UNIVERSIDADE FEDERAL DE ALFENAS

GIOVANI AUGUSTO FERREIRA

ANÁLISE DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DA UNIVERSIDADE FEDERAL DE ALFENAS À LUZ DA POLÍTICA NACIONAL DE SEGURANÇA DA INFORMAÇÃO

VARGINHA/MG

2024

GIOVANI AUGUSTO FERREIRA

ANÁLISE DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DA UNIVERSIDADE FEDERAL DE ALFENAS À LUZ DA POLÍTICA NACIONAL DE SEGURANÇA DA INFORMAÇÃO

Dissertação apresentada como parte dos requisitos para obtenção do título de Mestre em Administração Pública pela Universidade Federal de Alfenas. Área de concentração: Administração Pública.
Orientador: Prof. Dr. Paulo Roberto Rodrigues de Souza

VARGINHA/MG

2024

Sistema de Bibliotecas da Universidade Federal de Alfenas
Biblioteca Campus Varginha

Ferreira, Giovani Augusto.
Análise da Política de Segurança da Informação da Universidade Federal de Alfenas à luz da Política Nacional de Segurança da Informação / Giovani Augusto Ferreira. - Varginha, MG, 2024.
96 f. : il. -

Orientador(a): Paulo Roberto Rodrigues de Souza.
Dissertação (Mestrado em Administração Pública) - Universidade Federal de Alfenas, Varginha, MG, 2024.
Bibliografia.

1. Política de segurança. 2. Segurança da informação. 3. Conformidade legal. I. Souza, Paulo Roberto Rodrigues de, orient. II. Título.

Ficha gerada automaticamente com dados fornecidos pelo autor.

GIOVANI AUGUSTO FERREIRA

ANÁLISE DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DA UNIVERSIDADE FEDERAL DE ALFENAS À LUZ DA POLÍTICA NACIONAL DE SEGURANÇA DA INFORMAÇÃO

O Presidente da banca examinadora abaixo assina a aprovação da Dissertação apresentada como parte dos requisitos para a obtenção do título de Mestre em Administração Pública pela Universidade Federal de Alfenas. Área de concentração: Administração Pública.

Aprovada em: 2 de agosto de 2024.

Prof. Dr. Paulo Roberto Rodrigues de Souza

Presidente da Banca Examinadora

Instituição: Universidade Federal de Alfenas

Prof. Dr. Paulo Henrique de Lima Siqueira

Instituição: Universidade Federal de São João Del-Rei

Prof. Dr. Luiz Eduardo da Silva

Instituição: Universidade Federal de Alfenas

Documento assinado eletronicamente por **Paulo Roberto Rodrigues de Souza**, **Professor do Magistério Superior**, em 07/08/2024, às 11:31, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site https://sei.unifal-mg.edu.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **1305469** e o código CRC **C056A1A3**.

AGRADECIMENTOS

A Deus, por me guiar, iluminar e me dar forças para nunca desistir.

À minha esposa, Ana Rita, por estar ao meu lado todo o tempo, dando-me força e coragem para não desistir, e por toda compreensão que teve durante este processo.

Ao meu orientador, Prof. Dr. Paulo Roberto Rodrigues de Souza, pela disponibilidade, apoio e confiança.

Aos professores, Paulo Henrique e Luiz Eduardo, por prontamente aceitarem o convite para participação nas bancas qualificação e defesa, pelas críticas, apontamentos e sugestões.

Aos professores e colegas da turma do Mestrado Profissional em Administração Pública da Universidade Federal de Alfenas, pelas experiências vividas.

Aos colegas da Universidade Federal de Alfenas, pelo incentivo e apoio.

Aos meus pais, pelo amor, compreensão e apoio incondicional.

O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior – Brasil (CAPES) – Código de Financiamento 001

RESUMO

A segurança da informação na Administração Pública Federal é um tema crítico e de crescente importância devido ao aumento dos incidentes de segurança e vazamento de dados. Neste contexto, a pesquisa se concentra na análise da política de segurança da informação da Universidade Federal de Alfenas (UNIFAL-MG) em relação à legislação pertinente. O presente trabalho teve como objetivo geral analisar a política de segurança da informação da UNIFAL-MG em conformidade com a legislação. Os objetivos específicos incluíram a realização de pesquisa documental sobre políticas de segurança da informação, políticas governamentais e normas legais relacionadas à Administração Pública Federal; verificar a política de segurança da informação da UNIFAL-MG para identificar áreas que precisam de adequação à Política Nacional de Segurança da Informação; e a proposição de ajustes à política da UNIFAL-MG, se necessário. A relevância deste estudo reside na proteção das informações e sistemas de informação utilizados pelos órgãos públicos, que são essenciais para garantir a eficiência e transparência dos serviços prestados à população. O cumprimento das normas é obrigatório, e a conformidade legal é fundamental tanto do ponto de vista legal, administrativo quanto social. À época do desenvolvimento da política de segurança da informação da UNIFAL-MG seguiu um método estruturado, com participação em cursos de capacitação, formação de um Grupo de Trabalho no âmbito do Comitê Gestor de Tecnologia da Informação e estudo minucioso da legislação pertinente. A metodologia adotada nesta pesquisa foi de natureza aplicada, com objetivos exploratórios e descritivos. Ela envolveu a análise das não conformidades e lacunas identificadas, considerando as diretrizes estabelecidas pelas leis, normas e regulamentos aplicáveis, com especial atenção ao Decreto nº 9.637/2018 e se baseou em documentos legais, incluindo atos administrativos e normativas internas da instituição, como portarias, resoluções do Comitê de Governança Digital e do Conselho Universitário. Este trabalho visou contribuir para a adequação da política de segurança da informação da UNIFAL-MG à legislação, garantindo a proteção eficaz dos dados e sistemas de informação na instituição e, consequentemente, a eficiência e transparência dos serviços prestados à comunidade.

Palavras-chave: política de segurança; segurança da informação; conformidade legal.

ABSTRACT

Information security in the Federal Public Administration is a critical and increasingly important topic due to the rising incidents of security breaches and data leaks. In this context, the research focuses on analyzing the information security policy of the Federal University of Alfenas (UNIFAL-MG) in relation to relevant legislation. This study aims to provide a comprehensive examination of UNIFAL-MG's information security policy to ensure compliance with existing legislation. Specific objectives include conducting a literature review on information security policies, government policies, and legal regulations related to the Federal Public Administration. Additionally, the research will involve scrutinizing UNIFAL-MG's information security policy to identify areas requiring alignment with the National Information Security Policy and proposing necessary adjustments to the policy. The significance of this study lies in safeguarding the information and information systems used by public agencies, which are crucial for ensuring efficiency and transparency in services provided to the public. Adherence to these regulations is mandatory, and legal compliance is vital from legal, administrative, and social perspectives. During the development of UNIFAL-MG's information security policy, a structured approach was followed, involving participation in training courses, the formation of a Working Group within the scope of the Information Technology Management Committee, and a thorough examination of pertinent legislation. The research methodology adopted is of an applied nature, with exploratory and descriptive objectives. It includes an analysis of identified non-compliances and gaps, adhering to guidelines stipulated by applicable laws, regulations, and special attention to Decree No. 9,637/2018. The research will also draw on legal documents, such as administrative acts and internal regulations of the institution, including directives and resolutions issued by the Digital Governance Committee and University Council. This study aims to contribute to the alignment of UNIFAL-MG's information security policy with existing legislation, thereby ensuring effective protection of data and information systems within the institution and, consequently, promoting efficiency and transparency in the services provided to the community.

Keywords: security policy; information security; legal compliance.

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE ABREVIATURAS E SIGLAS

ABIN	Agência Brasileira de Inteligência
ABNT	Associação Brasileira de Normas Técnicas
APF	Administração Pública Federal
CAPES	Coordenação de Aperfeiçoamento de Pessoal de Nível Superior
CGD	Comitê de Governança Digital
CGTI	Comitê Gestor de Tecnologia da Informação
CGU	Controladoria-Geral da União
DSIC	Departamento de Segurança da Informação e Comunicação
Efoa	Escola de Farmácia e Odontologia de Alfenas
GSI/PR	Gabinete de Segurança Institucional da Presidência da República
GT	Grupo de Trabalho
IEC	International Electrotechnical Commission
IFES	Instituições Federais de Ensino Superior
ISO	International Organization for Standardization
NBR	Norma Brasileira
NTI	Núcleo de Tecnologia da Informação
PNSI	Política Nacional de Segurança da Informação
PoSIC	Política de Segurança da Informação e Comunicações
PSI	Política de Segurança da Informação
PSIC	Política de Segurança da Informação e Comunicação
PTT	Produto Técnico-Tecnológico
SGSI	Sistema de Gestão de Segurança da Informação
SISBIN	Sistema Brasileiro de Inteligência
SPELL	Scientific Periodicals Electronic Library
TCU	Tribunal de Contas da União
TIC	Tecnologia da Informação e Comunicação
UNIFAL-MG	Universidade Federal de Alfenas

SUMÁRIO

1 INTRODUÇÃO

1.1 RELEVÂNCIA E CONTEXTUALIZAÇÃO DO TEMA

A cada dia se torna mais comum nos depararmos com notícias relacionadas a incidentes de segurança. O volume de dados vazados é cada vez maior e o impacto desse vazamento tem tomado proporções inimagináveis para as organizações.

Uma pesquisa realizada pela Intel Security (Mcafee, 2017) afirmou que os funcionários internos são responsáveis por 43% dos vazamentos de dados corporativos e que 21% quase metade desse percentual, são de maneira acidental.

Para minimizar os impactos sobre os vazamentos de dados, existe a segurança da informação que auxilia na proteção dos dados (Hintzbergen, 2018). A segurança da informação é que ajuda a minimizar os incidentes com dados e que os princípios de confidencialidade, integridade e disponibilidade dos dados sejam seguidos (Fontes, 2017).

Na "era da informação", caracterizada por avanços tecnológicos em sistemas informatizados e transmissão de um significativo volume de dados em redes, a maneira pela qual as sociedades se comunicam sofreu uma revolução. A rapidez e a quantidade de dados informatizados trouxeram impactos para a economia, política e segurança, tanto nacional quanto internacional (Cavelty; Brunner, 2007a). No entanto, esse progresso tecnológico trouxe consigo novos riscos e perdas financeiras. Conforme um relatório da empresa Symantec, em 2017, o Brasil se tornou o segundo país com maior número de casos de crimes cibernéticos, afetando aproximadamente 62 milhões de pessoas e causando um prejuízo de US$ 22 bilhões, ficando atrás apenas da China, que teve prejuízos de US$ 66,3 bilhões. Um dos principais fatores que contribuem para o aumento desses crimes está relacionado à popularidade dos smartphones, cuja quantidade de aparelhos no Brasil ultrapassou 230 milhões, superando até mesmo a população do país (Symantec, 2018).

A área de segurança da informação tem passado por um rápido desenvolvimento, como evidenciado pelo aumento na disponibilidade de normas, padrões e adoção de boas práticas no contexto empresarial. A compreensão de que a segurança da informação é essencial para o êxito e a continuidade das atividades empresariais torna esse assunto uma responsabilidade da

alta administração das organizações. Integra-se aos demais elementos que constituem a Governança Corporativa, como a Governança Financeira, Governança de Relacionamentos, Governança de Ativos e Governança de Gestão de Pessoas, entre outros, a vertente da Governança de Segurança da Informação (Guimarães; Souza Neto; Lyra, 2018).

Na esfera da Administração Pública Federal (APF), a análise dos dados coletados pelo Tribunal de Contas da União (TCU) por meio da pesquisa de Perfil de Governança de Tecnologia da Informação - ciclo 2014, em relação à evolução das práticas concernentes às políticas e obrigações de segurança da informação, constata que, apesar do progresso identificado no período entre 2012 e 2014, a adoção das práticas apresentadas encontra-se significativamente abaixo das expectativas, indicando a presença de lacunas na coordenação e regulamentação da gestão organizacional da segurança da informação, o que expõe a APF a múltiplos riscos (Guimarães; Souza Neto; Lyra, 2018).

Inicialmente, o governo brasileiro abordou a segurança de dados e sistemas por meio do Gabinete de Segurança Institucional da Presidência da República (GSI/PR), em 2001, quando assumiu a coordenação das atividades de segurança da informação. Em seguida, em 2008, o Departamento de Segurança da Informação e Comunicação (DSIC), vinculado ao GSI/PR, foi estabelecido com a responsabilidade de planejar e coordenar a execução das atividades relacionadas à segurança da informação e comunicação no âmbito da administração pública federal. Com a aprovação do Decreto Nº 9.637, em 26 de dezembro de 2018, pelo Congresso Nacional, foi instituída a Política Nacional de Segurança da Informação (PNSI), com a finalidade de guiar a governança da segurança da informação, abrangendo áreas como segurança cibernética, defesa cibernética, segurança física e proteção de dados organizacionais, bem como ações destinadas a garantir a disponibilidade, integridade, confidencialidade e autenticidade da informação. No parágrafo único do Artigo 6º, o Decreto enfatiza que a elaboração da Estratégia Nacional de Segurança da Informação deve envolver a participação ativa da sociedade e dos órgãos públicos, enquanto o item VII do Artigo 12º estabelece que o GSI-PR deve estipular critérios para monitorar e avaliar a execução da PNSI e de seus componentes (Gavião *et al.*, 2022).

De acordo com a Secretaria de Fiscalização de Tecnologia da Informação (Brasil, 2015), no ano de 2014, constatou-se que 51% dos órgãos analisados adotaram integralmente a

Política de Segurança da Informação e Comunicações (PoSIC). Adicionalmente, 15% afirmaram possuir a política, porém a utilizavam de maneira parcial. Isso evidencia que 34% dos órgãos pesquisados não tinham a PoSIC formalmente estabelecida, ou seja, não possuíam o documento que refletisse a visão da Alta Administração sobre o tema, juntamente com as diretrizes para orientar as atividades de segurança da informação conforme as regulamentações do órgão, alinhadas ao Planejamento Estratégico, bem como as atribuições para cada processo ou tarefa realizada no órgão. Apesar de a PoSIC ser o principal guia para a gestão da segurança da informação, é alarmante constatar que apenas 66% dos órgãos participantes da pesquisa (51% integralmente e 15% parcialmente) possuíam uma política formalmente estabelecida como norma de cumprimento obrigatório. Contudo, mesmo com esforços governamentais para incentivar a implementação da PoSIC, algumas Instituições Federais de Ensino Superior (IFES) ainda não têm esse documento devidamente institucionalizado (Brasil, 2016). Essa constatação é apresentada no Levantamento de Governança de Tecnologia da Informação, conduzido pela Secretaria de Fiscalização de Tecnologia da Informação (Brasil, 2015). Segundo Brasil (2016), um total de 98 IFES participaram desse levantamento (Brasil, 2015), mas somente 47 delas declararam ter a PoSIC implementada. Entre essas, apenas 34 instituições a utilizavam integralmente, enquanto outras 13 ainda estavam em processo de implementação parcial. Por outro lado, 51 instituições indicaram que ainda não possuíam uma PoSIC em vigor, situação esta em que a Unifal-MG estava à época, uma vez que sua PoSIC foi estabelecida apenas em 2018, e assim pode-se fomentar o debate, passados 5 anos de sua implementação.

1.2 OBJETIVOS

1.2.1 Objetivo Geral

Analisar a política de segurança da informação da Universidade Federal de Alfenas frente aos requisitos estabelecidos pelo Decreto Nº 9.637/2018.

1.2.2 Objetivos Específicos

a) Realizar pesquisa documental sobre políticas de segurança da informação, das políticas governamentais e normas legais diretamente ligadas à Administração Pública Federal;
b) Fazer um levantamento da Política de Segurança da Informação e Comunicação (PSIC) da Universidade Federal de Alfenas, a fim de identificar os pontos que necessitam de adequação para estar em conformidade a Política Nacional de Segurança da Informação;
c) Propor adequações à PSIC da UNIFAL-MG, caso necessário.

1.3 JUSTIFICATIVA

A segurança da informação na administração pública federal é um tema de grande importância, visto que a proteção das informações e dos sistemas de informação utilizados pelos órgãos públicos é essencial para garantir a eficiência e transparência dos serviços prestados à população. Dessa forma, a pesquisa sobre a segurança da informação na administração pública federal é fundamental tanto do ponto de vista acadêmico, legal, administrativo quanto social.

A importância acadêmica deste tema está na necessidade de incentivar o debate sobre segurança da informação, com destaque especial para a conformidade legal, que é o foco principal deste trabalho. Com o objetivo de identificar na produção científica o nível exploratório sobre o tema, foi realizado em 06 de fevereiro de 2024, uma busca avançada no portal de periódicos da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES) e no portal da Scientific Periodicals Electronic Library (SPELL) utilizando dois termos das palavras chave desta pesquisa, conectados por um operador booleano ‘e’, são eles: ‘segurança da informação’ e ‘conformidade legal’. O uso do operador booleano garante que os resultados contenham ambos os termos, mesmo que possam estar distantes entre si. Para delimitar a busca foram excluídos trabalhos que não estivessem relacionados aos temas: Gestão, Administração Pública ou Tecnologia da Informação

Inicialmente, o resultado da busca apresentou apenas 8 trabalhos únicos nos referidos portais, conforme apresentado Quadro 4 do Apêndice A. No entanto, após filtrar de acordo

com os critérios definidos, apenas um trabalho trata da implantação da política de segurança da informação em um órgão da Administração Pública Federal, porém este não trata especificamente sobre a análise da conformidade legal da política de segurança da informação, tema central desta pesquisa.

Do ponto de vista legal, destaca-se a importância do Decreto nº 9.637/2018, que institui a Política de Segurança da Informação e Comunicações (PNSI) no âmbito da administração pública federal direta, autárquica e fundacional. A PNSI estabelece diretrizes e procedimentos para a proteção das informações e dos sistemas de informação utilizados pelos órgãos públicos, incluindo a implementação de um modelo de gestão de segurança da informação, a definição de procedimentos para o tratamento de incidentes de segurança da informação, a promoção da conscientização e capacitação dos servidores, entre outras medidas.

Quanto a visão administrativa, destaca-se a importância de se avaliar constantemente os riscos de segurança da informação e de se implementar medidas adequadas de proteção. A segurança da informação na administração pública federal brasileira é essencial para proteger informações confidenciais, garantir a continuidade dos serviços públicos e proteger os direitos individuais dos cidadãos. Também pode ajudar a mitigar ameaças cibernéticas, tornando o governo federal mais seguro e resiliente.

Quanto à relevância social, a pesquisa sobre a segurança da informação na administração pública é importante para garantir a transparência e eficiência dos serviços prestados à população, bem como a proteção dos dados pessoais dos cidadãos. O vazamento de informações sensíveis pode gerar danos significativos para a imagem da instituição e para a confiança da população no poder público.

Verifica-se, deste modo, que a pesquisa sobre a segurança da informação na administração pública federal é fundamental para garantir a proteção das informações e dos sistemas de informação utilizados pelos órgãos públicos, bem como para garantir a transparência e eficiência dos serviços prestados à população. Além disso, a implementação de políticas de segurança da informação é capaz de reduzir significativamente o risco de incidentes de segurança e prejuízos financeiros decorrentes desses incidentes.

Demonstra-se ainda, que esta pesquisa sendo desenvolvida de acordo com os objetivos apresentados, traz relevância ao tema, por contribuir em obter êxito no atingimento dos objetivos da PNSI, através da adequação da atual normativa aos requisitos apresentados na legislação vigente.

2 REFERENCIAL TEÓRICO

2.1 INFORMAÇÃO

Claude Shannon estabeleceu as bases matemáticas para a compreensão da informação como uma medida mensurável em sistemas de comunicação (Shannon, 1948). Norbert Wiener expandiu essa perspectiva ao investigar a interconexão entre humanos e máquinas na cibernética (Wiener, 1948). Marshall McLuhan ressaltou a influência dos meios de comunicação na percepção da informação, expressando que "o meio é a mensagem" (Mcluhan, 1964).

Umberto Eco aprofundou a compreensão da informação ao contextualizá-la em termos culturais e semióticos, destacando a comunicação de significados por meio de símbolos e signos (Eco, 1984). Manuel Castells examinou como a informação e a tecnologia estão reformulando as estruturas sociais na sociedade em rede do século XXI (Castells, 1996). Luciano Floridi enriqueceu a discussão contemporânea ao explorar a natureza da informação e da realidade em um mundo digital em constante evolução (Floridi, 2010).

O entendimento de informação no contexto tecnológico engloba a manipulação de dados para extrair significado e utilidade. A dinâmica da informação tecnológica é moldada pela influência dos meios de comunicação, como a internet e dispositivos eletrônicos, sobre a disseminação, processamento e interpretação de dados. Além disso, a digitalização da informação e a rápida troca de dados em redes globais sublinham a crescente importância de entender como a tecnologia molda a interconexão entre informações e sociedade.

No cenário acadêmico brasileiro, pensadores como Ciro Marcondes Filho têm contribuído para a compreensão da informação no âmbito tecnológico. Marcondes Filho enfoca a interseção entre tecnologia, comunicação e sociedade, destacando como a informação é transmitida e interpretada em um ambiente digital em constante evolução (Marcondes Filho, 2009). Sérgio Amadeu da Silveira também enriquece essa discussão ao abordar questões de inclusão digital e privacidade, analisando como a tecnologia influencia a formação de identidade e cidadania em uma sociedade cada vez mais conectada (Silveira, 2007).

No campo dos estudos de comunicação digital e cibercultura, André Lemos se destaca ao explorar as implicações da tecnologia na sociedade contemporânea. Suas análises enfatizam como a tecnologia impacta a cultura, as relações sociais e a construção de significados (Lemos, 2018). Além disso, as contribuições de Luli Radfahrer em design e interação digital oferecem uma visão aprofundada das mudanças na forma como interagimos e compreendemos a informação em um cenário digital (Radfahrer, 2016).

Raquel Recuero, por sua vez, acrescenta uma perspectiva relevante ao explorar as dinâmicas de redes sociais e interações online. Seus estudos detalham como a informação é compartilhada, disseminada e interpretada em plataformas digitais, lançando luz sobre as complexidades das relações virtuais (Recuero, 2014).

Conforme a NBR ISO/IEC 27002:2013, a informação pode manifestar-se em formatos físicos (como cartas e jornais) ou digitais (abrangendo arquivos de computadores, filmes e e-mails). Como mencionado por Fontes (2010), a informação, independentemente do meio, representa um ativo de considerável relevância tanto para indivíduos quanto para organizações, independentemente de seu tamanho ou setor de atuação no mercado. Isso é reforçado por Rios *et al*. (2017), que enfatizam que a dependência constante em informações é essencial para embasar processos decisórios, direcionar planejamento estratégico e operacional, e consequentemente, promover o progresso empresarial.

Dessa forma, como relatado por Dzazali e Hussein (2012), em virtude da alta significância da informação, organizações públicas confrontam o desafio de salvaguardá-la, guiadas pelas normas e diretrizes de segurança da informação provenientes de instâncias governamentais centrais. A intenção é implementar essas orientações nos recursos de tecnologia da informação das entidades subordinadas. A aplicação dessas medidas, em consonância com a NBR ISO 27002:2013, visa evitar que informações sejam indevidamente disponibilizadas ou acessadas por indivíduos não autorizados.

2.2 SEGURANÇA DA INFORMAÇÃO

A segurança da informação representa a salvaguarda de dados, informações e sistemas contra ameaças digitais, com o objetivo de preservar a integridade, confidencialidade e

disponibilidade desses ativos. Esse conceito requer uma abordagem abrangente, que engloba a identificação de riscos potenciais, a implementação de medidas de proteção, o treinamento dos usuários e a resposta a incidentes. Como destacado por Whitman e Mattord (2016), essa abordagem holística envolve ações como avaliação de vulnerabilidades, estabelecimento de políticas de segurança, atualizações regulares de sistemas e a criação de um plano eficaz de gestão de incidentes.

A implementação efetiva da segurança da informação também requer conscientização e educação contínuas dos usuários, a fim de reconhecer ameaças e adotar práticas seguras. Dhillon (2007) ressalta a importância de uma cultura organizacional de segurança, que envolva desde a alta administração até os colaboradores em todos os níveis. Essa cultura é essencial para manter os ativos digitais protegidos em um cenário onde ameaças cibernéticas estão em constante evolução. Em síntese, o conceito de segurança da informação demanda um esforço colaborativo que vai além de tecnologias isoladas, integrando políticas, processos e pessoas para mitigar riscos e proteger informações vitais.

A segurança da informação, como definida anteriormente, ganha ainda mais profundidade quando observada à luz das contribuições de pesquisadores brasileiros. No contexto nacional, Fagundes (2015) tem enfatizado a necessidade de abordar a segurança da informação como um processo contínuo de gerenciamento de riscos, destacando a importância de avaliar ameaças específicas enfrentadas pelo Brasil, como ciberataques direcionados a setores críticos.

Ademais, as perspectivas de Eller e Rust (2019) acrescentam uma dimensão humana crucial à equação da segurança da informação. Eles destacam a importância de educar os usuários para que compreendam não apenas as ameaças técnicas, mas também os impactos comportamentais e sociais das ações de segurança. Essa abordagem coaduna com a ideia de uma cultura de segurança, mencionada anteriormente.

A pesquisa de Sousa Júnior e Rocha (2020) destaca os desafios únicos enfrentados em um país com diversidades culturais e econômicas. Eles enfatizam a importância de adaptar estratégias de segurança da informação para atender às necessidades regionais e sociais, levando em conta fatores como acesso à tecnologia e níveis de conscientização.

No que se refere à confidencialidade, como ressaltado por Fontes (2010), a informação deve ser acessada somente por aqueles autorizados a fazê-lo. Goodrich e Tamassia (2013) também destacam a importância de garantir a confidencialidade, evitando qualquer divulgação não autorizada. Nesse contexto, a NBR ISO 27001:2013 conclui que a confidencialidade implica que a informação não esteja disponível ou acessível a indivíduos e entidades não autorizadas.

Diversas abordagens têm sido desenvolvidas para assegurar a confidencialidade, incluindo criptografia, controle de acesso, autenticação e segurança física, como apontado por Fontes (2010) e Goodrich e Tamassia (2013).

A integridade, por sua vez, envolve preservar a exatidão e completude da informação, conforme definido pela NBR ISO 27002:2013. Fontes (2010) reforça que a integridade requer que a informação seja alterada apenas por aqueles autorizados, garantindo sua correção e veracidade. Goodrich e Tamassia (2013) mencionam ferramentas como cópias de segurança que são projetadas para sustentar a integridade da informação.

A disponibilidade, definida pela NBR ISO 27002:2013, envolve assegurar que a informação esteja acessível e funcional a qualquer momento para entidades autorizadas. Essa característica auxilia a organização a cumprir seus objetivos e missões, como indicado por Fontes (2010). Goodrich e Tamassia (2013) também enfatizam que a redundância computacional, como dispositivos de backup, contribui para garantir a disponibilidade.

A autenticidade diz respeito à validade de ações, políticas e permissões originadas por indivíduos ou sistemas, de acordo com Goodrich e Tamassia (2013). Esse atributo é frequentemente garantido por meio de assinaturas digitais. Conforme a NBR ISO 27002:2013, confiabilidade é a capacidade de um sistema de informação tolerar falhas. Por outro lado, Fontes (2010) explica que o não-repúdio refere-se a atos legítimos que não podem ser negados por sua autoria, o que também pode ser garantido por assinaturas digitais.

2.3 NORMAS DE SEGURANÇA DA INFORMAÇÃO

As normas desempenham um papel crucial na formulação de um plano de segurança da informação, como observado por Karabacak e Sogukpinar (2006). Essas diretrizes

proporcionam uma abordagem sistemática para a gestão, visando à adoção das melhores práticas em termos de controles, avaliação do nível de risco aceitável e implementação das medidas adequadas para resguardar a confidencialidade, integridade e disponibilidade das informações, conforme destacado por Dey (2007).

A International Organization for Standardization (ISO), como organização global, é responsável por desenvolver e disseminar normas internacionalmente reconhecidas em diversas áreas, abrangendo segurança, qualidade e meio ambiente. Em paralelo, a International Electrotechnical Commission (IEC) concentra-se em normas voltadas para equipamentos elétricos e eletrônicos, frequentemente colaborando com a ISO na elaboração de padrões conjuntos.

No Brasil, a Associação Brasileira de Normas Técnicas (ABNT) desempenha um papel central na criação e adaptação de normas, resultando nas conhecidas Normas Brasileiras (NBR). Essas normas, embora tenham sua origem na internacionalização de padrões, são adaptadas para atender às particularidades e necessidades específicas do Brasil.

A interconexão entre essas normas é evidente quando normas ISO são incorporadas ou adaptadas como NBR pela ABNT. Isso demonstra a importância de uma abordagem globalizada, considerando padrões internacionais na formulação de normas nacionais. Essa relação facilita a integração do Brasil aos padrões globais, promovendo a qualidade, segurança e interoperabilidade em diversos setores.

É relevante mencionar que a citação indireta de normas deve seguir as diretrizes do padrão ABNT. As referências bibliográficas adequadas para as normas ISO e NBR, por exemplo, seguiriam a estrutura específica do estilo ABNT, incluindo título, número da norma e ano de publicação. Cada norma citada seria referenciada de acordo com as normas específicas do padrão ABNT.

A série 27000 de normas da ISO/IEC concentra-se nos requisitos, controles de segurança e orientação para a implementação de um Sistema de Gestão de Segurança da Informação (SGSI) na organização, como salientado por McGee *et al*. (2007).

2.3.1 Norma ISO/IEC 27001

A norma ISO 27001 teve origem com base na norma britânica BS7799 e na ISO/IEC 17799, como mencionado por Fenz *et al*. (2007). Seu propósito é oferecer um modelo para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar um Sistema de Gestão de Segurança da Informação (SGSI), de acordo com a NBR ISO/IEC 27001:2013. Essa norma representa o primeiro padrão da família ISO/IEC relacionado à segurança da informação (Fenz *et al*., 2007).

Essa norma é empregada globalmente por organizações comerciais e governamentais como fundamento para gerir a política e implementar a segurança da informação, conforme relatado anteriormente (Humphreys, 2008). A abrangência de sua utilização se estende a empresas de pequeno, médio e grande porte. De fato, o padrão foi concebido com flexibilidade para acomodar qualquer natureza de organização (Humphreys, 2008).

2.3.2 Norma ISO/IEC 27002

A ISO 27002 estabelece um conjunto de diretrizes representando as melhores práticas em segurança da informação, conforme indicado por Dey (2007). Essa norma compila os objetivos de controle e oferece uma gama de controles de segurança específicos, conforme evidenciado por Sahibudin *et al*. (2008). Os objetivos de controle e os controles mencionados na norma são desenvolvidos com o propósito de atender às necessidades identificadas por meio da análise e avaliação de riscos. De fato, a ISO 27002 serve como um guia pragmático para estabelecer os procedimentos de segurança da informação da organização, bem como eficazes práticas de gestão da segurança, contribuindo para fortalecer a confiança nas interações entre organizações (ABNT NBR ISO/IEC 27002).

Na norma ISO/IEC 27002:2013, são destacadas 39 categorias de controles de segurança da informação distribuídas em suas 14 seções, fornecendo diretrizes detalhadas para a implementação de práticas seguras. Essas categorias representam áreas específicas de enfoque que visam salvaguardar os ativos de informação de uma organização contra uma ampla gama de ameaças.

Dentro da seção 5, que trata da "Organização da Segurança da Informação", destaca-se a categoria 2, relacionada à "Governança da Segurança da Informação", definindo os princípios e estruturas que orientam a implementação eficaz das políticas de segurança.

A Seção 6, "Gestão de Ativos", abrange a categoria 7, que trata do "Inventário de Ativos". Este controle direciona a organização a estabelecer e manter um inventário abrangente de ativos de informação, essencial para uma gestão eficiente da segurança.

A Seção 7, "Segurança em Recursos Humanos", inclui a categoria 9, que versa sobre o "Processo de Recrutamento e Contração". Esse controle visa assegurar que os processos de seleção de pessoal integrem critérios de segurança desde o início.

No contexto da "Gestão de Acessos" (Seção 8), a categoria 14 destaca o "Responsabilidades do Usuário", delineando claramente as obrigações que os usuários têm em relação à segurança da informação.

A Seção 9, "Segurança Física e do Ambiente", enfoca, entre outras categorias, a 16, relacionada à "Segurança Contra Ameaças Externas". Esta categoria estabelece diretrizes para proteger os ativos de informação contra ameaças físicas externas.

Operações de segurança são abordadas na Seção 10, onde a categoria 19, "Gestão de Incidentes e Melhorias", destaca a importância de processos eficazes para identificação, resposta e aprendizado contínuo a partir de incidentes de segurança.

A Seção 11, "Controle de Comunicações e Gerenciamento de Redes", inclui a categoria 25, "Mídia de Comunicação", detalhando as práticas seguras para o gerenciamento de mídia utilizada para a comunicação de informações sensíveis.

No âmbito de "Aquisição, Desenvolvimento e Manutenção de Sistemas de Informação" (Seção 12), a categoria 29, "Testes de Sistemas", enfoca as melhores práticas para avaliação de segurança durante o desenvolvimento e testes de sistemas de informação.

A gestão de incidentes de segurança é explorada na Seção 13, onde a categoria 32, "Procedimentos de Gestão de Incidentes", detalha os passos apropriados para identificação, registro e resposta a incidentes.

Na Seção 14, que trata de "Aspectos de Segurança na Gestão da Continuidade do Negócio", a categoria 35, "Implementação da Solução de Continuidade do Negócio", orienta

sobre a implementação prática de planos de continuidade para garantir a resiliência da organização. (ABNT NBR ISO/IEC 27002).

2.4 LEGISLAÇÃO EM SEGURANÇA DA INFORMAÇÃO NA ADMINISTRAÇÃO PÚBLICA FEDERAL

O desenvolvimento de diversos dispositivos legais, incluindo normas, decretos, cartilhas e instruções normativas, que tratam da aplicação da segurança da informação na esfera federal tem seu cumprimento obrigatório (Souza, 2017). Essa abordagem é corroborada e complementada por Araújo (2012). No Brasil não se restringe a uma única Lei para tratar da segurança da informação; ao invés disso, várias normas presentes em sua legislação podem ser implementadas em relação ao tema.

A Lei nº 8.159, datada de 8 de janeiro de 1991, representa o primeiro marco legal no Brasil a abordar a gestão documental e a proteção de documentos de arquivo o que pode ser considerado um tratamento da informação. Conforme estabelecido pelo Artigo 1º da referida lei, é incumbência do Poder Público a responsabilidade pela gestão documental e pela salvaguarda especial dos documentos de arquivo. Esta legislação desempenha um papel essencial ao atuar como um instrumento de apoio à administração pública, à cultura e ao desenvolvimento científico, além de atribuir aos documentos de arquivo o status de elementos probatórios e informativos de relevância (Brasil, 1991).

A legislação concernente à inteligência no Brasil que está ligada à segurança da informação na administração pública federal é fundamentada pela Lei nº 9.883, datada de 7 de dezembro de 1999, que estabelece a criação do Sistema Brasileiro de Inteligência (SISBIN) e a instituição da Agência Brasileira de Inteligência (ABIN) (Brasil, 1999). A mencionada lei define o escopo e os procedimentos operacionais para o desenvolvimento e a coordenação das atividades de inteligência no país. Com o intuito de aprimorar e adequar a estrutura de inteligência do governo, o Decreto nº 11.426, de 1º de março de 2023, entra em vigor, visando à integração da Agência Brasileira de Inteligência à Casa Civil da Presidência da República. Esse decreto reflete uma atualização na estrutura organizacional, alinhando as atividades de inteligência com as diretrizes e as necessidades da administração pública (Brasil, 2023),

proporcionando maior eficiência e coordenação nas ações de segurança e proteção dos interesses nacionais.

O panorama legislativo brasileiro aborda seu primeiro avanço no que tange à uma política de segurança da informação, exemplificado pelo Decreto nº 3.505, de 13 de junho de 2000. Esse decreto estabelece a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal (Brasil, 2000), delineando diretrizes e parâmetros para proteger e gerenciar informações sensíveis e estratégicas do governo. Através dessa medida legal, busca-se criar um arcabouço normativo com o objetivo de garantir a confidencialidade, integridade e disponibilidade das informações, além de promover conscientização e responsabilidade na gestão da informação. Este decreto desempenha um papel essencial ao estabelecer a estrutura normativa para a gestão da segurança da informação no âmbito governamental, orientando a implementação de políticas, procedimentos e práticas para minimizar riscos cibernéticos e impactos de incidentes de segurança. Além disso, ele destaca a importância de considerar a segurança da informação como parte integrante da administração pública, seguindo diretrizes internacionais e padrões de boas práticas de segurança cibernética.

O Decreto nº 5.772, de 8 de maio de 2006, foi responsável por aprovar a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão e das Gratificações de Exercício em Cargo de Confiança do Gabinete de Segurança Institucional da Presidência da República. De acordo com esse decreto, o Artigo 8º atribui ao Departamento de Segurança da Informação e Comunicações as competências relacionadas à área de segurança da informação (Brasil, 2006).

À medida que o contexto evolui, com o Decreto nº 11.331, de 1º de janeiro de 2023, em seu Artigo 19, atualiza as competências do Departamento de Segurança da Informação e Cibernética, delineando responsabilidades mais amplas e contemporâneas relacionadas à cibersegurança (Brasil, 2023). Ao atualizar a estrutura organizacional e as responsabilidades dos órgãos governamentais, adaptando-se aos desafios crescentes no ambiente digital, abrangendo áreas cruciais como a segurança cibernética, a proteção de dados e a gestão de riscos associados à tecnologia da informação.

Além das regulamentações por meio de decretos, a legislação brasileira também contempla a segurança da informação por meio de instruções normativas. A Instrução Normativa GSI nº 1, de 13 de junho de 2008, desempenha um papel fundamental ao estabelecer diretrizes específicas para a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, tanto direta quanto indireta (Brasil, 2008). Por meio dessa instrução normativa, são definidos os parâmetros para a proteção, classificação, compartilhamento e armazenamento de informações sensíveis. Essa legislação, ao delinear os procedimentos e responsabilidades relacionados à gestão da segurança da informação no contexto governamental, busca assegurar que as informações estratégicas e sigilosas do governo sejam adequadamente gerenciadas, visando à preservação da confidencialidade, integridade e disponibilidade dos dados em um cenário cada vez mais digital e interconectado.

O arcabouço legal brasileiro relacionado à segurança da informação apresenta também o Decreto nº 7.845, de 14 de novembro de 2012. Este decreto exerce um papel crucial ao regulamentar os procedimentos concernentes ao credenciamento de segurança e ao tratamento de informações classificadas em todos os níveis de sigilo. Além disso, o decreto estabelece as diretrizes que permeiam o funcionamento do Núcleo de Segurança e Credenciamento, uma instância fundamental para a implementação eficiente das políticas de segurança em âmbito governamental. A regulamentação proporcionada por este decreto busca garantir a proteção adequada das informações sensíveis e sigilosas, traçando critérios, requisitos e processos para o manuseio, compartilhamento e armazenamento seguro dessas informações, em linha com a busca contínua por salvaguardar a integridade, confidencialidade e disponibilidade dos dados governamentais (Brasil, 2012).

O cenário da segurança da informação no Brasil tem sido moldado e atualizado por meio de decretos específicos, com o objetivo de fortalecer as diretrizes e a governança relacionadas à proteção de dados e informações. Nesse contexto, destaca-se o Decreto nº 9.637, datado de 26 de dezembro de 2018, que assume um papel central ao instituir a Política Nacional de Segurança da Informação. Através desse decreto, é estabelecida a estrutura básica para a gestão da segurança da informação em âmbito governamental (Brasil, 2018). A evolução desse arcabouço legal se dá com as alterações previstas no Decreto nº 10.641, datado de 2 de março de 2021, que introduz alterações ao Decreto nº 9.637/2018. Esse novo decreto,

reforça o compromisso do governo em adaptar-se às dinâmicas dentro da administração pública ao dispor sobre a governança da segurança da informação (Brasil, 2021).

Em consonância com o compromisso de aprimorar a governança da segurança da informação no âmbito governamental, destaca-se o Decreto nº 9.832, datado de 12 de junho de 2019, como mais um passo significativo na contínua evolução do regramento. Este decreto, ao alterar o Decreto nº 9.637/2018 e o Decreto nº 7.845/2012, estabelece um novo marco ao dispor sobre a composição, atribuições e funcionamento do Comitê Gestor da Segurança da Informação. O mencionado comitê assume um papel estratégico ao orientar, coordenar e supervisionar as atividades relacionadas à segurança da informação no âmbito governamental (Brasil, 2019).

O Decreto nº 10.222, em 5 de fevereiro de 2020, que ratifica a Aprovação da Estratégia Nacional de Segurança Cibernética. Nesse contexto, o objetivo desta estratégia é criar um regramento abrangente e orientador para o desenvolvimento de ações e políticas que visam proteger os sistemas de informações e infraestruturas críticas do país. Ela delineia princípios, diretrizes e objetivos que nortearão as iniciativas voltadas para a segurança cibernética, assegurando a proteção da soberania nacional, dos interesses públicos e da confiança na ambiente cibernético. O Decreto nº 10.222 representa um marco importante no fortalecimento das capacidades do Brasil em enfrentar ameaças cibernéticas, bem como estabelece uma base para a cooperação e coordenação interinstitucional para responder efetivamente aos desafios da era digital (Brasil, 2020).

A Instrução Normativa GSI/PR nº 3, datada de 28 de maio de 2021, emerge como uma peça fundamental no enquadramento da gestão de segurança da informação no âmbito da administração pública federal brasileira. Essa normativa desenha um panorama abrangente dos processos que envolvem a segurança da informação, estabelecendo diretrizes, padrões e procedimentos que devem ser adotados pelos órgãos e entidades públicas. A normativa reconhece a importância de salvaguardar ativos de informação e assegurar sua confidencialidade, integridade e disponibilidade, além de definir responsabilidades, papéis e requisitos para uma abordagem sistêmica e coordenada (Brasil, 2021). Ao detalhar os processos relacionados à gestão de segurança da informação, a Instrução Normativa GSI/PR nº

3 tem o propósito de alinhar as práticas e orientações para promover um ambiente seguro e resiliente nos órgãos e entidades da administração pública federal.

O Decreto nº 10.748, datado de 16 de julho de 2021, emerge como um marco relevante ao instituir a Rede Federal de Gestão de Incidentes Cibernéticos. Esse decreto traça um novo panorama no cenário da segurança cibernética, ao estabelecer uma estrutura abrangente e coordenada para lidar com incidentes cibernéticos no âmbito da administração pública federal brasileira (Brasil, 2021). A Rede Federal de Gestão de Incidentes Cibernéticos visa à identificação, ao tratamento e à resposta efetiva a incidentes cibernéticos que possam comprometer a segurança das informações e a operação dos sistemas governamentais. Dessa forma, o decreto consolida a capacidade de resiliência e proteção do governo contra ameaças cibernéticas, destacando a importância de uma abordagem cooperativa e colaborativa entre os órgãos e entidades da administração pública federal para garantir a integridade e a segurança das informações no ambiente digital.

No âmbito da evolução contínua das medidas voltadas para a segurança da informação, a Portaria GSI/PR nº 93, datada de 18 de outubro de 2021, apresenta-se como um passo significativo ao aprovar o glossário de segurança da informação. Essa iniciativa consolida a preocupação em estabelecer um referencial claro e padronizado para os termos e conceitos relacionados à segurança da informação, proporcionando uma compreensão uniforme e precisa desses elementos essenciais no contexto governamental (Brasil, 2021).

A evolução cronológica da legislação em Segurança da Informação no Brasil pode ser sintetizada de acordo do Quadro 1.

Quadro 1 – Cronologia da Legislação em Segurança da Informação no Brasil

(continua)

Legislação	Descrição
LEI No 8.159, DE 8 DE JANEIRO DE 1991	Dispõe sobre a política nacional de arquivos públicos e privados e dá outras providências.
LEI No 9.883, DE 7 DE DEZEMBRO DE 1999 DECRETO Nº 11.426, DE 1º DE MARÇO DE 2023	Institui o Sistema Brasileiro de Inteligência, cria a Agência Brasileira de Inteligência - ABIN, e dá outras providências. Integra a Agência Brasileira de Inteligência à Casa Civil da Presidência da República.
DECRETO No 3.505, DE 13 DE JUNHO DE 2000	Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal.

Quadro 1 – Cronologia da Legislação em Segurança da Informação no Brasil

(conclusão)

Legislação	Descrição
DECRETO Nº 5.772, DE 8 DE MAIO DE 2006 DECRETO Nº 11.331, DE 1º DE JANEIRO DE 2023	Aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão e das Gratificações de Exercício em Cargo de Confiança do Gabinete de Segurança Institucional da Presidência da República, tratando da organização e competências do Departamento de Segurança da Informação e Comunicações.
INSTRUÇÃO NORMATIVA GSI No 1, DE 13 DE JUNHO DE 2008	Disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, e dá outras providências.
DECRETO Nº 7.845, DE 14 DE NOVEMBRO DE 2012	Regulamenta procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo, e dispõe sobre o Núcleo de Segurança e Credenciamento.
DECRETO Nº 9.637, DE 26 DE DEZEMBRO DE 2018 DECRETO Nº 10.641, DE 2 DE MARÇO DE 2021	Institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação e dispõe sobre a governança da segurança da informação.
DECRETO Nº 9.832, DE 12 DE JUNHO DE 2019	Dispõe sobre o Comitê Gestor da Segurança da Informação.
DECRETO Nº 10.222, DE 5 DE FEVEREIRO DE 2020	Aprova a Estratégia Nacional de Segurança Cibernética.
INSTRUÇÃO NORMATIVA GSI/PR Nº 3, DE 28 DE MAIO DE 2021	Dispõe sobre os processos relacionados à gestão de segurança da informação nos órgãos e nas entidades da administração pública federal.
DECRETO Nº 10.748, DE 16 DE JULHO DE 2021	Institui a Rede Federal de Gestão de Incidentes Cibernéticos.
PORTARIA GSI/PR Nº 93, DE 18 DE OUTUBRO DE 2021	Aprova o glossário de segurança da informação.

Fonte: Elaborado pelo autor (2023).

2.5 POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

A política representa uma regra geral dentro do contexto organizacional, estabelecendo diretrizes e limites para a busca dos objetivos e metas institucionais. Nesse contexto, a política de segurança da informação (PSI) é um documento que delineia as diretrizes e controles de segurança, visando proteger os dados e informações da organização (Rios *et al.*, 2017; Albuquerque Jr.; Santos, 2014).

No campo da segurança da informação, a NBR ISO 27002:2013 estabelece que a PSI deve ser aprovada pela Alta Direção e disseminada amplamente, assegurando que todos os colaboradores e partes interessadas relevantes compreendam suas disposições (Weidman; Grossklags, 2018). A PSI, por sua vez, precisa ser clara e acessível, orientando as práticas de segurança da informação em conformidade com os requisitos de negócio, regulamentações e a missão da organização (ABNT, 2013; Monteiro, 2009).

A PSI, como prática recomendada, orienta as ações de segurança da informação e sua integração nos processos organizacionais. Contudo, é um documento dinâmico, requerendo revisões periódicas para manter sua relevância, adequação e eficácia diante das mudanças (Fontes, 2010). Segundo Martins e Eloff (2001), a PSI molda o comportamento dos funcionários, delineando o que é aceitável e as medidas de segurança para salvaguardar os bens físicos e dados tecnológicos. A ausência desse documento, conforme a NBR ISO 27002:2013, resulta na falta de orientações para as partes interessadas em situações de risco de segurança da informação.

No entanto, além da PSI, a conscientização e educação das partes interessadas são cruciais para implementar ações de segurança nos processos organizacionais (Weidman; Grossklags, 2018). Conforme a NBR ISO 27002:2013, a PSI deve incluir a definição de segurança da informação, o comprometimento da direção, estrutura de controle e análise de risco, além de definir responsabilidades na gestão da segurança (ABNT, 2013).

2.5.1 Elaboração da Política de Segurança da Informação na Unifal-MG

A criação da Política de Segurança da Informação e Comunicação (PSIC) na Universidade Federal de Alfenas (UNIFAL-MG) representou um importante processo na instituição. Esse esforço foi desencadeado em resposta à Constatação 1.13.1 do Relatório Nº 201203446 da Controladoria-Geral da União (CGU), que apontou a ausência de formalização da PSI na instituição. Para abordar essa carência, uma ampla fundamentação legal foi invocada, incluindo dispositivos como o Decreto 3.505/2000, que instituiu a Política de Segurança da Informação na Administração Pública Federal, delineando seus princípios e diretrizes. Além disso, o Decreto 7.845/2012 desempenhou um papel crucial, estabelecendo

diretrizes para a classificação da informação no âmbito do Poder Executivo, contribuindo assim para a proteção de dados sensíveis.

Outros instrumentos legais também se fizeram presentes, como a IN 04/2010 MPOG/SLTI, que exigiu normas de segurança para a contratação de fornecedores e serviços, reforçando a importância da segurança da informação em todos os aspectos das operações da UNIFAL-MG. O Acórdão TCU 1.603/2008-Plenário, por sua vez, estabeleceu princípios fundamentais para a gestão de Segurança da Informação e Comunicações (SIC) na Administração Pública Federal, orientando a instituição no caminho da conformidade legal e das melhores práticas. Ademais, a IN 01/2008 GSI desempenhou um papel disciplinador crucial na gestão de SIC na Administração Federal de Pessoal.

A legislação também evocou a Lei nº 12.527/2011, conhecida como Lei de Acesso à Informação, que trouxe consigo normas e regulamentos essenciais para o acesso à informação e a garantia da transparência. Por fim, o Marco Civil da Internet, que estabeleceu princípios, garantias, direitos e deveres para o uso da Internet no Brasil, complementou o quadro regulatório à época.

O processo de criação da PSIC na UNIFAL-MG seguiu um método estruturado, começando com a participação em um curso oferecido pela Rede Nacional de Ensino e Pesquisa (RNP), que capacitou os envolvidos com conhecimento sólido sobre segurança da informação. Em seguida, um Grupo de Trabalho (GT) foi constituído no âmbito do Comitê Gestor de Tecnologia da Informação (CGTI) para coordenar todo o processo. Esse GT realizou um estudo minucioso da legislação pertinente, assegurando a conformidade com os dispositivos legais que nortearam o projeto. Também conduziu um estudo comparativo das políticas de segurança de outras instituições de ensino, para se inspirar nas melhores práticas existentes.

Reuniões regulares do GT foram realizadas para avançar na elaboração da PSIC, enquanto discussões abertas com a comunidade acadêmica e administrativa permitiram a coleta de contribuições valiosas e esclarecimento de dúvidas. Após essa fase de consulta e discussão, o projeto de PSIC foi submetido ao CGTI, onde passou por análise detalhada, discussão intensiva e, finalmente, foi aprovado por unanimidade. Finalmente, a Resolução Consuni nº 08/18, datada de 02 de abril de 2018, formalizou a PSIC, dando início a uma nova

etapa na construção e fortalecimento da cultura de segurança da informação na UNIFAL-MG, atendendo de modo a se adaptar e cumprir as exigências legais e as melhores práticas em segurança da informação.

3 METODOLOGIA

3.1 OBJETO DE ESTUDO

A Universidade Federal de Alfenas (UNIFAL-MG) é uma instituição pública de ensino superior localizada na cidade de Alfenas, no estado de Minas Gerais, Brasil. A Instituição iniciou suas atividades como Escola de Farmácia e Odontologia de Alfenas (Efoa) foi fundada no dia 3 de abril de 1914. No ano de 2001, passou a ser Centro Universitário Federal (Efoa/Ceufe), aumentando o número de cursos de graduação; oferecendo cursos à distância e cursos de especialização. Em 2005, a Efoa/Ceufe foi transformada em Universidade Federal de Alfenas UNIFAL-MG e em 2009 foram iniciadas as atividades nos *campi* fora de sede nas cidades de Poços de Caldas e Varginha. A Instituição tem como missão promover a formação plena do ser humano, gerando, sistematizando e difundindo o conhecimento, comprometendo-se com a excelência no ensino, na pesquisa e na extensão, com base nos princípios da reflexão crítica, da ética, da liberdade de expressão, da solidariedade, da justiça, da inclusão social, da democracia, da inovação e da sustentabilidade. Sua visão é ser reconhecida, nacional e internacionalmente, por sua excelência acadêmica, científica, cultural e social, comprometida com o desenvolvimento humano, social, econômico e ambiental do país (UNIFAL-MG, 2021).

O Núcleo de Tecnologia da Informação (NTI) da UNIFAL-MG é uma unidade responsável pela gestão, desenvolvimento e manutenção dos recursos tecnológicos utilizados pela universidade. O NTI desempenha um papel crucial na integração da tecnologia da informação no ambiente acadêmico, administrativo e de pesquisa, proporcionando suporte técnico, infraestrutura e sistemas que apoiam as atividades universitárias.

O NTI da UNIFAL-MG busca manter a infraestrutura tecnológica atualizada, promover a segurança da informação e facilitar o acesso às ferramentas digitais necessárias para o desenvolvimento das atividades acadêmicas. Além disso, o NTI está envolvido na promoção de cursos e treinamentos que visam capacitar a comunidade universitária no uso eficiente das tecnologias disponíveis.

O Comitê de Governança Digital (CGD) da UNIFAL-MG é uma instância responsável por coordenar e orientar a utilização estratégica da tecnologia da informação e comunicação (TIC) na universidade. O CGD tem como objetivo principal alinhar as iniciativas tecnológicas com os objetivos estratégicos da instituição, garantindo a eficiência, transparência, segurança e conformidade nas práticas relacionadas à governança digital (UNIFAL-MG, 2023).

O CGD é composto por representantes da administração da UNIFAL-MG e suas responsabilidades incluem o estabelecimento de políticas de segurança da informação, a definição de diretrizes para aquisição e implantação de sistemas, a avaliação de riscos relacionados à TIC e a proposição de ações que promovam a inovação tecnológica alinhada com as demandas da universidade.

Em conjunto, a Universidade Federal de Alfenas (UNIFAL-MG), seu Núcleo de Tecnologia da Informação (NTI) e o Comitê de Governança Digital (CGD) representam uma estrutura dentro do ambiente acadêmico moderno e comprometido com a excelência educacional, a pesquisa avançada e a aplicação eficiente das tecnologias da informação para o benefício de toda a comunidade acadêmica.

3.2 ENQUADRAMENTO METODOLÓGICO

Este trabalho adotou uma tipologia de pesquisa baseada nas orientações de Prodanov e Freitas (2013). A pesquisa será de natureza aplicada, com objetivos exploratórios e descritivos, sendo que a pesquisa aplicada busca gerar conhecimento prático que possa ser aplicado para resolver problemas reais ou melhorar práticas existentes. Além disso, a abordagem exploratória permite uma investigação mais ampla e aprofundada sobre o tema complexo das políticas de segurança da informação de modo a permitir examinar questões como conformidade legal, melhores práticas e requisitos regulatórios. A abordagem descritiva da pesquisa é adequada para fornecer uma visão detalhada das práticas atuais relacionadas à segurança da informação na UNIFAL-MG, incluindo a análise da política existente e a identificação de áreas de não conformidade e lacunas, buscando investigar a conformidade da política de segurança da informação da Universidade Federal de Alfenas em relação à Política Nacional de Segurança da Informação (PNSI) condensado de acordo com Quadro 2.

Quadro 2 – Tipologia de pesquisa adotada

<table>
<tr><th colspan="4">Enquadramento Metodológico</th></tr>
<tr><th>Quanto à Natureza</th><th>Quanto à Forma de Abordagem do Problema</th><th>Quanto aos Fins da Pesquisa</th><th>Quanto aos Procedimentos</th></tr>
<tr><td rowspan="2">Aplicada</td><td rowspan="2">Qualitativa</td><td>Exploratório</td><td rowspan="2">Bibliográfica e documental</td></tr>
<tr><td>Descritivo</td></tr>
</table>

Fonte: Elaborado pelo autor (2023), baseado em Prodanov; Freitas (2013).

Conforme Marconi e Lakatos (2017), a escolha da abordagem qualitativa permite obter uma compreensão abrangente e aprofundada, ainda por tratar-se da análise da conformidade legal da política de segurança da informação, incorporando tanto aspectos subjetivos quanto objetivos. Isso é fundamental para uma análise completa e robusta, considerando a complexidade e a diversidade de elementos envolvidos na conformidade legal.

A abordagem qualitativa foi utilizada na coleta dados e informações sobre a política de segurança da informação vigente na instituição em estudo e baseia-se em fundamentações teóricas relevantes. Conforme Ludke e André (2013), a abordagem qualitativa permite explorar percepções, opiniões e experiências dos envolvidos, possibilitando uma compreensão mais profunda do contexto e das nuances da conformidade legal e também proporcionando insights valiosos sobre a relação entre a política de segurança da informação da instituição e os requisitos legais identificados.

3.3 COLETA DE DADOS

A abordagem da pesquisa documental, conforme delineada por Gil (2002), é altamente pertinente ao tratar do uso de legislações provenientes de diversas fontes. Ao realizar uma pesquisa documental sobre legislações, é possível empregar os princípios propostos por Gil para identificar, selecionar e analisar os documentos legais relevantes. A identificação das fontes pode envolver a busca em bases de dados jurídicos, repositórios governamentais e acervos legais. A seleção criteriosa de leis, regulamentos e documentos normativos se alinha à orientação de Gil para escolher documentos que melhor se ajustem ao escopo da pesquisa e para tanto pode-se considerar neste escopo os documentos que se enquadram na definição de "controles internos da gestão" disposto na Instrução Normativa Conjunta MP/CGU nº 01/16, que dispõe sobre controles internos, gestão de riscos e governança no âmbito do Poder Executivo Federal, inciso V do Art. 2º:

> V – controles internos da gestão: conjunto de regras, procedimentos, diretrizes, protocolos, rotinas de sistemas informatizados, conferências e trâmites de documentos e informações, entre outros, operacionalizados de forma integrada pela direção e pelo corpo de servidores das organizações, destinados a enfrentar os riscos e fornecer segurança razoável de que, na consecução da missão da entidade, os seguintes objetivos gerais serão alcançados: a) execução ordenada, ética, econômica, eficiente e eficaz das operações; b) cumprimento das obrigações de accountability; c) cumprimento das leis e regulamentos aplicáveis; e d) salvaguarda dos recursos para evitar perdas, mau uso e danos. O estabelecimento de controles internos no âmbito da gestão pública visa essencialmente aumentar a probabilidade de que os objetivos e metas estabelecidos sejam alcançados, de forma eficaz, eficiente, efetiva e econômica; (Brasil, 2016, p. 2).

A partir do entendimento apresentado, os documentos considerados na análise foram os atos administrativos e normativas internas da instituição tais como, e não se limitando a, portarias e as resoluções do Comitê de Governança digital e de Conselho Universitário.

A análise aprofundada de diversas legislações é fundamental para identificar padrões, tendências e abordagens regulatórias em diferentes contextos legais. Isso pode envolver a comparação de leis entre diferentes jurisdições, a evolução temporal das regulamentações e a identificação de lacunas ou inconsistências nas legislações analisadas. A triangulação de múltiplas fontes legais, sugerida por Gil, auxilia na validação das conclusões, permitindo que o pesquisador identifique convergências ou divergências nos princípios legais adotados.

A abordagem da pesquisa documental descrita por Gil (2002) pode ser relacionada aos pensamentos de Prodanov e Freitas (2013) no contexto de pesquisa e metodologia. Autores como Prodanov e Freitas costumam enfatizar a importância da escolha adequada dos métodos de pesquisa de acordo com os objetivos do estudo e a natureza do objeto de pesquisa.

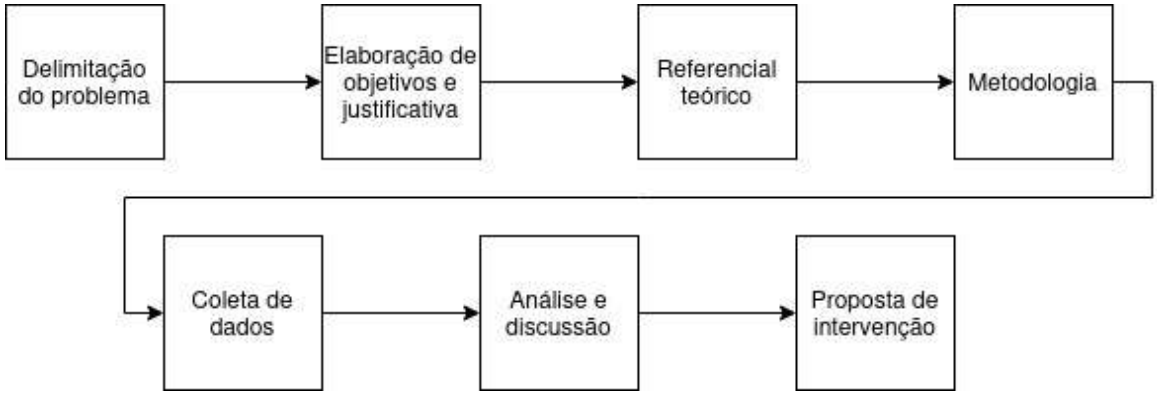
No trabalho de Prodanov e Freitas (2013), os autores também discutem a pesquisa documental como uma das modalidades de pesquisa bibliográfica, que se baseia na análise de documentos diversos para coletar dados e informações relevantes para a pesquisa. Eles enfatizam que essa abordagem é particularmente útil quando se busca explorar e analisar o conhecimento existente, como é o caso de leis e regulamentos.

A abordagem de Prodanov e Freitas (2013) também destaca a importância da crítica e interpretação dos documentos analisados, a fim de identificar conexões, contradições e lacunas no conhecimento existente. Essa visão se alinha ao processo de análise detalhada e registro de dados proposto por Gil (2002) na pesquisa documental.

3.4 FASES DA PESQUISA

Na busca pela realização dos objetivos propostos, estabeleceu-se o esquema delineado na Figura 1. Esse diagrama esclarece o planejamento adotado e ilustra as fases que compõem a execução da pesquisa.

Figura 1 – Diagrama das fases da pesquisa



Fonte: Elaborado pelo autor (2023).

3.5 PROCEDIMENTOS METODOLÓGICOS

Os métodos utilizados na análise documental incluem a leitura crítica, a categorização e a análise temática. A leitura crítica, conforme recomendado por Marconi e Lakatos (2017), envolve uma análise minuciosa e reflexiva dos documentos, identificando informações relevantes e requisitos legais aplicáveis à política de segurança da informação da instituição.

A análise da conformidade legal foi realizada por meio de um mapeamento dos requisitos legais identificados na revisão de literatura e também em políticas, regulamentos, normas, relatórios, manuais e outros em relação à política de segurança da informação da instituição e ao que compete à administração pública federal sobre o tema. Esse mapeamento permitirá identificar lacunas, não conformidades e áreas de melhoria, conforme preconizado por Gil (2017).

As recomendações para a conformidade legal foram baseadas nas lacunas e não conformidades identificadas, considerando as diretrizes e exigências estabelecidas pelas leis, normas e regulamentos aplicáveis, sendo que o objetivo desta pesquisa será analisar a conformidade legal da PSI da Unifal-MG de acordo com o disposto no Capítulo VI, Seção IV do Decreto nº 9.637, de 26 de dezembro de 2018, que trata das competências dos órgãos e das entidades da administração pública federal. Meirelles (2019) destaca a importância de fundamentar as recomendações em argumentos legais sólidos, visando garantir a adequação da política de segurança da informação aos requisitos legais identificados.

A categorização dos dados, conforme proposto por Gil (2017), consiste em agrupar as informações coletadas em categorias específicas, facilitando a identificação de lacunas e não conformidades. Essa abordagem permitiu uma organização sistemática dos dados, contribuindo para a análise comparativa e a identificação de padrões relevantes relacionados à conformidade legal.

De modo a operacionalizar a categorização dos dados, considerando o dispositivo legal utilizado para referência na conformidade legal, foi elaborado um roteiro conforme apresentado no Quadro 3:

Quadro 3 – Roteiro para verificação da conformidade legal

(continua)

Roteiro para verificação da conformidade legal em Segurança da Informação de acordo com Decreto Nº 9.637, de 26 de Dezembro de 2018.	
Competências gerais dos órgãos e entidades da administração pública federal	
Descrição	**Conforme**
Elaboração da política de segurança da informação e normas internas de segurança.	
Designação de um gestor de segurança da informação interno.	
Instituição de comitê de segurança da informação ou estrutura equivalente.	
Destinação de recursos orçamentários para ações de segurança da informação.	
Promoção de ações de capacitação e profissionalização dos recursos humanos em segurança da informação.	
Instituição e implementação de equipe de prevenção, tratamento e resposta a incidentes cibernéticos.	
Coordenação e execução de ações de segurança da informação.	
Consolidação e análise dos resultados de auditorias sobre a gestão de segurança da informação.	
Aplicação de ações corretivas e disciplinares em casos de violação da segurança da informação.	
Composição do comitê de segurança da informação interno	
Descrição	**Conforme**
Presença do gestor da segurança da informação.	
Representante da Secretaria-Executiva ou unidade equivalente.	
Representante de cada unidade finalística.	
Titular da unidade de tecnologia da informação e comunicação.	
Requisitos para o gestor de segurança da informação	
Descrição	**Conforme**
Designação de servidor público com formação ou capacitação técnica compatível.	
Edição de atos para funcionamento do comitê de segurança da informação	
Descrição	**Conforme**
Publicação de atos definindo a forma de funcionamento do comitê de segurança da informação.	
Competências da alta administração	
Descrição	**Conforme**
Promoção da simplificação administrativa, modernização da gestão pública e integração dos serviços públicos.	

Quadro 3 – Roteiro para verificação da conformidade legal

(conclusão)

Competências da alta administração	
Descrição	**Conforme**
Monitoramento do desempenho e avaliação da política de segurança da informação.	
Planejamento da execução de programas, projetos e processos relativos à segurança da informação.	
Estabelecimento de diretrizes para o processo de gestão de riscos de segurança da informação.	
Observância das normas estabelecidas pelo Gabinete de Segurança Institucional.	
Implementação de controles internos baseados na gestão de riscos de segurança da informação.	
Instituição de um sistema de gestão de segurança da informação integrado com de mecanismo de comunicação imediata sobre vulnerabilidades ou incidentes de segurança.	
Observância das normas e procedimentos específicos aplicáveis.	
Planejamento e execução de programas de segurança da informação	
Descrição	**Conforme**
Utilização de recursos criptográficos adequados.	
Aumento da resiliência dos ativos de tecnologia da informação e comunicação.	
Cooperação entre as equipes de prevenção, tratamento e resposta a incidentes cibernéticos de outras instituições.	
Priorização da interoperabilidade de tecnologias, processos, informações e dados.	
Sistema de gestão de segurança da informação	
Descrição	**Conforme**
Identificação das necessidades da organização quanto aos requisitos de segurança da informação.	
Incorporação das normas de segurança da informação estabelecidas pelo Gabinete de Segurança Institucional	
Descrição	**Conforme**
Incorporação das normas de segurança da informação em atos administrativos envolvendo ativos de tecnologia da informação.	

Fonte: Elaborado pelo autor (2023), baseado em Brasil (2018).

Além disso, a análise temática, como sugerido por Vergara (2016), foi empregada para identificar e analisar os temas e conceitos-chave presentes nos documentos. Isso permitiu uma

compreensão aprofundada das diretrizes e recomendações legais relacionadas à política de segurança da informação, enriquecendo a análise da conformidade legal.

A escolha desses métodos, embasada nas orientações de Ludke e André (2013), Marconi e Lakatos (2017), Gil (2017) e Vergara (2016), justifica-se pela sua aplicabilidade e relevância na análise de documentos, especialmente no contexto da pesquisa qualitativa. Esses métodos fornecem uma estrutura sólida para a análise documental, auxiliando na identificação das informações pertinentes, na categorização dos dados e na interpretação dos resultados.

Portanto, a adoção da abordagem qualitativa e dos métodos de leitura crítica, categorização e análise temática para a análise documental neste trabalho de dissertação contribuiu para a compreensão abrangente da conformidade legal da política de segurança da informação da instituição federal de ensino à luz da PNSI.

Ao final da análise documental, foi desenvolvida a análise dos resultados, contendo as principais descobertas, destacando-se as lacunas e não conformidades identificadas em relação aos requisitos legais. As recomendações para a conformidade legal foram baseadas nas informações obtidas durante a análise documental, fundamentadas nos argumentos legais sólidos, como sugerido por Meirelles (2019), por conseguinte com a recomendação de possíveis adequações à PSIC da Unifal-MG por meio da elaboração do Produto Técnico-Tecnológico (PTT) composto de um relatório técnico de conformidade legal.

4 ANALISE E DISCUSSÃO DOS RESULTADOS

Conforme o roteiro estabelecido no Quadro 3, foi enviado um pedido de acesso à informação através da plataforma Fala.BR, cadastrado sob o NUP: 23546.009740/2024-25, que tramitou na Unifal-MG pelo processo SEI nº 23087.000892/2024-17. Os questionamentos foram respondidos pela Gerência de Segurança da Informação – GSI/NTI e constam em sua íntegra no Anexo A deste trabalho.

As respostas obtidas foram analisadas, categorizadas de acordo com o roteiro previamente estabelecido, na qual para cada questão foi feita a análise junto ao dispositivo legal relacionado e, ao final desta seção, foi elaborado o Quadro 5 que apresenta um resumo comparativo dos questionamentos com a atribuição dos critérios: atendido, parcialmente atendido ou não atendido.

4.1 COMPETÊNCIAS GERAIS DOS ÓRGÃOS E ENTIDADES DA ADMINISTRAÇÃO PÚBLICA FEDERAL

A Política Nacional de Segurança da Informação (PNSI), conforme estabelecido pelo Decreto Nº 9.637, de 26 de dezembro de 2018, determina que os órgãos e entidades da administração pública federal devem elaborar suas políticas internas de segurança da informação, observando as diretrizes do Gabinete de Segurança Institucional da Presidência da República (Art. 15, inciso II). No caso da Universidade Federal de Alfenas (UNIFAL-MG), essa exigência se mostra atendida, evidenciada pela existência de uma política de segurança da informação e normas internas de segurança bem estabelecidas e constantemente atualizadas.

A Resolução Consuni 08/2018 aprova a Política de Segurança da Informação e Comunicação da UNIFAL-MG, que serve como a principal diretriz para a segurança da informação na instituição. Além disso, a UNIFAL-MG demonstra um compromisso contínuo com a atualização e expansão de suas normas internas, conforme refletido nas diversas resoluções adicionais que complementam e aprimoram a política inicial.

Essas resoluções indicam que a UNIFAL-MG não apenas possui uma política de segurança da informação em vigor, mas também está em constante revisão e melhoria. As

resoluções do Comitê de Governança Digital listadas no Quadro 4 descrevem resumidamente os tópicos abordados.

Quadro 4 – Comparativo das Resoluções CGD

Resolução	**Descrição**
Resolução CGD 02/2019	Estabelece diretrizes para o uso seguro dos perfis institucionais nas redes sociais, indicando a preocupação da instituição com a integridade e segurança das suas representações digitais.
Resolução CGD 03/2019	Define diretrizes para o gerenciamento e execução de cópias de segurança (backup), seu armazenamento e restauração, garantindo a resiliência e disponibilidade dos dados institucionais.
Resolução CGD 01/2020	Institui um esquema de classificação de acesso e segurança no Sistema Eletrônico de Informações (SEI), promovendo uma gestão segura e controlada das informações eletrônicas.
Resolução CGD 02/2020	Estabelece normas para o uso do serviço de e-mail institucional, essencial para a comunicação segura e oficial dentro da instituição.
Resolução CGD 03/2020	Normas de uso de credenciais de acesso, assegurando que os acessos sejam controlados e devidamente autorizados.
Resolução CGD 04/2020	Normas para o uso dos serviços disponíveis no GSuite for Education, garantindo que as ferramentas educacionais e colaborativas sejam utilizadas de forma segura.
Resolução CGD 05/2020	Diretrizes para o uso dos serviços de armazenamento e compartilhamento de arquivos, promovendo a segurança e integridade dos dados armazenados e compartilhados.
Resolução CGD 06/2020	Estabelece o processo de gestão de riscos de segurança da informação, fundamental para identificar, avaliar e mitigar riscos.
Resolução CGD 06/2020	Normas para a adesão institucional a serviços de tecnologia da informação, assegurando que todos os serviços tecnológicos estejam alinhados com os padrões de segurança da informação da instituição.

Fonte: Elaborado pelo autor (2024).

Portanto, a instituição atende ao critério estabelecido pelo Art. 15, inciso II, do Decreto Nº 9.637/2018, ao implementar e atualizar regularmente sua política de segurança da informação e normas internas. Esse compromisso contínuo com a atualização e a implementação de políticas abrangentes reflete uma governança sólida e alinhada com os princípios da PNSI, garantindo a proteção e a integridade das informações institucionais.

De acordo com o Decreto Nº 9.637, de 26 de dezembro de 2018, especificamente no Art. 15, inciso III, cada órgão ou entidade da administração pública federal deve designar um gestor de segurança da informação interno, indicado pela alta administração. Na Universidade Federal de Alfenas (UNIFAL-MG), essa exigência é plenamente atendida.

A designação formal de um gestor de segurança da informação na UNIFAL-MG está estabelecida na Resolução Consuni 10/2023, que altera a Resolução Consuni nº 80/2014. Segundo o Art. 17 da resolução, a Gerência de Segurança da Informação é responsável por diversas atribuições cruciais para a proteção e gestão da segurança da informação. O parágrafo único do mesmo artigo especifica que o Gerente de Segurança da Informação tem a responsabilidade de coordenar a Equipe de Tratamento e Resposta a Incidentes de Segurança em Redes Computacionais (ETIR/UNIFAL-MG) e atuar como Gestor de Segurança da Informação, conforme os requisitos da legislação vigente.

Essa estrutura organizacional e a clara designação de responsabilidades asseguram que a UNIFAL-MG possui uma liderança dedicada à segurança da informação, alinhada com os padrões estabelecidos pela PNSI. A presença de um gestor formalmente designado indica que as políticas e práticas de segurança da informação sejam implementadas de maneira eficaz e coordenada.

Portanto, a UNIFAL-MG cumpre o critério estabelecido pelo Art. 15, inciso III, do Decreto Nº 9.637/2018, ao ter um gestor de segurança da informação interno formalmente designado.

O Art. 15, inciso IV, do Decreto Nº 9.637, de 26 de dezembro de 2018, exige que os órgãos e entidades da administração pública federal instituam um comitê de segurança da informação ou uma estrutura equivalente para deliberar sobre os assuntos relativos à Política Nacional de Segurança da Informação (PNSI). A Universidade Federal de Alfenas (UNIFAL-MG) cumpre essa exigência através da constituição formal de seu Comitê de Govenança Digital (CGD).

Conforme o Regimento Interno do CGD, disponível no site institucional, o comitê desempenha um papel central na coordenação da formulação de políticas de Tecnologia da Informação (TI) e Segurança da Informação (SI). O Art. 3º do regimento especifica que

compete ao CGD coordenar a elaboração de propostas dessas políticas para subsequente aprovação pelo Conselho Universitário (Consuni).

A existência de tal comitê é crucial para a governança da segurança da informação, pois assegura que as políticas e normas sejam discutidas e formuladas de maneira coletiva, incorporando diversas perspectivas e expertises. Além disso, o CGD é responsável por garantir que as políticas de segurança da informação estejam alinhadas com as diretrizes e padrões nacionais, promovendo uma abordagem integrada e sistemática para a proteção das informações institucionais.

Portanto, a UNIFAL-MG atende ao critério estabelecido pelo Art. 15, inciso IV, do Decreto Nº 9.637/2018, ao ter formalmente constituído um comitê de segurança da informação. Este comitê não só coordena a formulação de políticas de TI e SI, mas também atua de forma essencial para a implementação eficaz da PNSI na instituição. A estrutura organizacional e a definição de responsabilidades dentro do CGD refletem o compromisso da UNIFAL-MG com a segurança da informação e a gestão eficiente dos riscos cibernéticos, fundamentais para a continuidade e resiliência das suas operações.

No que se refere ao Art. 15, inciso V, do Decreto Nº 9.637, de 26 de dezembro de 2018, os órgãos e entidades da administração pública federal devem destinar recursos orçamentários específicos para ações de segurança da informação. Na Universidade Federal de Alfenas (UNIFAL-MG), essa exigência é parcialmente atendida.

A resposta fornecida pela gerência indica que, embora existam recursos destinados à Tecnologia da Informação (TI) que são utilizados em parte para segurança da informação, não há um orçamento específico direcionado exclusivamente para essa finalidade. Isso sugere que as ações de segurança da informação são financiadas dentro do contexto mais amplo do orçamento de TI, sem uma alocação explícita e separada.

Essa abordagem pode limitar a capacidade da instituição de planejar e implementar ações de segurança da informação de forma proativa e estratégica. A alocação específica de recursos é essencial para garantir que as necessidades de segurança sejam plenamente atendidas e que haja uma resposta adequada às ameaças emergentes e aos requisitos regulatórios.

Portanto, embora a UNIFAL-MG utilize parte dos recursos de TI para segurança da informação, a ausência de um orçamento específico direcionado indica que o critério estabelecido pelo Art. 15, inciso V, do Decreto Nº 9.637/2018 é atendido apenas parcialmente. Para melhorar o atendimento a essa exigência, a instituição poderia considerar a criação de um orçamento dedicado para ações de segurança da informação, permitindo uma gestão mais focalizada e eficiente dos recursos destinados à proteção das suas informações e sistemas.

Essa análise destaca a necessidade de uma abordagem mais estruturada na alocação de recursos orçamentários para segurança da informação, o que é crucial para enfrentar os desafios crescentes no cenário de segurança cibernética. A implementação de um orçamento específico pode melhorar a resiliência e a capacidade de resposta da UNIFAL-MG, assegurando a continuidade e a integridade das operações institucionais.

O Art. 15, inciso VI, do Decreto Nº 9.637/2018, estabelece que os órgãos e entidades da administração pública federal devem promover ações de capacitação e profissionalização dos recursos humanos em temas relacionados à segurança da informação. Na Universidade Federal de Alfenas (UNIFAL-MG), essa exigência é atendida por meio de uma parceria com a Escola Superior de Redes (ESR) da Rede Nacional de Pesquisa (RNP).

A ESR é reconhecida como uma instituição de excelência no fornecimento de capacitação e treinamento em áreas como redes e segurança da informação. Através dessa parceria, os recursos humanos da UNIFAL-MG têm acesso a programas de capacitação que abrangem temas relacionados à segurança da informação, contribuindo para o aprimoramento das habilidades e conhecimentos necessários para lidar com os desafios em segurança cibernética.

Deste modo entende-se que há compromisso da UNIFAL-MG em investir no desenvolvimento profissional de seus colaboradores, garantindo que estejam adequadamente capacitados para lidar com as demandas cada vez mais complexas e dinâmicas da área de segurança da informação. Além disso, a parceria com uma instituição renomada como a ESR fortalece a qualidade e relevância dos programas de capacitação oferecidos aos colaboradores da universidade.

Portanto, a UNIFAL-MG cumpre integralmente o critério estabelecido pelo Art. 15, inciso VI, do Decreto Nº 9.637/2018, ao promover ações de capacitação e profissionalização

dos recursos humanos em segurança da informação por meio da parceria com a Escola Superior de Redes (ESR) da Rede Nacional de Pesquisa (RNP).

O Art. 15, inciso VII, do Decreto Nº 9.637/2018, estabelece que os órgãos e entidades da administração pública federal devem instituir e implementar uma equipe de prevenção, tratamento e resposta a incidentes cibernéticos. Na Universidade Federal de Alfenas (UNIFAL-MG), essa exigência é plenamente atendida conforme a Portaria nº 2252, de 2 de Dezembro de 2022.

A Portaria nº 2252 institui oficialmente a Equipe de Tratamento e Resposta a Incidentes de Segurança em Redes Computacionais (ETIR/UNIFAL-MG) e define suas diretrizes de funcionamento, incluindo seu posicionamento organizacional junto ao Núcleo de Tecnologia da Informação (NTI) da UNIFAL-MG. Essa equipe, conforme determinação do Reitor da universidade, integra a Rede Federal de Gestão de Incidentes Cibernéticos.

A existência e funcionamento adequado dessa equipe são fundamentais para garantir uma resposta eficiente e coordenada a incidentes de segurança cibernética na instituição. Além disso, estar integrado à Rede Federal de Gestão de Incidentes Cibernéticos fortalece a capacidade da UNIFAL-MG de colaborar e trocar informações relevantes com outras instituições no combate a ameaças cibernéticas.

Portanto, a UNIFAL-MG cumpre o critério estabelecido pelo Art. 15, inciso VII, do Decreto Nº 9.637/2018, ao ter formalmente instituída a Equipe de Tratamento e Resposta a Incidentes de Segurança em Redes Computacionais (ETIR/UNIFAL-MG) e estabelecer diretrizes para seu funcionamento conforme as normativas e regulamentações vigentes.

O Art. 15, inciso VIII, do Decreto Nº 9.637/2018, determina que os órgãos e entidades da administração pública federal devem coordenar e executar as ações de segurança da informação no âmbito de sua atuação. Na Universidade Federal de Alfenas (UNIFAL-MG), essa coordenação e execução são realizadas de forma integrada pelas equipes e comissões formalmente constituídas. A Gerência de Segurança da Informação (GSI) realiza ações coordenadas de segurança da informação de acordo com o regimento do Núcleo de Tecnologia da Informação (NTI). A Equipe de Tratamento e Resposta a Incidentes de Segurança em Redes Computacionais (ETIR) realiza ações coordenadas conforme estabelecido pela Portaria nº 2252, de 2 de dezembro de 2022. O Comitê de Governança Digital (CGD) coordena as

ações de segurança da informação e formula propostas de políticas de Segurança da Informação, conforme o Regimento Interno do CGD.

Destaca-se a integração dessas equipes e comissões, o que demonstra a realização de ações coordenadas de segurança da informação na UNIFAL-MG. Essa integração é fundamental para garantir a eficácia das medidas de segurança adotadas pela instituição, permitindo uma abordagem global e alinhada aos objetivos estratégicos de proteção das informações e sistemas. Assim, o critério estabelecido pelo dispositivo legal é plenamente atendido na universidade, evidenciando um comprometimento efetivo com a segurança da informação.

O Art. 15, inciso IX, do Decreto Nº 9.637/2018, determina que os órgãos e entidades da administração pública federal devem consolidar e analisar os resultados dos trabalhos de auditoria sobre a gestão de segurança da informação. No entanto, na situação atual da UNIFAL-MG, não há uma decisão formal ou plano aprovado para implementar essas ações.

A consolidação e análise dos resultados de auditorias são fundamentais para avaliar a eficácia das práticas de segurança da informação, identificar áreas de melhoria e tomar medidas corretivas quando necessário. Portanto, a ausência de iniciativas nesse sentido representa uma lacuna na gestão da segurança da informação na instituição.

Recomenda-se que a UNIFAL-MG avalie a necessidade de desenvolver um plano para implementar ações de consolidação e análise dos resultados de auditorias sobre a gestão de segurança da informação, de acordo com as diretrizes estabelecidas pelo dispositivo legal citado. Isso contribuirá para fortalecer as práticas de segurança da informação e garantir uma abordagem mais proativa na gestão de riscos e na proteção dos ativos de informação da universidade.

A instituição adota medidas disciplinares e corretivas diante de violações da segurança da informação, seguindo as diretrizes estabelecidas no Art. 15, inciso X do Decreto Nº 9.637/2018. Essas ações são fundamentais para garantir a integridade, confidencialidade e disponibilidade dos dados e sistemas, em conformidade com as normativas internas e externas da organização.

É importante destacar que a aplicação dessas medidas visa não apenas a punição, mas também a promoção de uma cultura de segurança da informação. Isso inclui a conscientização

dos colaboradores sobre a importância da proteção dos dados e a implementação de práticas seguras no ambiente de trabalho, contribuindo para a prevenção de futuras violações.

Essa abordagem demonstra o compromisso da instituição com a gestão eficaz da segurança da informação, buscando sempre aprimorar suas políticas e procedimentos para lidar de forma adequada e responsável com qualquer incidente relacionado à segurança dos dados.

4.2 COMPOSIÇÃO DO COMITÊ DE SEGURANÇA DA INFORMAÇÃO INTERNO OU ESTRUTURA EQUIVALENTE

A análise das respostas fornecidas sobre a composição do comitê de segurança da informação interno revela que a instituição ainda não possui uma decisão formal ou um plano aprovado para incluir o gestor de segurança da informação conforme exigido pelo Art. 15, § 1º, inciso I do Decreto Nº 9.637, de 26 de Dezembro de 2018. Este critério foi classificado como "não atendido", indicando uma área crítica que necessita de atenção para alinhar-se às exigências legais e garantir a eficácia da governança de segurança da informação.

No que diz respeito à presença de um representante da Secretaria-Executiva ou unidade equivalente no comitê, a resposta foi negativa, também classificada como "não atendido". A ausência de um representante desta unidade pode impactar a coordenação e a integração das ações de segurança da informação com outras áreas administrativas da instituição, principalmente no que se refere à tomadas de decisão, sublinhando outra lacuna na conformidade com o decreto.

Por outro lado, a instituição atendeu aos requisitos de incluir representantes de cada unidade finalística e o titular da unidade de tecnologia da informação e comunicação no comitê, conforme os incisos III e IV do mesmo artigo e parágrafo. A composição descrita no Art. 2º do Regimento Interno do CGD, que inclui uma representação das diversas unidades da instituição, reflete uma sinalização para integrar a segurança da informação em toda a estrutura organizacional. Esta conformidade fortalece a base para uma abordagem holística e colaborativa na gestão da segurança da informação.

4.3 REQUISITOS PARA O GESTOR DE SEGURANÇA DA INFORMAÇÃO

A análise do requisito de formação ou capacitação técnica compatível para o gestor de segurança da informação, conforme estipulado no Art. 15, § 4º do Decreto Nº 9.637, de 26 de Dezembro de 2018, revela que a instituição cumpre esta exigência. Mesmo que a resposta apontada para este questionamento, de que a Resolução Consuni 10/2023, que altera a Resolução Consuni nº 80/2014, Art 17 - Parágrafo único, estabelece claramente as atribuições do gestor de segurança da informação, o referido artigo não menciona explicitamente a formação técnica compatível. No entanto foi feita a verificação do currículo Lattes do atual gestor e confirmou-se que o mesmo possui a formação e capacitação necessárias para desempenhar suas funções.

Esta conformidade é fundamental para garantir que o gestor de segurança da informação tenha o conhecimento técnico e as habilidades necessárias para liderar a implementação e a manutenção das políticas de segurança da informação na instituição.

Ao assegurar que o gestor de segurança da informação possui a formação adequada, a instituição não só cumpre os requisitos legais, mas também fortalece sua capacidade de proteger dados e sistemas críticos contra ameaças e vulnerabilidades. Esta medida reflete uma abordagem proativa e profissional na gestão da segurança da informação, contribuindo para um ambiente mais seguro e confiável para todos os usuários da instituição.

4.4 EDIÇÃO DE ATOS PARA FUNCIONAMENTO DO COMITÊ DE SEGURANÇA DA INFORMAÇÃO

A análise da existência de atos publicados que definem a forma de funcionamento do comitê de segurança da informação, conforme estipulado no Art. 16 do Decreto Nº 9.637, de 26 de Dezembro de 2018, revela que a Universidade Federal de Alfenas (UNIFAL-MG) cumpre integralmente este requisito. O Regimento Interno do Comitê de Governança Digital (CGD) especifica as atribuições e o funcionamento do comitê, incluindo a coordenação da formulação de políticas de Tecnologia da Informação (TI) e Segurança da Informação (SI).

O Artigo 3º do Regimento Interno do CGD estabelece que compete ao comitê coordenar a elaboração de propostas de políticas tanto de TI quanto de SI. Assim o CGD assegura que as políticas desenvolvidas sejam abrangentes e estejam alinhadas com as necessidades institucionais e as melhores práticas de segurança da informação. A aprovação dessas políticas pelo Consuni garante um processo de validação e legitimação, reforçando a estrutura organizacional e o comprometimento com a segurança da informação.

A existência de tais atos publicados e bem definidos demonstra a maneira com que a UNIFAL-MG trata a governança e a gestão da segurança da informação. A clareza nas atribuições do CGD e a formalização de seu funcionamento proporcionam uma base sólida para a implementação eficaz das políticas de segurança da informação, contribuindo para a proteção dos dados e sistemas institucionais. Este alinhamento entre os requisitos legais e as práticas institucionais não só atende às exigências regulamentares, mas também fortalece a resiliência da instituição contra ameaças cibernéticas.

4.5 COMPETÊNCIAS DA ALTA ADMINISTRAÇÃO

A análise das ações promovidas pela alta administração da Universidade Federal de Alfenas (UNIFAL-MG) revela um compromisso com a simplificação administrativa, modernização da gestão pública e integração dos serviços públicos prestados pela instituição, conforme estipulado no Art. 17, inciso I, do Decreto Nº 9.637, de 26 de Dezembro de 2018. A Resolução 02/2022, que institui o Plano de Transformação Digital da UNIFAL-MG, é uma evidência sólida deste compromisso.

O Plano de Transformação Digital da UNIFAL-MG, elaborado em conformidade com o Decreto Nº 10.332, de 28 de abril de 2020, representa um esforço coordenado para modernizar os processos administrativos e integrar os serviços públicos. Este plano foi aprovado pelo Comitê de Governança Digital e submetido à Secretaria de Governo Digital do Ministério da Economia (SGD), demonstrando o alinhamento da instituição com as diretrizes nacionais de transformação digital e gestão pública eficiente.

A implementação do Plano de Transformação Digital inclui diversas iniciativas que visam a simplificação de processos administrativos e a modernização da gestão pública. Estas

iniciativas abrangem desde a digitalização de documentos e processos até a adoção de novas tecnologias para melhorar a eficiência e a transparência dos serviços públicos prestados. A integração dos serviços públicos também é um objetivo central, facilitando o acesso e a utilização dos serviços pela comunidade acadêmica e pelo público em geral.

Desta forma entende-se que as ações promovidas pela alta administração da UNIFAL-MG, conforme evidenciado pela Resolução 02/2022, atendem plenamente ao critério estabelecido pelo Art. 17, inciso I, do Decreto Nº 9.637, de 26 de Dezembro de 2018. A instituição não apenas cumpre os requisitos legais, mas também avança na direção de uma gestão pública mais moderna, eficiente e integrada.

A análise referente ao monitoramento do desempenho e avaliação da política de segurança da informação na Universidade Federal de Alfenas (UNIFAL-MG) revela uma área crítica que ainda necessita de desenvolvimento. Conforme o estipulado no Art. 17, inciso II, do Decreto Nº 9.637, de 26 de Dezembro de 2018, é essencial que as instituições federais implementem mecanismos para o monitoramento contínuo e a avaliação sistemática das políticas de segurança da informação. No entanto, a UNIFAL-MG ainda não possui uma decisão formal ou um plano aprovado para realizar tais atividades.

A ausência de um plano formal de monitoramento e avaliação implica que a instituição pode estar vulnerável a riscos de segurança não identificados ou mal gerenciados. O monitoramento contínuo e a avaliação periódica são práticas recomendadas para assegurar que as políticas de segurança da informação sejam eficazes e atualizadas conforme as novas ameaças e tecnologias emergem. Sem esses processos, é difícil garantir que a política de segurança da informação esteja cumprindo seus objetivos e protegendo adequadamente os ativos de informação da universidade.

Além disso, a falta de um sistema de monitoramento e avaliação impede a identificação de áreas que necessitam de melhorias e a implementação de ações corretivas apropriadas. Isto pode resultar em um ambiente de segurança da informação reativo em vez de proativo, onde as medidas são tomadas apenas após a ocorrência de incidentes, em vez de prevenir tais eventos através de uma gestão eficaz e contínua da segurança da informação.

Portanto, a implementação de um plano de monitoramento e avaliação é crucial para o fortalecimento da segurança da informação na UNIFAL-MG. Essa medida não apenas

atenderia ao requisito legal do Art. 17, inciso II, do Decreto Nº 9.637, de 26 de Dezembro de 2018, mas também contribuiria significativamente para a proteção dos dados e sistemas da instituição.

A avaliação do planejamento de execução de programas, projetos e processos relativos à segurança da informação na Universidade Federal de Alfenas (UNIFAL-MG) aponta para uma área em que a instituição ainda não atende plenamente aos requisitos legais estipulados pelo Art. 17, inciso IV, do Decreto Nº 9.637, de 26 de Dezembro de 2018. Atualmente, não há decisão formal ou plano aprovado que oriente essas ações dentro da universidade.

A ausência de planejamento formal em relação à execução de programas e projetos de segurança da informação pode resultar em iniciativas desconectadas e reativas, em vez de uma abordagem estratégica e coordenada. O planejamento estruturado é essencial para garantir que todas as ações de segurança da informação sejam alinhadas com os objetivos gerais da instituição, otimizem o uso dos recursos disponíveis e abordem proativamente as vulnerabilidades e ameaças emergentes.

Sem um plano formal, a execução de projetos e processos de segurança da informação pode carecer de direção clara e prioridades definidas. Isso dificulta a medição da eficácia das iniciativas implementadas e a realização de melhorias contínuas. Além disso, a falta de planejamento pode levar à redundância de esforços e à alocação inadequada de recursos, comprometendo a capacidade da universidade de responder de maneira eficiente e eficaz às exigências de segurança da informação.

Portanto, para atender plenamente ao Art. 17, inciso IV, do Decreto Nº 9.637, de 26 de Dezembro de 2018, e melhorar sua postura de segurança da informação, a UNIFAL-MG precisa desenvolver e aprovar um plano de execução abrangente para programas, projetos e processos relacionados à segurança da informação. Esse plano deve envolver todas as partes interessadas relevantes, definir metas claras e incluir mecanismos de monitoramento e avaliação para garantir a eficácia e a continuidade das ações de segurança da informação na universidade.

Ao se analisar o disposto no Art. 17, inciso V, do Decreto Nº 9.637, de 26 de Dezembro de 2018, no que diz respeito ao estabelecimento formal das diretrizes para o processo de gestão de riscos de segurança da informação, a Universidade Federal de Alfenas

(UNIFAL-MG) está plenamente de acordo com este requisito. A Resolução CGD 06/2020 é o documento que estabelece o processo de Gestão de Riscos de Segurança da Informação e Comunicações (GRSIC) na universidade. Esse documento tem como objetivo principal definir o escopo, as responsabilidades e os procedimentos necessários para a gestão eficaz dos riscos associados à segurança da informação.

A implementação de uma resolução específica como a CGD 06/2020 destaca a identificação, avaliação e mitigação de riscos que podem comprometer a integridade, a confidencialidade e a disponibilidade das informações institucionais. A formalização dessas diretrizes é fundamental para garantir que todos os riscos relevantes sejam identificados e tratados de maneira consistente e sistemática, minimizando possíveis impactos negativos nas operações e nos serviços da universidade.

O processo de Gestão de Riscos de Segurança da Informação estabelecido pela resolução envolve uma abordagem abrangente que inclui a avaliação contínua das ameaças e vulnerabilidades, a implementação de controles adequados para mitigar riscos e a revisão regular das políticas e procedimentos de segurança. Esta abordagem garante que a universidade esteja preparada para enfrentar os desafios de segurança de maneira proativa, fortalecendo sua resiliência contra incidentes de segurança e protegendo seus ativos de informação de maneira eficaz.

Portanto, a UNIFAL-MG, através da Resolução CGD 06/2020, não só cumpre os requisitos legais estabelecidos pelo Decreto Nº 9.637, de 26 de Dezembro de 2018, mas também adota práticas de gestão de riscos alinhadas com as melhores práticas. A formalização e a implementação dessas diretrizes são passos essenciais para a manutenção de um ambiente seguro e confiável para a gestão das informações institucionais.

De acordo com o Art. 17, inciso VI do Decreto Nº 9.637, de 26 de Dezembro de 2018, é essencial que as instituições observem as normas estabelecidas pelo Gabinete de Segurança Institucional (GSI). Na Universidade Federal de Alfenas (UNIFAL-MG), esta observância é garantida conforme as normativas internas do Comitê de Governança Digital (CGD) e é corroborada pelo último Relato Integrado publicado (UNIFAL-MG, 2023). A conformidade legal da gestão de Tecnologia da Informação e Comunicação (TIC) na UNIFAL-MG é mantida através do Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC), que

é avaliado e aprovado pelo CGD e pelo Conselho Universitário (CONSUNI), a instância máxima deliberativa da instituição.

O PDTIC da UNIFAL-MG é elaborado com o objetivo de assegurar o alinhamento com as diretrizes e normas do governo federal, bem como com as estratégias e normas institucionais. Este plano é revisado periodicamente para garantir que a instituição esteja em conformidade com as exigências legais e as melhores práticas do mercado. A observância das diretrizes estabelecidas pelo Governo Federal, órgãos de controle, Secretaria de Governo Digital (SGD) do Ministério da Economia, Sistema de Administração dos Recursos de Tecnologia da Informação (SISP), e pelo GSI/PR é um ponto central do planejamento e execução das políticas de TIC na UNIFAL-MG.

Assim, a UNIFAL-MG não apenas cumpre os requisitos legais, mas também busca continuamente aprimorar a gestão de TIC, observando padrões de mercado e regulamentações internas estabelecidas pelo CGD. Este compromisso com a conformidade e a melhoria contínua é essencial para a eficácia e a segurança das operações de TIC na instituição, atendendo plenamente ao critério estabelecido, sendo classificado como atendido.

De acordo com o Art. 17, inciso VII do Decreto Nº 9.637, de 26 de Dezembro de 2018, as instituições devem implementar controles internos baseados na gestão de riscos de segurança da informação. Na Universidade Federal de Alfenas (UNIFAL-MG), embora exista uma normativa que trata da gestão de riscos em segurança da informação, ainda não há uma decisão formal ou um plano aprovado para implementar esses controles internos de maneira efetiva.

A Resolução CGD 06/2020 estabelece o processo de Gestão de Riscos de Segurança da Informação no âmbito da UNIFAL-MG. Este documento tem por objetivo definir os procedimentos e responsabilidades para a identificação, avaliação, tratamento e monitoramento de riscos de segurança da informação e comunicações na instituição. No entanto, a ausência de uma implementação formal desses controles internos indica que, apesar de haver diretrizes estabelecidas, elas ainda não foram operacionalizadas no dia a dia da instituição.

A falta de implementação formal dos controles internos baseados na gestão de riscos representa uma lacuna significativa na estrutura de segurança da informação da UNIFAL-MG.

Sem a aplicação prática dessas diretrizes, a capacidade da instituição de identificar e mitigar riscos de segurança da informação de forma eficiente é limitada. Portanto, o critério relacionado a essa questão é classificado como não atendido.

Destaca-se a necessidade urgente de avançar da fase de planejamento para a execução prática das diretrizes de gestão de riscos. A implementação efetiva de controles internos é crucial para fortalecer a postura de segurança da informação da instituição, garantindo que as políticas e procedimentos estabelecidos sejam realmente aplicados e monitorados continuamente.

De acordo com o Art. 17, incisos VIII e IX do Decreto Nº 9.637, de 26 de Dezembro de 2018, as instituições devem instituir e implementar formalmente um sistema de gestão de segurança da informação que inclua mecanismos de comunicação imediata sobre vulnerabilidades ou incidentes de segurança. Na Universidade Federal de Alfenas (UNIFAL-MG), atualmente, não há uma decisão formal ou um plano aprovado para implementar um sistema desse tipo.

A ausência de um sistema de gestão de segurança da informação formalmente instituído e implementado representa uma falha significativa na infraestrutura de segurança da instituição. Embora existam normativas e diretrizes gerais para a segurança da informação, a falta de um sistema específico e de mecanismos de comunicação imediata impede uma resposta rápida e eficaz a possíveis vulnerabilidades ou incidentes de segurança. Isso significa que a instituição pode estar exposta a riscos que poderiam ser mitigados ou evitados com uma gestão mais proativa e estruturada.

Sem um sistema de gestão formal e mecanismos de comunicação imediata, a capacidade da UNIFAL-MG de identificar, reportar e responder a incidentes de segurança de maneira eficiente é severamente limitada. A implementação de tais sistemas é essencial para assegurar que todas as partes relevantes sejam informadas rapidamente em caso de incidentes, permitindo uma resposta coordenada e eficaz. Portanto, o critério relacionado a esta questão é classificado como não atendido.

Esta análise sublinha a necessidade urgente de a UNIFAL-MG desenvolver e implementar um sistema de gestão de segurança da informação que inclua mecanismos de comunicação imediata. A adoção dessas medidas é fundamental para fortalecer a postura de

segurança da instituição, garantindo que as ameaças sejam detectadas e mitigadas em tempo hábil, protegendo assim os ativos de informação e a continuidade das operações institucionais.

De acordo com o Art. 17, inciso X do Decreto Nº 9.637, de 26 de Dezembro de 2018, as instituições devem observar normas e procedimentos específicos aplicáveis às práticas de governança da segurança da informação. Na Universidade Federal de Alfenas (UNIFAL-MG), essa conformidade é assegurada conforme as normativas internas do Comitê de Governança Digital (CGD) e pelo último Relato Integrado publicado.

A UNIFAL-MG, por meio do seu Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC), busca manter o alinhamento com as diretrizes e normas do governo federal, além de suas próprias estratégias e normas institucionais. O PDTIC, avaliado e aprovado pelo CGD e pelo Conselho Universitário (CONSUNI), que é a instância máxima deliberativa da UNIFAL-MG, estabelece um marco de conformidade legal para a gestão de Tecnologia da Informação e Comunicação (TIC). Este alinhamento inclui a observância de diretrizes estabelecidas pelo Governo Federal, órgãos de controle, a Secretaria de Governo Digital (SGD) do Ministério da Economia, o Sistema de Administração dos Recursos de Tecnologia da Informação (SISP), e o Gabinete de Segurança Institucional da Presidência da República (GSI/PR).

Para assegurar a conformidade legal da gestão de TIC, a UNIFAL-MG não apenas adere às diretrizes governamentais, mas também observa padrões de mercado e regulamentações internas estabelecidas pelo CGD. Essa abordagem visa não só a conformidade legal, mas também a melhoria contínua da gestão de TIC na instituição. Assim, a UNIFAL-MG demonstra um compromisso robusto com a governança da segurança da informação, atendendo plenamente ao critério estipulado pelo Decreto.

Portanto, com base nas evidências fornecidas pelas normativas internas e práticas de governança adotadas, o critério relacionado à observância de normas e procedimentos específicos aplicáveis à governança da segurança da informação é classificado como atendido.

4.6 PLANEJAMENTO E EXECUÇÃO DE PROGRAMAS DE SEGURANÇA DA INFORMAÇÃO

Conforme o Art. 17, § 1º, inciso I do Decreto Nº 9.637, de 26 de Dezembro de 2018, as instituições devem fazer uso de recursos criptográficos adequados como parte do planejamento e execução de programas de segurança da informação. Na Universidade Federal de Alfenas (UNIFAL-MG), este requisito é atendido conforme a Resolução CGD 03/2020, que estabelece as normas de uso de credenciais de acesso no âmbito da instituição.

A Resolução CGD 03/2020 referencia explicitamente a Norma ABNT NBR ISO/IEC 27002 e a RFC 1244, que são reconhecidas normas internacionais de segurança da informação. A adoção dessas normas demonstra um compromisso com as melhores práticas em segurança da informação, incluindo o uso de técnicas criptográficas robustas para proteger dados e garantir a integridade e confidencialidade das informações.

A aplicação de recursos criptográficos adequados é fundamental para a proteção contra ameaças cibernéticas e para garantir a segurança dos dados sensíveis. Na UNIFAL-MG, a conformidade com essas normas é um componente central da política de segurança da informação, assegurando que as credenciais de acesso e outras informações críticas sejam protegidas de maneira eficaz.

Portanto, com base na implementação das normas mencionadas e o uso de recursos criptográficos adequados conforme estabelecido pela Resolução CGD 03/2020, o critério relacionado ao uso de recursos criptográficos adequados é classificado como atendido.

De acordo com o Art. 17, § 1º, inciso II do Decreto Nº 9.637, de 26 de Dezembro de 2018, as instituições devem realizar ações para aumentar a resiliência dos ativos de tecnologia da informação e comunicação (TIC). A Universidade Federal de Alfenas (UNIFAL-MG) atende a este requisito, conforme evidenciado no último Relato Integrado publicado (UNIFAL-MG, 2023).

A UNIFAL-MG destaca a sustentação dos serviços de TIC, o que consome uma grande quantidade de recursos humanos para monitoramento contínuo. Isso inclui a manutenção, sustentação, atualização e suporte para o funcionamento de cerca de 70 sistemas de informação. Além disso, são realizados monitoramentos de segurança da informação (firewall), monitoramento de datacenter, e monitoramento de conectividade, entre outros. A atualização de softwares e sistemas operacionais de vários laboratórios didáticos e serviços

como Firewall, DNS, Autenticação, CAFe, Eduroam, Servidor de Backup, e sítios eletrônicos também são partes integrantes desse esforço.

Especificamente, a instalação e configuração de uma storage e dois servidores, além de sistema de virtualização, sistemas operacionais e banco de dados, ampliaram consideravelmente a capacidade de processamento e armazenamento disponível para os serviços de TIC da UNIFAL-MG. A gestão e o monitoramento de segurança da informação são de responsabilidade da Gerência de Segurança da Informação, unidade do Núcleo de Tecnologia da Informação. Esta gerência realiza o acompanhamento diário dos backups de dados e servidores, a verificação de incidentes de segurança, entre outras atividades. Projetos de migração de serviços para ambientes mais seguros, tunning de servidores, e atualização e configuração de servidores firewall foram executados para aumentar a resiliência dos ativos de TIC.

Portanto, com base nas ações descritas e a conformidade com o dispositivo legal mencionado, conclui-se que a UNIFAL-MG atende ao critério de realizar ações para o aumento da resiliência dos ativos de tecnologia da informação e comunicação.

De acordo com o Art. 17, § 1º, inciso III do Decreto Nº 9.637, de 26 de Dezembro de 2018, é necessário que exista cooperação entre as equipes de prevenção, tratamento e resposta a incidentes cibernéticos de diferentes instituições. A Universidade Federal de Alfenas (UNIFAL-MG) atende a esse requisito, conforme estabelecido pela Portaria nº 2252, de 2 de Dezembro de 2022.

A referida portaria institui, no âmbito da UNIFAL-MG, a Equipe de Tratamento e Resposta a Incidentes de Segurança em Redes Computacionais (ETIR/UNIFAL-MG). Esta equipe tem diretrizes claras para o seu funcionamento e posicionamento organizacional dentro do Núcleo de Tecnologia da Informação (NTI) da UNIFAL-MG. A formalização dessa equipe e suas diretrizes de operação garantem uma estrutura organizada para a gestão de incidentes cibernéticos.

Além disso, a ETIR/UNIFAL-MG, conforme ato do Reitor da UNIFAL-MG, integra a Rede Federal de Gestão de Incidentes Cibernéticos. Esta integração promove a cooperação e a coordenação com outras instituições, permitindo uma resposta mais eficaz a incidentes cibernéticos através do compartilhamento de informações e recursos. Esta rede federal visa

fortalecer a capacidade de resposta a incidentes cibernéticos, proporcionando uma abordagem colaborativa e consolidada para a segurança da informação.

Portanto, com base na implementação da ETIR/UNIFAL-MG e sua integração na Rede Federal de Gestão de Incidentes Cibernéticos, a UNIFAL-MG cumpre o critério de cooperação entre as equipes de prevenção, tratamento e resposta a incidentes cibernéticos de outras instituições, atendendo plenamente ao dispositivo legal mencionado.

Conforme o Art. 17, § 1º, inciso IV do Decreto Nº 9.637, de 26 de Dezembro de 2018, as instituições devem priorizar a interoperabilidade de tecnologias, processos, informações e dados. A Universidade Federal de Alfenas (UNIFAL-MG) ainda não tem uma decisão formal ou plano aprovado que estabeleça claramente essa priorização. Apesar disso, é possível identificar esforços significativos para a interoperabilidade através de diversas iniciativas e serviços em operação na instituição.

O Plano de Transformação Digital da UNIFAL-MG e outros serviços em operação demonstram a utilização da interoperabilidade em vários aspectos. Por exemplo, o uso do login único gov.br, a rede “eduroam” e a Comunidade Acadêmica Federada (CAFe) são evidências da integração de tecnologias, processos, informações e dados na instituição. O login único gov.br permite aos cidadãos acessar serviços online de diversos órgãos do governo com uma única conta, tornando o processo mais ágil e seguro. Este recurso, segundo o Núcleo de Tecnologia de Informação (NTI) da UNIFAL-MG, facilita a identificação dos usuários e melhora a segurança no acesso aos serviços digitais.

A Comunidade Acadêmica Federada (CAFe) é um serviço de gestão de identidade que reúne instituições de ensino e pesquisa brasileiras, permitindo que usuários acessem serviços oferecidos pelas organizações participantes através de uma única conta. Este serviço inclui o acesso ao Portal de Periódicos da Capes, facilitando a pesquisa acadêmica e a disseminação de informações. Além disso, a rede “eduroam” oferece um serviço de mobilidade global desenvolvido para a comunidade de educação e pesquisa, disponível em cerca de 100 instituições no Brasil e coordenado pela Rede Nacional de Ensino e Pesquisa (RNP).

Embora a UNIFAL-MG ainda não tenha uma formalização específica que priorize a interoperabilidade de forma abrangente, as práticas existentes mostram um movimento claro nessa direção. Portanto, a instituição pode ser considerada como parcialmente atendendo a

este requisito, dado que a interoperabilidade é aplicada em várias áreas importantes, mas ainda falta uma priorização formal e abrangente.

4.7 SISTEMA DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO

Conforme o Art. 17, § 2º do Decreto Nº 9.637, de 26 de Dezembro de 2018, as instituições devem identificar as necessidades da organização quanto aos requisitos de segurança da informação em sistemas de gestão. Na Universidade Federal de Alfenas (UNIFAL-MG), ainda não há uma decisão formal estabelecida para identificar essas necessidades de forma sistemática e abrangente. No entanto, existem documentações informativas elaboradas e disponíveis internamente, além de ofícios que fornecem indicações de boas práticas em desenvolvimento seguro.

Essas documentações e ofícios são passos importantes para o alinhamento com os requisitos de segurança da informação. Eles demonstram um esforço proativo da instituição em sensibilizar e guiar suas equipes sobre as práticas recomendadas para assegurar a integridade, confidencialidade e disponibilidade das informações. Contudo, a ausência de uma formalização impede o atendimento total ao dispositivo legal, uma vez que a falta de um plano formalizado pode levar a inconsistências na aplicação das boas práticas e na adequação dos sistemas de gestão às necessidades específicas de segurança.

A formalização desse processo é crucial para garantir que todas as áreas e sistemas da organização estejam alinhados com as políticas de segurança da informação. A implementação de um sistema formalizado de gestão de segurança da informação assegura que as práticas recomendadas sejam seguidas de maneira consistente e eficaz, mitigando riscos e fortalecendo a proteção dos ativos de informação da instituição. Portanto, devido à falta de formalização, considera-se que o critério é atendido parcialmente.

4.8 INCORPORAÇÃO DAS NORMAS DE SEGURANÇA DA INFORMAÇÃO ESTABELECIDAS PELO GABINETE DE SEGURANÇA INSTITUCIONAL

As normas de segurança da informação estabelecidas pelo Gabinete de Segurança Institucional (GSI) são incorporadas aos atos administrativos envolvendo ativos de tecnologia da informação na Universidade Federal de Alfenas (UNIFAL-MG). Esta incorporação é refletida nas normativas internas do Comitê de Governança Digital (CGD) e é confirmada pelo último Relato Integrado publicado pela instituição. A UNIFAL-MG, através do seu Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC), busca garantir a conformidade legal e manter o alinhamento com as diretrizes e normas do governo federal, bem como com suas próprias estratégias e normas institucionais.

O PDTIC é avaliado e aprovado pelo CGD e pelo Conselho Universitário (CONSUNI), que é a instância máxima deliberativa da UNIFAL-MG. Este plano é uma ferramenta essencial para assegurar que a gestão de Tecnologia da Informação e Comunicação (TIC) da universidade observe e aplique as diretrizes estabelecidas pelo Governo Federal, pelos órgãos de controle, pela Secretaria de Governo Digital (SGD) do Ministério da Economia, pelo Sistema de Administração dos Recursos de Tecnologia da Informação (SISP), e pelo Gabinete de Segurança Institucional da Presidência da República (GSI/PR). Além disso, o PDTIC também considera padrões de mercado e regulamentações internas estabelecidas pelo CGD.

Portanto, a UNIFAL-MG demonstra um compromisso contínuo com a incorporação das normas de segurança da informação em seus atos administrativos, buscando sempre atender à legislação e melhorar a gestão de TIC na instituição. Esta abordagem abrangente garante que todas as atividades e processos relacionados aos ativos de tecnologia da informação estejam em conformidade com as normas de segurança estabelecidas, promovendo uma gestão eficaz e segura desses ativos.

4.9 RESUMO COMPARATIVO

O Quadro 5 apresenta um resumo comparativo entre os questionamentos analisados, o dispositivo legal relacionado e o critério de analise.

Quadro 5 – Resumo Comparativo

(continua)

Categoria	**Questão**	**Dispositivo Legal**	**Critério**
Competências gerais dos órgãos e entidades da administração pública federal	Existe na instituição uma política de segurança da informação e normas internas de segurança em vigor?	Art. 15, II, Decreto Nº 9.637/2018	Atendido
	Há um gestor de segurança da informação interno formalmente designado?	Art. 15, III, Decreto Nº 9.637/2018	Atendido
	Existe um comitê de segurança da informação ou estrutura equivalente formalmente constituída?	Art. 15, IV, Decreto Nº 9.637/2018	Atendido
	São destinados recursos orçamentários para ações de segurança da informação?	Art. 15, V, Decreto Nº 9.637/2018	Parcialmente Atendido
	São realizadas ações de capacitação e profissionalização dos recursos humanos em segurança da informação?	Art. 15, VI, Decreto Nº 9.637/2018	Atendido
	Existe uma equipe de prevenção, tratamento e resposta a incidentes cibernéticos formalmente Instituída?	Art. 15, VII, Decreto Nº 9.637/2018	Atendido
	As equipes e comissões formalmente constituídas realizam ações coordenadas de segurança da informação?	Art. 15, VIII, Decreto Nº 9.637/2018	Atendido
	São realizadas ações de consolidação e análise dos resultados de auditorias sobre a gestão de segurança da informação?	Art. 15, IX, Decreto Nº 9.637/2018	Não Atendido
	São aplicadas ações corretivas e disciplinares em casos de violação da segurança da informação?	Art. 15, X, Decreto Nº 9.637/2018	Atendido
Composição do comitê de segurança da informação interno ou estrutura equivalente	Conta com a presença do gestor da segurança da informação?	Art. 15, §1º, I, Decreto Nº 9.637/2018	Não Atendido
	Conta com a presença do representante da Secretaria-Executiva ou unidade equivalente?	Art. 15, §1º, II, Decreto Nº 9.637/2018	Não Atendido

Quadro 5 – Resumo Comparativo

(continuação)

Categoria	**Questão**	**Dispositivo Legal**	**Critério**
Composição do comitê de segurança da informação interno ou estrutura equivalente	Conta com a presença de um representante de cada unidade finalística?	Art. 15, §1º, III, Decreto Nº 9.637/2018	Atendido
	Conta com a presença do titular da unidade de tecnologia da informação e comunicação?	Art. 15, §1º, IV, Decreto Nº 9.637/2018	Atendido
Requisitos para o gestor de segurança da informação	O servidor público designado tem formação ou capacitação técnica compatível?	Art. 15, §4º, Decreto Nº 9.637/2018	Atendido
Edição de atos para funcionamento do comitê de segurança da informação	Existem atos publicados definindo a forma de funcionamento do comitê de segurança da informação?	Art. 16, Decreto Nº 9.637/2018	Atendido
Competências da alta administração	São promovidas ações de simplificação administrativa, modernização da gestão pública e integração dos serviços públicos prestados pela instituição?	Art. 17, I, Decreto Nº 9.637/2018	Atendido
	É realizado o monitoramento do desempenho e avaliação da política de segurança da informação?	Art. 17, II, Decreto Nº 9.637/2018	Não Atendido
	São realizadas ações de planejamento da execução de programas, projetos e processos relativos à segurança da informação?	Art. 17, IV, Decreto Nº 9.637/2018	Não Atendido
	Estão formalmente estabelecidas as diretrizes para o processo de gestão de riscos de segurança da informação?	Art. 17, V, Decreto Nº 9.637/2018	Atendido
	Há observância das normas estabelecidas pelo Gabinete de Segurança Institucional?	Art. 17, VI, Decreto Nº 9.637/2018	Atendido
	Há implementação de controles internos baseados na gestão de riscos de segurança da informação?	Art. 17, VII, Decreto Nº 9.637/2018	Não Atendido

Quadro 5 – Resumo Comparativo

(conclusão)

Categoria	**Questão**	**Dispositivo Legal**	**Critério**
Competências da alta administração	Há formalmente instituído e implementado um sistema de gestão de segurança da informação com mecanismo de comunicação imediata sobre vulnerabilidades ou incidentes de segurança?	Art. 17, VIII e IX, Decreto Nº 9.637/2018	Não Atendido
	Há observância de normas e procedimentos específicos aplicáveis?	Art. 17, X, Decreto Nº 9.637/2018	Atendido
Planejamento e execução de programas de segurança da informação	Faz uso de recursos criptográficos adequados?	Art. 17, §1º, I, Decreto Nº 9.637/2018	Atendido
	São realizadas ações para o aumento da resiliência dos ativos de tecnologia da informação e comunicação?	Art. 17, §1º, II, Decreto Nº 9.637/2018	Atendido
	Existe cooperação entre as equipes de prevenção, tratamento e resposta a incidentes cibernéticos de outras instituições?	Art. 17, §1º, III, Decreto Nº 9.637/2018	Atendido
	Há priorização na interoperabilidade de tecnologias, processos, informações e dados?	Art. 17, §1º, IV, Decreto Nº 9.637/2018	Parcialmente Atendido
Sistema de gestão de segurança da informação	São identificadas as necessidades da organização quanto aos requisitos de segurança da informação em sistemas de gestão?	Art. 17, §2º, Decreto Nº 9.637/2018	Parcialmente Atendido
Incorporação das normas de segurança da informação estabelecidas pelo Gabinete de Segurança Institucional	As normas de segurança da informação são incorporadas aos atos administrativos envolvendo ativos de tecnologia da informação?	Art. 18, Decreto Nº 9.637/2018	Atendido

Fonte: Elaborado pelo autor (2024).

5 CONSIDERAÇÕES FINAIS

A segurança da informação nas instituições públicas, especialmente nas universidades federais, é um tema de crescente relevância. A necessidade de proteger dados sensíveis e garantir a continuidade e integridade dos serviços prestados impõe desafios significativos para a gestão de tecnologia da informação. Este trabalho analisou a implementação e a conformidade das políticas de segurança da informação na Universidade Federal de Alfenas (UNIFAL-MG) em relação ao Decreto Nº 9.637/2018.

A análise da segurança da informação é essencial para identificar lacunas, fortalecer práticas de segurança e assegurar a conformidade com as normativas legais. Com a crescente digitalização e dependência de sistemas de informação, as universidades federais precisam adotar medidas robustas para proteger seus ativos informacionais contra ameaças cibernéticas.

O objeto de pesquisa deste trabalho é analisar a conformidade legal no atual estágio de implementação das políticas de segurança da informação na UNIFAL-MG, conforme os requisitos estabelecidos pelo Decreto Nº 9.637/2018. Foram avaliados diversos aspectos relacionados à gestão de segurança da informação, incluindo a existência de políticas, designação de responsáveis, ações de capacitação, e a aplicação de normas e procedimentos específicos.

O principal objetivo foi avaliar a conformidade da UNIFAL-MG com as exigências do Decreto Nº 9.637/2018. A metodologia envolveu a análise documental das resoluções internas, relatórios de gestão, portarias, e regimentos relacionados à segurança da informação. Foram verificadas a existência e a efetividade das práticas adotadas pela instituição, bem como a designação de responsabilidades e a realização de ações específicas para a proteção dos ativos informacionais.

Os achados indicam que a UNIFAL-MG possui diversas resoluções e práticas em vigor que atendem parcialmente ou totalmente aos requisitos legais. Por exemplo, a instituição possui políticas formais de segurança da informação e um comitê de governança digital que coordena ações de segurança. Entretanto, algumas áreas, como a consolidação e análise de auditorias e a implementação de controles internos baseados na gestão de riscos, ainda não atendem plenamente às exigências.

As análises indicam que a UNIFAL-MG tem se esforçado para implementar uma gestão de segurança da informação robusta, alinhando-se a normas internacionais como a ABNT NBR ISO/IEC 27002. A existência de resoluções como a CGD 03/2020, que trata do uso de credenciais de acesso, demonstra uma preocupação com a integridade e a segurança dos sistemas institucionais. A integração da Equipe de Tratamento e Resposta a Incidentes de Segurança em Redes Computacionais (ETIR) à Rede Federal de Gestão de Incidentes Cibernéticos é um exemplo de cooperação interinstitucional, essencial para a gestão de incidentes cibernéticos.

Entre as dificuldades encontradas, destaca-se a falta de formalização de algumas práticas e a ausência de monitoramento sistemático de certos aspectos da segurança da informação. Além disso, a implementação completa das normas exige recursos orçamentários e humanos que, por vezes, são limitados. A análise também foi limitada pela disponibilidade de documentos e informações acessíveis durante o período de estudo.

Para estudos futuros, sugere-se a realização de auditorias independentes para verificar a efetividade das medidas implementadas e a identificação de áreas de melhoria contínua. Além disso, é recomendada a ampliação das capacitações em segurança da informação para todos os níveis hierárquicos da instituição, bem como a implementação de um sistema de gestão de riscos mais abrangente. Outra sugestão seria a aplicação dessa estratégia em outras outras instituições de modo a ampliar essa verificação, fazendo um benchmarking e levantamento de boas práticas realizadas nas instituições públicas.

Como proposta de intervenção, conforme consta no Apêndice B deste trabalho, é apresentado um relatório de conformidade que aponta as lacunas e apresenta recomendações que podem colaborar para a melhoria da conformidade legal e fortalecer a segurança da informação na instituição.

Em conclusão, a UNIFAL-MG está trilhando um caminho certo para assegurar a conformidade com as exigências legais e proteger seus ativos informacionais. No entanto, há áreas que necessitam de aprimoramento contínuo e atenção especial para garantir uma gestão de segurança da informação eficaz e resiliente.

REFERÊNCIAS

ALBUQUERQUE JUNIOR, A. E.; SANTOS, E. M. Adoção de medidas de segurança da informação: um modelo de análise para institutos de pesquisa públicos. **Revista Brasileira de Administração Científica**, Aquidabã, v.5, n.2, p.46-59, 2014.

ARAÚJO, Wagner Junqueira de. Leis, decretos e normas sobre gestão da segurança da informação nos órgãos da administração pública federal. **Informação & Sociedade**: Estudos, [*s. l.*], v. 22, n. esp., p.13-24, 2012.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). **NBR ISO/IEC 27001**: Tecnologia da informação – Técnicas de segurança – Sistema de Gestão de segurança da informação – Requisitos. Rio de Janeiro: ABNT, 2013.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). **NBR ISO/IEC 27002**: Tecnologia da informação – Técnicas de segurança - Código de prática para a gestão da segurança da informação. Rio de Janeiro: ABNT, 2013.

BRASIL. Decreto nº 3.505, de 13 de junho de 2000. Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal. **Diário Oficial da União**, Brasília, DF, 14 jun. 2000. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto/d3505.htm. Acesso em: 24 ago. 2023.

BRASIL. Decreto nº 5.772, de 8 de maio de 2006. Aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão e das Gratificações de Exercício em Cargo de Confiança do Gabinete de Segurança Institucional da Presidência da República. **Diário Oficial da União**, Brasília, DF, 9 maio 2006. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2004-2006/2006/decreto/d5772.htm. Acesso em: 24 ago. 2023.

BRASIL. Decreto nº 7.845, de 14 de novembro de 2012. Regulamenta procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo, e dispõe sobre o Núcleo de Segurança e Credenciamento. **Diário Oficial da União**, Brasília, DF, 16 nov. 2012. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Decreto/D7845.htm. Acesso em: 24 ago. 2023.

BRASIL. Decreto nº 9.637, de 26 de dezembro de 2018. Institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação. **Diário Oficial da União**, Brasília, DF, 27 dez. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/decreto/D9637.htm. Acesso em: 24 ago. 2023.

BRASIL. Decreto nº 10.222, de 5 de fevereiro de 2020. Aprova a Estratégia Nacional de Segurança Cibernética. **Diário Oficial da União**, Brasília, DF, 6 fev. 2020. Disponível em:

http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/D10222.htm. Acesso em: 24 ago. 2023.

BRASIL. Decreto nº 10.641, de 2 de março de 2021. Altera o Decreto nº 9.637, de 26 de dezembro de 2018, que institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação. **Diário Oficial da União**, Brasília, DF, 3 mar. 2021. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/decreto/D10641.htm. Acesso em: 24 ago. 2023.

BRASIL. Decreto nº 10.748, de 16 de julho de 2021. Institui a Rede Federal de Gestão de Incidentes Cibernéticos. **Diário Oficial da União**, Brasília, DF, 19 jul. 2021. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/decreto/D10748.htm. Acesso em: 24 ago. 2023.

BRASIL. Decreto nº 11.331, de 1º de janeiro de 2023. Institui a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão e das Gratificações de Exercício em Cargo de Confiança do Gabinete de Segurança Institucional da Presidência da República. **Diário Oficial da União**, Brasília, DF, 1 jan. 2023. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2023-2026/2023/Decreto/D11331.htm. Acesso em: 24 ago. 2023.

BRASIL. Decreto nº 11.426, de 1º de março de 2023. Institui a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão e das Gratificações de Exercício em Cargo de Confiança do Gabinete de Segurança Institucional da Presidência da República. **Diário Oficial da União**, Brasília, DF, 2 mar. 2023. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2023-2026/2023/Decreto/D11426.htm. Acesso em: 24 ago. 2023.

BRASIL. **Instrução Normativa GSI No-1, de 13 de junho de 2008**. Disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, e dá outras providências. 2008. Disponível em: https://www.gov.br/governodigital/pt-br/legislacao/14_IN_01_gsidsic.pdf. Acesso em: 24 ago. 2023.

BRASIL. Instrução Normativa GSI/PR Nº 3, de 28 de maio de 2021. Dispõe sobre os processos relacionados à gestão de segurança da informação nos órgãos e nas entidades da administração pública federal. **Diário Oficial da União**, Brasília, DF, 31 maio 2021. Disponível em: https://www.in.gov.br/en/web/dou/-/instrucao-normativa-gsi/pr-n-3-de-28-de-maio-de-2021-322963172. Acesso em: 24 ago. 2023.

BRASIL. Lei nº 8.159, de 8 de janeiro de 1991. Dispõe sobre a política nacional de arquivos públicos e privados e dá outras providências. **Diário Oficial da União**, Brasília, DF, 9 jan. 1991. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8159.htm. Acesso em: 24 ago. 2023.

BRASIL. Lei nº 9.883, de 7 de dezembro de 1999. Institui o Sistema Brasileiro de Inteligência, cria a Agência Brasileira de Inteligência - ABIN, e dá outras providências. **Diário Oficial da União**, Brasília, DF, 8 dez. 1999. Disponível em: http://www.planalto.gov.br/ccivil_03/LEIS/L9883.htm. Acesso em: 24 ago. 2023.

BRASIL. Ministério do Planejamento, Orçamento e Gestão (MP). Controladoria-Geral da União (CGU). **Instrução Normativa Conjunta MP/CGU n. 01, de 2016**. 2016. Planejamento e Desenvolvimento Institucional. Disponível em: https://basedeconhecimento.cgu.gov.br/handle/1/295. Acesso em: 04 out. 2023.

BRASIL. Portaria GSI/PR Nº 93, de 18 de outubro de 2021. Aprova o glossário de segurança da informação. **Diário Oficial da União**, Brasília, DF, 19 out. 2021. Disponível em: https://www.in.gov.br/en/web/dou/-/portaria-gsi/pr-n-93-de-18-de-outubro-de-2021-353056370. Acesso em: 24 ago. 2023.

BRASIL. Tribunal de Contas da União. **Levantamento de pessoal de TI**. Brasília: TCU, 2015. (Sumário Executivo. Tecnologia da Informação).

CAVELTY, M. D.; BRUNNER, E. M. Introduction: information, power, and security: an outline of debates and implications. *In*: CAVELTY, M. D.; MAUER, V.; KRISHNA-HENSEL, S. F. **Power and security in the information age**: investigating the role of the state in cyberspace. Oxon: Routledge, 2007b. p. 1–18.

CASTELLS, M. **The rise of the network society**. Malden: Wiley-Blackwell, 1996.

DEY, M. Information security management: a practical approach. *In*: AFRICON CONFERENCE, 8., 2007, Windhoek, South Africa. **IEEE Xplore**, [*s. l.*], 2007. p. 1-6.

DHILLON, G. **Principles of information systems security**: texts and cases. [*S. l.*]: John Wiley & Sons, 2007.

DZAZALI, Suhazimah; HUSSEIN Zolait, Ali. Assessment of information security maturity: an exploration study of Malaysian public service organizations. **Journal of Systems and Information Technology**, [*s. l.*], v. 14, n. 1, p. 23-57, 2012.

ECO, U. **Semiótica e filosofia da linguagem**. São Paulo: Perspectiva, 2011.

ELLER, C.; RUST, L. F. A Relação entre tecnologia da informação e segurança da informação: uma revisão sistemática da literatura brasileira. **Gestão & Produção**, [*s. l.*], v. 26, n. 3, p. e4231, 2019.

FAGUNDES, L. L. Segurança da informação no Brasil: uma análise exploratória de seu estado atual e perspectivas. **Revista de Direito, Estado e Telecomunicações**, [*s. l.*], v. 7, n. 2, p. 12-37, 2015.

FENZ, S.; GOLUCH, G.; EKELHART, A.; RIEDL, B.; WEIPPL, E. Information security fortification by ontological mapping of the ISO/IEC 27001 Standard. *In*: PRDC 2007, 13., 2007. **Pacific Rim International Symposium on Dependable Computing**, [*s. l.*], 2007. p. 381 – 8.

FLORIDI, L**. Information**: a very short introduction. Oxford: Oxford University Press, 2010.

FONTES, Edison Luiz Gonçalves. **Segurança da informação**. São Paulo: Saraiva Educação, 2017.

FONTES, Edison Luiz Gonçalves. **Segurança da informação**: o usuário faz a diferença. 1. ed. São Paulo: Saraiva, 2010.

GAVIÃO, Luiz Octávio; SANTOS, Clarice Saraiva Andrade dos; OLIVEIRA, Leonardo Augusto dos Santos; PEREIRA, José Cristiano. Proposta de avaliação da política nacional de segurança da informação por processo de análise hierárquica. **Perspectivas em Ciência da Informação**, [*s. l.*], v. 27, n. 4, p. 108-145, out./dez. 2022.

GIL, Antônio Carlos. **Como elaborar projetos de pesquisa**. 4. ed. São Paulo: Atlas, 2002.

GIL. **Métodos e técnicas de pesquisa social**. 6. ed. São Paulo: Atlas, 2017.

GOODRICH, M. T.; TAMASSIA, R. **Introdução a segurança de computadores**. Porto Alegre: Bookman, 2013.

GUIMARÃES, Rogério; SOUZA NETO, João; LYRA, Mauricio Rocha. Modelo de governança de segurança da informação para a administração pública federal. **Perspectivas em Gestão & Conhecimento**, João Pessoa, v. 8, n. 3, p. 90-109, set./dez. 2018.

HINTZBERGEN, Jule *et al*. **Fundamentos de segurança da informação**: com base na ISO 27001 e na ISO 27002. Rio de Janeiro: Brasport, 2018.

HUMPHREYS, E. Information security management standards: compliance, governance and risk management. **Information Security Technical Report**, [*s. l.*], v. 13, n. 4, p. 247-255, 2008.

KARABACAK, B.; SOGUKPINAR, I. A quantitative method for ISO 17799 gap analysis. **Computers & Security**, [*s. l.*], v. 25, n. 6, p. 413-419, 2006.

LEMOS, A. **Cultura da conexão**: criatividade, emoção e direito no mundo contemporâneo. Porto Alegre: Sulina, 2018.

LUDKE, Menga; ANDRÉ, Marli Eliza Dalmazo Afonso de. **Pesquisa em educação**: abordagens qualitativas. São Paulo: EPU, 2013.

MARCONDES FILHO, C. **O Capital da informação**. São Paulo: Paulus, 2009.

MARCONI, Marina de Andrade; LAKATOS, Eva Maria. **Metodologia científica**. 7. ed. São Paulo: Atlas, 2017.

MARTINS, A.; ELOFF, J. H. P. Information security culture. *In*: GHONAIMY, M. A. *et al*. (ed.). **Security in the information society**. Boston, MA: Kluwer Academic Publishers, 2002. p. 203-214.

MCAFEE. **Grand theft data**: data exfiltration study: actors, tactics, and detection. 2017. Disponível em: https://www.mcafee.com/enterprise/en-us/assets/reports/rp-data-exfiltration.pdf. Acesso em: 03 ago. 2023.

MCGEE, A. R.; BASTRY, F. A.; CHANDRASHEKHAR, U.; VASIREDDY, S. R.; FLYNN, L. A. Using the Bell Labs security framework to enhance the ISO 17799/27001 information security management system. **Bell Labs Technical Journal**, [*s. l.*], v. 12, n. 3, p. 39-54, 2007.

MEIRELLES, Hely Lopes. **Direito administrativo brasileiro**. 45. ed. São Paulo: Malheiros, 2019.

MCLUHAN, M. **Understanding media**: the extensions of man. New York: McGraw-Hill, 1964.

MONTEIRO, I. **Proposta de um guia para elaboração de políticas de segurança da informação e comunicação em órgãos da APF**. 2009. Dissertação (Mestrado em Ciência da Computação) - Universidade de Brasília, Brasília, DF, 2009.

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

RADFAHRER, L. **A cultura da convergência**. 3. ed. São Paulo: Cengage Learning, 2016.

RECUERO, R. **Redes sociais na internet**. Porto Alegre: Sulina, 2014.

RIOS, O. K. L.; RIOS, V. P. S.; TEIXEIRA FILHO, J. G. A. Melhores práticas do COBIT, ITIL e ISO/IEC 27002 para implantação de política de segurança da informação em Instituições Federais do Ensino Superior. **Revista Gestão & Tecnologia**, Pedro Leopoldo, v. 17, n. 1, p. 130-153, jan./abr. 2017.

SAHIBUDIN, S.; SHARIFI, M.; AYAT, M. Combining ITIL, COBIT and ISO/IEC 27002 in order to design a comprehensive IT framework in organizations. *In*: ASIA INTERNATIONAL CONFERENCE ON MODELING & SIMULATIOn (AICMS), 2., 2008, Kuala Lumpur, Malaysia. **Proceedings**. Los Alamitos, California: CPS: IEEE, 2008. p. 749-753.

SHANNON, C. E. A mathematical theory of communication. **The Bell System Technical Journal**, New York, v. 27, n. 3, p. 379-423, 1948.

SILVEIRA, S. A. **Exclusão digital**: a miséria na era da informação. São Paulo: Fundação Perseu Abramo, 2007.

SOUZA, J. G. **Análise de tratamento de segurança da informação na gestão de riscos de governança de tecnologia da informação de uma instituição federal de ensino superior público federal**. 2017. Dissertação (Mestrado em Gestão e Tecnologia em Sistemas Produtivos) – Centro Estadual de Educação Tecnológica Paula Souza, São Paulo, 2017

SOUSA JÚNIOR, R. T.; ROCHA, A. R. Desafios e tendências para a segurança da informação no Brasil: um estudo exploratório. **RISTI-Revista Ibérica de Sistemas e Tecnologias de Informação**, [*s. l.*], n. 34, p. 16-30, 2020.

SYMANTEC. **Cyber Security Insights Report**: global results. [*S. l: s. n.*], 2018. Disponível em: https://www.nortonlifelock.com/content/dam/nortonlifelock/pdfs/reports/2017-ncsir-global-results-en.pdf. Acesso em: 24 ago. 2023.

UNIVERSIDADE FEDERAL DE ALFENAS (UNIFAL-MG). **Plano de Desenvolvimento Institucional - PDI**. Alfenas: UNIFAL-MG, 2021. Disponível em: https://www.unifal-mg.edu.br/planejamento/pdi-2021-2025-2/ Acesso em: 24 ago. 2023.

UNIVERSIDADE FEDERAL DE ALFENAS (UNIFAL-MG). **Comitê de Governança Digital - CGD**. Alfenas: UNIFAL-MG, 2024. Disponível em: https://www.unifal-mg.edu.br/portal/comite-de-governanca-digital/. Acesso em: 24 ago. 2023.

VERGARA, Sylvia Constant. **Projetos e relatórios de pesquisa em administração**. 16. ed. São Paulo: Atlas, 2016.

WEIDMAN, Jake; GROSSKLAGS, Jens. **What's in your policy? an analysis of the current state of information security policies in academic institutions**. 2018. Disponível em: https://aisel.aisnet.org/ecis2018_rp/23. Acesso em: 24 ago. 2023.

WHITMAN, M. E.; MATTORD, H. J. **Management of information security**. São Paulo: Cengage Learning, 2016.

WIENER, N. **Cybernetics**: or control and communication in the animal and the machine. Cambridge, MA: MIT Press, 1948.

APÊNDICE A – Busca Avançada dos Temas

Quadro 6 – Pesquisa pelos temas ‘segurança da informação’ e ‘conformidade legal’

(continua)

Autor(es)/Ano	Título do documento	Disponível em	Síntese
Pinto Filho, Jovino; Santa Rita, Luciana Peixoto; Pinto, Ibsen Mateus Bittencourt Santana. 2020	Política de Acesso à Informação nas Capitais Nordestinas: Análise do cumprimento da LAI pelo Poder Executivo Municipal	https://navus.sc.senac.br/navus/article/view/1357/pdf	Esta pesquisa teve o objetivo de verificar se o Poder Executivo das capitais nordestinas cumprem a Lei de Acesso à em seus sítios virtuais. O método utilizado foi quanti-qualitativo com desígnio exploratório-descritivo, por meio de investigação documental pesquisa bibliográfica, tendo como instrumento um formulário de observação com os requisitos determinados pela lei.
Nascimento, Eduardo Camargos Lagares do. 2012	Fatores culturais e estruturais que impactam na implantação da política de segurança da informação: um estudo de caso sobre o Ministério do Desenvolvimento Agrário	https://www.publicacoesacademicas.uniceub.br/gti/article/view/1681/1628	Os fatores culturais e estruturais estão entre os que mais implicam na adoção de fato de uma politica em segurança da informação no âmbito dos ministérios, o que tem se mostrado um grande desafio para as áreas gestoras dessa esfera. Ao considerar aspectos culturais, legais, estruturais, políticos e de recursos humanos, pode-se identificar o quão complexo e implantar qualquer tipo de campanha, politica ou governança.
Da Silva, Thaís Santos; De Rosso, Veridiana Vera; Speridião, Patrícia da Graça Leite. 2023	(In)segurança da rotulagem de alimentos infantis à base de cereais em relação à legislação brasileira vigente	https://www.e-publicacoes.uerj.br/demetra/article/view/72319/47306	Introdução: Os cereais são amplamente utilizados na alimentação das crianças. Objetivo: avaliar a composição nutricional e a rotulagem de alimentos infantis à base de cereais, em relação à legislação vigente. Material e Métodos: Estudo transversal, analítico e descritivo que avaliou alimentos à base de cereais, bem como a conformidade da rotulagem em relação à legislação brasileira vigente.
Costa, Alexsander Carvalho; Savino Filó, Maurício da Cunha. 2020	O conceito de privacidade diferencial em relação à reidentificação de dados pessoais	https://periodicos.uff.br/pragmatizes/article/view/41180/24694	O presente artigo tem por objetivo pesquisar uma das lacunas encontradas na Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018), que — se mal implementada em seu programa de conformidade — pode expor os dados de clientes e usuários. O problema de pesquisa se resume ao seguinte questionamento: há fragilidade na proteção de dados do cidadão, em razão dos mecanismos adotados pela legislação Brasileira? Num primeiro momento, tratou-se, brevemente, da anonimização de dados pessoais face à reidenticação, a fim de se poder tratar, posteriormente, da aplicação da privacidade diferencial.

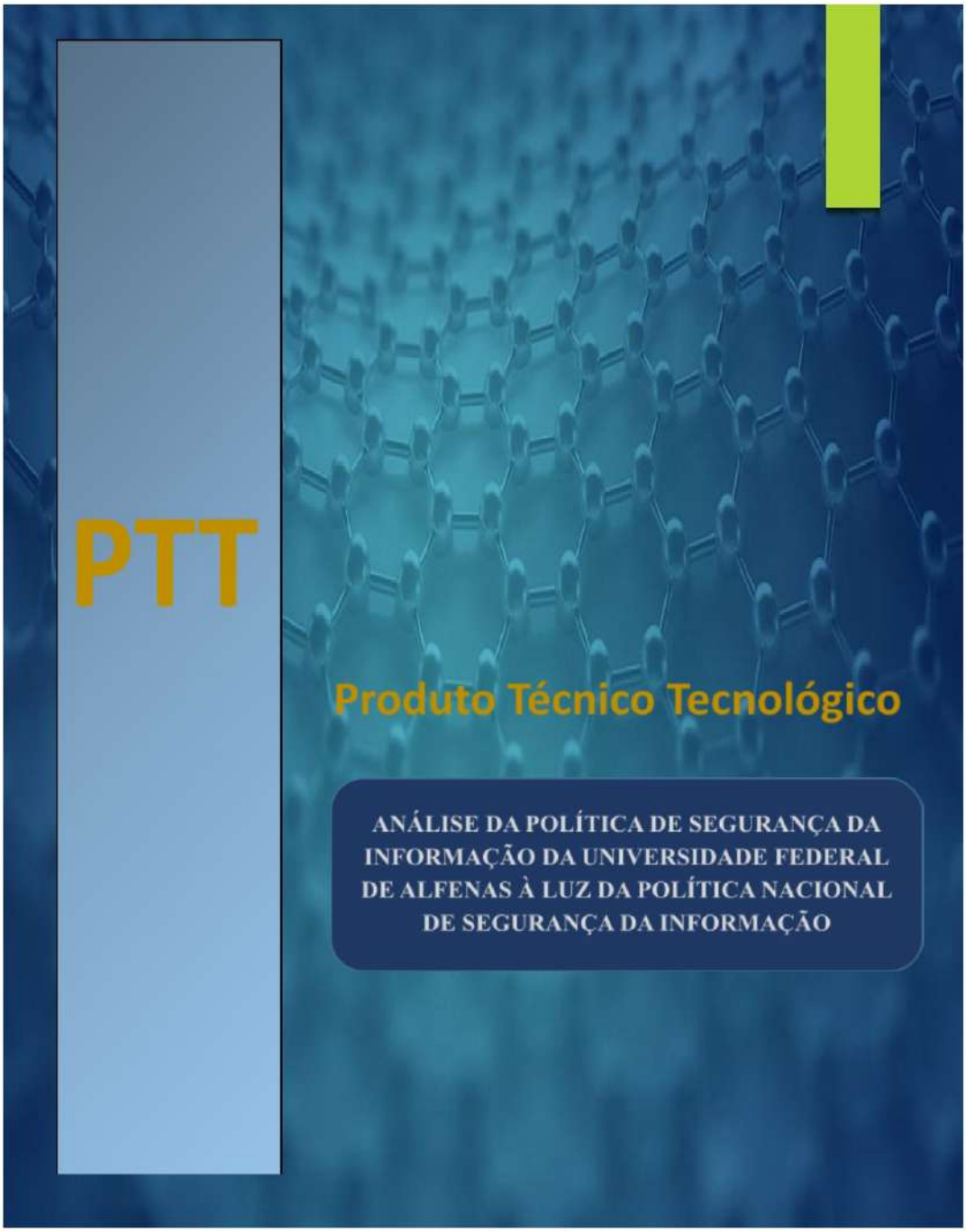
Quadro 6 – Pesquisa pelos temas ‘segurança da informação’ e ‘conformidade legal’

(conclusão)

Autor(es)/Ano	Título do documento	Disponível em	Síntese
Pinto, Anamelea De Campos; Silva, Júlio César Correia da; Mercado, Luis Paulo. 2019	DIÁLOGOS PERTINENTES ACERCA DA UTILIZAÇÃO DE RECURSOS EDUCACIONAIS ABERTOS PARA A EDUCAÇÃO	Acesso indisponível	A crescente profusão e difusão das tecnologias digitais de informação e comunicação (TDIC) possibilitaram a criação de novas práticas de ensino que incorporam a utilização de recursos multimidiáticos como facilitadores do processo de ensino e aprendizagem dos sujeitos conectados. Nesse sentido, os Recursos Educacionais Abertos (REA) surgem como uma proposta inovadora para o campo da educação e tem como objetivo constituir autores digitais mais responsáveis na edificação e partilha do conhecimento, possibilitando a engendração do conceito de abertura e liberdade face as especificidades do licenciamento em Creative Commons (CC) e as etapas de produção e execução dos REA.
De Santana Marins, Daniela; Mendes Kruschewsky Lordelo, Lidiane. 2023	ANÁLISE DAS ÁREAS AMBIENTALMENTE PROTEGIDAS NA BACIA DO RIO CAPIVARI EM CRUZ DAS ALMAS – BA A PARTIR DA UTILIZAÇÃO DOS DADOS DO CEFIR	Acesso indisponível	O Cadastro Ambiental Rural (CAR) é um instrumento de gestão ambiental criado pela Lei nº 12.651/12 em nível federal ou, em âmbito estadual na Bahia, denominado Cadastro Estadual Florestal de Imóveis Rurais. Seu principal objetivo é compilar informações sobre propriedades rurais, como Reserva Legal e Áreas de Preservação Permanente, para controle, monitoramento e planejamento ambiental e econômico, visando combater o desmatamento.
Rocha, Florisvaldo Silva. 2014	Editorial - Apresentação do Dossiê Educação a Distância	https://periodicos.ufs.br/edapeci/article/view/3612/pdf	Certamente Edgard Roquette-Pinto e Henry Morize[1] não imaginavam que suas ideias de levar educação e cultura aos lares brasileiros através das incipientes ondas do rádio, fossem embrionárias de um movimento que no século XXI assumiria proporções de tsunami, impulsionado tanto pelo surgimento de outras tecnologias da informação e da comunicação (TIC), quanto por sua diversificação e consequente difusão.
Pereira, Isadora Oliveira E.; Lemos, Lucas Brasileiro; Almeida, Paulo Henrique Ribeiro Fernandes; Lemos, Gisele Da Silveira. 2020	ERROS DE PRESCRIÇÃO E DISPENSAÇÃO DE ANTIMICROBIANOS EM UMA FARMÁCIA COMUNITÁRIA	https://periodicos2.uesb.br/index.php/rsc/article/view/5568/4678	Entende-se como prescrição o documento de cunho legal elaborado por profissionais de saúde, sujeito à legislação de controle e vigilância sanitária. Constitui uma importante ferramenta de comunicação entre profissionais e o paciente, que em presença de irregularidades pode proporcionar o uso incorreto de medicamentos. O objetivo deste estudo foi analisar erros de prescrição e dispensação de antimicrobianos em uma farmácia comunitária, de forma a verificar a frequência e fatores associados, de acordo com as legislações vigentes.

Fonte: Elaborado pelo autor (2024)

APÊNDICE B – Produto Técnico Tecnológico



PROFIAP
Mestrado Profissional em Administração Pública em rede

PROFIAP – UNIFAL-MG
Universidade Federal de Alfenas
Campus Varginha
Instituto de Ciências Sociais Aplicadas

Instituição afetada pela proposta
UNIFAL-MG - Universidade Federal de Alfenas

Professor Orientador
Prof. Paulo Roberto R. de Souza

Aluno Orientado
Giovani Augusto Ferreira

Data da apresentação
Agosto/2024

SUMÁRIO

RESUMO

Este relatório propõe uma intervenção na Universidade Federal de Alfenas (UNIFAL-MG) para resolver as questões de segurança da informação identificadas como não atendidas ou parcialmente atendidas, conforme os dispositivos legais do Decreto Nº 9.637/2018. A proposta abrange recomendações detalhadas para melhorar a conformidade legal e fortalecer a segurança da informação na instituição.

APRESENTAÇÃO

Título: Análise da política de segurança da informação da Universidade Federal de Alfenas à luz da Política Nacional de Segurança da Informação	
Ano: 2024	
A Produção é vinculada a Trabalho de Conclusão concluído? Sim	
Discente: Giovani Augusto Ferreira	
Tipo da produção: Técnica	**Subtipo de produção:** Serviços Técnicos
Natureza: Relatório Técnico	**Duração:** 12 meses
Número de Páginas: 11 páginas	**Disponibilidade:** Irrestrita
Instituição Financiadora: N/A	**Cidade:** Alfenas-MG
País: Brasil	**Divulgação:** Meio digital
Idioma: Português	

INSTITUIÇÃO/SETOR

Universidade Federal de Alfenas (UNIFAL-MG) / Comitê de Governança Digital (CGD), Núcleo de Tecnologia da Informação (NTI), e demais unidades envolvidas na gestão de segurança da informação.

PÚBLICO-ALVO DA INICIATIVA

- Gestores de Tecnologia da Informação
- Membros do Comitê de Governança Digital
- Equipe de Segurança da Informação
- Servidores e colaboradores da UNIFAL-MG

OBJETIVOS

Objetivo Geral

O objetivo desta intervenção é alinhar a UNIFAL-MG completamente com as diretrizes do Decreto Nº 9.637/2018, garantindo a total conformidade legal e fortalecendo a segurança da informação na instituição.

Objetivos Específicos

1. Assegurar a alocação adequada de recursos orçamentários para a segurança da informação.

2. Realizar ações de consolidação e análise dos resultados de auditorias sobre a gestão de segurança da informação.

3. Garantir a presença do gestor da segurança da informação e do representante da Secretaria-Executiva ou unidade equivalente no comitê de segurança.

4. Implementar um sistema de monitoramento contínuo e avaliação da política de segurança da informação.

5. Desenvolver e implementar um plano de execução de programas, projetos e processos relativos à segurança da informação.

6. Instituir controles internos robustos baseados na gestão de riscos de segurança da informação.

7. Formalizar e implementar um sistema de gestão de segurança da informação com comunicação imediata sobre vulnerabilidades ou incidentes.

8. Priorizar a interoperabilidade de tecnologias, processos, informações e dados.

9. Identificar e atender às necessidades da organização quanto aos requisitos de segurança da informação em sistemas de gestão.

ANÁLISE/DIAGNÓSTICO DA SITUAÇÃO-PROBLEMA

1. Recursos Orçamentários

◦ **Questão a ser tratada:** Recursos orçamentários para ações de segurança da informação estão parcialmente atendidos.

◦ **Dispositivo Legal:** Art. 15, inciso V.

◦ **Diagnóstico:** A alocação de recursos é insuficiente ou explicitamente alocada para cobrir todas as necessidades de segurança da informação, comprometendo a eficácia das medidas de proteção.

2. Auditorias

◦ **Questão a ser tratada:** Falta de ações de consolidação e análise dos resultados de auditorias sobre a gestão de segurança da informação.

◦ **Dispositivo Legal:** Art. 15, inciso IX.

◦ **Diagnóstico:** A ausência de auditorias regulares e análise de resultados impede a identificação de falhas e a implementação de melhorias contínuas em processos.

3. Composição do Comitê

◦ **Questão a ser tratada:** Falta de presença do gestor da segurança da informação e do representante da Secretaria-Executiva ou unidade equivalente no comitê de segurança.

◦ **Dispositivo Legal:** Art. 15, §1º, incisos I e II.

◦ **Diagnóstico:** A ausência desses membros críticos e no comitê prejudica a eficácia da governança nas ações em segurança da informação.

4. Monitoramento e Avaliação

◦ **Questão a ser tratada:** Falta de monitoramento do desempenho e avaliação da política de segurança da informação.

◦ **Dispositivo Legal:** Art. 17, inciso II.

◦ **Diagnóstico:** Sem monitoramento contínuo, é impossível avaliar a eficácia das políticas de segurança e fazer ajustes necessários em processos relacionados.

5. Planejamento de Programas

◦ **Questão a ser tratada:** Ausência de ações de planejamento da execução de programas, projetos e processos relativos à segurança da informação.

◦ **Dispositivo Legal:** Art. 17, inciso IV.

◦ **Diagnóstico:** A falta de planejamento impede a implementação eficaz de medidas de segurança, comprometendo a proteção de informações.

6. Controles Internos

◦ **Questão a ser tratada:** Falta de implementação de controles internos baseados na gestão de riscos de segurança da informação.

◦ **Dispositivo Legal:** Art. 17, inciso VII.

◦ **Diagnóstico:** A ausência de controles internos robustos deixa a instituição vulnerável a riscos de segurança não identificados.

7. Gestão de Segurança da Informação

◦ **Questão a ser tratada:** Falta de um sistema de gestão de segurança da informação com comunicação imediata sobre vulnerabilidades ou incidentes.

◦ **Dispositivo Legal:** Art. 17, incisos VIII e IX.

◦ **Diagnóstico:** A ausência desse sistema compromete a capacidade de resposta rápida a incidentes de segurança, aumentando o risco de danos.

8. Interoperabilidade

◦ **Questão a ser tratada:** Prioridade parcial na interoperabilidade de tecnologias, processos, informações e dados.

◦ **Dispositivo Legal:** Art. 17, §1º, inciso IV.

◦ **Diagnóstico:** A interoperabilidade limitada impede a integração eficaz dos sistemas, reduzindo a eficiência das operações com segurança.

9. Requisitos de Segurança em Sistemas de Gestão

◦ **Questão a ser tratada:** Identificação parcial das necessidades da organização quanto aos requisitos de segurança da informação em sistemas de gestão.

◦ **Dispositivo Legal:** Art. 17, §2º.

◦ **Diagnóstico:** A identificação inadequada das necessidades de segurança compromete a proteção dos sistemas de gestão, expondo a instituição a riscos.

PROPOSTA DE INTERVENÇÃO

1. Recursos Orçamentários

◦ **Questão a ser tratada:** Recursos orçamentários para ações de segurança da informação.

◦ **Dispositivo Legal:** Art. 15, inciso V.

◦ **Recomendação:** Garantir a destinação de orçamento específico e adequado para a segurança da informação. Justificar a alocação de recursos através de análises de risco e impacto para assegurar que os recursos sejam utilizados de forma eficiente e eficaz.

2. Auditorias

◦ Questão a ser tratada: Consolidação e análise dos resultados de auditorias sobre a gestão de segurança da informação.

◦ **Dispositivo Legal:** Art. 15, inciso IX.

◦ **Recomendação:** Implementar um programa regular de auditorias de segurança da informação interna e externa. Consolidar e analisar os resultados para identificar falhas e implementar melhorias contínuas. Publicar relatórios periódicos para garantir a transparência e a accountability.

3. Composição do Comitê

◦ **Questão a ser tratada:** Presença do gestor da segurança da informação e do representante da Secretaria-Executiva ou unidade equivalente no comitê de segurança.

◦ **Dispositivo Legal:** Art. 15, §1º, incisos I e II.

◦ **Recomendação:** Formalizar a designação e a participação do gestor da segurança da informação e do representante da Secretaria-Executiva no comitê. Atualizar o regimento do comitê para refletir essas mudanças e garantir sua implementação.

4. Monitoramento e Avaliação

◦ **Questão a ser tratada:** Monitoramento do desempenho e avaliação da política de segurança da informação.

◦ **Dispositivo Legal:** Art. 17, inciso II.

◦ **Recomendação:** Desenvolver e implementar um sistema de monitoramento contínuo do desempenho das políticas de segurança da informação. Realizar

avaliações periódicas e ajustes necessários para melhorar a eficácia das políticas.

5. Planejamento de Programas

◦ **Questão a ser tratada:** Planejamento da execução de programas, projetos e processos relativos à segurança da informação.

◦ **Dispositivo Legal:** Art. 17, inciso IV.

◦ **Recomendação:** Desenvolver um plano de ação detalhado para a execução de programas, projetos e processos de segurança da informação. Definir metas claras, responsabilidades e prazos para garantir a implementação eficaz das medidas de segurança.

6. Controles Internos

◦ **Questão a ser tratada:** Implementação de controles internos baseados na gestão de riscos de segurança da informação.

◦ **Dispositivo Legal:** Art. 17, inciso VII.

◦ **Recomendação:** Instituir controles internos robustos baseados em metodologias reconhecidas de gestão de riscos. Garantir que esses controles sejam revisados e atualizados regularmente para se manterem eficazes.

7. Gestão de Segurança da Informação

◦ **Questão a ser tratada:** Implementação de um sistema de gestão de segurança da informação com comunicação imediata sobre vulnerabilidades ou incidentes.

◦ **Dispositivo Legal:** Art. 17, incisos VIII e IX.

◦ **Recomendação:** Formalizar e implementar um sistema de gestão de segurança da informação com mecanismos de comunicação imediata sobre vulnerabilidades ou incidentes. Treinar a equipe para garantir uma resposta rápida e eficaz a qualquer incidente de segurança.

8. Interoperabilidade

◦ **Questão a ser tratada:** Prioridade na interoperabilidade de tecnologias, processos, informações e dados.

◦ **Dispositivo Legal:** Art. 17, §1º, inciso IV.

◦ **Recomendação:** Melhorar a interoperabilidade dos sistemas de segurança da informação. Garantir que tecnologias, processos, informações e dados sejam integrados de forma eficaz para aumentar a eficiência operacional e a segurança.

9. Requisitos de Segurança em Sistemas de Gestão

◦ **Questão a ser tratada:** Identificação das necessidades da organização

quanto aos requisitos de segurança da informação em sistemas de gestão.

◦ **Dispositivo Legal:** Art. 17, §2º.

◦ **Recomendação:** Realizar uma análise completa para identificar todas as necessidades de segurança da informação nos sistemas de gestão. Implementar as medidas necessárias para atender a essas necessidades e garantir a proteção adequada dos sistemas.

CONSIDERAÇÕES FINAIS

A implementação das recomendações propostas irá não só alinhar a UNIFAL-MG com as diretrizes do Decreto Nº 9.637/2018, mas também fortalecerá significativamente a segurança da informação da instituição. As ações sugeridas visam criar um ambiente mais seguro e resiliente, protegendo os dados institucionais e garantindo a continuidade dos serviços. A adoção dessas medidas promoverá uma cultura de segurança contínua e integrada, essencial para o sucesso e a sustentabilidade da UNIFAL-MG no cenário digital atual.

Essas recomendações, se implementadas, trarão benefícios a longo prazo, melhorando a segurança da informação e garantindo a conformidade legal da UNIFAL-MG. A participação ativa de todos os envolvidos e o compromisso com a melhoria contínua são fundamentais para o êxito desta proposta de intervenção.

ANEXO A – Pedido de Acesso à Informação

Plataforma Integrada de Ouvidoria e Acesso à Informação
Detalhes da Manifestação

Dados Básicos da Manifestação

Tipo de Manifestação:	Acesso à Informação
Esfera:	Federal
NUP:	23546.009740/2024-25
Órgão Destinatário:	UNIFAL-MG – Universidade Federal de Alfenas
Órgão de Interesse:	
Assunto:	Acesso à informação
Subassunto:	
Data de Cadastro:	26/01/2024
Situação:	Concluída
Data limite para resposta:	19/02/2024
Canal de Entrada:	Internet
Modo de Resposta:	Pelo sistema (com avisos por email)
Registrado Por:	096181
Tipo de formulário:	Acesso à Informação
Serviço:	
Outro Serviço:	

Teor da Manifestação

Resumo:	Solicitação relacionada a conformidade legal em segurança da informação
Extrato:	Solicito acesso a informação sobre as questões abaixo listadas, relacionadas à conformidade legal em segurança da informação na instituição, tomando por base o disposto no Capítulo VI, Seção IV do Decreto nº 9.637, de 26 de dezembro de 2018. Para cada questionamento sejam apresentados documentos comprobatórios e que se enquadram na definição de "controles internos da gestão" disposto na Instrução Normativa Conjunta MP/CGU nº 01/16, que dispõe sobre controles internos, gestão de riscos e governança no âmbito do Poder Executivo Federal, inciso V do Art. 2º: V – controles internos da gestão: conjunto de regras, procedimentos, diretrizes, protocolos, rotinas de sistemas informatizados, conferências e trâmites de documentos e informações, entre outros, operacionalizados de forma integrada pela direção e pelo corpo de servidores das organizações, destinados a enfrentar os riscos e fornecer segurança razoável de que, na consecução da missão da entidade, os seguintes objetivos gerais serão alcançados: a) execução ordenada, ética, econômica, eficiente e eficaz das operações; b) cumprimento das obrigações de accountability; c) cumprimento das leis e regulamentos aplicáveis; e d) salvaguarda dos recursos para evitar perdas, mau uso e danos. O estabelecimento de controles internos no âmbito da gestão pública visa essencialmente aumentar a probabilidade de que os objetivos e metas estabelecidos sejam alcançados, de forma eficaz, eficiente, efetiva e econômica; (BRASIL, 2016, p. 02). A partir do entendimento apresentado, os documentos podem

Plataforma Integrada de Ouvidoria e Acesso à Informação
Detalhes da Manifestação

ser considerados serão os atos administrativos e normativas internas da instituição tais como, e não se limitando a, portarias, resoluções do Comitê de Governança digital e de Conselho Universitário.

* Competências gerais dos órgãos e entidades da administração pública federal

1. Existe na instituição uma política de segurança da informação e normas internas de segurança em vigor?

2. Há um gestor de segurança da informação interno formalmente designado?

3. Existe um comitê de segurança da informação ou estrutura equivalente formalmente constituída?

4. São destinados recursos orçamentários para ações de segurança da informação?

5. São realizadas ações de capacitação e profissionalização dos recursos humanos em segurança da informação?

6. Existe uma equipe de prevenção, tratamento e resposta a incidentes cibernéticos formalmente instituída?

7. As equipes e comissões formalmente constituídas realizam ações coordenadas de segurança da informação?

8. São realizadas ações de consolidação e análise dos resultados de auditorias sobre a gestão de segurança da informação?

9. São aplicadas ações corretivas e disciplinares em casos de violação da segurança da informação?

* Composição do comitê de segurança da informação interno ou estrutura equivalente

1. Conta com a presença do gestor da segurança da informação?

2. Conta com a presença do representante da Secretaria-Executiva ou unidade equivalente.

3. Conta com a presença de um representante de cada unidade finalística.

4. Conta com a presença do titular da unidade de tecnologia da informação e comunicação.

* Requisitos para o gestor de segurança da informação

1. O servidor público designado tem formação ou capacitação técnica compatível?

* Edição de atos para funcionamento do comitê de segurança da informação

1. Existem atos publicados definindo a forma de funcionamento do comitê de segurança da informação?

* Competências da alta administração

1. São promovidas ações de simplificação administrativa, modernização da gestão pública e integração dos serviços

Plataforma Integrada de Ouvidoria e Acesso à Informação
Detalhes da Manifestação

públicos prestados pela instituição?

2. É realizado o monitoramento do desempenho e avaliação da política de segurança da informação?

3. São realizadas ações de planejamento da execução de programas, projetos e processos relativos à segurança da informação?

4. Estão formalmente estabelecidas as diretrizes para o processo de gestão de riscos de segurança da informação?

5. Há observância das normas estabelecidas pelo Gabinete de Segurança Institucional?

6. Há implementação de controles internos baseados na gestão de riscos de segurança da informação?

7. Há formalmente instituído e implementado um sistema de gestão de segurança da informação com mecanismo de comunicação imediata sobre vulnerabilidades ou incidentes de segurança?

8. Há observância de normas e procedimentos específicos aplicáveis?

* Planejamento e execução de programas de segurança da informação

1. Faz uso de recursos criptográficos adequados?

2. São realizadas ações para o aumento da resiliência dos ativos de tecnologia da informação e comunicação?

3. Existe cooperação entre as equipes de prevenção, tratamento e resposta a incidentes cibernéticos de outras instituições?

4. Há priorização na interoperabilidade de tecnologias, processos, informações e dados?

* Sistema de gestão de segurança da informação

1. São identificadas as necessidades da organização quanto aos requisitos de segurança da informação em sistemas de gestão?

* Incorporação das normas de segurança da informação estabelecidas pelo Gabinete de Segurança Institucional

1. As normas de segurança da informação são incorporadas aos atos administrativos envolvendo ativos de tecnologia da informação?

Proposta de melhoria:

Município do local do fato:

UF do local do fato:

Local:

Não há anexos originais da manifestação.

Plataforma Integrada de Ouvidoria e Acesso à Informação
Detalhes da Manifestação

Não há anexos complementares.

Não há textos complementares.

Não há envolvidos na manifestação.

Dados do Usuário

Tipo de identificação: Identidade Preservada

Login gov.br: Sim

Selos: Bronze - Cadastro via Balcão do INSS; Prata - Cadastro validado por Biometria Facial (Senatran); Bronze - Cadastro com validação de dados na Receita Federal; Prata - Cadastro validado em base de dados de servidores públicos da União

Nome: 096181

Campos Adicionais

Não há campos adicionais.

Dados das Respostas

Tipo de Resposta	Data/Hora	Teor da Resposta	Decisão
Resposta Conclusiva	19/02/2024 14:16	Agradecendo por seu contato, a Ouvidoria da UNIFAL-MG informa que sua manifestação foi analisada pelo setor pertinente e apresenta, no documento em anexo, a resposta. A Ouvidoria segue à sua disposição!	Acesso Concedido

Denúncia de descumprimento

Não há registro de denúncias de descumprimento.

Dados de Encaminhamento

Não há registros de encaminhamento.

Dados de Prorrogação

Não há registros de prorrogações.

Este documento é parte do processo 23087.000892/2024-17 e as respostas são baseadas no conhecimento que a Gerência de Segurança da Informação - GSI/NTI tem sobre as perguntas enviadas e que as mesmas podem divergir de respostas que forem enviadas pela Pró-Reitoria de Planejamento, Orçamento e Desenvolvimento Institucional, caso esta também responda.

- Competências gerais dos órgãos e entidades da administração pública federal

1. Existe na instituição uma política de segurança da informação e normas internas de segurança em vigor?

Sim.

Resolução Consuni 08/2018 - Aprova a Política de Segurança da Informação e Comunicação da UNIFAL-MG e dá outras providências.
Resolução CGD 02/2019 - Estabelece, no âmbito da Universidade Federal de Alfenas – UNIFAL-MG, diretrizes para o uso seguro dos perfis institucionais nas redes sociais (Resolução 12/2020 - Altera a Resolução CGD 02/2019).
Resolução CGD 03/2019 - Estabelece, no âmbito da Universidade Federal de Alfenas – UNIFAL-MG, diretrizes para gerenciamento e execução de cópias de segurança (backup), seu armazenamento e restauração.
Resolução CGD 01/2020 - Institui o Esquema de classificação de acesso e segurança no Sistema Eletrônico de Informações (SEI) no âmbito da Universidade Federal de Alfenas – UNIFAL-MG.
Resolução CGD 02/2020 - Estabelece as normas de uso do serviço de e-mail institucional da UNIFAL-MG (Resolução CGD 08/2020 - Altera a Resolução CGD 02/2020).
Resolução CGD 03/2020 - Estabelece as normas de uso de credenciais de acesso no âmbito da UNIFAL-MG.
Resolução CGD 04/2020 - Estabelece as normas de uso dos serviços disponíveis no GSuite for Education no âmbito da UNIFAL-MG.
Resolução CGD 05/2020 - Estabelece as diretrizes e normas para o uso dos serviços de armazenamento e compartilhamento de arquivos na UNIFALMG.
Resolução CGD 06/2020 - Estabelece Processo de Gestão de Riscos de Segurança da Informação no âmbito da UNIFAL-MG.
Resolução CGD 10/2020 - Estabelece as normas para adesão institucional a serviços de tecnologia de informação no âmbito da UNIFAL-MG.

2. Há um gestor de segurança da informação interno formalmente designado?

Sim

Conforme Resolução Consuni 10/2023 que altera a Resolução Consuni nº 80/2014, Art 17 - Parágrafo único.

3. Existe um comitê de segurança da informação ou estrutura equivalente formalmente constituída?

Sim

Conforme Regimento Interno do CGD:
https://www.unifal-mg.edu.br/portal/wp-content/uploads/sites/52/2021/07/007-2019-CGTI-revoga-res-112014_alt-resolucao-26.pdf

4. São destinados recursos orçamentários para ações de segurança da informação?

Não que esta Gerência tenha conhecimento. Existem recursos para Tecnologia da Informação que são utilizados em parte para a Segurança da Informação, mas não especificamente.

5. São realizadas ações de capacitação e profissionalização dos recursos humanos em segurança da informação?

Sim - Através de parceria com a ESR da RNP

6. Existe uma equipe de prevenção, tratamento e resposta a incidentes cibernéticos formalmente instituída?

Sim. Conforme Portaria nº 2252, de 2 de Dezembro de 2022:
https://sistemas.unifal-mg.edu.br/app/rh/gestaopessoas/relatorios/portaria.php?id=26186&tipo=html

7. As equipes e comissões formalmente constituídas realizam ações coordenadas de segurança da informação?

GSI - de acordo com regimento do NTI:
https://www.unifal-mg.edu.br/portal/wp-content/uploads/sites/52/2023/03/Resolucao-080-2014-aprovar-regimento-NTI-3736_alterada-pela-Res.-10_2023.pdf

ETIR - de acordo com Portaria nº 2252, de 2 de Dezembro de 2022:
https://sistemas.unifal-mg.edu.br/app/rh/gestaopessoas/relatorios/portaria.php?id=26186&tipo=html

CGD - de acordo com Regimento Interno do CGD (que também coordena a formulação de propostas de políticas de Segurança da Informação):
https://www.unifal-mg.edu.br/portal/wp-content/uploads/sites/52/2021/07/007-2019-CGTI-revoga-res-112014_alt-resolucao-26.pdf

8. São realizadas ações de consolidação e análise dos resultados de auditorias sobre a gestão de segurança da informação?

Ainda não há decisão formal ou plano aprovado para implementar.

9. São aplicadas ações corretivas e disciplinares em casos de violação da segurança da informação?

Conforme respectivas normas internas e externas, se necessário.

- Composição do comitê de segurança da informação interno ou estrutura equivalente

CGD - de acordo com Regimento Interno do CGD (que também coordena a formulação de propostas de políticas de Segurança da Informação): https://www.unifal-mg.edu.br/portal/wp-content/uploads/sites/52/2021/07/007-2019-CGTI-revoga-res-112014_alt-resolucao-26.pdf

1. Conta com a presença do gestor da segurança da informação?

Ainda não há decisão formal ou plano aprovado para implementar.

2. Conta com a presença do representante da Secretaria-Executiva ou unidade equivalente.

Não.

3. Conta com a presença de um representante de cada unidade finalística.

Sim.

4. Conta com a presença do titular da unidade de tecnologia da informação e comunicação.

Sim.

- Requisitos para o gestor de segurança da informação

1. O servidor público designado tem formação ou capacitação técnica compatível?

Sim. Conforme Resolução Consuni 10/2023 que altera a Resolução Consuni nº 80/2014, Art 17 - Parágrafo único.

- Edição de atos para funcionamento do comitê de segurança da informação

1. Existem atos publicados definindo a forma de funcionamento do comitê de segurança da informação?

Sim. De acordo com Regimento Interno do CGD (que também coordena a formulação de propostas de políticas de Segurança da Informação): https://www.unifal-mg.edu.br/portal/wp-content/uploads/sites/52/2021/07/007-2019-CGTI-revoga-res-112014_alt-resolucao-26.pdf

- Competências da alta administração

1. São promovidas ações de simplificação administrativa, modernização da gestão pública e integração dos serviços públicos prestados pela instituição?

Conforme Resolução 02/2022 - Institui o Plano de Transformação Digital da Universidade Federal de Alfenas.
https://www.unifal-mg.edu.br/portal/wp-content/uploads/sites/52/2022/12/Resolucao-CGD-N-02-2022.pdf

2. É realizado o monitoramento do desempenho e avaliação da política de segurança da informação?

Ainda não há decisão formal ou plano aprovado para implementar.

3. São realizadas ações de planejamento da execução de programas, projetos e processos relativos à segurança da informação?

Ainda não há decisão formal ou plano aprovado para implementar.

4. Estão formalmente estabelecidas as diretrizes para o processo de gestão de riscos de segurança da informação?

Resolução CGD 06/2020 - Estabelece Processo de Gestão de Riscos de Segurança da Informação no âmbito da UNIFAL-MG.

5. Há observância das normas estabelecidas pelo Gabinete de Segurança Institucional?

Sim. Ver citações nas normativas internas citadas ou em:
https://www.unifal-mg.edu.br/portal/comite-de-governanca-digital/
Ver também o último Relato Integrado publicado (página 126), disponível em:
https://www.unifal-mg.edu.br/planejamento/wp-content/uploads/sites/53/2023/05/Relato-Integrado-2022-Unifal-MG.pdf.pdf

6. Há implementação de controles internos baseados na gestão de riscos de segurança da informação?

Ainda não há decisão formal ou plano aprovado para implementar.

7. Há formalmente instituído e implementado um sistema de gestão de segurança da informação com mecanismo de comunicação imediata sobre vulnerabilidades ou incidentes de segurança?

Ainda não há decisão formal ou plano aprovado para implementar.

8. Há observância de normas e procedimentos específicos aplicáveis?

Sim. Conforme normativas internas citadas ou em:
https://www.unifal-mg.edu.br/portal/comite-de-governanca-digital/

- Planejamento e execução de programas de segurança da informação

1. Faz uso de recursos criptográficos adequados?

Sim. Conforme Resolução CGD 03/2020 - Estabelece as normas de uso de credenciais de acesso no âmbito da UNIFAL-MG.

2. São realizadas ações para o aumento da resiliência dos ativos de tecnologia da informação e comunicação?

Sim. Conforme último Relato Integrado publicado (páginas 126 a 131), disponível em:
https://www.unifal-mg.edu.br/planejamento/wp-content/uploads/sites/53/2023/05/Relato-Integrado-2022-Unifal-MG.pdf.pdf

3. Existe cooperação entre as equipes de prevenção, tratamento e resposta a incidentes cibernéticos de outras instituições?

Sim. Conforme Portaria nº 2252, de 2 de Dezembro de 2022:
https://sistemas.unifal-mg.edu.br/app/rh/gestaopessoas/relatorios/portaria.php?id=26186&tipo=html

4. Há priorização na interoperabilidade de tecnologias, processos, informações e dados?

Ainda não há decisão formal ou plano aprovado para implementar.

- Sistema de gestão de segurança da informação

1. São identificadas as necessidades da organização quanto aos requisitos de segurança da informação em sistemas de gestão?

Ainda não há decisão formal. Porém, há documentação informativa elaborada e disponível internamente, ofícios com indicações de boas práticas em desenvolvimento seguro.

- Incorporação das normas de segurança da informação estabelecidas pelo Gabinete de Segurança Institucional

1. As normas de segurança da informação são incorporadas aos atos administrativos envolvendo ativos de tecnologia da informação?

Sim. De acordo com citações nas normativas internas citadas ou em:
https://www.unifal-mg.edu.br/portal/comite-de-governanca-digital/
Ver também o último Relato Integrado publicado (página 126), disponível em:
https://www.unifal-mg.edu.br/planejamento/wp-content/uploads/sites/53/2023/05/Relato-Integrado-2022-Unifal-MG.pdf.pdf