UNIVERSIDADE FEDERAL DA PARAÍBA
CENTRO DE CIÊNCIAS APLICADAS E EDUCAÇÃO – CCAE
BACHARELADO EM ADMINISTRAÇÃO

ILDEFONSO MARCELINO RODRIGUES NETO

SEGURANÇA DA INFORMAÇÃO NO ÂMBITO DA ADMINISTRAÇÃO PÚBLICA MUNICIPAL: um estudo na Prefeitura Municipal de Mataraca

Mamanguape/PB
2024

ILDEFONSO MARCELINO RODRIGUES NETO

SEGURANÇA DA INFORMAÇÃO NO ÂMBITO DA ADMINISTRAÇÃO PÚBLICA MUNICIPAL: um estudo na Prefeitura Municipal de Mataraca

Trabalho de Conclusão de Curso apresentado ao curso de Bacharelado em Administração do Centro de Ciências Aplicadas e Educação da Universidade Federal da Paraíba, como requisito obrigatório para a obtenção do título de Bacharel em Administração, defendido e aprovado pela banca examinadora constituída pelos docentes:

gov.br
Documento assinado digitalmente
MARCIA MARIA DE MEDEIROS TRAVASSOS SAEG
Data: 22/10/2024 16:45:06-0300
Verifique em https://validar.iti.gov.br

Profª Drª Márcia Maria de Medeiros Travassos Saeger – UFPB
Orientadora/Presidente

gov.br
Documento assinado digitalmente
JULIO AFONSO SA DE PINHO NETO
Data: 23/10/2024 06:31:48-0300
Verifique em https://validar.iti.gov.br

Prof. Dr. Júlio Afonso Sá de Pinho Neto – UFPB
Membro da Banca Examinadora

gov.br
Documento assinado digitalmente
TABIRA DE SOUZA ANDRADE
Data: 23/10/2024 22:18:22-0300
Verifique em https://validar.iti.gov.br

Profª Ms. Tabira de Souza Andrade – UFPB
Membro da Banca Examinadora

Mamanguape/PB
2024

UNIVERSIDADE FEDERAL DA PARAÍBA
CENTRO DE CIÊNCIAS APLICADAS E EDUCAÇÃO
CURSO DE ADMINISTRAÇÃO

SEGURANÇA DA INFORMAÇÃO NO ÂMBITO DA ADMINISTRAÇÃO PÚBLICA MUNICIPAL: um estudo na Prefeitura Municipal de Mataraca

Ildefonso Marcelino Rodrigues Neto – UFPB – ildefonso.neto@academico.ufpb.br
Márcia Maria de Medeiros Travassos Saeger – UFPB – marcia@ccae.ufpb.br
Júlio Afonso Sá de Pinho Neto – UFPB – sadepinhojulio@gmail.com
Tabira de Souza Andrade – UFPB – tabirandrade@yahoo.com.br

RESUMO

A segurança da informação é fundamental para a proteção dos ativos informacionais contra acessos não autorizados, perda ou roubo, sendo de significativa importância que as organizações estabeleçam políticas que orientem as formas de controle da segurança. No contexto da administração pública municipal, a implementação de uma política de segurança da informação torna-se crucial, dado o volume significativo de dados e informações que diariamente circulam em diferentes setores. Nesse contexto, este artigo apresenta um estudo de caso, por meio do qual buscou-se identificar os elementos relacionados à segurança utilizados para a garantia da proteção dos ativos de informação da Prefeitura de Mataraca. Para alcançar esse objetivo, foi utilizada uma pesquisa exploratória e descritiva, do tipo estudo de caso e de abordagem qualitativa. A coleta de dados foi realizada por meio de entrevistas semiestruturadas, com seis servidores que lidam diretamente com sistemas de informações de diferentes setores da Prefeitura. A análise dos dados foi conduzida utilizando a técnica de análise de conteúdo, definindo-se categorias. Os resultados permitiram concluir que não há uma política de segurança da informação estabelecida na Prefeitura de Mataraca, e que as ações voltadas à segurança são realizadas exclusivamente por iniciativa dos servidores. Esse cenário evidencia a necessidade da instituição de uma política de segurança da informação na administração pública municipal.

Palavras-chave: Segurança da informação; Administração Pública; proteção de ativos informacionais.

ABSTRACT

Information security is essential for protecting informational assets against unauthorized access, loss, or theft. It is of significant importance that organizations establish policies to guide security control measures. In the context of municipal public administration, implementing an information security policy becomes crucial due to the significant volume of data and information circulating daily across different sectors. This article presents a case study aimed at identifying the security elements used to ensure the protection of information assets at the City Hall of Mataraca. To achieve this goal, an exploratory and descriptive research approach using qualitative methods was used. Data collection was carried out through semi-structured interviews with six employees directly involved in information systems from various sectors of the City Hall. Data analysis was conducted using content analysis technique to define categories. The results revealed that there is no established information security policy at the City Hall of Mataraca, and security actions are solely taken by employees. This scenario

highlights the need to establish an information security policy in municipal public administration.

Keywords: Information security; Public Administration; protection of information assets.

1 INTRODUÇÃO

A garantia da segurança da informação é fundamental para que os dados e informações estejam a salvo do acesso de pessoas não autorizadas, de possíveis alterações, perda ou roubo. É fundamental também que as organizações, independentemente do segmento em que atuam, atendam às regulamentações e leis sobre segurança e proteção de dados.

Nesse aspecto, a Lei Geral de Proteção de Dados (LGPD) no Brasil, ou Lei n° 13.709/2018, trouxe a garantia de proteção aos dados de pessoas físicas, tanto no meio físico, como digital. A referida lei surgiu como forma de facilitar o tratamento de dados com base em princípios de ética e boa-fé, e suas diretrizes visam atuar em prol da segurança e privacidade dos dados dos usuários, levantando dúvidas e direcionando soluções para que as organizações de quaisquer segmentos a implementem durante a coleta e manipulação dos dados (Fucciolo, 2022).

Para além disso, a segurança da informação, enquanto uma prioridade organizacional, contribui também para mitigar riscos de segurança, reduzir custos e contribuir com a eficiência, sobretudo em razão da redução do tempo gasto com retrabalho ou incidentes de segurança (Machado, 2014). No âmbito da administração pública municipal, diante dos diferentes atores com os quais ela interage, sejam servidores públicos, fornecedores, outros entes públicos e os próprios cidadãos, o volume de dados e informações que ficam sob sua responsabilidade é considerável, incluindo-se dados sensíveis.

No âmbito da LGPD, dados sensíveis são aqueles que podem ser utilizados para prejudicar ou discriminar alguém, a exemplo de convicção religiosa, origem racial, opinião política, dados biométricos ou dados de saúde (Brasil, 2018). Por esta razão, a instituição de uma política de segurança da informação é crucial para a garantia da adequada proteção dos ativos de informação.

Nesse contexto, é de suma importância considerar que a administração pública precisa apresentar uma postura diligente para implementar uma política de segurança da informação, razão pela qual a presente pesquisa parte do seguinte questionamento: **Quais os elementos relacionados à segurança considerados pela Prefeitura Municipal de Mataraca para garantir a proteção de seus ativos de informação?** Para responder a esse questionamento, a pesquisa tem como objetivo geral identificar os elementos relacionados à segurança utilizados

para a garantia da proteção dos ativos de informação da Prefeitura Municipal de Mataraca. De forma mais detalhada, foram traçados os seguintes objetivos específicos: a) apresentar os sistemas, tipos de dados e informações coletados e os usuários que acessam e/ou utilizam as informações no âmbito da Prefeitura Municipal de Mataraca; b) descrever os procedimentos para acesso aos sistemas da Prefeitura; c) detectar ações empreendidas para a implementação da segurança da informação na Prefeitura de Mataraca; d) identificar a adoção de ações voltadas para a análise crítica da segurança da informação no âmbito da Prefeitura Municipal de Mataraca.

Para atingir os objetivos propostos, foi utilizada a metodologia de estudo de caso, possibilitando uma análise aprofundada sobre a política de segurança da informação na Prefeitura Municipal de Mataraca.

Considerando a importância que a segurança da informação possui para as organizações, bem como para os atores que interagem direta e indiretamente com elas, identificar os elementos relacionados à política de segurança da informação é fundamental para a propositura de ações voltadas à proteção dos ativos informacionais, ao atendimento das exigências legais e à redução de riscos.

Nesse aspecto, a realização desta pesquisa encontra justificativa na possibilidade de contribuir com a promoção de novos conhecimentos sobre a temática, assim como pela possibilidade de, a partir de seus resultados, sugerir boas práticas orientadas à instituição ou ao fortalecimento de uma política de segurança da informação no âmbito da administração pública.

Quanto à sua estrutura, o artigo está dividido em cinco seções. A contextualização do tema, problemática, objetivos e justificativa são apresentadas na primeira seção. Em seguida, apresenta-se a discussão teórica sobre segurança da informação, na perspectiva de uma política institucional. Os procedimentos metodológicos para a realização da pesquisa são apresentados na terceira seção. Já os resultados são analisados na quarta seção, seguida das considerações finais da pesquisa.

2 FUNDAMENTAÇÃO TEÓRICA

A presente pesquisa fundamenta-se nos conceitos de Segurança da Informação (SI), bem como os elementos relacionados à política de segurança que visam a garantia da proteção dos ativos de informação contra ameaças.

2.1 SEGURANÇA DA INFORMAÇÃO: CONTEXTO HISTÓRICO E ASPECTOS FUNDAMENTAIS

A preocupação com a segurança da informação não é recente. Segundo Martins e Santos (2005), o processo de estabelecimento de regras e padrões de segurança começou na década de 1960, impulsionado pelo contexto da Guerra Fria. No entanto, em 1998, após o Centro de Investigação Nuclear da Índia, *Bhabha Atomic Research Centre*, sofrer uma série de ataques, surgiu a preocupação com a segurança da informação em vários países pelo mundo.

No Brasil, no final dos anos 2000, a Associação Brasileira de Normas Técnicas (ABNT) aceitou a norma ISO como padrão brasileiro, surgindo, em 2001, a NBR 17799: 2001 – Código de Prática para a Gestão da Segurança da Informação. No segundo semestre de 2005 foi lançada a nova versão da norma, a NBR ISO/IEC 17799:2005.

A ISO – *International Organization for Standartization* é uma entidade independente e não governamental que desenvolve e publica normas internacionais. Seu objetivo é criar padrão global de qualidade que garanta a segurança, eficiência e interoperabilidade de produtos, serviços e sistemas em uma ampla variedade de setores. Mariani (2006) afirma que esses conjuntos de normas formam um sistema de gestão da qualidade aplicável a qualquer organização, sem considerar seu tamanho ou se a organização é pública ou privada.

A NBR ISO/IEC 17799 fornece um código de prática para a gestão da segurança da informação, definindo-a como a preservação da confidencialidade, integridade e disponibilidade das informações. Além disso, outras propriedades, como autenticidade, legalidade, não repúdio e confiabilidade, também podem estar envolvidas (ABNT, 2005). Nesse contexto, a Segurança da Informação (SI)

> é obtida a partir da implementação de um conjunto de controles adequados, incluindo políticas, processos, procedimentos, estruturas organizacionais e funções de *software* e *hardware*. Estes controles precisam ser estabelecidos, implementados, monitorados, analisados criticamente e melhorados, onde necessário, para garantir que os objetivos do negócio e de segurança da organização sejam atendidos. Convém que isto seja feito em conjunto com outros processos de gestão do negócio (ABNT, 2005, p. ix).

Para Beal (2005), a SI pode ser entendida como o processo de proteger informações das ameaças, fornecendo um conjunto de orientações, normas, procedimentos e políticas, que visam a proteção dos ativos de informação de uma organização. É importante ressaltar que a SI envolve o planejamento cuidadoso das necessidades, recursos, capacidades, infraestrutura, devendo incluir todas as pessoas da organização e, se necessário, atores externos (ABNT, 2005). Isto se explica, pois, como o seu intuito é evitar ou minimizar riscos, o não envolvimento de todas as pessoas pode levar a ações que não estejam comprometidas com o propósito organizacional de segurança por parte de alguns colaboradores.

Machado (2014) destaca três princípios considerados importantes para que as informações sejam devidamente protegidas: Disponibilidade, Integridade e Confidencialidade.

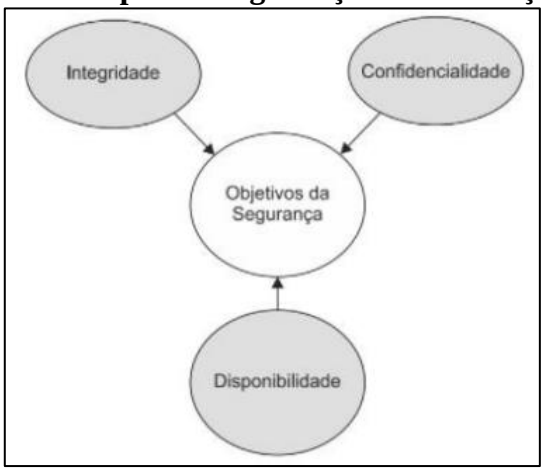
Confidencialidade: garantir que somente pessoas autorizadas dentro da organização tenham acesso à informação;

Integridade: garantir que a informação se mantenha íntegra, ou seja, que não tenha sido alterada em nenhum estágio, propositalmente ou não;

Disponibilidade: garantir que a informação esteja disponível no momento em que a organização precise para as atividades de seus colaboradores.

Conforme Machado (2014), os três princípios mencionados anteriormente formam a chamada Tríade CIA, que representa os pilares centrais de qualquer programa de segurança da informação.

Figura 1 – Princípios de segurança da informação (CIA)



Fonte: Machado (2014, p. 13).

Araújo, Araújo e Batista (2022) entendem que a SI deve estar sempre presente em todas as organizações que ficam de posse de grande volume de dados e informações, pois estes são ativos extremamente valiosos para qualquer organização. Os referidos autores afirmam ainda que a proteção da informação durante todo seu ciclo de vida é responsabilidade da organização, razão pela qual é essencial compreender os pilares fundamentais que sustentam a SI, de modo que as políticas de segurança sejam balizadas nestes princípios.

A ISO/IEC 27002:2022, que estabelece diretrizes e princípios gerais para implementar, manter e melhorar a gestão da SI, considerando os riscos do ambiente organizacional, define que a política de SI deve ser documentada, trazendo o conceito de segurança para a organização, os objetivos para atingi-la e formas de controle. Esta política deve refletir o compromisso da gestão organizacional com a SI (ISO/IEC 27002:2022).

Diante disso, nota-se que as organizações precisam desenvolver e adotar uma política de SI como prioridade institucional, a fim de garantir que seus ativos de informação estejam protegidos contra ameaças. Para tanto, é fundamental desenvolver um sistema de governança de TI, uma vez que essa política é parte de um sistema de gestão mais amplo, como será discutido a seguir.

2.2 GOVERNANÇA DE TECNOLOGIA DA INFORMAÇÃO

As organizações vivenciam constantes desafios para garantir a segurança dos dados e informações pelos quais é responsável. Nesse sentido, a identificação das causas que podem comprometer a segurança destes ativos, seja externa (vírus, *phishing*[1], negação de serviço distribuída[2], invasão de bancos de dados e sistemas), bem como interna (uso incorreto, acesso sem permissão, desconhecimento sobre o sistema) é fundamental para a instituição de práticas que orientem a segurança na organização (Baptista Júnior; Dian, 2021).

Entretanto, o planejamento e adoção de práticas de SI não é responsabilidade apenas do setor de TI ou, na ausência de um setor formalmente constituído, das pessoas que lidam com a tecnologia na organização. A SI é um compromisso institucional, sendo parte de um sistema amplo de gestão, onde a TI deve estar alinhada ao propósito organizacional, ou seja, um sistema de governança de TI (GovTI).

Segundo Fernandes e Abreu (2014), a GovTI busca o direcionamento da TI aos objetivos do negócio e o monitoramento contínuo para verificar a conformidade com as decisões tomadas pela administração da organização. Duarte e Lima (2018, p. 250) afirmam que a GovTI "espelha conceitos da governança corporativa, ao mesmo tempo em que se concentra no uso racional e efetivo da TI para alcançar as metas da organização".

É importante destacar que a governança corporativa "é um sistema formado por princípios, regras, estruturas e processos pelo qual as organizações são dirigidas e monitoradas, com vistas à geração de valor sustentável para a organização, para seus sócios e para a sociedade em geral" (IBGC, 2023, p. 17). Nessa perspectiva, a GovTI visa criar um sistema que oriente as políticas, processos, recursos e responsáveis pela gestão da TI na organização, visando o seu alinhamento com o negócio.

---

[1] *Phishing*: Envio de mensagens com iscas para atrair pessoas e obter informações pessoais.
[2] Negação de serviço distribuída (DDoS): É um ataque direcionado a inutilizar um *site*, servidor ou rede, impedindo que os usuários acessem serviços ou adquiram produtos.

Para Reis e Souza Neto (2019, p. 613), “o foco em controle e monitoramento dado pela Governança de TI, herdado da Governança Corporativa, é apropriado, o que indica que a implantação de um adequado sistema de GovTI por parte das organizações é um movimento de importância estratégica”. É possível perceber que a GovTI está relacionada ao nível estratégico da organização, com envolvimento no planejamento estratégico, no desenvolvimento de políticas e diretrizes para o uso da TI, além de planejamento dos recursos necessários ao uso da TI. Considerando a necessidade de alinhamento entre a TI e o negócio, a GovTI deverá promover uma cultura organizacional voltada para a aceitação e melhor uso da tecnologia da informação.

No contexto específico da administração pública, por se tratar do foco deste estudo, Reis e Souza Neto (2019) enfatizam que a área de TI vem recebendo atenção cada vez maior, diante do seu potencial de contribuição para a melhoria dos resultados à sociedade. Nesse aspecto, os autores afirmam que o Tribunal de Contas da União (TCU) vem realizando levantamentos, desde 2007, sobre a situação da GovTI na administração pública, identificando que, apesar da tendência de evolução em sua adoção, os resultados ainda estão longe do esperado, “o que sugere lacunas nas orientações para essa implantação” (Reis; Souza Neto, 2019, p. 611).

Nesse cenário, os autores identificaram dez fatores críticos de sucesso (FCS) à implantação da GovTI na administração pública federal, agrupados nas seguintes categorias: alta administração, comunicação, estratégia, partes interessadas, processos, requisitos e treinamento. O Quadro 1 apresenta os FCS por categoria.

Quadro 1 – Fatores críticos de sucesso à implantação da GovTI

Categorias	Fatores críticos de sucesso
Alta administração	- A implantação da GovTI deve ser decidida pela alta administração.
	- A alta administração deve apoiar continuamente a implantação da GovTI.
Comunicação	- Deve haver comunicação e cooperação eficiente entre as partes interessadas.
Estratégia	- A gestão de recursos de TI deve ter dimensão estratégica na organização.
	- A TI deve ser alinhada aos negócios.
Partes interessadas	- Identificar e envolver as partes interessadas.
	- Reter pessoas-chave para a implantação.
Processos	- Iniciar com alguns processos.
Requisitos	- Monitorar conformidades legais.
Treinamento	- Capacitar a equipe de TI para adotar as mudanças.

Fonte: Elaborado com base em Reis e Souza Neto (2019).

Com base no exposto no Quadro 1, a implantação da GovTI deve ser um compromisso da alta administração, sobretudo porque o envolvimento dos demais colaboradores da organização poderá ser consideravelmente comprometido se o compromisso com a adoção deste sistema de governança não vier dos níveis estratégicos.

Além disso, os processos de comunicação entre todos os envolvidos deverão ser cuidadosamente planejados, de modo que o papel da TI para a organização, as diretrizes para a sua utilização e requisitos de segurança sejam difundidos e compreendidos por todos.

Enquanto uma ação de nível estratégico, a TI não pode ser percebida como um departamento acessório, sendo essencial a compreensão da importância deste setor por toda a organização (Duarte; Lima, 2018). Esta percepção contribuirá para o planejamento da equipe, identificando-se as suas capacidades e eventuais necessidades de treinamento.

É importante destacar ainda a necessidade de adequação aos requisitos legais sobre o uso da TI, notadamente no que diz respeito aos mecanismos de garantia da segurança da informação. Nesse aspecto, Baptista Júnior e Dian (2021) chamam atenção para a Lei de Crimes Cibernéticos (Lei nº 12.737/2012), o Marco Civil da Internet (Lei nº 12.965/2014), bem como a Lei Geral de Proteção de Dados (Lei nº 13.709/2018), dispositivos legais que refletem a crescente preocupação com a SI no Brasil.

Pelo exposto, considerando a amplitude que um sistema de GovTI possui, nem sempre as organizações reconhecem o papel estratégico da TI, utilizando-a sem uma diretriz institucional alinhada ao seu propósito. A ausência deste sistema leva ao comprometimento da política de segurança da informação e maximiza os riscos de perda ou uso inadequado dos ativos informacionais, o que denota a importância da governança para quaisquer contextos organizacionais.

3 PROCEDIMENTOS METODOLÓGICOS

A pesquisa é um processo formal que representa o meio para obter respostas aos problemas que são propostos, utilizando métodos, técnicas e procedimentos para viabilizar a sua condução e obter resultados (Marconi; Lakatos, 2021).

Quanto à sua classificação, a pesquisa é de natureza aplicada, uma vez que, a partir de seus resultados, pretende sugerir boas práticas orientadas à instituição ou ao fortalecimento de uma política de segurança da informação à Prefeitura de Marcação. Prodanov e Freitas (2013, p. 51) entendem que a pesquisa aplicada “objetiva gerar conhecimentos para aplicação prática dirigidos à solução de problemas específicos. Envolve verdades e interesses locais”.

Do ponto de vista dos objetivos, a presente pesquisa se caracteriza como exploratória e descritiva. Marconi e Lakatos (2021) afirmam que os estudos exploratórios permitem maior familiaridade com o problema e a construção de hipóteses. Este tipo de pesquisa tem o intuito de obter uma visão inicial, por meio de levantamento bibliográfico, ou conversas com pessoas que possuem conhecimento ou experiência no ambiente de pesquisa, abordando todos os

aspectos relevantes e necessários. Já a pesquisa descritiva objetiva descrever as características de uma população, ou identificar relações entre variáveis (Prodanov; Freitas, 2013).

Em relação aos procedimentos técnicos, a pesquisa é classificada como um estudo de caso, que se refere ao levantamento com maior profundidade de determinado caso ou grupo humano sob todos os seus aspectos (Marconi; Lakatos, 2021). Seu principal objetivo é compreender uma situação específica e detalhar o caso que está sendo estudado.

Quanto à abordagem do problema, o trabalho consiste em uma pesquisa qualitativa, que se caracteriza principalmente pela interpretação do fato estudado, sem o uso de métodos e técnicas estatísticas para análise dos dados. Para Prodanov e Freitas (2013), na abordagem qualitativa o ambiente serve como uma fonte direta para a coleta de dados, necessitando de um trabalho mais intensivo de campo.

A coleta de dados da pesquisa se deu por meio de entrevistas semiestruturadas realizadas com servidores públicos que atuam na Prefeitura Municipal de Mataraca, utilizando os sistemas lá implantados. Prodanov e Freitas (2013) afirmam que a entrevista é a obtenção de informações de um entrevistado sobre determinado assunto ou problema. Para os autores, as entrevistas semiestruturadas permitem flexibilidade no roteiro, podendo explorar mais amplamente algumas questões.

Para a delimitação do número de entrevistados, buscou-se, inicialmente, identificar os setores existentes na Prefeitura de Mataraca, considerando a disposição de sua estrutura organizacional constante na Lei nº 522/2021. De acordo com este documento, a Prefeitura possui, enquanto órgãos de assessoramento, o Gabinete do Prefeito e do Vice-prefeito. Já como órgãos auxiliares, constam a Procuradoria Geral do Município, Secretaria Geral, Secretaria de Finanças, Administração e Planejamento e Contadoria Geral do Município. Por fim, como órgãos de administração específica, constam oito secretarias municipais: Secretaria de Educação e Desportos, Secretaria de Saúde, Secretaria de Obras Públicas e Serviços Urbanos, Secretaria de Agricultura, Secretaria de Meio Ambiente, Secretaria de Assistência Social, Secretaria de Indústria, Comércio e Turismo e Secretaria de Cultura.

É possível constatar que não há uma secretaria destinada à área de TI, embora os sistemas sejam utilizados por diferentes secretarias. Nesse aspecto, foi realizado um levantamento das secretarias ou setores que fazem uso de sistemas de informação, bem como o quantitativo de servidores que possuem acesso a eles, conforme apresentado na Tabela 1.

Tabela 1 – Sujeitos da pesquisa

Setores	Servidores com acesso a sistemas	Entrevistados
Secretaria de Finanças, Administração e Planejamento	03	01
Secretaria de Saúde	04	02
Secretaria de Educação	03	01
Contadoria Geral	02	01
Procuradoria	01	01
Total		**06**

Fonte: Elaboração própria (2024).

Deste modo, a pesquisa foi realizada a partir de entrevistas com seis servidores municipais. As entrevistas foram gravadas e as respostas transcritas para um editor de textos, para viabilizar a análise dos resultados. É importante destacar que, para evitar a identificação dos participantes, foram utilizados códigos para a representação de cada um, sem a indicação do setor em que atuam (E1 até E6). A numeração dos códigos se deu pela ordem de realização das entrevistas.

A análise dos dados coletados com as entrevistas se deu pela técnica da análise de conteúdo, com o método de definição de categorias proposto por Bardin (2011, p. 48). Para a autora, a análise de conteúdo consiste em

> [...] um conjunto de técnicas de análise das comunicações visando obter, por procedimentos sistemáticos e objetivos de descrição do conteúdo das mensagens, indicadores (quantitativos ou não) que permitam a inferência de conhecimentos relativos às condições de produção/recepção (variáveis inferidas) destas mensagens.

O Quadro 2 apresenta as categorias da pesquisa e os aspectos investigados em cada uma.

Quadro 2 – Categorias da pesquisa

Categorias	Aspectos analisados
Recursos	- Sistemas, tipos de dados e informações coletados e os usuários que acessam e/ou utilizam as informações; - Procedimentos para acesso aos sistemas.
Implementação	- Definição de segurança da informação; - Documentação para a orientação sobre SI; - Comprometimento da alta gestão sobre SI; - Responsáveis pela SI.
Análise crítica	- Levantamento de ameaças ou incidentes com SI; - Ações preventivas e corretivas visando a SI; - Instrumentos e/ou canais para compartilhar informações que minimizem erros ou incidentes; - Mecanismos de controle de SI; - Equipe responsável pela garantia de SI; - Treinamentos e capacitações em SI.

Fonte: Elaboração própria (2024).

As categorias da pesquisa foram definidas a partir proposta de política de segurança da informação contida na NBR ISO/IEC 17799.

4 APRESENTAÇÃO E DISCUSSÃO DOS RESULTADOS

Inicialmente, é apresentado o perfil dos sujeitos entrevistados, os quais, ocupam cargos em setores e secretarias relevantes da prefeitura de Municipal de Mataraca/PB. Durante as entrevistas, foram solicitadas informações para a caracterização desses participantes, incluindo: idade, gênero, nível de escolaridade, cargo ocupado e o período de tempo no qual desempenha sua função.

Os respondentes possuem idade entre 32 e 47 anos, sendo quatro do sexo masculino (E1, E2, E4 e E5) e dois do sexo feminino (E3 e E6). Quanto aos níveis de escolaridade, um dos respondentes tem ensino médio completo, um possui ensino superior incompleto, dois possuem ensino superior completo e outros dois possuem Pós-Graduação (Mestrado e Doutorado).

Quanto ao tempo de atuação na Prefeitura de Mataraca, identificou-se um tempo médio de 11 anos, sendo o menor período de seis meses e a atuação mais longa de 27 anos. Entre os cargos que ocupam, foram citados Operador de Sistema, Procurador Geral do município, Chefe de Tributação e Fiscalização, Secretário Escolar e Diretor de Contabilidade. É importante frisar que a investidura em cargo público se dá mediante concurso público, podendo ser também comissionado ou contratado, dos entrevistados sendo três em regime de trabalho comissionado (E1, E3 e E5) e três em regime de trabalho efetivo (E2, E4 e E6).

4.1 DESCRIÇÃO DOS RECURSOS

Esta primeira categoria da pesquisa é direcionada a apresentar os sistemas que a Prefeitura utiliza, bem como os dados e informações que são coletados e armazenados nesses sistemas e os usuários que acessam e/ou utilizam essas informações, bem como os procedimentos para acesso a esses sistemas.

Identificou-se que nem todos utilizam os sistemas, como foi o caso de E1, ao afirmar que não utiliza nenhum sistema interno da prefeitura, portanto, não há quaisquer procedimentos de acesso. Para a sua atuação, é necessário o uso de um sistema federal, que não tem cadastro na base de dados da Prefeitura de Mataraca.

No âmbito da Secretaria de Saúde, foram identificados diversos sistemas, sendo eles: CNES (Cadastro Nacional de Estabelecimento da Saúde); SIA (Sistema de Informacional Ambulatorial); E-Gestor AB (Sistema de Gestão de Atenção Básica); e, SISREG III (Sistema

Nacional de Regulação). Todos esses sistemas são disponibilizados e vinculados ao Ministério da Saúde (MS), que tem como objetivo apoiar a gestão, organização e monitoramento das ações de saúde pública.

O E2 é o operador principal destes sistemas, mas por se tratar de um sistema em que há a necessidade da integração com outros setores, outros profissionais também acessam, como médicos, enfermeiros e técnicos em enfermagem, para que essa rede de informações seja devidamente compartilhada e transmitida aos órgãos competentes.

O procedimento de acesso a esses sistemas é o mesmo para todos os usuários, tendo em vista que, por se tratar de sistemas vinculados ao MS, o acesso se dá por meio da conta GOV.BR, tendo por base o CPF como login e senha pessoal. E2 destaca que há um cadastro prévio na base da Secretaria da Saúde, para que terceiros não tenham acesso aos sistemas sem a devida liberação. Este cadastro para autorização de acesso configura uma ação de segurança do sistema, uma vez que, sem esse procedimento, qualquer pessoa com registro da conta GOV.BR poderia acessar os sistemas.

Há ainda o sistema PEC (Prontuário Eletrônico do Paciente), cujo acesso por cada profissional se dá por meio de um login e senha próprios. Sobre o PEC, E2 relata que há uma divisão por módulos, sendo o acesso a estes módulos dependente de cada função. Assim, um médico tem acesso ao seu módulo, enquanto outros profissionais não podem acessar este mesmo espaço.

Já na Secretaria de Administração, Finanças e Planejamento, é utilizado o sistema de Gestão Tributária, sistema esse que é contratado da empresa ELMAR Tecnologia. O sistema permite a gestão de recolhimento, lançamento e arrecadação de todos os tributos, vinculado com a conta do município. Segundo E4, o sistema é integrado de forma online, possibilitando que os contribuintes, após um cadastro, acessem para a consulta de situação fiscal, retiradas de certidões e emissão de notas fiscais, enquanto a equipe deste setor acompanha internamente, podendo efetuar medidas corretivas e orientações, através dos fiscais.

No âmbito da Contadoria Geral, é utilizado um sistema de contabilidade, por meio do qual as informações são alimentadas através de notas fiscais. O sistema armazena dados de empresas e CPF, quando se trata de pessoa física. São armazenados também dados de todos os funcionários do quadro de pessoal da Prefeitura. Para acesso ao sistema, E5 relata a necessidade de dois procedimentos: o primeiro é o acesso ao provedor do sistema, mediante login e senha. Em seguida, E5 afirma que é preciso “selecionar a unidade na qual eu vou trabalhar - Prefeitura de Mataraca - e colocar a segunda senha, então, são duas medidas de segurança iniciais para ter acesso ao banco de dados”.

Por fim, na Secretaria de Educação, são utilizados os seguintes sistemas: SABER (Ambiente Virtual de Apoio à Educação Estadual), Censo Escolar e Bolsa Família. Além dos dados pessoais dos alunos, como RG e CPF, os dados coletados e armazenados nesses sistemas são em relação à frequência e participação ativa na escola, tanto no dia a dia, bem como na progressão de seu conhecimento. Para acesso aos sistemas SABER e Bolsa Família, é necessário apenas login e senha.

Já o sistema do Censo, conforme relatado por E6, exige também a confirmação de imagens, procedimento conhecido como CAPTCHA (*Completely Automated Public Turing test to tell Computers and Humans Apart*), que, segundo Magalhães (2021), é um teste automatizado para diferenciar computadores e humanos. Esse procedimento é uma solução anti-spam, evitando que *sites* e sistemas sejam acessados por *bots*.

Nota-se que os diferentes sistemas utilizados coletam e armazenam dados pessoais, que são considerados sensíveis, além de dados financeiros de organizações e servidores públicos e dados de saúde da população assistida pelos serviços de saúde de Mataraca. Nesse aspecto, tendo em vista o tipo de dado processado e armazenado nesses sistemas, as diretrizes para tratamento e segurança destes dados devem ser cuidadosamente elaboradas, em atendimento à legislação vigente, como destacam Baptista Júnior e Dian (2021).

A partir dos relatos dos entrevistados, observou-se que o acesso a estes sistemas se dá por meio dos requisitos de segurança estabelecidos pelos próprios desenvolvedores dos sistemas, não havendo um método padronizado para acesso pelos usuários.

4.2 IMPLEMENTAÇÃO DA SEGURANÇA DA INFORMAÇÃO

A segunda categoria da pesquisa foi direcionada a identificar o entendimento dos entrevistados sobre a definição de segurança da informação, bem como a existência de documentação para a orientação sobre SI no âmbito da Prefeitura de Mataraca. Buscou-se também identificar a percepção dos entrevistados sobre o comprometimento da alta gestão com a SI e os responsáveis pela segurança.

Ao serem questionados sobre como definem segurança da informação, percebeu-se uma dificuldade nas respostas, limitando o entendimento à LGPD, à segurança do próprio sistema que utilizam em suas funções ou ao uso de antivírus. Nesse sentido, E1 comentou: “Eu entendo como Segurança da Informação dados sensíveis que tem que ser protegidos”.

Por outro lado, o entrevistado E2 definiu SI como sendo o uso de bons antivírus nos sistemas, mencionando que atualmente não há nenhuma proteção eficaz nos sistemas que utiliza, o que os torna vulneráveis a ataques de *hackers*.

Por sua vez, E4 relatou um episódio que ocorreu na Prefeitura, e que após tal situação, foram “obrigados” a adotar um modelo de segurança:

> A segurança da informação é algo extremamente importante, haja vista que nós tivemos problemas recentes com perda de dados, porque não tínhamos um sistema online, não estávamos trabalhando em nuvens, então, à medida que os computadores foram furtados, nós ficamos sem dados, perdemos muitos dados que tínhamos em nossa base. Tivemos muita dificuldade para poder recuperar, e recuperamos, mas de forma defeituosa. Então, a partir desse episódio, nós começamos a ter um pouco mais de zelo e cuidado com a segurança da informação (E4).

O relato evidencia a ausência de procedimentos que orientem o armazenamento dos dados, evitando a perda destes em situações como a relatada. Além disso, a adequada orientação sobre quais as informações que serão armazenadas, como se dará este armazenamento e quem terá acesso contribuirá para uma maior segurança das informações que devem ficar sob a responsabilidade da Prefeitura de Mataraca, sob o aspecto legal e para facilitar a rápida recuperação destas informações.

Identificou-se que nenhum dos entrevistados conseguiu formular um conceito sobre segurança da informação, mas apresentaram alguns elementos que podem estar associados à sua definição. Conforme Netto e Silveira (2007) afirmam, a SI é a área do conhecimento que visa a proteção da informação das ameaças à sua integridade, disponibilidade e confidencialidade, a fim de garantir a continuidade do negócio e minimizar os riscos.

Questionou-se, em seguida, sobre a existência de alguma orientação sobre a SI por parte da Prefeitura, considerando-se documentos que tragam tais orientações. Nesse aspecto, os entrevistados E1, E2, E3 e E6 foram enfáticos ao responderem não possuir nenhum conhecimento a respeito de documentos que tragam orientações sobre SI fornecidos ou elaborados pela Prefeitura de Mataraca. Nesse mesmo sentido, E4 reconhece a LGPD como sendo uma obrigação legal de todas as organizações, independente do seu porte, mas nem sequer ela está sendo efetivamente disseminada dentro da Prefeitura.

Diferente das respostas anteriores, E5 respondeu que acredita que a Prefeitura de Mataraca tenha um decreto relacionado à Lei Geral de Proteção de Dados. O entrevistado relata:

> Eu acredito que a Prefeitura de Mataraca tenha nem que seja um decreto regulamentando o acesso à Lei Geral de Proteção de Dados, no qual a Prefeitura se adequa a tudo que a LGPD coloca. Esse documento deve estar publicado no Diário Oficial do Município. Como o nosso município tem, além do Diário do Município, fixação no mural de avisos. Nós também publicamos no Diário da FAMUP, que já é um jornal que a gente entende por nível estadual. Muitos municípios já adotam ele como diário oficial do município, mas também está público na internet para qualquer usuário externo ter acesso a essa informação.

Como todo ato ou normativo administrativo no serviço público precisa ser publicado, sendo a publicidade um dos princípios da administração pública (Brasil, 2016), a partir deste relato, foi realizada uma busca nos portais mencionados, não sendo identificado nenhum tipo de documento semelhante, ou que tratasse de políticas de Segurança da Informação.

Quando questionados a respeito de como avaliam o comprometimento da alta gestão sobre a SI, todos os entrevistados não conseguiram responder de maneira clara e concisa, pontuando apenas como algo importante, levando esse comprometimento por parte da gestão apenas pelo aspecto físico/estrutural, como pode ser visto no comentário de E4: "Essa é uma questão importante, porque o olhar da gestão é um olhar um pouco estrutural, no sentido de prover estrutura física e outros itens de infraestrutura, mas ainda não foi captado essa demanda".

Ainda no que tange à avaliação do comprometimento por parte da alta gestão, E5 afirma: "A gente ainda não tem uma equipe formada para a gestão da segurança da informação, ou seja, cada setor da Prefeitura de Mataraca é detentor da segurança e da guarda de todos os documentos e informações contidas no setor".

Em se tratando dos responsáveis pela segurança da informação, todos os entrevistados afirmaram não ter nenhuma pessoa específica para esse fim. Dada a importância, E4 e E5 afirmaram que esta definição é algo urgente e necessário, devido à grande quantidade de dados e informações que diariamente são gerenciados em todos os setores da Prefeitura.

A análise dos relatos permite considerar que não existe nenhum documento emitido pela Prefeitura de Mataraca que traga orientações sobre a SI, ficando a cargo de cada servidor a compreensão e adoção de medidas que visem a segurança dos ativos informacionais. Tal situação evidencia a ausência de uma governança sólida nessa área, o que pode comprometer seriamente a integridade, confidencialidade e disponibilidade das informações municipais.

4.3 AÇÕES DE ANÁLISE CRÍTICA

Esta terceira categoria visa identificar a adoção de ações voltadas para análise crítica da segurança da informação no âmbito da prefeitura de Mataraca, considerando o levantamento de ameaças ou incidentes com SI, as ações preventivas e corretivas visando a SI, o uso de instrumentos e/ou canais para compartilhar informações que minimizem erros ou incidentes, a adoção de mecanismos de controle de SI, definição de uma equipe responsável pela garantia de segurança e realização de treinamentos e capacitações em SI.

Foi perguntado, inicialmente, se existe algum levantamento de ameaças ou incidentes à segurança da informação para orientar as ações da Prefeitura. Todos os entrevistados responderam que não existe esse levantamento até o momento. A3 relata que a Prefeitura de

Mataraca possui um único servidor que desenvolveu um sistema para acompanhar possíveis problemas nos computadores, entretanto, não tem conhecimento se há um levantamento dos incidentes com relação à segurança. Em complemento, E4 e E5 relataram que cada setor deve buscar maneiras de se proteger contra qualquer situação adversa que possa vir a acontecer, mas não há uma orientação institucional a partir desse levantamento.

Quanto à existência de ações preventivas e corretivas, mais uma vez, com base nas respostas dos entrevistados, observa-se que as ações são desenvolvidas por iniciativa própria. Nesse sentido, A3 afirma que inseriu um requisito de segurança para acesso aos dados de seu setor, por meio de códigos. Assim, um usuário que não tenha esses códigos, não consegue acessar as informações armazenadas no computador.

Para A5, a definição de ações que pudessem orientar os servidores quanto à SI depende de uma equipe que deveria ser constituída para ficar responsável pelo setor de segurança. A ausência dessa equipe leva cada um a buscar meios de proteger as informações e atender à LGPD.

Já A2 informou que, para evitar a perda de informações importantes, faz o *backup* do sistema, sendo esta uma iniciativa própria: “A iniciativa é minha, porque como faz muito tempo que eu trabalho com isso, muitas pessoas sofrem o erro disso”. A2 relata ainda que faz parte de um grupo em que as pessoas já compartilharam problemas pela perda de informações e que não tinham *backup* dos dados, o que serviu de alerta para não cometer o mesmo erro.

Em se tratando de instrumentos e/ou canais para compartilhamento de informações que minimizem os erros ou incidentes, os entrevistados E1, E2, E3, E4 e E6 responderam não ter conhecimento de nenhum. Enfatizando, E5 afirma: “A gente não tem nenhum instrumento que realmente combata algum incidente que ocorre com relação à segurança da informação”.

Quanto aos mecanismos de controle de SI, os entrevistados E2, E3 e E6 responderam não existir. Já E1, E4 e E5 entendem que cada setor deve buscar maneiras e métodos de controle para evitar problemas com relação à segurança da informação.

Por fim, foi perguntado aos entrevistados sobre a existência de uma equipe responsável pela garantia da segurança da informação e se existem treinamentos e capacitações sobre SI. Sem exceção, todos os entrevistados responderam que não existe essa equipe e nem incentivos para a participação em treinamentos e capacitações sobre SI. Sobre os treinamentos, A2 afirma que a participação se dá apenas quando o sistema que utiliza tem alguma atualização, mas, por se tratar de um sistema do governo federal, a iniciativa na oferta desses treinamentos não é da Prefeitura, assim como a temática não é segurança da informação. Já E6 relata:

> Em relação à segurança da informação, não existe treinamento. Nesses quinze anos eu nunca ouvi ninguém que fez ou que foi incentivado a fazer. As capacitações são realmente sobre os próprios programas, mas sobre a segurança das informações, não.

Diante dos relatos apresentados, é possível evidenciar que, além da ausência de uma política de SI, as ações que podem buscar a garantia de segurança são desenvolvidas exclusivamente por iniciativa dos servidores. Percebeu-se, inclusive, que nem todos os entrevistados apontaram exemplos de como utilizam, em suas atividades diárias, práticas voltadas para a SI.

Reis e Souza Neto (2019) entendem que a política de segurança da informação é parte de uma estrutura de Governança de TI. Esta, por sua vez, deve ser planejada a partir do comprometimento da alta administração, do estabelecimento dos meios adequados para comunicação das ações direcionadas à SI, do envolvimento e capacitação das pessoas para o adequado uso da TI.

Nesse aspecto, considerando o levantamento realizado a partir desta pesquisa, compreende-se ser essencial que a Prefeitura estabeleça e documente uma política de SI, considerando o conceito de SI, os objetivos para atingi-la e as formas de controle, como preconiza a ISO/IEC 27002:2022. Esta documentação será essencial para que a garantia da segurança dos ativos informacionais da Prefeitura de Mataraca seja buscada por todos os servidores, a partir de uma orientação institucional.

5 CONSIDERAÇÕES FINAIS

A presente pesquisa teve como objetivo identificar os elementos relacionados à segurança utilizados para a garantia da proteção dos ativos de informação da Prefeitura Municipal de Mataraca. Para tanto, foram entrevistados seis servidores da Prefeitura, de diferentes setores que lidam diretamente com sistemas por onde circulam informações pessoais, de saúde e financeiras.

A pesquisa realizou um levantamento teórico sobre a relevância da segurança da informação para as organizações que gerenciam ativos de informação. Isso permitiu não apenas compreender sua importância, mas também os impactos negativos para as organizações, sejam elas públicas ou privadas, que não adotam medidas de segurança para seus ativos de informação. Este levantamento orientou a investigação de campo, tendo como guia a proposta de política de segurança da informação contida na NBR ISO/IEC 17799.

Os resultados alcançados com a pesquisa permitem concluir que a Prefeitura de Mataraca apresenta vulnerabilidades a possíveis ameaças com relação aos seus ativos

informacionais, por não apresentar uma política que oriente os procedimentos de segurança em todos os setores. Com isto, as ações ficam ao encargo de cada servidor, por iniciativa própria.

Dessa forma, fica evidente a necessidade de criar e implementar uma Política de Segurança da Informação, integrando-se às políticas institucionais e ao planejamento estratégico da Prefeitura. Para tanto, recomenda-se que sejam estabelecidos, no documento onde a política ficará registrada: a) os recursos sobre os quais ela versará, incluindo sistemas, usuários e procedimentos de acesso, com as devidas medidas de segurança; b) as ações necessárias à sua implementação, definindo a segurança da informação no âmbito da Prefeitura de Mataraca, os documentos que irão orientar os procedimentos de segurança em todos os setores que façam uso de sistemas ou de outras ferramentas e ambientes digitais que contenham dados e informações de servidores, fornecedores e dos cidadãos do município, o papel da alta gestão nesse processo e a definição de uma equipe responsável pela gestão da SI na Prefeitura; c) as ações que viabilizem uma análise crítica da SI, a partir do levantamento de ameaças ou incidentes com segurança, da criação de canais para que sejam compartilhadas informações que orientem sobre a SI, minimizando erros e auxiliando na prevenção de incidentes, bem como da oferta de treinamentos e capacitações sobre segurança da informação aos servidores da Prefeitura.

Percebeu-se, a partir do levantamento teórico realizado, que o tema de política de segurança da informação em prefeituras municipais ainda é pouco abordado, sendo maior o direcionamento de pesquisas na administração pública federal. Assim, sugere-se, a título de estudos futuros, o desenvolvimento de pesquisas nessa área em outros municípios, dado o impacto significativo de proteger adequadamente as informações públicas e garantir a eficiência administrativa.

REFERÊNCIAS

ABNT – ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **Tecnologia da informação – Técnicas de Segurança – Código de prática para gestão de segurança da informação**. ABNT NBR ISO/IEC no 17.799:2005, de 30/09/2005. Disponível em: https://www.facom.ufu.br/~william/Disciplinas%202013-1/BSI%20-%20GSI035%20-%20Auditoria%20e%20Seguranca%20da%20Informacao/Materiais%20Auxiliares/NBR%20ISO-IEC%2017799-2005-NORMA.pdf. Acesso em: 09 de set. 2024.

ARAÚJO, Wagner Junqueira; ARAÚJO, Sueny Gomes Léda; BATISTA, Rafaela Romaniuc. Cenários para a implementação de políticas de segurança da informação em universidades públicas federais. **Ciência da Informação**, v. 51, n. 3, 2022.

BAPTISTA JUNIOR, José Henrique; DIAN, Maurício de Oliveira. A crescente importância da segurança da informação, sobretudo durante a pandemia. **Revista Interface Tecnológica,**

Taquaritinga. v. 18, n. 1, p. 56–67, 2021. Disponível em: https://revista.fatectq.edu.br/interfacetecnologica/article/view/1109. Acesso em: 5 set. 2024.

BARDIN, Laurence. **Análise de conteúdo**. São Paulo: Edições 70, 2011.

BEAL, Adriana. **Segurança da Informação**. São Paulo: Atlas, 2005.

BRASIL. **Constituição da República Federativa do Brasil**: texto constitucional promulgado em 5 de outubro de 1988, com as alterações determinadas pelas Emendas Constitucionais de Revisão nos 1 a 6/94, pelas Emendas Constitucionais nos 1/92 a 91/2016 e pelo Decreto Legislativo no 186/2008. Brasília: Senado Federal, Coordenação de Edições Técnicas, 2016. 496 p.

BRASIL. **Lei nº 13.709/2018, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 21 ago. 2024.

DUARTE, Luciano da Costa; LIMA, Eliomar A. Governança de TI no setor público: um estudo sobre o impacto na efetividade organizacional. In: VI ESCOLA REGIONAL DE INFORMÁTICA DE GOIÁS, 2018, Goiânia. **Anais** [...] Porto Alegre: Sociedade Brasileira de Computação, 2018. p. 239-252.

FERNANDES, Aguinaldo Aragon; ABREU, Vladimir Ferraz de. **Implantando a Governança de TI:** da estratégia à gestão dos processos e serviços. 4. ed. Rio de Janeiro: Editora Brasport, 2024.

FUCCIOLO, Gabriel de Oliveira Brandão. **A lei geral de proteção de dados (LGPD) e o direito à privacidade.** 2022. 36f. Monografia Jurídica (Bacharelado em Direito) – Escola de Direito e Relações Internacionais, Pontifícia Universidade Católica de Goiás, Goiânia, 2022. Disponível em: file:///C:/Users/ildef/OneDrive/%C3%81rea%20de%20Trabalho/Meu%20TCC/Gabriel%20Fucciolo%20de%20Oliveira%20Brand%C3%A3o.pdf. Acesso em: 21 ago. 2024

IBGC – INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA. **Código de Melhores Práticas de Governança Corporativa**. 6. ed. São Paulo: IBGC, 2023.

ISO/IEC 27002:2022. **Segurança da informação, segurança cibernética e proteção da privacidade**: controles de segurança da informação. Disponível em https://www.iso.org/obp/ui/en/#iso:std:iso-iec:27002:ed-3:v2:en. Acesso em 11 set. 2024.

MACHADO, Felipe Nery Rodrigues. **Segurança da informação**: princípios e controle de ameaças. 1. ed. São Paulo: Érica, 2014.

MAGALHÃES, André Lourenti. **O que é CAPTCHA e reCAPTCHA?** 2021. Disponível em: https://canaltech.com.br/internet/o-que-e-captcha-recaptcha/. Acesso em: 25 set. 2024.

MARCONI, Marina de Andrade; LAKATOS, Eva Maria. **Metodologia científica**. 9. ed. São Paulo: Atlas, 2021.

MARIANI, Édio João. As normas ISO. **Revista Científica Eletrônica de Administração**, Garça, v. 6, n. 10, p. 6, jun., 2006. Disponível em: www.revista.inf.br. Acesso em: 25 ago. 2024.

MARTINS, Alaíde Barbosa; SANTOS, Celso Alberto Saibel. Uma metodologia para implantação de um sistema de gestão de segurança da informação. **Revista de Gestão da Tecnologia e Sistemas de Informação,** Salvador, V. 2, n. 2, p. 121-136, junho, 2005. Disponível em: https://www.scielo.br/j/jistm/a/hQnY4VLTvnP3rwhjxnxrYct/?lang=pt&format=pdf. Acesso em: 10 set. 2024.

NETTO, Abner da Silva; SILVEIRA, Marco Antonio Pinheiro da. Gestão da segurança da informação: fatores que influenciam sua adoção em pequenas e médias empresas. **Revista de Gestão da Tecnologia de Informação,** São Paulo, v. 4, n. 3, p. 375-397, agosto, 2007. Disponível em: https://www.scielo.br/j/jistm/a/Vx8Ypv6mDjxdYkKKrfYVgqz/?format=pdf&lang=pt. Acesso em: 10 set. 2024.

PRODANOV, Cleber Cristiano; FREITAS, Ernani Cesar. **Metodologia do trabalho científico**: métodos e técnicas da pesquisa e do trabalho acadêmico. 2. ed. Novo Hamburgo: Feevale, 2013.

REIS, André Luiz Nascimento; SOUZA NETO, João. Fatores críticos de sucesso na implantação da governança da tecnologia da informação na administração pública federal. **Revista do Serviço Público**, v. 70, n. 4, 2019.