INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA FLUMINENSE

PROGRAMA DE PÓS-GRADUAÇÃO EM SISTEMAS APLICADOS À ENGENHARIA E GESTÃO

Bruno Netto Barbosa Paixão

MMSI.BR: UMA PROPOSTA DE MODELO DE MATURIDADE EM SEGURANÇA DA INFORMAÇÃO

Campos dos Goytacazes / RJ
2020

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA FLUMINENSE

PROGRAMA DE PÓS-GRADUAÇÃO EM SISTEMAS APLICADOS À ENGENHARIA E GESTÃO

BRUNO NETTO BARBOSA PAIXÃO

MMSI.BR: UMA PROPOSTA DE MODELO DE MATURIDADE EM SEGURANÇA DA INFORMAÇÃO

DSc. Simone Vasconcelos Silva
(Orientadora)

Dissertação de Mestrado apresentada ao Programa de Pós-Graduação do Instituto Federal de Educação, Ciência e Tecnologia Fluminense, no Curso de Mestrado Profissional em Sistemas Aplicados à Engenharia e Gestão (MPSAEG), como parte dos requisitos necessários à obtenção do título de Mestre em Sistemas Aplicados à Engenharia e Gestão.

Campos dos Goytacazes / RJ
2020

Biblioteca Anton Dakitsch
CIP - Catalogação na Publicação

P149m Paixão, Bruno
MMSI.BR: UMA PROPOSTA DE MODELO DE MATURIDADE EM SEGURANÇA DA INFORMAÇÃO / Bruno Paixão - 2020.
190 f.: il. color.

Orientadora: Simone Vasconcelos Silva

Dissertação (mestrado) -- Instituto Federal de Educação, Ciência e Tecnologia Fluminense, Campus Campos Centro, Curso de Mestrado Profissional em Sistemas Aplicados à Engenharia e Gestão, Campos dos Goytacazes, RJ, 2020.
Referências: f. 116 a 119.

1. Segurança da informação. 2. Modelo de maturidade. 3. Privacidade. 4. LGPD. I. Vasconcelos Silva, Simone, orient. II. Título.

Elaborada pelo Sistema de Geração Automática de Ficha Catalográfica da Biblioteca Anton Dakitsch do IFF com os dados fornecidos pelo(a) autor(a).

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA FLUMINENSE

PROGRAMA DE PÓS-GRADUAÇÃO EM SISTEMAS APLICADOS À ENGENHARIA E GESTÃO

Bruno Netto Barbosa Paixão

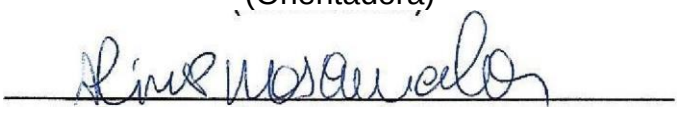
MMSI.BR: UMA PROPOSTA DE MODELO DE MATURIDADE EM SEGURANÇA DA INFORMAÇÃO

Dissertação de Mestrado apresentada ao Programa de Pós-Graduação do Instituto Federal de Educação, Ciência e Tecnologia Fluminense, no Curso de Mestrado Profissional em Sistemas Aplicados à Engenharia e Gestão (MPSAEG), como parte dos requisitos necessários à obtenção do título de Mestre em Sistemas Aplicados à Engenharia e Gestão.

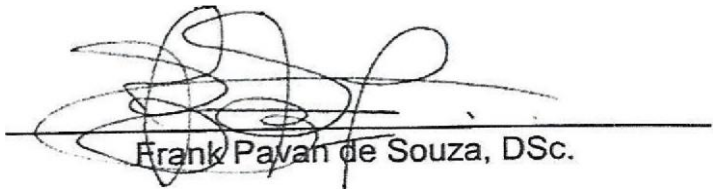
Aprovado em 29 de setembro de 2020.

Banca Examinadora

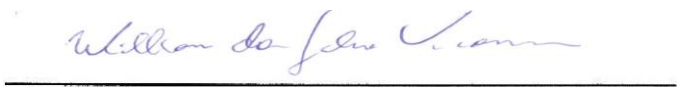
Simone Vasconcelos Silva, DSc.
Instituto Federal de Educação, Ciência e Tecnologia Fluminense
(Orientadora)



Aline Pires Vieira de Vasconcelos, DSc.
Instituto Federal de Educação, Ciência e Tecnologia Fluminense



Instituto Federal de Educação, Ciência e Tecnologia Fluminense



William da Silva Vianna, DSc.
Instituto Federal de Educação, Ciência e Tecnologia Fluminense

DEDICATÓRIA

A Deus por ter me concedido a sabedoria e disciplina necessárias para concluir este trabalho.

A minha esposa Juliana e as minhas filhas Sarah e Alice por todo apoio, carinho e amor que serviram como combustíveis para que eu pudesse me manter motivado e comprometido para alcançar o meu objetivo.

A minha mãe Maria Inês e a minha avó Rosa Maria por terem me ensinado os valores que carrego comigo até hoje e que me norteiam em minhas escolhas e ações.

AGRADECIMENTOS

Agradeço primeiramente a Deus por ter me capacitado e abençoado com saúde, sabedoria e resiliência para que eu pudesse superar os desafios e atingir este marco profissional. Ao Instituto Federal Fluminense pela oportunidade e aos meus professores pelos ensinamentos transmitidos ao longo da minha formação. Especialmente, a minha professora e orientadora, Simone Vasconcelos Silva agradeço a disponibilidade, ensinamentos e direcionamentos durante a orientação deste trabalho. À minha família e amigos manifesto gratidão eterna por terem me acompanhado durante toda a minha jornada profissional.

RESUMO

Os sistemas de informação estão se tornando cada vez mais acessíveis e integrados. Paralelamente, as redes de telecomunicações se expandem de forma acelerada para dar atender a demanda por serviços de tecnologia da informação (TI). Desta forma, as organizações se veem obrigadas a investirem em tecnologia para sobreviverem em um mercado globalizado, competitivo e de inovações disruptivas. Na era da informação, onde os dados tornaram-se um ativo fundamental para as organizações, a missão de proteger as informações e conhecimentos gerados a partir dos dados tornou-se talvez um dos maiores desafios enfrentados pelas empresas na atualidade. Devido a relevância e valor atribuído aos dados, o número de ataques e ameaças cibernéticas vem crescendo exponencialmente, provocando a capacidade das organizações em resguardar a confidencialidade das informações corporativas, bem como a privacidade de seus clientes e funcionários. Com o objetivo de otimizar a segurança da informação (SI) e privacidade nas organizações, a presente dissertação objetiva propor um novo modelo de maturidade em segurança da informação tendo como base as melhores práticas em SI e a Lei Geral de Proteção de Dados (LGPD). Para tanto, realizou-se inicialmente uma revisão da literatura com a análise de trabalhos correlatos, modelos de maturidade em segurança da informação e legislação com foco em privacidade. Em seguida, foi desenvolvido o modelo com base nas melhores práticas de privacidade e proteção de dados. Após, o modelo foi validado por meio de entrevistas baseadas em questionário semiestruturado com profissionais atuantes na área de segurança da informação e privacidade. A partir dos feedbacks recebidos, o modelo foi aprimorado e um novo questionário de avaliação de maturidade foi publicado. Os resultados das avaliações individuais foram enviados para os participantes com o objetivo de auxiliar estas organizações em seu processo de fortalecimento da segurança da informação e adequação à Lei Geral de Proteção de Dados. Conclui-se que o modelo proposto venha a se tornar uma referência para as organizações brasileiras, sobretudo a partir do aumento da preocupação em relação ao tema segurança cibernética após a pandemia do COVID-19 e a vigência da LGPD.

Palavras-chave: Segurança da informação, modelo de maturidade, privacidade, LGPD.

ABSTRACT

The Information systems are becoming increasingly accessible and integrated, in parallel telecommunications networks are expanding at an accelerated rate to accommodate the demand for information technology (IT) services. In this way, organizations are forced to invest in technology to survive in a globalized, competitive and disruptive innovation market. In the information age, where data has become a fundamental asset for organizations, the mission to protect the information and knowledge generated from data has become perhaps one of the biggest challenges facing companies today. Due to the relevance and value attributed to the data, the number of cyber-attacks and threats has been growing exponentially, calling into question the ability of organizations to safeguard the confidentiality of corporate information, as well as the privacy of their customers and employees. In order to optimize information security (IS) and privacy in organizations, this dissertation aims to propose a new maturity model for information security based on the best practices in IS and the Brazilian General Data Protection Law (LGPD). To this end, a literature review was initially carried out with the analysis of related works, maturity models in information security and legislation with a focus on privacy. Then, the model was developed based on the best privacy and data protection practices. Afterwards, the model was validated through interviews based on a semi-structured questionnaire with professionals working in the area of information security and privacy. Based on the feedbacks received, the model was improved and a new maturity assessment questionnaire was published. The results of the individual assessments were sent to the participants in order to assist these organizations in their process of strengthening information security and adapting to the LGPD. It is expected that the model will present itself as a reference for Brazilian organizations, mainly due to the increased concern regarding the cybersecurity theme after the COVID-19 pandemic and the LGPD.

Keywords: Information security, maturity model, LGPD.

FIGURAS

QUADROS

SIGLAS

ABNT	Associação Brasileira de Normas Técnicas
CCSMM	Community Cyber Security Maturity Model
CERT.br	Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil
CMM	Capability Maturity Model
COBIT	Control Objectives for Information and Related Technology
DDOS	Distributed Denial of Service
DOS	Denial of Service
DNS	Domain Name System
GDPR	General Data Protection Regulation
IOT	Internet of Things
IP	Internet Protocol
ISACA	Information Systems Audit and Control Association
ISO	International Standards Organization
LAN	Local Area Network
LGPD	Lei Geral de Proteção de Dados
PIB	Produto Interno Bruto
SGSI	Sistema de Gestão da Segurança da Informação
SI	Segurança da Informação
SQL	Structured Query Language
SSE-CMM	System Security Engineering Capability Maturity Model
TI	Tecnologia da Informação
XSS	Cross-site scripting
WAN	Wide Area Network

SUMÁRIO

1. INTRODUÇÃO

1.1. Contextualização

À luz da transformação digital, a tecnologia da informação (TI) tornou-se crucial no suporte, sustentabilidade e crescimento das organizações. Nos tempos atuais a criação de valor para as partes interessadas é frequentemente impulsionada pela digitalização e tecnologia empregadas em novos modelos de negócios que aliam processos eficientes e inovação. Sendo assim, as empresas estão cada vez mais dependentes da tecnologia para sobreviverem e se diferenciarem em mercado globalizado e competitivo (ISACA, 2019).

Na era da informação, os dados se tornaram o ativo mais importante para as empresas e a gestão da segurança da informação assumiu um papel fundamental para o sucesso destas. A maioria das organizações está conectada à Internet por razões comerciais e isso é um risco potencial devido aos ataques cibernéticos, hackers e violações de segurança e privacidade. As ameaças de segurança podem causar sérios impactos para a operação das empresas, tais como indisponibilidade de serviços, furto / manipulação de dados, sequestro de dados e sistemas corporativos. Para reduzir o seu nível de exposição e vulnerabilidades as empresas devem implementar medidas técnicas e organizacionais de proteção (SFORZA; STERLE, 2017).

No entanto, mesmo utilizando as melhores soluções tecnológicas e seguindo as boas práticas e normas de segurança as organizações não estão imunes a incidentes de segurança da informação, por isto devem estar cientes dos riscos e preparadas para administrar situações de crise, utilizando as melhores soluções tecnológicas para cada etapa do processo de gerenciamento de segurança cibernética. Crises estas como as violações que são relatados diariamente nos noticiários e que afetam todos os domínios do casual ao crítico. Como exemplo é possível citar o caso da Equifax em 2017, onde dados sensíveis e pessoais de 143 milhões de consumidores foram expostos, ocasionando uma multa de R$ 2,6 bilhões para a companhia de classificação de crédito como parte de um acordo com as autoridades dos Estados Unidos (WILLIAMS; MCGRAW; MIGUES, 2018).

Empresas gastam milhões de dólares na aquisição, implantação e desenvolvimento de soluções de SI, mas suas áreas de maior fragilidade e perdas permanecem sendo seus funcionários. Isto se deve à falta de conscientização, treinamentos e experiência na área segurança. Os ataques cibernéticos costumam ser bem sucedidos nas organizações onde há falta de qualificação ou número limitado de funcionários de TI empregados para acompanhar o ritmo contínuo de avanço da área de SI. Portanto, a realização de simulados, treinamentos e seleção adequada de funcionários é uma medida fundamental para todas as organizações reduzirem suas vulnerabilidades de SI. As organizações precisam estabelecer políticas e promover o entendimento do pessoal de todos os níveis, para que estejam cientes de seus papéis e responsabilidades na proteção contra ameaças à segurança (DOUCEK et al., 2019).

A definição de segurança cibernética evoluiu bastante nas últimas décadas, a partir do conceito fundamental que é definido como a qualidade ou o estado de segurança que é estar livre de perigo. Portanto, a segurança cibernética pode ser vista como um sistema de processos e soluções tecnológicas que protegem os recursos e usuários do espaço cibernético de ameaças. Para acompanhar a inovação tecnológica, o ciberespaço cresceu para incluir redes sociais, nuvens, *Internet of Things* [1](IOT), cidades inteligentes, redes inteligentes e outros sistemas definidos por software (LE; HOANG, 2017).

Muitos sistemas de informação não têm sido projetados para serem seguros, a segurança que pode ser alcançada através de meios técnicos é limitada e está apoiada por procedimentos e gerenciamentos apropriados. A identificação de quais controles devem ser implementados requer planejamento e atenção cuidadosa em nível de detalhes. Um sistema de gestão da segurança da informação bem-sucedido requer apoio de todos os funcionários da organização. Isto pode também exigir a participação de acionistas, fornecedores ou outras partes externas. Orientações de especialistas externos podem também ser necessárias. De um modo geral, uma segurança da informação eficaz também garante à direção e a outras partes interessadas que os ativos da organização estão razoavelmente seguros e protegidos

[1] Internet das coisas é um conceito que se refere à interconexão digital de objetos cotidianos com a internet, conexão dos objetos mais do que das pessoas. Em outras palavras, a internet das coisas nada mais é que uma rede de objetos físicos capaz de reunir e de transmitir dados.

contra danos, agindo como um facilitador dos negócios (ABNT NBR ISO/IEC 27002, 2013).

Nos últimos anos a partir dos movimentos disruptivos de inovação tecnológica e com o surgimento de novos serviços de tecnologia a privacidade de dados pessoais ganhou destaque, contudo foi vista como um obstáculo à inovação, onde a alegação era que esta aumentava os custos de governança de dados sem fornecer benefícios reais. Todavia, a privacidade passou a ser adotada como facilitadora da inovação, uma vez que a confiança do consumidor é fundamental para a realização de negócios com produtos e serviços orientados a dados na internet. As organizações estão fazendo uso de ferramentas para proteger a privacidade de seus clientes por perceberem que podem se beneficiar de uma abordagem proativa à proteção de dados, criando confiança e demonstrando a responsabilidade no processamento de dados pessoais (FRIEDEWALD et al., 2020).

Há vários desafios para as organizações associados a privacidade digital, como compartilhamento de dados de forma segura, controle responsável de dados, prestação de contas ou transparência (tanto em relação aos órgãos reguladores bem como aos usuários). No contexto da tecnologia, podemos discutir privacidade, direitos de dados e segurança cibernética como três áreas essenciais para a manutenção da liberdade e dignidade dos indivíduos. Deste modo, as Leis de proteção à privacidade de dados pessoais foram criadas para assegurar a defesa do direito humano fundamental a privacidade (MICHAEL et al., 2019) .

A privacidade e a proteção de dados são dois domínios diferentes quando avaliados os alvos e partes interessadas, contudo não há privacidade sem proteção de dados. A proteção de dados consiste na implementação de medidas técnicas e organizacionais para manter a segurança da informação, onde o trabalho neste domínio é realizado principalmente por técnicos e os principais objetivos são o gerenciamento e mitigação de riscos nas organizações, utilizando as melhores práticas documentadas e padrões internacionais. A privacidade diz respeito à proteção dos direitos fundamentais dos cidadãos, os chamados titulares de dados, sendo dirigida principalmente por advogados. A avaliação de risco e tratamentos são focados nos titulares dos dados e não nas organizações. Todavia, as medidas de segurança implementadas devem estar alinhadas ao negócio sendo eficazes para assegurar a privacidade dos titulares dos dados (MEINTS, 2009).

A forma como as instituições lidam com a segurança cibernética e a privacidade de dados pessoais é essencial para estabelecer um controle eficaz, eficiente e sustentável. Para que as organizações possam melhorar a segurança cibernética, a indústria e a comunidade técnica desenvolveram modelos de maturidade em segurança da informação capazes de medir os níveis segurança cibernética das empresas e classificá-las em diferentes categorias para a melhoria contínua. Portanto, é necessário que as organizações identifiquem quais são os principais modelos de maturidade de segurança da informação existentes no mercado e busquem se adequar aos mesmos (REA-GUAMAN et al., 2017).

As organizações necessitam de avaliações de segurança da informação periódicas para testar seus controles e determinar a sua conformidade com um modelo de maturidade de segurança da informação ou métricas específicas e predefinidas. A avaliação de segurança pode permitir à organização aumentar a eficiência e desempenho, uma vez que é muito importante na organização o gerenciamento e planejamento. A classificação de segurança em organizações deve basear-se na análise de seus controles e maturidade. O modelo de maturidade é considerado uma das ferramentas para avaliação de desempenho e segurança na organizações (GHAFFARI; ARABSORKHI, 2018).

1.2. **Justificativa**

Organizações de todos os tipos e tamanhos (incluindo o setor privado e público, organizações comerciais e sem fins lucrativos), coletam, processam, armazenam e transmitem informações em diferentes formatos, incluindo o eletrônico, físico e verbal (por exemplo, conversações e apresentações). O valor da informação vai além das palavras escritas, números e imagens: conhecimento, conceitos, ideias e marcas são exemplos de formas da informação. Deste modo, um incidente de segurança pode comprometer significativamente o negócio de uma organização, bem como gerar prejuízos intangíveis para a sua marca. Por isso é crucial que os controles de segurança nas organizações sejam efetivos de modo a assegurar a confidencialidade, autenticidade, integridade, disponibilidade e irretratabilidade de suas informações (ABNT NBR ISO/IEC 27002, 2013).

Os crimes cibernéticos têm custado caro a economia global, em 2018 foram quase 600 bilhões de dólares, o que correspondeu a 0,8% do PIB global. O relatório "*The Economic Impact of Cybercrime: No Slowing Down*" (O impacto econômico do crime cibernético: sem indícios de desaceleração) dá prosseguimento ao popular relatório de 2014 que quantificou as perdas globais na ordem de 500 bilhões de dólares, o equivalente a 0,7% da receita global na época. O mesmo estudo apontou que as perdas das empresas brasileiras com crimes virtuais foram de 10 bilhões de dólares (32,4 bilhões de reais) por ano, sendo o Brasil a segunda maior fonte de ataques virtuais no mundo, ficando apenas atrás da China no Ranking (CSIS; MCAFEE, 2018)

Ainda, segundo o estudo, os alvos preferenciais são as instituições financeiras, afetadas por problemas como sites falsos, cartões clonados e malwares direcionados. Os crimes virtuais são responsáveis por 95% das perdas financeiras dessas companhias. Um fato constatado na pesquisa é que no caso do Brasil, chama a atenção que a maioria (54%) dos ataques tem origem no próprio país, enquanto em outras nações, a origem é internacional. Isso indica que há uma "expertise" nacional do crime.

Os incidentes de segurança da informação têm crescido no Brasil segundo estatísticas do CERT.br, Grupo de Resposta a Incidentes de Segurança para a Internet no Brasil, mantido pelo NIC.br do Comitê Gestor da Internet no Brasil. O órgão atua como ponto central para notificações de incidentes de segurança no país, provendo a coordenação e o apoio no processo de resposta a incidentes e, quando necessário, colocando as partes envolvidas em contato. O CERT.br também atua através do trabalho de conscientização em segurança e com análise de tendências e correlação entre eventos na Internet brasileira. A Figura 1 apresenta o total de incidentes reportados por ano no Brasil.

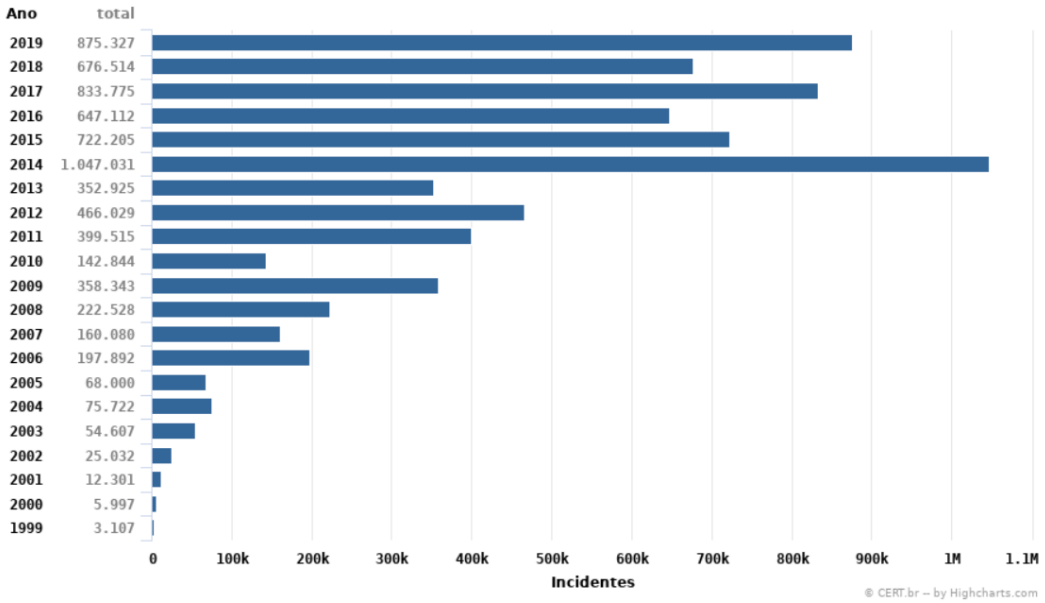


Figura 1: Total de Incidentes reportados por Ano. Fonte: CERT.BR (2020).

Além da preocupação das empresas brasileiras com a segurança da informação, se faz necessária a adequação das mesmas a Lei Geral de Proteção de Dados (LGPD), sancionada em agosto de 2018 que dispõe sobre o tratamento de dados pessoais por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade, bem como o livre desenvolvimento da personalidade da pessoa natural. A Lei brasileira se aplica a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam armazenados os dados, contanto que eles sejam de pessoas brasileiras (DARYUS, 2020).

Segundo pesquisa realizada pela Serasa Experian (2019), 85% das empresas brasileiras afirmaram que ainda não estavam preparadas para garantir os direitos e deveres em relação ao tratamento de dados pessoais exigidos pela Lei de Proteção de Dados (LGPD). Os resultados da pesquisa realizada foram obtidos a partir de entrevista com executivos (Gerentes, Diretores e C-level) de 508 companhias de 18 ramos de atividades, com diferentes portes e atuação nos segmentos B2C[2] e B2B[3]. Em relação aos impactos em tecnologia nas organizações para adequação à Lei Geral

[2] *Business-to-consumer*, B2C, também *business-to-customer*, é o comércio efetuado diretamente entre a empresa produtora, vendedora ou prestadora de serviços e o consumidor final.
[3] *Business-to-business*, expressão identificada pela sigla B2B, é a denominação do comércio estabelecido entre empresas.

de Proteção de dados é esperado que sejam muito significativos por 40,2 % das empresas entrevistadas conforme demonstra o Quadro 1.

Quadro 1: Impacto esperado em tecnologia para adequação à LGPD. Fonte: Serasa Experian (2019).

	Financeiro (bancos, financeiras, seguradoras e corretoras (%)	Comércio e Varejo (%)	Construção e Engenharia (%)	Saúde e Hospitalar (%)	Serviços (%)	Tecnologia (%)	Outros (%)	Média Geral (%)
Muito significativo	45,5	43,9	41,9	47,8	37	43,8	31,3	40,2
Algum impacto	36,4	30,9	19,4	26,1	35,9	45,8	28,1	32,9
Baixo	13,6	15,4	32,3	8,7	13	4,2	18,8	15,4
Não haverá impacto	0	4,1	3,2	8,7	9,8	2,1	10,9	6,1
Não sei	4,5	5,7	3,2	8,7	4,3	4,2	10,9	5,5

Os resultados da pesquisa demonstram ainda que 72% das companhias entrevistadas com mais de 100 funcionários pretendem contratar uma pessoa de mercado especializada ou uma consultoria/assessoria para se adequarem à primeira lei federal voltada exclusivamente à proteção de dados conforme demonstrado na Figura 2.

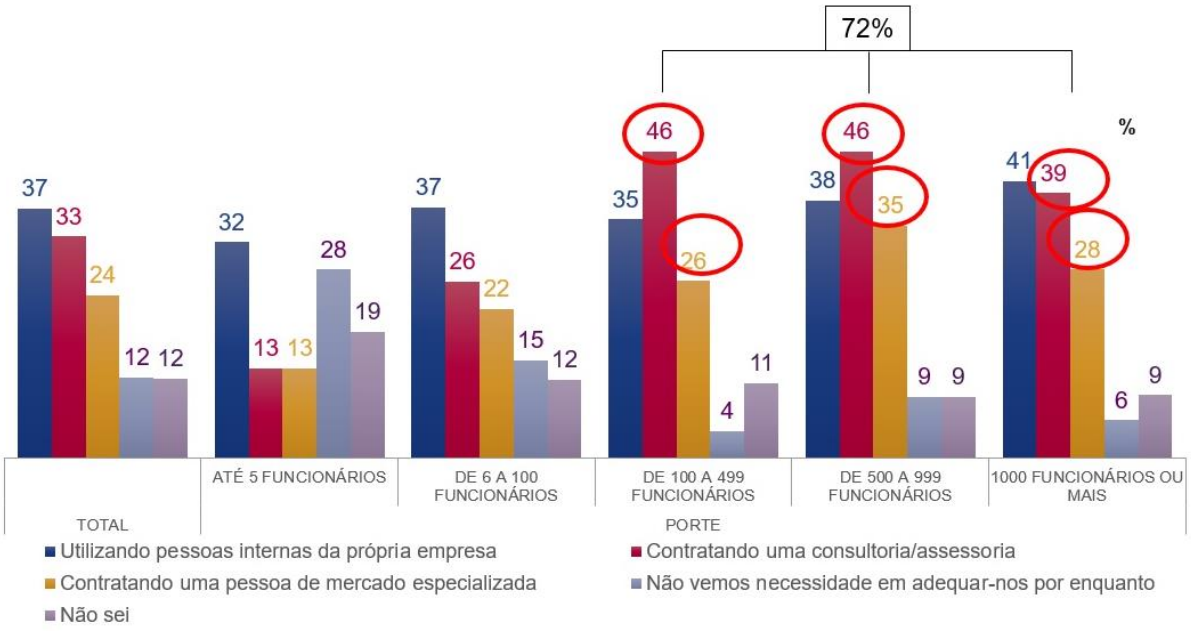


Figura 2: Estratégia de adequação à LGPD das empresas brasileiras. Fonte: Serasa Experian (2019).

A criticidade da segurança da informação para o bom funcionamento das atividades econômicas e empresarias, a importância da adequação das organizações brasileiras a Lei Geral de Proteção de Dados e a observância dos padrões e boas práticas de segurança norteiam e justificam o desenvolvimento deste trabalho. Onde é proposto um modelo de maturidade para otimização da privacidade e proteção de dados nas organizações.

O modelo proposto estabelece os critérios para a sua aplicação prática, visando propiciar uma análise de maturidade das instituições avaliadas no que tange aos seus processos e controles relacionados à segurança da informação, bem como aspectos de gestão da privacidade da informação com base nas normas ABNT NBR ISO/IEC 27001:2013, ABNT NBR ISO/IEC 27002:2013 e ABNT NBR ISO/IEC 27701:2019 respectivamente, bem como a sua aderência à Lei Geral de Proteção de Dados Nº 13.709, de 14 de Agosto de 2018.

Diferente dos outros modelos de maturidade em segurança da informação existentes, o modelo intitulado MMSI.br (Modelo de Maturidade em Segurança da Informação Brasileiro) tem como foco o cenário brasileiro e se apresenta como uma referência capaz de nortear as organizações nacionais para avaliação e otimização dos seus controles de segurança da informação, mecanismos de gestão da privacidade e proteção de dados pessoais.

1.3. **Objetivos**

O presente trabalho tem por objetivo propor um novo modelo de maturidade em segurança da informação com foco em proteção de dados e privacidade voltado para organizações brasileiras que buscam se adequar à Lei Geral de Proteção de Dados (LGPD).

Os objetivos específicos são:

- Elaborar o modelo de maturidade de segurança da informação com foco na realidade das empresas brasileiras;
- Realizar uma avaliação pública para que organizações possam avaliar o seu nível de aderência em relação ao modelo proposto, bem como sugerir melhorias. E enviar o feedback aos participantes da avaliação, contendo os resultados individuais obtidos.

1.4. **Estrutura do trabalho**

O trabalho foi organizado em seis capítulos dispostos de acordo com a estrutura apresentada a seguir:

No Capítulo 2 é realizada a fundamentação teórica com o descritivo do cenário atual de segurança cibernética, a explanação dos conceitos relacionados à segurança da informação, modelos de maturidade de segurança da informação, leis e regulamentos relacionados a privacidade e trabalhos relacionados.

No Capítulo 3 é apresentada a estruturação da metodologia, bem como as ferramentas e técnicas utilizadas para a realização do trabalho.

O Capítulo 4 apresenta o modelo de maturidade em segurança da informação que é objeto deste trabalho.

O Capítulo 5 é dedicado a apresentação dos resultados da aplicação do modelo de maturidade em segurança da informação proposto através de uma pesquisa realizada com organizações.

O último capítulo descreve uma breve conclusão sobre o trabalho realizado, os benefícios que o trabalho pode trazer para as organizações, limitações e sugestões para trabalhos futuros.

2. REVISÃO BIBLIOGRÁFICA

2.1. Cenário atual de segurança da informação

A pandemia do COVID-19 tornou-se a partir de novembro de 2019 o assunto mais importante no cenário global e teve associado um surto de crimes cibernéticos em todo o mundo. Com a necessidade de isolamento social a dependência por ambientes virtuais cresceu significativamente, onde a convergência entre a tecnologia, computação e dispositivos de comunicação transformou radicalmente a maneira como as pessoas estão se socializando e trabalhando. Sistemas computacionais tornaram-se vitais para que as organizações continuem a operar, possibilitando que seus funcionários continuem a trabalhar remotamente (NAIDOO, 2020).

Ainda segundo Naidoo (2020) várias organizações tiveram que se adequar repentinamente para implementar o regime de trabalho Home Office para seus colaboradores, onde a prioridade era preparar os usuários para retomarem as suas atividades laborais o mais rápido possível, isto culminou em vulnerabilidades de segurança devido a disponibilização de soluções tecnológicas para trabalho remoto de forma abrupta e inadequada. Muitos colaboradores estão trabalhando sem as proteções de segurança habitualmente fornecidas antes da pandemia nas instalações físicas da organização.

Durante a crise humanitária causada pelo corona vírus, os cibercrimes estão aumentando exponencialmente, pois criminosos tem se aproveitado do cenário para aplicar golpes e cometer fraudes via *phishing* e engenharia social associados a pandemia do COVID-19. O tema tem sido explorado massivamente e a falta de percepção de risco por parte de usuários inadvertidos, bem como a dependência por redes de comunicação eletrônica e sistemas de informação tem contribuído para o aumento da efetividade dos ataques. Somente no mês de março de 2020 houve um crescimento de ataques cibernéticos ao redor do mundo de cinco vezes se comparado ao mês anterior. Ainda no mesmo período, foram rastreados mais de 42.000 sites suspeitos com domínios contendo "COVID" e "corona" (HAWDON; PARTI; DEARDEN, 2020).

2.2. **Conceitos de segurança da informação**

A segurança da informação é alcançada pela implementação de um conjunto adequado de controles, incluindo políticas, processos, procedimentos, estrutura organizacional e funções de software e hardware. Estes controles precisam ser estabelecidos, implementados, monitorados, analisados criticamente e melhorados, quando necessário, para assegurar que os objetivos do negócio e a segurança da informação da organização sejam atendidos. Um sistema de gestão da segurança da informação (SGSI) considera uma visão holística e coordenada dos riscos de segurança da informação da organização, para implementar um conjunto de controles de segurança da informação detalhado, com base na estrutura global de um sistema de gestão coerente (ABNT NBR ISO/IEC 27002, 2013).

Ainda segundo a abordagem de processo para a gestão da segurança da informação, apresentada na norma ABNT NBR ISO/IEC 27002:2013 intitulada “Código de prática para controles de segurança da informação”, inclui a importância de:

- Compreender os requisitos de segurança da informação da organização e a necessidade de estabelecer políticas e objetivos para a segurança da informação;
- Implementar e operar controles para gerenciar os riscos de segurança da informação da organização no contexto dos riscos gerais de negócio da organização;
- Monitorar e revisar o desempenho e a eficácia do Sistema de Gerenciamento de Segurança da Informação (Information Security Management System – ISMS);
- Melhoria contínua baseada em medições objetivas.

O sistema de gestão da segurança da informação é responsável por preservar a confidencialidade, integridade e disponibilidade da informação por meio da aplicação de um processo de gestão de riscos e fornece confiança para as partes interessadas de que os riscos são adequadamente gerenciados. É fundamental que um sistema de gestão da segurança da informação seja parte de, e esteja integrado com, os processos da organização e com a estrutura de administração global, e que a

segurança da informação seja considerada no projeto dos processos, sistemas de informação e controles (ABNT NBR ISO/IEC 27001, 2013).

Um programa de segurança pode ter diversos objetivos, mas os princípios mais importantes são a confidencialidade, integridade e disponibilidade. Estes pilares são referidos como o triângulo CID (Figura 3). O nível de segurança requerido para executar esses princípios é diferente para cada empresa, pois cada uma tem sua própria combinação de objetivos e requisitos de negócio e de segurança. Todos os controles de segurança, mecanismos e proteções são implementados para prover um ou mais desses princípios, e todos os riscos, ameaças e vulnerabilidades são medidos pela sua capacidade potencial de comprometer um ou todos os princípios do triângulo CID (HINTZBERGEN et al., 2018)

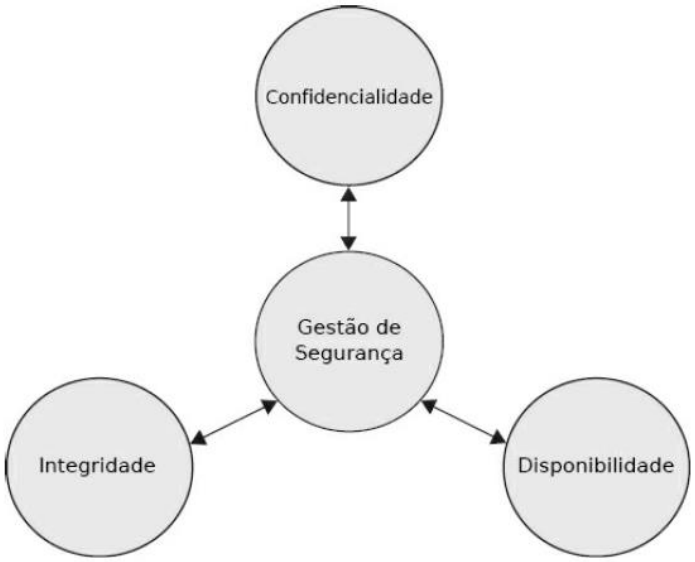


Figura 3: Triângulo CID. Fonte: (HINTZBERGEN et al., 2018)

Ainda segundo o mesmo autor, os princípios do triângulo CID são descritos a seguir:

- Confidencialidade – Toda informação deve ser protegida de acordo com o grau de sigilo de seu conteúdo, visando limitar seu acesso e uso às pessoas a quem é destinada.

- Integridade – Toda informação deve ser mantida na condição em que foi disponibilizada por seu proprietário, visando protegê-la contra alterações indevidas, intencionais ou acidentais.

- Disponibilidade – Toda informação gerada ou adquirida por um indivíduo ou instituição deve estar disponível para seus usuários, quando eles necessitem delas para qualquer finalidade.

Apesar do consenso de que esses elementos formam a tríade que a segurança da informação, os princípios da autenticidade e o não repúdio são aspectos essenciais para a consecução dos objetivos da segurança da informação. As propriedades adicionais supracitadas são descritas conforme a norma ISO/IEC 27000 (2018).

- Autenticidade – Garantia de que a informação seja proveniente da fonte à qual ela é atribuída.

- Irretratabilidade da comunicação (não repúdio) – Proteção contra a alegação por parte de um dos participantes de uma comunicação de que não ocorreu.

Esses atributos da informação são atômicos, no sentido de que não são divididos em outras partes constituintes, isto é não se sobrepõem e se referem a aspectos únicos da informação. Qualquer violação da segurança da informação pode ser descrita como aquilo que afeta um ou mais desses atributos fundamentais da informação.

A compreensão da segurança da informação, além dos conceitos primários já explanados, perpassa o entendimento de conceitos secundários que a circundam em todo o seu processo de proteção à informação, estes são apresentados no Quadro 2.

Quadro 2: Conceitos e definições de segurança da informação. Fonte: (ISO/IEC 27000, 2018)

Conceito	Definição
Ativo	Qualquer coisa que tenha valor para a organização. Tais como instalações, informação (digital ou impressa), software, hardware. mas também em pessoas, habilidades, experiência e coisas intangíveis, como reputação e imagem.

Ataque	Tentar destruir, expor, alterar, desativar, roubar ou obter acesso não autorizado ou fazer uso não autorizado de um ativo.
Vulnerabilidade	Fraqueza de um ativo ou controle que pode ser explorada por uma ou mais ameaças.
Ameaça	Causa potencial de um incidente indesejado, a qual pode resultar no dano a um sistema ou organização.
Informação	É o dado que tem significado em algum contexto para quem o recebe. Após processamento, o dado pode ser entendido como informação.
Risco	Efeito da incerteza sobre os objetivos. É a combinação da probabilidade de um evento e sua consequência (impacto).

É fundamental que uma organização identifique seus requisitos de segurança dentre as principais fontes existentes:

- A avaliação dos riscos à organização, levando em conta a estratégia e os objetivos globais de negócio da organização. Por meio de uma avaliação do risco, as ameaças aos ativos são identificadas, a vulnerabilidade e a probabilidade de ocorrência são avaliadas e o potencial impacto é estimado.

- Os requisitos legais, determinados por estatutos, regulamentos e contratos que uma organização, seus parceiros comerciais, contratantes e provedores de serviço têm que satisfazer, e seu ambiente sociocultural.

- O conjunto de princípios, objetivos e requisitos de negócio para o manuseio, processamento, armazenamento, comunicação e arquivamento da informação que uma organização desenvolveu para apoiar suas operações.

Os recursos empregados na implementação de controles precisam ser equilibrados para evitar prejuízos ao negócio, pois estes podem ser ocasionados por problemas de segurança originados pela ausência ou ineficiência de controles. O resultado da avaliação do risco irá ajudar a guiar e a determinar as ações de gestão adequadas e as prioridades para gerir os riscos da segurança da informação e a

implementar os controles selecionados para proteger contra esses riscos (HINTZBERGEN et al., 2018).

Uma abordagem sistemática de gestão de riscos de segurança da informação é necessária para identificar as necessidades da organização, a relação aos requisitos de segurança da informação e criar um sistema de gestão de segurança da informação (SGSI) eficaz. Convém que essa abordagem seja adequada ao ambiente da organização e, em particular, esteja alinhada com o processo maior de gestão de riscos corporativos. Os esforços de segurança devem lidar com os riscos de maneira efetiva e no tempo apropriado, onde e quando forem necessários. Deste modo, a gestão de riscos de segurança da informação precisa ser parte integrante das atividades de gestão de segurança da informação e dever ser aplicada tanto à implementação quanto à operação cotidiana de um SGSI (ABNT NBR ISO/IEC 27005, 2019)

Ainda segundo a norma supracitada, a gestão de riscos de segurança da informação deve ser tratada como um processo contínuo, definindo os contextos interno e externo, avaliando os riscos e tratando os mesmos de acordo com um plano de tratamento a fim de implementar as recomendações e decisões. Convém que a gestão de riscos analise os possíveis acontecimentos e suas consequências, antes de decidir o que será feito e quando será feito, a fim de reduzir os riscos a um nível aceitável.

Mesmo diante do trabalho contínuo das organizações no tratamento de riscos relacionados à segurança da informação, surgem novas técnicas, ferramentas e métodos de ataque diariamente no cenário mundial. Atacar deixou de ser um privilégio das pessoas com plenos conhecimentos tecnológicos. Nesse contexto, estabelece-se uma guerra em que, de um lado, atuam os profissionais de segurança da informação, que têm o objetivo de neutralizar os possíveis ataques que a organização possa sofrer, e, de outro, os atacantes que tentam, a todo custo, empreender ações contra a segurança informacional (NETO; ARAÚJO, 2020).

Ainda segundo os autores, as ameaças à segurança da informação podem ser classificadas de acordo com a técnica empregada para sua realização e o objetivo a ser alcançado. As principais são apresentadas a seguir:

- **Engenharia social:** Consiste em técnicas para enganar e ludibriar pessoas, a fim de obter informações que possam comprometer a segurança da organização. Suas ações são direcionadas a persuadir, muitas vezes abusando da ingenuidade ou da confiança do usuário para obter acesso não autorizado a recursos ou informações sigilosas;
- **Injeção de SQL:** É um tipo de ameaça de segurança que se aproveita de falhas em sistemas que interagem com bases de dados através de comandos SQL, onde o atacante consegue inserir uma instrução SQL personalizada e indevida dentro de uma consulta através da entradas de dados de uma aplicação, como formulários ou URL de uma aplicação;
- ***XSS (Cross-site scripting):*** É um tipo de ataque praticado normalmente em aplicações web que objetiva a injeção de código malicioso dentro das páginas web vistas por outros usuários. Um script de exploração de vulnerabilidade cross-site pode ser usado pelos atacantes para escapar aos controles de acesso que usam a política de mesma origem;
- ***DoS (Denial of Service):*** São ataques que objetivam interromper um serviço ou um computador conectado à internet, com a geração de sobrecarga no processamento do computador alvo ou no tráfego de dados da rede à qual o alvo está conectado;
- ***DDoS (Distributed Denial of Service*)**: Segue o mesmo conceito do *DoS*, porém difere por ser um ataque originado a partir de diversos equipamentos, ou seja, um conjunto de computadores é utilizado para tirar de operação um ou mais serviços;
- ***Phishing*****:** Objetiva capturar informações confidenciais, por meio de uma fraude eletrônica. Utiliza-se de pretextos falsos, com o intuito de receber informações sensíveis dos usuários, e ocorre com mais frequência por meio do envio de e-mails e páginas web falsas;
- ***Pharming*****:** É uma variante do Phishing que explora as vulnerabilidades dos browsers, dos sistemas operacionais e dos servidores DNS (Domain Name System), com o objetivo de redirecionar os usuários a páginas web falsas para obter suas informações sensíveis;
- ***IP Spoofing*****:** Tem o objetivo de assumir a identidade de outro computador, através do envio de pacotes contendo IPs falsos de origem de outra máquina;

- ***Malware*:** Este termo genérico abrange todos os tipos de programa que executam ações maliciosas em um computador, seja com a intervenção do usuário ou não, tais como: vírus, cavalos de Tróia, adware, spyware, backoors, keyloggers, worms, bots, rootkits etc.;
- ***Ransomware:*** É um tipo de malware que restringe o acesso ao sistema infectado como uma espécie de sequestro de dados e cobra um resgate em criptomoedas para que o acesso seja restabelecido;
- **Ataques de força bruta:** Utiliza criptoanálise para buscar exaustivamente a descoberta de senhas nos mais variados meios tecnológicos, web, servidores, ativos de rede etc.;
- **Envenenamento ou *Spoofing* de DNS:** É um tipo de ataque virtual que explora vulnerabilidades no servidor de nomes de domínio para desviar o tráfego dos servidores legítimos para caminhos falsos.

Para cada tipo de ameaça devem ser adotadas medidas de segurança específicas e adequados para o tratamento do risco. As medidas podem ser técnicas e organizacionais, tais como soluções tecnológicas, políticas, treinamentos, etc. O sucesso no estabelecimento de um sistema de segurança da informação depende de todas as áreas da organização. Deste modo os usuários tem um papel muito importante na manutenção da segurança da informação das instituições em que atuam, deste modo devem ser envolvidos diretamente nos processos e programas relacionados à segurança da informação (NAKAMURA; GEUS, 2007).

No Quadro 3, são apresentados algumas das principais medidas de segurança da informação.

Quadro 3: Medidas de SI. Fonte: Adaptado de CERT.BR (2020).

MEDIDA	DESCRIÇÃO
Política de segurança	A política de segurança é considerada como um importante mecanismo de segurança, tanto para as instituições como para os usuários, pois com ela é definir os direitos e as responsabilidades das partes envolvidas, bem como as penalidades em caso não cumprimento.

Notificação de incidentes e abusos	Um incidente de segurança pode ser definido como qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança de sistemas de computação ou de redes de computadores. Este deve ser notificado para contribuir na detecção e proteção de outros usuários.
Contas e senhas	Contas e senhas são o mecanismo de autenticação mais usado para o controle de acesso a sites e serviços oferecidos pela Internet. É por meio deste mecanismo que os sistemas conseguem verificar a autenticidade e definir as ações que o usuário pode realizar.
Criptografia	Possui importância fundamental para a segurança da informação, uma vez que é a base para diversas tecnologias e protocolos utilizados com objetivo de garantir confidencialidade, integridade, autenticação e irretratabilidade das informações. Este mecanismo transforma dados legíveis em ilegíveis utilizando um código de maneira que somente entidades autorizadas e detentoras da chave de criptografia conseguem descriptografar e interpretar os dados.
Hashing	São cálculos matemáticos utilizados em algoritmos que produzem o histórico da informação possibilitando identificar se ela foi alterada. Algoritmos de cálculo de hashing são usados para garantir a integridade e identificar se ocorreram mudanças não previstas.
Assinatura digital	É a combinação de mecanismos de hashing e criptografia, utilizada para garantir a autenticidade, a integridade e a irretratabilidade da informação.
Controle de acesso	Trata da limitação de acesso às informações e deve ser implementado considerando a “necessidade de conhecer” e a “necessidade de acesso”. A norma recomenda que as permissões de acesso sejam aprovadas pelo responsável pela informação. Além disso, o recurso de “perfil” pode ser adotado para autorizar não somente os acessos, mas também as ações individuais ou de um grupo de usuários.

Backup	São cópias de segurança que garantem a recuperação das informações em caso de perda ou indisponibilidade das mesmas em suas bases originais.
Certificados Digitais	Materializam o uso da assinatura digital e possibilitam o uso da criptografia, sendo emitidos por autoridades certificadoras que atestam que as informações utilizadas em sua geração são verdadeiras e válidas por um determinado tempo. Com o uso de funções matemáticas é possível se obter garantia da autenticidade, irretratabilidade, integridade e confidencialidade.
Registro de eventos (logs)	É o registro de atividade gerado por programas e serviços de um computador. Ele pode ficar armazenado em arquivos, na memória do computador ou em bases de dados.”
Honeypot	É o nome dado a um software, cuja função é detectar ou impedir a ação de um agente externo estranho ao sistema, enganando-o, fazendo-o pensar que esteja de fato explorando uma vulnerabilidade daquele sistema.
Antimalware	São ferramentas responsáveis por procurar, detectar e anular/remover programas com códigos maliciosos de um computador.
AntiSpam	São filtros responsáveis por evitar que mensagens indesejadas cheguem até a caixa de entrada de e-mails de usuários.
Firewall	Firewall é um sistema de proteção contra acessos não autorizados a partir da análise de pacotes e restrição de tráfego de rede. Este elemento pode ser um hardware e/ou software.
WAF	Um WAF (*Web Application Firewall*) filtra, monitora e bloqueia o tráfego HTTP para um aplicativo ou site da Web. Ao inspecionar o tráfego, o WAF pode evitar ataques decorrentes de vulnerabilidades de segurança em sistemas Web, tais como injeção de SQL e XSS.

DLP	O DLP (*Data Loss Prevention*) é um software capaz de prevenir contra a perda de dados, detectando possíveis violações de dados e impedindo transmissões e extração de dados.
MDM	O MDM (*Mobile Device Management*) é um sistema de gerenciamento de dispositivos móveis que protege, monitora, gerencia e suporta estes equipamentos. Geralmente inclui funcionalidades de distribuição de aplicativos, dados e definições de configuração para todos os tipos de dispositivos móveis.
IPS	Um IPS (*Intrusion Prevention System*) é um Sistema de Prevenção de Intrusão que utiliza tecnologia de segurança de rede e prevenção contra ameaças para examinar fluxos de tráfego de rede para detectar e prevenir invasões. Este controle de segurança atua monitorando a rede em busca de atividades suspeitas, sendo capaz de interrompê-las e de notificar a equipe de segurança automaticamente.
IAM	O IAM (*Identity and Access Management*) é um sistema de gerenciamento de identidades e acessos que atua sob uma estrutura de políticas e tecnologias para garantir que as pessoas em uma organização tenham o acesso adequado e limitado aos recursos de tecnologia estritamente necessários para o desempenho de suas funções.
SIEM	Uma solução de SIEM (*Security Information and Event Management*) permite que os eventos gerados por diversas aplicações de segurança (tais como firewalls, proxies, IPS e *antimalwares* sejam coletados, normalizados, armazenados e correlacionados. Possibilitando a rápida identificação e resposta aos incidentes de segurança da informação.

2.3. Normas de segurança da informação e proteção à privacidade de dados

As principais referências normativas de segurança da informação e proteção à privacidade de dados são as normas da família 27000 da *International Organization for Standardization* (ISO), específicas para gestão da segurança da informação, adotadas pela Associação Brasileira de Normas Técnicas (ABNT).

ISO/IEC 27000:2018 - Tecnologia da informação - Técnicas de segurança - Sistemas de gestão de segurança da informação - Visão geral e vocabulário: Este documento fornece a visão geral dos sistemas de gerenciamento de segurança da informação (SGSI). Ele também fornece termos e definições comumente usados na família de padrões SGSI. Este documento é aplicável a todos os tipos e tamanhos de organização (por exemplo, empresas comerciais, agências governamentais, organizações sem fins lucrativos).

ABNT NBR ISO/IEC 27001:2013 - Tecnologia da informação - Técnicas de segurança - Sistemas de gestão de segurança da informação: A norma especifica os requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão da segurança da informação (SGSI) dentro do contexto da organização. Esta Norma também inclui requisitos para a avaliação e tratamento de riscos de segurança da informação voltados para as necessidades da organização. Os requisitos definidos nesta Norma são genéricos e são pretendidos para serem aplicáveis a todas as organizações, independentemente do tipo, tamanho ou natureza.

ABNT NBR ISO/IEC 27002:2013 - Tecnologia da informação - Técnicas de segurança - Código de prática para a gestão da segurança da informação: O objetivo da norma é estabelecer diretrizes e princípios gerais para iniciar, implementar, manter e melhorar a gestão da segurança da informação, por meio da definição de controles que podem ser utilizados para atender aos requisitos identificados por meio da análise/avaliação de riscos. A norma está estruturada em 14 seções de controles de segurança da informação, divididas em 35 objetivos de controle. São definidos 114 controles aplicáveis à segurança da informação. A norma ABNT NBR ISO/IEC 27002:2013 prevê que as organizações possam vir a utilizar controles adicionais àqueles que ela recomenda.

ABNT NBR ISO/IEC 27003:2018 - Tecnologia da informação - Técnicas de segurança - Diretrizes para implantação de um sistema de gestão da segurança da informação: Esta Norma foca os aspectos críticos necessários para a implantação

e projeto bem-sucedidos de um Sistema de Gestão da Segurança da Informação (SGSI), de acordo com a ABNT NBR ISO IEC 27001:2013. A norma descreve o processo de especificação e projeto do SGSI desde a concepção até a elaboração dos planos de implantação. Ela descreve o processo de obter a aprovação da direção para implementar o SGSI, define um projeto para implementar um SGSI e fornece diretrizes sobre como planejar o projeto do SGSI, resultando em um plano final para implantação do projeto do SGSI. A intenção desta Norma é que ela seja usada pelas organizações que desejam implementar um SGSI.

ABNT NBR ISO/IEC 27004:2017 - Tecnologia da informação - Técnicas de segurança – Sistemas de gestão da segurança da informação - Monitoramento, medição, análise e avaliação: Este documento tem como objetivo auxiliar as organizações a avaliar o desempenho da segurança da informação e a eficácia do sistema de gestão de segurança da informação, a fim de atender aos requisitos da ABNT NBR ISO/IEC 27001:2013, 9.1: monitoramento, medição, análise e avaliação. Os resultados do monitoramento e medição de um sistema de gestão de segurança da informação (SGSI) podem apoiar as decisões relacionadas à governança, gestão, eficácia operacional e melhoria contínua do SGSI.

ABNT NBR ISO/IEC 27005:2019 - Tecnologia da informação — Técnicas de segurança — Gestão de riscos de segurança da informação: A norma fornece as diretrizes para a avaliação de riscos da segurança da informação, de acordo com os conceitos definidos na ABNT NBR ISO/IEC 27001. Entretanto, não inclui um método específico para a gestão de riscos de segurança da informação, pois estabelece que cabe à organização definir sua abordagem ao processo de gestão de riscos, levando em conta, por exemplo, o escopo do seu SGSI, o contexto da gestão de riscos e o seu setor de atividade econômica. Esta Norma é do interesse de gestores e pessoal envolvidos com a gestão de riscos de segurança da informação em uma organização e, quando apropriado, em entidades externas que dão suporte a essas atividades

A ABNT NBR ISO/IEC 27701:2019 - Técnicas de segurança — Extensão da ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 para gestão da privacidade da informação — Requisitos e diretrizes: Esta norma especifica os requisitos e fornece as diretrizes para o estabelecimento, implementação, manutenção e melhoria contínua de um Sistema de Gestão de Privacidade da Informação (SGPI) na forma de uma extensão das ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 para a gestão da privacidade dentro do contexto da organização.

Este documento especifica os requisitos relacionados ao SGPI e fornece as diretrizes para os controladores de dados pessoais (DP) e operadores de DP que têm responsabilidade e responsabilização com o tratamento de DP. Este documento é aplicável a todos os tipos e tamanhos de organizações, incluindo as companhias públicas e privadas, entidades governamentais e organizações sem fins lucrativos, que são controladoras de DP e/ou que são operadoras de DP.

2.4. **Leis de proteção à privacidade de dados pessoais**

As evoluções em tecnologia da informação, tais como o *Internet of Things* (IOT), *Big Data*[4] e o paradigma da computação em nuvem permitem que organizações privadas coletem e processem grandes quantidades de dados para empregar várias técnicas analíticas de modo a extrair informações importantes para otimizar seus negócios. Infelizmente, esses benefícios apresentam um alto custo em termos de exposição à privacidade de usuários, dada a sensibilidade dos dados que geralmente são processados em servidores de terceiros. Sabendo que não há privacidade sem proteção de dados e considerando os crescentes incidentes de violação de dados as organizações têm buscado implementar novos controles de segurança para preservação da privacidade em práticas de manipulação de dados. Sobretudo por terem ciência sobre os graves danos à reputação que estas violações causam e a necessidade de conformidade com o as leis de proteção de dados pessoais (FRIEDEWALD et al., 2020).

As empresas que atuam com a coleta e tratamentos de dados ocupam cada vez mais posições de destaque na economia do século XXI, referida muitas vezes como Economia Digital. Companhias que desenvolveram a capacidade de enxergar nos dados uma nova fonte de riqueza, largaram na frente da corrida na economia digital e se tornaram gigantes muito devido à habilidade de coletar e processar dados em grande escala. Neste cenário destacam-se empresas como Amazon, Alibaba, Google e Facebook como alguns exemplos presentes no cotidiano e que, em regra, não cobram nada dos usuários pelo uso de seus serviços (RODRIGUES BRANCHER; BEPPU, 2019).

[4] Big Data é a área do conhecimento que estuda como tratar, analisar e obter informações a partir de conjuntos de dados grandes demais para serem analisados por sistemas tradicionais

O ano de 2018 foi marcado por grandes evoluções no campo da proteção de dados pessoais, tanto para o mercado quanto para a sociedade civil. Em maio, o Regulamento Geral de Proteção de Dados (GDPR, na sigla em inglês) passou a valer na União Europeia (UE) e refletiu no Brasil com a sanção presidencial da Lei 13.709/2018, conhecida como Lei Geral de Proteção de Dados (LGPD). A maior parte dos aspectos da sociedade atual giram em torno de dados, de empresas marketing digital a bancos, comércio e governos. Quase todos os processos de compra de produtos ou contratação de serviços envolvem a coleta e análise de dados. As leis GDPR e LGPD tratam sobretudo da forma como são coletados, armazenados, processados e utilizados os dados pessoais de consumidores (MIRANDA, 2019).

2.4.1. **General Data Protection Regulation (GDPR)**

O Regulamento Geral de Proteção de Dados (RGPD) foi publicado no Jornal Oficial da União Europeia em 4 de maio de 2016, após quatro anos em elaboração. A vigência do regulamento passou a valer a partir de 25 de maio de 2018. Este regulamento fornece atualizações abrangentes de várias regras de proteção de dados que o mundo não via há mais de 20 anos. Qualquer empresa que processe dados pessoais de cidadãos da UE estará sujeita a GDPR. Em caso de não conformidade a empresa está suscetível a severas multas que podem ultrapassar € 20 milhões ou até 4% da receita global da empresa (KABANOV, 2016).

O GDPR ocasionou um “efeito dominó”, visto que passou a exigir que os demais países e empresas que buscassem manter relações comerciais com a UE também tivessem uma legislação de mesmo nível que o GDPR. Isso porque o Estado que não possuísse lei de mesmo nível passaria a poder sofrer algum tipo de barreira econômica ou dificuldade de fazer negócios com os países da UE. Considerando o contexto econômico, esse é um risco que a maioria das nações não gostaria de assumir (PECK, 2020).

Segundo o preâmbulo (2) e (13) do GDPR (2016) o regulamento tem como objetivo:

- Contribuir para a realização de um espaço de liberdade, segurança e justiça e de uma união econômica, para o progresso econômico e social, a consolidação

e a convergência das economias no nível do mercado interno e para o bem-estar das pessoas físicas;

- Assegurar um nível coerente de proteção das pessoas físicas no âmbito da União e evitar que as divergências constituam um obstáculo à livre circulação de dados pessoais no mercado interno;
- Garantir a segurança jurídica e a transparência aos envolvidos no tratamento de dados pessoais, aos órgãos públicos e à sociedade como um todo;
- Impor obrigações e responsabilidades iguais aos controladores e processadores, que assegurem um controle coerente do tratamento dos dados pessoais;
- Possibilitar uma cooperação efetiva entre as autoridades de controle dos diferentes Estados-Membros.

2.4.2. **Lei Geral de Proteção de Dados (LGPD)**

A Lei Geral de Proteção de Dados Pessoais (LGPD), Lei n° 13.709 de 14 de agosto de 2018, cuja vigência se deu a partir de 18 de setembro de 2020, é a legislação brasileira que determina como os dados pessoais dos cidadãos podem ser coletados e tratados e quais punições, decorrentes de eventuais transgressões, devem ser aplicadas. A lei de proteção de dados cria um vínculo jurídico entre o indivíduo e seus dados, justificado pela identidade da informação, isto é, dos dados com a pessoa. A partir da vulnerabilidade de dados pessoais disponibilizados, mormente os expostos na internet, o governo brasileiro optou por criar legislação específica sobre a proteção de dados pessoais. A LGPD adveio do Projeto de Lei 53/2018, que se baseou nas diretrizes do Regulamento Geral sobre a Proteção de Dados da União Europeia, e, após aprovação nas duas casas legislativas, foi sancionada (RODRIGUES BRANCHER; BEPPU, 2019) .

O artigo 5° da LGPD define dado pessoal como qualquer informação que identifique precisamente ou torne identificável uma pessoa natural, assim como nomes, domicílio, números de telefone, infrações administrativas e penais, dentre outras. A determinação da característica da pessoalidade de um dado advém da possibilidade de se identificar uma pessoa concretamente, diferenciando-o do restante da coletividade. Por sua vez, dado pessoal sensível é aquele que versa sobra a origem

racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, estado de saúde ou vida sexual de uma pessoa natural (BRASIL, 2018).

Segundo Doneda (2019) a Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. Baseia-se na livre iniciativa, no desenvolvimento econômico e tecnológico do país, em consonância com a dignidade e o exercício da cidadania. No âmbito da LGPD, o tratamento dos dados pessoais pode ser realizado por dois “agentes de tratamento”, o Controlador e o Operador:

- **Controlador:** É definido pela Lei como a pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais. No âmbito da Administração Pública, o Controlador será a pessoa jurídica do órgão ou entidade pública sujeita à Lei, representada pela autoridade imbuída de adotar as decisões acerca do tratamento de tais dados;

- **Operador:** É a pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador, aí incluídos agentes públicos no sentido amplo que exerçam tal função, bem como pessoas jurídicas diversas daquela representada pelo Controlador, que exerçam atividade de tratamento no âmbito de contrato ou instrumento congênere.

Por tratamento entende-se toda operação, automatizada ou não, realizada com dados pessoais, tais como a coleta, utilização, acesso, transmissão, processamento, arquivamento, armazenamento ou transferência. Qualquer operação de tratamento de dados pessoais realizada no território nacional, por pessoa natural ou pessoa jurídica de direito público ou privado, cujos titulares estejam localizados no Brasil, ou que tenha por finalidade a oferta de produtos ou serviços no Brasil, estão sujeitos à LGPD, que passa a exigir o consentimento expresso do usuário para esta operação (MALDONADO; BLUM, 2019).

Ainda segundo os autores é enfatizada a importância da definição adequada das bases legais para justificar o tratamento de dados pessoais no sentido de assegurar a conformidade com as referidas hipóteses legais e princípios da LGPD. Deste modo a Lei prevê dez bases legais válidas para fundamentar o tratamento dos dados pessoais por parte dos Controladores:

- Mediante o fornecimento de consentimento pelo titular;
- Para o cumprimento de obrigação legal ou regulatória pelo controlador;
- Pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV da Lei;
- Para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
- Quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;
- Para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);
- Para a proteção da vida ou da incolumidade física do titular ou de terceiros;
- Para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;
- Quando necessário para atender aos interesses legítimos do controlador ou de terceiros, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais;
- Para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

Segundo Peck (2020), dentre os princípios da LGPD, destacam-se o da finalidade, adequação, necessidade, livre acesso, qualidade de dados, transparência, segurança, prevenção, não discriminação e responsabilização e prestação de contas. A definição de cada princípio é apresentada a seguir:

- **Finalidade:** Os dados somente devem ser utilizados para as finalidades específicas para as quais foram coletados e informados aos seus titulares;
- **Adequação:** Trata da compatibilização do uso dos dados com a finalidade informada;
- **Necessidade:** Define a limitação do uso do dado ao mínimo necessário para se atingir a finalidade desejada;
- **Livre acesso:** Relaciona-se com as garantias, aos titulares dos dados, de informações facilitadas, que devem ser disponibilizadas de forma gratuita, caso haja requerimento por parte do titular;
- **Qualidade:** Garante a exatidão, clareza, relevância e atualização dos dados;
- **Transparência:** Deve ser aplicada no intuito de oferecer dados claros e precisos sobre a realização do tratamento e agentes de tratamento;
- **Segurança:** Visa à proteção dos dados de acesso pessoais não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão de dados;
- **Prevenção:** Decorre da adoção de medidas com o objetivo de precaver a ocorrência de danos em virtude do tratamento de dados pessoais;
- **Não discriminação:** Impossibilita que os dados sejam usados para fins discriminatórios, ilícitos ou abusivos;
- **Responsabilização e prestação de contas:** Devem ocorrer fundamentadas na demonstração da adoção de medidas eficazes e capazes de comprovar o cumprimento das normas de proteção de dados por parte do agente.

De acordo com o artigo 17, a lei cita como seu destinatário “Toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade”. Dentre os direitos que o titular dos dados pessoais possui, destaca-se o direito de acesso, que garante a obtenção de todos os dados pessoais que estão sendo tratados, mediante requisição aos controladores e, em consequência, os direitos de retificação e atualização, haja vista a obrigação dos agentes de os manter sempre corretos e atualizados (BRASIL, 2018).

Ademais, citam-se, ainda, como direitos do titular de dados o direito de confirmação da existência de tratamento; de anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o

disposto na lei; de portabilidade dos dados a outro fornecedor de serviço ou produto; de eliminação dos dados pessoais tratados com o consentimento do titular; de informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados; de informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa e de revogação do consentimento, a ser realizada de forma gratuita (BRASIL, 2018).

Os agentes de tratamento devem adotar medidas técnicas e organizacionais de segurança em consonância com o artigo 46°, aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito. Qualquer incidente de violação de dados pessoais deve ser comunicado à Autoridade Nacional de Proteção de Dados (ANPD), órgão da administração pública indireta responsável por zelar, implementar e fiscalizar o cumprimento da lei. A comunicação com a ANPD deverá ocorrer por meio formal e através da figura do Encarregado, pessoa indicada pelo controlador e operador para atuar como representante da organização junto a Autoridade Nacional de Proteção de Dados e os titulares. A notificação de uma eventual violação de dados pessoais deve contemplar a descrição minuciosa dos dados afetados e indicação das medidas técnicas e de segurança utilizadas, bem como as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do incidente (PECK, 2020).

Outro aspecto relevante é o fluxo de dados para outros países, a chamada transferência internacional de dados, que somente será permitida para países ou organismos internacionais que proporcionem grau de proteção de dados pessoais compatível com a lei brasileira ou mediante oferecimento de garantias do regime de proteção de dados local (RODRIGUES BRANCHER; BEPPU, 2019).

As empresas ficam responsáveis por, através de seus agentes de tratamento, elaborar relatório de impacto à proteção de dados pessoais (RIPD), com descrição dos tipos de dados coletados, o fundamento da coleta e a metodologia utilizada para a coleta e garantia da segurança das informações, no que resulta na importância da contratação e consultoria de empresas especializadas em segurança da informação confiáveis. Isto posto, percebe-se importante papel a ser exercido pelas empresas em relação à proteção de dados pessoais (RAMOS; GOMES, 2019).

A LGPD vai além da GDPR, expandindo o escopo da proteção de dados. A Lei abrange organizações públicas e privadas, onde a multa simples para infração pode

chegar a R$ 50 milhões de reais. De acordo com o Art. 42º, II, § 2º, dependendo do contexto, o ônus da prova pode ser invertido, isto é, a culpa é transferida do titular dos dados para organização envolvida. A LGPD, no Art. 6º, VI, determina o princípio da transparência: “garantia, aos titulares de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial” (MALDONADO; BLUM, 2019).

2.5. **Modelos de maturidade em segurança da informação**

Há muitos modelos de segurança desenvolvidos, porém cada um deles se concentra em aspectos de segurança específicos, tais como riscos, ativos, redes, dados e aplicativos. Deste modo, dificilmente um modelo de segurança considera a segurança da informação de forma completa. Sabe-se que uma única vulnerabilidade pode ser explorada e comprometer todo um sistema de segurança. Nos últimos anos, vários modelos de maturidade de segurança foram propostos para o gerenciamento geral da segurança com o objetivo de auxiliar organizações a avaliarem seus sistemas e controles de segurança (LE; HOANG, 2016) .

Recentemente, muitos modelos foram desenvolvidos para aumentar a segurança do espaço cibernético. Dependendo das abordagens dos pesquisadores e da escala de suas pesquisas sobre o espaço cibernético, esses estudos se concentram em diferentes ângulos de segurança da informação, tais como tecnologias, hardware, software, dados, informações, rede e gerenciamento de riscos. Entre os modelos propostos, o modelo de maturidade em segurança cibernética fornece, em certa medida, um roteiro para as organizações medirem, avaliarem e aprimorarem seus níveis de proteção de dados e segurança da informação. Em relação a outros modelos, fornece aos gerentes uma base sólida para fazer uma avaliação da relevância e efetividade de seus controles (CARCARY et al., 2016).

O Modelo de Maturidade em Capacidade - *Capability Maturity Model* (CMM) é considerada uma base para os demais modelos, pois refere-se amplamente a uma abordagem de melhoria de processos. O CMM foi desenvolvido pelo Software Engineering Institute (SEI) em meados da década de 1980 e foi concebido para avaliação de risco na contratação de empresas de software pelo Departamento de Defesa dos Estados Unidos que desejava ser capaz de avaliar os processos de desenvolvimento utilizados pelas empresas que concorriam em licitações como

indicação da previsibilidade da qualidade, custos e prazos nos projetos contratados. Como um modelo de processo é uma coleção estruturada de práticas que descrevem as características de processos efetivos e as práticas incluídas são aquelas comprovados pela experiência como eficazes (REA-GUAMAN et al., 2017).

Os modelos de maturidade mostram o nível de integridade de certas capacidades, definindo os níveis de conformidade dos objetos analisados com os padrões estabelecidos por meio de diferentes conjuntos de critérios multidimensionais. A estrutura do modelo de maturidade em segurança cibernética pode ser explicada em termos de suas funções, componentes principais e tipo. Os modelos mais recentes de maturidade em segurança cibernética são modelos híbridos, onde se elevam os níveis e domínios de segurança para uma estrutura integrada (KARLSSON; KOLKOWSKA; PRENKERT, 2016).

Ainda segundo os autores, um modelo de maturidade de capacidade de segurança cibernética fornece uma referência por qual uma organização pode avaliar o nível atual de maturidade de suas práticas, processos e definir metas e prioridades para melhoria da segurança cibernética. Os modelos de maturidade de capacidade em segurança cibernética são geralmente estruturados através dos seguintes elementos:

- **Áreas ou dimensões:** Uma área agrupa conceitos comuns de processos organizacionais e cada área não é necessariamente independente das outras.

- **Fatores e indicadores:** Fatores são os objetivos que devem ser cumpridos em cada uma das áreas do modelo e os indicadores servem para visualizar o progresso em direção a objetivos.

- **Nível de maturidade:** É o resultado da avaliação do cumprimento dos fatores e indicadores dentro das áreas ou dimensões da organização. Os níveis de faixa de maturidade de um nível inicial em que uma organização pode ter começado a considerar segurança cibernética, para uma comparação dinâmica em que uma organização é capaz de adaptar-se rapidamente às mudanças no cenário de segurança cibernética sobre ameaças, vulnerabilidades, riscos, estratégia econômica ou mudanças nas necessidades organizacionais.

A principal função de um modelo de maturidade é servir como base para avaliar e comparar o desempenho do avaliado a um padrão, apresentando meios para identificar lacunas e desenvolver planos de melhoria. Os principais componentes de um modelo são os níveis de maturidade (escala de medição de segurança ou estados de transição), domínios de segurança (grupos lógicos de práticas e processos), atributos que são o conteúdo principal do modelo, organizados por domínios e níveis; métodos de diagnóstico para avaliação, medição, identificação de lacunas e benchmarking; roteiros de melhoria para orientar esforços de melhoria, como Planejar-Executar-Verificar-Agir (LE; HOANG, 2016).

Para identificar os principais modelos de maturidade de segurança da informação foi realizada uma revisão sistemática com base em artigos científicos e pesquisas realizadas até o presente momento, como resultado foram elencados os modelos de maturidade de segurança cibernética a seguir: (DOE, 2019), (CIAS, 2017), (BOSTON, 2017), (NIST, 2018) e (NEWHOUSE et al., 2017). C2M2 - *Cybersecurity Capability Maturity Model,* CCSMM - *The Community Cyber Security Maturity Model,* O-ISM3 – *Open Information Security Management Maturity Model,* CSF - *Cybersecurity Framework e* NICE - *National Cybersecurity Education Initiative.*

Além dos modelos de maturidade em segurança da informação supracitados, na revisão sistemática foram identificados outros modelos de maturidade de capacidade, contudo estes não foram abordados neste trabalho porque somente os mais específicos e referenciados foram levados em consideração. Portanto, alguns dos modelos que não foram considerados são:

Control Objectives for Information and related Technology COBIT que é um modelo que não trata completamente da questão da segurança cibernética, mas se concentra em Governança de TI (ISACA, 2019).

E a ABNT NBR ISO/IEC 27001 que fornece as diretrizes para estabelecer um sistema de gerenciamento de segurança da informação em uma empresa, porém não oferece um modelo de capacidade e maturidade associado à segurança cibernética (ABNT NBR ISO/IEC 27001, 2013).

2.5.1. **Cybersecurity Capability Maturity Model (C2M2)**

O Modelo de Maturidade em Cibersegurança (C2M2) foi desenvolvido pelo Departamento de Energia (DOE) em colaboração com a Universidade Carnegie

Mellon para ajudar organizações de infraestrutura a avaliarem e melhorarem suas práticas de segurança cibernética. Este modelo foi usado para criar o recurso de segurança cibernética do subsetor de eletricidade Modelo (ES-C2M2) e o subsetor de petróleo e gás natural Cyber Modelo de Capacidade de Segurança (ONG-C2M2).

O modelo está organizado em dez domínios e cada domínio é um agrupamento lógico de práticas de segurança cibernética. As práticas em cada domínio são organizadas em objetivos, que representam conquistas dentro do domínio. Para medir o nível de maturidade do sistema cibernético C2M2 usa uma escala de níveis de indicadores de maturidade (MILs) 0-3, onde 0 é não realizada, 1 é iniciado, 2 é executado e 3 é gerenciado (DOE, 2019).

O C2M2 fornece orientação descritiva e não prescritiva, onde o conteúdo do modelo é apresentado em um alto nível de abstração, para que possa ser interpretado por organizações de vários tipos, estruturas e tamanhos.

2.5.2. **The Community Cyber Security Maturity Model (CCSMM)**

Desenvolvido pelo Center for Infrastructure Assurance and Security (CIAS) of the University of San Antonio, Texas, o modelo de maturidade em segurança cibernética da comunidade (CCSMM) foi projetado para atender às necessidades dos estados e comunidades de desenvolver um programa viável e sustentável de segurança cibernética. A única versão (1.0) do modelo foi publicada no ano de 2006.

O modelo é capaz de identificar as características das comunidades e estados, bem como a maturidade de seu programa de segurança cibernética. Utiliza aspectos como conhecimento de segurança cibernética, políticas e procedimentos de segurança, troca de informações internamente e entre organizações, treinamento e educação em segurança cibernética (WHITE, 2007)

O Modelo Comunitário de Maturidade em Segurança Cibernética possui 5 níveis que vão de inicial ao de vanguarda, onde o seu principal diferencial é a terceira dimensão, incluindo organização, comunidade e estado. Este modelo é aplicável a sistemas cibernéticos de diferentes de tamanhos. Esse modelo foi implementado em cinco estados dos Estados Unidos da América com financiamento do National Cyber Security Division of Departament of Homeland Security (EUA).

2.5.3. **Open Information Security Management Maturity Model (O-ISM3)**

Em 2007, o modelo (ISM3) foi desenvolvido pelo consórcio ISM3 com cinco níveis: indefinido, definido, gerenciado, controlado e otimizado. Este modelo se concentra na avaliação, especificação, implementação e aprimoramento de informações orientadas ao processo sistemas de gerenciamento de segurança. A vantagem do modelo é que ele considera a cultura organizacional como um problema de segurança. Além disso, é baseado em padrões anteriores de segurança cibernética e práticas como ISO 9000 e ISO 17799/27001. É também aplicável a organizações de tamanhos diferentes (BOSTON, 2017).

2.5.4. **NIST Cybersecurity Framework**

O NIST Cybersecurity Framework foi desenvolvido em 2014 para atendimento a infraestruturas críticas, resultante de uma determinação federal americana nº13.636, todavia foi amplamente adotado nos setores público e privado nos mais diversos tamanhos organizacionais. O Framework do NIST é uma estrutura que consiste em padrões, diretrizes e melhores práticas para gerenciar riscos relacionados à segurança cibernética. A abordagem priorizada, flexível e econômica do framework ajuda a promover a proteção e a resiliência da infraestrutura crítica e de outros setores importantes para a economia e a segurança. O modelo é composto pelas seguintes etapas (NIST, 2018):

- Identificar: O objetivo é realizar um inventário de dados, dispositivos, aplicativos e a infraestrutura subjacente que processa e armazena esses dados. A partir do inventário é possível identificar ameaças e vulnerabilidades no ambiente, permitindo que os esforços sejam concentrados na proteção dos ativos mais críticos ou valiosos para a organização;

- Proteger: Após definir o que será protegido são estabelecidas as medidas para salvaguardar os dados. A abordagem de camadas de segurança é fundamental para proteger a conectividade, aplicativos e o próprio ativo;

- Detectar: Consiste no monitoramento contínuo do ambiente para detectar eventos e possíveis incidentes. A estratégia de monitoramento e tecnologias devem ser continuamente aprimoradas para que a detecção seja eficiente e eficaz;

- Responder: Determina a formalização de um plano de resposta a incidentes que seja conhecido pela organização e seus respondentes. Como a detecção, a resposta deve ser rápida para que a continuidade dos negócios seja restaurada;

- Recuperar: Consiste na recuperação da organização após uma interrupção ocasionada por uma violação. A restauração dos negócios e da operação de TI devem ser priorizadas sem afetar a investigação do incidente, pois esta etapa desempenha um papel fundamental para aprimoramento dos controles de segurança.

2.5.5. **National Initiative for Cybersecurity Education (NICE)**

O modelo *National Cybersecurity Education Initiative* (NICE) foi criado em 2014 e concentra-se na estrutura de segurança cibernética do pessoal, especificamente na gestão de talentos e no papel do planejamento de pessoal (NEWHOUSE et al., 2017).

O modelo de maturidade NICE segmenta atividades-chave em três áreas principais:

- Processo e Análise: Processo representa as atividades associadas com as etapas que uma organização realiza para realizar o planejamento da força de trabalho e como estas são integradas com outros processos de negócios importantes em toda a organização. Análise representa as atividades associadas aos dados de oferta e demanda, bem como o uso de ferramentas, modelos e métodos para realizar análises de planejamento da força de trabalho.

- Governança integrada: Representa as atividades associadas ao estabelecimento estruturas de governança, desenvolvimento e fornecimento de orientação para a tomada de decisões. É o alicerce para a força de trabalho geral de uma organização, estratégia de planejamento e visão, bem como atribuições de responsabilidade, promoção de integração e emissão de orientações de planejamento.

- Profissionais treinados e tecnologia capacitadora: Representa as atividades associadas com o estabelecimento de um quadro profissional de planejadores de força de trabalho dentro de uma organização.

2.5.6. **Consolidação de modelos de segurança da informação**

Para consolidar a compreensão dos modelos de maturidade e como eles são aplicados na segurança cibernética foi elaborada o Quadro 4 que demonstra os recursos desses modelos.

Quadro 4: Modelos de maturidade em segurança da informação e privacidade. Fonte: Adaptado de Le & Hoang (2016).

	Modelos de Maturidade de Segurança da Informação	**Organização / Autor**	**Propósitos e Forças**	**Níveis de Maturidade**				
				1	**2**	**3**	**4**	**5**
1	Cyber Security Capability Maturity Model (C2M2), 2019	Department of Energy (DOE)	Avaliação da implementação e gerenciamento em infraestrutura crítica	Não realizada	Iniciada	Realizada	Gerenciada	
2	Community Cyber Security Maturity Model (CCSMM), 2007	White	Esforço comunitário e capacidade de comunicação nas comunidades	Inicial	Avançada	Auto Avaliada	Integrada	Vanguarda
3	Information Security Management Maturity Model (ISM3), 2017	ISM3 Consortium	Prevenir e mitigar incidentes e otimizar o uso de informações, dinheiro, pessoas, tempo e infraestrutura	Indefinido	Definido	Gerenciado	Controlado	Otimizado
4	Cyber Security Framework (CSF-NIST), 2018	NIST	Melhorar a infraestrutura crítica federal por meio de um conjunto de atividades destinadas a desenvolver perfis individuais para as operadoras.	Identificar	Proteger	Detectar	Responder	Recuperar
5	NICE's Cyber Security Capability Maturity Model, 2017	The US DHS	Planejamento da força de trabalho para práticas recomendadas de segurança cibernética	Limitada	Progredindo	Otimizada		

3. METODOLOGIA

Neste capítulo é apresentada a classificação da pesquisa e os procedimentos metodológicos utilizados neste trabalho, bem como o detalhamento de cada etapa realizada.

3.1. Classificação da pesquisa

Do ponto de vista de sua natureza, este trabalho é uma pesquisa aplicada uma vez que de acordo com Silva & Menezes (2005), pesquisas deste tipo “objetivam gerar conhecimentos para aplicação prática e dirigidos à solução de problemas específicos”.

Quanto a forma de abordagem, pode ser classificada como qualitativa, uma vez que foi realizada uma análise dos trabalhos publicados referentes modelos de maturidade em segurança da informação (GIL, 2008).

Em relação aos objetivos, a pesquisa desenvolvida, classifica-se como exploratória, pois visa à descoberta, o achado, a elucidação de fenômenos ou a explicação daqueles que não eram aceitos apesar de evidentes. A exploração representa, atualmente, um importante diferencial competitivo em termos de concorrência (GONÇALVES, 2005).

Do ponto de vista dos procedimentos técnicos realizados, é classificada como bibliográfica Silva & Menezes (2005), pelo fato de utilizar como base os trabalhos já publicados na área e, de acordo com Gil (2008), trabalhos que recebem essa classificação são elaborados a partir de material já publicado, e nesse caso, principalmente, a partir de artigos científicos.

3.2. Etapas da pesquisa

A pesquisa foi estruturada nas seguintes etapas para a realização do trabalho proposto:

- ETAPA 1 - Realizar uma pesquisa bibliográfica relacionada com modelos de maturidade e normas de segurança da informação. Levantamento

das publicações acerca do tema com o principal objetivo de auxiliar o desenvolvimento e a escrita da dissertação a partir de trabalhos correlatos;

- ETAPA 2 - Analisar os requisitos necessários para a proposta de um novo modelo de maturidade a partir da análise de modelos de maturidade existentes e normas consolidadas de segurança da informação, além de legislação brasileira para privacidade de dados pessoais;

- ETAPA 3 – Desenvolver o modelo de maturidade em segurança da informação brasileiro (MMSI.br);

- ETAPA 4 – Elaborar e divulgar uma pesquisa em forma de questionário semiestruturado para validar o modelo proposto com um grupo seleto de profissionais e coletar feedbacks dos participantes;

- ETAPA 5 – Prover melhorias no modelo e no questionário a partir das críticas e sugestões enviadas pelos participantes da fase de validação do modelo;

- ETAPA 6 – Divulgar o questionário publicamente e manter a seção de feedbacks para permitir a constante evolução do modelo;

- ETAPA 7 – Enviar um relatório textual e gráfico para os respondentes com o objetivo de demonstrar o nível de aderência das organizações avaliadas ao modelo;

- ETAPA 8 – Gerar estatísticas sobre a aderência das organizações participantes ao modelo proposto por segmento de negócio.

A representação gráfica das etapas da metodologia é demonstrada na Figura 4.

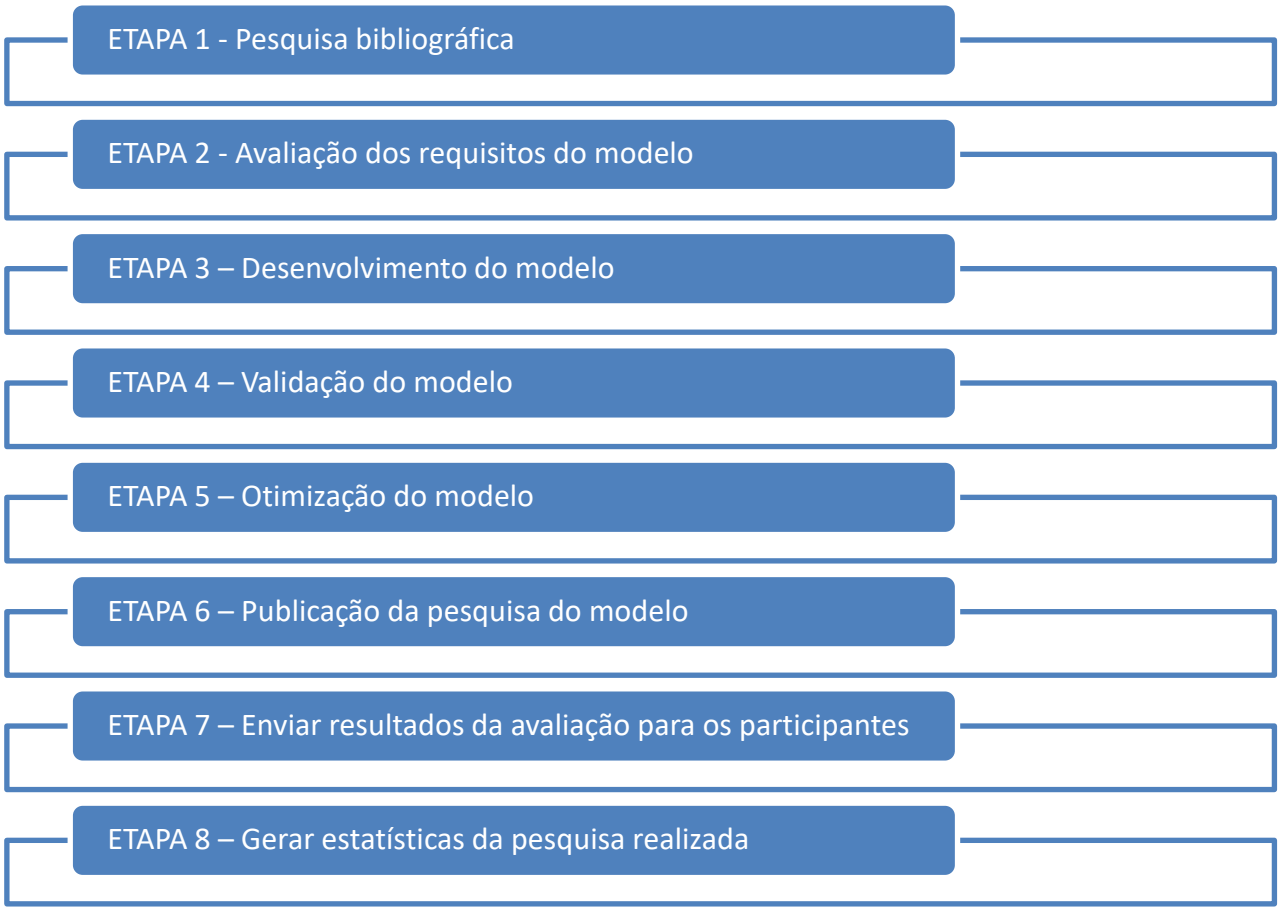


Figura 4: Etapas da metodologia. Fonte: Elaborado pelo Autor.

A seção 3.3 detalha os aspectos da primeira etapa da metodologia, as demais etapas serão apresentadas nos capítulos sub sequentes.

3.3. **Pesquisa bibliográfica**

Os termos “information security", “cybersecurity”, “privacy”, “data protection”, “maturity” e “capability” foram definidos como palavras-chaves, com o objetivo de encontrar resultados relacionados ao tema modelos de maturidade de segurança da informação.

A partir disso foi criada a query apresentada no Quadro 5, que englobou somente os tipos de documentos artigos, publicações em conferências e capítulos de livros. Foram considerados documentos de todas as áreas de pesquisas publicados entre 2016 e 2020 disponíveis no Scopus.

Quadro 5 – Query utilizada para a pesquisa. Fonte: Scopus.

```
(TITLE-ABS-KEY ( cybersecurity OR "information security" )
AND TITLE-ABS-KEY ( privacy OR "data protection" )
AND TITLE-ABS-KEY ( "maturity" OR "capability" ) )
AND
(LIMIT-TO ( DOCTYPE,"cp" )
OR LIMIT-TO ( DOCTYPE,"ar" )
OR LIMIT-TO ( DOCTYPE,"ch" ) )
AND (
LIMIT-TO ( PUBYEAR,2020)
OR LIMIT-TO ( PUBYEAR,2019)
OR LIMIT-TO ( PUBYEAR,2018)
OR LIMIT-TO ( PUBYEAR,2017)
OR LIMIT-TO ( PUBYEAR,2016)
)
```

Na pesquisa foram identificadas 102 publicações e para a seleção dos artigos foram lidos os resumos dos documentos apresentados como resultado. Após foram selecionados 36 artigos, pois estes apresentaram maior aderência ao objeto de estudo deste trabalho. Além da base de consulta Scopus foram utilizadas também fontes complementares, tais como bases legais, Google acadêmico e Google Search. A Figura 5 demonstra o volume de publicações relacionadas por ano.

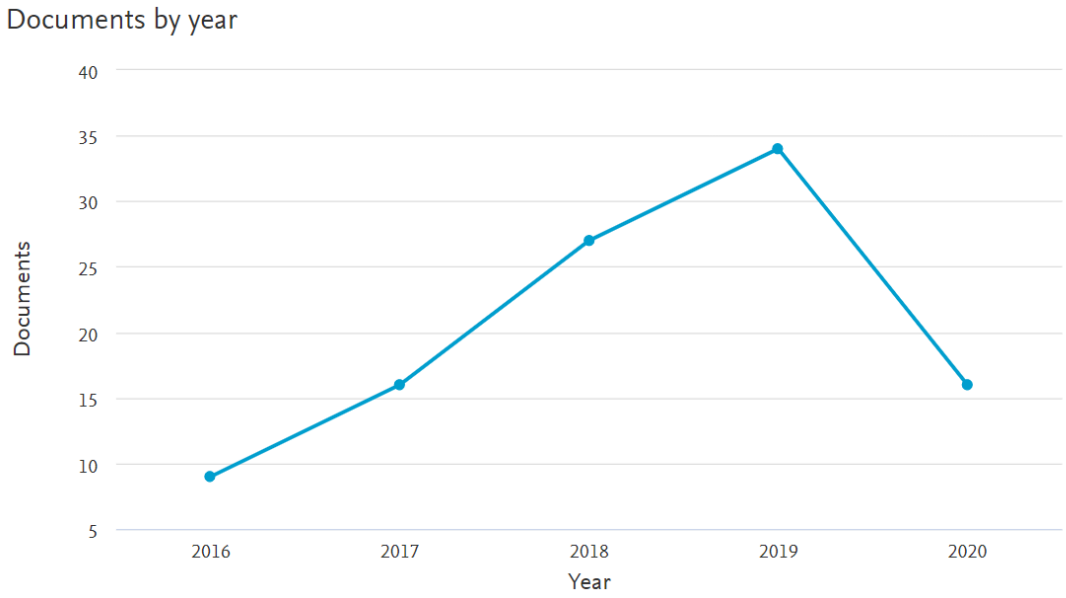


Figura 5 - Volume de publicações relacionadas por ano. Fonte: Scopus.

A partir da pesquisa bibliográfica detalhada acima foi possível selecionar os trabalhos relacionados descritos a seguir.

Em sua dissertação de mestrado Jansen (2008) propôs um instrumento de avaliação da maturidade dos processos de segurança da informação para instituições hospitalares. O trabalho apresenta revisão da literatura com a aplicação de pré-testes com especialistas em segurança da informação. Foi realizado estudo exploratório, de natureza qualitativa, com aplicação de questionários semiestruturados para estudo de caso em 3 instituições hospitalares. A semelhança com o presente trabalho está na utilização como referências a norma ABNT NBR ISO/IEC 27001. A principal diferença está no objetivo do estudo, uma vez que o modelo proposto pelo autor é específico para a área hospitalar e não apresenta um método para medição do nível de conformidade das organizações em relação à Lei Geral de Proteção de Dados.

No artigo “Modelo de avaliação da maturidade da segurança da informação” (RIGON; WESTPHALL, 2011), Evandro Rigon e Carla Westphall apresentaram um processo para a gestão da maturidade da segurança da informação por meio de um método de medição e um conjunto de controles que tratam a segurança da informação. A semelhança com o presente trabalho está na utilização como referências a norma ABNT NBR ISO/IEC 27002 e o modelo de maturidade para o gerenciamento da segurança da informação O-ISM3 (The Open Group Information Security Management Maturity Model). A principal diferença está no objetivo do estudo, uma vez que o modelo proposto pelos autores não apresenta um método para medição do nível de conformidade das organizações em relação à Lei Geral de Proteção de Dados.

No artigo “*Maturity Model of Information Security for Software Developers*” (SILVA; BARROS, 2017) apresentam um modelo de Maturidade de Segurança da Informação baseado na norma ISO/IEC 27002, tendo por objetivo auxiliar as empresas de software a avaliarem sua situação com relação à segurança da informação. Os autores adaptaram os 114 controles da ISO/IEC em 35 itens que são analisados através de questionário. O modelo proposto é composto por cinco níveis de maturidade (Ad Hoc, Gerenciado, Definido, Gerenciado Quantitativamente e Otimizado) e foi avaliado por especialistas e, posteriormente, por empresas. De acordo com a soma das pontuações obtidas em cada uma das 35 perguntas do questionário as empresas são categorizadas em determinado nível de maturidade. A

semelhança com o presente trabalho está na utilização como referência da norma ABNT NBR ISO/IEC 27002. A principal diferença está no objetivo do estudo, uma vez que o modelo proposto pelos autores foca no em empresas de software e não apresenta um método para medição do nível de conformidade das organizações em relação à Lei Geral de Proteção de Dados.

No modelo MR-MPS-SV da Softex (2015) são definidos os níveis de maturidade MPS e os processos relacionados a serviços, com seus propósito e resultados esperados e os atributos de processo, que definem o nível de capacidade dos processos esperada em cada nível de maturidade. O Modelo tem como referências técnicas a Norma Internacional ISO/IEC 20000:2011 (ISO/IEC, 2011), a Norma Internacional ISO/IEC 33020:2015 (ISO/IEC, 2015) e o modelo CMMI-SVC® 2 (SEI, 2010). O processo 9.5.6 apresenta os resultados esperados para Gerência da Segurança da Informação (GSI). A semelhança do MR-MPS-SV com o presente trabalho reside no fato que os resultados esperados relacionados de GSI para gestão de serviços estarem integralmente contemplados no modelo de segurança proposto. A principal diferença está no objetivo do estudo, uma vez que o modelo da Softex foca em gestão de serviços e não em segurança da informação.

No artigo “Modelo de maturidade de proteção de dados pessoais para o setor micro financeiro no Peru” GARCIA et al. (2018) foi apresentada uma proposta de modelo e como resultado foi realizada uma avaliação em cinco empresas do setor financeiro do pais, cujos resultados obtidos foram analisados para validar o modelo e ajudar as organizações em seu processo de proteção de dados pessoais. A semelhança com o presente trabalho está na utilização como referência da norma ABNT NBR ISO/IEC 27001. A principal diferença está no objetivo do estudo, uma vez que o modelo proposto pelos autores foca no em empresas financeiras e não apresenta um método para medição do nível de conformidade das organizações em relação à Lei Geral de Proteção de Dados.

No artigo “Um novo e adaptativo modelo de maturidade em segurança cibernética” GHAFFARI & ARABSORKHI (2018) apresentaram uma proposta de modelo capaz de avaliar a maturidade em segurança da informação das organizações. Além disso, o modelo determina a quantidade de progresso com base em um conjunto de critérios específicos. A semelhança com o presente trabalho está

na utilização como referência da norma ISO/IEC 27001 e 27002. A principal diferença está no objetivo do estudo, uma vez que o modelo proposto pelos autores não apresenta um método para medição do nível de conformidade das organizações em relação à Lei Geral de Proteção de Dados.

Outros trabalhos relacionados à avaliação da segurança da informação foram consultados. Contudo, o escopo dos trabalhos limitava-se a apresentar características da segurança da informação e realizar análises de adequação à norma ABNT NBR ISO/IEC 27002 através de estudos de caso por avaliação de adequação ou por aplicação de questionários. As avaliações realizadas foram pontuais, não sendo apresentadas formas para medição e acompanhamento da evolução da segurança da informação das organizações avaliadas.

A principal contribuição e distinção do modelo de maturidade em segurança da informação proposto no presente trabalho em relação aos demais, está no fato deste ser aplicável a diversos segmentos de negócio brasileiro, levando em consideração as melhores práticas em proteção de dados e privacidade segundo as normas ISO 27001, ISO 27002, ISO 27701 e a Lei nº 13.709/2018 (LGPD).

4. MODELO DE MATURIDADE EM SEGURANÇA DA INFORMAÇÃO - MMSI.BR

4.1. Estrutura do modelo

O modelo de maturidade em segurança da informação brasileiro (MMSI.BR) foi desenvolvido com o objetivo de otimizar a segurança e a privacidade de dados nas organizações, independente do seu porte ou segmento de negócio. Para tal, foi baseado nas principais normas técnicas relacionadas e legislação brasileira. A Figura 6 demonstra as referências do modelo proposto.

Figura 6 – Referências MMSI.br. Fonte: Elaborado pelo Autor.

No modelo de avaliação apresentado neste trabalho se destacam as seguintes características:

a) Utilizar uma estrutura de processo de gestão que possibilite a avaliação e a melhoria contínuas da segurança da informação a partir da norma ABNT NBR ISO/IEC 27001;

b) Utilizar como base um conjunto específico e adequado de controles reconhecidos internacionalmente que tratem a segurança da informação e a privacidade de dados

de forma abrangente, tais como as normas ABNT NBR ISO/IEC 27002 e ABNT NBR ISO/IEC 27701;

c) Fornecer um meio para aferir a situação atual da segurança da informação e privacidade de dados nas organizações avaliadas. Para tal, foi derivado do modelo de segurança da informação O-ISM3;

d) Prover subsídio para identificar ações de melhoria oportunas e viáveis, baseada na efetividade dos controles de proteção de dados, privacidade e nas condições dos processos de negócio da organização;

e) Avaliar medidas técnicas e organizacionais em prol da conformidade com a Lei Nº 13.709 de 14 de agosto de 2018 (LGPD);

Na concepção estrutural do modelo foram levados em consideração quatro elementos principais: domínios, processos, capacidade e maturidade.

- Domínios representam o agrupamento de processos por área de conhecimento;
- Processos são a menor unidade atômica do modelo, estes são controlados usando práticas de gerenciamento;
- Capacidade é definida pelas métricas de um processo, permitindo que suas práticas de gerenciamento revelem o seu status;
- Maturidade é resultado da análise de capacidade de processos e domínios que operam em conjunto para estabelecer os controles de segurança e privacidade.

A Figura 7 apresenta os cinco níveis de capacidade de processo: Inicial, parcial, definido, gerenciado e otimizado.

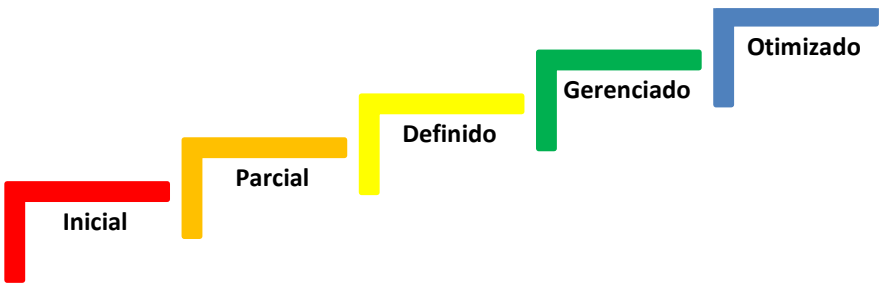


Figura 7 – Níveis de maturidade do MMSI.br. Fonte: Elaborado pelo Autor.

O Quadro 6 especifica os requisitos necessários para um processo atingir cada nível de capacidade e seu respectivo mapeamento para práticas de gerenciamento. A capacidade do processo é determinada pelas métricas produzidas pelo processo, estas são classificadas por tipo.

Quadro 6: Níveis de capacidade de processo. Fonte: Elaborado pelo Autor

Nível de Capacidade	Descrição
1 – Inicial	Não implementado e/ou sem documentação
2 - Parcial	Implementado e/ou documentado parcialmente
3 - Definido	Completamente implementado e documentado com revisões pontuais
4 - Gerenciado	Completamente implementado e documentado com revisões e avaliação de eficácia dos controles periodicamente
5 - Otimizado	Completamente implementado e documentado com revisões e avaliação de eficácia dos controles executadas periodicamente. Realização periódica de benchmarking e auditoria externa com o objetivo de melhoria contínua.

4.2. **Avaliação e melhoria contínua**

As áreas de tecnologia e segurança da informação são dinâmicas, os elementos associados tais como sistemas, usuários, dados e riscos estão em constante mudança. Deste modo, os requisitos de segurança da informação são alterados abruptamente e de forma cíclica. As mudanças afetam diretamente a segurança dos sistemas ao passo que estão associadas a elas novas ameaças e vulnerabilidades. A aderência aos procedimentos instituídos pela organização raramente é conseguida e os procedimentos se tornam desatualizados com o tempo, deste modo se torna necessária a reavaliação periódica da segurança da informação, através de um processo cíclico de gestão que possa ser repetido e reavaliado de tempos em tempos (NIELES et al., 2017).

O ciclo Plan-Do-Check-Act (PDCA), além de ser considerado o método mais utilizado para gestão da qualidade, pode condicionar a gestão das organizações a um ciclo lógico de melhorias contínuas para alcançar os resultados esperados. Um resultado é alcançado mais eficientemente quando as atividades e os recursos relacionados são gerenciados como processos, devendo ser mapeados, analisados e

controlados de forma inter-relacionada como um sistema, contribuindo para o sucesso das organizações (FIGUEIREDO, 2016) .

De acordo com a norma ABNT NBR ISO/IEC 27001 (2013), a abordagem de processo para a gestão da segurança da informação encoraja que os usuários administradores do SGSI enfatizem a importância de:

a) entendimento dos requisitos de segurança da informação de uma organização e da necessidade de estabelecer uma política e objetivos para a segurança de informação;

b) implementação e operação de controles para gerenciar os riscos de segurança da informação de uma organização no contexto dos riscos de negócio globais da organização;

c) monitoração e análise crítica do desempenho e eficácia do SGSI;

d) melhoria contínua baseada em medições objetivas.

4.3. **Controles de segurança da informação**

O modelo de maturidade apresentado neste trabalho utiliza a estrutura de objetivos de controle e controles da norma ABNT NBR ISO/IEC 27002 (2013) reconhecidos internacionalmente por serem adequados à gestão da segurança da informação. A versão utilizada, de 2013, contém 14 seções de controle de segurança da informação de um total de 35 objetivos de controle e 114 controles que referenciados no modelo apresentado.

Para cada controle sugerido pela norma que for considerado aplicável à organização será realizada uma avaliação de conformidade com as necessidades do negócio, fazendo-se uso de um método de medição para o registro da avaliação.

Cabe ressaltar que a estrutura da norma, apesar de ser abrangente, pode não conter todos os controles necessários aos diversos tipos de organizações, e poderá ser necessária a avaliação de controles adicionais que suportem os riscos, objetivos ou requisitos específicos aos quais a organização estiver submetida e necessite estar em conformidade.

4.4. **Métricas e avaliação**

A avaliação dos processos de acordo com um modelo de maturidade é atividade chave para implementação de governança. Após identificar processos e controles críticos, o uso de um modelo de maturidade permite a análise para identificação de lacunas que representam risco e a sua apresentação à administração. Com base nessa análise poderão ser avaliados e desenvolvidos planos para melhoria dos processos e controles considerados deficientes até o nível de desenvolvimento desejado. A medição por níveis de maturidade é capaz de fornecer a transparência do processo de gestão e permitir a realização de comparações entre ciclos de avaliação, bem como a realização de benchmarking entre organizações (COANDĂ; CIOACĂ; BRATU, 2017)

A abordagem por níveis de maturidade adotada neste trabalho deriva do modelo O-ISM3 (Open Information Security Management Maturity Model), este apresenta cinco níveis de classificação, onde baseada em uma escala simples de maturidade que demonstra como um processo evolui de uma capacidade Inicial (1) para uma capacidade otimizada (5).

4.5. **Domínios e processos**

O modelo é composto por 86 processos distribuídos em 12 domínios, estes são responsáveis por agrupar e organizar os processos relacionados aos mesmos objetivos, contribuindo para a categorização e avaliação dos gaps das organizações. Os domínios que compõem o modelo MMSI.br são apresentados a seguir:

- Estrutura de governança;
- Inventário de dados pessoais;
- Política de privacidade e proteção de dados;
- Privacidade de dados nas operações;
- Treinamento e conscientização;
- Gerenciamento de riscos de segurança da informação;
- Gerenciamento de riscos de terceiros;

- Plano de comunicação;
- Resposta aos titulares dos dados;
- Monitoramento de novas práticas operacionais;
- Gerenciamento de violação de privacidade de dados;
- Tratamento de dados.

A Figura 8 demonstra os níveis de maturidade e domínios do modelo MMSI.br.

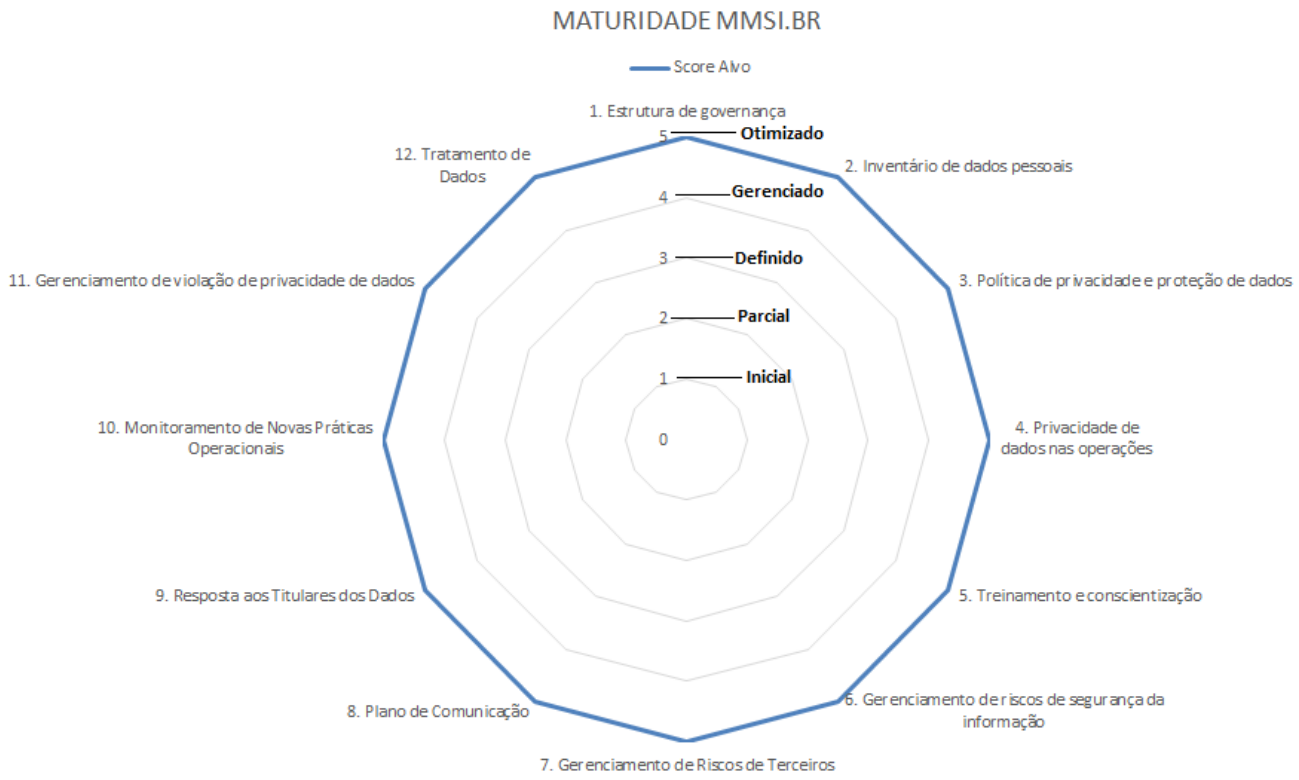


Figura 8 – Gráfico de radar com domínios e níveis de Maturidade do MMSI.br.
Fonte: Elaborado pelo Autor.

A Figura 9 demonstra o gráfico com um exemplo de avaliação de uma organização com o seu nível de maturidade por cada domínio do modelo MMSI.br.

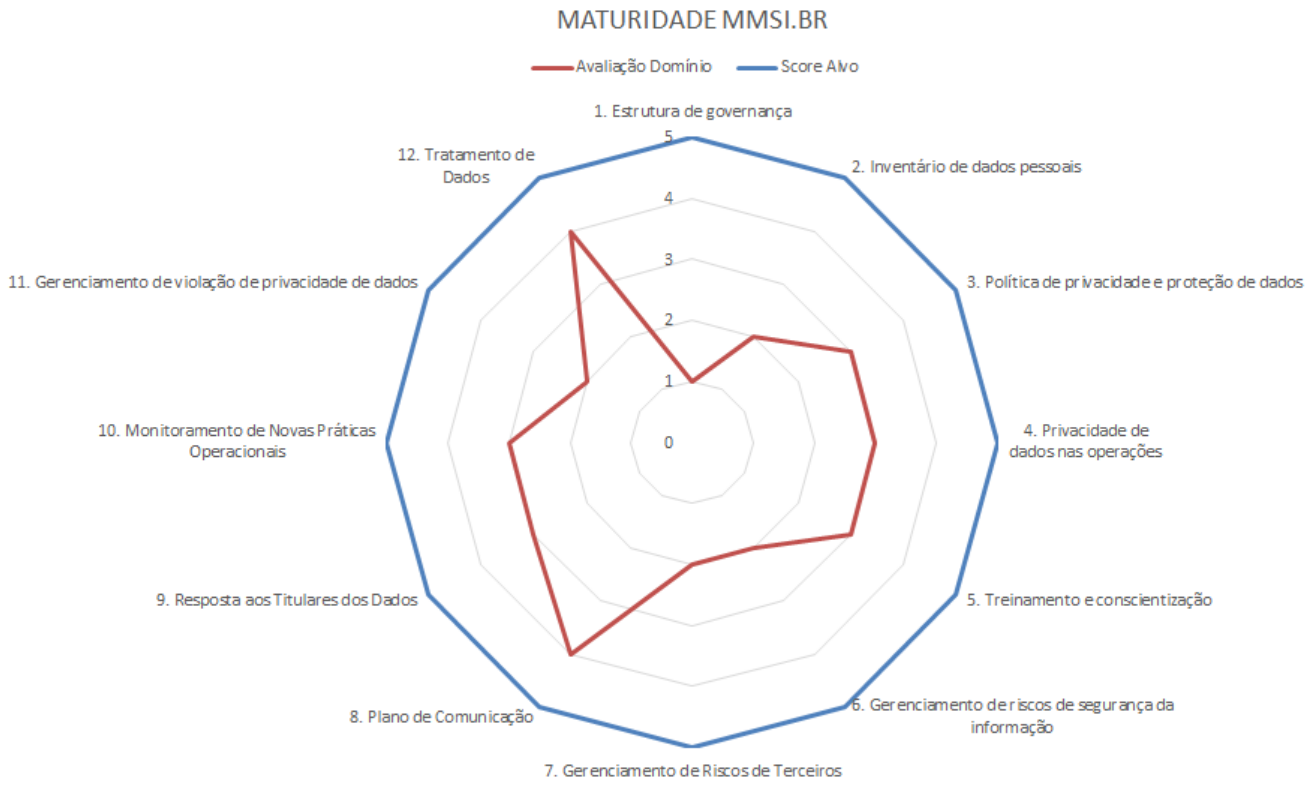


Figura 9 – Gráfico de radar com exemplo de resultado da aplicação do MMSI.br.
Fonte: Elaborado pelo Autor.

Conforme demonstrado no exemplo disposto na Figura 9, a organização avaliada apresentou nos domínios “Plano de comunicação” e “Tratamento de Dados” o nível de maturidade 4 – Gerenciado, tendo nos processos relacionados a estes domínios os melhores níveis de avaliação. Em contraponto, a organização teve seu menor nível de maturidade aferido no domínio “Estrutura de Governança” onde a avaliação atingiu o nível 1 – Inicial de maturidade, segundo o MMSI.br.

Como a avaliação do MMSI.br é realizada por processo a pontuação de cada domínio é calculada com base na média das avaliações dos processos associados. De modo a evidenciar os pontos fortes e fracos de cada organização avaliada.

O agrupamento dos processos por domínios é descrito na próxima seção, onde são demonstradas as capacidades associadas a cada nível de maturidade presente no modelo, permitindo a classificação adequada durante o processo de avaliação das organizações.

4.5.1. **Estrutura de governança**

Convém que a organização indique uma ou mais pessoas responsáveis pelo desenvolvimento, implementação, manutenção e monitoramento de um programa amplo de privacidade e governança da organização, para assegurar *compliance* com todas leis e regulamentações aplicáveis, relacionadas ao tratamento de dados pessoais (DP). O Quadro 7 mostra os processos referentes a este domínio com suas referências com as principais normas técnicas e lei geral de proteção de dados (LGPD).

Quadro 7: Processos do domínio estrutura de governança. Fonte: Elaborado pelo Autor.

ID do Processo	Processo	LGPD	ISO 27001 / 27002	ISO 27701
1.1	Atribuir a responsabilidade pela privacidade e proteção dos dados a um indivíduo (encarregado de dados)	Art. 41	5.1, 5.3, 6.1.1, 7.2.2	6.3.1.1, 6.4.2.2
1.2	Envolver a alta direção em privacidade e proteção de dados e atribuir responsabilidade pela privacidade e proteção dos dados em toda a organização	Art. 50	6.1.1	
1.3	Conduzir comunicação regular junto às partes interessadas internas da organização o status do gerenciamento de privacidade e proteção de dados	Art. 41, §2º	5.1.1	6.3.1.1
1.4	Reportar às partes interessadas externas da organização o status do gerenciamento de privacidade (por exemplo, órgãos reguladores, terceiros, clientes)	--	5.1.1	
1.5	Realizar uma avaliação de risco de privacidade e proteção de dados da empresa (DPIA)	Art. 50	4.1, 5.1.1, 18	5.2.1, 6.2.1.1, 6.3.1.1, 6.4.2.2, 6.15.1.3, 7.2.8
1.6	Integrar a privacidade de dados nas avaliações e relatórios de riscos corporativos	--	--	--
1.7	Manter um programa e uma estratégia visando assegurar a privacidade e proteção de dados	--	--	--
1.8	Exigir que os funcionários reconheçam e concordem em aderir às políticas de privacidade e proteção de dados	--	7.1.2, 7.2.2, 7.2.3	

No Quadro 8 são descritos detalhadamente os níveis de maturidade dos processos associados ao domínio estrutura de governança.

Quadro 8 - Níveis de maturidade dos processos do domínio estrutura de governança. Fonte: Elaborado pelo Autor.

ID do Processo	Processo	1 – Inicial	2 - Parcial	3 – Determinado	4 – Gerenciado	5 - Otimizado
		Resultados Esperados				
1.1	Atribuir a responsabilidade pela privacidade e proteção dos dados a um indivíduo (encarregado de dados)	Não há responsável atribuído	Responsável definido, mas não nomeado formalmente	Responsável definido e nomeado formalmente	Responsável definido, nomeado formalmente, reporta diretamente a alta direção sem acumular cargo	Responsável definido, nomeado formalmente, reporta diretamente a alta direção sem acumular cargo. O professional é certificado para atuar como encarregado de dados
1.2	Envolver a alta direção em privacidade e proteção de dados e atribuir responsabilidade pela privacidade e proteção dos dados em toda a organização	Não há comitê de privacidade e proteção de dados	Há comitê de privacidade e proteção de dados sem reuniões regulares	Há comitê de privacidade e proteção de dados com reuniões regulares	Há comitê de privacidade e proteção de dados com reuniões regulares, com a participação de membros das áreas de TI, Segurança, Jurídico e DPO	Há comitê de privacidade e proteção de dados com reuniões regulares, com a participação de membros das áreas de TI, Segurança, Jurídico, DPO (Líder) e Diretoria (Patrocinador).
1.3	Conduzir comunicação regular junto às partes interessadas internas da organização o status do gerenciamento de privacidade e proteção de dados	Não há comunicação e nem um plano definido.	Comunicação ocorre de forma esporádica, mas sem um plano definido.	Comunicação ocorre periodicamente e tem um plano definido.	Comunicação ocorre periodicamente e tem um plano definido. São utilizados múltiplos canais para atingir as partes interessadas	Há um plano de comunicação com periodicidade e responsável definido. São utilizados múltiplos canais para atingir as partes interessadas. A efetividade dos canais é medida através de indicadores
1.4	Reportar às partes interessadas externas da organização o status do gerenciamento de privacidade (por exemplo, órgãos reguladores, terceiros, clientes)	Não há comunicação e nem um plano definido.	Comunicação ocorre de forma esporádica, mas sem um plano definido.	Comunicação ocorre periodicamente e tem um plano definido.	Comunicação ocorre periodicamente e tem um plano definido. São utilizados múltiplos canais para atingir as partes interessadas	Há um plano de comunicação com periodicidade e responsável definido. São utilizados múltiplos canais para atingir as partes interessadas. A efetividade dos canais é medida através de indicadores

1.5	Realizar uma avaliação de risco de privacidade e proteção de dados da empresa (DPIA)	Os processos que tratam dados pessoais não estão mapeados	Os processos que tratam dados pessoais estão mapeados parcialmente	Os processos que tratam dados pessoais estão mapeados	Os processos que tratam dados pessoais estão mapeados e há um DPIA	Os processos que tratam dados pessoais estão mapeados, há um DPIA e um plano de ação com responsáveis definidos
1.6	Integrar a privacidade de dados nas avaliações e relatórios de riscos corporativos	Riscos relativos à privacidade de dados não estão mapeados.	Riscos relativos à privacidade de dados estão parcialmente mapeados.	Riscos relativos à privacidade de dados estão mapeados.	Riscos relativos à privacidade de dados estão mapeados, tem responsáveis e estão associados a um plano de ação.	Riscos relativos à privacidade de dados estão mapeados, tem responsáveis, estão associados a um plano de ação e são auditados.
1.7	Manter um programa e uma estratégia visando assegurar a privacidade e proteção de dados	Não há programa ou estratégia para a assegurar a privacidade e proteção de dados.	Ações para assegurar a privacidade e proteção de dados são tomadas, mas não há um programa definido.	Ações para assegurar a privacidade e proteção de dados são tomadas de acordo com um programa definido.	Ações para assegurar a privacidade e proteção de dados são tomadas de acordo com um programa definido. Há indicadores para medir a efetividade das ações.	Ações para assegurar a privacidade e proteção de dados são tomadas de acordo com um programa definido. Há indicadores para medir a efetividade das ações. São realizadas auditorias periódicas.
1.8	Exigir que os funcionários reconheçam e concordem em aderir às políticas de privacidade e proteção de dados	Não há política de privacidade e proteção de dados	Há política de privacidade e proteção de dados, mas não é reconhecida e assinada pelos funcionários em sua totalidade	Há política de privacidade e proteção de dados, esta é reconhecida e assinada pelos funcionários em sua totalidade	Há política de privacidade e proteção de dados, esta é reconhecida e assinada pelos funcionários em sua totalidade. O documento é revisado periodicamente.	Há política de privacidade e proteção de dados, esta é reconhecida e assinada pelos funcionários em sua totalidade. O documento é revisado periodicamente e as alterações são informadas aos funcionários.

4.5.2. **inventário de dados pessoais**

Convém que a organização determine e mantenha de maneira segura os registros necessários ao suporte às suas obrigações para o tratamento de dados pessoais. Uma maneira de manter os registros de tratamento dos dados é ter um inventário ou uma lista de atividades de tratamento de dados pessoais que a organização realiza. O Quadro 9 mostra os processos referentes a este domínio com suas referências com as principais normas técnicas e lei geral de proteção de dados (LGPD).

Quadro 9 - Processos do domínio inventário de dados pessoais. Fonte: Elaborado pelo Autor.

ID do Processo	Processo	LGPD	ISO 27001 / 27002	ISO 27701
2.1	Manter um inventário de dados pessoais que são tratados	Art. 37	8.1.1	6.12.1.2, 7.5.2, 7.5.3, 7.5.4, 8.2.6, 8.4.2, 8.5.2, 8.5.3
2.2	Classificar os dados pessoais tratados	--	8.2	
2.3	Obter aprovação dos reguladores e/ou autoridades para processamento de dados e registrar bancos de dados onde o registro é necessário para aprovação prévia	Art. 33, 36	--	7.5.1, 8.5.1
2.4	Manter registros do mecanismo de transferência usado para fluxos de dados transfronteiriços e aprovações de órgãos reguladores	Art. 33, Art. 37	13.2	7.5.1, 8.5.1

No Quadro 10 são descritos detalhadamente os níveis de maturidade dos processos associados ao domínio inventário de dados pessoais. Fonte: Autor.

Quadro 10 - Níveis de maturidade dos processos do domínio inventário de dados pessoais. Fonte: Elaborado pelo Autor.

ID do Processo	Processo	1 – Inicial	2 - Parcial	3 - Determinado	4 – Gerenciado	5 - Otimizado
		Resultados Esperados				
2.1	Manter um inventário de dados pessoais que são tratadas	Não há um inventário dos dados pessoais tratados	Há um inventário parcial dos dados pessoais tratados	Há um inventário completo dos dados pessoais tratados em formato 5W2H ou sistema	Há um inventário completo dos dados pessoais tratados em formato 5W2H ou sistema. Isso é revisado periodicamente e mantido descentralizadamente	Há um inventário completo dos dados pessoais tratados em formato 5W2H ou sistema. Isso é revisado periodicamente e mantido centralizadamente.
2.2	Classificar os dados pessoais tratados	Não há política de classificação de dados	Há política de classificação de dados de dados, mas dados são classificados parcialmente	Há política de classificação de dados de dados e estão são classificados manualmente	Há política de classificação de dados de dados e estes são classificados automaticamente	Há política de classificação de dados de dados e estes são classificados automaticamente. Há monitoração de dados através de solução de Data Loss Prevention (DLP).
2.3	Obter aprovação dos reguladores e/ou autoridades para processamento de dados e registrar bancos de dados onde o este é necessário para aprovação prévia	Dados sensíveis não estão mapeados e são tratados sem aprovação das autoridades	Dados sensíveis estão parcialmente mapeados e são tratados sem aprovação das autoridades	Dados sensíveis estão mapeados e são tratados com aprovação das autoridades	Dados sensíveis estão mapeados e são tratados com aprovação das autoridades. São utilizados recursos de mascaramento e pseudoanonimização	Dados sensíveis estão mapeados e são tratados com aprovação das autoridades. São utilizados recursos de mascaramento e anonimização.
2.4	Manter registros do mecanismo de transferência usado para fluxos de dados transfronteiriços e aprovações de órgãos reguladores	Dados pessoais são transferidos internacionalmente, mas sem adoção de mecanismo de transferências e aprovação das autoridades	Dados pessoais são transferidos internacionalmente, são adotados parcialmente mecanismos de transferências, tais como RCV e Cláusulas contratuais.	Dados pessoais são transferidos internacionalmente com permissão das autoridades, são adotados mecanismos de transferências, tais como RCV e Cláusulas contratuais.	Dados pessoais são transferidos internacionalmente com permissão das autoridades, são adotados mecanismos de transferências, tais como RCV e Cláusulas contratuais. Bases legais estão definidas para a transferência de dados.	Dados pessoais são transferidos internacionalmente com permissão das autoridades, são adotados mecanismos de transferências, tais como RCV e Cláusulas contratuais. Bases legais estão definidas para a transferência de dados. Transferências ocorrem via canal criptografado utilizando VPN Site to Site.

4.5.3. **POLÍTICA DE PRIVACIDADE E PROTEÇÃO DE DADOS**

A política de privacidade é um dos instrumentos de implementação do *privacy by design* ou privacidade desde a concepção, esta é uma abordagem ligada à engenharia de Sistemas que preza pela privacidade do usuário durante todo o processo de construção de uma solução. Este documento é considerado uma medida organizacional para a proteção de dados e tem como objetivo dar visibilidade ao tratamento de dados pessoais em um determinado serviço, atendendo aos princípios da Lei Geral de Proteção de Dados Pessoais (LGPD). O Quadro 11 mostra os processos associados a este domínio com suas referências as principais normas técnicas e a LGPD.

Quadro 11: Processos do domínio política de privacidade e proteção de dados. Fonte: Elaborado pelo Autor.

ID do Processo	Processo	LGPD	ISO 27001 / 27002	ISO 27701
3.1	Manter uma política de privacidade e proteção de dados para funcionários contendo as bases legais para o tratamento de dados pessoais	Art. 6, 7, 10, 11, 14, 15 e 50	5.1, 6.1.2, 6.2, 8.2.1, 8.2.2, 8.3.1, 8.3.2, 8.3.3, 9.2.1, 9.2.2, 9.4.2, 10, 11.2.7, 11.2.9, 12.3.1, 12.4.1, 12.4.2, 13.2.1, 13.2.4, 14.1.2, 14.3.1, 15.1.2, 16.1.1, 18.1.1, 18.1.3	5.2.1, 6.2.1.1, 6.3.2.1, 6.5.2.1, 6.5.2.2, 6.5.3.1, 6.5.3.2, 6.5.3.3, 6.6.2.1, 6.6.2.2, 6.6.4.2, 6.8.2.7, 6.8.2.9, 6.9.3.1, 6.9.4.1, 6.9.4.2, 6.10.2.1, 6.10.2.4, 6.11.1.2, 6.11.1.3, 6.12.1.2, 6.13.1.1, 6.15.1.1, 6.15.1.3, 7.2.1, 7.2.2, 7.2.8, 7.3.6, 7.4.1, 7.4.3, 7.4.4, 7.4.5, 7.4.6, 7.4.8, 7.4.9, 8.2.2, 8.4.1, 8.4.3
3.2	Manter uma política de privacidade e proteção de dados para terceiros contendo as bases legais para o tratamento de dados pessoais	Art. 6, 7, 10, 11, 14, 15 e 50	5.1, 6.1.2, 6.2, 8.2.1, 8.2.2, 8.3.1, 8.3.2, 8.3.3, 9.2.1, 9.2.2, 9.4.2, 10, 11.2.7, 11.2.9, 12.3.1, 12.4.1, 12.4.2, 13.2.1, 13.2.4, 14.1.2, 14.3.1,	5.2.1, 6.2.1.1, 6.3.2.1, 6.5.2.1, 6.5.2.2, 6.5.3.1, 6.5.3.2, 6.5.3.3, 6.6.2.1, 6.6.2.2, 6.6.4.2, 6.8.2.7, 6.8.2.9, 6.9.3.1, 6.9.4.1,6.9.4.2, 6.10.2.1, 6.10.2.4, 6.11.1.2, 6.11,3.1, 6.12.1.2, 6.13.1.1, 6.15.1.1, 6.15.1.3, 7.2.1 7.2.2, 7.2.8, 7.3.6, 7.4.1, 7.4.3, 7.4.4,

			15.1.2, 16.1.1, 18.1.1, 18.1.3,	7.4.5, 7.4.6, 7.4.8, 7.4.9, 8.2.2, 8.4.1, 8.4.3
3.3	Integrar ética ao tratamento de dados através de códigos de conduta organizacional	Art. 50, II	--	--
3.4	Manter atualizados procedimentos para coleta e uso de dados pessoais e dados sensíveis	Art. 11 e 14	8.1.3	7.2.2, 7.2.4, 7.2.3, 7.3.1, 7.3.3, 7.3.9

No Quadro 12 são descritos detalhadamente os níveis de maturidade dos processos associados ao domínio política de privacidade e proteção de dados.

Quadro 12 - Níveis de maturidade dos processos do domínio inventário de dados pessoais. Fonte: Elaborado pelo Autor.

ID do Processo	Processo	1 – Inicial	2 - Parcial	3 - Determinado	4 – Gerenciado	5 - Otimizado
		Resultados Esperados				
3.1	Manter uma política de privacidade e proteção de dados para funcionários contendo as bases legais para o tratamento de dados pessoais	Não há política de privacidade e proteção de dados para funcionários	Há política de privacidade e proteção de dados para funcionários	Há política de privacidade e proteção de dados para funcionários e estes foram treinados	Há política de privacidade e proteção de dados para funcionários e estes foram treinados. O documento é revisado periodicamente.	Há política de privacidade e proteção de dados para funcionários e estes foram treinados. O documento é revisado periodicamente e divulgado adequadamente na organização.
3.2	Manter uma política de privacidade e proteção de dados para terceiros contendo as bases legais para o tratamento de dados pessoais	Não há política de privacidade e proteção de dados para terceiros	Há política de privacidade e proteção de dados para terceiros	Há política de privacidade e proteção de dados para terceiros e estes foram treinados	Há política de privacidade e proteção de dados para terceiros e estes foram treinados. O documento é revisado periodicamente.	Há política de privacidade e proteção de dados para terceiros e estes foram treinados. O documento é revisado periodicamente e divulgado adequadamente na organização.
3.3	Integrar ética ao tratamento de dados através de códigos de conduta organizacional	Não há um código de conduta e ética organizacional	Há um código de conduta e ética organizacional, mas não aborda privacidade e proteção de dados	Há um código de conduta e ética organizacional que aborda privacidade e proteção de dados	Há um código de conduta e ética organizacional que aborda privacidade e proteção de dados	Há um código de conduta e ética organizacional que aborda privacidade e proteção de dados. Colaboradores recebem treinamento específico.

3.4	Manter atualizados procedimentos para coleta e uso de dados pessoais e dados sensíveis	Não há procedimentos documentados	Há procedimentos parcialmente documentados	Todos os procedimentos relacionados estão documentados	Todos os procedimentos relacionados estão documentados e são revisados periodicamente	Todos os procedimentos relacionados estão documentados, são revisados e auditados periodicamente

4.5.4. **Privacidade de dados nas operações**

Integrar a privacidade de dados nas operações e projetos consiste em estabelecer mecanismo para normatização, registro de consentimentos de titulares e resposta as solicitações dos titulares dos dados. O Quadro 13 mostra os processos associados a este domínio com suas referências as principais normas técnicas e a LGPD.

Quadro 13: Processos do domínio Privacidade de dados nas operações. Fonte: Elaborado pelo Autor.

ID do Processo	Processo	LGPD	ISO 27001 / 27002	ISO 27701
4.1	Manter políticas e procedimentos para identificação e manutenção da qualidade dos dados (válidos e atualizados).	Art. 6 e 37	6.2.1, 7.2.2, 8.2.2, 8.3.1, 8.3.2, 8.3.3, 9.2.1, 9.2.2, 9.4.2, 11.2.7, 11.2.9, 12.3.1, 12.4.1, 12.4.2, 13.2.1, 13.2.4, 14.1.2, 14.3.1, 16.1.1, 18.1.1, 18.1.3	6.3.2.1, 6.4.2.2, 6.5.2.1, 6.5.2.2, 6.5.3.1, 6.5.3.2, 6.5.3.3, 6.6.2.1, 6.6.2.2, 6.6.4.2, 6.8.2.7, 6.8.2.9, 6.9.3.1, 6.9.4.1, 6.9.4.2, 6.10.2.1, 6.10.2.4, 6.11.1.2, 6.11.3.1, 6.12.1.2, 6.13.1.1, 6.15.1.1, 6.15.1.3, 7.2.1, 7.2.2, 7.2.6, 7.2.8, 7.3.6, 7.4.1, 7.4.3, 7.4.4, 7.4.5, 7.4.6, 7.4.8, 7.4.9, 8.2.2, 8.4.1, 8.4.3
4.2	Manter políticas e procedimentos para revisar o tratamento total ou parcialmente por meios automatizados, tais como uso de cookies e mecanismos de rastreamento de clientes	Art. 20	8, 9.2, 9.4, 12, 13	--

4.3	Manter políticas e procedimentos para obter consentimento válido por parte dos titulares dos dados	Art. 8	--	--
4.4	Manter políticas e procedimentos para retenção e destruição segura de dados pessoais	Art. 6 e 16	8.2.2,8.3.1,8.3.2,8.3.3,9.2.1,9.2.2,9.4.2,11,12.3.1,12.4.1,12.4.2,13.2.1,13.2.4,14.1.2,14.3.1,16.1.1,18.1.1,18.1.3	6.3.2.1,6.4.2.2,6.5.2.1,6.5.2.2,6.5.3.1,6.5.3.2,6.5.3.3,6.6.2.1,6.6.2.2,6.6.4.2,6.8.2.7,6.8.2.9,6.9.3.1,6.9.4.1,6.9.4.2,6.10.2.1,6.10.2.4,6.11.1.2,6.11.3.1,6.12.1.2,6.13.1.1,6.15.1.1,6.15.1.3,7.2.1,7.2.2,7.2.6,7.2.8,7.3.6,7.4.1,7.4.3,7.4.4,7.4.5,7.4.6,7.4.8,7.4.9,8.2.2,8.4.1,8.4.3
4.5	Integrar privacidade e proteção de dados em práticas de marketing direto com clientes por email e telefone	--	8.1.3, 9.2,9.4,12, 13	7.3.2,7.3.5
4.6	Integrar a privacidade e proteção de dados nas práticas de recrutamento, seleção e contratação de colaboradores	--	7.1,15	--
4.7	Integrar a privacidade de dados ao uso de práticas de mídia social da organização	--	8.1.3	7.2.2,7.2.3
4.8	Integrar a privacidade e proteção de dados nas políticas / procedimentos Bring Your Own Device (BYOD), se houver	--	6.2,8.1.2,8.1.3,11.2	--
4.9	Integrar a privacidade e proteção de dados nas práticas de segurança e medicina do trabalho	--	--	--
4.10	Integrar a privacidade e proteção de dados em práticas para monitorar funcionários	--	7.2,7.3,12.4	--
4.11	Integrar a privacidade e proteção de dados ao uso de vigilância de CFTV / vídeo	--	8.1.3	--
4.12	Integrar a privacidade e proteção de dados ao uso de dispositivos de localização geográfica (rastreamento e / ou localização)	--	8.1.3	--
4.13	Integrar a privacidade dos dados no acesso delegado às contas de email da empresa dos funcionários (por exemplo, férias, LOA, rescisão)	--	8.1.3	--

4.14	Integrar a privacidade e proteção de dados às práticas de descoberta eletrônica	--	8.1.3, 9.2,9.4.4,12.7	--
4.15	Integrar a privacidade e proteção de dados em práticas para divulgação e para fins de aplicação da lei	Art. 50, §3º		--

No Quadro 14 são descritos detalhadamente os níveis de maturidade dos processos associados ao domínio privacidade de dados nas operações.

Quadro 14 - Níveis de maturidade dos processos do domínio privacidade de dados nas operações. Fonte: Elaborado pelo Autor.

ID do Processo	Processo	1 – Inicial	2 - Parcial	3 - Determinado	4 – Gerenciado	5 - Otimizado
		Resultados Esperados				
4.1	Manter políticas e procedimentos para identificação e manutenção da qualidade dos dados (válidos e atualizados).	Não há políticas e procedimentos relacionados documentados	Há políticas e procedimentos relacionados parcialmente documentados	Há políticas e procedimentos relacionados documentados	Há políticas e procedimentos relacionados documentados e são revisados periodicamente	Há políticas e procedimentos relacionados documentados, estes são revisados e auditados periodicamente
4.2	Manter políticas e procedimentos para revisar o tratamento total ou parcialmente por meios automatizados, tais como uso de cookies e mecanismos de rastreamento de clientes	Não há políticas e procedimentos relacionados documentados	Há políticas e procedimentos relacionados parcialmente documentados	Há políticas e procedimentos relacionados documentados	Há políticas e procedimentos relacionados documentados e são revisados periodicamente	Há políticas e procedimentos relacionados documentados, estes são revisados e auditados periodicamente
4.3	Manter políticas e procedimentos para obter	Não há políticas e procedimentos	Há políticas e procedimentos relacionados	Há políticas e procedimentos	Há políticas e procedimentos relacionados	Há políticas e procedimentos relacionados documentados, estes são

	consentimento válido por parte dos titulares dos dados	relacionados documentados	parcialmente documentados	relacionados documentados	documentados e são revisados periodicamente	revisados e auditados periodicamente
4.4	Manter políticas e procedimentos para retenção e destruição segura de dados pessoais	Não há políticas e procedimentos relacionados documentados	Há políticas e procedimentos relacionados parcialmente documentados	Há políticas e procedimentos relacionados documentados	Há políticas e procedimentos relacionados documentados e são revisados periodicamente	Há políticas e procedimentos relacionados documentados, estes são revisados e auditados periodicamente
4.5	Integrar privacidade e proteção de dados em práticas de marketing direto com clientes por email e telefone	Não há políticas e procedimentos relacionados documentados	Há políticas e procedimentos relacionados parcialmente documentados	Há políticas e procedimentos relacionados documentados	Há políticas e procedimentos relacionados documentados e são revisados periodicamente	Há políticas e procedimentos relacionados documentados, estes são revisados e auditados periodicamente
4.6	Integrar a privacidade e proteção de dados nas práticas de recrutamento, seleção e contratação de colaboradores	Não há políticas e procedimentos relacionados documentados	Há políticas e procedimentos relacionados parcialmente documentados	Há políticas e procedimentos relacionados documentados	Há políticas e procedimentos relacionados documentados e são revisados periodicamente	Há políticas e procedimentos relacionados documentados, estes são revisados e auditados periodicamente
4.7	Integrar a privacidade de dados ao uso de práticas de mídia social da organização	Não há políticas e procedimentos relacionados documentados	Há políticas e procedimentos relacionados parcialmente documentados	Há políticas e procedimentos relacionados documentados	Há políticas e procedimentos relacionados documentados e são revisados periodicamente	Há políticas e procedimentos relacionados documentados, estes são revisados e auditados periodicamente
4.8	Integrar a privacidade e proteção de dados nas políticas / procedimentos Bring Your Own Device (BYOD), se houver	Não há políticas e procedimentos relacionados documentados	Há políticas e procedimentos relacionados parcialmente documentados	Há políticas e procedimentos relacionados documentados	Há políticas e procedimentos relacionados documentados e são revisados periodicamente	Há políticas e procedimentos relacionados documentados, estes são revisados e auditados periodicamente
4.9	Integrar a privacidade e proteção de dados nas práticas de segurança e medicina do trabalho	Não há políticas e procedimentos relacionados documentados	Há políticas e procedimentos relacionados parcialmente documentados	Há políticas e procedimentos relacionados documentados	Há políticas e procedimentos relacionados documentados e são revisados periodicamente	Há políticas e procedimentos relacionados documentados, estes são revisados e auditados periodicamente
4.10	Integrar a privacidade e proteção de dados em práticas para monitorar funcionários	Não há políticas e procedimentos relacionados documentados	Há políticas e procedimentos relacionados parcialmente documentados	Há políticas e procedimentos relacionados documentados	Há políticas e procedimentos relacionados documentados e são revisados periodicamente	Há políticas e procedimentos relacionados documentados, estes são revisados e auditados periodicamente

4.11	Integrar a privacidade e proteção de dados ao uso de vigilância por vídeo (CFTV)	Não há políticas e procedimentos relacionados documentados	Há políticas e procedimentos relacionados parcialmente documentados	Há políticas e procedimentos relacionados documentados	Há políticas e procedimentos relacionados documentados e são revisados periodicamente	Há políticas e procedimentos relacionados documentados, estes são revisados e auditados periodicamente
4.12	Integrar a privacidade e proteção de dados ao uso de dispositivos de geolocalização geográfica	Não há políticas e procedimentos relacionados documentados	Há políticas e procedimentos relacionados parcialmente documentados	Há políticas e procedimentos relacionados documentados	Há políticas e procedimentos relacionados documentados e são revisados periodicamente	Há políticas e procedimentos relacionados documentados, estes são revisados e auditados periodicamente
4.13	Integrar a privacidade dos dados no acesso delegado às contas de email da empresa dos funcionários (por exemplo, férias, LOA, rescisão)	Não há políticas e procedimentos relacionados documentados	Há políticas e procedimentos relacionados parcialmente documentados	Há políticas e procedimentos relacionados documentados	Há políticas e procedimentos relacionados documentados e são revisados periodicamente	Há políticas e procedimentos relacionados documentados, estes são revisados e auditados periodicamente
4.14	Integrar a privacidade e proteção de dados às práticas de descoberta eletrônica	Não há políticas e procedimentos relacionados documentados	Há políticas e procedimentos relacionados parcialmente documentados	Há políticas e procedimentos relacionados documentados	Há políticas e procedimentos relacionados documentados e são revisados periodicamente	Há políticas e procedimentos relacionados documentados, estes são revisados e auditados periodicamente
4.15	Integrar a privacidade e proteção de dados em práticas para divulgação e para fins de aplicação da lei	Não há políticas e procedimentos relacionados documentados	Há políticas e procedimentos relacionados parcialmente documentados	Há políticas e procedimentos relacionados documentados	Há políticas e procedimentos relacionados documentados e são revisados periodicamente	Há políticas e procedimentos relacionados documentados, estes são revisados e auditados periodicamente

4.5.5. **Treinamento e Conscientização**

Estabelecer um programa de treinamento e conscientização ligado à privacidade e proteção de dados consiste em disseminar a cultura em segurança, apresentando os princípios para os usuários de modo a promover o engajamento e a consciência

sobre o papel de cada um para a proteção e privacidade dos dados na organização. O Quadro 15 mostra os processos associados a este domínio com suas referências as principais normas técnicas e a LGPD.

Quadro 15: Processos do domínio treinamento e conscientização. Fonte: Elaborado pelo Autor.

ID do Processo	Processo	LGPD	ISO 27001 / 27002	ISO 27701
5.1	Conduzir treinamento em privacidade e proteção de dados	Art. 41, 50	7.2.2	6.3.1.1, 6.4.2.2
5.2	Incorporar a privacidade e proteção dos dados ao treinamento operacional, como RH, segurança etc.	Art. 41, III	7.2.2	--
5.3	Desenvolver e publicar boletim de privacidade e proteção de dados ou incorporar a privacidade e proteção de dados às comunicações corporativas existentes	--	--	--
5.4	Prover um repositório de informações de privacidade e proteção de dados, por exemplo, uma intranet interna de privacidade e proteção de dados	Art. 41, III	7.2.2	--
5.5	Realizar eventos de conscientização de privacidade e proteção de dados (por exemplo, um dia / semana anual de privacidade de dados)	Art. 41, III	7.2.2	--
5.6	Fornecer educação e treinamento contínuos para o DPO e manter a certificação dos responsáveis pela privacidade e proteção dos dados	Art. 41, III	--	--

No Quadro 16 são descritos detalhadamente os níveis de maturidade dos processos associados ao domínio Treinamento e conscientização.

Quadro 16 - Níveis de maturidade dos processos do domínio Treinamento e conscientização. Fonte: Elaborado pelo Autor.

ID do Processo	Processo	1 – Inicial	2 - Parcial	3 - Determinado	4 – Gerenciado	5 - Otimizado
		Resultados Esperados				
5.1	Conduzir treinamento em privacidade e proteção de dados	Não Treinamento em privacidade e proteção de dados	Há treinamento em privacidade e proteção de dados, mas não periódico	Há treinamento em privacidade e proteção de dados periodicamente	Há treinamento em privacidade e proteção de dados periodicamente com realização de avaliação de impacto	Há treinamento em privacidade e proteção de dados periodicamente com realização de avaliação de impacto. O resultado das avaliações é utilizado para aprimoramento contínuo do treinamento.
5.2	Incorporar a privacidade e proteção dos dados ao treinamento operacional, como RH, segurança, etc	O treinamento de privacidade e proteção de dados não faz parte do treinamento de ambientação.	Há treinamento parcial de privacidade e proteção de dados durante ambientação.	Há treinamento completo de privacidade e proteção de dados durante ambientação.	Há treinamento completo de privacidade e proteção de dados durante ambientação. Ao final é realizada uma avaliação de impacto.	Há treinamento completo de privacidade e proteção de dados durante ambientação. Ao final é realizada uma avaliação de impacto e os resultados são utilizados para o aprimoramento contínuo do treinamento.
5.3	Desenvolver e publicar boletim de privacidade e proteção de dados ou incorporar a privacidade e proteção de dados às comunicações corporativas existentes	Não há boletim de privacidade e proteção de dados enviado pela área de comunicação.	Há boletim não periódico de privacidade e proteção de dados enviado pela área de comunicação.	Há boletim periódico de privacidade e proteção de dados enviado pela área de comunicação.	Há boletim periódico de privacidade e proteção de dados enviado pela área de comunicação. São utilizados muito canais de divulgação para melhor atingimento do público alvo	Há boletim periódico de privacidade e proteção de dados enviado pela área de comunicação. São utilizados muito canais de divulgação para melhor atingimento do público alvo. Há métricas de aferição da efetividade dos canais de comunicação.
5.4	Fornecer um repositório de informações de privacidade e proteção de dados, por exemplo, uma intranet interna de privacidade e e proteção de dados	Não há repositório de materiais relacionados a privacidade e proteção de dados.	Há repositório de materiais relacionados a privacidade e proteção de dados. Contudo este não é divulgado.	Há repositório de materiais relacionados a privacidade e proteção de dados. Este é divulgado	Há repositório de materiais relacionados a privacidade e proteção de dados. Este é divulgado e atualizado periodicamente manualmente.	Há repositório de materiais relacionados a privacidade e proteção de dados. Este é divulgado e atualizado periodicamente automaticamente.

5.5	Realizar eventos de conscientização de privacidade e proteção de dados (por exemplo, um dia / semana anual de privacidade de dados)	Não são realizados eventos de conscientização de privacidade e proteção de dados	São realizados eventos de conscientização de privacidade e proteção de dados, mas sem calendário pré-definido.	São realizados eventos de conscientização de privacidade e proteção de dados, com calendário pré-definido.	São realizados eventos de conscientização de privacidade e proteção de dados, com calendário pré-definido. O evento conta com a participação da diretoria e gerência.	São realizados eventos de conscientização de privacidade e proteção de dados, com calendário pré-definido. O evento conta com a participação da diretoria e gerência. Há métricas para aferir o nível de participação e engajamento dos colaboradores.
5.6	Fornecer educação e treinamento contínuos para o DPO e manter a certificação dos responsáveis pela privacidade e proteção dos dados	Não são realizados treinamentos para o DPO	São realizados treinamentos não periódicos para o DPO	São realizados treinamentos periódicos para o DPO.	São realizados treinamentos periódicos para o DPO. E as certificações são renovadas não periodicamente	São realizados treinamentos periódicos para o DPO. E as certificações são renovadas periodicamente

4.5.6. **Gerenciamento de riscos de segurança da informação**

Mapear os riscos de segurança da informação é um passo fundamental para entendimento das vulnerabilidades da organização bem como para definição das estratégias de tratamento aos riscos. O Quadro 17 mostra os processos associados a este domínio com suas referências as principais normas técnicas e a LGPD.

Quadro 17: Processos do domínio Gerenciamento de riscos de segurança da informação. Fonte: Elaborado pelo Autor.

ID do Processo	Processo	LGPD	ISO 27001 / 27002	ISO 27701
6.1	Integrar o risco de privacidade e proteção de dados nas avaliações de risco de segurança	Art. 50	5.1, 6.1.2, 6.2, 8 ,10,12.3.1, 14.1.2, 15.1.2, 18.1.1, 18.2.1, 18.2.3	5.2.1, 5.2.3, 5.2.4, 5.4.1.2, 5.4.1.3, 6.9.3.1, 6.11.1.2, 6.12.1.2, 6.15.1.1, 6.15.2.1, 6.15.2.3, 7.2.1, 7.4.5, 8.2.2
6.2	Integrar privacidade e proteção de dados em uma política de segurança da informação	Art. 6, 46, 49	5.1, 6.1.2,6.2,6.2.1,7.2.2, 8.2.2,8.3.1,8.3.2,8.3.3,9.2.1 ,9.2.2,9.4.2,10,11.2.7,11.2. 9,12.3.1,12.4.1,12.4.2,13.2. 1,13.2.4,14.1.2,14.3.1, 15.1.2,16.1.1,18.1.1,18.1.3, 18.2.3	5.2.1, 5.2.3, 5.2.4, 5.4.1.2, 5.4.1.3, 6.3.2.1, 6.4.2.2, 6.5.2.1, 6.5.2.2, 6.5.3.1, 6.5.3.2,6.5.3.3, 6.6.2.1, 6.6.2.2, 6.6.4.2, 6.8.2.7, 6.8.2.9, 6.9.3.1, 6.9.4.1, 6.9.4.2, 6.10.2.1, 6.10.2.4, 6.11.1.2, 6.11.3.1, 6.12.1.2, 6.13.1.1,6.15.1.1, 6.15.1.3, 6.15.2.1, 6.15.2.3, 7.2.1,7.2.2,7.2.6,7.2.8,7.3.6,7.4.1,7.4.3,7. 4.4,7.4.5,7.4.6,7.4.8,7.4.9,8.2.2,8.4.1,8.4. 3
6.3	Manter medidas técnicas de segurança (por exemplo, detecção de intrusões, firewalls, monitoramento)	Art. 46	6.1.2, 6.2,8.3, 9, 11.2,12.2,12.4,12.5,12.6, 13, 14	5.2.1,5.2.3,5.2.4,5.4.1.2,5.4.1.3, 6.9.3.1,6.11.1.2,6.12.1.2,6.15.1.1,6.15.2.1 ,6.15.2.3,7.2.1,7.4.5,8.2.2
6.4	Manter medidas para criptografar dados pessoais em repouso e em movimento	--	10, 18.1.5	5.2.1,5.2.3,5.2.4,5.4.1.2,5.4.1.3, 6.9.3.1,6.11.1.2,6.12.1.2,6.15.1.1,6.15.2.1 ,6.15.2.3,7.2.1,7.4.5,8.2.2
6.5	Manter procedimentos para restringir o acesso a dados pessoais (por exemplo, acesso baseado em função, segregação de funções)	--	8.1.3, 9,12.4	5.2.1, 5.2.3, 5.2.4, 5.4.1.2, 5.4.1.3, 6.9.3.1, 6.11.1.2, 6.12.1.2, 6.15.1.1, 6.15.2.1, 6.15.2.3, 7.2.1, 7.4.5, 8.2.2
6.6	Integrar a privacidade e proteção de dados a uma política de segurança corporativa (proteção de instalações físicas e ativos físicos)	--	11	--
6.7	Manter plano de continuidade de negócios	--	12.3, 17	6.9.3

6.8	Manter uma estratégia de prevenção de perda de dados (backup)	--	17,2	--
6.9	Conduzir testes regulares quanto ao desempenho de segurança de dados (pentest)	--	18.2.1	5.2.1,5.2.3,5.2.4,5.4.1.2,5.4.1.3, 6.9.3.1,6.11.1.2,6.12.1.2,6.15.1.1,6.15.2.1 ,6.15.2.3,7.2.1,7.4.5,8.2.2
6.10	Manter uma certificação de segurança (por exemplo, ISO)	--	--	--

No Quadro 18 são descritos detalhadamente os níveis de maturidade dos processos associados ao domínio gerenciamento de riscos de segurança da informação.

Quadro 18 - Níveis de maturidade dos processos do domínio Gerenciamento de riscos de segurança da informação. Fonte: Elaborado pelo Autor.

ID do Processo	Processo	1 – Inicial	2 - Parcial	3 - Determinado	4 – Gerenciado	5 - Otimizado
		Resultados Esperados				
6.1	Integrar o risco de privacidade e proteção de dados nas avaliações de risco de segurança	Na matriz de risco da organização não estão listados riscos relacionados a privacidade e proteção de dados.	Na matriz de risco da organização estão listados parcialmente os riscos relacionados a privacidade e proteção de dados.	Na matriz de risco da organização estão listados os riscos relacionados a privacidade e proteção de dados.	Na matriz de risco da organização estão listados os riscos relacionados a privacidade e proteção de dados. Há um plano de ação para cada um dos riscos.	Na matriz de risco da organização estão listados os riscos relacionados a privacidade e proteção de dados. Há um plano de ação para cada um dos riscos. Os controles são auditados periodicamente.
6.2	Integrar privacidade e proteção de dados em uma política de segurança da informação	Não há política de segurança da informação e privacidade	Há política de segurança da informação, mas não política de privacidade e	Há política de segurança da informação e uma política de privacidade e	Há política de segurança da informação e uma política de privacidade e proteção de dados baseada na ISO 27701	Há política de segurança da informação e uma política de privacidade e proteção de dados baseada na ISO 27701. Os controles são auditados periodicamente.

			proteção de dados ou vice versa	proteção de dados.		
6.3	Manter medidas técnicas de segurança (por exemplo, detecção de intrusões, firewalls, monitoramento)	Não há medidas técnicas de segurança implementadas	Há algumas medidas técnicas de segurança implementadas	As principais medidas técnicas de segurança estão implementadas	As principais medidas técnicas de segurança estão implementadas e se atualizam com novas assinaturas de ameaças continuamente.	As principais medidas técnicas de segurança estão implementadas e se atualizam com novas assinaturas de ameaças continuamente. Há métricas de avaliação definidas para checar a efetividade dos controles.
6.4	Manter medidas para criptografar dados pessoais em repouso e em movimento	Não há medidas técnicas de criptografia implementadas	Há medidas técnicas de criptografia implementadas parcialmente	Há medidas técnicas de criptografia implementadas para proteção de dados em repouso e movimento	Há medidas técnicas de criptografia implementadas para proteção de dados em repouso e movimento. Há retenção de logs de acessos ou tentativas de acesso a arquivos criptografados.	Há medidas técnicas de criptografia implementadas para proteção de dados em repouso e movimento. Há retenção de logs de acessos ou tentativas de acesso a arquivos criptografados. São enviados alertas automáticos em caso de incidentes e violações de acesso.
6.5	Manter procedimentos para restringir o acesso a dados pessoais (por exemplo, acesso baseado em função, segregação de funções)	Não há matriz de segregação de funções	Há matriz de segregação de funções, parcial. Com a definição de usuários e perfis de alguns sistemas.	Há matriz de segregação de funções com a definição de usuários e perfis de acesso em cada sistema.	Há matriz de segregação de funções com a definição de usuários e perfis de acesso em cada sistema. A matriz é revisada periodicamente.	Há matriz de segregação de funções com a definição de usuários e perfis de acesso em cada sistema. A matriz é revisada periodicamente. São realizadas auditorias para conferência dos acessos face a matriz.
6.6	Integrar a privacidade e proteção de dados a uma política de segurança corporativa (proteção de instalações físicas e ativos físicos)	Não há medidas técnicas de segurança física implementadas	Há algumas medidas técnicas de segurança física implementadas	As principais medidas técnicas de segurança física estão implementadas	As principais medidas técnicas de segurança estão implementadas e dispõem de registro de log.	As principais medidas técnicas de segurança estão implementadas e dispõem de registro de log. Os controles são testados periodicamente.
6.7	Manter plano de continuidade de negócios	Não há PCN	Há PCN parcial	Há PCN	Há PCN baseado na ISO 22301	Há PCN baseado na ISO 22301 e são realizados testes

						periódicos de recuperação em caso de desastre.
6.8	Manter uma estratégia de prevenção de perda de dados (backup)	Não há backup	Há backup não periódico	Há backup periódico	Há backup periódico com testes de recuperação esporádicos.	Há backup periódico com testes de recuperação esporádicos. Dados são armazenados em local diferente da produção.
6.9	Conduzir testes regulares quanto ao desempenho de segurança de dados (pentest)	Não são realizados teste de intrusão	São realizados teste de intrusão não periódicos	São realizados teste de intrusão periódicos WAN to LAN Black Box	São realizados teste de intrusão periódicos WAN to LAN e LAN to LAN Black Box	São realizados teste de intrusão periódicos WAN to LAN e LAN to LAN White Box
6.10	Manter uma certificação de segurança (por exemplo, ISO)	Não há certificação de segurança	Há certificação de segurança expirada	Há certificação de segurança vigente	Há certificação de segurança vigente e há métricas de aferição de conformidade com a norma base	Há certificação de segurança vigente e há métricas de aferição de conformidade com a norma base. São realizadas auditorias periódicas.

4.5.7. **Gerenciamento de Riscos de Terceiros**

Mapear os riscos relacionados aos clientes, fornecedores, operadores / processadores e afiliados é um passo importante para atingimento da conformidade e para o nivelamento dos padrões de estratégias com operadores. O Quadro 19 mostra os processos associados a este domínio com suas referências as principais normas técnicas e a LGPD.

Quadro 19: Processos do domínio Gerenciamento de riscos de terceiros. Fonte: Elaborado pelo Autor.

ID do Processo	Processo	LGPD	ISO 27001 / 27002	ISO 27701
7.1	Manter política de privacidade e proteção de dados para terceiros (por exemplo, clientes, fornecedores, processadores, afiliados)	Art. 39	6.1.4, 15	5.2.1, 6.10.2.4, 6.12.1.2, 6.15.1.1, 7.2.6, 8.2.4, 8.2.5, 8.5.6, 8.5.7, 8.5.8, 5.2.3, 5.2.4, 5.4.1.2, 5.4.1.3, 6.9.3.1, 6.11.1.2, 6.12.1.2, 6.15.1.1, 6.15.2.1, 6.15.2.3, 7.2.1, 7.4.5, 8.2.2
7.2	Manter procedimentos para executar contratos ou acordos com todos os processadores	Art. 39	13.2, 14.1, 15, 18.1.2, 18.2.2	5.2.1,6.10.2.4,6.12.1.2,6.15.1.1,7.2.6,8.2.4,8.2.5,8.56.,8.5.7,8.5.8
7.3	Realizar a devida diligência em torno da postura de privacidade e proteção de dados, segurança de dados de fornecedores / operadores em potencial	Art. 39	13.2.4,15.1.2, 18	5.2.1,6.10.2.4,6.12.1.2,6.15.1.1,7.2.6,8.2.4,8.2.5,8.56.,8.5.7,8.5.8
7.4	Realizar due diligence em fontes de dados de terceiros	--	--	--
7.5	Manter um processo de avaliação de risco de privacidade e proteção de dados do fornecedor	Art. 39	15	--
7.6	Manter uma política que rege o uso de provedores de nuvem	--	9.1,13, 15, 18	--
7.7	Manter procedimentos para lidar com casos de não conformidade com contratos e acordos	--	--	--
7.8	Analisar os contratos de longo prazo para verificar riscos de privacidade de dados novos ou em evolução	--	13.2.4, 15, 18	--

No Quadro 20 são descritos detalhadamente os níveis de maturidade dos processos associados ao domínio Gerenciamento de riscos de terceiros.

Quadro 20 - Níveis de maturidade dos processos do domínio Gerenciamento de riscos de terceiros. Fonte: Elaborado pelo Autor.

ID do Processo	Processo	1 – Inicial	2 - Parcial	3 - Determinado	4 – Gerenciado	5 - Otimizado
		Resultados Esperados				
7.1	Manter política de privacidade e proteção de dados para terceiros (por exemplo, clientes, fornecedores, processadores, afiliados)	Não há políticas relacionadas documentadas	Há políticas relacionadas parcialmente documentadas	Há políticas relacionadas documentadas	Há políticas relacionadas documentadas e são revisadas periodicamente	Há políticas relacionadas documentadas, estas são revisadas e auditadas periodicamente
7.2	Manter procedimentos para executar contratos ou acordos com todos os processadores	Não há procedimentos relacionados documentadas	Há procedimentos relacionados parcialmente documentados	Há procedimentos relacionados documentados	Há procedimentos relacionados documentados e são revisados periodicamente	Há procedimentos relacionados documentados, estes são revisados e auditados periodicamente
7.3	Realizar a devida diligência em torno da postura de privacidade e proteção de dados, segurança de dados de fornecedores / operadores em potencial	Não é feita diligência em torno de operadores em potencial	É feita diligência parcial em torno de operadores em potencial	É feita diligência em torno de operadores em potencial	É feita diligência em torno de operadores em potencial. Este precisam apresentar relatórios periódicos que comprovem a eficiência dos controles de proteção e privacidade.	É feita diligência em torno de operadores em potencial. Este precisam apresentar relatórios periódicos que comprovem a eficiência dos controles de proteção e privacidade. São realizadas auditorias periodicamente.
7.4	Realizar due diligence em fontes de dados de terceiros	Não é feita diligência em torno de fontes de dados de terceiros	É feita diligência parcial em torno de fontes de dados de terceiros	É feita diligência em torno de fontes de dados de terceiros	É feita diligência em torno de fontes de dados de terceiros. Este precisam apresentar relatórios periódicos que comprovem a eficiência dos controles de proteção e privacidade.	É feita diligência em torno de fontes de dados de terceiros. Este precisam apresentar relatórios periódicos que comprovem a eficiência dos controles de proteção e privacidade. São realizadas auditorias periodicamente.

7.5	Manter um processo de avaliação de risco de privacidade e proteção de dados do fornecedor	Não há procedimentos relacionados documentadas	Há procedimentos relacionados parcialmente documentados	Há procedimentos relacionados documentados	Há procedimentos relacionados documentados e são revisados periodicamente	Há procedimentos relacionados documentados, estes são revisados e auditados periodicamente
7.6	Manter uma política que rege o uso de provedores de nuvem	Não há políticas relacionadas documentadas	Há políticas relacionadas parcialmente documentadas	Há políticas relacionadas documentadas	Há políticas relacionadas documentadas e são revisadas periodicamente	Há políticas relacionadas documentadas, estas são revisadas e auditadas periodicamente
7.7	Manter procedimentos para lidar com casos de não conformidade com contratos e acordos	Não há procedimentos relacionados documentadas	Há procedimentos relacionados parcialmente documentados	Há procedimentos relacionados documentados	Há procedimentos relacionados documentados e são revisados periodicamente	Há procedimentos relacionados documentados, estes são revisados e auditados periodicamente
7.8	Analisar os contratos de longo prazo para verificar riscos de privacidade de dados novos ou em evolução	Não há análise de contratos	Há análise de alguns contratos	Há análise de todos os contratos	Há análise de todos os contratos periodicamente para manter aderência a legislação vigente.	Há análise de todos os contratos periodicamente para manter aderência a legislação vigente. Há mecanismo implantado para análise de impacto automático em contratos.

4.5.8. **Plano de comunicação**

Estabelecer um plano para comunicação com os titulares dos dados e com a Autoridade Nacional de Proteção de Dados é peça chave para demonstrar a conformidade com a LGPD, ao passo que define os canais, periodicidade e eventos para que a comunicação seja realizada. O Quadro 21 mostra os processos associados a este domínio com suas referências as principais normas técnicas e a LGPD.

Quadro 21: Processos do domínio Plano de comunicação. Fonte: Elaborado pelo Autor.

ID do Processo	Processo	LGPD	ISO 27001 / 27002	ISO 27701
8.1	Manter um aviso de privacidade e proteção de dados que detalha as práticas de tratamento de dados pessoais da organização	Art. 6, 7, 9, 14	8	7.2.2,7.2.3,7.3.2,7.3.3,7.3.4,7.3.5,7.3.6,7.3.10,7.4.7,
8.2	Fornecer aviso de privacidade e proteção de dados em todos os pontos em que os dados pessoais são coletados	Art. 9, 14	8, 9.2, 9.3, 9.4, 11.1, 12, 13, 18.1.1	7.3.2,7.3.3,7.3.4,7.3.5,7.3.6,7.3.10,7.4.7
8.3	Fornecer aviso nas comunicações de marketing (por exemplo, e-mails, folhetos, ofertas)	Art. 6	--	--
8.4	Fornecer aviso em contratos e termos	Art. 6	15	--
8.5	Manter scripts para uso dos funcionários para explicar ou fornecer o aviso de privacidade e proteção de dados	Art. 6	--	--
8.6	Manter um selo de privacidade e proteção de dados ou marca de confiança para aumentar a confiança do cliente	--	--	--

No Quadro 22 são descritos detalhadamente os níveis de maturidade dos processos associados ao domínio Plano de comunicação.

Quadro 22 - Níveis de maturidade dos processos do domínio Plano de comunicação. Fonte: Elaborado pelo Autor.

ID do Processo	Processo	1 – Inicial	2 - Parcial	3 - Determinado	4 – Gerenciado	5 - Otimizado
		Resultados Esperados				
8.1	Manter um aviso de privacidade e proteção de dados que detalha as práticas de tratamento de dados pessoais da organização	Não há qualquer aviso.	Há aviso parcial	Há aviso de privacidade e proteção de dados que detalha as	Há aviso de privacidade e proteção de dados que detalha as práticas de tratamento de dados pessoais da	Há aviso de privacidade e proteção de dados que detalha as práticas de tratamento de dados pessoais da organização. O mesmo é

				práticas de tratamento de dados pessoais da organização	organização. O mesmo é revisado periodicamente.	revisado periodicamente e adequado de acordo com as melhores práticas.
8.2	Fornecer aviso de privacidade e proteção de dados em todos os pontos em que os dados pessoais são coletados	Não há qualquer aviso.	Há aviso parcial	Há aviso de privacidade e proteção de dados que detalha as práticas de tratamento de dados pessoais da organização	Há aviso de privacidade e proteção de dados que detalha as práticas de tratamento de dados pessoais da organização. O mesmo é revisado periodicamente.	Há aviso de privacidade e proteção de dados que detalha as práticas de tratamento de dados pessoais da organização. O mesmo é revisado periodicamente e adequado de acordo com as melhores práticas.
8.3	Fornecer aviso nas comunicações de marketing (por exemplo, e-mails, folhetos, ofertas)	Não há qualquer aviso.	Há aviso parcial	Há aviso de privacidade e proteção de dados que detalha as práticas de tratamento de dados pessoais da organização	Há aviso de privacidade e proteção de dados que detalha as práticas de tratamento de dados pessoais da organização. O mesmo é revisado periodicamente.	Há aviso de privacidade e proteção de dados que detalha as práticas de tratamento de dados pessoais da organização. O mesmo é revisado periodicamente e adequado de acordo com as melhores práticas.
8.4	Fornecer aviso em contratos e termos	Não há qualquer aviso.	Há aviso parcial	Há aviso de privacidade e proteção de dados que detalha as práticas de tratamento de dados pessoais da organização	Há aviso de privacidade e proteção de dados que detalha as práticas de tratamento de dados pessoais da organização. O mesmo é revisado periodicamente.	Há aviso de privacidade e proteção de dados que detalha as práticas de tratamento de dados pessoais da organização. O mesmo é revisado periodicamente e adequado de acordo com as melhores práticas.
8.5	Manter scripts para uso dos funcionários para explicar ou fornecer o aviso de privacidade e proteção de dados	Não há qualquer script.	Há script parcial	Há scripts para uso dos funcionários para explicar ou fornecer o aviso de privacidade e	Há scripts para uso dos funcionários para explicar ou fornecer o aviso de privacidade e proteção de dados. Os mesmos são revisados periodicamente.	Há scripts para uso dos funcionários para explicar ou fornecer o aviso de privacidade e proteção de dados. Os mesmos são revisados periodicamente e adequado segundo as melhores práticas.

				proteção de dados		
8.6	Manter um selo de privacidade e proteção de dados ou marca de confiança para aumentar a confiança do cliente	Não há qualquer selo.	Há um selo expirado.	Há um selo vigente.	Há um selo vigente e um processo de renovação periódico.	Há um selo vigente e um processo de renovação periódico. Com auditorias regulares

4.5.9. **Resposta aos titulares dos dados**

A resposta aos titulares dos dados é dever do Controlador, para tal este deve estabelecer os meios para que os titulares possam exercem os seus direitos a qualquer tempo, bem como devem tratar as solicitações e reclamações dos titulares dos dados. O Quadro 23 mostra os processos associados a este domínio com suas referências as principais normas técnicas e a LGPD.

Quadro 23: Processos do domínio Resposta aos titulares dos dados. Fonte: Elaborado pelo Autor.

ID do Processo	Processo	LGPD	ISO 27001 / 27002	ISO 27701
9.1	Manter procedimentos para tratar de reclamações	Art. 50	--	--
9.2	Manter procedimentos para responder a solicitações de acesso a dados pessoais	Art. 6, 18, 19	9.1.2,9.2, 12.4, 13.2	7.3.2,7.3.9,7.5.1,7.5.2,8.3.1
9.3	Manter procedimentos para responder a solicitações e / ou fornecer um mecanismo para os indivíduos atualizarem ou corrigirem seus dados pessoais	Art. 18	9.1.2,9.2, 12.4, 13.2	7.3.6,7.3.7

9.4	Manter procedimentos para responder a pedidos de exclusão, restrição ou oposição ao processamento	Art. 8 (5), 18, 20	9.1.2,9.2, 12.4, 13.2	7.2.2,7.3.2,7.2.4, 7.3.3,7.3.4, 7.3.5,8.2.3
9.5	Manter procedimentos para responder a pedidos de informações	Art. 18	--	--
9.6	Manter procedimentos para responder a solicitações de portabilidade de dados	Art. 18	13,2	7.3.8
9.7	Manter procedimentos para responder a pedidos a serem esquecidos ou para apagar dados	Art. 18	9.1.2,9.2, 12.4, 13.2	7.2.2,7.3.6,7.3.7
9.8	Manter perguntas frequentes (FAQ) para responder a perguntas de indivíduos	Art. 6	--	--
9.9	Investigar as causas raízes das reclamações de proteção de dados	--	--	--
9.10	Monitorar e reportar métricas para reclamações de privacidade e proteção de dados (por exemplo, quantidade, causa raiz)	--	--	--

No Quadro 24 são descritos detalhadamente os níveis de maturidade dos processos associados ao domínio Resposta aos titulares dos dados.

Quadro 24 - Níveis de maturidade dos processos do domínio Resposta aos titulares dos dados. Fonte: Elaborado pelo Autor.

ID do Processo	Processo	1 – Inicial	2 - Parcial	3 - Determinado	4 – Gerenciado	5 - Otimizado
		Resultados Esperados				
9.1	Manter procedimentos para tratar de reclamações	Não há procedimentos relacionados documentados	Há procedimentos relacionados parcialmente documentados	Há procedimentos relacionados documentados	Há procedimentos relacionados documentados e são revisados periodicamente	Há procedimentos relacionados documentados, estes são revisados e auditados periodicamente

9.2	Manter procedimentos para responder a solicitações de acesso a dados pessoais	Não há procedimentos relacionados documentados	Há procedimentos relacionados parcialmente documentados	Há procedimentos relacionados documentados	Há procedimentos relacionados documentados e são revisados periodicamente	Há procedimentos relacionados documentados, estes são revisados e auditados periodicamente
9.3	Manter procedimentos para responder a solicitações e / ou fornecer um mecanismo para os indivíduos atualizarem ou corrigirem seus dados pessoais	Não há procedimentos relacionados documentados	Há procedimentos relacionados parcialmente documentados	Há procedimentos relacionados documentados	Há procedimentos relacionados documentados e são revisados periodicamente	Há procedimentos relacionados documentados, estes são revisados e auditados periodicamente
9.4	Manter procedimentos para responder a pedidos de exclusão, restrição ou oposição ao processamento	Não há procedimentos relacionados documentados	Há procedimentos relacionados parcialmente documentados	Há procedimentos relacionados documentados	Há procedimentos relacionados documentados e são revisados periodicamente	Há procedimentos relacionados documentados, estes são revisados e auditados periodicamente
9.5	Manter procedimentos para responder a pedidos de informações	Não há procedimentos relacionados documentados	Há procedimentos relacionados parcialmente documentados	Há procedimentos relacionados documentados	Há procedimentos relacionados documentados e são revisados periodicamente	Há procedimentos relacionados documentados, estes são revisados e auditados periodicamente
9.6	Manter procedimentos para responder a solicitações de portabilidade de dados	Não há procedimentos relacionados documentados	Há procedimentos relacionados parcialmente documentados	Há procedimentos relacionados documentados	Há procedimentos relacionados documentados e são revisados periodicamente	Há procedimentos relacionados documentados, estes são revisados e auditados periodicamente
9.7	Manter procedimentos para responder a pedidos a serem esquecidos ou para apagar dados	Não há procedimentos relacionados documentados	Há procedimentos relacionados parcialmente documentados	Há procedimentos relacionados documentados	Há procedimentos relacionados documentados e são revisados periodicamente	Há procedimentos relacionados documentados, estes são revisados e auditados periodicamente
9.8	Manter perguntas frequentes (FAQ) para responder a perguntas de indivíduos	Não há procedimentos relacionados documentados	Há procedimentos relacionados parcialmente documentados	Há procedimentos relacionados documentados	Há procedimentos relacionados documentados e são revisados periodicamente	Há procedimentos relacionados documentados, estes são revisados e auditados periodicamente
9.9	Investigar as causas raízes das reclamações de proteção de dados	Não há procedimentos	Há procedimentos relacionados	Há procedimentos	Há procedimentos relacionados documentados e são	Há procedimentos relacionados documentados,

		relacionados documentados	parcialmente documentados	relacionados documentados	revisados periodicamente	estes são revisados e auditados periodicamente
9.10	Monitorar e reportar métricas para reclamações de privacidade e proteção de dados (por exemplo, quantidade, causa raiz)	Não há procedimentos relacionados documentados	Há procedimentos relacionados parcialmente documentados	Há procedimentos relacionados documentados	Há procedimentos relacionados documentados e são revisados periodicamente	Há procedimentos relacionados documentados, estes são revisados e auditados periodicamente

4.5.10. **Monitoramento de novas práticas operacionais**

O monitoramento de novas práticas operacionais consiste em avaliar e atualizar o relatório de impacto sobre proteção de dados (RIPD) mediante os novos projetos e processos da organização, bem como integrar o *Privacy by design* em todas as novas iniciativas. O Quadro 25 mostra os processos associados a este domínio com suas referências as principais normas técnicas e a LGPD.

Quadro 25: Processos do domínio Monitoramento de novas práticas operacionais. Fonte: Elaborado pelo Autor.

ID do Processo	Processo	LGPD	ISO 27001 / 27002	ISO 27701
10.1	Manter procedimento de verificação de identidade dos titulares	--	--	--
10.2	Integrar o Privacy by Design no desenvolvimento de sistemas e produtos da organização	Art. 46	5,6, 10,14.2	5.2.1, 6.11.2.1,6.11.2.5,7.4.2,
10.3	Manter diretrizes e modelos de DPIA em conformidade com a LGPD	Art. 5, XVII, 38	18.1.1	5.2.2,7.2.5

No Quadro 26 são descritos detalhadamente os níveis de maturidade dos processos associados ao domínio Monitoramento de novas práticas operacionais.

Quadro 26 - Níveis de maturidade dos processos do domínio Monitoramento de novas práticas operacionais. Fonte: Elaborado pelo Autor.

ID do Processo	Processo	1 – Inicial	2 - Parcial	3 - Determinado	4 – Gerenciado	5 - Otimizado
		Resultados Esperados				
10.1	Manter procedimento de verificação de identidade dos titulares	Não há procedimentos relacionados documentados	Há procedimentos relacionados parcialmente documentados	Há procedimentos relacionados documentados	Há procedimentos relacionados documentados e são revisados periodicamente	Há procedimentos relacionados documentados, estes são revisados e auditados periodicamente
10.2	Integrar o Privacy by Design no desenvolvimento de sistemas e produtos da organização	Aspectos de privacidade não são considerados no desenvolvimento de sistemas e produtos da organização	Aspectos de privacidade não são requisitos chave de sistemas e produtos da organização, mas são considerados	Aspectos de privacidade são requisitos chave no desenvolvimento de sistemas e produtos da organização	Aspectos de privacidade são requisitos chave no desenvolvimento de sistemas e produtos da organização. Ocorrem revisões periódicas dos sistemas em busca de falhas que possam comprometer a privacidade.	Aspectos de privacidade são requisitos chave no desenvolvimento de sistemas e produtos da organização. Ocorrem revisões periódicas dos sistemas em busca de falhas que possam comprometer a privacidade.
10.3	Manter diretrizes e modelos de DPIA em conformidade com a LGPD	Não há DPIA	Há DPIA parciais	Há DPIA de todos os processos que tratam dados pessoais na organização. Os DPIA de dados sensíveis são relatados para os reguladores	Há DPIA de todos os processos que tratam dados pessoais na organização. Os DPIA de dados sensíveis são relatados para os reguladores. Os documentos são revisados periodicamente junto as áreas de negócio.	Há DPIA de todos os processos que tratam dados pessoais na organização. Os DPIA de dados sensíveis são relatados para os reguladores. Os documentos são revisados periodicamente junto as áreas de negócio. Há um plano de ação que é objeto de auditoria periódica.

4.5.11. **Gerenciamento de violação de privacidade de dados**

O gerenciamento de violação de privacidade de dados consiste na tratativa de incidentes que se caracterizem como violação de dados pessoais, onde através de um plano de resposta a incidentes a organização é capaz de tratar o ocorrido e endereçar a ações de análise e recuperação. O Quadro 27 mostra os processos associados a este domínio com suas referências as principais normas técnicas e a LGPD.

Quadro 27: Processos do domínio Gerenciamento de violação de privacidade de dados. Fonte: Elaborado pelo Autor.

ID do Processo	Processo	LGPD	ISO 27001 / 27002	ISO 27701
11.1	Manter um plano de resposta a incidentes / violações da privacidade de dados	Art. 48, 5	16	6.13.1.1,6.13.1.5,
11.2	Manter um protocolo de notificação de violação (para as pessoas afetadas) e relatórios (para reguladores, agências de crédito, órgãos policiais)	Art. 48	4.2, 6.1.3,16.1.1, 16.1.5, 18.1.1	6.13.1.1,6.13.1.5, 7.3.1,7.3.3,7.3.9,
11.3	Manter o registro quanto o rastreamento de incidentes / violações de privacidade e proteção de dados	--	16.1.2	6.13.1.1,6.13.1.5,
11.4	Monitorar e reportar as métricas de incidentes / violações de privacidade e proteção de dados (por exemplo, natureza da violação, risco, causa raiz)	--	16.1.3	--
11.5	Realizar testes periódicos do plano de violação / incidente de privacidade e proteção de dados	--	17.1.3	--
11.6	Envolver uma equipe de investigação forense	--	--	--
11.7	Obter cobertura de seguro de violação de privacidade e proteção de dados	--	17	--

No Quadro 28 são descritos detalhadamente os níveis de maturidade dos processos associados ao domínio Gerenciamento de violação de privacidade de dados.

Quadro 28 - Níveis de maturidade dos processos do domínio Gerenciamento de violação de privacidade de dados. Fonte: Elaborado pelo Autor.

ID do Processo	Processo	1 – Inicial	2 - Parcial	3 - Determinado	4 – Gerenciado	5 - Otimizado
		Resultados Esperados				
11.1	Manter um plano de resposta a incidentes / violações da privacidade de dados	Não há procedimentos relacionados documentados	Há procedimentos relacionados parcialmente documentados	Há procedimentos relacionados documentados	Há procedimentos relacionados documentados e são revisados periodicamente	Há procedimentos relacionados documentados, estes são revisados e auditados periodicamente
11.2	Manter um protocolo de notificação de violação (para as pessoas afetadas) e relatórios (para reguladores, agências de crédito, órgãos policiais)	Não há procedimentos relacionados documentados	Há procedimentos relacionados parcialmente documentados	Há procedimentos relacionados documentados	Há procedimentos relacionados documentados e são revisados periodicamente	Há procedimentos relacionados documentados, estes são revisados e auditados periodicamente
11.3	Manter o registro quanto o rastreamento de incidentes / violações de privacidade e proteção de dados	Não há procedimentos relacionados documentados	Há procedimentos relacionados parcialmente documentados	Há procedimentos relacionados documentados	Há procedimentos relacionados documentados e são revisados periodicamente	Há procedimentos relacionados documentados, estes são revisados e auditados periodicamente
11.4	Monitorar e reportar as métricas de incidentes / violações de privacidade e proteção de dados (por exemplo, natureza da violação, risco, causa raiz)	Não há procedimentos relacionados documentados	Há procedimentos relacionados parcialmente documentados	Há procedimentos relacionados documentados	Há procedimentos relacionados documentados e são revisados periodicamente	Há procedimentos relacionados documentados, estes são revisados e auditados periodicamente
11.5	Realizar testes periódicos do plano de violação / incidente de privacidade e proteção de dados	Não são realizados testes periódicos do plano de violação / incidente de privacidade e	São realizados testes não periódicos do plano de violação / incidente de privacidade e	São realizados testes periódicos do plano de violação / incidente de privacidade e proteção de dados	São realizados testes periódicos do plano de violação / incidente de privacidade e proteção de dados. O plano é constantemente	São realizados testes periódicos do plano de violação / incidente de privacidade e proteção de dados. O plano é constantemente aprimorado a partir do resultado dos testes. São realizadas auditorias do plano.

		proteção de dados	proteção de dados		aprimorado a partir do resultado dos testes	
11.6	Envolver uma equipe de investigação forense	Não há procedimentos relacionados documentados	Há procedimentos relacionados parcialmente documentados	Há procedimentos relacionados documentados	Há procedimentos relacionados documentados e são revisados periodicamente	Há procedimentos relacionados documentados, estes são revisados e auditados periodicamente
11.7	Obter cobertura de seguro de violação de privacidade e proteção de dados	Não há cobertura de seguro de violação de privacidade e proteção de dados	Há cobertura parcial de seguro de violação de privacidade e proteção de dados	Há cobertura completa de seguro de violação de privacidade e proteção de dados	Há cobertura completa de seguro de violação de privacidade e proteção de dados. São monitorados indicadores de segurança pela seguradora.	Há cobertura completa de seguro de violação de privacidade e proteção de dados. São monitorados indicadores de segurança pela seguradora e realizadas auditorias periódicas.

4.5.12. **Tratamento de dados**

O domínio tratamento de dados define os processos necessários para regulamentar as atividades envolvendo dados pessoais, deste a documentação das atividades executadas até a definição das bases legais. O Quadro 29 mostra os processos associados a este domínio com suas referências as principais normas técnicas e a LGPD.

Quadro 29: Processos do domínio Gerenciamento de violação de privacidade de dados. Fonte: Elaborado pelo Autor.

ID do Processo	Processo	LGPD	ISO 27001 / 27002	ISO 27701
12.1	Conduzir auditorias internas do programa de privacidade e proteção de dados	Art. 50	9.2, 17.1.3	5.2.1,6.2.1.1,6.3.1.1, 6.4.2.2, 6.15.1.3,7.2.8,

12.2	Conduzir avaliações com base em eventos externos, como reclamações / violações, entre outros	Art. 18, 46,48	16.1.2	--
12.3	Envolver a auditoria externas para avaliações independentes	Art. 50	18.2.1	--
12.4	Monitorar e reportar as métricas de privacidade e proteção de dados	--	--	--
12.5	Manter a documentação como evidência a fim de demonstrar conformidade e / ou prestação de conta	Art. 6, 50	5,12.1.1,13.2.2,17.1.2, 18.2	5.2.1, 6.2.1.1,6.3.2.1,6.4.2.2,6.5.2.1,6.5.2.2,6.5.3.1,6.5.3.2,6.5.3.3,6.6.2.1,6.6.2.2,6.6.4.2,6.8.2.7,6.8.2.9,6.9.3.1, 6.9.4.1,6.9.4.2,6.10.2.1,6.10.2.4,6.11.1.2,6.11.3.1, 6.12.1.2,6.13.1.1,6.15.1.1,6.15.1.3,7.2.1,7.2.2,7.2.6, 7.2.8,7.3.6,7.4.1,7.4.3,7.4.4,7.4.5,7.4.6,7.4.8,7.4.9, 8.2.2, 8.4.1,8.4.3

No Quadro 30 são descritos detalhadamente os níveis de maturidade dos processos associados ao domínio Tratamento de dados.

Quadro 30 - Níveis de maturidade dos processos do domínio Tratamento de dados. Fonte: Elaborado pelo Autor.

ID do Processo	Processo	1 – Inicial	2 - Parcial	3 - Determinado	4 – Gerenciado	5 - Otimizado
		Resultados Esperados				
12.1	Conduzir auditorias internas do programa de privacidade e proteção de dados	Não são realizadas auditorias internas	São realizadas auditorias internas não periódicas.	São realizadas auditorias internas periódicas.	São realizadas auditorias internas periódicas. O resultado é utilizado para elaboração de um plano de ação.	São realizadas auditorias internas periódicas. O resultado é utilizado para elaboração de um plano de ação que é monitorado e apresentado para a diretoria.
12.2	Conduzir avaliações com base em eventos externos, como reclamações / violações, entre outros	Não há avaliações de eventos externos	As avaliações de eventos externos ocorrem de forma ad-hoc	Todos os eventos externos são avaliados	Todos os eventos externos são avaliados e há indicadores para monitoramento da eficiência do processo.	Todos os eventos externos são avaliados e há indicadores para monitoramento da eficiência do processo. São realizadas auditorias periódicas.

12.3	Envolver a auditoria externas para avaliações independentes	Não são realizadas auditorias externas	São realizadas auditorias externas não periódicas.	São realizadas auditorias externas periódicas.	São realizadas auditorias externas periódicas. O resultado é utilizado para elaboração de um plano de ação.	São realizadas auditorias externas periódicas. O resultado é utilizado para elaboração de um plano de ação que é monitorado e apresentado para a diretoria.
12.4	Monitorar e reportar as métricas de privacidade e proteção de dados	Não há métricas relacionadas documentadas	Há métricas relacionadas parcialmente documentadas	Há métricas relevantes e relacionadas documentadas	Há métricas relevantes e relacionadas documentadas. Indicadores são monitorados constantemente	Há métricas relevantes e relacionadas documentadas. Indicadores são monitorados constantemente. São estabelecidas metas para evolução contínua.
12.5	Manter a documentação como evidência a fim de demonstrar conformidade e / ou prestação de conta	Não há documentação relacionada	Há documentação parcial relacionada	Há documentação relacionada	Há documentação relacionada, a revisão é periódica	Há documentação relacionada, a revisão e auditorias são periódicas.

4.6. **Validação do modelo e versão otimizada**

Participaram da etapa de validação do modelo profissionais com plenos conhecimentos acerca da Lei Geral de Proteção de Dados e Segurança da informação, visando elencar sugestões e críticas construtivas em relação ao modelo proposto. Para tal, a amostra foi composta de três profissionais com experiência acima de cinco anos na área de segurança da informação.

Estes responderam ao questionário publicado na web elaborado a partir da ferramenta Google Forms (Apêndice A) e na seção de feedback descreveram os principais pontos de melhoria para o Modelo de Maturidade de Segurança da Informação Brasileiro (MMSI.br), o quais são apresentados a seguir:

- Relacionar mais processos para avaliação da efetividade dos controles de segurança da informação nas organizações;
- Criar tópico específico para identificar quais as organizações dispõem de orçamento específico para tratar o tema privacidade e proteção de dados;
- Tentar reduzir a quantidade de perguntas do modelo, pois este foi considerado extenso por alguns dos participantes.

Após avaliar os feedbacks recebidos na fase de homologação foram realizadas alterações no modelo. A versão original do modelo continha dez processos relacionados ao domínio “Gerenciamento de riscos de segurança da informação”, contudo após a análise dos feedbacks conclui-se que era necessário expandir a avaliação no domínio, isto culminou na inclusão seis novos processos:

- 6.11 - Manter um sistema de gerenciamento de dispositivos móveis (MDM);
- 6.12 - Manter um sistema de gerenciamento e correlação de eventos de segurança (SIEM);
- 6.13 - Manter um sistema de gerenciamento de vulnerabilidades;
- 6.14 - Manter um sistema de gerenciamento de acesso remoto seguro;
- 6.15 - Manter um sistema de gerenciamento de acesso as interfaces de rede;
- 6.16 - Manter um sistema de gerenciamento de mídias de armazenamento removível.

Referente a sugestão de criação de um tópico específico para identificar quais as organizações dispõem de orçamento específico para tratar o tema privacidade e

proteção de dados. Foi avaliada como não procedente, visto que o modelo se atém exclusivamente as questões técnicas das organizações para realização das avaliações.

Sobre a sugestão de reduzir o número de perguntas do modelo foi avaliado que algumas questões eram abordadas indiretamente por outros tópicos possibilitando a sua exclusão sem prejuízos aos objetivos do modelo. Os tópicos suprimidos foram:

- 3.3 - Integrar ética ao tratamento de dados através de códigos de conduta organizacional;
- 4.7 - Integrar a privacidade de dados ao uso de práticas de mídia social da organização;
- 4.8 - Integrar a privacidade e proteção de dados nas políticas / procedimentos Bring Your Own Device (BYOD), se houver;
- 4.10 - Integrar a privacidade e proteção de dados em práticas para monitorar funcionários;
- 4.13 - Integrar a privacidade dos dados no acesso delegado às contas de email da empresa dos funcionários (por exemplo, férias e rescisão);
- 4.14 - Integrar a privacidade e proteção de dados às práticas de descoberta eletrônica;
- 4.15 - Integrar a privacidade e proteção de dados em práticas para divulgação e para fins de aplicação da lei;
- 5.3 - Desenvolver e publicar boletim de privacidade e proteção de dados ou incorporar a privacidade e proteção de dados às comunicações corporativas existentes;
- 7.4 - Realizar due diligence em fontes de dados de terceiros;
- 7.7 - Manter procedimentos para lidar com casos de não conformidade com contratos e acordos;
- 8.6 - Manter um selo de privacidade e proteção de dados ou marca de confiança para aumentar a confiança do cliente;
- 11.6 - Envolver uma equipe de investigação forense.

Diante das mudanças na versão original para contemplar as sugestões de melhoria que foram consideradas pertinentes na fase de validação, o número total de questões foi alterado de 86 para 80 na versão final do modelo.

5. APLICAÇÃO DO MODELO

A etapa de aplicação do modelo consistiu na publicação de um novo formulário web elaborado a partir da ferramenta Google Forms (Apêndice B), considerando os feedbacks recebidos na etapa de validação. A divulgação da pesquisa ocorreu via grupos de WhatsApp destinados a profissionais atuantes na área de privacidade e proteção de dados.

O período considerado para apuração dos resultados e envio das avaliações para os participantes foi de 01/08/2020 à 18/09/2020.

A amostra foi composta de vinte e seis participantes localizados em oito estados. A Figura 10 demonstra o quantitativo de participantes por UF.

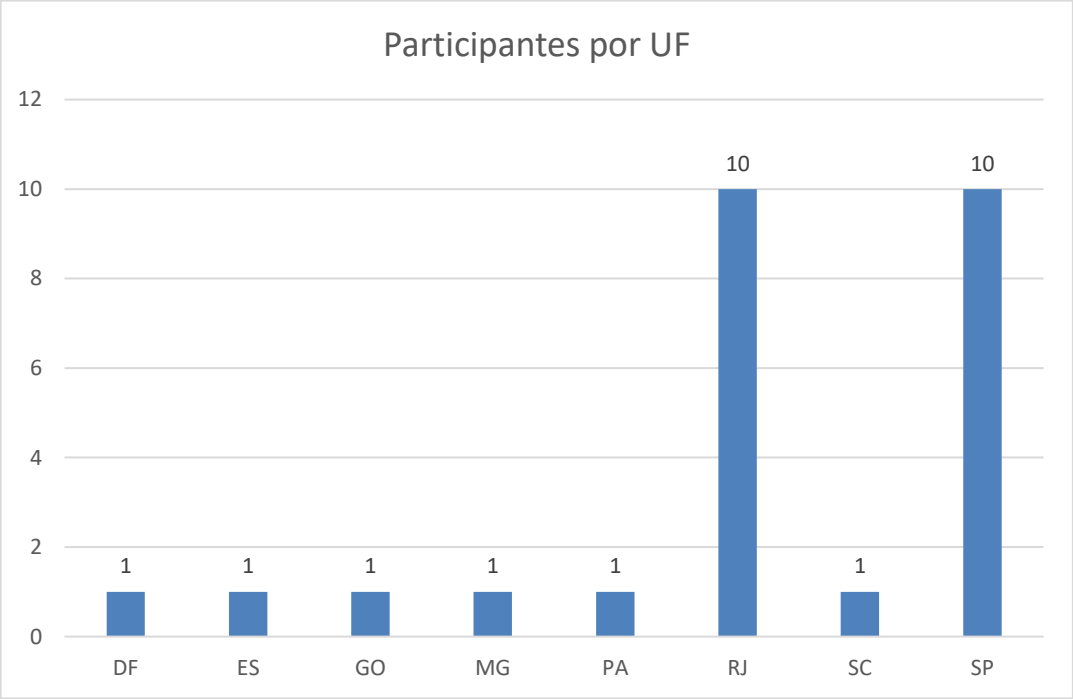


Figura 10: Participantes por UF. Fonte: Elaborado pelo Autor.

Os respondentes atuam em organizações de diversos seguimentos, tais como Tecnologia, Serviços, Saúde / Hospitalar, Logística, Indústria, Governo, Financeiro / Seguradoras / Corretoras, Educação e Comércio / Varejo. A Figura 11 demonstra a proporção de organizações por segmento.

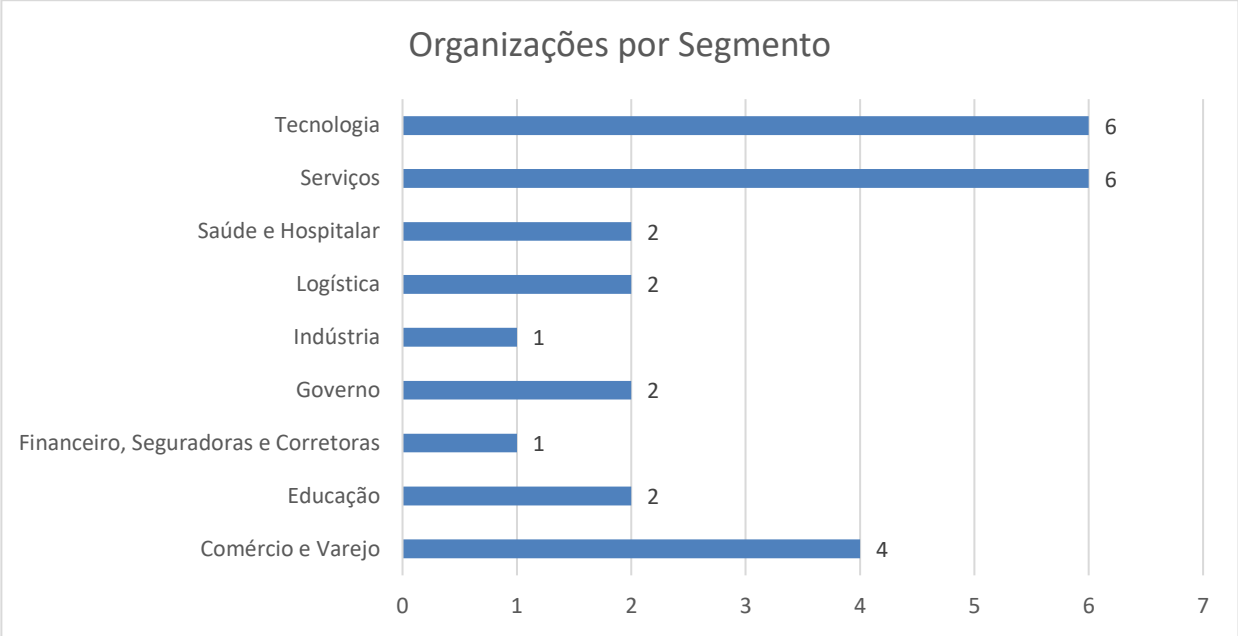


Figura 11: Organizações por Segmento. Fonte: Elaborado pelo Autor.

As organizações participantes foram classificadas de acordo com seu número de colaboradores, conforme apresentada na Figura 12.

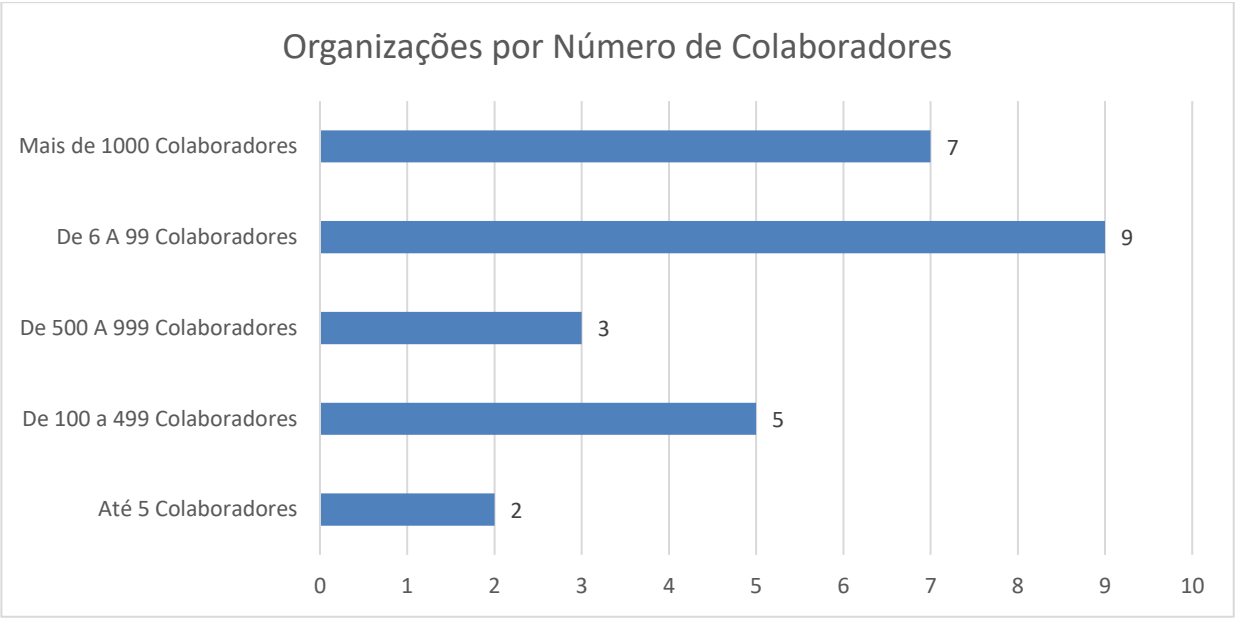


Figura 12: Organizações por número de colaboradores. Fonte: Elaborado pelo Autor.

Os respondentes receberam o relatório individualmente com o resultado do nível de maturidade e aderência ao MMSI.br das organizações avaliadas em formato textual e gráfico. O Quadro 31 demonstra um exemplo de relatório textual.

Quadro 31: Relatório textual do resultado do Assessment MMSI.br. Fonte: Elaborado pelo Autor.

Carimbo de data/hora	8/25/2020 16:23:55
Endereço de e-mail	x@x.com.br
Nome e Sobrenome	XXX
UF	XX
Organização	XX
Segmento Empresarial	Educação
Número de Colaboradores	De 100 a 499 Colaboradores

Processo Avaliado	**Resposta**	**Maturidade por processo**	**Maturidade por domínio**	
1.1 - Atribuir a responsabilidade pela privacidade e proteção dos dados a um indivíduo (encarregado de dados)	1 - Não há responsável atribuído	1	**1. Estrutura de governança**	1,8
1.2 - Envolver a alta direção em privacidade e proteção de dados e atribuir responsabilidade pela privacidade e proteção dos dados em toda a organização	2 - Há comitê de privacidade e proteção de dados sem reuniões regulares	2		
1.3 - Conduzir comunicação regular junto às partes interessadas internas da organização com status do gerenciamento de privacidade e proteção de dados	2 - Comunicação ocorre de forma esporádica, mas sem um plano definido.	2		
1.4 - Reportar às partes interessadas externas da organização o status do gerenciamento de privacidade (por exemplo, órgãos reguladores, terceiros, clientes)	1 - Não há comunicação e nem um plano definido.	1		
1.5 - Realizar uma avaliação de risco de privacidade e proteção de dados da empresa (DPIA)	2 - Os processos que tratam dados pessoais estão mapeados parcialmente	2		
1.6 - Integrar a privacidade de dados nas avaliações e relatórios de riscos corporativos	2 - Riscos relativos à privacidade de dados estão parcialmente mapeados	2		
1.7 - Manter uma estratégia e um programa de proteção e privacidade de dados (P&PD)	2 - Ações para assegurar a privacidade e proteção de	2		

	dados são tomadas, mas não há um programa definido.			
1.8 - Exigir que os funcionários reconheçam e concordem em aderir às políticas de privacidade e proteção de dados	2 - Há política de privacidade e proteção de dados, mas não é reconhecida e assinada pelos funcionários em sua totalidade	2		
2.1 - Manter um inventário de dados pessoais que são tratados	1 - Não há um inventário dos dados pessoais tratados	1	**2. Inventário de dados pessoais**	1,5
2.2 - Classificar os dados pessoais tratados	2 - Há política de classificação de dados de dados, mas dados são classificados parcialmente	2		
2.3 - Obter aprovação dos reguladores e/ou autoridades para processamento de dados e registrar bancos de dados onde este é necessário para aprovação prévia	0 - Não se aplica.	0		
2.4 - Manter registros do mecanismo de transferência usado para fluxos de dados transfronteiriços e aprovações de órgãos reguladores	0 - Não se aplica.	0		
3.1 - Manter uma política de privacidade e proteção de dados para funcionários contendo as bases legais para o tratamento de dados pessoais	1 - Não há política de privacidade e proteção de dados para funcionários	1	**3. Política de privacidade e proteção de dados**	1,0
3.2 - Manter uma política de privacidade e proteção de dados para terceiros (fornecedores e parceiros) contendo as bases legais para o tratamento de dados pessoais	1 - Não há política de privacidade e proteção de dados para terceiros	1		
3.3 - Manter atualizados procedimentos para coleta e uso de dados pessoais e dados sensíveis	1 - Não há procedimentos documentados	1		
4.1 - Manter políticas e procedimentos para identificação e manutenção da qualidade dos dados (válidos e atualizados).	1 - Não há políticas e procedimentos relacionados documentados	1	**4. Privacidade de dados nas operações**	1,4

4.2 - Manter políticas e procedimentos para revisar o tratamento total ou parcialmente por meios automatizados, tais como uso de cookies e mecanismos de rastreamento de clientes	1 - Não há políticas e procedimentos relacionados documentados	1		
4.3 - Manter políticas e procedimentos para obter consentimento válido por parte dos titulares dos dados	1 - Não há políticas e procedimentos relacionados documentados	1		
4.4 - Manter políticas e procedimentos para retenção e destruição segura de dados pessoais	1 - Não há políticas e procedimentos relacionados documentados	1		
4.5 - Integrar privacidade e proteção de dados em práticas de marketing direto com clientes por email e telefone	2 - Há políticas e procedimentos relacionados parcialmente documentados	2		
4.6 - Integrar a privacidade e proteção de dados nas práticas de recrutamento, seleção e contratação de colaboradores	2 - Há políticas e procedimentos relacionados parcialmente documentados	2		
4.7 - Integrar a privacidade e proteção de dados nas práticas de segurança e medicina do trabalho	2 - Há políticas e procedimentos relacionados parcialmente documentados	2		
4.8 - Integrar a privacidade e proteção de dados ao uso de vigilância por vídeo (CFTV)	2 - Há políticas e procedimentos relacionados parcialmente documentados	2		
4.9 - Integrar a privacidade e proteção de dados ao uso de dispositivos de geolocalização geográfica	1 - Não há políticas e procedimentos relacionados documentados	1		
5.1 - Conduzir treinamento em privacidade e proteção de dados	2 - Há treinamento em privacidade e proteção de dados, mas não periódico	2	**5. Treinamento e conscientização**	1,2
5.2 - Incorporar a privacidade e proteção dos dados ao treinamento operacional, como RH, segurança, etc	1 - O treinamento de privacidade e proteção de dados não faz parte do treinamento de ambientação.	1		
5.3- Fornecer um repositório de informações de privacidade e proteção de dados, por exemplo, uma intranet interna de privacidade e e proteção de dados	1 - Não há repositório de materiais relacionados a privacidade e proteção de dados.	1		
5.4 - Realizar eventos de conscientização de privacidade e proteção de dados (por	1 - Não são realizados eventos de conscientização	1		

exemplo, um dia / semana anual de privacidade de dados)	de privacidade e proteção de dados			
5.5 - Fornecer educação e treinamento contínuos para o DPO e manter a certificação dos responsáveis pela privacidade e proteção dos dados	1 - Não são realizados treinamentos para o DPO	1		
6.1 - Integrar privacidade e proteção de dados em uma política de segurança da informação	2 - Há política de segurança da informação, mas não política de privacidade ou vice versa	2	**6. Gerenciamento de riscos de segurança da informação**	3,9
6.2 - Integrar a segurança da informação na matriz de riscos da organização	2 - Na matriz de risco da organização estão listados parcialmente os riscos relacionados a segurança da informação.	2		
6.3 - Manter medidas técnicas de segurança e proteção de dados	5 - As principais medidas técnicas de segurança estão implementadas, tais como firewall e antimalware nas estações de trabalho e servidores. As atualizações de assinaturas ocorrem automaticamente. Há auditorias internas periódicas para aferir a efetividade dos controles.	5		
6.4 - Manter medidas para criptografar dados pessoais em repouso e em movimento	4 - Há medidas técnicas de criptografia implementadas para proteção de dados em repouso e movimento. Há retenção de logs de acessos ou tentativas de acesso a arquivos criptografados.	4		
6.5 - Manter procedimentos para restringir o acesso a dados pessoais (por exemplo, acesso baseado em função, segregação de funções)	4 - Há matriz de segregação de funções com a definição de usuários e perfis de acesso em cada sistema. A matriz é revisada periodicamente.	4		

6.6 - Manter os controles físicos de segurança da informação corporativa (proteção de instalações físicas e ativos físicos)	5 - As principais medidas técnicas de segurança física estão implementadas, tais como CFTV e controle de acesso. Há registro dos logs e os ativos são monitorados por sistema de CMDB. Os controles são auditados periodicamente.	5		
6.7 - Manter plano de continuidade de negócios (PCN)	4 - Há PCN baseado na ISO 22301, são executados testes e atualizações periódicas	4		
6.8 - Manter uma estratégia de prevenção de perda de dados pessoais	4 - Há backup periódico dos servidores que armazenam dados pessoais com testes de recuperação esporádicos.	4		
6.9 - Conduzir testes de intrusão para aferir o desempenho e efetividade dos controles de segurança	5 - São realizados teste de intrusão periódicos WAN to LAN e LAN to LAN White Box	5		
6.10 - Manter um sistema de prevenção de intrusos (IPS)	4 - Há IPS implantado para monitoramento e intercepção de ameaças. Há profissional alocado para resposta aos incidentes.	4		
6.11 - Manter um sistema de gerenciamento de dispositivos móveis (MDM)	3 - Há MDM implantado para monitoramento e controle de dispositivos.	3		
6.12 - Manter um sistema de gerenciamento e correlação de eventos de segurança (SIEM)	4 - Há SIEM implantado para coleta e notificação em caso de alertas de segurança. Os eventos de segurança são relacionados	4		
6.13 - Manter um sistema de gerenciamento de vulnerabilidades	4 - Há sistema de gerenciamento de vulnerabilidades implantado para consulta e obtenção de medidas de remediação. Um profissional é responsável por corrigir as vulnerabilidades	4		

6.14 - Manter um sistema de gerenciamento de acesso remoto seguro	4 - Há sistema de gerenciamento de acesso remoto seguro implantado com VPN e MFA.	4		
6.15 - Manter um sistema de gerenciamento de acesso as interfaces de rede	5 - Há sistema de gerenciamento de acesso as interfaces de rede através de VLAN e PortSecurity, com autenticação integrada via Radius e Health Check antes de autorizar acesso do host.	5		
6.16 - Manter um sistema de gerenciamento de mídias de armazenamento removível	4 - Há sistema de gerenciamento de mídias de armazenamento removível e há restrição de dispositivos. Há possibilidade de flexibilização por dispositivo e por período.	4		
7.1 - Manter política de privacidade e proteção de dados para terceiros (por exemplo, clientes, fornecedores, processadores, afiliados)	2 - Há políticas relacionadas parcialmente documentadas	2	**7. Gerenciamento de Riscos de Terceiros**	2,2
7.2 - Manter procedimentos para executar contratos ou acordos com todos os operadores	2 - Há procedimentos relacionados parcialmente documentados	2		
7.3 - Realizar a devida diligência em torno da postura de privacidade e proteção de dados, segurança de dados de fornecedores / operadores em potencial	2 - É feita diligência parcial em torno de operadores através de contrato.	2		
7.4 - Manter um processo de avaliação de risco de privacidade e proteção de dados do fornecedor (pré e pós contrato)	2 - Há procedimentos relacionados parcialmente documentados	2		
7.5 - Manter uma política que rege o uso de serviços em nuvem	3 - Há políticas relacionadas documentadas	3		
7.6 - Analisar os contratos para verificar riscos de privacidade de dados	2 - Há análise de alguns contratos sob não periódica	2		
8.1 - Manter um aviso de privacidade e proteção de dados que detalha as	3 - Há aviso de privacidade e proteção de dados que detalha as práticas de	3	**8. Plano de Comunicação**	3,4

práticas de tratamento de dados pessoais da organização	tratamento de dados pessoais da organização			
8.2 - Fornecer aviso de privacidade e proteção de dados em todos os pontos em que os dados pessoais são coletados	2 - Há aviso informal	2		
8.3 - Fornecer aviso nas comunicações de marketing (por exemplo, e-mails, folhetos, ofertas)	4 - Há aviso de privacidade e proteção de dados que detalha as práticas de tratamento de dados pessoais da organização. O mesmo é revisado periodicamente.	4		
8.4 - Fornecer aviso em contratos e termos	4 - Há aviso de privacidade e proteção de dados que detalha as práticas de tratamento de dados pessoais da organização. O mesmo é revisado periodicamente.	4		
8.5 - Manter scripts para uso dos funcionários para explicar ou fornecer o aviso de privacidade e proteção de dados	4 - Há scripts para uso dos funcionários para explicar ou fornecer o aviso de privacidade e proteção de dados. Os mesmos são revisados periodicamente.	4		
9.1 - Manter procedimentos e ferramenta para tratar de reclamações	2 - Há procedimentos relacionados parcialmente documentados	2	**9. Resposta aos Titulares dos Dados**	1,9
9.2 - Manter procedimentos e ferramenta para responder a solicitações de acesso a dados pessoais	2 - Há procedimentos relacionados parcialmente documentados	2		
9.3 - Manter procedimentos e ferramenta para responder a solicitações e / ou fornecer um mecanismo para os indivíduos atualizarem ou corrigirem seus dados pessoais	2 - Há procedimentos relacionados parcialmente documentados	2		
9.4 - Manter procedimentos e ferramenta para responder a pedidos de exclusão, restrição ou oposição ao processamento	1 - Não há procedimentos relacionados documentados	1		
9.5 - Manter procedimentos e ferramenta para responder a pedidos de informações	1 - Não há procedimentos relacionados documentados	1		

9.6 - Manter procedimentos e ferramenta para responder a solicitações de portabilidade de dados	2 - Há procedimentos relacionados parcialmente documentados	2		
9.7 - Manter procedimentos e ferramentas para responder a pedidos a serem esquecidos ou para apagar dados	2 - Há procedimentos relacionados parcialmente documentados	2		
9.8 - Manter perguntas frequentes (FAQ) para responder as dúvidas dos titulares dos dados	3 - Há procedimentos relacionados documentados	3		
9.9 - Investigar as causas raízes das reclamações de proteção de dados	2 - Há procedimentos relacionados parcialmente documentados	2		
9.10 - Monitorar e reportar métricas para reclamações de privacidade e proteção de dados (Tempo de resposta, quantidade, causa raiz)	2 - Há procedimentos relacionados parcialmente documentados	2		
10.1 - Manter procedimento de verificação de identidade dos titulares	2 - Há procedimentos relacionados parcialmente documentados	2	**10. Monitoramento de Novas Práticas Operacionais**	2,7
10.2 - Integrar o Privacy by Design no desenvolvimento de sistemas e produtos da organização	3 - Aspectos de privacidade são requisitos chave no desenvolvimento de sistemas e produtos da organização	3		
10.3 - Manter diretrizes e modelos de DPIA (Data Protection Impact Assessment) em conformidade com à LGPD	3 - Há DPIA de todos os processos que tratam dados pessoais na organização. Os DPIA de dados sensíveis são relatados para os reguladores	3		
11.1 - Manter um plano de resposta a incidentes / violações da privacidade de dados	3 - Há procedimentos relacionados documentados	3	**11. Gerenciamento de violação de privacidade de dados**	3,0
11.2 - Manter um protocolo de notificação de violação (para as pessoas afetadas) e relatórios (para reguladores, agências de crédito, órgãos policiais)	2 - Há procedimentos relacionados parcialmente documentados	2		
11.3 - Manter o registro quanto o rastreamento de incidentes / violações de privacidade e proteção de dados	2 - Há procedimentos relacionados parcialmente documentados	2		

11.4 - Monitorar e reportar as métricas de incidentes / violações de privacidade e proteção de dados (natureza da violação, risco, causa raiz)	4 - Há procedimentos relacionados documentados e são revisados periodicamente	4		
11.5 - Realizar testes periódicos do plano de violação / incidente de privacidade e proteção de dados	4 - São realizados testes periódicos do plano de violação / incidente de privacidade e proteção de dados. O plano é constantemente aprimorado a partir do resultado dos testes	4		
11.6 - Obter cobertura de seguro de violação de privacidade e proteção de dados	3 - Há cobertura completa de seguro de violação de privacidade e proteção de dados	3		
12.1 - Conduzir auditorias internas do programa de privacidade e proteção de dados	3 - São realizadas auditorias internas periódicas.	3	**12. Tratamento de Dados**	2,6
12.2 - Conduzir avaliações com base em eventos externos, como reclamações / violações, entre outros	3 - Todos os eventos externos são avaliados	3		
12.3 - Envolver a auditoria externas para avaliações independentes	2 - São realizadas auditorias externas não periódicas.	2		
12.4 - Monitorar e reportar as métricas de privacidade e proteção de dados	3 - Há métricas relevantes e relacionadas documentadas	3		
12.5 - Manter a documentação como evidência a fim de demonstrar conformidade e / ou prestação de conta	2 - Há documentação parcial relacionada	2		

Feedback	
O que você achou do modelo de maturidade de segurança da informação proposto?	interessante
Pontos Fortes do Modelo	Abrangente
Pontos Fracos do Modelo	Extenso

A Figura 13 apresenta um exemplo de relatório gráfico do resultado do assessment do MMSI.br.

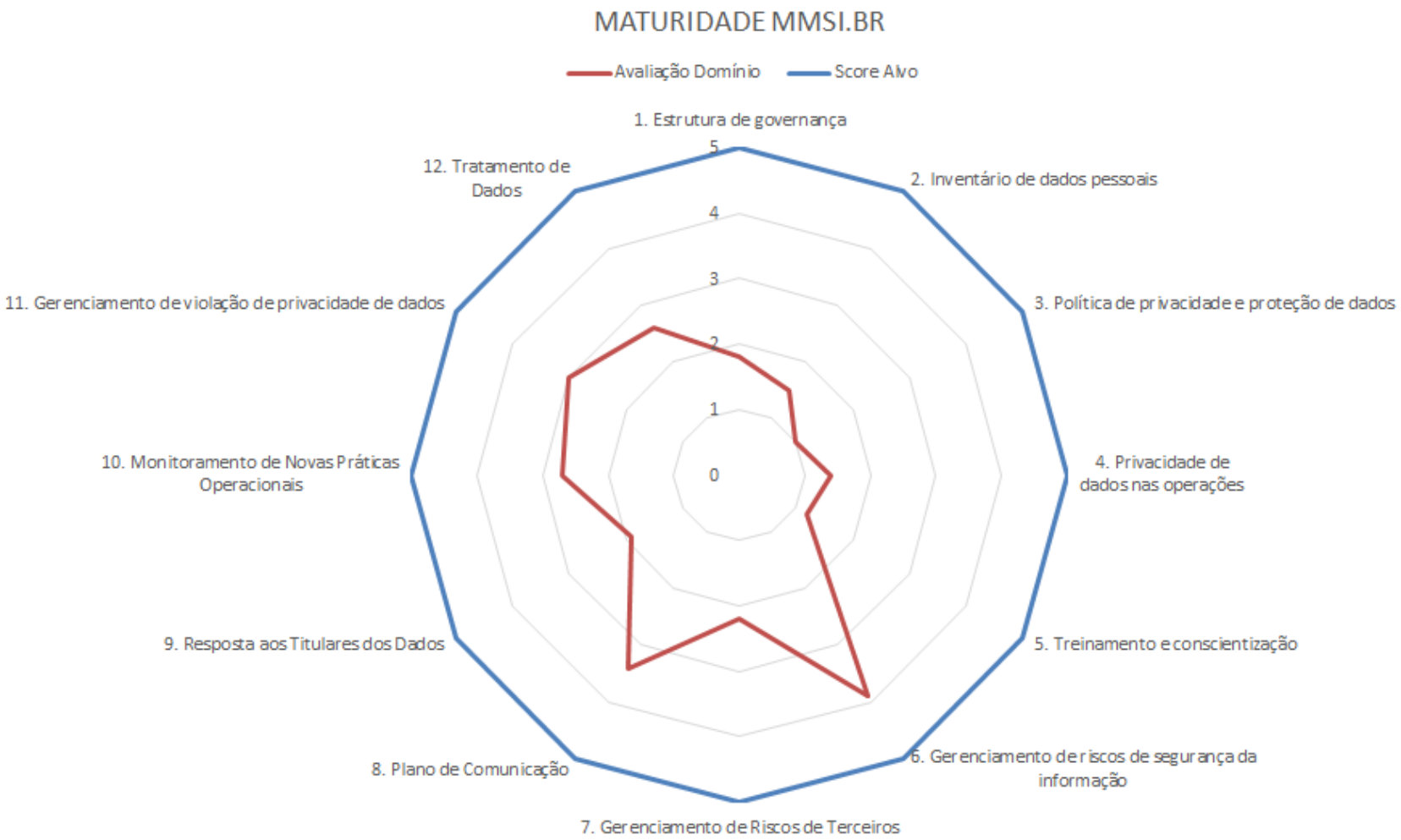


Figura 13: Gráfico radar de resultado de Assessment MMSI.br Fonte: Elaborado pelo Autor.

A partir dos resultados obtidos pelos participantes da pesquisa foi realizada uma análise quanto ao nível de aderência ao modelo MMSI.br por segmento organizacional. Para tanto, foi considerada para fins de cálculo o score máximo de 400 pontos por participante, tendo em vista o nível máximo de maturidade por processo que é 5 x 80 que corresponde ao número de processos avaliados (questões).

Após a apuração da pontuação individual dos participantes, foi calculada a aderência dos mesmos em nível percentual a partir da divisão do score obtido por 400. Em seguida as organizações participantes foram agrupadas por segmento, com seu respectivo nível de aderência ao modelo. Por fim, foi calculada a média de aderência por segmento organizacional conforme é apresentado na Figura 14.

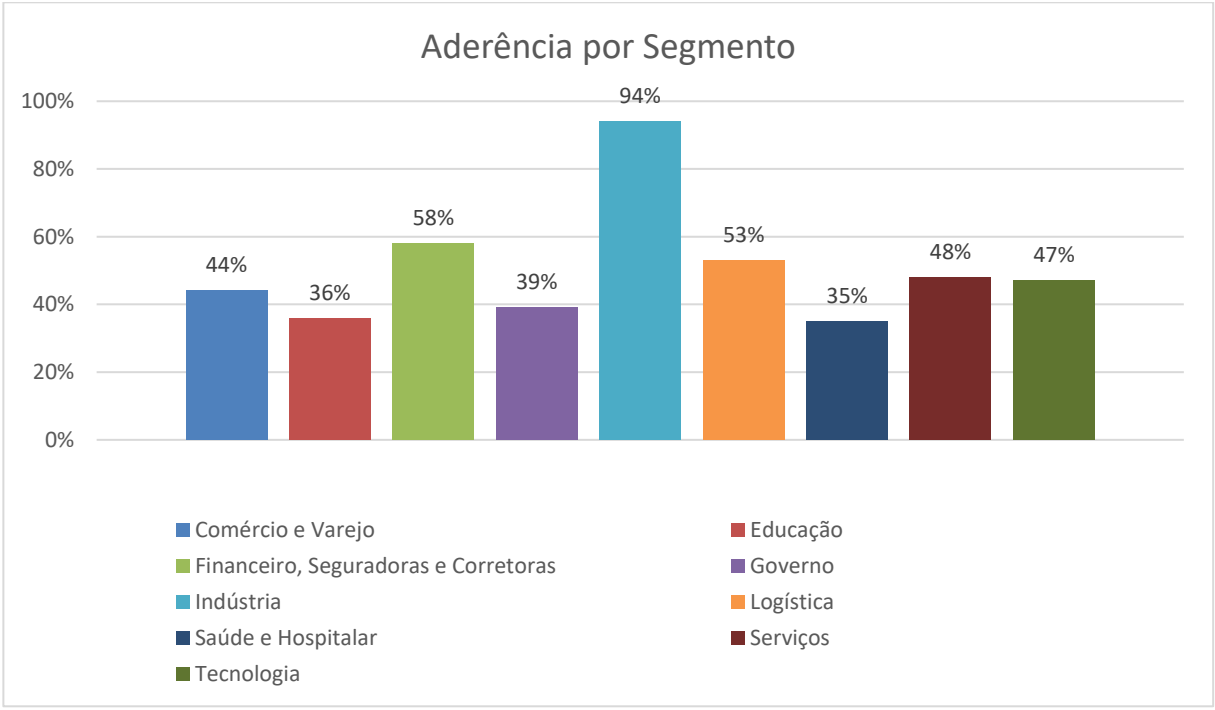


Figura 14: Aderência ao MMSI.br por segmento organizacional.

5. CONCLUSÃO

O modelo proposto teve boa aceitação por parte dos participantes da pesquisa, onde dentre os aspectos mais citados na avaliação foram a “abrangência do modelo” por 77% dos respondentes e o “detalhismo” por 58%. Espera-se que com a vigência da Lei Geral de Proteção de Dados a partir de 18 de setembro de 2020 o modelo se torne uma referência para as organizações em sua jornada para adequação a nova Lei e sobretudo para a disseminação de uma cultura organizacional de segurança da informação e privacidade.

No trabalho foram definidos os processos, domínios e capacidades considerados como critérios fundamentais para a avaliação das organizações brasileiras em relação ao seu nível de aderência a Lei Geral de Proteção de Dados, visando auxilia-las em seu processo de busca pela conformidade com a LGPD a partir da sinalização de suas principais forças e fraquezas em privacidade e proteção de dados.

Os objetivos definidos para este trabalho foram atingidos integralmente:

- Foi elaborado o modelo de maturidade de segurança da informação com foco na realidade das empresas brasileiras;
- Foram realizadas as avaliações públicas para que organizações pudessem tomar ciência sobre o seu nível de aderência em relação ao modelo proposto, bem como sugerir melhorias;
- Foram enviados os relatórios individuais para os participantes da avaliação, contendo os resultados na forma textual e gráfica.

As principais limitações identificadas residem no tempo relatado pelos participantes para o preenchimento do formulário de avaliação de aderência ao modelo e sobre a necessidade de conhecimento prévio em segurança da informação e privacidade para a participação na pesquisa, impactando diretamente no número de respondentes. Uma outra oportunidade de melhoria identificada está relacionada ao esforço para apuração manual do resultado e envio do relatório individual para cada participante.

Deste modo como trabalho futuro propõem-se o desenvolvimento de um sistema web para avaliação das organizações no MMSI.br, cujo processo de apuração do resultado seja realizado de forma automática e o envio do relatório seja automático, e preferencialmente realizado logo após preenchimento da

pesquisa pelo participante. Sugere-se também que seja avaliada a proporcionalidade do modelo em relação ao porte das organizações e as particularidades de cada segmento de negócio, objetivando uma análise mais específica e de modo a promover o benchmarking entre as organizações. Há ainda a possiblidade de estabelecimento de parcerias com instituições ou com a comunidade para melhoria contínua do modelo.

Visando ampliar a amostra, expandir os segmentos organizacionais participantes e assegurar a melhoria contínua do modelo a partir do recebimento de sugestões e críticas, o formulário será mantido com acesso público e de forma gratuita durante o ano corrente.

6. REFERÊNCIAS BIBLIOGRÁFICAS

ABNT NBR ISO/IEC 27001. **NBRISO/IEC27001: Tecnologia da informação - Técnicas de segurança - Sistemas de gestão de segurança da informação - Requisitos**. Disponível em: <https://www.normas.com.br/visualizador-slim/Viewer.asp?ns=25074&token=087e24e5-5274-4c29-89b4-4cbd2ce92688&sid=arxmpb4htbtu111gjzwl54tl&email=brunonbpaixao@gmail.com>. Acesso em: 18 maio. 2020.

ABNT NBR ISO/IEC 27002. **NBRISO/IEC27002: Tecnologia da informação - Técnicas de segurança - Código de Prática para controles de segurança da informação**. Disponível em: <https://www.normas.com.br/visualizador-slim/Viewer.asp?ns=21529&token=778a4f34-a23f-4a57-9810-3a23849ccb26&sid=arxmpb4htbtu111gjzwl54tl&email=brunonbpaixao@gmail.com>. Acesso em: 18 maio. 2020.

ABNT NBR ISO/IEC 27005. **NBRISO/IEC27005: Tecnologia da informação — Técnicas de segurança — Gestão de riscos de segurança da informação**. Disponível em: <https://www.normas.com.br/visualizador-slim/Viewer.asp?ns=27395&token=b42a628f-7d1f-46ab-abf0-82d1d707cc1d&sid=arxmpb4htbtu111gjzwl54tl&email=brunonbpaixao@gmail.com>. Acesso em: 24 maio. 2020.

BOSTON, V. A. **O-ISM3 Open Information Security Management Maturity Model**. Disponível em: <https://drive.google.com/file/d/1Z7_aRB6WKUZcvn4EcX-HdmIsj2sLvQUB/view?usp=sharing>. Acesso em: 18 jun. 2020.

BRASIL. **L13709**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 20 abr. 2020.

CARCARY, M. et al. A Framework for Information Security Governance and Management. **IT Professional**, v. 18, n. 2, p. 22–30, mar. 2016.

CERT.BR. **Estatísticas do CERT.br -- Incidentes**. Disponível em: <https://www.cert.br/stats/incidentes/>. Acesso em: 21 abr. 2020a.

CERT.BR. **Cartilha de Segurança -- Mecanismos de segurança**. Disponível em: <https://cartilha.cert.br/mecanismos/>. Acesso em: 18 set. 2020b.

CIAS. **The CCSMM**. Disponível em: <https://cias.utsa.edu/the-ccsmm.html>. Acesso em: 18 jun. 2020.

COANDĂ, H.; CIOACĂ, C.; BRATU, A. THE ANALYSIS OF BENCHMARKING APPLICATION IN CYBER SECURITY. **SCIENTIFIC RESEARCH AND EDUCATION IN THE AIR FORCE**, v. 19, n. 2, p. 57–62, 31 jul. 2017.

CSIS; MCAFEE. O impacto econômico do crime cibernético: sem indícios de desaceleração Resumo executivo. p. 4, 2018.

DARYUS. **GDPR x LGPDP x ISO 27001 WHITEPAPER.pdf**, 2020.

DOE. **Cybersecurity Capability Maturity Model (C2M2) Program**. Disponível em: <https://www.energy.gov/ceser/activities/cybersecurity-critical-energy-infrastructure/energy-sector-cybersecurity-0>. Acesso em: 18 jun. 2020.

DONEDA, D. **Da Privacidade à Proteção de Dados Pessoais 2º edição - thomsonreuters**. Disponível em: <https://www.livrariart.com.br/da-privacidade-a-protecao-de-dados-pessoais-2-edicao/p>. Acesso em: 20 set. 2020.

DOUCEK, P. et al. (EDS.). **Research and Practical Issues of Enterprise Information Systems: 13th IFIP WG 8.9 International Conference, CONFENIS 2019, Prague, Czech Republic, December 16–17, 2019, Proceedings**. Cham: Springer International Publishing, 2019. v. 375

FIGUEIREDO, A. T. S. DE. Proposta de implantação de um sistema de gestão de segurança da informação. 26 fev. 2016.

FRIEDEWALD, M. et al. (EDS.). **Privacy and Identity Management. Data for Better Living: AI and Privacy: 14th IFIP WG 9.2, 9.6/11.7, 11.6/SIG 9.2.2 International Summer School, Windisch, Switzerland, August 19–23, 2019, Revised Selected Papers**. Cham: Springer International Publishing, 2020. v. 576

GARCIA, A. et al. **Personal data protection maturity model for the micro financial sector in Peru**. 2018 4th International Conference on Computer and Technology Applications (ICCTA). **Anais**... In: 2018 4TH INTERNATIONAL CONFERENCE ON COMPUTER AND TECHNOLOGY APPLICATIONS (ICCTA). Istanbul: IEEE, maio 2018Disponível em: <https://ieeexplore.ieee.org/document/8398649/>. Acesso em: 9 fev. 2020

GDPR. REGULATION (EU) 2016/ 679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL - of 27 April 2016 - on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/ 46/ EC (General Data Protection Regulation). p. 88, 2016.

GHAFFARI, F.; ARABSORKHI, A. **A New Adaptive Cyber-security Capability Maturity Model**. 2018 9th International Symposium on Telecommunications (IST). **Anais**... In: 2018 9TH INTERNATIONAL SYMPOSIUM ON TELECOMMUNICATIONS (IST). Tehran, Iran: IEEE, dez. 2018Disponível em: <https://ieeexplore.ieee.org/document/8661018/>. Acesso em: 19 abr. 2020

GIL, A. C. **Métodos e técnicas de pesquisa social (6a. ed.).** Sao Paolo: Editora Atlas S.A., 2008.

GONÇALVES, H. DE A. **Manual de metodologia da pesquisa científica**. São Paulo: Avercamp, 2005.

HAWDON, J.; PARTI, K.; DEARDEN, T. E. Cybercrime in America amid COVID-19: the Initial Results from a Natural Experiment. **American Journal of Criminal Justice**, v. 45, n. 4, p. 546–562, ago. 2020.

HINTZBERGEN, J. et al. **Fundamentos de Segurança da Informação: Com base na ISO 27001 e na ISO 27002**. Rio de Janeiro: Brasport, 2018.

ISACA. **COBIT 2019 Framework: Introduction and Methodology**. Disponível em: <https://www.isaca.org/bookstore/bookstore-cobit_19-digital/wcb19fim>. Acesso em: 25 abr. 2020.

ISO/IEC 27000. **ISO/IEC 27000**. Disponível em: <https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-5:v1:en>. Acesso em: 27 abr. 2020.

JANSEN, L. A. INSTRUMENTO DE AVALIAÇÃO DE MATURIDADE EM PROCESSOS DE SEGURANÇA DA INFORMAÇÃO: ESTUDO DE CASO EM INSTITUIÇÕES HOSPITALARES. p. 166, 2008.

KABANOV, I. Scalable Frameworks for Application Security and Data Protection. In: JAHANKHANI, H. et al. (Eds.). . **Global Security, Safety and Sustainability - The Security Challenges of the Connected World**. Communications in Computer and Information Science. Cham: Springer International Publishing, 2016. v. 630p. 82–95.

KARLSSON, F.; KOLKOWSKA, E.; PRENKERT, F. Inter-organisational information security: a systematic literature review. **Information and Computer Security**, v. 24, n. 5, p. 418–451, 14 nov. 2016.

LE, N. T.; HOANG, D. B. **Can maturity models support cyber security?** 2016 IEEE 35th International Performance Computing and Communications Conference (IPCCC). **Anais**... In: 2016 IEEE 35TH INTERNATIONAL PERFORMANCE COMPUTING AND COMMUNICATIONS CONFERENCE (IPCCC). Las Vegas, NV, USA: IEEE, dez. 2016Disponível em: <http://ieeexplore.ieee.org/document/7820663/>. Acesso em: 2 dez. 2019

LE, N. T.; HOANG, D. B. Capability Maturity Model and Metrics Framework for Cyber Cloud Security. **Scalable Computing: Practice and Experience**, v. 18, n. 4, p. 277–290, 24 nov. 2017.

MALDONADO, V. N.; BLUM, R. O. **LGPD, lei geral de proteção de dados: comentada : obra de acordo com decreto 9.637/18, lei 13.787/18, medida provisória 869/18**. [s.l: s.n.].

MEINTS, M. The Relationship between Data Protection Legislation and Information Security Related Standards. In: MATYÁŠ, V. et al. (Eds.). . **The Future of Identity in the Information Society**. IFIP Advances in Information and Communication Technology. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009. v. 298p. 254–267.

MICHAEL, K. et al. **Privacy, Data Rights and Cybersecurity: Technology for Good in the Achievement of Sustainable Development Goals**. 2019 IEEE International Symposium on Technology and Society (ISTAS). **Anais**... In: 2019 IEEE INTERNATIONAL SYMPOSIUM ON TECHNOLOGY AND SOCIETY (ISTAS). Medford, MA, USA: IEEE, nov. 2019Disponível em: <https://ieeexplore.ieee.org/document/8937956/>. Acesso em: 20 abr. 2020

MIRANDA, J. **Atos legislativos**. Coimbra: Almedina, 2019.

NAIDOO, R. A multi-level influence model of COVID-19 themed cybercrime. **European Journal of Information Systems**, v. 29, n. 3, p. 306–321, 3 maio 2020.

NAKAMURA, E. T.; GEUS, P. L. DE. **Segurança de redes em ambientes cooperativos**. São Paulo (SP): Novatec, 2007.

NETO, P. T. M.; ARAÚJO, W. J. D. **Segurança da informação: uma visão sistêmica para implantação em organizações**. [s.l.] figshare, 2020. p. 5339754 Bytes

NEWHOUSE, W. et al. **National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework**. Gaithersburg, MD: National Institute of Standards and Technology, 7 ago. 2017. Disponível em: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf>. Acesso em: 18 jun. 2020.

NIELES, M. et al. **An introduction to information security**. [s.l: s.n.].

NIST. **Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1**. Gaithersburg, MD: National Institute of Standards and Technology, 2018. Disponível em: <http://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf>. Acesso em: 18 set. 2020.

PECK, P., Patricia. **Proteção de Dados Pessoais: Comentários à Lei n. 13.709/2018 -LGPD**. [s.l.] Saraiva Educação S.A., 2020.

RAMOS, L. C. P.; GOMES, A. V. M. LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS E SEUS REFLEXOS NAS RELAÇÕES DE TRABALHO. **SCIENTIA IURIS**, p. 20, 2019.

REA-GUAMAN, A. M. et al. **Maturity models in cybersecurity: A systematic review**. 2017 12th Iberian Conference on Information Systems and Technologies (CISTI). **Anais**... In: 2017 12TH IBERIAN CONFERENCE ON INFORMATION SYSTEMS AND TECHNOLOGIES (CISTI). Lisbon, Portugal: IEEE, jun. 2017Disponível em: <http://ieeexplore.ieee.org/document/7975865/>. Acesso em: 2 dez. 2019

RIGON, E. A.; WESTPHALL, C. M. **Artigo - MODELO DE AVALIAÇÃO DA MATURIDADE DA SEGURANÇA DA INFORMAÇÃO.pdf**, 2011.

RODRIGUES BRANCHER, P. M.; BEPPU, A. C. **Proteção de dados pessoais no Brasil: uma nova visão a partir da lei no. 13.709/2018**. [s.l: s.n.].

SERASA EXPERIAN. **85% das empresas declaram que ainda não estão prontas para atender às exigências da Lei de Proteção de Dados Pessoais, mostra pesquisa da Serasa Experian**. Disponível em: </sala-de-imprensa/85-das-empresas-declaram-que-ainda-nao-estao-prontas-para-atender-as-exigencias-da-lei-de-protecao-de-dados-pessoais-mostra-pesquisa-da-serasa-experian>. Acesso em: 21 abr. 2020.

SFORZA, A.; STERLE, C. (EDS.). **Optimization and Decision Science: Methodologies and Applications**. Cham: Springer International Publishing, 2017. v. 217

SILVA, M. P.; BARROS, R. M. **Artigo - Maturity Model of Information Security for Software Developers.pdf**IEEE Latin America Transactions, , 2017.

SILVA; MENEZES. **Metodologia da Pesquisa e Elaboração de Dissertação**. Disponível em: <https://www.researchgate.net/publication/312125489_Metodologia_da_Pesquisa_e_Elaboracao_de_Dissertacao>. Acesso em: 20 set. 2020.

SOFTEX. **MODELO - MR-MPS-SV 2015.pdf**, 2015. Disponível em: <https://softex.br/mpsbr/guias/#>. Acesso em: 14 jul. 2020

WHITE, G. **The Community Cyber Security Maturity Model**. 2007 40th Annual Hawaii International Conference on System Sciences (HICSS'07). **Anais**... In: 2007 40TH ANNUAL HAWAII INTERNATIONAL CONFERENCE ON SYSTEM SCIENCES (HICSS'07). Waikoloa, HI, USA: IEEE, 2007Disponível em: <http://ieeexplore.ieee.org/document/4076571/>. Acesso em: 3 dez. 2019

WILLIAMS, L.; MCGRAW, G.; MIGUES, S. Engineering Security Vulnerability Prevention, Detection, and Response. **IEEE Software**, v. 35, n. 5, p. 76–80, set. 2018.

Apêndice A – Formulário para validação do modelo de maturidade em segurança da informação brasileiro (MMSI.br)

Validação MMSI.br

Esta pesquisa tem como objetivo a validação do modelo de maturidade em segurança da informação brasileiro (MMSI.br). Neste são avaliados 86 processos organizados em 12 domínios com foco em privacidade e proteção de dados.

A maturidade de cada processo é classificada de 1 a 5, onde 1 é o nível inicial e 5 é o otimizado. A maturidade de cada domínio é calculada a partir da média da maturidade de seus processos. Os dados coletados serão utilizados para gerar uma análise gráfica similar a figura abaixo a ser disponibilizada para os participantes através do email de contato informado.

As estatísticas globais da pesquisa poderão ser publicadas de forma anônima (organizações não serão divulgadas), na dissertação de mestrado que está sendo desenvolvida em torno do modelo de maturidade aqui apresentado.

Em caso de dúvidas ou sugestões entre em contato através do email brunonbpaixao@gmail.com.

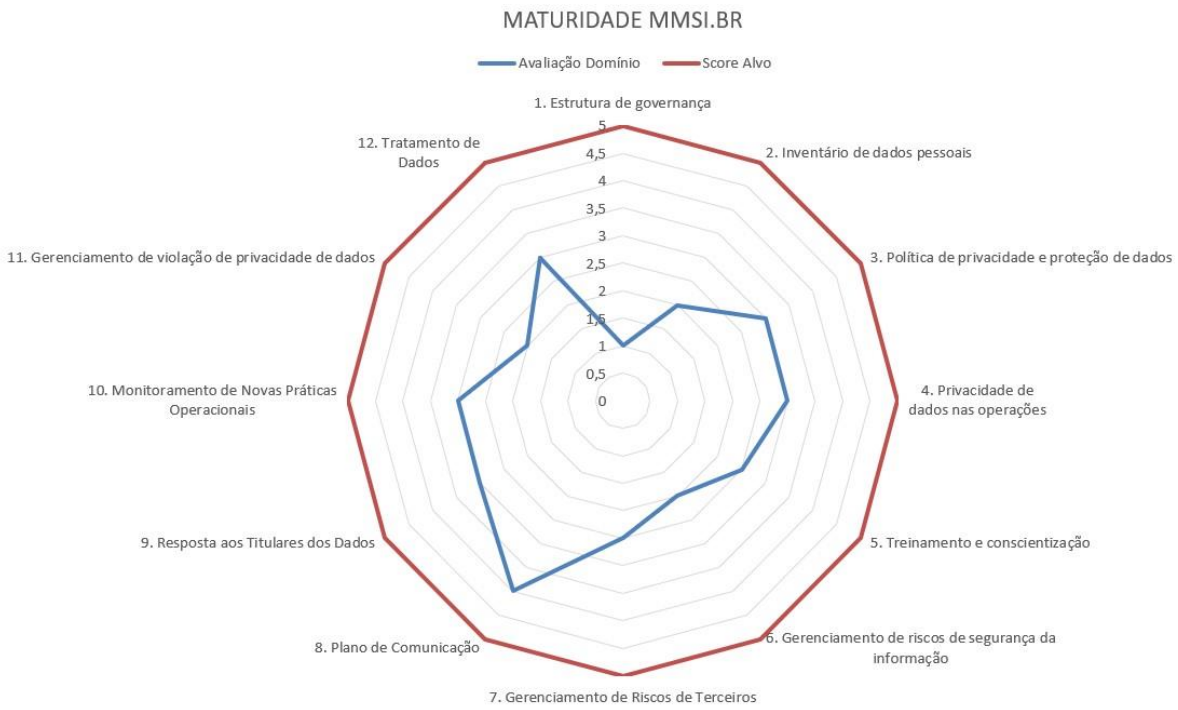
Obrigado

Bruno Paixão https://www.linkedin.com/in/brunonbpaixao/

*Obrigatório

1. Endereço de e-mail *

Gráfico de Radar



2. Nome e Sobrenome

Minimização (Art. 6, III - LGPD)

3. UF *

4. Organização

5. Segmento Empresarial *

- [ ] Comércio e Varejo
- [ ] Serviços
- [ ] Logística
- [ ] Educação
- [ ] Saúde e Hospitalar
- [ ] Tecnologia
- [ ] Construção e Engenharia
- [ ] Financeiro, Seguradoras e Corretoras

Outros

6. Número de Colaboradores *

- [ ] Até 5 Colaboradores
- [ ] De 6 A 99 Colaboradores
- [ ] De 100 a 499 Colaboradores
- [ ] De 500 A 999 Colaboradores
- [ ] Mais de 1000 Colaboradores

1. Estrutura de governança

7. 1.1 - Atribuir a responsabilidade pela privacidade e proteção dos dados a um indivíduo (encarregado de dados) *

- [ ] 1 - Não há responsável atribuído
- [ ] 2 - Responsável definido, mas não nomeado formalmente
- [ ] 3 - Responsável definido e nomeado formalmente
- [ ] 4 - Responsável definido, nomeado formalmente, reporta diretamente a alta direção sem acumular cargo
- [ ]

5 - Responsável definido, nomeado formalmente, reporta diretamente a alta direção sem acumular cargo. O profissional é certificado para atuar como encarregado de dados

8. 1.2 - Envolver a alta direção em privacidade e proteção de dados e atribuir responsabilidade pela privacidade e proteção dos dados em toda a organização *

- [ ] 1 - Não há comitê de privacidade e proteção de dados
- [ ] 2 - Há comitê de privacidade e proteção de dados sem reuniões regulares
- [ ] 3 - Há comitê de privacidade e proteção de dados com reuniões regulares
- [ ] 4 - Há comitê de privacidade e proteção de dados com reuniões regulares, com a participação de membros das áreas de TI, Segurança, Jurídico e DPO
- [ ] 5 - Há comitê de privacidade e proteção de dados com reuniões regulares, com a participação de membros das áreas de TI, Segurança, Jurídico, DPO (Líder) e Diretoria (Patrocinador).

9. 1.3 - Conduzir comunicação regular junto às partes interessadas internas da organização o status do gerenciamento de privacidade e proteção de dados *

- [ ] 1 - Não há comunicação e nem um plano definido.
- [ ] 2 - Comunicação ocorre de forma esporádica, mas sem um plano definido.
- [ ] 3 - Comunicação ocorre periodicamente e tem um plano definido.
- [ ] 4 - Comunicação ocorre periodicamente e tem um plano definido. São utilizados múltiplos canais para atingir as partes interessadas
- [ ] 5 - Há um plano de comunicação com periodicidade e responsável definido. São utilizados múltiplos canais para atingir as partes interessadas. A efetividade dos canais é medida através de indicadores

10. 1.4 - Reportar às partes interessadas externas da organização o status do gerenciamento de privacidade (por exemplo, órgãos reguladores, terceiros, clientes) *

1 - Não há comunicação e nem um plano definido.

2 - Comunicação ocorre de forma esporádica, mas sem um plano definido.

3 - Comunicação ocorre periodicamente e tem um plano definido.

4 - Comunicação ocorre periodicamente e tem um plano definido. São utilizados múltiplos canais para atingir as partes interessadas

5 - Há um plano de comunicação com periodicidade e responsável definido. São utilizados múltiplos canais para atingir as partes interessadas. A efetividade dos canais é medida através de indicadores

11. 1.5 - Realizar uma avaliação de risco de privacidade e proteção de dados da empresa (DPIA) *

1 - Os processos que tratam dados pessoais não estão mapeados

2 - Os processos que tratam dados pessoais estão mapeados parcialmente

3 - Os processos que tratam dados pessoais estão mapeados

4 - Os processos que tratam dados pessoais estão mapeados e há um DPIA

5 - Os processos que tratam dados pessoais estão mapeados, há um DPIA e um plano de ação com responsáveis definidos

12. 1.6 - Integrar a privacidade de dados nas avaliações e relatórios de riscos corporativos *

1 - Riscos relativos à privacidade de dados não estão mapeados 2 - Riscos relativos à privacidade de dados estão parcialmente mapeados

3 - Riscos relativos à privacidade de dados estão mapeados.

4 - Riscos relativos à privacidade de dados estão mapeados, tem responsáveis e estão associados a um plano de ação.

5 - Riscos relativos à privacidade de dados estão mapeados, tem responsáveis, estão associados a um plano de ação e são auditados.

13. 1.7 - Manter um programa e uma estratégia visando assegurar a privacidade e proteção de dados *

1 - Não há programa ou estratégia para a assegurar a privacidade e proteção de dados.

2 - Ações para assegurar a privacidade e proteção de dados são tomadas, mas não há um programa definido.

3 - Ações para assegurar a privacidade e proteção de dados são tomadas de acordo com um programa definido.

4 - Ações para assegurar a privacidade e proteção de dados são tomadas de acordo com um programa definido. Há indicadores para medir a efetividade das ações.

5 - Ações para assegurar a privacidade e proteção de dados são tomadas de acordo com um programa definido. Há indicadores para medir a efetividade das ações. São realizadas auditorias periódicas.

14. 1.8 - Exigir que os funcionários reconheçam e concordem em aderir às políticas de privacidade e proteção de dados *

- [ ] 1 - Não há política de privacidade e proteção de dados
- [ ] 2 - Há política de privacidade e proteção de dados, mas não é reconhecida e assinada pelos funcionários em sua totalidade
- [ ] 3 - Há política de privacidade e proteção de dados, esta é reconhecida e assinada pelos funcionários em sua totalidade
- [ ] 4 - Há política de privacidade e proteção de dados, esta é reconhecida e assinada pelos funcionários em sua totalidade. O documento é revisado periodicamente.
- [ ] 5 - Há política de privacidade e proteção de dados, esta é reconhecida e assinada pelos funcionários em sua totalidade. O documento é revisado periodicamente e as alterações são informadas aos funcionários.

2. Inventário de dados pessoais

15. 2.1 - Manter um inventário de dados pessoais que são tratados *

- [ ] 1 - Não há um inventário dos dados pessoais tratados
- [ ] 2 - Há um inventário parcial dos dados pessoais tratados
- [ ] 3 - Há um inventário completo dos dados pessoais tratados em formato 5W2H ou sistema
- [ ] 4 - Há um inventário completo dos dados pessoais tratados em formato 5W2H ou sistema. Isso é revisado periodicamente e mantido descentralizadamente
- [ ]

5 - Há um inventário completo dos dados pessoais tratados em formato 5W2H ou sistema. Isso é revisado periodicamente e mantido centralizadamente.

16. 2.2 - Classificar os dados pessoais tratados *

- [ ] 1 - Não há política de classificação de dados
- [ ] 2 - Há política de classificação de dados de dados, mas dados são classificados parcialmente
- [ ] 3 - Há política de classificação de dados de dados e estão são classificados manualmente
- [ ] 4 - Há política de classificação de dados de dados e estes são classificados automaticamente
- [ ] 5 - Há política de classificação de dados de dados e estes são classificados automaticamente. Há monitoração de dados através de solução de Data Loss Prevention (DLP).

17. 2.3 - Obter aprovação dos reguladores e/ou autoridades para processamento de dados e registrar bancos de dados onde este é necessário para aprovação prévia *

- [ ] 1 - Dados sensíveis não estão mapeados e são tratados sem aprovação das autoridades
- [ ] 2 - Dados sensíveis estão parcialmente mapeados e são tratados sem aprovação das autoridades
- [ ] 3 - Dados sensíveis estão mapeados e são tratados com aprovação das autoridades
- [ ] 4 - Dados sensíveis estão mapeados e são tratados com aprovação das autoridades. São utilizados recursos de mascaramento e pseudoanonimização
- [ ] 5 - Dados sensíveis estão mapeados e são tratados com aprovação das autoridades. São utilizados recursos de mascaramento e anonimização.

18. 2.4 - Manter registros do mecanismo de transferência usado para fluxos de dados transfronteiriços e aprovações de órgãos reguladores *

1 - Dados pessoais são transferidos internacionalmente, mas sem adoção de mecanismo de transferências e aprovação das autoridades

2 - Dados pessoais são transferidos internacionalmente, são adotados parcialmente mecanismos de transferências, tais como RCV e Cláusulas contratuais.

3 - Dados pessoais são transferidos internacionalmente com permissão das autoridades, são adotados mecanismos de transferências, tais como RCV e Cláusulas contratuais.

4 - Dados pessoais são transferidos internacionalmente com permissão das autoridades, são adotados mecanismos de transferências, tais como RCV e Cláusulas contratuais. Bases legais estão definidas para a transferência de dados.

5 - Dados pessoais são transferidos internacionalmente com permissão das autoridades, são adotados mecanismos de transferências, tais como RCV e Cláusulas contratuais. Bases legais estão definidas para a transferência de dados. Transferências ocorrem via canal criptografado utilizando VPN Site to Site.

3. Política de privacidade e proteção de dados

19. 3.1 - Manter uma política de privacidade e proteção de dados para funcionários contendo as bases legais para o tratamento de dados pessoais *

1 - Não há política de privacidade e proteção de dados para funcionários

2 - Há política de privacidade e proteção de dados para funcionários

3 - Há política de privacidade e proteção de dados para funcionários e estes foram treinados

4 - Há política de privacidade e proteção de dados para funcionários e estes foram treinados. O documento é revisado periodicamente.

5 - Há política de privacidade e proteção de dados para funcionários e estes foram treinados. O documento é revisado periodicamente e divulgado adequadamente na organização.

20. 3.2 - Manter uma política de privacidade e proteção de dados para terceiros contendo as bases legais para o tratamento de dados pessoais *

1 - Não há política de privacidade e proteção de dados para terceiros

- [ ] 2 - Há política de privacidade e proteção de dados para terceiros
- [ ] 3 - Há política de privacidade e proteção de dados para terceiros e estes foram treinados
- [ ] 4 - Há política de privacidade e proteção de dados para terceiros e estes foram treinados. O documento é revisado periodicamente.
- [ ] 5 - Há política de privacidade e proteção de dados para terceiros e estes foram treinados. O documento é revisado periodicamente e divulgado adequadamente na organização.

21. 3.3 - Integrar ética ao tratamento de dados através de códigos de conduta organizacional *

- [ ] 1 - Não há um código de conduta e ética organizacional
- [ ] 2 - Há um código de conduta e ética organizacional, mas não aborda privacidade e proteção de dados
- [ ] 3 - Há um código de conduta e ética organizacional que aborda privacidade e proteção de dados
- [ ] 4 - Há um código de conduta e ética organizacional que aborda privacidade e proteção de dados. O documento é revisado periodicamente.
- [ ] 5 - Há um código de conduta e ética organizacional que aborda privacidade e proteção de dados. O documento é revisado periodicamente e colaboradores recebem treinamento específico.

22. 3.4 - Manter atualizados procedimentos para coleta e uso de dados pessoais e dados sensíveis *

- [ ] 1 - Não há procedimentos documentados
- [ ] 2 - Há procedimentos parcialmente documentados
- [ ] 3 - Todos os procedimentos relacionados estão documentados
- [ ] 4 - Todos os procedimentos relacionados estão documentados e são revisados periodicamente
- [ ] 5 - Todos os procedimentos relacionados estão documentados, são revisados e auditados periodicamente

4. Privacidade de dados nas operações

23. 4.1 - Manter políticas e procedimentos para identificação e manutenção da qualidade dos dados (válidos e atualizados). *

- [ ] 1 - Não há políticas e procedimentos relacionados documentados
- [ ] 2 - Há políticas e procedimentos relacionados parcialmente documentados
- [ ] 3 - Há políticas e procedimentos relacionados documentados
- [ ] 4 - Há políticas e procedimentos relacionados documentados e são revisados periodicamente
- [ ] 5 - Há políticas e procedimentos relacionados documentados, estes são revisados e auditados periodicamente

24. 4.2 - Manter políticas e procedimentos para revisar o tratamento total ou parcialmente por meios automatizados, tais como uso de cookies e mecanismos de rastreamento de clientes *

- [ ] 1 - Não há políticas e procedimentos relacionados documentados
- [ ] 2 - Há políticas e procedimentos relacionados parcialmente documentados
- [ ] 3 - Há políticas e procedimentos relacionados documentados
- [ ] 4 - Há políticas e procedimentos relacionados documentados e são revisados periodicamente
- [ ] 5 - Há políticas e procedimentos relacionados documentados, estes são revisados e auditados periodicamente

25. 4.3 - Manter políticas e procedimentos para obter consentimento válido por parte dos titulares dos dados *

- [ ] 1 - Não há políticas e procedimentos relacionados documentados
- [ ] 2 - Há políticas e procedimentos relacionados parcialmente documentados
- [ ] 3 - Há políticas e procedimentos relacionados documentados
- [ ] 4 - Há políticas e procedimentos relacionados documentados e são revisados periodicamente
- [ ] 5 - Há políticas e procedimentos relacionados documentados, estes são revisados e auditados periodicamente

26. 4.4 - Manter políticas e procedimentos para retenção e destruição segura de dados pessoais *

- [ ] 1 - Não há políticas e procedimentos relacionados documentados
- [ ] 2 - Há políticas e procedimentos relacionados parcialmente documentados
- [ ] 3 - Há políticas e procedimentos relacionados documentados
- [ ] 4 - Há políticas e procedimentos relacionados documentados e são revisados periodicamente
- [ ] 5 - Há políticas e procedimentos relacionados documentados, estes são revisados e auditados periodicamente

27. 4.5 - Integrar privacidade e proteção de dados em práticas de marketing direto com clientes por email e telefone *

- [ ] 1 - Não há políticas e procedimentos relacionados documentados

28. 4.6 - Integrar a privacidade e proteção de dados nas práticas de recrutamento, seleção e contratação de colaboradores *

- [ ] 1 - Não há políticas e procedimentos relacionados documentados
- [ ] 2 - Há políticas e procedimentos relacionados parcialmente documentados
- [ ] 3 - Há políticas e procedimentos relacionados documentados
- [ ] 4 - Há políticas e procedimentos relacionados documentados e são revisados periodicamente
- [ ] 5 - Há políticas e procedimentos relacionados documentados, estes são revisados e auditados periodicamente

29. 4.7 - Integrar a privacidade de dados ao uso de práticas de mídia social da organização *

- [ ] 1 - Não há políticas e procedimentos relacionados documentados
- [ ] 2 - Há políticas e procedimentos relacionados parcialmente documentados
- [ ] 3 - Há políticas e procedimentos relacionados documentados
- [ ] 4 - Há políticas e procedimentos relacionados documentados e são revisados periodicamente
- [ ] 5 - Há políticas e procedimentos relacionados documentados, estes são revisados e auditados periodicamente

30. 4.8 - Integrar a privacidade e proteção de dados nas políticas / procedimentos Bring Your Own Device (BYOD), se houver *

- [ ] 1 - Não há políticas e procedimentos relacionados documentados

31. 4.9 - Integrar a privacidade e proteção de dados nas práticas de segurança e medicina do trabalho *

- [ ] 1 - Não há políticas e procedimentos relacionados documentados
- [ ] 2 - Há políticas e procedimentos relacionados parcialmente documentados
- [ ] 3 - Há políticas e procedimentos relacionados documentados
- [ ] 4 - Há políticas e procedimentos relacionados documentados e são revisados periodicamente
- [ ] 5 - Há políticas e procedimentos relacionados documentados, estes são revisados e auditados periodicamente

32. 4.10 - Integrar a privacidade e proteção de dados em práticas para monitorar funcionários *

- [ ] 1 - Não há políticas e procedimentos relacionados documentados
- [ ] 2 - Há políticas e procedimentos relacionados parcialmente documentados
- [ ] 3 - Há políticas e procedimentos relacionados documentados
- [ ] 4 - Há políticas e procedimentos relacionados documentados e são revisados periodicamente
- [ ] 5 - Há políticas e procedimentos relacionados documentados, estes são revisados e auditados periodicamente

33. 4.11 - Integrar a privacidade e proteção de dados ao uso de vigilância por vídeo (CFTV) *

- [ ] 1 - Não há políticas e procedimentos relacionados documentados

34. 4.12 - Integrar a privacidade e proteção de dados ao uso de dispositivos de geolocalização geográfica *

- [ ] 1 - Não há políticas e procedimentos relacionados documentados
- [ ] 2 - Há políticas e procedimentos relacionados parcialmente documentados
- [ ] 3 - Há políticas e procedimentos relacionados documentados
- [ ] 4 - Há políticas e procedimentos relacionados documentados e são revisados periodicamente
- [ ] 5 - Há políticas e procedimentos relacionados documentados, estes são revisados e auditados periodicamente

35. 4.13 - Integrar a privacidade dos dados no acesso delegado às contas de email da empresa dos funcionários (por exemplo, férias e rescisão) *

- [ ] 1 - Não há políticas e procedimentos relacionados documentados
- [ ] 2 - Há políticas e procedimentos relacionados parcialmente documentados
- [ ] 3 - Há políticas e procedimentos relacionados documentados
- [ ] 4 - Há políticas e procedimentos relacionados documentados e são revisados periodicamente
- [ ] 5 - Há políticas e procedimentos relacionados documentados, estes são revisados e auditados periodicamente

36. 4.14 - Integrar a privacidade e proteção de dados às práticas de descoberta eletrônica *

- [ ] 1 - Não há políticas e procedimentos relacionados documentados

37. 4.15 - Integrar a privacidade e proteção de dados em práticas para divulgação e para fins de aplicação da lei *

- [ ] 1 - Não há políticas e procedimentos relacionados documentados
- [ ] 2 - Há políticas e procedimentos relacionados parcialmente documentados
- [ ] 3 - Há políticas e procedimentos relacionados documentados
- [ ] 4 - Há políticas e procedimentos relacionados documentados e são revisados periodicamente
- [ ] 5 - Há políticas e procedimentos relacionados documentados, estes são revisados e auditados periodicamente

5. Treinamento e conscientização

38. 5.1 - Conduzir treinamento em privacidade e proteção de dados *

- [ ] 1 - Não Treinamento em privacidade e proteção de dados
- [ ] 2 - Há treinamento em privacidade e proteção de dados, mas não periódico
- [ ] 3 - Há treinamento em privacidade e proteção de dados periodicamente
- [ ] 4 - Há treinamento em privacidade e proteção de dados periodicamente com realização de avaliação de impacto
- [ ] 5 - Há treinamento em privacidade e proteção de dados periodicamente com realização de avaliação de impacto. O resultado das avaliações é utilizado para aprimoramento contínuo do treinamento.

39. 5.2 - Incorporar a privacidade e proteção dos dados ao treinamento operacional, como RH, segurança, etc *

- [ ] 1 - O treinamento de privacidade e proteção de dados não faz parte do treinamento de ambientação.
- [ ] 2 - Há treinamento parcial de privacidade e proteção de dados durante ambientação.
- [ ] 3 - Há treinamento completo de privacidade e proteção de dados durante ambientação.
- [ ] 4 - Há treinamento completo de privacidade e proteção de dados durante ambientação. Ao final é realizada uma avaliação de impacto.

5 - Há treinamento completo de privacidade e proteção de dados durante ambientação. Ao final é realizada uma avaliação de impacto e os resultados são utilizados para o aprimoramento contínuo do treinamento.

40. 5.3 - Desenvolver e publicar boletim de privacidade e proteção de dados ou incorporar a privacidade e proteção de dados às comunicações corporativas existentes *

( ) 1 - Não há boletim de privacidade e proteção de dados enviado pela área de comunicação.

( ) 2 - Há boletim não periódico de privacidade e proteção de dados enviado pela área de comunicação.

( ) 3 - Há boletim periódico de privacidade e proteção de dados enviado pela área de comunicação.

( ) 4 - Há boletim periódico de privacidade e proteção de dados enviado pela área de comunicação. São utilizados muito canais de divulgação para melhor atingimento do público alvo

( ) 5 - Há boletim periódico de privacidade e proteção de dados enviado pela área de comunicação. São utilizados muito canais de divulgação para melhor atingimento do público alvo. Há métricas de aferição da efetividade dos canais de comunicação.

41. 5.4 - Fornecer um repositório de informações de privacidade e proteção de dados, por exemplo, uma intranet interna de privacidade e e proteção de dados *

( ) 1 - Não há repositório de materiais relacionados a privacidade e proteção de dados.

( ) 2 - Há repositório de materiais relacionados a privacidade e proteção de dados. Contudo este não é divulgado.

( ) 3 - Há repositório de materiais relacionados a privacidade e proteção de dados. Este é divulgado

( ) 4 - Há repositório de materiais relacionados a privacidade e proteção de dados. Este é divulgado e atualizado periodicamente manualmente.

( ) 5 - Há repositório de materiais relacionados a privacidade e proteção de dados. Este é divulgado e atualizado periodicamente automaticamente.

42. 5.5 - Realizar eventos de conscientização de privacidade e proteção de dados (por exemplo, um dia / semana anual de privacidade de dados) *

- [ ] 1 - Não são realizados eventos de conscientização de privacidade e proteção de dados
- [ ] 2 - São realizados eventos de conscientização de privacidade e proteção de dados, mas sem calendário pré-definido.
- [ ] 3 - São realizados eventos de conscientização de privacidade e proteção de dados, com calendário pré-definido.
- [ ] 4 - São realizados eventos de conscientização de privacidade e proteção de dados, com calendário pré-definido. O evento conta com a participação da diretoria e gerência.
- [ ] 5 - São realizados eventos de conscientização de privacidade e proteção de dados, com calendário pré-definido. O evento conta com a participação da diretoria e gerência. Há métricas para aferir o nível de participação e engajamento dos colaboradores.

43. 5.6 - Fornecer educação e treinamento contínuos para o DPO e manter a certificação dos responsáveis pela privacidade e proteção dos dados *

- [ ] 1 - Não são realizados treinamentos para o DPO
- [ ] 2 - São realizados treinamentos não periódicos para o DPO
- [ ] 3 - São realizados treinamentos periódicos para o DPO.
- [ ] 4 - São realizados treinamentos periódicos para o DPO. E as certificações são renovadas não periodicamente
- [ ] 5 - São realizados treinamentos periódicos para o DPO. E as certificações são renovadas periodicamente

6. Gerenciamento de riscos de segurança da informação

44. 6.1 - Integrar o risco de privacidade e proteção de dados nas avaliações de risco de segurança *

- [ ] 1 - Na matriz de risco da organização não estão listados riscos relacionados a privacidade e proteção de dados.
- [ ] 2 - Na matriz de risco da organização estão listados parcialmente os riscos relacionados a privacidade e proteção de dados.
- [ ]
- [ ]

3 - Na matriz de risco da organização estão listados os riscos relacionados a privacidade e proteção de dados.

4 - Na matriz de risco da organização estão listados os riscos relacionados a privacidade e proteção de dados. Há um plano de ação para cada um dos riscos.

5 - Na matriz de risco da organização estão listados os riscos relacionados a privacidade e proteção de dados. Há um plano de ação para cada um dos riscos. Os controles são auditados periodicamente.

45. 6.2 - Integrar privacidade e proteção de dados em uma política de segurança da informação *

1 - Não há política de segurança da informação e privacidade

2 - Há política de segurança da informação, mas não política de privacidade e proteção de dados ou vice versa

3 - Há política de segurança da informação e uma política de privacidade e proteção de dados.

4 - Há política de segurança da informação com base nas ISOs 27001 e 27002 e uma política de privacidade e proteção de dados baseada na ISO 27701

5 - Há política de segurança da informação com base nas ISOs 27001 e 27002 e uma política de privacidade e proteção de dados baseada na ISO 27701. Os controles são auditados periodicamente.

46. 6.3 - Manter medidas técnicas de segurança e proteção de dados *

1 - Não há medidas técnicas de segurança implementadas

2 - Há algumas medidas técnicas de segurança implementadas, tais como firewall e antimalware nas estações e servidores

3 - As principais medidas técnicas de segurança estão implementadas, tais como firewall, antimalware, IPS, DLP, SIEM e Criptografia nas estações.

4 - As principais medidas técnicas de segurança estão implementadas, tais como firewall, antimalware, IPS, DLP, SIEM e Criptografia nas estações. As atualizações de assinaturas ocorrem automaticamente.

5 - As principais medidas técnicas de segurança estão implementadas, tais como firewall, antimalware, IPS, DLP, SIEM e Criptografia nas estações. As atualizações de

assinaturas ocorrem automaticamente. Há auditorias periódicas para aferir a efetividade dos controles.

47. 6.4 - Manter medidas para criptografar dados pessoais em repouso e em movimento *

- [ ] 1 - Não há medidas técnicas de criptografia implementadas
- [ ] 2 - Há medidas técnicas de criptografia implementadas parcialmente
- [ ] 3 - Há medidas técnicas de criptografia implementadas para proteção de dados em repouso e movimento
- [ ] 4 - Há medidas técnicas de criptografia implementadas para proteção de dados em repouso e movimento. Há retenção de logs de acessos ou tentativas de acesso a arquivos criptografados.
- [ ] 5 - Há medidas técnicas de criptografia implementadas para proteção de dados em repouso e movimento. Há retenção de logs de acessos ou tentativas de acesso a arquivos criptografados. São enviados alertas automáticos em caso de incidentes e violações de acesso.

48. 6.5 - Manter procedimentos para restringir o acesso a dados pessoais (por exemplo, acesso baseado em função, segregação de funções) *

- [ ] 1 - Não há matriz de segregação de funções
- [ ] 2 - Há matriz de segregação de funções, parcial. Com a definição de usuários e perfis de alguns sistemas.
- [ ] 3 - Há matriz de segregação de funções com a definição de usuários e perfis de acesso em cada sistema.
- [ ] 4 - Há matriz de segregação de funções com a definição de usuários e perfis de acesso em cada sistema. A matriz é revisada periodicamente.
- [ ] 5 - Há matriz de segregação de funções com a definição de usuários e perfis de acesso em cada sistema. A matriz é revisada periodicamente. São realizadas auditorias para conferência dos acessos face a matriz.

49. 6.6 - Integrar a privacidade e proteção de dados a uma política de segurança corporativa (proteção de instalações físicas e ativos físicos) *

1 - Não há medidas técnicas de segurança física implementadas

2 - Há algumas medidas técnicas de segurança física implementadas tais como CFTV e Catracas

3 - As principais medidas técnicas de segurança física estão implementadas, tais como CFTV, Catracas, Biometria para Datacenter.

4 - As principais medidas técnicas de segurança física estão implementadas, tais como CFTV, Catracas, Biometria para Datacenter. Há registro dos logs e os ativos são monitorados por sistema de CMDB.

5 - As principais medidas técnicas de segurança física estão implementadas, tais como CFTV, Catracas, Biometria para Datacenter. Há registro dos logs e os ativos são monitorados por sistema de CMDB. Os controles são auditados periodicamente.

50. 6.7 - Manter plano de continuidade de negócios (PCN) *

1 - Não há PCN

2 - Há PCN, mas não são executados testes periódicos e nem atualizações

3 - Há PCN, são executados testes e atualizações periódicas

4 - Há PCN baseado na ISO 22301, são executados testes e atualizações periódicas

5 - Há PCN baseado na ISO 22301, são executados testes e atualizações periódicas. Há mecanismo de recuperação automatizada em caso de desastres.

51. 6.8 - Manter uma estratégia de prevenção de perda de dados pessoais *

1 - Não há backup dos servidores que armazenam dados pessoais

2 - Há backup não periódico dos servidores que armazenam dados pessoais

3 - Há backup periódico dos servidores que armazenam dados pessoais

4 - Há backup periódico dos servidores que armazenam dados pessoais com testes de recuperação esporádicos.

5 - Há backup periódico dos servidores que armazenam dados pessoais com testes de recuperação esporádicos. Dados de backup são armazenados em local geograficamente distante (mínimo 500m) da produção.

52. 6.9 - Conduzir testes regulares quanto ao desempenho de segurança de dados *

- [ ] 1 - Não são realizados testes de intrusão
- [ ] 2 - São realizados teste de intrusão não periódicos
- [ ] 3 - São realizados teste de intrusão periódicos WAN to LAN Black Box
- [ ] 4 - São realizados teste de intrusão periódicos WAN to LAN e LAN to LAN Box Black
- [ ] 5 - São realizados teste de intrusão periódicos WAN to LAN e LAN to LAN WhiteBox

53. 6.10 - Manter uma certificação de segurança *

- [ ] 1 - Não há certificação de segurança
- [ ] 2 - Há certificação de segurança expirada
- [ ] 3 - Há certificação de segurança vigente
- [ ] 4 - Há certificação de segurança vigente e há métricas de aferição de conformidade com a norma base
- [ ] 5 - Há certificação de segurança vigente e há métricas de aferição de conformidade com a norma base. São realizadas auditorias periódicas.

7. Gerenciamento de Riscos de Terceiros

54. 7.1 - Manter política de privacidade e proteção de dados para terceiros (por exemplo, clientes, fornecedores, processadores, afiliados) *

- [ ] 1 - Não há políticas relacionadas documentadas
- [ ] 2 - Há políticas relacionadas parcialmente documentadas
- [ ] 3 - Há políticas relacionadas documentadas
- [ ] 4 - Há políticas relacionadas documentadas e são revisadas periodicamente
- [ ] 5 - Há políticas relacionadas documentadas, estas são revisadas e auditadas periodicamente

55. 7.2 - Manter procedimentos para executar contratos ou acordos com todos os processadores *

- [ ] 1 - Não há procedimentos relacionados documentadas
- [ ] 2 - Há procedimentos relacionados parcialmente documentados
- [ ] 3 - Há procedimentos relacionados documentados
- [ ] 4 - Há procedimentos relacionados documentados e são revisados periodicamente
- [ ] 5 - Há procedimentos relacionados documentados, estes são revisados e auditados periodicamente

56. 7.3 - Realizar a devida diligência em torno da postura de privacidade e proteção de dados, segurança de dados de fornecedores / operadores em potencial *

- [ ] 1 - Não é feita diligência em torno de operadores
- [ ] 2 - É feita diligência parcial em torno de operadores através de contrato.
- [ ] 3 - É feita diligência em torno de operadores através de contratos e políticas de privacidade e proteção de dados
- [ ] 4 - É feita diligência em torno de operadores em potencial. Este precisam apresentar relatórios periódicos que comprovem a eficiência dos controles de proteção e privacidade.
- [ ] 5 - É feita diligência em torno de operadores em potencial. Este precisam apresentar relatórios periódicos que comprovem a eficiência dos controles de proteção e privacidade. São realizadas auditorias periodicamente.

57. 7.4 - Realizar due diligence em fontes de dados de terceiros *

- [ ] 1 - Não é feita diligência em torno de fontes de dados de terceiros
- [ ] 2 - É feita diligência parcial em torno de fontes de dados de terceiros
- [ ] 3 - É feita diligência em torno de fontes de dados de terceiros
- [ ] 4 - É feita diligência em torno de fontes de dados de terceiros. Este precisam apresentar relatórios periódicos que comprovem a eficiência dos controles de proteção e privacidade.

5 - É feita diligência em torno de fontes de dados de terceiros. Este precisam apresentar relatórios periódicos que comprovem a eficiência dos controles de proteção e privacidade. São realizadas auditorias periodicamente.

58. 7.5 - Manter um processo de avaliação de risco de privacidade e proteção de dados do fornecedor *

- 1 - Não há procedimentos relacionados documentadas
- 2 - Há procedimentos relacionados parcialmente documentados
- 3 - Há procedimentos relacionados documentados
- 4 - Há procedimentos relacionados documentados e são revisados periodicamente
- 5 - Há procedimentos relacionados documentados, estes são revisados e auditados periodicamente

59. 7.6 - Manter uma política que rege o uso de serviços em nuvem *

- 1 - Não há políticas relacionadas documentadas
- 2 - Há políticas relacionadas parcialmente documentadas
- 3 - Há políticas relacionadas documentadas
- 4 - Há políticas relacionadas documentadas e são revisadas periodicamente
- 5 - Há políticas relacionadas documentadas, estas são revisadas e auditadas periodicamente

60. 7.7 - Manter procedimentos para lidar com casos de não conformidade com contratos e acordos *

- [ ] 1 - Não há políticas relacionadas documentadas
- [ ] 2 - Há políticas relacionadas parcialmente documentadas
- [ ] 3 - Há políticas relacionadas documentadas
- [ ] 4 - Há políticas relacionadas documentadas e são revisadas periodicamente
- [ ] 5 - Há políticas relacionadas documentadas, estas são revisadas e auditadas periodicamente

61. 7.8 - Analisar os contratos de longo prazo para verificar riscos de privacidade de dados novos ou em evolução *

- [ ] 1 - Não há análise de contratos
- [ ] 2 - Há análise de alguns contratos sob não periódica
- [ ] 3 - Há análise de todos os contratos não periódica
- [ ] 4 - Há análise de todos os contratos periodicamente para manter aderência a legislação vigente.
- [ ] 5 - Há análise de todos os contratos periodicamente para manter aderência a legislação vigente. Há mecanismo implantado para análise de impacto automático em contratos.

8. Plano de Comunicação

62. 8.1 - Manter um aviso de privacidade e proteção de dados que detalha as práticas de tratamento de dados pessoais da organização *

- [ ] 1 - Não há qualquer aviso
- [ ] 2 - Há aviso informal
- [ ] 3 - Há aviso de privacidade e proteção de dados que detalha as práticas de tratamento de dados pessoais da organização
- [ ] 4 - Há aviso de privacidade e proteção de dados que detalha as práticas de tratamento de dados pessoais da organização. O mesmo é revisado periodicamente.
- [ ] 5 - Há aviso de privacidade e proteção de dados que detalha as práticas de tratamento de dados pessoais da organização. O mesmo é revisado periodicamente e adequado de acordo com as melhores práticas.

63. 8.2 - Fornecer aviso de privacidade e proteção de dados em todos os pontos em que os dados pessoais são coletados *

- [ ] 1 - Não há qualquer aviso
- [ ] 2 - Há aviso informal
- [ ] 3 - Há aviso de privacidade e proteção de dados que detalha as práticas de tratamento de dados pessoais da organização
- [ ] 4 - Há aviso de privacidade e proteção de dados que detalha as práticas de tratamento de dados pessoais da organização. O mesmo é revisado periodicamente.
- [ ] 5 - Há aviso de privacidade e proteção de dados que detalha as práticas de tratamento de dados pessoais da organização. O mesmo é revisado periodicamente e adequado de acordo com as melhores práticas.

64. 8.3 - Fornecer aviso nas comunicações de marketing (por exemplo, e-mails, folhetos, ofertas) *

- [ ] 1 - Não há qualquer aviso
- [ ] 2 - Há aviso informal
- [ ] 3 - Há aviso de privacidade e proteção de dados que detalha as práticas de tratamento de dados pessoais da organização
- [ ] 4 - Há aviso de privacidade e proteção de dados que detalha as práticas de tratamento de dados pessoais da organização. O mesmo é revisado periodicamente.
- [ ] 5 - Há aviso de privacidade e proteção de dados que detalha as práticas de tratamento de dados pessoais da organização. O mesmo é revisado periodicamente e adequado de acordo com as melhores práticas.

65. 8.4 - Fornecer aviso em contratos e termos *

- [ ] 1 - Não há qualquer aviso
- [ ] 2 - Há aviso informal
- [ ] 3 - Há aviso de privacidade e proteção de dados que detalha as práticas de tratamento de dados pessoais da organização
- [ ] 4 - Há aviso de privacidade e proteção de dados que detalha as práticas de tratamento de dados pessoais da organização. O mesmo é revisado periodicamente.
- [ ] 5 - Há aviso de privacidade e proteção de dados que detalha as práticas de tratamento de dados pessoais da organização. O mesmo é revisado periodicamente e adequado de acordo com as melhores práticas.

66. 8.5 - Manter scripts para uso dos funcionários para explicar ou fornecer o aviso de privacidade e proteção de dados *

- [ ] 1 - Não há qualquer script
- [ ] 2 - Há script informal
- [ ] 3 - Há scripts para uso dos funcionários para explicar ou fornecer o aviso de privacidade e proteção de dados
- [ ] 4 - Há scripts para uso dos funcionários para explicar ou fornecer o aviso de privacidade e proteção de dados. Os mesmos são revisados periodicamente.
- [ ] 5 - Há scripts para uso dos funcionários para explicar ou fornecer o aviso de privacidade e proteção de dados. Os mesmos são revisados periodicamente e adequado segundo as melhores práticas.

67. 8.6 - Manter um selo de privacidade e proteção de dados ou marca de confiança para aumentar a confiança do cliente *

- [ ] 1 - Não há qualquer
- [ ] selo 2 - Há um selo
- [ ] expirado.
- [ ] 3 - Há um selo vigente.
- [ ] 4 - Há um selo vigente e um processo de renovação periódico.
- [ ] 5 - Há um selo vigente e um processo de renovação periódico. Com auditorias regulares

9. Resposta aos Titulares dos Dados

68. 9.1 - Manter procedimentos para tratar de reclamações *

- [ ] 1 - Não há procedimentos relacionados documentados
- [ ] 2 - Há procedimentos relacionados parcialmente documentados
- [ ] 3 - Há procedimentos relacionados documentados
- [ ] 4 - Há procedimentos relacionados documentados e são revisados periodicamente
- [ ] 5 - Há procedimentos relacionados documentados, estes são revisados e auditados periodicamente

69. 9.2 - Manter procedimentos para responder a solicitações de acesso a dados pessoais *

- [ ] 1 - Não há procedimentos relacionados documentados
- [ ] 2 - Há procedimentos relacionados parcialmente documentados
- [ ] 3 - Há procedimentos relacionados documentados
- [ ] 4 - Há procedimentos relacionados documentados e são revisados periodicamente
- [ ] 5 - Há procedimentos relacionados documentados, estes são revisados e auditados periodicamente

70. 9.3 - Manter procedimentos para responder a solicitações e / ou fornecer um mecanismo para os indivíduos atualizarem ou corrigirem seus dados pessoais *

- [ ] 1 - Não há procedimentos relacionados documentados
- [ ] 2 - Há procedimentos relacionados parcialmente documentados
- [ ] 3 - Há procedimentos relacionados documentados
- [ ] 4 - Há procedimentos relacionados documentados e são revisados periodicamente
- [ ] 5 - Há procedimentos relacionados documentados, estes são revisados e auditados periodicamente

71. 9.4 - Manter procedimentos para responder a pedidos de exclusão, restrição ou oposição ao processamento *

- [ ] 1 - Não há procedimentos relacionados documentados
- [ ] 2 - Há procedimentos relacionados parcialmente documentados
- [ ] 3 - Há procedimentos relacionados documentados
- [ ] 4 - Há procedimentos relacionados documentados e são revisados periodicamente
- [ ] 5 - Há procedimentos relacionados documentados, estes são revisados e auditados periodicamente

72. 9.5 - Manter procedimentos para responder a pedidos de informações *

- [ ] 1 - Não há procedimentos relacionados documentados
- [ ] 2 - Há procedimentos relacionados parcialmente documentados
- [ ] 3 - Há procedimentos relacionados documentados
- [ ] 4 - Há procedimentos relacionados documentados e são revisados periodicamente
- [ ] 5 - Há procedimentos relacionados documentados, estes são revisados e auditados periodicamente

73. 9.6 - Manter procedimentos para responder a solicitações de portabilidade de dados *

- [ ] 1 - Não há procedimentos relacionados documentados
- [ ] 2 - Há procedimentos relacionados parcialmente documentados
- [ ] 3 - Há procedimentos relacionados documentados
- [ ] 4 - Há procedimentos relacionados documentados e são revisados periodicamente
- [ ] 5 - Há procedimentos relacionados documentados, estes são revisados e auditados periodicamente

74. 9.7 - Manter procedimentos para responder a pedidos a serem esquecidos ou para apagar dados *

- [ ] 1 - Não há procedimentos relacionados documentados
- [ ] 2 - Há procedimentos relacionados parcialmente documentados
- [ ] 3 - Há procedimentos relacionados documentados
- [ ] 4 - Há procedimentos relacionados documentados e são revisados periodicamente
- [ ] 5 - Há procedimentos relacionados documentados, estes são revisados e auditados periodicamente

75. 9.8 - Manter perguntas frequentes (FAQ) para responder a perguntas de indivíduos *

- [ ] 1 - Não há procedimentos relacionados documentados
- [ ] 2 - Há procedimentos relacionados parcialmente documentados
- [ ] 3 - Há procedimentos relacionados documentados
- [ ] 4 - Há procedimentos relacionados documentados e são revisados periodicamente
- [ ] 5 - Há procedimentos relacionados documentados, estes são revisados e auditados periodicamente

76. 9.9 - Investigar as causas raízes das reclamações de proteção de dados *

- [ ] 1 - Não há procedimentos relacionados documentados
- [ ] 2 - Há procedimentos relacionados parcialmente documentados
- [ ] 3 - Há procedimentos relacionados documentados
- [ ] 4 - Há procedimentos relacionados documentados e são revisados periodicamente
- [ ] 5 - Há procedimentos relacionados documentados, estes são revisados e auditados periodicamente

77. 9.10 - Monitorar e reportar métricas para reclamações de privacidade e proteção de dados (Tempo de resposta, quantidade, causa raiz) *

- [ ] 1 - Não há procedimentos relacionados documentados
- [ ] 2 - Há procedimentos relacionados parcialmente documentados
- [ ] 3 - Há procedimentos relacionados documentados
- [ ] 4 - Há procedimentos relacionados documentados e são revisados periodicamente
- [ ] 5 - Há procedimentos relacionados documentados, estes são revisados e auditados periodicamente

10. Monitoramento de Novas Práticas Operacionais

78. 10.1 - Manter procedimento de verificação de identidade dos titulares *

- [ ] 1 - Não há procedimentos relacionados documentados
- [ ] 2 - Há procedimentos relacionados parcialmente documentados
- [ ] 3 - Há procedimentos relacionados documentados
- [ ] 4 - Há procedimentos relacionados documentados e são revisados periodicamente
- [ ] 5 - Há procedimentos relacionados documentados, estes são revisados e auditados periodicamente

79. 10.2 - Integrar o Privacy by Design no desenvolvimento de sistemas e produtos da organização *

- [ ] 1 - Aspectos de privacidade não são considerados no desenvolvimento de sistemas e produtos da organização
- [ ] 2 - Aspectos de privacidade não são requisitos chave de sistemas e produtos da organização, mas são considerados
- [ ] 3 - Aspectos de privacidade são requisitos chave no desenvolvimento de sistema se produtos da organização
- [ ]

4 - Aspectos de privacidade são requisitos chave no desenvolvimento de sistema se produtos da organização. Ocorrem revisões internas periódicas dos sistemas em busca de falhas que possam comprometer a privacidade.

5 - Aspectos de privacidade são requisitos chave no desenvolvimento de sistemas e produtos da organização. Ocorrem revisões internas e externas periódicas dos sistemas em busca de falhas que possam comprometer a privacidade.

80. 10.3 - Manter diretrizes e modelos de DPIA (Data Protection Impact Assessment) em conformidade com à LGPD *

1 - Não há DPIA

2 - Há DPIA incompletos

3 - Há DPIA de todos os processos que tratam dados pessoais na organização. Os DPIA de dados sensíveis são relatados para os reguladores

4 - Há DPIA de todos os processos que tratam dados pessoais na organização. Os DPIA de dados sensíveis são relatados para os reguladores. Os documentos são revisados periodicamente junto as áreas de negócio.

5 - Há DPIA de todos os processos que tratam dados pessoais na organização. Os DPIA de dados sensíveis são relatados para os reguladores. Os documentos são revisados periodicamente junto as áreas de negócio. Há um plano de ação que é objeto de auditoria periódica.

11. Gerenciamento de violação de privacidade de dados

81. 11.1 - Manter um plano de resposta a incidentes / violações da privacidade de dados *

1 - Não há procedimentos relacionados documentados

2 - Há procedimentos relacionados parcialmente documentados

3 - Há procedimentos relacionados documentados

4 - Há procedimentos relacionados documentados e são revisados periodicamente

5 - Há procedimentos relacionados documentados, estes são revisados e auditados periodicamente

82. 11.2 - Manter um protocolo de notificação de violação (para as pessoas afetadas) e relatórios (para reguladores, agências de crédito, órgãos policiais) *

- [ ] 1 - Não há procedimentos relacionados documentados
- [ ] 2 - Há procedimentos relacionados parcialmente documentados
- [ ] 3 - Há procedimentos relacionados documentados
- [ ] 4 - Há procedimentos relacionados documentados e são revisados periodicamente
- [ ] 5 - Há procedimentos relacionados documentados, estes são revisados e auditados periodicamente

83. 11.3 - Manter o registro quanto o rastreamento de incidentes / violações de privacidade e proteção de dados *

- [ ] 1 - Não há procedimentos relacionados documentados
- [ ] 2 - Há procedimentos relacionados parcialmente documentados
- [ ] 3 - Há procedimentos relacionados documentados
- [ ] 4 - Há procedimentos relacionados documentados e são revisados periodicamente
- [ ] 5 - Há procedimentos relacionados documentados, estes são revisados e auditados periodicamente

84. 11.4 - Monitorar e reportar as métricas de incidentes / violações de privacidade e proteção de dados (natureza da violação, risco, causa raiz) *

- [ ] 1 - Não há procedimentos relacionados documentados
- [ ] 2 - Há procedimentos relacionados parcialmente documentados
- [ ] 3 - Há procedimentos relacionados documentados
- [ ] 4 - Há procedimentos relacionados documentados e são revisados periodicamente
- [ ] 5 - Há procedimentos relacionados documentados, estes são revisados e auditados periodicamente

85. 11.5 - Realizar testes periódicos do plano de violação / incidente de privacidade e proteção de dados *

- [ ] 1 - Não são realizados testes periódicos do plano de violação / incidente de privacidade e proteção de dados
- [ ] 2 - São realizados testes não periódicos do plano de violação / incidente de privacidade e proteção de dados
- [ ] 3 - São realizados testes periódicos do plano de violação / incidente de privacidade e proteção de dados
- [ ] 4 - São realizados testes periódicos do plano de violação / incidente de privacidade e proteção de dados. O plano é constantemente aprimorado a partir do resultado dos testes
- [ ] 5 - São realizados testes periódicos do plano de violação / incidente de privacidade e proteção de dados. O plano é constantemente aprimorado a partir do resultado dos testes. São realizadas auditorias do plano.

86. 11.6 - Envolver uma equipe de investigação forense *

- [ ] 1 - Não há procedimentos relacionados documentados
- [ ] 2 - Há procedimentos relacionados parcialmente documentados
- [ ] 3 - Há procedimentos relacionados documentados
- [ ] 4 - Há procedimentos relacionados documentados e são revisados periodicamente
- [ ] 5 - Há procedimentos relacionados documentados, estes são revisados e auditados periodicamente

87. 11.7 - Obter cobertura de seguro de violação de privacidade e proteção de dados *

- [ ] 1 - Não há cobertura de seguro de violação de privacidade e proteção de dados
- [ ] 2 - Há cobertura parcial de seguro de violação de privacidade e proteção de dados
- [ ] 3 - Há cobertura completa de seguro de violação de privacidade e proteção de dados
- [ ] 4 - Há cobertura completa de seguro de violação de privacidade e proteção dedados. São monitorados indicadores de segurança pela seguradora.
- [ ] 5 - Há cobertura completa de seguro de violação de privacidade e proteção dedados. São monitorados indicadores de segurança pela seguradora e realizadas auditorias periódicas.

12. Tratamento de Dados

88. 12.1 - Conduzir auditorias internas do programa de privacidade e proteção de dados *

- [ ] 1 - Não são realizadas auditorias internas
- [ ] 2 - São realizadas auditorias internas não periódicas.
- [ ] 3 - São realizadas auditorias internas periódicas.
- [ ] 4 - São realizadas auditorias internas periódicas. O resultado é utilizado para elaboração de um plano de ação.
- [ ] 5 - São realizadas auditorias internas periódicas. O resultado é utilizado para elaboração de um plano de ação que é monitorado e apresentado para a diretoria.

89. 12.2 - Conduzir avaliações com base em eventos externos, como reclamações / violações, entre outros *

1 - Não há avaliações de eventos externos

- [ ] 2 - As avaliações de eventos externos ocorrem de forma ad-hoc
- [ ] 3 - Todos os eventos externos são avaliados
- [ ] 4 - Todos os eventos externos são avaliados e há indicadores para monitoramento da eficiência do processo.
- [ ] 5 - Todos os eventos externos são avaliados e há indicadores para monitoramento da eficiência do processo. São realizadas auditorias periódicas.

90. 12.3 - Envolver a auditoria externas para avaliações independentes *

- [ ] 1 - Não são realizadas auditorias externas
- [ ] 2 - São realizadas auditorias externas não periódicas.
- [ ] 3 - São realizadas auditorias externas periódicas.
- [ ] 4 - São realizadas auditorias externas periódicas. O resultado é utilizado para elaboração de um plano de ação.
- [ ] 5 - São realizadas auditorias externas periódicas. O resultado é utilizado para elaboração de um plano de ação que é monitorado e apresentado para a diretoria.

91. 12.4 - Monitorar e reportar as métricas de privacidade e proteção de dados *

- [ ] 1 - Não há métricas relacionadas documentadas
- [ ] 2 - Há métricas relacionadas parcialmente documentadas
- [ ] 3 - Há métricas relevantes e relacionadas documentadas
- [ ] 4 - Há métricas relevantes e relacionadas documentadas. Indicadores são monitorados constantemente
- [ ] 5 - Há métricas relevantes e relacionadas documentadas. Indicadores são monitorados constantemente. São estabelecidas metas para evolução contínua.

92. 12.5 - Manter a documentação como evidência a fim de demonstrar conformidade e / ou prestação de conta *

- ◯ 1 - Não há documentação relacionada
- ◯ 2 - Há documentação parcial relacionada
- ◯ 3 - Há documentação relacionada
- ◯ 4 - Há documentação relacionada, a revisão é periódica
- ◯ 5 - Há documentação relacionada, a revisão e auditorias são periódicas.

Obrigado por ter preenchido a pesquisa, falta pouco para o término. Como o modelo de maturidade de segurança da informação é um modelo aberto a comunidade fique Feedback à vontade para contribuir com críticas, sugestões e elogios.

93. O que você achou do modelo de maturidade de segurança da informação proposto?

_____

_____

_____

_____

_____

94. Pontos Fortes do Modelo

Marque todas que se aplicam.

- ☐ Abrangente
- ☐ Detalhado
- ☐ Objetivo
- Outro: ☐ _____

95. Pontos Fracos do Modelo

Marque todas que se aplicam.

- [ ] Superficial
- [ ] Extenso
- [ ] Incompleto

Outro: [ ] _____

Apêndice B – Versão atual do Modelo de maturidade em segurança da informação brasileiro (MMSI.br)

Apêndice B – Versão atual do questionário para avaliação de maturidade em segurança da informação brasileiro (MMSI.br)

Pesquisa MMSI.br

Esta pesquisa tem como objetivo aferir o nível de aderência das organizações brasileiras à Lei Geral de Proteção de Dados (LGPD), a partir do modelo de maturidade de segurança da informação brasileiro (MMSI.br). Neste são avaliados 80 processos organizados em 12 domínios com foco em privacidade e proteção de dados.

A maturidade de cada processo é classificada de 1 a 5, onde 1 é o nível inicial e 5 é o otimizado. A maturidade de cada domínio é calculada a partir da média da maturidade de seus processos. Os dados coletados serão utilizados para gerar uma análise gráfica similar a figura abaixo a ser disponibilizada para os participantes através do email de contato informado.

As estatísticas globais da pesquisa poderão ser publicadas de forma anônima na dissertação de mestrado que está sendo desenvolvida em torno do modelo de maturidade aqui apresentado.

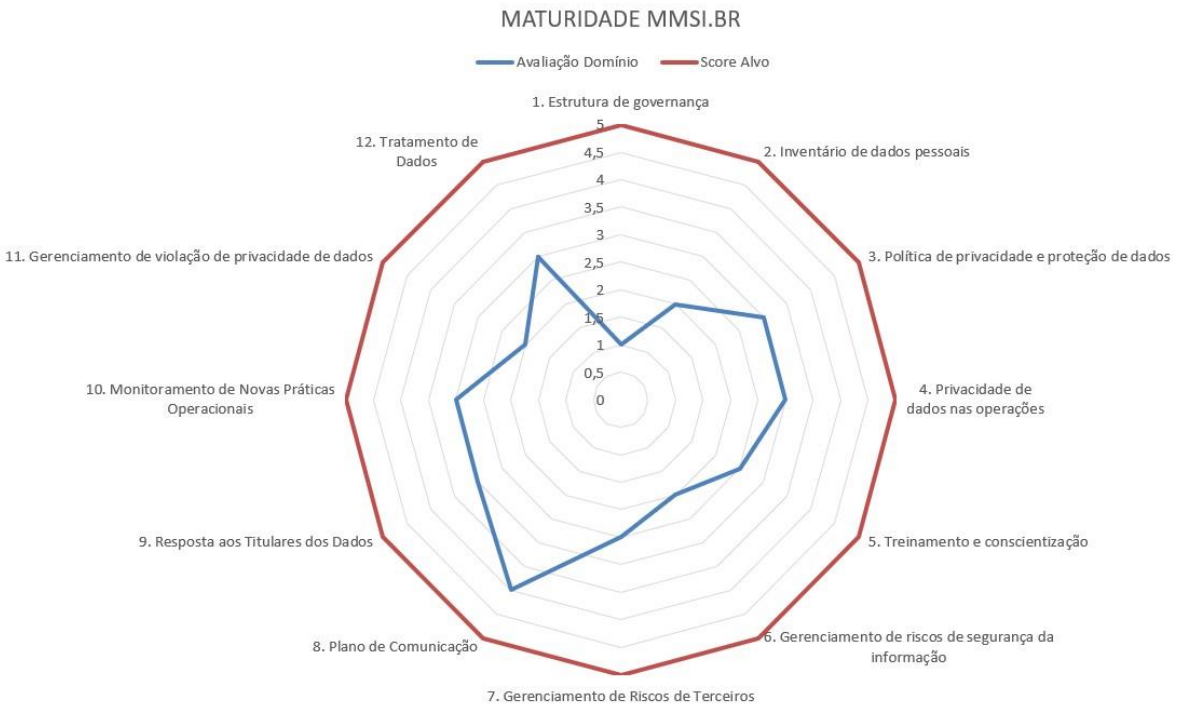
Em caso de dúvidas ou sugestões entre em contato através do email brunonbpaixao@gmail.com.

Obrigado

Bruno Paixão
https://www.linkedin.com/in/brunonbpaixao/
*Obrigatório

1. Endereço de e-mail *

Gráfico de Radar - MMSI.br



2. Nome e Sobrenome

Minimização (Art. 6, III - LGPD)

3. UF *

4. Organização

5. Segmento Empresarial *

- [ ] Comércio e Varejo
- [ ] Serviços
- [ ] Logística
- [ ] Educação
- [ ] Saúde e Hospitalar
- [ ] Tecnologia
- [ ] Construção e Engenharia
- [ ] Financeiro, Seguradoras e Corretoras

Outros

6. Número de Colaboradores *

- [ ] Até 5 Colaboradores
- [ ] De 6 A 99 Colaboradores
- [ ] De 100 a 499 Colaboradores
- [ ] De 500 A 999 Colaboradores
- [ ] Mais de 1000 Colaboradores

1. Estrutura de governança

7. 1.1 - Atribuir a responsabilidade pela privacidade e proteção dos dados a um indivíduo (encarregado de dados) *

- ( ) 1 - Não há responsável atribuído
- ( ) 2 - Responsável definido, mas não nomeado formalmente
- ( ) 3 - Responsável definido e nomeado formalmente
- ( ) 4 - Responsável definido, nomeado formalmente, reporta diretamente a alta direção sem acumular cargo
- ( ) 5 - Responsável definido, nomeado formalmente, reporta diretamente a alta direção sem acumular cargo. O profissional é certificado para atuar como encarregado de dados

8. 1.2 - Envolver a alta direção em privacidade e proteção de dados e atribuir responsabilidade pela privacidade e proteção dos dados em toda a organização *

- ( ) 1 - Não há comitê de privacidade e proteção de dados
- ( ) 2 - Há comitê de privacidade e proteção de dados sem reuniões regulares
- ( ) 3 - Há comitê de privacidade e proteção de dados com reuniões regulares
- ( ) 4 - Há comitê de privacidade e proteção de dados com reuniões regulares, com a participação de membros das áreas de TI, Segurança, Jurídico e DPO
- ( ) 5 - Há comitê de privacidade e proteção de dados com reuniões regulares, com a

participação de membros das áreas de TI, Segurança, Jurídico, DPO (Líder) e Diretoria (Sponsor).

9. 1.3 - Conduzir comunicação regular junto às partes interessadas internas da organização com status do gerenciamento de privacidade e proteção de dados *

- ( ) 1 - Não há comunicação e nem um plano definido.
- ( ) 2 - Comunicação ocorre de forma esporádica, mas sem um plano definido.
- ( ) 3 - Comunicação ocorre periodicamente e tem um plano definido.
- ( ) 4 - Comunicação ocorre periodicamente e tem um plano definido. São utilizados múltiplos canais para atingir as partes interessadas
- ( )

5 - Há um plano de comunicação com periodicidade e responsável definido. São utilizados múltiplos canais para atingir as partes interessadas. A efetividade dos canais é medida através de indicadores

10. 1.4 - Reportar às partes interessadas externas da organização o status do gerenciamento de privacidade (por exemplo, órgãos reguladores, terceiros, clientes) *

- 1 - Não há comunicação e nem um plano definido.
- 2 - Comunicação ocorre de forma esporádica, mas sem um plano definido.
- 3 - Comunicação ocorre periodicamente e tem um plano definido.
- 4 - Comunicação ocorre periodicamente e tem um plano definido. São utilizados múltiplos canais para atingir as partes interessadas
- 5 - Há um plano de comunicação com periodicidade e responsável definido. São utilizados múltiplos canais para atingir as partes interessadas. A efetividade dos canais é medida através de indicadores

11. 1.5 - Realizar uma avaliação de risco de privacidade e proteção de dados da empresa (DPIA) *

- 1 - Os processos que tratam dados pessoais não estão mapeados
- 2 - Os processos que tratam dados pessoais estão mapeados parcialmente
- 3 - Os processos que tratam dados pessoais estão mapeados e há um DPIA
- 4 - Os processos que tratam dados pessoais estão mapeados, há um DPIA e os GAPs estão classificados pelo grau do risco
- 5 - Os processos que tratam dados pessoais estão mapeados, há um DPIA, os GAPs estão classificados pelo grau do risco e o gestão das atividades é feita através plano de ação.

12. 1.6 - Integrar a privacidade de dados nas avaliações e relatórios de riscos corporativos *

- [ ] 1 - Riscos relativos à privacidade de dados não estão mapeados 2 - Riscos relativos à privacidade de dados estão parcialmente mapeados
- [ ] 3 - Riscos relativos à privacidade de dados estão mapeados.
- [ ] 4 - Riscos relativos à privacidade de dados estão mapeados, tem responsáveis e estão associados a um plano de ação.
- [ ] 5 - Riscos relativos à privacidade de dados estão mapeados, tem responsáveis, estão associados a um plano de ação e são auditados.

13. 1.7 - Manter uma estratégia e um programa de proteção e privacidade de dados (P&PD) *

- [ ] 1 - Não há programa ou estratégia para a assegurar a privacidade e proteção de dados.
- [ ] 2 - Ações para assegurar a privacidade e proteção de dados são tomadas, mas não há um programa definido.
- [ ] 3 - Ações para assegurar a privacidade e proteção de dados são tomadas de acordo com um programa definido.
- [ ] 4 - Ações para assegurar a privacidade e proteção de dados são tomadas de acordo com um programa definido. Há indicadores para medir a efetividade das ações.
- [ ] 5 - Ações para assegurar a privacidade e proteção de dados são tomadas de acordo com um programa definido. Há indicadores para medir a efetividade das ações. São realizadas auditorias periódicas.

14. 1.8 - Exigir que os funcionários reconheçam e concordem em aderir às políticas de privacidade e proteção de dados *

1 - Não há política de privacidade e proteção de dados

2 - Há política de privacidade e proteção de dados, mas não é reconhecida e assinada pelos funcionários em sua totalidade

- [ ]
- [ ]

- [ ] 3 - Há política de privacidade e proteção de dados, esta é reconhecida e assinada pelos funcionários em sua totalidade
- [ ] 4 - Há política de privacidade e proteção de dados, esta é reconhecida e assinada pelos funcionários em sua totalidade. O documento é revisado periodicamente.
- [ ] 5 - Há política de privacidade e proteção de dados, esta é reconhecida e assinada pelos funcionários em sua totalidade. O documento é revisado periodicamente e as alterações são informadas aos funcionários.

2. Inventário de dados pessoais

15. 2.1 - Manter um inventário de dados pessoais que são tratados *

- [ ] 1 - Não há um inventário dos dados pessoais tratados
- [ ] 2 - Há um inventário parcial dos dados pessoais tratados
- [ ] 3 - Há um inventário completo dos dados pessoais tratados em formato 5W2H ou sistema
- [ ] 4 - Há um inventário completo dos dados pessoais tratados em formato 5W2H ou sistema. Isso é revisado periodicamente e mantido descentralizadamente
- [ ] 5 - Há um inventário completo dos dados pessoais tratados em formato 5W2H ou sistema. Isso é revisado periodicamente e mantido centralizadamente.

16. 2.2 - Classificar os dados pessoais tratados *

- [ ] 1 - Não há política de classificação de dados
- [ ] 2 - Há política de classificação de dados de dados, mas dados são classificados parcialmente
- [ ] 3 - Há política de classificação de dados de dados e estão são classificados manualmente
- [ ] 4 - Há política de classificação de dados de dados e estes são classificados automaticamente
- [ ]

5 - Há política de classificação de dados de dados e estes são classificados automaticamente. Há monitoração de dados através de solução de Data Loss Prevention (DLP).

17. 2.3 - Obter aprovação dos reguladores e/ou autoridades para processamento de dados e registrar bancos de dados onde este é necessário para aprovação prévia *

- [ ] 0 - Não se aplica.
- [ ] 1 - Dados sensíveis não estão mapeados e são tratados sem aprovação das autoridades
- [ ] 2 - Dados sensíveis estão parcialmente mapeados e são tratados sem aprovação das autoridades
- [ ] 3 - Dados sensíveis estão mapeados e são tratados com aprovação das autoridades
- [ ] 4 - Dados sensíveis estão mapeados e são tratados com aprovação das autoridades. São utilizados recursos de mascaramento e pseudo anonimização
- [ ] 5 - Dados sensíveis estão mapeados e são tratados com aprovação das autoridades. São utilizados recursos de mascaramento e anonimização.

18. 2.4 - Manter registros do mecanismo de transferência usado para fluxos de dados transfronteiriços e aprovações de órgãos reguladores *

- [ ] 0 - Não se aplica.
- [ ] 1 - Dados pessoais são transferidos internacionalmente, mas sem adoção de mecanismo de transferências e aprovação das autoridades
- [ ] 2 - Dados pessoais são transferidos internacionalmente, são adotados parcialmente mecanismos de transferências, tais como RCV e Cláusulas contratuais.
- [ ] 3 - Dados pessoais são transferidos internacionalmente com permissão das autoridades, são adotados mecanismos de transferências, tais como RCV e Cláusulas contratuais.
- [ ] 4 - Dados pessoais são transferidos internacionalmente com permissão das autoridades, são adotados mecanismos de transferências, tais como RCV e Cláusulas contratuais. Bases legais estão definidas para a transferência de dados.
- [ ] 5 - Dados pessoais são transferidos internacionalmente com permissão das autoridades, são adotados mecanismos de transferências, tais como RCV e Cláusulas

contratuais. Bases legais estão definidas para a transferência de dados. Transferências ocorrem via canal criptografado utilizando VPN Site to Site.

3. Política de privacidade e proteção de dados

19. 3.1 - Manter uma política de privacidade e proteção de dados para funcionários contendo as bases legais para o tratamento de dados pessoais *

- [ ] 1 - Não há política de privacidade e proteção de dados para funcionários
- [ ] 2 - Há política de privacidade e proteção de dados para funcionários
- [ ] 3 - Há política de privacidade e proteção de dados para funcionários e estes foram treinados
- [ ] 4 - Há política de privacidade e proteção de dados para funcionários e estes foram treinados. O documento é revisado periodicamente.
- [ ] 5 - Há política de privacidade e proteção de dados para funcionários e estes foram treinados. O documento é revisado periodicamente e são divulgadas alterações.

20. 3.2 - Manter uma política de privacidade e proteção de dados para terceiros (fornecedores e parceiros) contendo as bases legais para o tratamento de dados pessoais *

- [ ] 1 - Não há política de privacidade e proteção de dados para terceiros
- [ ] 2 - Há política de privacidade e proteção de dados para terceiros
- [ ] 3 - Há política de privacidade e proteção de dados para terceiros e estes foram treinados
- [ ] 4 - Há política de privacidade e proteção de dados para terceiros e estes foram treinados. O documento é revisado periodicamente.
- [ ] 5 - Há política de privacidade e proteção de dados para terceiros e estes foram treinados. O documento é revisado periodicamente e divulgado adequadamente na organização.

21. 3.3 - Manter atualizados procedimentos para coleta e uso de dados pessoais e dados sensíveis *

1 - Não há procedimentos documentados

- [ ] 2 - Há procedimentos parcialmente documentados
- [ ] 3 - Todos os procedimentos relacionados estão documentados
- [ ] 4 - Todos os procedimentos relacionados estão documentados e são revisados periodicamente
- [ ] 5 - Todos os procedimentos relacionados estão documentados, são revisados e auditados periodicamente

4. Privacidade de dados nas operações

22. 4.1 - Manter políticas e procedimentos para identificação e manutenção da qualidade dos dados (válidos e atualizados). *

- [ ] 1 - Não há políticas e procedimentos relacionados documentados
- [ ] 2 - Há políticas e procedimentos relacionados parcialmente documentados
- [ ] 3 - Há políticas e procedimentos relacionados documentados
- [ ] 4 - Há políticas e procedimentos relacionados documentados e são revisados periodicamente
- [ ] 5 - Há políticas e procedimentos relacionados documentados, estes são revisados e auditados periodicamente

23. 4.2 - Manter políticas e procedimentos para revisar o tratamento total ou parcialmente por meios automatizados, tais como uso de cookies e mecanismos de rastreamento de clientes *

- [ ] 1 - Não há políticas e procedimentos relacionados documentados
- [ ] 2 - Há políticas e procedimentos relacionados parcialmente documentados
- [ ] 3 - Há políticas e procedimentos relacionados documentados
- [ ] 4 - Há políticas e procedimentos relacionados documentados e são revisados periodicamente
- [ ] 5 - Há políticas e procedimentos relacionados documentados, estes são revisados e auditados periodicamente

24. 4.3 - Manter políticas e procedimentos para obter consentimento válido por parte dos titulares dos dados *

- [ ] 1 - Não há políticas e procedimentos relacionados documentados
- [ ] 2 - Há políticas e procedimentos relacionados parcialmente documentados
- [ ] 3 - Há políticas e procedimentos relacionados documentados
- [ ] 4 - Há políticas e procedimentos relacionados documentados e são revisados periodicamente
- [ ] 5 - Há políticas e procedimentos relacionados documentados, estes são revisados e auditados periodicamente

25. 4.4 - Manter políticas e procedimentos para retenção e destruição segura de dados pessoais *

- [ ] 1 - Não há políticas e procedimentos relacionados documentados
- [ ] 2 - Há políticas e procedimentos relacionados parcialmente documentados
- [ ] 3 - Há políticas e procedimentos relacionados documentados
- [ ] 4 - Há políticas e procedimentos relacionados documentados e são revisados periodicamente
- [ ] 5 - Há políticas e procedimentos relacionados documentados, estes são revisados e auditados periodicamente

26. 4.5 - Integrar privacidade e proteção de dados em práticas de marketing direto com clientes por email e telefone *

- [ ] 1 - Não há políticas e procedimentos relacionados documentados
- [ ] 2 - Há políticas e procedimentos relacionados parcialmente documentados
- [ ] 3 - Há políticas e procedimentos relacionados documentados
- [ ] 4 - Há políticas e procedimentos relacionados documentados e são revisados periodicamente
- [ ] 5 - Há políticas e procedimentos relacionados documentados, estes são revisados e auditados periodicamente

27. 4.6 - Integrar a privacidade e proteção de dados nas práticas de recrutamento, seleção e contratação de colaboradores *

- [ ] 1 - Não há políticas e procedimentos relacionados documentados
- [ ] 2 - Há políticas e procedimentos relacionados parcialmente documentados
- [ ] 3 - Há políticas e procedimentos relacionados documentados
- [ ] 4 - Há políticas e procedimentos relacionados documentados e são revisados periodicamente
- [ ] 5 - Há políticas e procedimentos relacionados documentados, estes são revisados e auditados periodicamente

28. 4.7 - Integrar a privacidade e proteção de dados nas práticas de segurança e medicina do trabalho *

- [ ] 1 - Não há políticas e procedimentos relacionados documentados
- [ ] 2 - Há políticas e procedimentos relacionados parcialmente documentados
- [ ] 3 - Há políticas e procedimentos relacionados documentados
- [ ] 4 - Há políticas e procedimentos relacionados documentados e são revisados periodicamente
- [ ] 5 - Há políticas e procedimentos relacionados documentados, estes são revisados e auditados periodicamente

29. 4.8 - Integrar a privacidade e proteção de dados ao uso de vigilância por vídeo (CFTV) *

- [ ] 1 - Não há políticas e procedimentos relacionados documentados
- [ ] 2 - Há políticas e procedimentos relacionados parcialmente documentados
- [ ] 3 - Há políticas e procedimentos relacionados documentados
- [ ] 4 - Há políticas e procedimentos relacionados documentados e são revisados periodicamente
- [ ] 5 - Há políticas e procedimentos relacionados documentados, estes são revisados e auditados periodicamente

30. 4.9 - Integrar a privacidade e proteção de dados ao uso de dispositivos de geolocalização geográfica *

- 1 - Não há políticas e procedimentos relacionados documentados
- 2 - Há políticas e procedimentos relacionados parcialmente documentados
- 3 - Há políticas e procedimentos relacionados documentados
- 4 - Há políticas e procedimentos relacionados documentados e são revisados periodicamente
- 5 - Há políticas e procedimentos relacionados documentados, estes são revisados e auditados periodicamente

5. Treinamento e conscientização

31. 5.1 - Conduzir treinamento em privacidade e proteção de dados *

- 1 - Não Treinamento em privacidade e proteção de dados
- 2 - Há treinamento em privacidade e proteção de dados, mas não periódico
- 3 - Há treinamento em privacidade e proteção de dados periodicamente
- 4 - Há treinamento em privacidade e proteção de dados periodicamente com realização de avaliação de impacto
- 5 - Há treinamento em privacidade e proteção de dados periodicamente com realização de avaliação de impacto. O resultado das avaliações é utilizado para aprimoramento contínuo do treinamento.

32. 5.2 - Incorporar a privacidade e proteção dos dados ao treinamento operacional, como RH, segurança, etc *

- 1 - O treinamento de privacidade e proteção de dados não faz parte do treinamento de ambientação.
- 2 - Há treinamento parcial de privacidade e proteção de dados durante ambientação.
- 3 - Há treinamento completo de privacidade e proteção de dados durante ambientação.
- 4 - Há treinamento completo de privacidade e proteção de dados durante ambientação. Ao final é realizada uma avaliação de impacto.

5 - Há treinamento completo de privacidade e proteção de dados durante ambientação. Ao final é realizada uma avaliação de impacto e os resultados são utilizados para o aprimoramento contínuo do treinamento.

33. 5.3- Fornecer um repositório de informações de privacidade e proteção de dados, por exemplo, uma intranet interna de privacidade e e proteção de dados *

- ( ) 1 - Não há repositório de materiais relacionados a privacidade e proteção de dados.
- ( ) 2 - Há repositório de materiais relacionados a privacidade e proteção de dados. Contudo este não é divulgado.
- ( ) 3 - Há repositório de materiais relacionados a privacidade e proteção de dados. Este é divulgado
- ( ) 4 - Há repositório de materiais relacionados a privacidade e proteção de dados. Este é divulgado e atualizado periodicamente manualmente.
- ( ) 5 - Há repositório de materiais relacionados a privacidade e proteção de dados. Este é divulgado e atualizado periodicamente automaticamente.

34. 5.4 - Realizar eventos de conscientização de privacidade e proteção de dados (por exemplo, um dia / semana anual de privacidade de dados) *

- ( ) 1 - Não são realizados eventos de conscientização de privacidade e proteção de dados
- ( ) 2 - São realizados eventos de conscientização de privacidade e proteção de dados, mas sem calendário pré-definido.
- ( ) 3 - São realizados eventos de conscientização de privacidade e proteção de dados, com calendário pré-definido.
- ( ) 4 - São realizados eventos de conscientização de privacidade e proteção de dados, com calendário pré-definido. O evento conta com a participação da diretoria e gerência.
- ( ) 5 - São realizados eventos de conscientização de privacidade e proteção de dados, com calendário pré-definido. O evento conta com a participação da diretoria e gerência. Há métricas para aferir o nível de participação e engajamento dos colaboradores.

35. 5.5 - Fornecer educação e treinamento contínuos para o DPO e manter a certificação dos responsáveis pela privacidade e proteção dos dados *

1 - Não são realizados treinamentos para o DPO

- [ ] 2 - São realizados treinamentos não periódicos para o DPO
- [ ] 3 - São realizados treinamentos periódicos para o DPO.
- [ ] 4 - São realizados treinamentos periódicos para o DPO. E as certificações são renovadas não periodicamente
- [ ] 5 - São realizados treinamentos periódicos para o DPO. E as certificações são renovadas periodicamente

6. Gerenciamento de riscos de segurança da informação

36. 6.1 - Integrar privacidade e proteção de dados em uma política de segurança da informação *

- [ ] 1 - Não há política de segurança da informação e privacidade
- [ ] 2 - Há política de segurança da informação, mas não política de privacidade ou vice versa
- [ ] 3 - Há política de segurança da informação e uma política de privacidade.
- [ ] 4 - Há política de segurança da informação com base nas ISOs 27001 e 27002 e uma política de privacidade baseada na ISO 27701
- [ ] 5 - Há política de segurança da informação com base nas ISOs 27001 e 27002 e uma política de privacidade baseada na ISO 27701. Os controles são auditados periodicamente.

37. 6.2 - Integrar a segurança da informação na matriz de riscos da organização *

- [ ] 1 - Na matriz de risco da organização não estão listados riscos relacionados a segurança da informação.
- [ ] 2 - Na matriz de risco da organização estão listados parcialmente os riscos relacionados a segurança da informação.
- [ ] 3 - Na matriz de risco da organização estão listados os riscos relacionados a segurança da informação.
- [ ] 4 - Na matriz de risco da organização estão listados os riscos de segurança da informação. Há um plano de ação para cada um dos riscos.
- [ ]

5 - Na matriz de risco da organização estão listados os riscos relacionados a segurança da organização. Há um plano de ação para cada um dos riscos. Os controles são auditados periodicamente.

38. 6.3 - Manter medidas técnicas de segurança e proteção de dados *

- ( ) 1 - Não há medidas técnicas de segurança implementadas
- ( ) 2 - Há algumas medidas técnicas de segurança implementadas, tais como firewall e antimalware nas estações ou servidores
- ( ) 3 - As principais medidas técnicas de segurança estão implementadas em estações de trabalho e servidores, tais como firewall e antimalware
- ( ) 4 - As principais medidas técnicas de segurança estão implementadas, tais como firewall e antimalware. As atualizações de assinaturas ocorrem automaticamente.
- ( ) 5 - As principais medidas técnicas de segurança estão implementadas, tais como firewall e antimalware nas estações de trabalho e servidores. As atualizações de assinaturas ocorrem automaticamente. Há auditorias internas periódicas para aferir a efetividade dos controles.

39. 6.4 - Manter medidas para criptografar dados pessoais em repouso e em movimento *

- ( ) 1 - Não há medidas técnicas de criptografia implementadas
- ( ) 2 - Há medidas técnicas de criptografia implementadas parcialmente
- ( ) 3 - Há medidas técnicas de criptografia implementadas para proteção de dados em repouso e movimento
- ( ) 4 - Há medidas técnicas de criptografia implementadas para proteção de dados em repouso e movimento. Há retenção de logs de acessos ou tentativas de acesso a arquivos criptografados.
- ( ) 5 - Há medidas técnicas de criptografia implementadas para proteção de dados em repouso e movimento. Há retenção de logs de acessos ou tentativas de acesso a arquivos criptografados. São enviados alertas automáticos em caso de incidentes e violações de acesso.

40. 6.5 - Manter procedimentos para restringir o acesso a dados pessoais (por exemplo, acesso baseado em função, segregação de funções) *

( ) 1 - Não há matriz de segregação de funções

( ) 2 - Há matriz de segregação de funções, parcial. Com a definição de usuários e perfis de alguns sistemas.

( ) 3 - Há matriz de segregação de funções com a definição de usuários e perfis de acesso em cada sistema.

( ) 4 - Há matriz de segregação de funções com a definição de usuários e perfis de acesso em cada sistema. A matriz é revisada periodicamente.

( ) 5 - Há matriz de segregação de funções com a definição de usuários e perfis de acesso em cada sistema. A matriz é revisada periodicamente. São realizadas auditorias para conferência dos acessos face a matriz.

41. 6.6 - Manter os controles físicos de segurança da informação corporativa (proteção de instalações físicas e ativos físicos) *

1 - Não há medidas técnicas de segurança física implementadas

( ) 2 - Há algumas medidas técnicas de segurança física implementadas tais como
( )
CFTV ou Controle de acesso

( ) 3 - As principais medidas técnicas de segurança física estão implementadas, tais como CFTV e CA.

( ) 4 - As principais medidas técnicas de segurança física estão implementadas, tais como CFTV e Controle de acesso. Há registro dos logs e os ativos são monitorados por sistema de CMDB.

( ) 5 - As principais medidas técnicas de segurança física estão implementadas, tais como CFTV e controle de acesso. Há registro dos logs e os ativos são monitorados por sistema de CMDB. Os controles são auditados periodicamente.

42. 6.7 - Manter plano de continuidade de negócios (PCN) *

1 - Não há PCN

2 - Há PCN, mas não são executados testes periódicos e nem atualizações

- [ ] 3 - Há PCN, são executados testes e atualizações periódicas
- [ ] 4 - Há PCN baseado na ISO 22301, são executados testes e atualizações periódicas
- [ ] 5 - Há PCN baseado na ISO 22301, são executados testes e atualizações periódicas. Há mecanismo de recuperação automatizada em caso de desastres.

43. 6.8 - Manter uma estratégia de prevenção de perda de dados pessoais *

- [ ] 1 - Não há backup dos servidores que armazenam dados pessoais
- [ ] 2 - Há backup não periódico dos servidores que armazenam dados pessoais
- [ ] 3 - Há backup periódico dos servidores que armazenam dados pessoais
- [ ] 4 - Há backup periódico dos servidores que armazenam dados pessoais com testes de recuperação esporádicos.
- [ ] 5 - Há backup periódico dos servidores que armazenam dados pessoais com testes de recuperação esporádicos. Dados de backup são armazenados em local geograficamente distante (mínimo 500m) da produção.

44. 6.9 - Conduzir testes de intrusão para aferir o desempenho e efetividade dos controles de segurança *

- [ ] 1 - Não são realizados testes de intrusão
- [ ] 2 - São realizados teste de intrusão não periódicos
- [ ] 3 - São realizados teste de intrusão periódicos WAN to LAN Black Box
- [ ] 4 - São realizados teste de intrusão periódicos WAN to LAN e LAN to LAN GrayBox
- [ ] 5 - São realizados teste de intrusão periódicos WAN to LAN e LAN to LAN WhiteBox

45. 6.10 - Manter um sistema de prevenção de intrusos (IPS) *

- [ ] 1 - Não há IPS implantado
- [ ] 2 - Há IPS implantado apenas para monitoramento
- [ ] 3 - Há IPS implantado para monitoramento e intercepção de ameaças.
- [ ] 4 - Há IPS implantado para monitoramento e intercepção de ameaças. Há profissional alocado para resposta aos incidentes.
- [ ] 5 - Há IPS implantado para monitoramento e intercepção de ameaças. Há SOC alocado para resposta aos incidentes.

46. 6.11 - Manter um sistema de gerenciamento de dispositivos móveis (MDM) *

- [ ] 1 - Não há MDM implantado
- [ ] 2 - Há MDM implantado apenas para monitoramento
- [ ] 3 - Há MDM implantado para monitoramento e controle de dispositivos.
- [ ] 4 - Há MDM implantado para monitoramento e restrição de apps a serem instalados nos dispositivos corporativos.
- [ ] 5 - Há MDM implantado para monitoramento e restrição de apps a serem instalados nos dispositivos corporativos e pela política BYOD (Bring Your Own Device).

47. 6.12 - Manter um sistema de gerenciamento e correlação de eventos de segurança (SIEM) *

- [ ] 1 - Não há SIEM implantado
- [ ] 2 - Há SIEM implantado apenas para coleta de logs
- [ ] 3 - Há SIEM implantado para coleta e notificação em caso de alertas de segurança.
- [ ] 4 - Há SIEM implantado para coleta e notificação em caso de alertas de segurança. Os eventos de segurança são relacionados
- [ ] 5 - Há SIEM implantado para coleta e notificação em caso de alertas de segurança. Os eventos de segurança são relacionados e tratado pelo SOC.

48. 6.13 - Manter um sistema de gerenciamento de vulnerabilidades *

1 - Não há sistema de gerenciamento de vulnerabilidades implantado

2 - Há sistema de gerenciamento de vulnerabilidades implantado apenas para consulta

3 - Há sistema de gerenciamento de vulnerabilidades implantado para consulta e obtenção de medidas de remediação

4 - Há sistema de gerenciamento de vulnerabilidades implantado para consulta e obtenção de medidas de remediação. Um profissional é responsável por corrigir as vulnerabilidades

5 - Há sistema de gerenciamento de vulnerabilidades implantado para consulta e obtenção de medidas de remediação. O SOC é o responsável por corrigir as vulnerabilidades.

49. 6.14 - Manter um sistema de gerenciamento de acesso remoto seguro *

1 - Não há sistema de gerenciamento de acesso remoto seguro implantado

2 - Há sistema de gerenciamento de acesso remoto seguro implantado com conexão direta (DNAT)

3 - Há sistema de gerenciamento de acesso remoto seguro implantado com VPN

4 - Há sistema de gerenciamento de acesso remoto seguro implantado com VPN e MFA.

5 - Há sistema de gerenciamento de acesso remoto seguro implantado com VPN,MFA e segregação de acesso por grupo de usuário.

50. 6.15 - Manter um sistema de gerenciamento de acesso as interfaces de rede *

1 - Não há sistema de gerenciamento de acesso as interfaces de rede

2 - Há sistema de gerenciamento de acesso as interfaces de rede através de VLAN

3 - Há sistema de gerenciamento de acesso as interfaces de rede através de VLAN e PortSecurity

4 - Há sistema de gerenciamento de acesso as interfaces de rede através de VLAN e PortSecurity, com autenticação integrada via Radius.

5 - Há sistema de gerenciamento de acesso as interfaces de rede através de VLANe PortSecurity, com autenticação integrada via Radius e Health Check antes de autorizar acesso do host.

51. 6.16 - Manter um sistema de gerenciamento de mídias de armazenamento removível *

- [ ] 1 - Não há sistema de gerenciamento de mídias de armazenamento removível
- [ ] 2 - Há sistema de gerenciamento de mídias de armazenamento removível contudo não há restrição de dispositivos
- [ ] 3 - Há sistema de gerenciamento de mídias de armazenamento removível e há restrição de dispositivos
- [ ] 4 - Há sistema de gerenciamento de mídias de armazenamento removível e há restrição de dispositivos. Há possibilidade de flexibilização por dispositivo e por período.
- [ ] 5 - Há sistema de gerenciamento de mídias de armazenamento removível e há restrição de dispositivos. Há possibilidade de flexibilização por dispositivo e por período. Mídias de armazenamento removível são criptografadas.

7. Gerenciamento de Riscos de Terceiros

52. 7.1 - Manter política de privacidade e proteção de dados para terceiros (por exemplo, clientes, fornecedores, processadores, afiliados) *

- [ ] 1 - Não há políticas relacionadas documentadas
- [ ] 2 - Há políticas relacionadas parcialmente documentadas
- [ ] 3 - Há políticas relacionadas documentadas
- [ ] 4 - Há políticas relacionadas documentadas e são revisadas periodicamente
- [ ] 5 - Há políticas relacionadas documentadas, estas são revisadas e auditadas periodicamente

53. 7.2 - Manter procedimentos para executar contratos ou acordos com todos os operadores *

- [ ] 1 - Não há procedimentos relacionados documentadas
- [ ] 2 - Há procedimentos relacionados parcialmente documentados
- [ ] 3 - Há procedimentos relacionados documentados
- [ ] 4 - Há procedimentos relacionados documentados e são revisados periodicamente
- [ ] 5 - Há procedimentos relacionados documentados, estes são revisados e auditados periodicamente

54. 7.3 - Realizar a devida diligência em torno da postura de privacidade e proteção de dados, segurança de dados de fornecedores / operadores em potencial *

- [ ] 1 - Não é feita diligência em torno de operadores
- [ ] 2 - É feita diligência parcial em torno de operadores através de contrato.
- [ ] 3 - É feita diligência em torno de operadores através de contratos e políticas de privacidade e proteção de dados
- [ ] 4 - É feita diligência em torno de operadores em potencial. Este precisam apresentar relatórios periódicos que comprovem a eficiência dos controles de proteção e privacidade.
- [ ] 5 - É feita diligência em torno de operadores em potencial. Este precisam apresentar relatórios periódicos que comprovem a eficiência dos controles de proteção e privacidade. São realizadas auditorias periodicamente.

55. 7.4 - Manter um processo de avaliação de risco de privacidade e proteção de dados do fornecedor (pré e pós contrato) *

- [ ] 1 - Não há procedimentos relacionados documentadas
- [ ] 2 - Há procedimentos relacionados parcialmente documentados
- [ ] 3 - Há procedimentos relacionados documentados
- [ ] 4 - Há procedimentos relacionados documentados e são revisados periodicamente

5 - Há procedimentos relacionados documentados, estes são revisados e auditados periodicamente

56. 7.5 - Manter uma política que rege o uso de serviços em nuvem *

- [ ] 1 - Não há políticas relacionadas documentadas
- [ ] 2 - Há políticas relacionadas parcialmente documentadas
- [ ] 3 - Há políticas relacionadas documentadas
- [ ] 4 - Há políticas relacionadas documentadas e são revisadas periodicamente
- [ ] 5 - Há políticas relacionadas documentadas, estas são revisadas e auditadas periodicamente

57. 7.6 - Analisar os contratos para verificar riscos de privacidade de dados *

- [ ] 1 - Não há análise de contratos
- [ ] 2 - Há análise de alguns contratos sob não periódica
- [ ] 3 - Há análise de todos os contratos não periódica
- [ ] 4 - Há análise de todos os contratos periodicamente para manter aderência a legislação vigente.
- [ ] 5 - Há análise de todos os contratos periodicamente para manter aderência a legislação vigente. Há mecanismo implantado para análise de impacto automático em contratos.

8. Plano de Comunicação

58. 8.1 - Manter um aviso de privacidade e proteção de dados que detalha as práticas de tratamento de dados pessoais da organização *

1 - Não há qualquer aviso

2 - Há aviso informal

- [ ] 3 - Há aviso de privacidade e proteção de dados que detalha as práticas de tratamento de dados pessoais da organização
- [ ] 4 - Há aviso de privacidade e proteção de dados que detalha as práticas de tratamento de dados pessoais da organização. O mesmo é revisado periodicamente.
- [ ] 5 - Há aviso de privacidade e proteção de dados que detalha as práticas de tratamento de dados pessoais da organização. O mesmo é revisado periodicamente e adequado de acordo com as melhores práticas.

59. 8.2 - Fornecer aviso de privacidade e proteção de dados em todos os pontos em que os dados pessoais são coletados *

- [ ] 1 - Não há qualquer aviso
- [ ] 2 - Há aviso informal
- [ ] 3 - Há aviso de privacidade e proteção de dados que detalha as práticas de tratamento de dados pessoais da organização
- [ ] 4 - Há aviso de privacidade e proteção de dados que detalha as práticas de tratamento de dados pessoais da organização. O mesmo é revisado periodicamente.
- [ ] 5 - Há aviso de privacidade e proteção de dados que detalha as práticas de tratamento de dados pessoais da organização. O mesmo é revisado periodicamente e adequado de acordo com as melhores práticas.

60. 8.3 - Fornecer aviso nas comunicações de marketing (por exemplo, e-mails, folhetos, ofertas) *

- [ ] 1 - Não há qualquer aviso
- [ ] 2 - Há aviso informal
- [ ] 3 - Há aviso de privacidade e proteção de dados que detalha as práticas de tratamento de dados pessoais da organização
- [ ] 4 - Há aviso de privacidade e proteção de dados que detalha as práticas de tratamento de dados pessoais da organização. O mesmo é revisado periodicamente.
- [ ] 5 - Há aviso de privacidade e proteção de dados que detalha as práticas de tratamento de dados pessoais da organização. O mesmo é revisado periodicamente e adequado de acordo com as melhores práticas.

61. 8.4 - Fornecer aviso em contratos e termos *

- [ ] 1 - Não há qualquer aviso
- [ ] 2 - Há aviso informal
- [ ] 3 - Há aviso de privacidade e proteção de dados que detalha as práticas de tratamento de dados pessoais da organização
- [ ] 4 - Há aviso de privacidade e proteção de dados que detalha as práticas de tratamento de dados pessoais da organização. O mesmo é revisado periodicamente.
- [ ] 5 - Há aviso de privacidade e proteção de dados que detalha as práticas de tratamento de dados pessoais da organização. O mesmo é revisado periodicamente e adequado de acordo com as melhores práticas.

62. 8.5 - Manter scripts para uso dos funcionários para explicar ou fornecer o aviso de privacidade e proteção de dados *

- [ ] 1 - Não há qualquer script
- [ ] 2 - Há script informal
- [ ] 3 - Há scripts para uso dos funcionários para explicar ou fornecer o aviso de privacidade e proteção de dados
- [ ] 4 - Há scripts para uso dos funcionários para explicar ou fornecer o aviso de privacidade e proteção de dados. Os mesmos são revisados periodicamente.
- [ ] 5 - Há scripts para uso dos funcionários para explicar ou fornecer o aviso de privacidade e proteção de dados. Os mesmos são revisados periodicamente e adequado segundo as melhores práticas.

9. Resposta aos Titulares dos Dados

63. 9.1 - Manter procedimentos e ferramenta para tratar de reclamações *

- [ ] 1 - Não há procedimentos relacionados documentados
- [ ] 2 - Há procedimentos relacionados parcialmente documentados
- [ ] 3 - Há procedimentos relacionados documentados
- [ ] 4 - Há procedimentos relacionados documentados e são revisados periodicamente
- [ ] 5 - Há procedimentos relacionados documentados, estes são revisados e auditados periodicamente

64. 9.2 - Manter procedimentos e ferramenta para responder a solicitações de acesso a dados pessoais *

- [ ] 1 - Não há procedimentos relacionados documentados
- [ ] 2 - Há procedimentos relacionados parcialmente documentados
- [ ] 3 - Há procedimentos relacionados documentados
- [ ] 4 - Há procedimentos relacionados documentados e são revisados periodicamente
- [ ] 5 - Há procedimentos relacionados documentados, estes são revisados e auditados periodicamente

65. 9.3 - Manter procedimentos e ferramenta para responder a solicitações e / ou fornecer um mecanismo para os indivíduos atualizarem ou corrigirem seus dados pessoais *

- [ ] 1 - Não há procedimentos relacionados documentados
- [ ] 2 - Há procedimentos relacionados parcialmente documentados
- [ ] 3 - Há procedimentos relacionados documentados
- [ ] 4 - Há procedimentos relacionados documentados e são revisados periodicamente
- [ ] 5 - Há procedimentos relacionados documentados, estes são revisados e auditados periodicamente

66. 9.4 - Manter procedimentos e ferramenta para responder a pedidos de exclusão, restrição ou oposição ao processamento *

- [ ] 1 - Não há procedimentos relacionados documentados
- [ ] 2 - Há procedimentos relacionados parcialmente documentados
- [ ] 3 - Há procedimentos relacionados documentados
- [ ] 4 - Há procedimentos relacionados documentados e são revisados periodicamente
- [ ] 5 - Há procedimentos relacionados documentados, estes são revisados e auditados periodicamente

67. 9.5 - Manter procedimentos e ferramenta para responder a pedidos de informações *

- [ ] 1 - Não há procedimentos relacionados documentados
- [ ] 2 - Há procedimentos relacionados parcialmente documentados
- [ ] 3 - Há procedimentos relacionados documentados
- [ ] 4 - Há procedimentos relacionados documentados e são revisados periodicamente
- [ ] 5 - Há procedimentos relacionados documentados, estes são revisados e auditados periodicamente

68. 9.6 - Manter procedimentos e ferramenta para responder a solicitações de portabilidade de dados *

- [ ] 1 - Não há procedimentos relacionados documentados
- [ ] 2 - Há procedimentos relacionados parcialmente documentados
- [ ] 3 - Há procedimentos relacionados documentados
- [ ] 4 - Há procedimentos relacionados documentados e são revisados periodicamente

5 - Há procedimentos relacionados documentados, estes são revisados e auditados periodicamente

69. 9.7 - Manter procedimentos e ferramentas para responder a pedidos a serem esquecidos ou para apagar dados *

- [ ] 1 - Não há procedimentos relacionados documentados
- [ ] 2 - Há procedimentos relacionados parcialmente documentados
- [ ] 3 - Há procedimentos relacionados documentados
- [ ] 4 - Há procedimentos relacionados documentados e são revisados periodicamente
- [ ] 5 - Há procedimentos relacionados documentados, estes são revisados e auditados periodicamente

70. 9.8 - Manter perguntas frequentes (FAQ) para responder as dúvidas dos titulares dos dados *

- [ ] 1 - Não há procedimentos relacionados documentados
- [ ] 2 - Há procedimentos relacionados parcialmente documentados
- [ ] 3 - Há procedimentos relacionados documentados
- [ ] 4 - Há procedimentos relacionados documentados e são revisados periodicamente
- [ ] 5 - Há procedimentos relacionados documentados, estes são revisados e auditados periodicamente

71. 9.9 - Investigar as causas raízes das reclamações de proteção de dados *

- [ ] 1 - Não há procedimentos relacionados documentados
- [ ] 2 - Há procedimentos relacionados parcialmente documentados
- [ ] 3 - Há procedimentos relacionados documentados
- [ ] 4 - Há procedimentos relacionados documentados e são revisados periodicamente
- [ ] 5 - Há procedimentos relacionados documentados, estes são revisados e auditados periodicamente

72. 9.10 - Monitorar e reportar métricas para reclamações de privacidade e proteção de dados (Tempo de resposta, quantidade, causa raiz) *

- [ ] 1 - Não há procedimentos relacionados documentados
- [ ] 2 - Há procedimentos relacionados parcialmente documentados
- [ ] 3 - Há procedimentos relacionados documentados
- [ ] 4 - Há procedimentos relacionados documentados e são revisados periodicamente
- [ ] 5 - Há procedimentos relacionados documentados, estes são revisados e auditados periodicamente

10. Monitoramento de Novas Práticas Operacionais

73. 10.1 - Manter procedimento de verificação de identidade dos titulares *

- [ ] 1 - Não há procedimentos relacionados documentados
- [ ] 2 - Há procedimentos relacionados parcialmente documentados
- [ ] 3 - Há procedimentos relacionados documentados
- [ ] 4 - Há procedimentos relacionados documentados e são revisados periodicamente
- [ ] 5 - Há procedimentos relacionados documentados, estes são revisados e auditados periodicamente

74. 10.2 - Integrar o Privacy by Design no desenvolvimento de sistemas e produtos da organização *

( ) 1 - Aspectos de privacidade não são considerados no desenvolvimento de sistemas e produtos da organização

( ) 2 - Aspectos de privacidade não são requisitos chave de sistemas e produtos da organização, mas são considerados

( ) 3 - Aspectos de privacidade são requisitos chave no desenvolvimento de sistema se produtos da organização

( ) 4 - Aspectos de privacidade são requisitos chave no desenvolvimento de sistema se produtos da organização. Ocorrem revisões internas periódicas dos sistemas em busca de falhas que possam comprometer a privacidade.

( ) 5 - Aspectos de privacidade são requisitos chave no desenvolvimento de sistemas e produtos da organização. Ocorrem revisões internas e externas periódicas dos sistemas em busca de falhas que possam comprometer a privacidade.

75. 10.3 - Manter diretrizes e modelos de DPIA (Data Protection Impact Assessment) em conformidade com à LGPD *

( ) 1 - Não há DPIA

( ) 2 - Há DPIA incompletos

( ) 3 - Há DPIA de todos os processos que tratam dados pessoais na organização. Os DPIA de dados sensíveis são relatados para os reguladores

( ) 4 - Há DPIA de todos os processos que tratam dados pessoais na organização. Os DPIA de dados sensíveis são relatados para os reguladores. Os documentos são revisados periodicamente junto as áreas de negócio.

( ) 5 - Há DPIA de todos os processos que tratam dados pessoais na organização. Os DPIA de dados sensíveis são relatados para os reguladores. Os documentos são revisados periodicamente junto as áreas de negócio. Há um plano de ação que é objeto de auditoria periódica.

11. Gerenciamento de violação de privacidade de dados

76. 11.1 - Manter um plano de resposta a incidentes / violações da privacidade de dados *

- [ ] 1 - Não há procedimentos relacionados documentados
- [ ] 2 - Há procedimentos relacionados parcialmente documentados
- [ ] 3 - Há procedimentos relacionados documentados
- [ ] 4 - Há procedimentos relacionados documentados e são revisados periodicamente
- [ ] 5 - Há procedimentos relacionados documentados, estes são revisados e auditados periodicamente

77. 11.2 - Manter um protocolo de notificação de violação (para as pessoas afetadas) e relatórios (para reguladores, agências de crédito, órgãos policiais) *

- [ ] 1 - Não há procedimentos relacionados documentados
- [ ] 2 - Há procedimentos relacionados parcialmente documentados
- [ ] 3 - Há procedimentos relacionados documentados
- [ ] 4 - Há procedimentos relacionados documentados e são revisados periodicamente
- [ ] 5 - Há procedimentos relacionados documentados, estes são revisados e auditados periodicamente

78. 11.3 - Manter o registro quanto o rastreamento de incidentes / violações de privacidade e proteção de dados *

- [ ] 1 - Não há procedimentos relacionados documentados
- [ ] 2 - Há procedimentos relacionados parcialmente documentados
- [ ] 3 - Há procedimentos relacionados documentados
- [ ] 4 - Há procedimentos relacionados documentados e são revisados periodicamente
- [ ] 5 - Há procedimentos relacionados documentados, estes são revisados e auditados periodicamente

79. 11.4 - Monitorar e reportar as métricas de incidentes / violações de privacidade e proteção de dados (natureza da violação, risco, causa raiz) *

1 - Não há procedimentos relacionados documentados

2 - Há procedimentos relacionados parcialmente documentados

3 - Há procedimentos relacionados documentados

4 - Há procedimentos relacionados documentados e são revisados periodicamente

5 - Há procedimentos relacionados documentados, estes são revisados e auditados periodicamente

80. 11.5 - Realizar testes periódicos do plano de violação / incidente de privacidade e proteção de dados *

1 - Não são realizados testes periódicos do plano de violação / incidente de privacidade e proteção de dados

2 - São realizados testes não periódicos do plano de violação / incidente de privacidade e proteção de dados

3 - São realizados testes periódicos do plano de violação / incidente de privacidade e proteção de dados

4 - São realizados testes periódicos do plano de violação / incidente de privacidade e proteção de dados. O plano é constantemente aprimorado a partir do resultado dos testes

5 - São realizados testes periódicos do plano de violação / incidente de privacidade e proteção de dados. O plano é constantemente aprimorado a partir do resultado dos testes. São realizadas auditorias do plano.

81. 11.6 - Obter cobertura de seguro de violação de privacidade e proteção de dados *

1 - Não há cobertura de seguro de violação de privacidade e proteção de dados

2 - Há cobertura parcial de seguro de violação de privacidade e proteção de dados

3 - Há cobertura completa de seguro de violação de privacidade e proteção de

4 - Há cobertura completa de seguro de violação de privacidade e proteção dedados. São monitorados indicadores de segurança pela seguradora.

5 - Há cobertura completa de seguro de violação de privacidade e proteção dedados. São monitorados indicadores de segurança pela seguradora e realizadas auditorias periódicas.

12. Tratamento de Dados

82. 12.1 - Conduzir auditorias internas do programa de privacidade e proteção de dados *

- 1 - Não são realizadas auditorias internas
- 2 - São realizadas auditorias internas não periódicas.
- 3 - São realizadas auditorias internas periódicas.
- 4 - São realizadas auditorias internas periódicas. O resultado é utilizado para elaboração de um plano de ação.
- 5 - São realizadas auditorias internas periódicas. O resultado é utilizado para elaboração de um plano de ação que é monitorado e apresentado para a diretoria.

83. 12.2 - Conduzir avaliações com base em eventos externos, como reclamações / violações, entre outros *

- 1 - Não há avaliações de eventos externos
- 2 - As avaliações de eventos externos ocorrem de forma ad-hoc
- 3 - Todos os eventos externos são avaliados
- 4 - Todos os eventos externos são avaliados e há indicadores para monitoramento da eficiência do processo.
- 5 - Todos os eventos externos são avaliados e há indicadores para monitoramento da eficiência do processo. São realizadas auditorias periódicas.

84. 12.3 - Envolver a auditoria externas para avaliações independentes *

- [ ] 1 - Não são realizadas auditorias externas
- [ ] 2 - São realizadas auditorias externas não periódicas.
- [ ] 3 - São realizadas auditorias externas periódicas.
- [ ] 4 - São realizadas auditorias externas periódicas. O resultado é utilizado para elaboração de um plano de ação.
- [ ] 5 - São realizadas auditorias externas periódicas. O resultado é utilizado para elaboração de um plano de ação que é monitorado e apresentado para a diretoria.

85. 12.4 - Monitorar e reportar as métricas de privacidade e proteção de dados *

- [ ] 1 - Não há métricas relacionadas documentadas
- [ ] 2 - Há métricas relacionadas parcialmente documentadas
- [ ] 3 - Há métricas relevantes e relacionadas documentadas
- [ ] 4 - Há métricas relevantes e relacionadas documentadas. Indicadores são monitorados constantemente
- [ ] 5 - Há métricas relevantes e relacionadas documentadas. Indicadores são monitorados constantemente. São estabelecidas metas para evolução contínua.

86. 12.5 - Manter a documentação como evidência a fim de demonstrar conformidade e / ou prestação de conta *

- [ ] 1 - Não há documentação relacionada
- [ ] 2 - Há documentação parcial relacionada
- [ ] 3 - Há documentação relacionada
- [ ] 4 - Há documentação relacionada, a revisão é periódica
- [ ] 5 - Há documentação relacionada, a revisão e auditorias são periódicas.

Obrigado por ter preenchido a pesquisa, falta pouco para o término. Como o modelo de maturidade de segurança da informação é um modelo aberto a comunidade fique Feedback à vontade para contribuir com críticas, sugestões e elogios.

87. O que você achou do modelo de maturidade de segurança da informação proposto?

88. Pontos Fortes do Modelo
Marque todas que se aplicam.

- [ ] Abrangente
- [ ] Detalhado
- [ ] Objetivo
- [ ] Outro: _____

89. Pontos Fracos do Modelo
Marque todas que se aplicam.

- [ ] Superficial
- [ ] Extenso
- [ ] Incompleto
- [ ] Outro: _____