, 126, 1° andar do Prédio I da Faculdade de Ciências Médicas
Bairro: Barão Geraldo **CEP:** 13.083-887
UF: SP **Município:** CAMPINAS
Telefone: (19)3521-8936 **Fax:** (19)3521-7187 **E-mail:** cep@unicamp.br

Informação, Cibersegurança e Proteção da Privacidade - Sistemas de Gestão da Segurança da Informação – Requisitos", se alinhando ao contido na ISO/IEC 27002:2022.Além disso, novas cláusulas foram introduzidas em sua estrutura, com o fito de harmonizar o documento frente a outras normas de sistema de gestão, tal como a ISO 22301:2019.Outra mudança expressiva foi no Anexo A da ISO/IEC 27001:2022, que traz o referencial de controles de segurança da informação. Alguns desses controles foram fundidos entre si, vinte e três foram renomeados, cinquenta e sete aglutinados em vinte e quatro, e um controle dividido em dois.Com a ocorrência dessas mudanças, os controles que antes eram 114 no total, passaram a ter 93 na versão atual, os quais se reestruturam em quatro grandes grupos que são: Controles organizacionais, perfazendo (37) controles, Controle de Pessoas (8), Controles físicos (14) e Controles tecnológicos (34).A nova versão evidenciou ainda 11 novos controles, os quais foram dispostos em três campos de atuação, sendo eles: Organizacional, com o total de (3) controles, Ambiente Físico (1) e Novos Tecnológicos (7), o qual aborda, dentre outros temas, o mascaramento e prevenção de vazamentos de dados. Destarte, a presente pesquisa objetiva analisar a temática citada – avaliando esses 11 novos controles que foram evidenciados pela ISO 27001:2022, provendo uma contribuição junto a empresas brasileiras de todos os setores que atuam com o segmento de Tecnologia.

Hipótese:
Devido à natureza exploratória da presente proposta, os autores avaliam que não se faz necessária a estruturação de uma hipótese. De acordo com Gil (2017), estudos exploratórios visam trazer maior familiaridade com um determinado problema, tornando-o mais explícito ou permitindo a construção de hipóteses. Appolinário (2012) relata que pesquisas descritivas de levantamento, por exemplo, prescindem deste elemento, ou ainda, aquelas pesquisas cujas perguntas são do tipo "quais as características de?".

Metodologia Proposta:
O questionário foi estruturado tomando por base os 11 (onze) novos controles da ISO 27001:2022. Assim, o trabalho visa entender a importância e as interações entre cada uma das variáveis, provendo um entendimento sobre cada nó e seu relacionamento, auxiliando na compreensão da importância de cada um desses controles para a norma.Nesse aspecto, o trabalho busca verificar o nível de importância para cada um dos 11 novos controles que são: Inteligência de Ameaças, Segurança da informação para uso de serviços em nuvem, Prontidão de TIC para a continuidade dos negócios, Monitoramento de segurança física, Gestão de configuração, Exclusão de

informação, Mascaramento de dados, Prevenção de vazamento de dados, Atividades de monitoramento, Filtragem da Web e Codificação segura.Uma vez obtido estas informações, será avaliado o nível de influência entre cada um dos controles nos demais, permitindo identificar as relações causais entre os conceitos presentes nos mapas cognitivos, provendo insghts para tomada de decisão pelas organizações, na implantação de um Sistema de Gestão da Segurança da Informação.As orientações para uma construção adequada do questionário e de uma pesquisa exploratória tiveram como base Cooper e Schindler (2013).A coleta de dados se dará por meio de uma survey, que seguirá as recomendações de Forza (2002). Por meio de uma escala linguística, os respondentes indicarão a relação de importância entre cada um dos 11 novos controles evidenciados pele norma e as relações causais entre eles, tomando por base os termos BAIXÍSSIMA, BAIXA, MÉDIA, ALTA e MUITO ALTA, avaliando, nesse aspecto, empresas brasileiras.A análise de dados será realizada por meio da técnica Fuzzy Cognitive Maps (KOZO, 1986). O tempo estimado de participação dos respondentes na survey é de 30 minutos.

Critério de Inclusão:
Para ser incluído na lista de possíveis participantes da pesquisa, o respondente deve ter conhecimento sobre segurança da informação. Para encontrá-los os pesquisadores utilizarão de suas redes de contatos e buscas em currículos Lattes e redes sociais profissionais

Critério de Exclusão:
Serão excluídos da pesquisa informações incompletas coletadas e os dados de participantes que por motivos pessoais (ou quaisquer outros motivos) ordenarem a exclusão de seus dados, mesmo após o período de coleta. Entendemos que o participante tem este direito se assim desejar. Isso só não ocorrerá nos casos em que for impossível a identificação do questionário do participante. Esse fato foi esclarecido no processo de consentimento.

Metodologia de Análise de Dados:
A análise de dados será realizada por meio da técnica Fuzzy Cognitive Maps (KOZO, 1986).

Objetivo da Pesquisa:
Objetivo Primário:
A presente pesquisa exploratória tem por objetivo identificar a importância e as correlações entre os 11 novos controles em empresas brasileiras, propiciando uma avaliação sobre cada um desses controles, e o grau de correlação entre cada um deles. Com isso, será possível demonstrar o

impacto de cada uma desses novos controles na implantação de um Sistema de Gestão da Segurança da Informação. Para tanto, é necessário obter como base a opinião de especialistas no assunto, empregando, para a análise, a técnica Fuzzy Cognitive Maps.

Objetivo Secundário:

As informações exploratórias obtidas na pesquisa em muito contribuirão para os debates sobre os novos controles que foram evidenciados na atualização da Norma ISO 27001:2022 e sua aplicabilidade em empresas brasileiras.

Avaliação dos Riscos e Benefícios:

Segundo informações do pesquisador:

Riscos:

Entendemos que, para os estudos propostos, os riscos não são mensuráveis e previsíveis, visto que o participante tem a liberdade de apresentar sua opinião dentro de um assunto pré-definido. Entretanto, caso sinta qualquer tipo de desconforto, o participante tem o direito de não responder ou procurar os responsáveis pela pesquisa para esclarecer dúvidas.

Benefícios:

Os resultados desta pesquisa trazem de forma indireta benefícios relacionados para a na área de engenharia de produção, mais especificamente na subárea de modelos de gestão.

Comentários e Considerações sobre a Pesquisa:

Este protocolo se refere ao Projeto de Pesquisa intitulado “Análise dos novos controles evidenciados pela ISO 27001:2022 com uso do Fuzzy Cognitive Maps”, cujo Pesquisador responsável é Jefferson de Souza Pinto, com a colaboração dos pesquisadores assistentes Rosley Anholon e Reginaldo da Silva Leme. A Instituição Proponente é a Faculdade de Engenharia Mecânica da UNICAMP. Segundo as Informações Básicas do Projeto, a pesquisa tem orçamento estimado de R$ 500,00 (Quinhentos reais) para materiais de escritório e o cronograma apresentado contempla início do estudo para janeiro de 2024, com término em junho de 2024. Serão abordados ao todo 10 pessoas, sendo todos com conhecimento sobre segurança da informação.

Considerações sobre os Termos de apresentação obrigatória:

Foram analisados os seguintes documentos de apresentação obrigatória:

1 - Folha de Rosto Para Pesquisa Envolvendo Seres Humanos: Foi apresentado o documento “Folha_de_rosto_Reginaldo_2023.pdf” devidamente preenchido, datado e assinado.

2 - Projeto de Pesquisa: Foram analisados os documentos “Projeto_Detalhado.pdf” e

"PB_INFORMAÇÕES_BÁSICAS_DO_PROJETO_2223065.pdf" de 09/10/2023. Adequado.
3 - Orçamento financeiro e fontes de financiamento: Informações sobre orçamento financeiro incluídas nos documentos "Projeto_Detalhado.pdf" e "PB_INFORMAÇÕES_BÁSICAS_DO_PROJETO_2223065.pdf" de 09/10/2023. De acordo com o pesquisador, o financiamento é próprio e se espera gastar R$500,00. Adequado.
4 - Cronograma: Informações sobre o cronograma incluídas nos documentos "Projeto_Detalhado.pdf" e "PB_INFORMAÇÕES_BÁSICAS_DO_PROJETO_2223065.pdf" de 09/10/2023. Adequado.
5 - Termo de Consentimento Livre e Esclarecido: Foi apresentado o documento "TCLE_participantes.pdf", que contém o TCLE para o responsável. Adequado.
6 - Currículo do pesquisador principal e demais colaboradores: Foi apresentado o currículo do pesquisador principal, e o projeto detalhado apresenta os links para os currículos Lattes de todos os pesquisadores.
7 - Comprovante do vínculo institucional do pesquisador responsável com a Unicamp. Foi apresentada cópia de identidade funcional da UNICAMP do pesquisador principal. Adequado.
8 - Outros documentos que acompanham o Protocolo de Pesquisa:
• Questionário a ser aplicado nos participantes, arquivo "Questionario_Participantes.pdf". Adequado.
• Texto do convite de participação na pesquisa a ser enviado aos possíveis participantes, arquivo "Convite_Participante.pdf". Adequado.

Conclusões ou Pendências e Lista de Inadequações:
Projeto aprovado com as seguintes recomendações:
TCLE:
1- Informar, além dos benefícios indiretos que foram adequadamente descritos, que não há benefícios diretos em participar desta pesquisa.

Considerações Finais a critério do CEP:
- O participante da pesquisa deve receber uma via do Termo de Consentimento Livre e Esclarecido, na íntegra, por ele assinado (quando aplicável).

- O participante da pesquisa tem a liberdade de recusar-se a participar ou de retirar seu consentimento em qualquer fase da pesquisa, sem penalização alguma e sem prejuízo ao seu cuidado (quando aplicável).

- O pesquisador deve desenvolver a pesquisa conforme delineada no protocolo aprovado. Se o

pesquisador considerar a descontinuação do estudo, esta deve ser justificada e somente ser realizada após análise das razões da descontinuidade pelo CEP que o aprovou. O pesquisador deve aguardar o parecer do CEP quanto à descontinuação, exceto quando perceber risco ou dano não previsto ao participante ou quando constatar a superioridade de uma estratégia diagnóstica ou terapêutica oferecida a um dos grupos da pesquisa, isto é, somente em caso de necessidade de ação imediata com intuito de proteger os participantes.

- O CEP deve ser informado de todos os efeitos adversos ou fatos relevantes que alterem o curso normal do estudo. É papel do pesquisador assegurar medidas imediatas adequadas frente a evento adverso grave ocorrido (mesmo que tenha sido em outro centro) e enviar notificação ao CEP e à Agência Nacional de Vigilância Sanitária – ANVISA – junto com seu posicionamento.

- Eventuais modificações ou emendas ao protocolo devem ser apresentadas ao CEP de forma clara e sucinta, identificando a parte do protocolo a ser modificada e suas justificativas e aguardando a aprovação do CEP para continuidade da pesquisa. Em caso de projetos do Grupo I ou II apresentados anteriormente à ANVISA, o pesquisador ou patrocinador deve enviá-las também à mesma, junto com o parecer aprovatório do CEP, para serem juntadas ao protocolo inicial.

- Relatórios parciais e final devem ser apresentados ao CEP, inicialmente seis meses após a data deste parecer de aprovação e ao término do estudo.

-Lembramos que segundo a Resolução 466/2012 , item XI.2 letra e, “cabe ao pesquisador apresentar dados solicitados pelo CEP ou pela CONEP a qualquer momento”.

-O pesquisador deve manter os dados da pesquisa em arquivo, físico ou digital, sob sua guarda e responsabilidade, por um período de 5 anos após o término da pesquisa.

Este parecer foi elaborado baseado nos documentos abaixo relacionados:

Tipo Documento	Arquivo	Postagem	Autor	Situação
Informações	PB_INFORMAÇÕES_BÁSICAS_DO_P	09/10/2023		Aceito

Endereço: Rua Tessália Vieira de Camargo, 126, 1° andar do Prédio I da Faculdade de Ciências Médicas
Bairro: Barão Geraldo **CEP:** 13.083-887
UF: SP **Município:** CAMPINAS
Telefone: (19)3521-8936 **Fax:** (19)3521-7187 **E-mail:** cep@unicamp.br

Básicas do Projeto	ETO_2223065.pdf	10:09:54		Aceito
Outros	Questionario_Participantes.pdf	09/10/2023 10:08:17	REGINALDO DA SILVA LEME	Aceito
Projeto Detalhado / Brochura Investigador	Projeto_Detalhado.pdf	08/10/2023 11:42:55	REGINALDO DA SILVA LEME	Aceito
Outros	Convite_Participante.pdf	08/10/2023 11:34:46	REGINALDO DA SILVA LEME	Aceito
TCLE / Termos de Assentimento / Justificativa de Ausência	TCLE_participantes.pdf	08/10/2023 11:31:35	REGINALDO DA SILVA LEME	Aceito
Cronograma	Cronograma.png	06/10/2023 08:07:26	REGINALDO DA SILVA LEME	Aceito
Outros	Carteira_Funcional_Reginaldo.pdf	05/10/2023 10:25:10	REGINALDO DA SILVA LEME	Aceito
Folha de Rosto	Folha_de_rosto_Reginaldo_2023.pdf	02/10/2023 15:41:31	JEFFERSON DE SOUZA PINTO	Aceito
Outros	Carteira_Funcional_Jefferson.pdf	01/10/2023 23:17:27	JEFFERSON DE SOUZA PINTO	Aceito

Situação do Parecer:
Aprovado

Necessita Apreciação da CONEP:
Não

CAMPINAS, 31 de Outubro de 2023

Assinado por:
Renata Maria dos Santos Celeghini
(Coordenador(a))

ANEXO D – Termo de Consentimento Livre e Esclarecido (TCLE)

TERMO DE CONSENTIMENTO LIVRE E ESCLARECIDO

Análise dos novos controles evidenciados pela ISO 27001:2022 com uso do Fuzzy Cognitive Maps

Prof. Dr. Jefferson de Souza Pinto; Prof. Dr. Rosley Anholon; Reginaldo da Silva Leme.

Número do CAAE: 74829723.3.0000.5404

Você está sendo convidado a participar como voluntário de uma pesquisa. Este documento, chamado Termo de Consentimento Livre e Esclarecido, visa assegurar seus direitos como participante e você poderá manter uma via deste, caso assim deseje.
Por favor, leia com atenção e calma, aproveitando para esclarecer suas dúvidas. Se houver perguntas antes ou mesmo depois de indicar sua concordância por meio eletrônico, você poderá esclarecê-las com os pesquisadores. Se preferir, pode levar este Termo para casa e consultar seus familiares ou outras pessoas antes de decidir participar. Não haverá nenhum tipo de penalização ou prejuízo se você não aceitar participar ou retirar sua autorização em qualquer momento.

Justificativa e objetivo:

Com o advento da revisão ocorrida na ISO/IEC 27001 no ano de 2022, diversas mudanças foram identificadas em sua estrutura. Dentre elas, as mais significativas foram a inserção de novas cláusulas em sua estrutura e ajustes nos controles contidos no Anexo A da referida norma.
Em relação as mudanças no Anexo A, alguns controles foram fundidos entre si, vinte e três foram renomeados, cinquenta e sete aglutinados em vinte e quatro, e um controle dividido em dois.
Com a ocorrência dessas mudanças, os controles que antes eram 114 no total, passaram a ter 93 na versão atual. Dentre esses 93 controles, a norma evidenciou 11 novos controles que não faziam parte da versão de 2013, os quais foram dispostos em três campos de atuação, sendo eles: Organizacional, com o total de (3) controles, Ambiente Físico (1) e Novos Tecnológicos (7).
A pesquisa a ser desenvolvida baseia-se em estudo exploratório com o fito de identificar a importância e as correlações entre os 11 novos controles evidenciados, em empresas brasileiras, propiciando uma avaliação sobre a sua importância e o nível de influência entre cada um dos deles nos demais, permitindo identificar as relações causais entre os conceitos presentes nos mapas cognitivos, provendo insights para tomada de decisão pelas organizações, frente a estes novos controles. Com isso, será possível demonstrar o impacto de cada um desses novos controles na implantação de um Sistema de Gestão da Segurança da Informação.
A pesquisa foi estruturada em um questionário com uma escala que possibilitará aos pesquisadores a coleta de informações e a criação de um banco de dados. São utilizados como base os conceitos dos sistemas de gestão empresarial, bem como a base da opinião de especialistas no assunto e a técnica *Fuzzy Cognitive Maps*. Você está sendo convidado para participar deste estudo como um destes especialistas.

Procedimentos:

Inicialmente, assinale no formulário eletrônico (*Google Forms*) a opção de que você aceita participar da pesquisa como voluntário. Na primeira parte do questionário, insira algumas informações que permitirão sua caracterização. Posteriormente, são apresentadas os 11 novos controles evidenciados pela norma ISO/IEC 27001:2022:

Rubrica do pesquisador:_____Rubrica do participante:_____

1) Inteligência de Ameaças
2) Segurança da informação para uso de serviços em nuvem
3) Prontidão de TIC para a continuidade dos negócios
4) Monitoramento de segurança física
5) Gestão de configuração
6) Exclusão de informação
7) Mascaramento de dados
8) Prevenção de vazamento de dados
9) Atividades de monitoramento
10) Filtragem da Web
11) Codificação segura.

Para cada um dos aspectos analisados, indique por meio da escala, o que você julga em relação ao impacto de cada um dos novos controles evidenciados pela ISO 27001:2022, em empresas brasileiras, atribuindo **BAIXÍSSIMA, BAIXA, MÉDIA, ALTA** e **MUITO ALTA** para cada um deles.

Em seguida, relacione o nível de influência de cada um desses 11 controles, atribuindo **BAIXÍSSIMA, BAIXA, MÉDIA, ALTA** e **MUITO ALTA** para cada correlação entre eles. O tempo estimado para elaborar sua resposta completa é de 30 minutos. Você possui o direito de não responder a pergunta, se assim desejar.

Desconfortos e riscos:

Não há riscos previsíveis nesta pesquisa. A participação é voluntária e anônima e, também, não há custos. Destaca-se, entretanto, que existem os riscos característicos do próprio ambiente virtual, meios eletrônicos e/ou atividades não presenciais em função das limitações das tecnologias utilizadas, bem como limitações que nos impedem assegurar total confidencialidade e ausência de violação de informações. Você não deve participar deste estudo caso sinta qualquer desconforto em fornecer as informações. Mesmo após o início da pesquisa, você poderá interromper o preenchimento a qualquer momento e sem prejuízos.

Reforça-se ainda que todas as recomendações do ofício denominado "Orientações para procedimentos em pesquisas com qualquer etapa em ambiente virtual" serão seguidas.

Para salvar uma via do TCLE, basta imprimir a página referente ao TCLE presente no questionário através das opções do seu navegador.

Benefícios:

Não há benefícios diretos em participar desta pesquisa, todavia, a publicação do material irá contribuir para a compreensão do nível de importância para cada novo controle evidenciado pela ISO 27001:2022 em empresas brasileiras.

Acompanhamento e assistência:

A todo o momento, os responsáveis por essa pesquisa estarão disponíveis via meios eletrônicos (e-mails, telefone, entre outros) para prestar assistência e acompanhamento. O participante receberá a assistência integral e imediata, de forma gratuita, pelo tempo que for necessário em caso de danos decorrentes da pesquisa. Os contatos dos pesquisadores serão apresentados posteriormente.

Rubrica do pesquisador:_____Rubrica do participante:_____

Sigilo e privacidade:

Você tem a garantia de que sua identidade será mantida em sigilo e nenhuma informação será dada a outras pessoas que não façam parte da equipe de pesquisadores. Na divulgação dos resultados desse estudo, seu nome não será citado.

Ressarcimento e Indenização:

Não há custos relacionados à participação nesta pesquisa. Você terá a garantia ao direito de indenização diante de eventuais danos decorrentes da pesquisa.

Tratamento dos dados:

Todo processo de manipulação, tratamento e armazenamento dos dados serão realizados exclusivamente pelos pesquisadores pertencentes a este projeto. Esta pesquisa prevê o armazenamento dos dados coletados em repositório por no mínimo 5 anos (Resolução CNS 466-12). O repositório de dados é digital e acessado somente por esta equipe de pesquisadores através de senha. Sua identidade não será revelada nesses dados, pois como mencionado trata-se de uma pesquisa anônima (sem identificação).
Esta pesquisa prevê o armazenamento dos dados, anonimizados, coletados nesta pesquisa, em repositório institucional de dados, em local virtual, de acesso público, com objetivo de possível reutilização, verificação e compartilhamento, em trabalhos de colaboração científica com outros pesquisadores. Sua identidade não será revelada nesses dados, pois os mesmos serão armazenados de forma anônima (isto é, os dados não terão identificação), utilizando mecanismos que impeçam a possibilidade de associação, direta ou indireta, com você. Cabe ressaltar que a pessoa que compartilhar os dados anonimizados também não terá possibilidade de identificar os participantes dos quais os dados originaram. Sendo assim, não haverá possibilidade de reversão da anonimização.

Recrutamento de participantes:

O recrutamento dos participantes da pesquisa será realizado de forma individual, via rede social (LinkedIn), ou e-mail, ou seja, com apenas um emitente e um destinatário, visando não permitir identificação de outros participantes e visualização de seus dados de contato. A carta convite individual terá link para acesso ao Termo de Consentimento Livre e Esclarecido para anuência e ao formulário de pesquisa via *Google Forms*. No qual após o aceite do TCLE será direcionado às perguntas. Caso o participante não concorde, basta fechar a guia do navegador.

Contato:

Em caso de dúvidas sobre a pesquisa, você poderá entrar em contato com os pesquisadores:

1) **Jefferson de Souza Pinto**. Professor Colaborador Doutor da Faculdade de Engenharia Mecânica. Rua Mendeleyev, 200, Departamento de Engenharia de Manufatura e Materiais (DEMM), Faculdade de Engenharia Mecânica (FEM), Universidade Estadual de Campinas, telefone: (19) 3521-3312, e-mail jeffsouzap@fem.unicamp.br.

2) **Rosley Anholon**. Professor Colaborador Doutor da Faculdade de Engenharia Mecânica. Rua Mendeleyev, 200, Departamento de Engenharia de Manufatura e Materiais (DEMM), Faculdade

Rubrica do pesquisador:_____Rubrica do participante:_____

de Engenharia Mecânica (FEM), Universidade Estadual de Campinas, telefone: (19) 3521-3312, e-mail jeffsouzap@fem.unicamp.br.

3) **Reginaldo da Silva Leme**. Aluno de mestrado da Faculdade de Engenharia Mecânica. Rua Mendeleyev, 200, Departamento de Engenharia de Manufatura e Materiais (DEMM), Faculdade de Engenharia Mecânica (FEM), Universidade Estadual de Campinas, e-mail arlemrecchia@gmail.com.

Em caso de denúncias ou reclamações sobre sua participação e sobre questões éticas do estudo, você poderá entrar em contato com a secretaria do Comitê de Ética em Pesquisa (CEP) da UNICAMP das 08:00hs às 11:30hs e das 13:00hs as 17:30hs na Rua: Tessália Vieira de Camargo, 126; CEP 13083-887 Campinas – SP; telefone (19) 3521-8936 ou (19) 3521-7187; e-mail: cep@unicamp.br. Em havendo a necessidade da intermediação da comunicação ser acessível em Libras você pode fazer contato com a Central TILS da Unicamp no site https://www.prg.unicamp.br/tils/.

O Comitê de Ética em Pesquisa (CEP).

O papel do CEP é avaliar e acompanhar os aspectos éticos de todas as pesquisas envolvendo seres humanos. A Comissão Nacional de Ética em Pesquisa (CONEP) tem por objetivo desenvolver a regulamentação sobre proteção dos seres humanos envolvidos nas pesquisas. Desempenha um papel coordenador da rede de Comitês de Ética em Pesquisa (CEPs) das instituições, além de assumir a função de órgão consultor na área de ética em pesquisas.

Consentimento livre e esclarecido:

Após ter recebido esclarecimentos sobre a natureza da pesquisa, seus objetivos, métodos, benefícios previstos, potenciais riscos e o incômodo que esta possa acarretar, indique o aceite à pesquisa no próprio questionário eletrônico. Para formalizar este aceite, clique na opção botão: aceito participar da pesquisa.

Nome do(a) participante:
_____

_____Data: ____/_____/_____.
(Assinatura do participante ou nome e assinatura do seu RESPONSÁVEL LEGAL)

Responsabilidade do Pesquisador:

Asseguro ter cumprido as exigências da resolução 466/2012 CNS/MS e complementares na elaboração do protocolo e na obtenção deste Termo de Consentimento Livre e Esclarecido.

Asseguro, também, ter explicado e fornecido uma via deste documento ao participante da pesquisa. Informo que o estudo foi aprovado pelo CEP perante o qual o projeto foi apresentado e pela CONEP, quando pertinente. Comprometo-me a utilizar o material e os dados obtidos

Rubrica do pesquisador:_____Rubrica do participante:_____

nesta pesquisa exclusivamente para as finalidades previstas neste documento ou conforme o consentimento dado pelo participante da pesquisa.

_____Data: .
(Assinatura do pesquisador)

Rubrica do pesquisador:_____Rubrica do participante:_____

ANEXO E – Comprovação de Submissão em Periódico

emerald PUBLISHING

Information and Computer Security

Home | Author

Author Dashboard

Author Dashboard

1 Manuscripts I Have Co-Authored

Start New Submission

5 Most Recent E-mails

Manuscripts I Have Co-Authored

STATUS	ID	TITLE	CREATED	SUBMITTED
Contact Journal AE: Not Assigned EIC: Furnell, Steven • Awaiting Reviewer Scores	ICS-10-2024-0269	Information security management: a fuzzy DEMATEL analysis of the new ISO/IEC 27001:2022 controls View Submission Submitting Author: Sigahi, Tiago Cover Letter	23-Oct-2024	23-Oct-2024

Gmail

Tiago Sigahi <tiagosigahi@gmail.com>

Information and Computer Security - ICS-10-2024-0269

1 mensagem

Information and Computer Security <onbehalfof@manuscriptcentral.com> 23 de outubro de 2024 às 11:16
Responder a: Steven.Furnell@nottingham.ac.uk
Para: tiagosigahi@gmail.com

23-Oct-2024

Dear Prof. Sigahi:

Your manuscript entitled "Information security management: a fuzzy DEMATEL analysis of the new ISO/IEC 27001:2022 controls" has been successfully submitted online and is presently being given full consideration for publication in the Information and Computer Security.

Your manuscript ID is ICS-10-2024-0269.

Please mention the above manuscript ID in all future correspondence or when calling the office for questions. If there are any changes in your street address or e-mail address, please log in to Manuscript Central at https://mc.manuscriptcentral.com/iacs and edit your user information as appropriate.

You can also view the status of your manuscript at any time by checking your Author Centre after logging in to https://mc.manuscriptcentral.com/iacs.

Please note that Emerald requires you to clear permission to re-use any material not created by you. If there are permissions outstanding, please upload these when you submit your revision or send directly to Emerald if your paper is accepted immediately. Emerald is unable to publish your paper with permissions outstanding.

Thank you for submitting your manuscript to the Information and Computer Security.

Sincerely,
Steven Furnell
Information and Computer Security

ANEXO F – Artigo Submetido

Information and Computer Security

Emerald Information Management and Computer Security

Information security management: a fuzzy DEMATEL analysis of the new ISO/IEC 27001:2022 controls

Journal:	*Information and Computer Security*
Manuscript ID	ICS-10-2024-0269
Manuscript Type:	Original Article
Keywords:	Information security, Risk Management, Fuzzy logic, Decision making, Decision support systems

SCHOLARONE™
Manuscripts

Information security management: a fuzzy DEMATEL analysis of the new ISO/IEC 27001:2022 controls

Abstract:

Purpose: This paper aims to analyze the cause-and-effect relationship and the level of influence between the eleven new information security controls proposed by ISO/IEC 27001:2022.

Design/methodology/approach: A survey with twenty-two experts was conducted to assess the influences between each of these controls by means of a pairwise comparison. Then, the fuzzy DEMATEL method was applied to evaluate the relationships and the influence degree between controls.

Findings: The most influential controls and those most impacted were identified. Furthermore, the analysis identified the central, driving, independent and impact controls, as well as their priority in the allocation of resources for their management. Thus, this study provides a clear and concise level of detail on the cause-and-effect relationships between each of the new controls, providing decision-makers with valuable information for incorporating and managing them into their organization's information security management system.

Originality: The originality of the study lies in its focus on analyzing the cause-and-effect relationships among the newly proposed information security controls in ISO/IEC 27001:2022. It provides a novel approach to assessing the level of influence between these controls, which has not been extensively explored in prior research. The study's identification of central, driving, and impact controls offers practical insights for resource prioritization in information security management, adding a valuable layer of guidance for organizations seeking to implement the new standards effectively.

Keywords: ISO/IEC 27001:2022; Information security; Risk management; Fuzzy DEMATEL.

1. Introduction

In a world of constant technological evolution, cybercrime has been on the rise, with new threats emerging constantly, putting the data and information of various organizations at risk (International Organization for Standardization, 2022).

For example, in 2023, Brazil suffered 60 billion attempted attacks, many of them innovative and unique, including new variants of malware and ransomware (Fortinet, 2024). This shows how important it is for organizations to be prepared to deal with this scenario.

Although there have been technical advances that have significantly improved the ability to search for data leaks, vulnerabilities in computer systems and communication networks, there are still challenges in effectively detecting new and complex cyber-attacks (Ozkan-Okay et al., 2023).

Information and Computer Security

Faced with such a scenario, it is of the utmost importance that safeguard measures are taken so that information and data remain safe and protected, which must be based on comprehensive guidelines that allow strategic decision-making by the organization, guaranteeing business continuity (Mtair Al-Hawamleh et al., 2020).

One way to ensure that organizations manage such risks is through the implementation of an Information Security Management System (ISMS), in which ISO/IEC 27001 stands out as an internationally recognized guideline that provides a framework for its operationalization.

This standard provides a model for establishing, implementing, maintaining and continually improving an ISMS, bringing benefits and guarantees regarding the preservation of confidentiality, integrity and availability of information, through a risk management process, providing confidence to stakeholders that such risks are identified and adequately managed (International Organization for Standardization, 2022).

To this end, Annex A of this standard contains various controls that must be applied, allowing organizations to assess their possible Information Security failures (Suorsa & Helo, 2024), their assets, communication and access controls (Kaban & Legowo, 2018), as well as the possibility of determining the maturity level of their ISMS (Legowo & Juhartoyo, 2022).

In this context, Humphreys (2016) reports that the adoption of these controls allows organizations to implement risk-based security practices, adapted to their specific needs, which is crucial for their cyber resilience.

As noted, controls are of great importance to the ISMS, working in conjunction with the requirements and processes contained in the standard to mitigate the risks related to Information Security. In this regard, it is worth highlighting that Annex A controls underwent changes when the standard was updated in December 2022. Several were grouped, some renamed and eleven new ones incorporated.

By highlighting these eleven new controls, the need arises to evaluate the relationship and level of influence between each of them, since the information security management of a complex system involves an assessment of cause and effect in their relationships and mutual influences (Ho et al., 2015).

Therefore, the objective of this article is to evaluate the level of influence and impact of each of these eleven new controls on the ISMS through the application of the fuzzy DEMATEL method, supporting decision-making for their incorporation (Si et al., 2018).

2. Theoretical background

2.1 Information Security Management System (ISMS)

An Information Security Management System encompasses policies, procedures, guidelines and associated resources and activities, which are managed collectively to achieve the organization's business objectives (International Organization for Standardization, 2018).

Information and Computer Security

Its structure is based on an assessment of risks and their levels of acceptance by organizations, which are evaluated through appropriate controls that guarantee the protection of these assets, which is a strategic decision for an organization (International Organization for Standardization, 2018).

By establishing an ISMS, the organization imperatively demonstrates to its customers that the information shared is managed securely and correctly (Kitsios et al., 2022), since the ISMS represents one of the most complex management systems to implement in an organization (Raković, 2021).

Its application also allows rigorous processes and controls to be implemented not only to manage the quality of the internal and external processes and services provided, but also those related to the privacy and confidentiality of the data collected, protecting it consistently (Hannigan et al., 2019).

Furthermore, by implementing an ISMS, organizations become more resilient to information security threats and cyber-attacks (Kitsios et al. 2023) in the face of a wide range of threats from various sources (International Organization for Standardization, 2018).

2.2 ISO/IEC 27000, 27001 and 27002

The ISO/IEC 27000 standard originated from the British Standard *BS* 7799a, which was published in 1995, written by the Department of Industry and Commerce of the United Kingdom Government, and addressed, in its first part, the best practices for Information Security Management (Calder & Watkins, 2005).

Its structure provides an introduction and overview of the ISO 27000 family, with clear definitions and vocabulary about the ISMS. The framework includes the ISO/IEC 27001 and ISO/IEC 27002 standards, among others.

ISO/IEC 27001 is the world's best-known standard for Information Security Management Systems (International Organization for Standardization, 2022), which defines requirements that an ISMS must meet in order to mitigate the risks related to cyber security.

First published in 2005, this standard has undergone two revisions, the first in 2013 and the last in 2022, with significant changes compared to its previous version.

The first change was to the title of the standard, which was renamed "Information Security, Cybersecurity and Privacy Protection - Information Security Management Systems - Requirements", in line with ISO/IEC 27002:2022.

In addition, new clauses have been introduced into its structure to harmonize the document with other management system standards, such as ISO 22301:2019.

Another significant change was in Annex A of ISO/IEC 27001:2022, which provides a reference for information security controls. Its structure was consolidated from 14 areas in the 2013 version to 4 main areas in the 2022 version, which are: Organizational Controls, People Controls, Physical Controls and Technological Controls.

Furthermore, some of these controls have been merged together, twenty-three have been renamed, fifty-seven merged into twenty-four, one control split into two and

Information and Computer Security

thirty-five kept in their essence, although they may have undergone minor updates in their wording or clarity.

The new version also included eleven new controls, which were divided into three of the four groups mentioned above, as shown in Table I.

As a result of these changes, the controls, which previously totaled 114, are now 93 in the current version, which have been restructured into: organizational controls, making up controls (37), people controls (8), physical controls (14), and technological controls (34).

[INSERT TABLE I HERE]

Another noteworthy point is that this standard can be certified, which translates into a guarantee that the certified organization has implemented an ISMS in accordance with the standards described, which increases the degree of trust by interested parties (Calder & Watkins, 2008).

ISO/IEC 27002:2022's structure is based on providing guidelines on the implementation of generic information security controls, including implementation guidance, in the context of an ISMS based on ISO/IEC 27001:2022 (International Organization for Standardization, 2022a).

Some of the controls in this standard modify the risk, while others maintain it (International Organization for Standardization, 2022a), as is the case, for example, with a security policy.

The security controls listed in table A.1 of Annex A of ISO/IEC 27001:2022 are directly derived from and aligned with those listed in ISO/IEC 27002:2022, sections 5 to 8, which must be used in accordance with sub-item 6.1.3 of ISO/IEC 27001:2022.

In this way, ISO 27002 integrates with ISO 27001, providing a framework for international best practices in information security, systems management and interoperability, as well as providing data for an external auditor to examine the implementation of a certifiable ISMS (Calder & Watkins, 2008).

3. Methods

DEMATEL (Decision-making Trial and Evaluation Laboratory) emerges as a Multicriteria Decision Method adept at unraveling intricate interrelationships among various factors within a problem domain. Through the quantitative analysis of direct and indirect relationships, DEMATEL offers a comprehensive perspective, informed by expert opinions on the degree of influence one element exerts over another (Si et al., 2018). Notably, DEMATEL facilitates visualization of its findings through a two-dimensional diagram, positioning relevance relationships along the x-axis and cause-and-effect relationships along the y-axis. This method excels in capturing multidirectional relationships, contrasting with techniques like AHP, which typically assume unidirectional relationships and independence among factors (Chien et al., 2014).

Information and Computer Security

However, while DEMATEL provides valuable insights into complex systems' interdependencies, it falls short in addressing human subjectivity and data vagueness (Si et al., 2018). To mitigate this limitation, the integration of fuzzy logic into DEMATEL methodology emerges as a promising solution (Chien; Wu; Huang, 2014). This approach, known as fuzzy DEMATEL, accommodates imprecision and uncertainty inherent in real-world data, enhancing the methodology's applicability in scenarios characterized by subjective judgments and ambiguous information (Si et al., 2018; Zadeh, 1965).

The following are the steps for applying the fuzzy DEMATEL method in this research (Chien et al., 2014).

- Step 1 – To set an expert panel: the initial phase involves forming an expert panel and determining the factors to be assessed for causal relations.
- Step 2 – To define the fuzzy direct assessment matrix $\tilde{Z} = [\tilde{z}_{ij}]_{nXn}$: after the identification of the analyzed factors, pairwise comparisons should be conducted by the expert panel regarding the influence level of element i over element j.
- Step 3 – To calculate the initial direct assessment matrix Z: defuzzification of the matrix $\tilde{Z} = [\tilde{z}_{ij}]_{nXn}$ should be conducted.
- Step 4 – To normalize the initial direct assessment matrix Z, generating matrix X.
- Step 5 – To calculate the total-relation matrix, T, where I correspond to the identity matrix: $T = X.(I - X)^{-1}$
- Step 6 – To calculate the R and C vectors: this process occurs by calculating the sum of rows, R, and columns, C, of the total-relation matrix, T. In the context of this study, 'R' symbolizes the overarching impact of one factor i on another factor j, while 'C' signifies the comprehensive effects endured by factor j, as a result of factor i.
- Step 7 – Calculation of $(R + C)$ and $(R - C)$ and elaboration of the fuzzy DEMATEL causal diagram: In this step, $(R + C)$ quantifies the significance of each factor and gauges its relationship with others. Conversely, $(R - C)$ determines the nature of the relationship between factors: a positive sign indicates influence on other factors, while a negative sign signifies being influenced by other factors.

4. Results

4.1. Fuzzy DEMATEL questionnaire

The data collection questionnaire was prepared based on the eleven controls that were highlighted in the 2022 version of the ISO 27001 standard in line with ISO 27002:2022.

Information and Computer Security

To this end, each control was duly identified and analyzed according to its definition, purposes, guidelines and other information described by the standards, so that experts had a clear and concise level of detail, avoiding misinterpretations about its functionality and applicability.

Next, factors described in Table II were defined, which correspond to each of the new controls highlighted, and contain an explicit description of their operation within the ISMS.

[INSERT TABLE II HERE]

Subsequently, respondents (the experts) were asked to report the level of influence of one factor in relation to each of the others, through pairwise comparisons (Lin & Wu, 2008), based on the linguistic scale described in the following subsection (3.1.2.), resulting in the database used to apply the fuzzy DEMATEL method.

4.2. Linguistic terms and triangular fuzzy numbers

Since human assessments may contain ambiguities (Wu & Lee, 2007), the following linguistic terms (Li, 1999) were defined and used to assess the influences between factors in the developed questionnaire (Null, Very Low, Low, Medium, High, and Very High).

Fuzzy sets can be used to deal with imprecision and uncertainty, especially when associated with linguistic variables, a concept known as "computing with words" (Zadeh, 1965). In this regard, for each of the linguistic terms, a corresponding triangular fuzzy number was defined (Si et al., 2018), as shown in Table III.

[INSERT TABLE III HERE]

4.3. Acquisition of decision makers' assessments

To determine the cause-and-effect relationships between the analyzed factors, it is essential to consult a group of qualified experts, which provide insights that capture the complexity of these interdependencies (Wu & Lee, 2007).

In this sense, Technology Directors, also known as Chief Technology Officers (CTO) of Brazilian companies, were chosen as a group of experts. They have a strategic and comprehensive vision of the organizational technological panorama, in addition to extensive experience in managing and implementing complex technological solutions, which makes them capable of providing precise, clear and relevant contributions to the study.

Using the linguistic scale in Table III, twenty-two experts evaluated the mutual relations of influence between each pair of factors, obtaining the matrix $\tilde{Z}$ for each of the factors, such as, for example, the threat intelligence factor (C1) presented in Table IV.

[INSERT TABLE IV HERE]

Information and Computer Security

4.4. Information transformation

Then, each linguistic evaluation was replaced by its corresponding triangular fuzzy number, as shown in Table V, which shows some fuzzy values related to factor C1, to exemplify the process.

[INSERT TABLE V HERE]

4.5. Aggregation of information

The next step was the aggregation of the triangular fuzzy numbers. In this study, the aggregation was performed by the simple average (Si et al., 2018) between each of the vertices, according to Equation 1, obtaining the aggregated matrix shown in Table VI.

$$\tilde{Z}_{ij} = \left(Z_{ij1}, Z_{ij2}, Z_{ij3}\right) = \frac{1}{l}\sum_{k=1}^{l} \tilde{z}_{ij}^{k} = \frac{1}{l}\sum_{k=1}^{l} \tilde{z}_{ij1}^{k}, \frac{1}{l}\sum_{k=1}^{l} \tilde{z}_{ij2}^{k}, \frac{1}{l}\sum_{k=1}^{l} \tilde{z}_{ij3}^{k} \qquad \text{(Equation 1)}$$

[INSERT TABLE VI HERE]

4.6. Defuzzyfication of the relation matrix

Once the matrix Z has been aggregated, using a defuzzyfication method, it is possible to obtain the fuzzy matrix of direct influences (Si et al., 2018). There are several methods to perform the defuzzyfication of a matrix, for the proposed study the Center of Area (COA) method was chosen, demonstrated by Si et al. (2018), in which, through the application of Equation 2, the average of the values existing in each row is calculated, obtaining the defuzzyfied relationship matrix shown in Table VII.

$$y = l + \frac{(m-l)+(u-l)}{3} \quad \text{or} \quad y = \frac{l+m+u}{3} \qquad \text{(Equation 2)}$$

[INSERT TABLE VII HERE]

4.7. Normalization of the matrix Z

Once defuzzyfied, the next step is to perform the normalization of the matrix Z. To this end, using Equation 3, the sum of each line of matrix Z was performed, obtaining at the end the value of S, which corresponds to the maximum value obtained between the sums of the lines, as shown in Table VIII.

$$S = \frac{max}{1 \le i \le n} \sum_{j=1}^{n} Z_{ij} \qquad \text{(Equation 3)}$$

Information and Computer Security

[INSERT TABLE VIII HERE]

Once the maximum value S was obtained, Equation 4 was applied, which divides each row of each column of matrix Z by the value of S, resulting in the normalized matrix X, as shown in Table IX.

$$X = \frac{Z}{S} \qquad \text{(Equation 4)}$$

[INSERT TABLE IX HERE]

4.8. Total influence matrix *T*

The next step described by Si et al. (2018) is the construction of the Total Influence Matrix T, which is obtained through Equation 5, in which the multiplication of matrix X by the inverse of Matrix $I - X$ is performed, where I corresponds to the identity matrix.

$$T = X.(I - X)^{-1} \qquad \text{(Equation 5)}$$

Once matrix T has been obtained, it is possible to calculate vectors R and C (Si et al., 2018) using Equation 6, where R is the sum of the rows of matrix T and C is the sum of the columns, from which the values contained in Table X were obtained.

$$R = \left[\sum_{j=1}^{n} t_{ij}\right]_{nx1}, \quad C = \left[\sum_{j=1}^{n} t_{ij}\right]_{1xn} \qquad \text{(Equation 6)}$$

[INSERT TABLE X HERE]

5. Discussion

5.1. Prominence and relation

Once the vectors R and C are obtained, it is possible to calculate the Prominence and Relation of the factors, Table XI, in which the horizontal axis $(R + C)$ illustrates the strength of the influences that are given and received while the vertical axis $(R - C)$ shows the effect to which the factor contributes in the system (Si et al., 2018). Furthermore, when positive, it means that it influences the other factors and can be grouped as a cause factor, while if it is negative, then the factor is being influenced and should be grouped as an effect (Si et al., 2018).

[INSERT TABLE XI HERE]

In this sense, Table XI allows to identify, among the controls highlighted by the ISO/IEC 27001:2022 standard, which are the Cause controls (C1, C2, C3, C9 and C11), which are the factors that have the most influence, while the others (C4, C5, C6, C7, C8

Information and Computer Security

and C10) are considered Effect controls, that is, they are more affected by the other controls than they affect them, which translates into meaningful information for understanding the relationships between these new controls that were highlighted.

5.2. Causal Relational Diagram

With the values ($R + C$ and $R - C$) defined, another important step is to construct the Causal Diagram (CD), presented in Figure 1, which graphically represents the cause-and-effect relationships between the factors (Si et al., 2018).

[INSERT FIGURE 1 HERE]

The vector $R + C$ is called "Prominence" because it reveals the importance of the criterion's weight, while the vector $R - C$ is called "Relationship" because it divides the criteria into a cause-and-effect group, in which if positive the criterion generally belongs to the Cause group, while if negative, it belongs to the Effect group (Chien et al., 2014).

With the diagram constructed, it is possible to perform an analysis by quadrants, based on the calculation of the average $R + C$ (Si et al., 2018), in which the diagram is divided into four quadrants, as shown in Figure 1, which allows obtaining valuable information about each of them according to their position.

Quadrant I is called "Core Factors"; those contained in quadrant II are the "Driving factors"; those in Quadrant III are identified as "Independent Factors" and the factors in Quadrant IV are "Impact Factors" (Si et al., 2018).

Based on the distribution shown in Figure 1, it can be observed that, in the first quadrant, the Threat Intelligence (C1), Information Security for the use of cloud services (C2) and ICT Readiness for business continuity (C3) controls are arranged as Central Factors of the system, which have high prominence and high relationship, being key factors that are classified as a priority target in the use of resources for their management (Chien et al., 2014).

In the second quadrant we have the controls that are part of the "Driving factors", namely Secure Development (C9) and Data Masking (C11), which have low prominence and a high relationship in which, if independent, they will affect a small number of other factors, which are classified in second place in the use of management resources (Chien et al., 2014).

In the third quadrant, the factors defined as Independent are outlined, namely Discarding or deleting information (C10) and Physical security monitoring (C4). This quadrant contains factors that have low prominence and high relationship, which have low interaction with other factors, qualifying in third place for the use of management resources (Chien et al., 2014).

In the fourth quadrant, typified as Impact Factor, are located the controls of Monitoring Activities (C6), Configuration Management (C5), Web Filtering (C8) and Data Leakage Prevention (C7), which have high prominence and low relationship, and must be

Information and Computer Security

managed, but cannot be improved directly, ranking last in relation to the use of management resources (Chien et al., 2014).

With the information obtained from the quadrant analysis, decision-makers can visually detect the complex causal relationships between factors (Si et al., 2018), easily identifying those that are considered key factors in the system and that should be prioritized in the allocation of resources, which provides decision-makers with a strategic and assertive assessment in the management and maintainability of these controls within the ISMS.

5.3. Relational Influence Map

The Relational Influence Map (RIM) is built based on the information obtained from the matrix T and provides a graphical representation of the interactions between factors (Si et al., 2018), which provides valuable information for decision makers.

It should be noted that, in some situations, depending on the total number of elements contained, their representation can lead to a very complex map (Sara et al., 2015), if all relationships are considered.

In this sense, the construction of the RIM of this work was based on the definition of a limit value (Si et al., 2018) which is obtained by applying Equation 7, which calculates an average between all the elements of matrix T, which allows the RIM to present only the most important relationships between the controls.

$$\propto = \sum_{i=1}^{n}\sum_{j=1}^{n}[tij]/N \qquad \text{(Equation 7)}$$

Considering the limit value obtained, which was 1.244, the controls that served as a basis for the construction of the RIM presented in Figure 2 were defined, which are highlighted in green in the matrix T, as shown in Table XII.

[INSERT TABLE XII HERE]

[INSERT FIGURE 2 HERE]

Based on the RIM obtained, decision makers can graphically evaluate the main influences between the system controls, obtaining valuable information for decision making regarding the incorporation and management of these new controls within the organizations' ISMS.

6. Conclusions

This study used the fuzzy DEMATEL method to analyze the cause-and-effect relationship and the level of influence between the eleven new controls highlighted by ISO 27001:2022. The study allowed us to identify which controls have the most influence on

Information and Computer Security

the system and which are most influenced, which translates into important information for understanding the relationships between these new controls that were highlighted.

Another significant contribution of the research is in the results presented by the causal diagram and its division into quadrants. Based on the information obtained, decision-makers can evaluate the complex relationships between each of the controls, identifying which are the key, guiding, independent and impactful controls within the system, as well as the priority in the allocation of resources for each of them, which allows a strategic and assertive evaluation for their management and maintainability within the ISMS.

Another highlight is the RIM, which gives decision-makers a graphical view of the main relationships between controls, adding value to the analysis process by illustrating the cause-and-effect connections between them. This map facilitates identifying the relationships considered strong and most important between the identified controls, which allows for a better understanding of the internal dynamics and the prioritization of strategic actions for their integration into the ISMS.

In view of the above, the study presents valuable information for incorporating and managing the new information security controls highlighted by ISO 27001:2022 when implemented in organizations' Information Security Management Systems.

As limitations, it can be stated that the study was conducted based on Brazilian technology companies. Therefore, controls may have greater or lesser influence depending on the technological scenario in which they are based.

Once these controls are implemented in the ISMS, for future research, it is suggested that their impact be analyzed on each of the Groups to which they belong, assessing the cause-and-effect relationships between them, providing novel opportunities for improvement.

Statements and Declarations

Disclosure of interest: The authors report there are no competing interests to declare.

Ethical considerations: This research was evaluated and approved by the Research Ethics Committee of the State University of Campinas (Certificate of Approval no. 74829723.3.0000.5404).

Consent to participate: The Informed Consent Form was presented to and obtained from all participants in digital written format.

Funding statement: Not applicable.

Data availability: Data will be made available on request.

References

Aslan, Ö., Aktuğ, S.S., Ozkan -Okay, M., Yilmaz, AA, & Akin, E. (2023). A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. *Electronics, 12* (6), 1333.

Information and Computer Security

Calder, A., & Watkins, S. (2005). *IT governance: A manager's guide to data security and BS 7799/ISO 17799.* Kogan Page Publishers.

Calder, A., & Watkins, S. (2008). *IT governance: A manager's guide to data security and ISO 27001/ISO 27002.* Kogan Page Ltd.

Chang, YH, Yeh, CH, & Cheng, JH (1998). Decision support for bus operations under uncertainty: a fuzzy expert system approach. *Omega, 26* (3), 367-380.

Chien, K. F., Wu, Z. H., & Huang, S. C. (2014). Identifying and assessing critical risk factors for BIM projects: Empirical study. *Automation in construction, 45,* 1-15.

Cooper, D. R., & Schindler, P. S. (2013). *Research Methods in Management-12th edition.* McGraw Hill Brazil.

Fortinet. (2024). *Report 2023 Threat Landscape.* https://www.fortinet.com/br/resources/analyst-reports/threat-report-2h-2023#:~:text=In 2H 2023%2C we observed, scale enterprises and critical industries.

Gil, AC (2002). *How to prepare research projects.* Editora Atlas SA.

Gil, AC (2008). *Social research methods and techniques.* 6th ed. Editora Atlas SA.

Hannigan, L., Deyab, G., Al Thani, A., Al Marri, A., & Afifi, N. (2019). The implementation of an integrated management system at Qatar biobank.

Hawamleh, AMA, Alorfi, ASM, Al- Gasawneh, JA, & Al-Rawashdeh, G. (2020). Cyber security and ethical hacking: The importance of protecting user data. *Solid State Technology, 63* (5), 7894-7899.

Ho, L. H., Hsu, M. T., & Yen, T. M. (2015). Identifying core control items of information security management and improving strategies by applying fuzzy DEMATEL. *Information & Computer Security, 23* (2), 161-177.

Humphreys, E. (2016). *Implementing the ISO/IEC 27001:2013 ISMS Standard.* Artech house.

International Organization for Standardization. (2022). Information technology – Security techniques – Information security management systems – Requirements (ISO/IEC 27001:2022). Geneva, Switzerland: ISO.

International Organization for Standardization. (2022a). Information security, cybersecurity and privacy protection — Information security controls (ISO/IEC 27002). Geneva, Switzerland: ISO.

International Organization for Standardization. (2018). Information technology — Security techniques — Information security management systems — Overview and vocabulary (5th ed.). Geneva, Switzerland: ISO.

Kaban, E., & Legowo, N. (2018). Audit information system risk management using iso 27001 framework at private bank. *Journal of Theoretical & Applied Information Technology, 96* (1).

Information and Computer Security

Kitsios, F., Chatzidimitriou, E., & Kamariotou, M. (2022). Developing a risk analysis strategy framework for impact assessment in information security management systems: A case study in it consulting industry. *Sustainability, 14* (3), 1269.

Kitsios, F., Chatzidimitriou, E., & Kamariotou, M. (2023). The ISO/IEC 27001 information security management standard: how to extract value from data in the IT sector. *Sustainability, 15* (7), 5828.

Legowo, N., & Juhartoyo, Y. (2022). Risk management; risk assessment of information technology security system at bank using ISO 27001. *Journal of System and Management Sciences, 12* (3), 181-199.

Li, R.J. (1999). Fuzzy method in group decision making. *Computers & Mathematics with Applications, 38* (1), 91-101.

Lin, C.J., & Wu, W.W. (2008). A causal analytical method for group decision-making under fuzzy environments. *Expert Systems with Applications, 34* (1), 205-213.

Marconi, MDA, & Lakatos, EM (2003). *Fundamentals of scientific methodology.* Atlas.

Prodanov, CC, & De Freitas, EC (2013). *Methodology of scientific work: methods and techniques of research and academic work-2nd Edition.* Publisher Feevale.

Raković, R. (2021). Project of isms implementation in organization–aspects and practical experiences. *European project management journal, 11* (1), 20-30.

Rouquayrol, MZ (2018). *Epidemiology & Health* (8th ed.).

Sara, J., Stikkelman, R. M., & Herder, P. M. (2015). Assessing relative importance and mutual influence of barriers for CCS deployment of the ROAD project using AHP and DEMATEL methods. *International Journal of Greenhouse Gas Control, 41,* 336-357.

Si, S.L., You, X.Y., Liu, H.C., & Zhang, P. (2018). DEMATEL technique: a systematic review of the state-of-the-art literature on methodologies and applications. *Mathematical problems in Engineering, 2018* (1), 3696457.

Suorsa, M., & Helo, P. (2024). Information security failures identified and measured–ISO/IEC 27001: 2013 controls ranked based on GDPR penalty case analysis. *Information Security Journal: A Global Perspective, 33* (3), 285-306.

Topa, I., & Karyda, M. (2019). From theory to practice: guidelines for enhancing information security management. *Information & Computer Security, 27* (3), 326-342.

Wu, W. W., & Lee, Y. T. (2007). Developing global managers' competencies using the fuzzy DEMATEL method. *Expert systems with applications, 32* (2), 499-507.

Zadeh, L. A. (1965). Fuzzy sets. *Information and control, 8* (3), 338-353.

Information and Computer Security

Table I. New controls highlighted by ISO 27001:2022.

Groups	Controls
Organizational	Threat intelligence Information security for the use of cloud services ICT readiness for business continuity
Physical	Physical security monitoring
Technological	Configuration management Disposal or deletion of information Data masking Data leakage prevention Monitoring activities Web filtering Secure development

Source: Authors' own creation.

Information and Computer Security

Table II. Influencing factors of the new ISO 27001:2022 controls.

Factors	Description
C1	Collection and analysis of information related to information security threats, producing threat intelligence, so that appropriate mitigation actions can be taken.
C2	Specification and management of information security for the use of cloud services, evaluating processes of acquisition, use, management and exit of services.
C3	Plan, implement, maintain and test ICT readiness, based on business continuity objectives, ensuring the availability of the organization's information and other associated assets during disruption.
C4	Continuous monitoring of facilities to detect and prevent unauthorized physical access.
C5	Security, hardware, software, services and network configurations, with the aim that they are established, documented, implemented, monitored and critically analyzed, so that they are not modified by unauthorized or incorrect changes.
C6	Monitoring anomalous behavior and executing appropriate actions to assess possible information security incidents in networks, systems and applications.
C7	Detection and prevention of unauthorized disclosure and extraction of information by individuals or systems, preventing data leaks whether through systems, networks, or any other devices that process, store or transmit sensitive information.
C8	Protecting systems from being compromised by *malware* and preventing access to unauthorized web resources, reducing exposure to malicious content.
C9	Writing software securely, addressing secure coding principles in software development to reduce the number of potential information security vulnerabilities.
C10	No unnecessary exposure of sensitive information, being in compliance with legal, statutory, regulatory and contractual requirements, deleting information stored in information systems, devices or any other storage media when no longer needed.
C11	Masking data so that it is used in accordance with the organization's topic-specific policy, limiting the exposure of sensitive data, including personal data, and complying with legal, statutory, regulatory and contractual requirements.

Source: Authors' own creation.

Information and Computer Security

Table III. Linguistic terms and triangular fuzzy numbers.

Linguistic Terms	Triangular fuzzy numbers
Very High (VH)	(0.75, 1, 1)
High (HI)	(0.5, 0.75, 1)
Average (M)	(0.25, 0.5, 0.75)
Low (LI)	(0, 0.25, 0.5)
Very low (Z)	(0, 0, 0.25)
Null (0)	(0, 0, 0.25)

Source: Authors' own creation.

Information and Computer Security

Table IV. Linguistic assessment for criterion C1 (Threat intelligence).

Z1	C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	C11
		VH	VH	VH	VH	VH	VH	VH	VH	VH	VH
		HI	VH	VH	HI	VH	VH	VH	HI	VH	HI
		VH	VH	VH	VH	VH	VH	VH	VH	VH	VH
		HI	HI	VH	VH	VH	HI	HI	HI	HI	M
		HI	0	0	HI	0	0	M	HI	0	0
		VH	HI	VH	VH	HI	HI	VH	HI	M	LI
		VH	HI	HI	VH	HI	VH	VH	HI	HI	HI
		VH	VH	VH	VH	VH	VH	VH	VH	VH	VH
		M	LI	LI	M	HI	HI	HI	LI	Z	0
		VH	VH	VH	M	VH	HI	VH	M	Z	Z
		VH	HI	HI	VH	VH	HI	VH	M	M	M
		M	HI	M	HI	M	VH	HI	M	HI	HI
		VH	VH	HI	HI	VH	HI	HI	HI	HI	M
		HI	LI	LI	M	LI	LI	HI	M	M	HI
		HI	HI	VH	VH	HI	VH	VH	HI	VH	VH
		VH	VH	VH	VH	VH	VH	VH	VH	HI	HI
		VH	HI	VH	VH	VH	VH	VH	VH	HI	HI
		VH	HI	VH	HI	VH	VH	VH	VH	VH	VH
		VH	VH	0	VH	VH	VH	VH	VH	HI	M
		HI	HI	HI	VH	HI	HI	VH	VH	VH	HI
		HI	M	M	HI	HI	M	VH	M	LI	LI
		HI	VH	M	VH	M	VH	VH	VH	VH	VH

Source: Authors' own creation.

Information and Computer Security

Table V. Some triangular fuzzy numbers corresponding to linguistic evaluations of factor C1.

Z1	C1	C2			C3			C4		
		l	***m***	***u***	***l***	***m***	***u***	***l***	***m***	***u***
		0.75	1	1	0.75	1	1	0.75	1	1
		0.5	0.75	1	0.75	1	1	0.75	1	1
		0.75	1	1	0.75	1	1	0.75	1	1
		0.5	0.75	1	0.5	0.75	1	0.75	1	1
		0.5	0.75	1	0	0	0.25	0	0	0.25
		0.75	1	1	0.5	0.75	1	0.75	1	1
		0.75	1	1	0.5	0.75	1	0.5	0.75	1
		0.75	1	1	0.75	1	1	0.75	1	1
		0.25	0.5	0.75	0	0.25	0.5	0	0.25	0.5
		0.75	1	1	0.75	1	1	0.75	1	1
		0.75	1	1	0.5	0.75	1	0.5	0.75	1
		0.25	0.5	0.75	0.5	0.75	1	0.25	0.5	0.75
		0.75	1	1	0.75	1	1	0.5	0.75	1
		0.5	0.75	1	0	0.25	0.5	0	0.25	0.5
		0.5	0.75	1	0.5	0.75	1	0.75	1	1
		0.75	1	1	0.75	1	1	0.75	1	1
		0.75	1	1	0.5	0.75	1	0.75	1	1
		0.75	1	1	0.5	0.75	1	0.75	1	1
		0.75	1	1	0.75	1	1	0	0	0.25
		0.5	0.75	1	0.5	0.75	1	0.5	0.75	1
		0.5	0.75	1	0.25	0.5	0.75	0.25	0.5	0.75
		0.5	0.75	1	0.75	1	1	0.25	0.5	0.75

Source: Authors' own creation.

Information and Computer Security

Table VI. Relationship matrix aggregated using simple average.

	C1			C2			C3		
	l	***m***	***u***	***l***	***m***	***u***	***l***	***m***	***u***
C1	0.0000	0.0000	0.0000	0.6136	0.8636	0.9773	0.5227	0.7614	0.9091
C2	0.5568	0.7955	0.9091	0.0000	0.0000	0.0000	0.6250	0.8750	0.9886
C3	0.4886	0.7273	0.8864	0.5114	0.7500	0.8977	0.0000	0.0000	0.0000
C4	0.4432	0.6477	0.7841	0.4205	0.6136	0.7727	0.4318	0.6477	0.7955
C5	0.4318	0.6591	0.8295	0.5227	0.7614	0.9091	0.5795	0.8182	0.9318
C6	0.5682	0.8068	0.9091	0.5455	0.7841	0.8977	0.5227	0.7727	0.8864
C7	0.4545	0.6705	0.8409	0.5227	0.7500	0.8864	0.4205	0.6364	0.7955
C8	0.5455	0.7955	0.9091	0.5227	0.7500	0.8750	0.5114	0.7500	0.8750
C9	0.5114	0.7273	0.8295	0.5000	0.7273	0.8409	0.4773	0.6932	0.8182
C10	0.5000	0.7273	0.8636	0.5227	0.7614	0.9091	0.4545	0.6818	0.8409
C11	0.4205	0.6136	0.7727	0.5000	0.7273	0.8750	0.4091	0.6136	0.7955
	C4			**C5**			**C6**		
	l	***m***	***u***	***l***	***m***	***u***	***l***	***m***	***u***
C1	0.5000	0.7273	0.8523	0.6136	0.8636	0.9659	0.5682	0.8068	0.9205
C2	0.4886	0.7159	0.8636	0.5568	0.7955	0.9432	0.5227	0.7727	0.9205
C3	0.5227	0.7614	0.9205	0.5227	0.7727	0.9091	0.5909	0.8409	0.9659
C4	0.0000	0.0000	0.0000	0.4659	0.6932	0.8409	0.5227	0.7500	0.8523
C5	0.4886	0.6932	0.8182	0.0000	0.0000	0.0000	0.5568	0.7955	0.9205
C6	0.5000	0.7273	0.8636	0.5795	0.8295	0.9318	0.0000	0.0000	0.0000
C7	0.4659	0.6705	0.8068	0.5455	0.7727	0.8977	0.5682	0.7955	0.8977
C8	0.4545	0.6818	0.8523	0.5795	0.8295	0.9432	0.5568	0.8068	0.9091
C9	0.4432	0.6364	0.7955	0.5341	0.7727	0.8864	0.5000	0.7273	0.8636
C10	0.4091	0.6136	0.7841	0.4318	0.6591	0.8295	0.4886	0.7273	0.8636
C11	0.3523	0.5227	0.7045	0.3977	0.5909	0.7614	0.4091	0.6023	0.7500
	C7			**C8**			**C9**		
	l	***m***	***u***	***l***	***m***	***u***	***l***	***m***	***u***
C1	0.5795	0.8182	0.9318	0.6705	0.9205	0.9886	0.5227	0.7727	0.9205
C2	0.5682	0.8182	0.9659	0.5909	0.8295	0.9318	0.4318	0.6705	0.8523
C3	0.5227	0.7614	0.8977	0.5227	0.7500	0.9091	0.4545	0.6818	0.8523
C4	0.4659	0.6818	0.8182	0.5227	0.7500	0.8523	0.3182	0.5000	0.6818
C5	0.5455	0.7841	0.9091	0.5795	0.8182	0.9432	0.4432	0.6591	0.8295
C6	0.6023	0.8523	0.9318	0.5795	0.8295	0.9318	0.4545	0.6932	0.8523
C7	0.0000	0.0000	0.0000	0.5114	0.7273	0.8636	0.4318	0.6477	0.8068
C8	0.5227	0.7614	0.8750	0.0000	0.0000	0.0000	0.4773	0.6932	0.8523
C9	0.5568	0.7955	0.9205	0.5909	0.8295	0.9432	0.0000	0.0000	0.0000
C10	0.5227	0.7614	0.8977	0.4886	0.7045	0.8523	0.4886	0.7159	0.8523
C11	0.5682	0.7955	0.9091	0.4091	0.6023	0.7727	0.4773	0.6932	0.8409

Information and Computer Security

	C10			C11		
	l	m	u	l	m	u
C1	0.4659	0.6818	0.8409	0.4091	0.6250	0.8068
C2	0.5000	0.7386	0.8977	0.4545	0.6932	0.8636
C3	0.3977	0.6250	0.8409	0.3864	0.6136	0.8182
C4	0.3636	0.5455	0.7273	0.3295	0.5000	0.6591
C5	0.4318	0.6477	0.8182	0.3864	0.6023	0.7955
C6	0.5341	0.7727	0.8864	0.3750	0.6023	0.7614
C7	0.5114	0.7386	0.8750	0.4318	0.6591	0.8409
C8	0.4659	0.6932	0.8523	0.4205	0.6364	0.8068
C9	0.6136	0.8636	0.9773	0.5455	0.7955	0.9318
C10	0.0000	0.0000	0.0000	0.4659	0.7045	0.8409
C11	0.5568	0.7841	0.8977	0.0000	0.0000	0.0000

Source: Authors' own creation.

Information and Computer Security

Table VII. Defuzzyfied matrix Z.

Factors	C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	C11
C1	0.000	0.818	0.731	0.693	0.814	0.765	0.777	0.860	0.739	0.663	0.614
C2	0.754	0.000	0.830	0.689	0.765	0.739	0.784	0.784	0.652	0.712	0.670
C3	0.701	0.720	0.000	0.735	0.735	0.799	0.727	0.727	0.663	0.621	0.606
C4	0.625	0.602	0.625	0.000	0.667	0.708	0.655	0.708	0.500	0.545	0.496
C5	0.640	0.731	0.777	0.667	0.000	0.758	0.746	0.780	0.644	0.633	0.595
C6	0.761	0.742	0.727	0.697	0.780	0.000	0.795	0.780	0.667	0.731	0.580
C7	0.655	0.720	0.617	0.648	0.739	0.754	0.000	0.701	0.629	0.708	0.644
C8	0.750	0.716	0.712	0.663	0.784	0.758	0.720	0.000	0.674	0.670	0.621
C9	0.689	0.689	0.663	0.625	0.731	0.697	0.758	0.788	0.000	0.818	0.758
C10	0.697	0.731	0.659	0.602	0.640	0.693	0.727	0.682	0.686	0.000	0.670
C11	0.602	0.701	0.606	0.527	0.583	0.587	0.758	0.595	0.670	0.746	0.000

Source: Authors' own creation.

Information and Computer Security

Table VIII. Calculation of the maximum value of the matrix Z.

Factors	Value
C1	7.473*
C2	7.379
C3	7.034
C4	6.133
C5	6.970
C6	7.261
C7	6.814
C8	7.068
C9	7.216
C10	6.788
C11	6.375

Source: Authors' own creation. ***Note**: Maximum value.

Information and Computer Security

Table IX. Normalized matrix X.

Factors	C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	C11
C1	0.000	0.109	0.098	0.093	0.109	0.102	0.104	0.115	0.099	0.089	0.082
C2	0.101	0.000	0.111	0.092	0.102	0.099	0.105	0.105	0.087	0.095	0.090
C3	0.094	0.096	0.000	0.098	0.098	0.107	0.097	0.097	0.089	0.083	0.081
C4	0.084	0.081	0.084	0.000	0.089	0.095	0.088	0.095	0.067	0.073	0.066
C5	0.086	0.098	0.104	0.089	0.000	0.101	0.100	0.104	0.086	0.085	0.080
C6	0.102	0.099	0.097	0.093	0.104	0.000	0.106	0.104	0.089	0.098	0.078
C7	0.088	0.096	0.083	0.087	0.099	0.101	0.000	0.094	0.084	0.095	0.086
C8	0.100	0.096	0.095	0.089	0.105	0.101	0.096	0.000	0.090	0.090	0.083
C9	0.092	0.092	0.089	0.084	0.098	0.093	0.101	0.105	0.000	0.109	0.101
C10	0.093	0.098	0.088	0.081	0.086	0.093	0.097	0.091	0.092	0.000	0.090
C11	0.081	0.094	0.081	0.070	0.078	0.079	0.101	0.080	0.090	0.100	0.000

Source: Authors' own creation.

Information and Computer Security

Table X. Matrix T with calculations of vectors R and C.

Factors	C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	C11	R
C1	1.235	1.381	1.336	1.266	1.394	1.391	1.420	1.425	1.265	1.309	1.205	14.628
C2	1.310	1.266	1.331	1.250	1.372	1.371	1.404	1.399	1.240	1.298	1.197	14.437
C3	1.252	1.299	1.178	1.205	1.314	1.323	1.342	1.337	1.191	1.236	1.142	13.820
C4	1.106	1.143	1.117	0.984	1.162	1.169	1.186	1.188	1.042	1.090	1.003	12.189
C5	1.236	1.291	1.263	1.189	1.214	1.309	1.334	1.333	1.181	1.228	1.132	13.710
C6	1.294	1.338	1.303	1.235	1.356	1.264	1.387	1.381	1.226	1.283	1.171	14.237
C7	1.214	1.264	1.221	1.163	1.279	1.283	1.217	1.298	1.156	1.213	1.115	13.422
C8	1.264	1.305	1.272	1.203	1.326	1.325	1.348	1.255	1.199	1.248	1.149	13.894
C9	1.277	1.323	1.286	1.217	1.340	1.339	1.373	1.371	1.135	1.285	1.183	14.131
C10	1.215	1.262	1.222	1.155	1.264	1.272	1.302	1.292	1.159	1.123	1.116	13.383
C11	1.140	1.192	1.151	1.085	1.190	1.193	1.237	1.214	1.097	1.150	0.975	12.624
C	13.545	14.065	13.679	12.952	14.211	14.240	14.549	14.491	12.890	13.463	12.388	

Source: Authors' own creation.

Information and Computer Security

Table XI. Calculated $R + C$ and RC values.

Factor	R	C	$R + C$	$R - C$	Cause or Effect
C1	14.628	13.545	28.173	1.083	**Cause**
C2	14.437	14.065	28.502	0.372	**Cause**
C3	13.820	13.679	27.499	0.141	**Cause**
C4	12.189	12.952	25.142	-0.763	**Effect**
C5	13.710	14.211	27.921	-0.501	**Effect**
C6	14.237	14.240	28.477	-0.003	**Effect**
C7	13.422	14.549	27.971	-1.127	**Effect**
C8	13.894	14.491	28.385	-0.598	**Effect**
C9	14.131	12.890	27.021	1.241	**Cause**
C10	13.383	13.463	26.846	-0.080	**Effect**
C11	12.624	12.388	25.011	0.236	**Cause**

Source: Authors' own creation.

Information and Computer Security

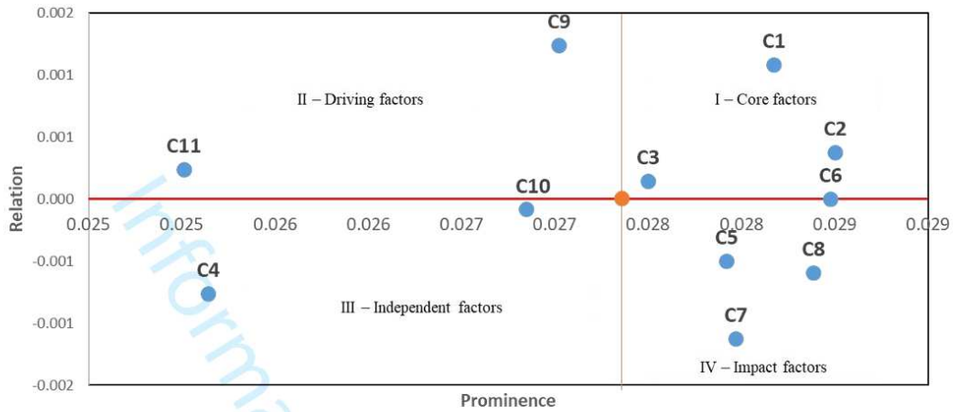
Table XII. Influence of criteria in relation to the mean of matrix T.

Factors	C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	C11
C1	1.235	1.381	1.336	1.266	1.394	1.391	1.420	1.425	1.265	1.309	1.205
C2	1.310	1.266	1.331	1.250	1.372	1.371	1.404	1.399	1.240	1.298	1.197
C3	1.252	1.299	1.178	1.205	1.314	1.323	1.342	1.337	1.191	1.236	1.142
C4	1.106	1.143	1.117	0.984	1.162	1.169	1.186	1.188	1.042	1.090	1.003
C5	1.236	1.291	1.263	1.189	1.214	1.309	1.334	1.333	1.181	1.228	1.132
C6	1.294	1.338	1.303	1.235	1.356	1.264	1.387	1.381	1.226	1.283	1.171
C7	1.214	1.264	1.221	1.163	1.279	1.283	1.217	1.298	1.156	1.213	1.115
C8	1.264	1.305	1.272	1.203	1.326	1.325	1.348	1.255	1.199	1.248	1.149
C9	1.277	1.323	1.286	1.217	1.340	1.339	1.373	1.371	1.135	1.285	1.183
C10	1.215	1.262	1.222	1.155	1.264	1.272	1.302	1.292	1.159	1.123	1.116
C11	1.140	1.192	1.151	1.085	1.190	1.193	1.237	1.214	1.097	1.150	0.975

Source: Authors' own creation.

Information and Computer Security

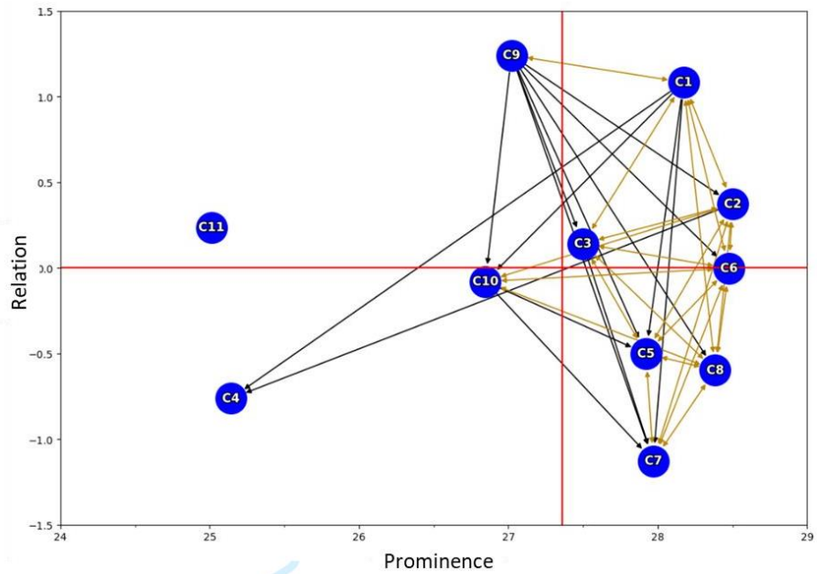
Figure 1. Causal Diagram and its Quadrants



Source: Authors' own creation.

Information and Computer Security

Figure 2. Relational Influence Map.



Source: Authors' own creation.

and Computer Security