



**Centro Universitário do Planalto Central Aparecido dos Santos - UNICEPLAC**  
**Curso de Sistemas de Informação**  
**Trabalho de Conclusão de Curso**

**Gerenciamento de projetos & Segurança da Informação:**  
os impactos da gestão de projetos na segurança da informação.

Gama-DF

2021

**MARCELO JUNIO SIQUEIRA GONÇALO  
PEDRO HENRIQUE ALMEIDA MESQUITA  
FABIO RODRIGUES DE SOUZA**

**Gerenciamento de projetos & Segurança da Informação:  
os impactos da gestão de projetos na segurança da informação.**

Artigo apresentado como requisito para conclusão do curso de Bacharelado em Sistemas de Informação pelo Centro Universitário do Planalto Central Aparecido dos Santos – Uniceplac.

Orientador: Prof. Me. Jorge Alberto dos Santos

Gama-DF

2021

**MARCELO JUNIO SIQUEIRA GONÇALO  
PEDRO HENRIQUE ALMEIDA MESQUITA  
FABIO RODRIGUES DE SOUZA**

**Gerenciamento de projetos & Segurança da Informação: os impactos da gestão de projetos na segurança da informação.**

Artigo apresentado como requisito para conclusão do curso de Bacharelado em Sistemas de Informação pelo Centro Universitário do Planalto Central Aparecido dos Santos – Uniceplac.

Gama-DF, 05 de dezembro de 2021.

**Banca Examinadora**

---

Prof. Jorge Alberto dos Santos  
Orientador

---

Prof. Nome completo  
Examinador

---

Prof. Nome Completo  
Examinador

# **Gerenciamento de projetos & Segurança da Informação:** os impactos da gestão de projetos na segurança da informação.

Marcelo Junio Siqueira Gonçalves

Pedro Henrique Almeida Mesquita

Fabio Rodrigues de Souza

## **Resumo:**

Essa pesquisa trata-se de analisar os impactos que a gestão de projetos tem na segurança da informação no ambiente de um do projeto de TI. O gerenciamento de projetos é de enorme importância para grande parte das organizações públicas e privadas e, nem sempre recebe a devida atenção quando um projeto é iniciado. A falta do uso do processo de gerenciamento de projetos pode contribuir para o não tratamento de diversas falhas na área de segurança da informação. O gerenciamento de projetos possui diversas áreas que possuem seus objetivos definidos, e dentre elas existem áreas que acabam afetando diretamente a segurança da informação, não somente do projeto, mas como da empresa de uma maneira geral. Os resultados deste trabalho demonstram que o gerenciamento de projetos pode contribuir de maneira positiva para área de segurança da informação.

**Palavras-chave:** Gerenciamento de Projetos. Segurança da Informação. PMBOK.

## **Abstract:**

This research is about analyzing the impacts that project management has on information security in the environment of an IT project. Project management is of enormous importance for most public and private organizations and it doesn't always receive due attention when a project is initiated. The lack of use of the project management process can contribute to the non-treatment of several failures in the information security area. Project management has several areas that have their objectives defined, and among them there are areas that end up directly affecting information security, not only for the project, but for the company in general. The results of this work demonstrate that project management can positively contribute to the information security area.

**Keywords:** *Management of projects. Information security, PMBOK.*

## 1 INTRODUÇÃO

O uso de sistemas de informação tem sido cada vez mais percebido em inúmeras atividades no ambiente das empresas públicas e da iniciativa privada. A integração desses sistemas é dada pela facilitação e efetividade de seus resultados quando aplicada corretamente. Entretanto, a integração de sistemas computacionais abre brechas para diversas ameaças que comprometem diretamente a área de segurança da informação.

A segurança da informação é de grande importância para o contexto que envolve os sistemas de informação. No aspecto em que é aberto espaço para novas tecnologias, também são endereçadas trilhas para novas falhas de segurança e possíveis ameaças digitais. Por isso, é necessária uma revisão de métodos, procedimentos e frameworks de segurança da informação quando possível, para que se tenha a melhoria dos serviços de TI.

Todo projeto de TIC – Tecnologia da Informação e Comunicação - que utilize boas práticas de mercado se utiliza de métodos para gerenciamento de projetos, é essa gestão que se responsabilizará pelo sucesso ou falha de um projeto na área de TI – Tecnologia da Informação. Quando se planeja um projeto é necessário ter em mente que essa gerência será responsável por planejar diversas etapas do projeto, desde etapas imediatas à possíveis situações de riscos futuras. Há vários processos por trás de um planejamento de um projeto, e alguns desses processos podem afetar a segurança da informação e até mesmo a segurança do projeto todo.

Diante das primeiras abordagens apresentadas este trabalho científico tem como objetivo geral analisar os aspectos teóricos da forma como o gerenciamento de um projeto podem impactar a área de segurança da informação.

## 2 GERENCIAMENTO DE PROJETOS

Para abordar o assunto sobre gerenciamento de projetos é necessário o entendimento do que é um projeto. Projeto, segundo o guia PMBOK (*Project Management Body of Knowledge, 2012*), pode-se resumir como um esforço temporário empreendido para criar um produto, serviço ou resultado exclusivo, ou seja, atingir a meta do projeto dentro de um prazo determinado. Projetos são mecanismos que impulsionam empresas para realizar novos serviços ou melhorar

seus serviços existentes. Porém, para que o projeto obtenha sucesso e cumpra suas metas, é necessário um planejamento adequado das etapas do projeto.

Segundo o guia PMBOK (PMI – *Project Managment Institute*, 2012) o gerenciamento de projetos pode ser categorizado como um conjunto de ferramentas, ideias e práticas que são utilizadas para planejar, executar, monitorar e encerrar um projeto. Essa gestão é dividida em diversas áreas de conhecimento, que proporcionam um planejamento e controle de projetos por meio da conexão destas várias áreas.

O guia PMBOK é um guia criado para, basicamente, orientar e indicar boas práticas no gerenciamento de projetos. Hors, Cora et al (2012, p. 480-490) diz que o PMBOK descreve 42 processos em 5 grupos, sendo eles Iniciação, Planejamento, Execução, Monitoramento e Conclusão. Dividindo esses processos nas 9 áreas de conhecimento: Integração, Escopo, Tempo, Custo, Qualidade, Pessoas, Comunicações, Riscos e Aquisições. É fortemente recomendado basear seu gerenciamento de projetos a partir deste guia, é seguindo suas instruções e conscientizando o uso dessas diversas áreas de conhecimento que é possível obter uma gerência de projetos sólida e bem planejada.

O gerenciamento de projetos é utilizado por diversas empresas, a sua relevância se dá por conta de sua efetividade no âmbito profissional. Essa gestão pode facilitar, padronizar e assegurar a efetividade de um planejamento quando executado corretamente. A implantação de uma boa gestão de projetos pode fazer toda a diferença entre o sucesso ou falha de um projeto, podendo afetar não só o serviço da empresa como outras áreas da mesma, como a segurança da informação.

## **2.1 Vantagens de usar o gerenciamento de projetos**

Sem a organização, padronização e monitoramento executado pelo gerenciamento de projetos, é muito comum o projeto fracassar e prejudicar bastante uma empresa ao ponto de não retorno no mercado. É observado em vários estudos que as empresas que seguem os padrões determinados pelo guia PMBOK, utilizam de frameworks de apoio e efetuam de fato todos os passos de um bom gerenciamento de projetos obtiveram uma melhor recepção no mercado. Já em

empresas que começaram sem um bom gerenciamento de projetos, porém, aplicaram essas boas práticas após a empresa ter sido criada, é possível ver aumentos na eficácia de produção e melhora geral de serviços.

O gerenciamento de projetos não é apenas importante para o desenvolvimento do projeto como também é capaz de trazer inúmeros benefícios empresariais dentro do mercado. Dentre essas diversas vantagens, vale evidenciar sete delas; maior controle de processos, representando a centralização de etapas, recursos, prazos e envolvidos; cumprimento de cronograma, sendo o comprometimento de entregar etapas dentro do prazo estipulado do projeto; monitoramento da lucratividade, muito útil para controle de despesas e conscientizar a gestão de custos; riscos minimizados, antecipa soluções preventivas e corretivas para minimizar riscos e impedir possíveis problemas futuros dentro do projeto; agilidade na tomada de decisões, facilita a tomada de ações imediatas e eficazes quando necessário dentro de um projeto; maior engajamento do time, uma equipe empenhada ao projeto aumenta bastante a qualidade dos processos e facilita o monitoramento do projeto quando necessário a tomada de decisões e maior satisfação do cliente, pois é de interesse do gerenciamento de projetos a concordância com o cliente sobre o projeto e seu resultado esperado.

## **2.2 Importância de uma gestão de projetos adequada para área de sistemas de informação**

De acordo com Rabechini Jr. (1996), é necessário identificar quais competências uma empresa precisa construir para ganhar e manter uma vantagem competitiva no mercado empresarial. Uma visão de negócio adequada é necessária para se manter competitivo no meio organizacional. Pinto & Slevin (1983) definem que um projeto bem-sucedido é aquele que consegue atingir quatro principais critérios: tempo, custo, eficácia e satisfação do cliente. Esses critérios de êxito dos projetos de TI, podem ser aplicados para os sistemas de informação, que são itens relevantes no contexto de prestação de serviços de TI de uma empresa.

Os sistemas de informação nas organizações podem ser implementados como métodos que permitem a coleta, armazenagem, recuperação e disseminação de informações para fins específicos dessa organização (TURBAN et al, 2007). Os sistemas de informação apoiam diretamente funções operacionais, gerenciais e de tomada de decisões dentro de organizações

(RAINER JR. e CEGIELSKI, 2011). Entende-se que o gerenciamento de projetos pode afetar as informações de uma organização, que por vez afeta como o gerenciamento de projetos decorre e auxilia no projeto inteiro. Gerenciamento de projetos e sistemas de informação se complementam e auxiliam um ao outro dentro de uma organização, e é a partir dessa relação mútua que é possível melhorar e padronizar boas práticas no meio organizacional. Dentre a ajuda mútua, uma área que pode ser beneficiada com o uso do gerenciamento de projetos é a de segurança da informação.

### **3 SEGURANÇA DA INFORMAÇÃO**

A segurança da informação é de grande importância na área de tecnologia da informação e comunicação (TIC). A informação tem ganhado muita importância para as organizações nos últimos anos. De acordo com Freitas & Kladis (1995) a importância da informação aumenta de acordo com o crescimento da sociedade e das organizações. Informação pode ser vista como um recurso estratégico para auxiliar e melhorar os serviços das organizações e ser considerada como uma ferramenta com diversas utilidades. Porém, essas informações sempre estarão sujeitas a vulnerabilidades e ameaças, por isso, é necessário reduzir possíveis riscos à essas informações visando minimizar as perdas da organização. A segurança da informação surge no cenário empresarial para proteger e gerenciar as informações dentro do ambiente organizacional.

De acordo com Dias (2004) a definição de segurança da informação é a proteção de informações, sistemas, recursos e serviços contra erros e manipulações não autorizadas das informações. A segurança da informação seria uma forma de minimizar impactos de possíveis falhas de segurança que possam comprometer as informações. A Associação Brasileira de Normas Técnicas – ABNT (2013) conceitua que a segurança da informação é definida por três pilares: a integridade; que confirma a validação da informação; a disponibilidade, que afirma a disponibilidade da informação quando exigida por processos de negócios presentes ou futuros; e a confidencialidade, que se compromete com a proteção de informações e a divulgação indevida dessas informações.

É necessário ter disciplina organizacional e investimentos em segurança da informação para minimizar riscos. A segurança da informação depende de um conjunto de processos executados com boas políticas e regulamentações fundamentadas (Arruda et al. 2020). E foi a



partir dessa necessidade de boas práticas e padronização que os conceitos das ISO/IEC 27001 e ISO/IEC 27002 foram criadas. Essas normas foram criadas com o intuito de modelar de maneira eficiente um SGSI (Sistema de Gestão de Segurança da Informação) dentro de organizações, e é a partir dessas padronizações que é possível aumentar o nível de segurança da informação no meio organizacional.

### **3.1 ISO 27001 e ISO 27002**

ISO – *International Standardization of Organization* - é a sigla conhecida e traduzida para representar a Organização Internacional de Normalização, sua criação tem o propósito de facilitar a coordenação e padronizar práticas internacionalmente. A ABNT ISO/IEC 27001 foi criada com a ideia de padronizar práticas para gestão da segurança da informação, enquanto a norma ABNT ISO/IEC 27002 tem o objetivo de definir diretrizes sobre as metas determinadas para a gestão da segurança da informação (ABNT, 2005). A ISO 27001 diz que é ideal que a alta administração da organização deveria criar planos de contingências para garantir que todo o pessoal responsável pelas mudanças tenha a competência necessária para executar de maneira apropriada as tarefas estabelecidas (NBR ISO/IEC 27001, 2006).

De acordo com a Associação Brasileira de Normas Técnicas (ABNT) em referência à Norma Brasileira (NBR) a ISO/IEC 27002, os controles em sistemas de informação, quando executados corretamente, tem como princípio garantir que os objetivos dos negócios da organização e a segurança da informação sejam atendidos (NBR ISO/IEC 27002, 2013). A ISO/IEC 27002 é uma norma que auxilia e tem como objetivo garantir que os principais pilares da segurança da informação (confidencialidade, integridade e disponibilidade) estejam de acordo com o esperado de uma organização que almeja por uma segurança de dados eficiente.

### 3.2 Gestão de Segurança da Informação

Os riscos que os avanços tecnológicos trouxeram para as organizações são diversos. Como as informações começaram a se concentrar em um único lugar, a grande quantidade dessas informações começou a ser um problema para a segurança, o uso de microcomputadores, redes locais e remotas, disseminação de informática para diversos setores da sociedade e abertura comercial da internet contribui para o aumento de riscos de segurança da informação (Silva Netto et al. 2007), e com o intuito de diminuir esses riscos e implementar boas práticas, a Gestão de Segurança da Informação (GSI) foi criada.

GSI pode ser considerada como um processo administrativo, que em conjunto com a ISO 27002 pode gerir dados e informações importantes da organização. Para Sêmola (2003), a gestão de segurança da informação pode ser classificada em três aspectos sendo; tecnológicos, como redes, computadores, internet e outros derivados; físicos, sendo esses os possíveis riscos e vulnerabilidades no ambiente da organização; e por fim humanos, que são os usuários informados incorretamente, por muitas vezes são os principais responsáveis por falhas de segurança. É comum que as organizações foquem mais no aspecto tecnológico, deixando os aspectos físicos e humanos vulneráveis e fracos contra possíveis ataques.

A ISO 27002 (2013) define 127 controles que serve de base para o sistema de gestão de segurança da informação, agrupado em 11 seções: Política de Segurança da Informação; Organização da Segurança da Informação; Gestão de Ativos; Segurança em Recursos Humanos; Segurança Física e do Ambiente; Gestão das Operações e Comunicações; Controle de Acesso; Aquisição, Desenvolvimento e Manutenção dos Sistemas de Informação; Gestão de Incidentes da Segurança da Informação; Gestão da Continuidade do Negócio e Conformidade (Silva Netto et al. 2007). O SGSI (Sistema de gestão de segurança da informação) tem o propósito de auxiliar a gestão de projeto a manter e melhorar a segurança do projeto, a adoção da ISO 27002 em conjunto com um SGSI eficiente, permite a organização estar em concordância com boas práticas de gestão da segurança da informação, consequentemente reforçando a segurança da informação dessa organização.

## 4 PROCEDIMENTOS METODOLÓGICOS

O guia PMBOK é uma forma de padronizar os processos de planejamento de projetos, aprimorando a eficiência do projeto, entretanto, o PMBOK apenas auxilia na etapa de planejamento e execução de projetos de TI. Seguindo a abordagem mais conhecida do gerenciamento de projetos, geralmente nas fases de planejamento e de monitoramento e controle que a segurança da informação pode ficar comprometida, é a parte crucial que se deve utilizar ao máximo os conhecimentos providos a partir do PMBOK para assegurar quais possíveis falhas podem ocorrer e como isso afeta a segurança do meio de trabalho onde o projeto está sendo desenvolvido. Essas observações que podem ser consideradas detalhes são de imensa importância, são essas especificações que definem como o projeto inteiro irá se comportar em diante do planejamento.

O uso de boas práticas de governança de TI para organizações é importante, não somente o guia PMBOK, mas também de frameworks de apoio, governança de TI competente dentre outros, que podem auxiliar as organizações em sua busca por uma melhor segurança de informação. Também é necessário conscientizar as organizações da importância das informações que a empresa possui, independentemente do tipo de serviço prestado por ela. Embora a maioria das organizações já tenham compreendido a necessidade de segurança da informação, diversas outras organizações subestimam a importância que suas informações carregam para a execução de seus serviços e no funcionamento deles como um todo, essa falta de atenção faz com que seus serviços, e possíveis projetos futuros, fiquem vulneráveis a ataques. Quando a organização que faz descaso de suas informações e conseqüentemente da segurança delas, descobre a real importância dessas informações: ou um ataque já foi efetuado, acarretando prejuízos, ou a organização já está bastante vulnerável a ataques.

Para realização deste trabalho foram realizadas pesquisas em artigos acadêmicos, livros temáticos e sítios renomados para correlacionar os assuntos gerenciamento de projetos e segurança da informação. De fato, os assuntos se complementam, pois pode-se observar que a necessidade de inovação e padronização de serviços das organizações aumentou muito com o passar dos anos, porém a quantidade de ataques cibernéticos também aumentara

proporcionalmente. O gerenciamento de projetos é uma ferramenta muito importante para o mercado empresarial e o seu uso é de extrema importância não somente para o sucesso da organização e de seus serviços, como também para a segurança da informação da organização. Os artigos citados neste trabalho evidenciam a necessidade de conscientizar as organizações de boas práticas na hora de planejar seus serviços, ocasionando em uma melhora de serviços e segurança da informação na organização.

## **5 APRESENTAÇÃO E ANÁLISE DOS DADOS**

O conceito de gestão da segurança da informação ainda é um tema para ser explorado com mais cuidado e intensidade nas organizações. A necessidade de estabelecer processos e ferramentas para gerenciar as atividades relacionadas à segurança da informação surgiu a partir das dificuldades encontradas pelas empresas na utilização desses recursos com segurança e conformidade. As empresas estão mais conscientes hoje do valor das informações, principalmente as organizacionais, e estão cada vez mais protegendo seus dados e informações. Segundo ABNT (2008), administrar as vulnerabilidades de segurança da informação aos quais se está sujeito contribui de maneira significativa para o sucesso da organização e de seus negócios.

Em tempos modernos grande parte das organizações já possuem determinada consciência organizacional acerca da importância da informação para o negócio. Porém, observa-se que ainda falta conscientizar a importância do gerenciamento efetivo e seguro dessas informações no meio organizacional. O uso das informações para uma empresa pode ser usado de diversas formas, e é necessário saber como gerenciar o uso dessas informações com segurança, seja na organização toda para até mesmo em pequenos projetos dentro dessa organização. O GSI auxilia a organização a manter o uso seguro de informações quando necessário ou planejado algo dentro da organização, como um projeto novo, migração de um serviço, aprimoramento de um serviço já existente da organização dentre outros. O gerenciamento inadequado dessas informações pode causar diversas falhas de segurança (da informação, do projeto e da organização toda), possivelmente deixando a organização vulnerável à ataques e sequestro dessas informações.

Para exemplificar os impactos do gerenciamento da informação em uma organização, utilizou-se um caso recente ocorrido nos Estados Unidos. Foi publicada pela BBC News a notícia de que houve um ataque cibernético à maior rede de oleodutos dos EUA, a Colonial Pipeline. O

ataque ocorreu porque a facção criminosa (grupo conhecido mundialmente como *DarkSide*) encontrou uma maneira de invadir o sistema a partir da grande quantidade de usuários que acessavam o sistema remotamente. De acordo com alguns pesquisadores e com a ajuda da *Digital Shadows* (empresa de segurança cibernética) foi descoberto que a facção obteve detalhes de *logins* de funcionários a partir dos programas de acesso remoto (como *GoogleView*, *Teamspeak* etc), conseguindo assim subtrair mais de 100 GB de informações da empresa e exigindo um resgate pago pelas informações. A empresa teve a reação imediata de desligar parte de seus sistemas para conter o problema, porém os estragos já tinham ido além de somente prejuízos financeiros.

Constatou-se que cerca de 45% de todas as formas de abastecimento da costa leste dos EUA eram providas a partir dessa única organização. Por conta deste ataque cibernético vários funcionários não puderam trabalhar porque não tinham como abastecer seus carros, afetando muitas outras empresas e seus funcionários, além dos relatos de analistas que deduziram um aumento nos preços dos combustíveis, que deveriam sofrer um aumento entre 2 à 3% a mais que o comum devido a essa falha geral no sistema. É necessário aprofundar a pesquisa para entender os fatores que impactaram a empresa, e a causa raiz que gerou esse incidente. Porém, em uma primeira análise, pode ter ocorrido falhas na hora de planejar a migração de seus serviços para as plataformas remotas.

Uma gestão de projetos de TI não necessariamente evitaria o ataque, entretanto, alguns eventos de riscos seriam mitigados, e os prejuízos poderiam ser menores, se a organização tivesse tido um melhor gerenciamento de segurança da informação, que estivesse em conformidade com o guia PMBOK. Se durante a migração de seus serviços a organização tivesse revisado com a GSI sobre os riscos que essa migração traria para as informações da organização e se o planejamento desta migração tivesse ocorrido de maneira menos apressada e mais segura, os prejuízos causados poderiam ter sido bem menores e mais controláveis, essa é a importância de um bom gerenciamento de projeto e do gerenciamento de segurança da informação.

De acordo com a teoria de base adotada e conforme análises realizadas, alguns itens que o gerenciamento de projetos poderia ter auxiliado a área de segurança da informação para o exemplo ofertado neste trabalho seriam:

- a) O uso de um gerenciamento de segurança da informação otimizado, pois poderia ser de interesse da organização gerenciar as atividades de seus serviços de maneira segura e seguindo padrões de mercado.
- b) A fiscalização e uso adequado do processo de gerenciamento de acesso, que tem como uma de suas funções principais realizar o monitoramento de perfis que tem acesso a infraestrutura de TI ou serviços de TI no ambiente da organização.
- c) A transição de serviços de TI que estivesse de acordo com boas práticas de gerenciamento de projetos, minimizando os impactos que poderiam ser causados durante a transição do serviço da organização quando o mesmo foi requisitado.

## **CONSIDERAÇÕES FINAIS**

Muitos projetos de TI são planejados e executados todos os dias, porém, nem sempre os mesmos são gerenciados de maneira inteligente e segura. É necessário a conscientização da importância de um bom gerenciamento para o sucesso e segurança do meio de trabalho, é a partir desse princípio que a leitura e a utilização correta de meios eficientes e seguros da gerência de projetos podem deixar de ser considerado apenas um detalhe e realmente ser validado como algo vital no ramo de TI.

Se levarmos em consideração as consequências do ocorrido na Colonial Pipeline e como toda a situação decorreu, imagine a importância de uma boa gerência nas etapas de planejamentos em organizações como bancos, redes federais, eleições etc. O bom manuseio de gerenciamento causaria um aumento significativo na qualidade e demanda da mão de obra de profissionais da área de TI, além de garantir mais segurança cibernética à usuários mais mal informados à tecnologia. Muito dos casos de falhas na segurança da informação vêm a partir do manuseio indevido dos usuários sobre o conhecimento e uso seguro do sistema, por isso é necessário que as organizações informem seus funcionários sobre a importância de um bom gerenciamento de projetos e segurança da informação. É a partir da conscientização dos usuários, uso eficiente de frameworks de apoio e uma governança de TI competente que é possível diminuir as vulnerabilidades que as organizações possuem, dificultando e diminuindo a probabilidade de ataques futuros.

## REFERÊNCIAS

ABNT (2008). ABNT NBR ISO/IEC 27005 - Gestão de riscos de segurança da informação. Associação Brasileira de Normas Técnicas, Rio de Janeiro.

Arruda, Paulo Cesar Andrade ; Da Silva, Marcio Lima ; Pedro, Edilson Da Silva

Cadernos de Prospecção, 2020-07-12, Vol.13 (4), p.1053 [Periódico revisado por pares] Rabechini Jr., Roque, Carvalho, Marly Monteiro de e Laurindo, Fernando José Barbin Fatores críticos para implementação de gerenciamento por projetos: o caso de uma organização de pesquisa. Production [online]. 2002, v. 12, n. 2 [Acessado 3 Novembro 2021] , pp. 28-41. Disponível em: <<https://doi.org/10.1590/S0103-65132002000200004>>. E pub 25 Maio 2007. ISSN 1980-5411. <https://doi.org/10.1590/S0103-65132002000200004>.

Jannuzzi, Celeste Aída Sirotheau Corrêa, Falsarella, Orandi Mina e Sugahara, Cibele Roberta Sistema de informação: um entendimento conceitual para a sua aplicação nas organizações empresariais. Perspectivas em Ciência da Informação [online]. 2014, v. 19, n. 4 [Acessado 3 Novembro 2021] , pp. 94-117. Disponível em: <<https://doi.org/10.1590/1981-5344/1927>>. Epub 06 Jan 2015. ISSN 1981-5344. <https://doi.org/10.1590/1981-5344/1927>.

Associação Brasileira de Normas Técnicas. NBR ISO/IEC 27001. (2006). Tecnologia da informação — Técnicas de segurança — Sistemas de gestão de segurança da informação — Requisitos.

Associação Brasileira de Normas Técnicas. NBR ISO/IEC 27002. (2013). Tecnologia da informação - Técnicas de segurança - Código de prática para controles de segurança da informação.

AS/NZS (2004). AS/NZS 4360: 2004 - Risk Management. Australian/New Zealand Standard, Atralia: GPO Box 5420, Sydney/New Zealand: Private Bag 2439, Wellington 6020.

Buogo, Mateus ; Fachinelli, Ana Cristina ; Giacomello, Cíntia Paese A.to.Z (Curitiba, Brazil), 2020-07-02, Vol.8 (2), p.49-59

Buogo, M., Fachinelli, A. C. & Giacomello, C. P. (2019). Gestão do conhecimento e segurança da informação. AtoZ: novas práticas em informação e conhecimento, 8(2), 49 – 59. Recuperado de: <http://dx.doi.org/10.5380/atoz.v8i2.69687>

Dias, C. (2004). Segurança e auditoria na tecnologia da informação. Rio de Janeiro: Axcel.

Freitas, H., & Kladis, C. M. (1995). Da informação è política informacional das organizações: um

quadro conceitual. *Revista de Administração Pública*, 29 (3), 73–86.

Galegale, Napoleão Verardi, Fontes, Edison Luiz Gonçalves e Galegale, Bernardo Perri Uma contribuição para a segurança da informação: um estudo de casos múltiplos com organizações brasileiras | 1 Artigo elaborado a partir da dissertação de mestrado de Edison Luiz Gonçalves Fontes, intitulada “Política de segurança da informação: uma contribuição para o estabelecimento de um padrão mínimo”, Centro Estadual de Educação Tecnológica Paula Souza (CEETEPS), 2011. . *Perspectivas em Ciência da Informação* [online]. 2017, v. 22, n. 03 [Acessado 7 Novembro 2021] , pp. 75-97. Disponível em: <<https://doi.org/10.1590/1981-5344/2866>>. Epub Jul-Sep 2017. ISSN 1981-5344. <https://doi.org/10.1590/1981-5344/2866>.

Hors, Cora et al. Application of the enterprise management tools Lean Six Sigma and PMBOK in developing a program of research management. *Einstein* (São Paulo) [online]. 2012, v. 10, n. 4 [Accessed 22 October 2021] , pp. 480-490. Available from: <<https://doi.org/10.1590/S1679-45082012000400015>>. Epub 22 Jan 2013. ISSN 2317-6385. <https://doi.org/10.1590/S1679-45082012000400015>.

Marciano, João Luiz e Lima-Marques, Mamede O enfoque social da segurança da informação. *Ciência da Informação* [online]. 2006, v. 35, n. 3 [Acessado 21 Outubro 2021] , pp. 89-98. Disponível em: <<https://doi.org/10.1590/S0100-19652006000300009>>. Epub 01 Out 2007. ISSN 1518-8353. <https://doi.org/10.1590/S0100-19652006000300009>.

Pellosso Piurcosky, Fabrício, et al. “A Lei Geral de Proteção de Dados Pessoais Em Empresas Brasileiras: Uma Análise de Múltiplos Casos.” *Suma de Negócios*, vol. 10, no. 23, 15 June 2019, pp. 89–99, 10.14349/sumneg/2019.v10.n23.a2. Accessed 26 Jan. 2020.

PINTO, J.K. & D.P.SLEVIN. *Critical Factors in Successful Project Implementation in: Cleland, D. I.; King, W, R. Project Management Handbook Van Nostrand Reinhold, New York, 1983.*

RABECHINI JR., R. ; YU, A. S. O ;CORREA, E. S. O ; Correa, E. S. O *Monitoramento Tecnológico E as Decisões nas Empresas. In: XIX Simpósio da Gestão da Inovação Tecnológica, São Paulo, outubro, 1996.*

RAINER JR, R.K.; CEGIELSKI, C.G. *Introdução a Sistemas de Informação Rio de Janeiro: Campus, 2012*

Silva Netto, Abner da e Silveira, Marco Antonio Pinheiro da *Gestão da segurança da informação: fatores que influenciam sua adoção em pequenas e médias empresas. JISTEM - Journal of Information Systems and Technology Management* [online]. 2007, v. 4, n. 3 [Acessado 9 Novembro 2021] , pp. 375-397. Disponível em: <<https://doi.org/10.1590/S1807-17752007000300007>>. Epub 11 Mar 2011. ISSN 1807-1775. <https://doi.org/10.1590/S1807-17752007000300007>.

TURBAN, E.; RANIER JR., R. K.; POTTER, R.E. *Introdução a sistemas de Informação uma abordagem gerencial Tradução Daniel Vieira. Rio de Janeiro: Elsevier, 2007.*

TURBAN, E.; RAINER JR., R.K.; POTTER, R.E. *Administração de Tecnologia da*



Informação Teoria & Prática. Rio de Janeiro: Campus, 2005.

VIEW OF INFOSECRM: UMA ABORDAGEM ONTOLÓGICA PARA A GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO. 2021. Sbc.org.br. Available at: <https://sol.sbc.org.br/journals/index.php/isys/article/view/221/201>. Accessed on: 7 Dec. 2021.

“O Ataque de Hackers a Maior Oleoduto Dos EUA Que Fez Governo Declarar Estado de Emergência.” BBC News Brasil, 10 May 2021, [www.bbc.com/portuguese/internacional-57055618](http://www.bbc.com/portuguese/internacional-57055618). Accessed 7 Dec. 2021.

### **Agradecimentos**

Agradecimento à faculdade e ao professor Me. Jorge Alberto dos Santos por nos proporcionar o conhecimento necessário para a execução deste trabalho.