UNIVERSIDADE FEEVALE

VINÍCIUS NUNES KELLER

##### MODELO DE MATURIDADE EM SEGURANÇA DA INFORMAÇÃO APLICADO A GESTÃO EXECUTIVA

(Título Provisório)

###### Anteprojeto de Trabalho de Conclusão

Novo Hamburgo

2022

VINÍCIUS NUNES KELLER

##### MODELO DE MATURIDADE EM SEGURANÇA DA INFORMAÇÃO APLICADO A GESTÃO EXECUTIVA

(Título Provisório)

Anteprojeto de Trabalho de Conclusão de Curso, apresentado como requisito parcial

à obtenção do grau de Bacharel em

Sistemas de Informação pela

Universidade Feevale

Orientador: Sandra Teresinha Miorelli

Novo Hamburgo

2022

**RESUMO**

Com a avanço da tecnologia, cada vez mais a informação está distribuída, não apenas no meio digital, mas também em processos, ambientes físicos e pessoas, cada uma dessas áreas está sujeita a níveis diferentes de vulnerabilidades, representando um risco para a confidencialidade, integridade ou a disponibilidade das atividades de uma organização. Isso gera uma necessidade da organização em entender o quão seguras estão as suas informações e à quais possíveis vulnerabilidades ela está exposta. As inúmeras possibilidades de vulnerabilidades que todas as áreas possam trazer, geram um questionamento de como identificar quais informações já possuem um nível adequado de segurança e quais ainda não possuem. Por onde iniciar essa busca e como progredir nesses controles é uma atividade complexa que não deve ficar amparada ao conhecimento empírico de um gestor. Uma maneira de medir o quão hábil são os processos de uma organização é utilizando uma avaliação de maturidade através de um modelo de maturidade, que apontam o estágio em que a organização está situada em determinado quesito, apoiando o gestor executivo a definir o melhor caminho para obter o máximo sucesso. Sendo assim, este trabalho tem por objetivo, pesquisar modelos de maturidade em segurança da informação, que possa(m) ser usados para identificar o estágio em que uma organização se encontra em relação a segurança da informação e elaborar um modelo que possa amparar as tomadas de decisões na progressão de controles.

Palavras-chave: Segurança da informação. Modelos de maturidade. Gestão de segurança da informação.

**SUMÁRIO**

MOTIVAÇÃO 6

METODOLOGIA 9

CRONOGRAMA 11

BIBLIOGRAFIA 13

# MOTIVAÇÃO

Nos últimos anos, o avanço da tecnologia tornou possível a integração dos dados em nível global, tornando possível a troca de informações vitais, por meio da união das telecomunicações, Internet, comunicações digitais em banda larga, dispositivos móveis e digitalização dos conteúdos de mídia. Essa integração cria uma “infraestrutura de base” que aumenta ainda mais esse avanço e desenvolvimento tecnológico (TURBAN, 2013).

Esse crescimento da tecnologia, traz consigo uma necessidade de segurança da informação, pois, conforme cita Liguori (2021), a medida em que o ambiente digital está cada vez mais presente, tanto para a realização de atividades pessoais quanto para profissionais, mais surge a necessidade da obtenção de um conjunto de técnicas para garantir a confidencialidade, integridade, disponibilidade e resiliência dos sistemas de informação.

Em concordância a isso, em 1992 foi criada a certificação ISO 27001, que tem por objetivo garantir que a organização adote um conjunto de requisitos, processos e controles que mitiguem e venham a gerir corretamente os riscos das organizações (ABNT NBR ISO/IEC 27001, 2022).

Diante disso, sabe-se que é a própria arquitetura da internet que possibilita ou impossibilita todos os comportamentos que acontecem de forma online, por isso, a possibilidade de controle dos conteúdos, como monitorar e filtrar, dependem diretamente dos provedores de conexão e aplicação e das limitações impostas por mecanismos de segurança das redes, como os empregados na área de segurança da informação (LIGUORI, 2021).

Além disso, conforme a norma ISO 27001, “uma das grandes preocupações da atualidade é efetivamente a confiança no tratamento adequado da informação sensível da organização” (ABNT NBR ISO/IEC 27001, 2022).

Por muito tempo, houve uma falta de compreensão da importância de focar um único setor da empresa em somente desempenhar a função de acompanhar e gerenciar os riscos que podem afetar as informações organizacionais. Os ataques eram geridos depois que aconteciam, não havia um mecanismo de prevenção para proteger a empresa dessas ameaças. Para as organizações, essa prevenção tratava-se de um custo, ainda não era considerada um investimento que poderia evitar o interrompimento de suas atividades e, por isso, não era colocada como um processo essencial dentro das etapas produtivas (TURBAN, 2013).

Segundo Kerzner (2003, apud Harrison et al., 2006, p. 2):

[...] a simples utilização do gerenciamento de projetos sem a avaliação do grau de padronização, do nível de eficiência e da eficácia de sua metodologia, mesmo que por um longo período de tempo não eleva o nível de excelência da empresa com relação ao gerenciamento de projetos. Ao invés disso, o resultado de sua aplicação sem controle e padronização pode ser representado por uma sucessão de erros e fracassos, fazendo com que a empresa passe por um lento e duro aprendizado através das ações de seus próprios erros e não através dos ensinamentos e das melhores práticas de outras empresas. É em um cenário como o descrito acima, que um modelo de maturidade em gerenciamento de projetos, busca fornecer um suporte para que a empresa possa definir, avaliar e desenvolver seus processos de gerenciamento de projetos com o objetivo de atingir vantagens competitivas, através de um diferencial de seu desempenho em relação à concorrência.

Além disso, Sêmola (2014) afirma que, para uma consistente análise de riscos, é preciso contar com recursos humanos que tenham diferentes competências, ferramentas automatizadas que auxiliem no apoio e gestão do levantamento e uma base de conhecimento em segurança, que esteja constantemente se atualizando.

Para isso, inicialmente neste momento do trabalho já apresento dois modelos de maturidade que desempenham, atualmente, auxílio no processo de segurança da informação dentro das empresas: Esses modelos de maturidade são: CobiT (ITG1, 2007) e OWASP (SAMM).

 Além disso, esta pesquisa possui uma motivação pessoal do pesquisador buscando conhecer uma nova área em sua carreira profissional e que apresenta uma grande carência no mercado de profissionais que entendam a necessidade de cada ação dentro da área de segurança da informação e saibam aplicar de forma equilibrada e sensata buscando agregar valor ao contexto de cada organização.

Por fim, este trabalho busca amparar o gestor nas tomadas de decisões olhando para o processo de como iniciar e progredir dentro da área de segurança da informação em uma organização. Para isso propõe responder a seguinte questão de pesquisa: como identificar o estágio em que a organização se encontra em relação a segurança da informação e como progredir nesse âmbito a partir de uma estratégia estruturada e validada com um modelo de maturidade?

**OBJETIVOS**

Objetivo geral

 Identificar o estágio em que uma organização se encontra em relação a segurança da informação e como progredir nesse âmbito a partir de uma estratégia estruturada e validada com um modelo de maturidade.

Objetivos específicos

1. Mapear modelos de maturidade existentes para segurança da informação;
2. Identificar em que estágio de maturidade a organização de encontra;
3. Mapear estratégias de como progredir dentro do modelo;
4. Aplicar as estratégias de identificação de estágio de maturidade e progressão dentro do modelo em uma organização.

# METODOLOGIA

Quanto a sua natureza, segundo Prodanov e Freitas (2013), este estudo é caracterizado como pesquisa aplicada, pois objetiva gerar conhecimento para a prática dirigida a solução de um problema específico. O trabalho será abordado de forma qualitativa e quantitativa, pois sua avaliação acontecerá com base na conformidade da solução perante a problemática proposta. A figura a seguir indica os demais conceitos a serem adotados na metodologia deste trabalho.

Figura 1 – Tipos de pesquisa cientifica



Fonte: adaptado de Prodanov e Freitas (2013)

No que tange aos fins da pesquisa, pode-se enquadrar este projeto como uma pesquisa exploratória, seguindo a ideia de Prodanov e Freitas (2013), já que o conhecimento necessário para sua realização terá fundamentação em levantamentos bibliográficos e análises de exemplos.

Os procedimentos que serão adotados no desenvolvimento deste trabalho, enquadram-se em duas categorias, ambas amparadas pelos conceitos de Prodanov e Freitas (2013), sendo elas:

a) Pesquisa bibliográfica: o conhecimento necessário para produção do trabalho será extraído de material publicado, como livros, revistas artigos científicos e especificações técnicas;

b) Pesquisa experimental: será determinado um objeto de estudo e as variáveis capazes de influenciá-lo, assim com as formas de controle e observação dos seus efeitos sobre o objeto.

Este estudo se dará na pesquisa bibliográfica sobre o tema modelos de maturidade para o contexto de segurança da informação, elucidando os motivos de adoção, as práticas implantadas, os benefícios percebidos e as dificuldades enfrentadas ao implantar e progredir dentro de um modelo de maturidade. Utilizando informações e conhecimentos adquiridos a partir da leitura de livros, fóruns, sites de tecnologia, informática e profissionais da área o presente trabalho busca entender os modelos de maturidade para a segurança da informação onde será possível identificar o estágio de uma organização dentro do modelo e como progredir dentro do mesmo.

O processo será fragmentado em etapas onde será necessário buscar e entender os modelos existem e relacioná-los de forma adequada a realidade das organizações. Este modelo será aplicado em uma organização onde será possível mensurar o nível e eficácia dele.

# CRONOGRAMA

Trabalho de Conclusão I

|  |  |
| --- | --- |
| Etapa  | Meses |
| Ago | Set | Out | Nov | Dez |
| Escolha do tema de pesquisa. |  |  |  |  |  |
| Revisão da literatura em segurança da informação. |  |  |  |  |  |
| Elaboração do anteprojeto com justificativa, objetivos, problematização e metodologia. |  |  |  |  |  |
| Pesquisar sobre modelos de maturidade em segurança da informação. |  |  |  |  |  |
| Levantamento de estudo de caso/empresas que utilizam modelos de maturidade em segurança da informação. |  |  |  |  |  |
| Levantamento do local para aplicação do modelo. |  |  |  |  |  |
| Escrita do Trabalho de conclusão I. |  |  |  |  |  |

Trabalho de Conclusão II

|  |  |
| --- | --- |
| Etapa  | Meses |
| Fev | Mar | Abr | Mai | Jun |
| Definir um modelo de maturidade conforme resultados identificados interiormente. |  |  |  |  |  |
| Aplicar o modelo proposto na organização escolhida identificando em que nível de maturidade a organização se encontra |  |  |  |  |  |
| A partir da identificação utilizar o modelo para progredir amparar na decisão de como progredir dentro dele. |  |  |  |  |  |
| Avaliar os resultados obtidos. |  |  |  |  |  |
| Finalizar monografia atribuindo os resultados do estudo. |  |  |  |  |  |

# BIBLIOGRAFIA

ABNT NBR ISO/IEC 27001:2013. **Sistemas de gestão da segurança da informação**. Portal Informativo. Disponível em: <https://www.27001.pt/>. Acesso em 06 de junho de 2022.

HARRISON, P. D.; MARTINS, M. R.; TSAI, LWK. **Uma aplicação do modelo de maturidade PMBoK maturity model**. Encontro Nacional de Engenharia de Produção – Enegep, v. 26, 2006.

ITGI *–* IT GOVERNANCE INSTITUTE*.* CobiT 4.1 - **Control Objectives for Information and related Technology - Framework***.* Rolling Meadows - USA: [s.n.], 2007.
Disponível em < https://www.isaca.org/resources/cobit>. Acesso em 11 de setembro de 2022.

LIGUORI, Carlos. **Direito e criptografia**: direitos fundamentais, segurança da informação e os limites da regulação jurídica na tecnologia. São Paulo: Saraiva Jur, 2021.

OWASP **(SAMM) - Software Assurance Maturity Model (SAMM).** Disponível em < https://owasp.org/www-project-samm/>. Acesso em 11 de setembro de 2022.

PRODANOV, C. C.; DE FREITAS, E. C. **Metodologia do trabalho científico: métodos e técnicas da pesquisa e do trabalho acadêmico**. 2ª Edição. Editora Feevale, 2013.

SÊMOLA, M. **Gestão da segurança da informação: uma visão executiva**. 2. ed. Rio de Janeiro: Elsevier/Campus: 2014.

TURBAN, E. **Tecnologia da Informação para Gestão**. 8. Porto Alegre, RS: Bookman, 2013. recurso on-line.