INTERFACE TECNOLÓGICA

APLICAÇÃO DO COBIT 2019 NA SEGURANÇA DA INFORMAÇÃO: a importância da prevenção

APPLICATION OF COBIT 2019 IN INFORMATION SECURITY: the importance of prevention

Isabela de Melo Franco – ifranco@ufrrj.br
Universidade Federal Rural do Rio de Janeiro (UFRRJ) – Seropédica – RJ – Brasil

DOI: 10.31510/infa.v20i1.1592
Data de submissão: 20/03/2023
Data do aceite: 29/05/2023
Data da publicação: 30/06/2023

RESUMO

O número de ataques cibernéticos vem crescendo exponencialmente nos últimos anos, demandando uma maior precaução das organizações quanto à segurança da informação. Nesse cenário, o objetivo deste artigo é apresentar, por meio de uma pesquisa bibliográfica, o *Control Objectives for Information and Related Technologies* 2019, mais conhecido como COBIT 2019, como uma estrutura de apoio para as empresas se organizarem na perspectiva da segurança cibernética ou cibersegurança, através da governança e gestão. Ademais, outros conceitos como tipos e casos reais de ataques cibernéticos, bem como investimentos esperados na área da segurança da informação são desenvolvidos. Por fim, espera-se que com essa pesquisa seja possível atingir um grau mais elevado de conscientização quanto à proteção de sistemas de informação, prevenção e investimentos contra ataques cibernéticos; incentivar a adoção da estrutura do COBIT 2019 e de seus processos-chave APO13 e DSS05 (relacionados à segurança) nas empresas e impulsionar a elaboração de estudos na área.

Palavras-chave: COBIT 2019; Segurança da Informação; Ataques Cibernéticos; APO13; DSS05.

ABSTRACT

The number of cyberattacks has been growing exponentially in recent years, demanding greater precaution from organizations regarding information security. In this scenario, the objective of this article is to present, through a bibliographical research, the Control Objectives for Information and Related Technologies 2019, better known as COBIT 2019, as a support structure for companies to organize themselves from the perspective of cybersecurity, through governance and management. In addition, other concepts such as types and real cases of cyberattacks, as well as expected investments in information security are developed. Finally, it is expected that with this research it will be possible to reach a higher level of awareness regarding the protection of information systems, prevention and investments against cyberattacks; encourage the adoption of the COBIT 2019 framework and its key processes APO13 and DSS05 (related to security) in companies and encourage the preparation of studies in the area.

Keywords: COBIT 2019; Information Security; Cyberattacks; APO13; DSS05.

1 INTRODUÇÃO

O COBIT consiste em um modelo para o gerenciamento da governança e gestão da Informação e Tecnologia (I&T) da organização como um todo. Nele, é possível determinar os elementos que caracterizam quais decisões precisam ser definidas, bem como o motivo e a atribuição de responsabilidade para a tomada de decisão (SOUZA NETO; MACEDO, 2021).

Lançada em 1996 pela ISACA, a primeira versão do COBIT surgiu com a premissa de ser um conjunto de objetivos de controle que visavam auxiliar a área de auditoria financeira a se adaptar em ambientes ligados à Tecnologia da Informação (TI). Com um potencial de expansão além do domínio da auditoria, em 1998 foi lançado o COBIT 2, com enfoque em controle. Em seguida, o modelo evoluiu, e no ano 2000 foi lançado o COBIT 3, abarcando diretrizes de gerenciamento (CHIARI, 2021).

Adicionalmente, Chiari (2021) ressalta que nos anos 2005 e 2007 foram lançadas as versões 4 e 4.1 do COBIT, respectivamente, como resultado do aumento da conscientização sobre a demanda de elementos acerca da governança de TI. Após, o COBIT 5 foi lançado em 2012, tendo como principais alterações a integração com outros conjuntos de metodologias e boas práticas. Enfim, em 2019 surge sua versão mais recente: o COBIT 2019, tendo como atualizações mais relevantes as orientações para dar suporte à organização para criar uma solução personalizada de governança de TI, como fatores de desenho e áreas de foco.

Nesse contexto, é importante distinguir a governança da gestão. A governança geralmente é atribuída ao conselho de administração da empresa e tem o objetivo de avaliar as demandas das partes interessadas; monitorar a conformidade e o desempenho organizacional e definir a direção priorizando as tarefas e utilizando a tomada de decisão. Por outro lado, a gestão, em geral, é de responsabilidade da gestão executiva, com um presidente na liderança. Tem o propósito de planejar, construir, executar e monitorar atividades, de acordo com a orientação da direção, de maneira a alcançar as metas da organização (SOUZA NETO; MACEDO, 2021).

Conforme o ISACA (2018), o COBIT 2019 descreve três princípios para um framework de governança que podem servir como base para alcançar essas metas organizacionais. Os

princípios são baseados em um modelo conceitual, são abertos e flexíveis e são alinhados com os padrões principais, podendo ser detalhados a seguir:

> 1. Um framework de governança deve ser baseado em um modelo conceitual, identificando os componentes-chave e relacionamentos entre os componentes, para maximizar a consistência e permitir a automação.
>
> 2. Um framework de governança deve ser aberto e flexível. Deve permitir a adição de novos conteúdos e a capacidade de abordar novos problemas da maneira mais flexível, mantendo integridade e consistência.
>
> 3. Um framework de governança deve estar alinhado com os principais padrões, estruturas e regulamentos relacionados. (ISACA, 2018, p.18, tradução nossa)

Quando a governança e gestão são empregadas seguindo as orientações do COBIT, os reflexos da atuação no ambiente de trabalho são extremamente positivos. Seguindo essa linha de raciocínio, Baldissera (2021) realça algumas vantagens do COBIT nas organizações: ampliação na eficiência do campo da Tecnologia em Informação; otimização de investimentos em TI, com uma visão abrangente do negócio; maior segurança da informação e maior entendimento entre as partes envolvidas, a partir do uso de uma linguagem comum entre os colaboradores da empresa.

Para que a governança e a gestão sejam aplicadas sem eventuais entraves, é necessário investir em segurança da informação, especialmente frente ao aumento de ataques cibernéticos nos últimos anos. Nesse sentido, Santos e Silva (2021), destacam que, atualmente, a evolução tecnológica vem mudando consideravelmente a forma de produção, organização e disponibilização das informações, visto que a capacidade dos sistemas de comunicação e redes propicia continuamente o acesso informacional de diversas maneiras possíveis. Diante disso, a segurança da informação se converteu em um aspecto essencial nas organizações.

O objetivo deste artigo é apresentar o COBIT 2019 como uma estrutura capaz de apoiar empresas na perspectiva da cibersegurança através da governança e gestão, assim como discorrer sobre a relevância de determinados assuntos, como segurança da informação, tipos e casos reais de ataques cibernéticos, investimentos esperados na área e processos-chave APO13 e DSS05 para apoiar a segurança organizacional.

2 SEGURANÇA DA INFORMAÇÃO

De acordo com Oliveira e Filgueiras (2022), a segurança da informação abarca boas práticas e ações que visam proteger um determinado conjunto de dados. Esses parâmetros

podem ser utilizados em qualquer tipo de empresa que trabalha com dados, tendo em vista que é necessário preservar a seguridade de suas informações. GAT INFOSEC (2022a) demonstra que a segurança da informação possui cinco pilares (mais conhecidos como Tríade CIA – *Confidentiality, Integrity and Availability*, com mais dois complementos que vieram ao longo do tempo) que podem auxiliar na preservação dos dados:

- **Confidencialidade**: Assegura que os dados estejam acessíveis aos usuários a que se destinam e protegidos contra acessos não autorizados;
- **Integridade**: Representa o respeito à confiabilidade, consistência, preservação e precisão dos dados ao longo de todo o seu ciclo de vida;
- **Disponibilidade**: Permite o acesso em tempo integral pelos usuários, juntamente com a garantia da estabilidade dos processos concernentes ao sistema;
- **Autenticidade**: Aprova a autorização do usuário para seu acesso, transmissão e recebimento de informações. Um exemplo disso é a utilização de login e senhas;
- **Irretratabilidade ou Não Repúdio**: Certifica que uma entidade ou pessoa não seja capaz de negar a autoria de determinada informação fornecida, ou seja, é a possibilidade de provar por quem, o que e onde foi executada determinada ação no sistema, impossibilitando a negação desse ato (GAT INFOSEC, 2022a).

Uma organização que aplica esses pilares no seu dia a dia demonstra que possui cautela e se importa com a integridade das informações de seus colaboradores, clientes, *stakeholders* e de sua companhia como um todo. Esse tipo de atitude precisa ser cada vez mais adotada nas empresas, principalmente diante dos inúmeros ataques cibernéticos da contemporaneidade, cada vez mais frequentes e com técnicas inovadoras.

2.1 Ataques cibernéticos

Os ataques cibernéticos podem ser definidos como uma tentativa bem-sucedida ou não, de um *hacker* em danificar, roubar, sequestrar ou destruir um sistema ou rede que possui conexão com a internet. Essas investidas são feitas de diversas maneiras: através de vírus, *malware*, fraude, roubo de identidade, extorsão etc., todas com o intuito de violar dados confidenciais/sensíveis de pessoas ou empresas (ZIMMER, 2020). Existem várias categorias de ataques cibernéticos e, para se prevenir, é importante conhecê-las. Posto isso, o Blog Unyleya (2020) elencou dez principais tipos de ataques cibernéticos:

1) ***Backdoor***: A tradução literal de *backdoor* é "porta dos fundos", sendo um tipo de cavalo de troia (ou *Trojan*), que permite que o invasor ganhe acesso ao sistema remotamente. É relevante salientar que nem sempre os *backdoors* são mal intencionados, considerando a variedade de aplicativos que já vêm com um *backdoor* instalado pelo desenvolvedor do sistema, a fim de facilitar a execução de manutenções ou atualizações;

2) ***Phishing***: É uma técnica de engenharia social que se aproveita da confiança de um usuário para realizar o roubo de seus dados. Isso pode acontecer quando o cibercriminoso se passa por uma pessoa ou instituição confiável para ludibriar o usuário, usando *links* de e-mails como isca e de várias outras formas;

3) ***Spoofing***: Tem associação com a falsificação de endereços de e-mails, de *Domain Name System* (DNS) e de *Internet Protocol address* (IP). Desse modo, o indivíduo pode simular que determinado endereço de e-mail ou IP é autêntico e confiável, mudar o DNS para redirecionar um domínio para um endereço de IP diferente etc. Ainda que o *Spoofing* se pareça com o *Phishing*, suas abordagens são diferentes. O *Phishing* não demanda obrigatoriamente o *download* do *malware*, porque sua meta é roubar informações sigilosas. Por outro lado, o *Spoofing* tem a finalidade de roubar a identidade do usuário, agindo como outra pessoa, o que é uma falsificação;

4) **Manipulação de *Uniform Resource Locator* (URL)**: Visa fazer o servidor divulgar páginas que ele não possui acesso autorizado. Um exemplo disso é a alteração manual de URL, a partir do teste de várias combinações, a fim de encontrar um endereço que abrange uma área restrita;

5) ***Denial of Service* (DoS)**: Esse tipo de ataque que significa, em português, Negação de Serviço e corresponde a uma grande quantidade de pedidos de pacotes, acaba ocasionando uma sobrecarga em um computador ou servidor. Como consequência, o sistema não consegue mais responder, se tornando indisponível para seus usuários;

6) ***Distributed Denial of Service* (DDoS)**: Diferentemente do ataque DoS que não é capaz de atingir sistemas mais sofisticados, a técnica DDoS, traduzida como Negação de Serviço Distribuído, consegue compartilhar os pedidos de inúmeras máquinas. Isso quer dizer que um computador mestre pode dominar outras máquinas, de forma a acessar o mesmo recurso de um servidor ao mesmo tempo, resultando em uma sobrecarga de sistemas que podem ser considerados robustos;

7) ***Direct Memory Access* (DMA)**: Definido na tradução como Acesso Direto à Memória, esse ataque viabiliza o acesso imediato à *Random Access Memory*, ou memória RAM pelo *hardware* da máquina sem passar pelo processador. Essa ação permite a aceleração do processamento e da taxa de transferência do computador, o que pode ser utilizado para chegar na memória RAM através de um periférico, ainda que sem um s*oftware*;

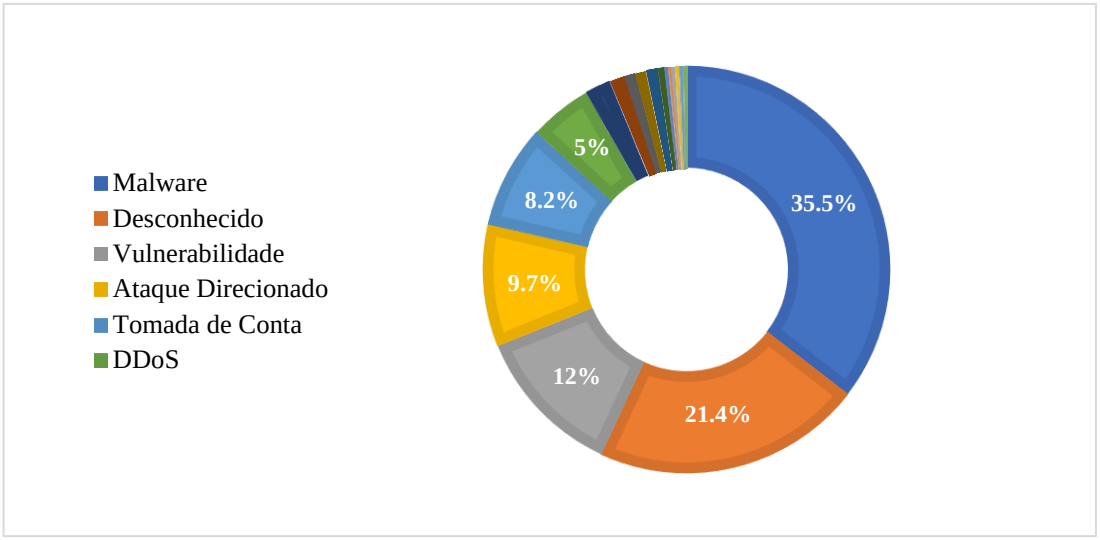
8) ***Eavesdropping***: Traduzido como "bisbilhotar", é uma ação em que o *hacker* faz uso de distintos sistemas de telefonia, mensagens instantâneas, e-mail e serviços de internet para roubar dados e utilizá-los de maneira imprópria (sem alterar informações), infringindo a confidencialidade da vítima;

9) ***Decoy***: Compreende uma simulação de um programa legítimo, que tem o propósito de pegar as informações armazenadas do usuário por meio de seu *login*;

10) ***Shoulder Surfing***: Oriundo da expressão "espiar sobre os ombros", não é um ataque que faz uso de ferramenta ou tecnologia. É apenas o ato de olhar a tela de um usuário, quando este está acessando dados sensíveis.

O *Phishing* é bastante comum no Brasil, assim como o ataque de ***Ransomware***, que consiste em um *malware* que sequestra dados, bloqueando o acesso do usuário a seus dispositivos ou arquivos e exigindo um pagamento anônimo online (geralmente em criptomoedas) para que esse acesso seja devolvido (NEGÓCIO SEGURO AIG, 2022). Complementarmente, Passeri (2023) fez um compilado de ataques cibernéticos ocorridos em vários países (incluindo o Brasil), de modo a representar os que aconteceram em abril de 2023, apresentados no Gráfico 1:

Gráfico 1 – Distribuição dos principais ataques cibernéticos ocorridos em abril de 2023



Fonte: Adaptado de Hackmageddon (2023)

Perante a esse cenário abundante de ataques, um relatório intitulado *Global Cybersecurity Outlook* foi compartilhado durante o Fórum Econômico Mundial que ocorreu em janeiro de 2023, em Davos, Suíça. Esse documento foi redigido em parceria com a empresa Accenture e coletou informações de mais de 300 executivos e especialistas em cibersegurança a nível global. Esses especialistas e executivos apontaram que haverá um evento cibernético catastrófico em cerca de dois anos, e que será capaz de causar muitos prejuízos às organizações no mundo inteiro (MACHADO, 2023).

> O relatório Outlook deste ano revela que 93% dos líderes cibernéticos e 86% dos líderes empresariais consideram "moderadamente provável" ou "muito provável" que a instabilidade geopolítica global leve a um evento cibernético catastrófico e de longo alcance nos próximos dois anos (WEF; ACCENTURE, 2023, p. 8, tradução nossa).

> Os entrevistados disseram que inteligência artificial (IA) e aprendizado de máquina (20%), maior adoção de tecnologia em nuvem (19%) e avanços na identidade do usuário e gerenciamento de acesso (15%) terão maior influência em suas estratégias de risco cibernético nos próximos dois anos (WEF; ACCENTURE, 2023, p. 11, tradução nossa).

Tendo em vista esse prognóstico de risco cibernético, as organizações precisam se conscientizar e investir em segurança cibernética, mesmo que não ocorra nenhum evento desastroso nos próximos anos. A segurança cibernética:

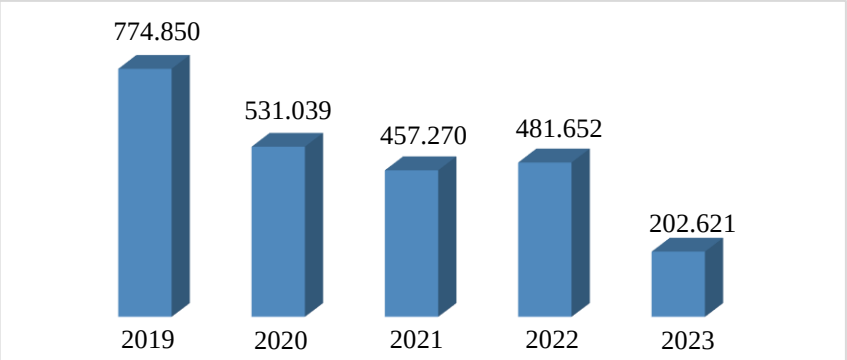
> Também conhecida como cibersegurança, consiste na prática de proteger pessoas, sistemas, redes e ativos de ataques cibernéticos que visam obter acesso a hardware e dados, alterar ou destruir informações sensíveis para obter ganho próprio, realizar extorsão financeira e, em casos extremos, afetar ou causar a paralisação da operação dos alvos (GAT INFOSEC, p. 9, 2022b).

O Boston Consulting Group – BCG (2022) estimou que até o final de 2022, os gastos com segurança da informação e tecnologia de gerenciamento de riscos chegariam a aproximadamente 168 bilhões de dólares. Além disso, "A frequência e o custo dos ataques cibernéticos estão se acelerando. Globalmente, estima-se que o custo do cibercrime aumentou de US$ 445 bilhões em 2015 para mais de US$ 2,2 trilhões hoje." (BCG, 2022, tradução nossa). Apesar do grande investimento feito em cibersegurança, ainda não foi possível deter as investidas cada vez mais elaboradas dos *hackers*. Esse fato pode ser comprovado na esfera do Brasil, que sofreu inúmeros ataques cibernéticos ao longo de 2022, demonstrados a seguir:

1) Extorsões do grupo Lapsus$, que já atacou as Lojas Americanas, o Submarino, os Correios, o Ministério da Saúde e algumas empresas privadas; **2)** Ataque de *Ransomware* ao governo federal pelo grupo Everest, que vendeu o acesso à rede para terceiros, implicando aproximadamente 3 *terabytes* de informações confidenciais; **3)** Invasão de sistemas da TV Record, onde foram sequestrados arquivos de quadros, reportagens e outras informações, causando significativos prejuízos à programação da emissora; **4)** Ataque de *Ransomware* ao Banco de Brasília, com sequestro de informações sigilosas de clientes. Para a devolução dessas informações, foi solicitado um pagamento 50 *bitcoins*, representando aproximadamente 5 milhões de reais; **5)** Duplo ataque aos sistemas da Golden Cross (dois ataques no mesmo mês), que comprometeram a segurança da empresa, ainda que esta tenha afirmado que o acesso ao banco de dados dos clientes continuou normal e não houve evidências de exposição dos dados armazenados (ZIMMER, 2022).

Nesse contexto, outro ponto de atenção são os incidentes de segurança, que são caracterizados por quaisquer eventos adversos confirmados, associados à violação na segurança de dados pessoais, como acesso ilícito, acidental ou não autorizado, que tenha como consequência uma ameaça às liberdades e aos direitos do titular dos dados pessoais (SEGURANÇA DA INFORMAÇÃO UFRJ, 2023). O Gráfico 2 exibe a quantidade de notificações de incidentes recebidas pelo Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br), demonstrando um grande volume ao longo dos últimos anos:

Gráfico 2 – Notificações de incidentes recebidas pelo CERT.br (2019-04/2023)



Fonte: Adaptado de CERT.br (2023)

Diante de todos esses ataques e incidentes, fica cada vez mais evidente a importância da segurança da informação. Ao longo de 2023, espera-se um crescimento de 13% em cibersegurança, principalmente para a prevenção de ataques de *Ransomware*, a maior ameaça na perspectiva operacional das empresas. O ChatGPT, que está em alta, também representa um risco, uma vez que pessoas mal intencionadas podem usá-lo para a criação de códigos maliciosos em escala industrial (IGLESIAS ÁLVAREZ, 2023). Logo, a prevenção contra ameaças é imprescindível para manter estável a situação financeira e operativa de uma empresa.

3 PROCEDIMENTOS METODOLÓGICOS

O desenvolvimento deste estudo é alicerçado na Pesquisa Bibliográfica, que corresponde à leitura, análise e intepretação de diversos tipos de documentos, como periódicos científicos, livros, monografias, teses, relatórios etc. Esses documentos, em sua maioria, são resultados da confecção de um trabalho científico (MAZUCATO, 2018).

> Não por acaso, esse tipo de pesquisa também exige planejamento e, após uma análise da literatura disponível sobre o tema estudado, o material angariado deve ser triado, estabelecendo-se assim, um plano de leitura do mesmo. Nesse caso, espera-se uma leitura atenta e sistematizada acompanhada de resenhas, anotações e fichamentos que, por sua vez, servirão de subsídios e de fundamentação teórica para a feitura da pesquisa (MAZUCATO, 2018, p.66).

Ademais, Severino (2014) relata que a pesquisa bibliográfica utiliza categorias teóricas ou dados previamente trabalhados e registrados por outros pesquisadores, fazendo uso desses textos como fontes de temas a serem pesquisados. Dessa forma, o pesquisador trabalha com fundamentação nas contribuições dos autores de estudos analíticos.

4 RESULTADOS E DISCUSSÃO

Tendo em vista os problemas concernentes à Segurança da Informação expostos anteriormente, é aconselhável adotar o COBIT 2019 nas empresas, pois ele fornece processos-chave de apoio para auxiliar as organizações na prevenção contra ameaças de segurança. Esses processos estão listados em meio a 40 objetivos de governança e gestão, constando seu código de referência, nome e propósito (SOUZA NETO; MACEDO, 2021). As referências que vão ao encontro do tema abordado nesse artigo são a APO13 e a DSS05, detalhadas no Quadro 1:

Quadro 1 – Objetivos de Governança e Gestão no prisma da Segurança da Informação

REFERÊNCIA	NOME	PROPÓSITO
APO13	Segurança gerenciada	Manter o impacto e a ocorrência de incidentes de segurança da informação dentro dos níveis de apetite ao risco da organização.
DSS05	Serviços de segurança gerenciados	Minimizar o impacto das vulnerabilidades e incidentes de segurança da informação operacional nos negócios.

Fonte: Adaptado de Souza Neto e Macedo (2021)

Como foi possível observar, as referências pertencem a dois domínios: APO e DSS. Segundo Souza Neto e Macedo (2021), o domínio APO tem o significado de *Align, Plan, and Organize* ou Alinhar, Planejar e Organizar, abordando a organização em geral, as atividades e estratégias de gestão da Tecnologia da Informação. Os autores também salientam que esse domínio inclui os seguintes processos:

01 Estrutura de gestão de TI gerenciada;
02 Estratégia gerenciada;
03 Arquitetura corporativa gerenciada;
04 Inovação gerenciada;
05 Portfólio gerenciado;
06 Orçamento e custos gerenciados;
07 Recursos humanos gerenciados;
08 Relacionamentos gerenciados;
09 Contratos de serviços gerenciados;
10 Fornecedores gerenciados;
11 Qualidade gerenciada;
12 Risco gerenciado;
13 **Segurança gerenciada**;
14 Dados gerenciados.

Por outro ângulo, o domínio DSS significa *Deliver, Service, and Support* ou Entregar, prestar Serviços e dar Suporte, respectivamente, e tem o enfoque na prestação e suporte de

serviços de TI, abrangendo serviços de segurança. Seus processos são: 01 Operações gerenciadas; 02 Solicitações e incidentes de serviço gerenciados; 03 Problemas gerenciados; 04 Continuidade gerenciada; **05 Serviços de segurança gerenciados** e 06 Controles de processos de negócios gerenciados (SOUZA NETO; MACEDO, 2021).

Considerando os domínios e processos-chave apresentados, a adoção do *framework* COBIT é recomendada para inúmeros tipos de empresas. Por ter uma visão holística, o COBIT 2019 possui vários benefícios, como: otimização de recursos e riscos; geração de valor para o negócio; flexibilidade; métodos para implementação; desempenho gerenciado e outros (CHIARI, 2021).

5 CONSIDERAÇÕES FINAIS

A segurança da informação pode ser considerada como um investimento indispensável para qualquer tipo de organização, independentemente de porte. Como a realização de ataques cibernéticos é praticamente inevitável e os *hackers* estão se aprimorando constantemente com a utilização de técnicas altamente sofisticadas, a melhor solução é a prevenção.

Em termos de gastos, a prevenção é muito mais barata que a consequência de um ataque. Para garantir essa prevenção, o COBIT fornece diversos direcionamentos para auxiliar qualquer empresa na estruturação de um sistema de segurança da informação, baseado nas melhores práticas de governança e gestão.

Logo, espera-se que com essa pesquisa seja possível ampliar a conscientização sobre a proteção de sistemas de informação, a importância da segurança da informação, a prevenção de ataques cibernéticos e os investimentos neste segmento. Por fim, também espera-se incentivar a adoção/aplicação do COBIT 2019 nas organizações e impulsionar a elaboração de estudos neste campo do conhecimento.

REFERÊNCIAS

BALDISSERA, O. O que é COBIT, os benefícios e a relação com a governança de TI. **Pós PUCPR Digital**, 2021. Disponível em: https://posdigital.pucpr.br/blog/cobit. Acesso em: 02 jun. 2023.

CHIARI, R. COBIT 2019: o que é, quais os princípios e diferenças do COBIT 5. **ITSM na Prática**, 2021. Disponível em: https://www.itsmnapratica.com.br/tudo-sobre-cobit-2019. Acesso em: 20 jan. 2023.

CINCO pilares da segurança da informação. **GAT INFOSEC**, 2022a. Disponível em: https://www.gat.digital/blog/5-pilares-da-seguranca-da-informacao. Acesso em: 18 jan. 2023.

CONHEÇA os 10 principais ataques cibernéticos da atualidade. **Blog Unyleya**, 2020. Disponível em: https://blog.unyleya.edu.br/bitbyte/ataques-ciberneticos. Acesso em: 19 jan. 2023.

GAT INFOSEC (ed.). **Gerenciamento da superfície de ataque**: inventário exposto e risco de terceiros: identificação e gestão de ativos, riscos e vulnerabilidades cibernéticas. GAT INFOSEC, 2022b. Disponível em: https://www.gat.digital/wp-content/uploads/2022/11/ebook-superficie-20221026.pdf. Acesso em: 20 jan. 2023.

IGLESIAS ÁLVAREZ, I. Investimento em cibersegurança deverá crescer 13% em 2023. **Computer World**, 2023. Disponível em: https://www.computerworld.com.pt/2023/01/19/investimento-em-ciberseguranca-devera-crescer-13-em-2023. Acesso em: 20 jan. 2023.

INCIDENTES de Segurança da Informação. **Segurança da Informação UFRJ**, 2023. Disponível em: https://www.security.ufrj.br/denuncie-um-incidente. Acesso em: 03 jun. 2023.

INCIDENTES notificados ao CERT.br. **CERT.br**, 2023. Disponível em: https://stats.cert.br/incidentes. Acesso em: 03 jun. 2023.

ISACA (ed.). **COBIT 2019 Framework**: introduction and methodology. Illinois: ISACA, 2018. Disponível em: https://community.mis.temple.edu/mis5203sec003spring2020/files/2019/01/COBIT-2019-Framework-Introduction-and-Methodology_res_eng_1118.pdf. Acesso em: 17 jan. 2023.

OLIVEIRA, E. V.; FILGUEIRAS, R. A importância da segurança da informação para as organizações. **Revista Alomorfia**. Presidente Prudente, São Paulo, v.6, n.1, p. 438-447, 2022. Disponível em: https://www.alomorfia.com.br/index.php/alomorfia/article/view/137. Acesso em: 18 jan. 2023.

MACHADO, L. C-levels alertam: catástrofe cibernética ainda está por vir. **Security Report**, 2023. Disponível em: https://www.securityreport.com.br/destaques/alerta-para-os-cisos-catastrofe-cibernetica-esta-por-vir. Acesso em: 20 jan. 2023.

MAZUCATO, T. (org.). **Metodologia da pesquisa e do trabalho científico**. Penápolis: FUNEPE, 2018. Disponível em: https://faculdadefastech.com.br/fotos_upload/2022-02-16_10-06-51.pdf. Acesso em: 17 jan. 2023.

PASSERI, P. April 2023 Cyber Attacks Timeline. **Hackmageddon**, 2023. Disponível em: https://www.hackmageddon.com/2023/05/30/april-2023-cyber-attacks-timeline. Acesso em: 02 jun. 2023.

QUAIS são os principais ataques cibernéticos no Brasil? **Negócio Seguro AIG**, 2022. Disponível em: https://www.negocioseguroaig.com.br/servicos-e-comercio/tendencia/principais-ataques-ciberneticos-no-brasil. Acesso em: 19 jan. 2023.

SANTOS, R. B.; SILVA, T. B. P. Gestão da segurança da informação e comunicações: análise ergonômica para avaliação de comportamentos inseguros. **RDBCI**: Rev. Dig. Bibliotec e Ci. Info. Campinas, São Paulo, v. 19, p. 1-31, 2021. Disponível em: https://brapci.inf.br/index.php/res/v/164871. Acesso em: 17 jan. 2023.

SEVERINO, A. J. **Metodologia do trabalho científico**. São Paulo: Cortez, 2014. Disponível em: https://www.ufrb.edu.br/ccaab/images/AEPE/Divulga%C3%A7%C3%A3o/LIVROS/Metodologia_do_Trabalho_Cient%C3%ADfico_-_1%C2%AA_Edi%C3%A7%C3%A3o_-_Antonio_Joaquim_Severino_-_2014.pdf. Acesso em: 17 jan. 2023.

SOUZA NETO, J; MACEDO, L. P. (ed.). **Cartilha COBIT 2019**. Brasília: ISACA, 2021. Disponível em: https://www.researchgate.net/publication/355397119_Cartilha_COBIT_2019_versao_1. Acesso em: 17 jan. 2023.

TURNING a cybersecurity strategy into reality: a holistic performance management framework. **Boston Consulting Group (BCG)**, 2022. Disponível em: https://www.bcg.com/pt-br/publications/2022/cybersecurity-performance-management-framework. Acesso em: 20 jan. 2023.

WORLD ECONOMIC FORUM (WEF); ACCENTURE (org.). **Global Cybersecurity Outlook 2023**. Suíça: WEF, 2023. Disponível em: https://www.weforum.org/reports/global-cybersecurity-outlook-2023. Acesso em: 20 jan. 2023.

ZIMMER, K. Como se prevenir de um ataque cibernético: para pequenas empresas. **Lumiun Blog**, 2020. Disponível em: https://www.lumiun.com/blog/como-se-prevenir-de-um-ataque-cibernetico-para-pequenas-empresas. Acesso em: 19 jan. 2023.

ZIMMER, K. Relatório de Cibersegurança de 2022: tudo que rolou no ano. **Lumiun Blog**, 2022. Disponível em: https://www.lumiun.com/blog/relatorio-de-ciberseguranca-de-2022-tudo-que-rolou-no-ano. Acesso em: 20 jan. 2023.