COMBINAÇÃO DE ONTOLOGIAS NO CONTEXTO DA PROTEÇÃO DA INFRAESTRUTURA CRÍTICA BRASILEIRA

Combining Ontologies in the Context of the Brazilian Critical Infrastructure Protection

Antônio Carlos Pereira de Britto (1), Edilson Ferneda (2), Hércules do Prado (3), Fernando William Cruz (4), Rafael Gostinski Ferreira (*in memoriam*) **(5)**

(1) Agencia Brasileira de Inteligência, Brasil, acbtto@gmail.com

(2) Universidade Católica de Brasília, Brasil, eferneda@gmail.com

(3) Universidade Católica de Brasília, Brasil, prado.hercules@gmail.com

(4) Universidade de Brasília, Brasil, fwcruz@gmail.com

(5) Agencia Brasileira de Inteligência, Brasil, rgostinski@gmail.com

Resumo

A Agência de Inteligência Brasileira (Abin) é responsável pela elaboração do Plano de Proteção ao Conhecimento no âmbito do Sistema Brasileiro de Inteligência (SISBIN). Para isto, utiliza conhecimentos relativos à segurança da informação e comunicação para a proteção da infraestrutura crítica nacional. Contudo, o conhecimento sobre essa proteção encontra-se fragmentado nos processos de análise de risco, de tratamento da segurança computacional e de governança da segurança da informação, representadas por um conjunto de ontologias. Este artigo relata a experiência da Abin no uso de técnicas e ferramentas de Engenharia de Ontologias para a combinação de ontologias e extração do conhecimento relacionado à proteção da infraestrutura de TIC da APF. Esse conhecimento auxilia o trabalho colaborativo dos vários atores envolvidos nesse processo no âmbito do SISBIN.

Palavras chave: Gestão de Segurança da Informação. Proteção do Conhecimento. Ontologias. Combinação de Ontologias.

Abstract

The Brazilian Intelligence Agency (Abin) is responsible for preparing the Knowledge Protection Plan under the Brazilian Intelligence System (SISBIN). For this, it applies knowledge related to information and communication security for protecting the national critical infrastructure. In this context, Abin produces

strategic recommendations for the Federal Public Administration (APF), prospects its vulnerabilities and safeguards its critical ICT infrastructure. However, knowledge about this protection is fragmented in the processes of risk analysis, computational security and information security governance, represented by a set of ontologies. This article reports Abin's experience in using Ontology Engineering techniques and tools for the combination of ontologies and knowledge extraction related to the protection of ICT infrastructure of APF. This knowledge helps the collaborative work of the many actors involved in this process within SISBIN.

Keywords: Security Information Management. Protection of Knowledge. Ontologies. Ontologies combination.

1 Introdução

A Agência Brasileira de Inteligência (Abin), como órgão central da Inteligência de Estado no Brasil, foi criada pela Lei nº 9.883, em 7 de dezembro de 1999. Estabeleceu-se então a comunidade de Inteligência no âmbito do Sistema Brasileiro de Inteligência (SISBIN), que abrange os instrumentos políticos, legais e meios para o cumprimento da obrigação constitucional da produção de conhecimento com a finalidade de assessorar a Presidência da República (PR) em suas decisões estratégicas.

Em sua instrumentação doutrinária, política e legal, o SISBIN vem investindo no tratamento colaborativo das informações oferecidas pelos órgãos parceiros do sistema. Nos níveis tático e operacional, o sistema busca a integração dos esforços de órgãos civis e militares para a produção de conhecimento pela incorporação de práticas de Gestão do Conhecimento (GC) mediadas pela Tecnologia da Informação (TI), sendo a proteção do conhecimento considerada uma questão estratégica na área de Contrainteligência (Balué e Nascimento 2006). Nesse contexto, várias são as oportunidades de melhorias nos processos de inteligência de estado, respaldadas pela Abin por cinco eixos estratégicos (Brasil 2017):

- a elaboração da Estratégica Nacional de Inteligência e do Plano Nacional de Inteligência, no escopo das ações decorrentes da Política Nacional de Inteligência (PNI);
- a consolidação da Abin como órgão gestor da atividade de Inteligência Estratégica, que assessora, de forma tempestiva, os agentes do Estado, interagindo agendas e ações de

Inteligência no âmbito dos Sistemas de Inteligência nacional e internacional, em proveito do cenário preventivo brasileiro;

- a promoção de formação dos quadros funcionais, com valorização ainda maior dos programas de capacitação, sobretudo nas áreas de operações e análise de inteligência:
- a estruturação e agregação de valor ao Planejamento Institucional e a Governança Corporativa, com a criação de unidade específica para atuar de forma integrada e transversal no desenvolvimento institucional e na modernização de processos, capacitando a Agência a responder aos desafios imediatos e de longo prazo;
- a atuação estruturada em Inteligência e Segurança Cibernética, mediante o emprego de recursos tecnológicos que permitam a exploração de grande volume de dados e propiciem vantagem competitiva na produção do conhecimento que irá subsidiar o processo decisório.

A criptografia de estado é um componente vital de ligação para garantir a segurança e independência tecnológicas como recursos essenciais à soberania nacional, bem como na capacitação da representação do conhecimento e recuperação da informação (Brasil 2017). Na Abin, há outras áreas de interesse além da criptografia de estado, como *Big Data*, Inteligência Artificial e Engenharia de Ontologias. Obtém-se, assim, vantagem estratégica por meio da utilização do crescente número de conceitos e informações, seja no âmbito interno ou externo ao País ou interno à própria organização, para a interoperabilidade dos sistemas do SISBIN. Dessa forma, são necessários aparatos tecnológicos cada vez mais complexos, alocados para atender a demandas da atividade de Inteligência e Contrainteligência, como a necessidade de mitigação de problemas causados por incompatibilidade terminológica utilizada pelos diversos atores em relação a temas de interesse comum. Daí a necessidade de um vocabulário compartilhado e consensual que viabilize a integração de conceitos, informações, procedimentos e práticas que propiciem o alinhamento entre as TIC e o foco de atuação da instituição (Probst et al. 2002; Ferreira 2007). Assim, a construção de vocabulários possibilita a produção do conhecimento para a Inteligência na perspectiva da Computação, e tem nas ontologias uma área de conhecimento viável para consolidar essa visão (Abin 2019). Nesse contexto, trabalha-se com um conjunto de

ontologias distintas, com foco em domínios específicos, mas que podem suportar o processo decisório em outros domínios.

Ontologias podem ser reusadas a partir de um esforço de combinação, o que engloba a utilização de técnicas de integração dessas ontologias (Klein 2001). Tal integração pode ser realizada pela fusão das ontologias ou mantendo-as íntegras. Em ambos os casos, o alinhamento dos conceitos envolvidos deve ser garantido mediante a concordância entre os especialistas dos domínios concernentes.

Ontologias viabilizam um comum acordo no uso do vocabulário compartilhado de maneira coerente e consistente (Gruber 2009). No contexto deste trabalho, as ontologias são utilizadas para regular o alinhamento entre os termos e as relações entre os conceitos a eles associados. As relações entre termos, criados pela comunidade, interagem pelo uso de conceitos específicos que levam a um significado na representação de conhecimentos e facultam que usuários formulem consultas usando os termos especificados. Percebe-se, nesse caso, que ontologias potencializam uma linguagem (conjunto de termos) a ser utilizada para formular consultas na recuperação da informação (Guarino 1995). Desse modo, as ontologias se apresentam como um modelo de relacionamento de entidades em um domínio particular do conhecimento que, no SISBIN, resultam em formas de representação das suas principais áreas de interesse, como a segurança cibernética na Administração Pública Federal (APF).

É preciso, então, passar dos níveis de aplicação, domínio e tarefa para a produção de novas ontologias e o casamento de ontologias existentes em um processo de reuso. O reuso de ontologias pelos parceiros do SISBIN exige a conservação da identidade das ontologias originais e deve viabilizar a interoperabilidade semântica visando à colaboração dos atores envolvidos, conforme a Doutrina de Inteligência da Abin (2016).

A obtenção e proteção de conhecimento implica, por sua vez, em preocupações estratégicas: a compatibilidade semântica representada nas várias ontologias elaboradas no âmbito desse sistema para viabilizar o trabalho colaborativo da Agência como órgão central. Assim, setores da Abin utilizam a Engenharia de Ontologias por meio de métodos e estruturas disponibilizadas nos ambientes de pesquisa e desenvolvimento.

Este artigo apresenta a visão do reuso de ontologias, mais especificamente a combinação de ontologias de segurança computacional e da informação, agregadas no âmbito do Plano Nacional de Proteção ao Conhecimento (PNPC), para o proveito das decisões estratégicas do SISBIN no domínio da Segurança da Informação e Comunicações e da Segurança Cibernética, organizando diretivas e recomendações para a Proteção da Infraestrutura Crítica da APF.

2 Segurança da informação e sistemas críticos

Os conceitos de segurança da informação, infraestrutura crítica e gestão do risco à informação são articulados para a definição de termos e relações que levam a esquemas teóricos e arcabouços legais na Inteligência de Estado para a proteção da APF. Nesse particular, as relações entre os termos e conceitos são criadas por especialistas a fim de propiciar consultas para a extração de conhecimento de forma a viabilizar a proteção dos sistemas. Em contexto mais abrangente, várias outras ontologias são implementadas na Inteligência, e estas definem a linguagem, aqui entendida como um conjunto de termos, utilizada para formular questionamentos dentro do escopo e da situação de interesse.

2.1 Segurança da informação e comunicações

Na perspectiva deste trabalho, informações consistem em um conjunto de dados, processados ou não, em qualquer mídia de suporte, a partir das quais se pode inferir conhecimentos (Vieira 2007). A informação é, do ponto de visa da Inteligência de Estado, o fator estratégico mais relevante se comparada aos recursos energéticos e naturais de um país.

Hoje, a informação é um importante vetor para a geração de riquezas no contexto da produção globalizada, levando à necessidade de se promover uma "gestão mais eficiente" dos seus recursos, originando a área de Segurança da Informação e das Comunicações (SIC) (Vieira 2007). Essa área é responsável por assegurar algumas das propriedades das informações institucionais, corporativas e pessoais, de forma a preservar seu valor intrínseco. Essas propriedades são:

- Disponibilidade: as informações podem ser acessadas e utilizadas por indivíduos, equipamentos ou sistemas autorizados;
- Integridade: as informações são preservadas, inclusive quanto à origem e ao destino;

- Autenticidade: as informações foram produzidas, expedidas, recebidas ou modificadas por determinado indivíduo, equipamento ou sistema;
- Confidencialidade: as informações não foram acessadas por pessoas, equipamentos ou sistemas não autorizados;
- Irretratabilidade (ou Não Repúdio): as informações estão garantidas quanto à autoria em determinadas ações, impedindo o repúdio (a negação) da mesma; e
- Legalidade (ou conformidade): as informações estão garantidas com relação a medidas legais cabíveis e aplicadas quando necessárias.

Cada vez mais, os sistemas de informação e redes de computadores são colocados à prova por diversos tipos de ameaças à segurança da informação, incluindo fraudes eletrônicas, roubo de informação, espionagem, sabotagem, vandalismo, fogo, inundação e outros acidentes. Há muito foram identificados problemas causados por vírus, *worms*, *hackers*, *crackers*, empregados insatisfeitos ou ex-empregados, programas maliciosos e ataques de negação de serviços (Nakamura e Lima 2004).

2.2 Segurança cibernética no contexto da Inteligência no Brasil

Na APF, a segurança da informação é atribuição do Gabinete de Segurança Institucional da Presidência da República (GSI/PR), que trata o tema da Segurança Cibernética no Brasil. Canongia e Mandarino Júnior (2010) propõem diretrizes para a Segurança Cibernética no Brasil, fundamentadas no arcabouço técnico-jurídico de Segurança da Informação e Comunicações e da Proteção à Infraestrutura Crítica no âmbito da APF (Canongia e Mandarino Júnior 2010).

Nesse contexto, são desenvolvidas visões técnico-estratégicas por especialistas de diferentes órgãos da APF que enriquecem e fomentam discussões e propostas de melhorias para o contexto da Segurança da Informação e reafirma a Segurança Cibernética como um desafio contemporâneo e uma função estratégica de Estado, haja vista sua relevância para a manutenção das infraestruturas críticas de um país, tais como Energia, Defesa, Transporte, Telecomunicações, Finanças e da própria Informação (Nakamura e Lima 2004).

Diante desse desafio, as nações devem estar preparadas para evitar ou minimizar ataques cibernéticos a redes e sistemas de informação de governo, bem como de todos os demais segmentos

da sociedade. O entendimento sobre a importância da segurança cibernética caracteriza-se cada vez mais como condição *sine qua non* para o seu desenvolvimento, requerendo para tanto, dentre outras ações, a promoção de diálogos e de intercâmbios de ideias, de iniciativas, de conhecimentos, de melhores práticas, para a cooperação no tema, no País e entre países.

O GSI/PR apoia-se na Abin para realizar as ações do Plano Nacional de Proteção ao Conhecimento Sensível (PNPC), que reúne e consolida resultados de avaliação das vulnerabilidades associadas aos sistemas críticos da APF e trata dos consequentes impactos à Segurança da Informação e Segurança Cibernética. A produção e representação desse conhecimento no PNPC é implementada por meio da combinação de ontologias de Gestão da Segurança da Informação e Comunicação (GSIC) e de Segurança Computacional (SC) no escopo da análise de vulnerabilidades e avaliação de risco à Infraestrutura da Tecnologia da Informação da APF.

2.3 Antecedentes históricos

Com o surgimento e a evolução das tecnologias digitais da informação, habilitou-se o acesso simultâneo a sistemas e bases de dados, com a necessidade do estabelecimento de regras para a segurança das informações e dos meios operacionais para garanti-las. Como primeira iniciativa neste sentido, a família de normas ISO/IEC 27000 abrange um conjunto de normas para Sistemas de Gestão de Segurança da Informação (SGSI) inter-relacionadas por modelos, padrões e diretivas.

O PNPC possui, dentre os seus segmentos de atuação, a proteção de sistemas de informação, tendo a ISO/IEC 27002, publicada pela Associação Brasileira de Normas Técnicas (ABNT 2013) como padrão para a realização de diagnósticos de conformidade, uma das etapas de implementação do Programa de Proteção ao Conhecimento (PPC), da Abin. Segundo Raposo (2010), várias metodologias de avaliação de risco são aplicadas aos diversos tipos de instituições parceiras do PPC, verificando a conformidade dos sistemas de TIC locais com a ISO/IEC 27002 e utilizando-se de outros métodos de extração de informações que subsidiam a avaliação de estratégia para a salvaguarda contra ameaças.

Com o surgimento do conceito de Espaço Cibernético advindo dos avanços tecnológicos, verifica-se um movimento acentuado de rearranjo das proposições das nações em termos de segurança e defesa. A Segurança Cibernética vem se caracterizando cada vez mais como uma função estratégica de Estado, essencial à manutenção e preservação das infraestruturas críticas. Por infraestruturas críticas (IC) entende-se as instalações, serviços, bens e sistemas cuja interrupção ou destruição, total ou parcial, provocará sério impacto social, econômico, político, ambiental, internacional ou à segurança do Estado e da sociedade.

No Brasil, os conceitos e as interpelações de Segurança e Defesa Cibernética, propostos pela Inteligência de Estado e Forças Singulares (Exército, Marinha e Aeronáutica), vêm sendo construídos dinamicamente. Entende-se que o escopo de atuação da Segurança Cibernética compreende não só a Segurança em Tecnologia da Informação, mas também aspectos e atitudes tanto de prevenção quanto de repressão (Brasil 2010), e que Defesa Cibernética compreende ações operacionais de combates ofensivos (Brasil 2015).

Fica evidente que a proteção efetiva das IC requer comunicação em escala mundial, coordenação e cooperação entre todas as partes interessadas. Soma-se a isso o fato de que os países desenvolvidos vêm cada vez mais tratando do tema com bastante propriedade e seriedade, notadamente após o episódio de 11 de setembro de 2001, nos Estados Unidos. Cabe acrescentar que, desde então, os resultados das ações já empreendidas fazem parte de ampla discussão que ocorre sistematicamente em fóruns internacionais.

2.4 Gestão do risco na segurança da informação e comunicação

A evolução de um modelo de segurança baseado em gestão de risco permite uma visão mais acurada do nível de segurança adequado às necessidades de uma organização, que não pode ser alcançado considerando-se apenas os aspectos da infraestrutura técnica. A organização terá uma falsa sensação de segurança se concentrar suas ações apenas nessa questão. A segurança é um problema que precisa ser considerado e tratado de forma integrada com os seus componentes estratégicos. No entanto, muitas organizações adotam uma abordagem centrada na tecnologia (Nakamura e Lima 2004).

A ISO/IEC 27002 (ABNT 2013) fornece a terminologia adotada na gestão de riscos que se constitui no processo de identificar e avaliar os riscos, reduzindo-os a um nível aceitável e implementando os mecanismos para a manutenção deste nível. Riscos de segurança da informação dizem respeito principalmente a eventos que ameaçam seus princípios básicos (integridade, disponibilidade, confidencialidade e autenticidade, irretratabilidade e conformidade). Os controles ou salvaguardas de segurança devem sempre ser adotados como consequência da avaliação dos riscos.

Segundo a ISO/IEC 27005 (ABNT 2019), os gastos com a implementação de controles de segurança precisam ser balanceados de acordo com os potenciais danos causados por possíveis falhas na segurança da informação, identificados por meio de análise e avaliação sistemática e periódica dos riscos de segurança. Nessa fase são identificadas as ameaças e vulnerabilidades dos ativos, e realizada a estimativa das probabilidades da ocorrência das ameaças e dos impactos potenciais aos negócios. Os resultados da análise e avaliação de riscos ajudam a direcionar e a determinar as ações gerenciais apropriadas e as prioridades na implementação dos controles para a proteção contra estes riscos. Na fase do tratamento de riscos são definidos os controles a serem utilizados. Estes controles podem ser escolhidos a partir da norma ISO/IEC 27002 (ABNT 2013), baseados tanto em requisitos legais como nas melhores práticas de segurança para confrontar as ameaças mapeadas.

Dois outros conceitos citados pela norma que podem ser mais bem explicitados com a ajuda da ISO/IEC Guide 73 (ABNT 2005) são ameaça, causa potencial de um incidente que pode resultar em dano para o sistema ou para a organização, e vulnerabilidade, fraqueza de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças. Quando se trata de riscos, aponta-se para o estudo das ameaças que exploram as vulnerabilidades existentes nos ativos ou sistemas e nos impactos decorrentes para os processos de negócios associados a esses ativos.

Uma redução de risco fornece subsídios para a ação conjunta dos processos de gestão da informação e de gestão do conhecimento, ambos em apoio à estratégia e à missão organizacional, que contribuem para o surgimento de uma importante propriedade emergente, a inteligência institucional, no processo de tomada de decisão (Tarapanoff 2004).

2.5 Gestão da segurança da informação e comunicações

A adoção de um modelo de GSIC não é uma tarefa simples e imediata, pois requer um conjunto de ações coordenadas, constantes e gradativas, com apoio executivo, orçamento, tecnologia e pessoas conscientizadas da sua importância. Nesse sentido, GSIC refere-se ao processo de desenvolver, implementar, direcionar e monitorar as estratégias e a atividade de segurança da organização.

A formulação de um modelo de GSIC deve ser considerada como uma ação estratégica, estabelecendo um conjunto de recursos e princípios nos quais projetos devem ser priorizados e gerenciados com o objetivo de atingir as determinações e orientações de uma política de segurança (Fernandes e Abreu 2008 p. 203).

2.6 Governança de Tecnologia da Informação vs. Gestão de Segurança da Informação e Comunicação

A Governança de Tecnologia da Informação é uma estrutura de relacionamentos e processos para dirigir e controlar uma organização na busca dos seus objetivos, adicionando valor ao mesmo tempo em que equilibra os riscos em relação ao retorno das TIC e seus processos. É responsabilidade da alta administração alinhar as estruturas organizacionais e processos de forma a garantir que as TIC sustentem e estendam as estratégias e objetivos da organização (Fernandes e Abreu 2008 p. 13-14).

Nas duas últimas décadas, vem surgindo uma série de modelos de melhores práticas de governança das TIC. Alguns desses modelos são originais e outros são derivados de outros modelos (Fernandes e Abreu 2008 p. 200-201). Dentre esses modelos destaca-se o *Project Management Body of Knowledge* – PMBOK (Project Management Institute 2008), utilizado na implantação do modelo de GSIC na APF (Britto 2008).

2.7 A proteção da infraestrutura crítica

Em um contexto no qual a interdependência entre diferentes IC é cada vez maior, a preocupação com a sua proteção tem sua relevância potencializada. Muitos países já tomaram consciência da importância da SIC, sendo que muitos deles possuem iniciativas específicas sobre o assunto, contando inclusive com órgãos governamentais responsáveis exclusivamente por essa

proteção (Canongia e Mandarino Júnior 2010). No Brasil, o GSI/PR tem a responsabilidade de promover a SIC no âmbito da APF, em consonância com os esquemas normativos internacionais dos quais é participante e colaborador.

Um ator importante na proteção da IC em nível mundial é o *Computer Security Incident Response Team* (CSIRT) que, no Brasil, tem o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança (CERT) como uma de suas instâncias. O CERT, parceiro estratégico do GSI/PR para segurança cibernética do país, é mantido pelo Comitê Gestor da Internet (CGI), organização responsável por receber, analisar e responder notificações e atuar frente a incidentes de segurança em sistemas computacionais. O CERT presta serviços para empresas, órgãos governamentais, organizações acadêmicas, para a Rede Nacional de Pesquisas (RNP) e demais instituições internacionais relacionadas a redes brasileiras conectadas à Internet.

A abordagem sob a qual a SIC é tratada varia de país para país. Grande parte dos países desenvolvidos a tratam em termos de uma IC, na qual a informação é a prioridade, o que é justificado pela variedade de serviços básicos que dependem da infraestrutura de rede.

2.8 A proteção do conhecimento na Administração Pública Federal

O PNPC realiza diagnósticos dos segmentos que o compõem (Áreas e Instalações, Documentos e Materiais, Pessoal e Sistemas de Informação), emitindo relatórios de conformidade para a instituição parceira (Raposo 2010). Especificamente no segmento das TIC, onde os saltos tecnológicos acontecem de forma sistêmica, impõe-se uma constante necessidade de atualização. Diagnósticos na instituição parceira devem acompanhar essa evolução, sob pena de o produto oferecido pelo PNPC ser inadequado ou não atender às suas expectativas. Daí a necessidade de mecanismos que propiciem uma gestão de risco e segurança cibernética adequada às IC. Visto que as áreas envolvidas muitas vezes servem-se de estruturas de conhecimento e conjuntos de terminologias distintas para conceitos similares, são necessários mecanismos que garantam a integração dessas estruturas e a interoperabilidade semântica de seus termos. Nesse sentido, a combinação de ontologias vem sendo considerada uma abordagem relevante (Abin 2019). A utilização de ontologias no contexto do PNPC cria as condições e oportunidades para a proteção

do conhecimento na APF unindo os domínios de SIC, Gestão do Risco nas IC e as necessidades de Governança de Tecnologia da Informação.

Assim, o interesse no tema SIC e IC está estruturado de forma a fornecer os conceitos e as definições para o entendimento dos modelos e das metodologias de implantação na APF. A SIC considera a Segurança da Informação como uma das áreas de conhecimento da Gestão de Tecnologia da Informação, que demanda a manutenção do valor intrínseco das informações e dos seus sistemas. Uma gestão apropriada da crescente dependência do País pelas IC justifica sua proteção no contexto da SIC. Tendo como princípio essa necessidade de proteção, a GSIC desenvolve e relaciona os vários modelos de gestão de riscos e conformidade, requisitos e metodologias que compõem a Governança de TI, o que envolve normas e padrões tais como PMBOK e ISO em uma visão totalizante voltada para o tema de confluência entre SIC e IC.

3 Ontologias

Na Ciência da Informação, assim como para a Ciência da Computação, uma ontologia é vista como a representação de um vocabulário associado a um domínio ou assunto específico (Almeida 2020 p. 23-25). Na definição clássica de Gruber (1993), ontologia é uma especificação explícita e formal de uma conceitualização compartilhada. Nessa definição, "especificação explícita" diz respeito a conceitos, propriedades, relações, funções, restrições e axiomas explicitamente definidos, "*formal*" significa ser legível e manipulável por computadores; por "*conceitualização*" entende-se que a ontologia é um modelo abstrato de um fenômeno do mundo real, e "*compartilhado*" quer dizer que ela representa um conhecimento consensual. Pode-se concluir que uma ontologia busca esclarecer uma estrutura de conhecimento. Determinado o domínio, a ontologia é um sistema de representação do conhecimento deste domínio. Para se estruturar um sistema de representação de conhecimento eficiente e seu vocabulário, é preciso realizar uma análise ontológica formal do domínio.

Uma ontologia define, assim, uma linguagem (conjunto de termos) utilizada para formular consultas (Guarino 1998). Desse modo, as ontologias se apresentam como um modelo de relacionamento de entidades em um domínio particular do conhecimento. O objetivo de sua

construção é a necessidade de um vocabulário compartilhado onde as informações possam ser trocadas e reutilizadas pelos usuários de uma comunidade, sejam eles humanos ou agentes de software. O trabalho envolvido na construção é complexo e envolve critérios e metodologias. No entanto, a possibilidade de reuso de ontologias está entre as justificativas para investimento nessa abordagem de representação do conhecimento.

O reuso de ontologias, tratado no âmbito da Engenharia de Ontologias (Keet 2020), considera algoritmos e ferramentas para o casamento de ontologias que, de acordo com Euzenat e Shvaiko (2013), podem ser integradas, mapeadas, alinhadas e combinadas. Para Mitra et al. (2000), ontologias podem também ser articuladas.

4 Materiais e métodos

Esta pesquisa descreve uma experiência inovadora da Abin em integração de ontologias e foi desenvolvida por meio da análise de registros documentais disponíveis na área de engenharia de ontologias da Agência e da observação direta em seu ambiente de projeto, particularmente daqueles relativos ao reuso de ontologias.

A análise foi contextualizada nos princípios da Arquitetura da Informação, conforme concebidos por Lima-Marques (2005), e utilizou o marco teórico da engenharia de ontologias, em especial da sua integração, levantado por meio de busca bibliográfica na literatura disponível. Para operacionalizar a análise, foi adotado o tratamento qualitativo proposto por Swenson e Hughes (2006). Esses autores propõem uma abordagem metodológica baseada na Teoria Fundamentada em Dados de Charmaz (2009), assim como nas técnicas de modelagem de Strauss e Corbin (2008).

Como fontes de dados foram utilizados os projetos de ontologias da Abin e analisados sistemas específicos usados para tratamento de ontologias. O tratamento das informações levantadas seguiu uma abordagem qualitativa, com a identificação de técnicas e procedimentos e o desenvolvimento do modelo, ambas iniciativas vinculadas à Teoria Fundamentada nos Dados. Os procedimentos de análise permitiram a criação do modelo pela identificação dos conceitos, propriedades e dimensões a partir dos dados.

5 Resultados e análises

Esta seção apresenta um extrato da combinação de duas ontologias, a primeira relativa à Segurança Computacional (OntoSeC) e a outra na área de Gestão de Risco à Informação (InfoSecRM). A ontologia resultante constitui-se em um instrumento de apoio à decisão quanto à proteção da IC da APF.

5.1 Ontologias no âmbito do plano nacional de proteção ao conhecimento

A aquisição e a representação de conhecimento por meio de ontologias são um importante elo entre a Ciência da Informação, em particular a Arquitetura da Informação, e a Ciência da Computação (Lima-Marques 2005). Da confluência entre essas áreas surgem contribuições que facilitam tanto a comunicação como o processamento da informação e do conhecimento em nível semântico para a Inteligência e a Contrainteligência (Sfetcu 2019; Kul e Upadhyaya 2015).

No nível epistemológico, a obtenção do conhecimento no escopo do PNPC considera os princípios de viabilidade e de oportunidade dessa aquisição apregoados pela Doutrina da Atividade de Inteligência e envolve a proteção desse conhecimento (Abin 2016). No nível científico, a aquisição e representação do conhecimento no contexto da Inteligência contemplam a etnografia e a pesquisa fundamentada nos dados para selecionar as melhores ferramentas e métodos (Afonso 2006; Fernandes e Abreu 2008; Leite 2014; Whetten 2003). Do ponto de vista técnico e instrumental, as atividades de Inteligência e Segurança Cibernética oferecem ao PNPC a oportunidade de explorar o expressivo volume e o ineditismo de suas informações para subsidiar o processo decisório da APF (Leite 2014; Roratto 2012; Patrício 2005).

No contexto dos Sistemas de Recuperação de Informação (SRI), a organização e a extração de informações são condicionadas à tecnologia associada. Atualmente, fontes de dados de todos os tipos têm proliferado com a disponibilização de informações em rede, principalmente na Web. Entretanto, a recuperação dos conteúdos informativos muitas vezes não é realizada de forma satisfatória devido à falta de ferramentas de acesso adequadas que viabilizem, por exemplo, o controle terminológico, o que pode remeter ao uso de ontologias de domínio (Campos 2005; Campos 2007).

O uso de ontologias envolve iniciativas de integração de sistemas e de bases de dados, não só para uma maior compatibilização de dados, mas também para agregar iniciativas de descrição e recuperação de serviços e recursos para a descoberta de conhecimento (Campos 2005; Campos 2007). No entanto, ainda hoje vale a observação de Campos (2007) também quanto à escassez de ferramentas semânticas voltadas para a construção e uso de ontologias.

A recuperação da informação dirigida por ontologias vem norteando os trabalhos do SISBIN, consideradas as diretrizes de recuperação da informação e extração de conhecimento do PNPC (Abin 2019). No contexto da segurança da informação e proteção da infraestrutura crítica da APF, o PNPC vem se servindo, entre outras, da Ontologia de Segurança Computacional (OntoSeC) e da Ontologia da Gestão de Risco à Informação (InfoSecRM).

5.1.1 Ontologia de Segurança Computacional – OntoSeC

OntoSeC é voltada para a estruturação da informação e recuperação de conhecimento no campo da Segurança Computacional (Martimiano 2006). É uma contribuição ao CSIRT em apoio a ações de recepção, revisão e resposta a incidentes de segurança da informação. Em função desse trabalho, a partir de 2008, o PNPC passa a considerar ontologias de segurança computacional no tratamento e integração dos domínios de SIC, análise de risco, governança de TI e conformidade. O objetivo é a proteção do conhecimento relativo à infraestrutura da TI na APF, vista como crítica e estratégica para a defesa nacional (Canongia e Mandarino Júnior 2010).

Como uma ontologia reflete uma visão humana de um domínio de conhecimento, se aquele que a utiliza muda sua interpretação a respeito de um determinado conceito ou relacionamento, a ontologia deve incorporar essa mudança. Caso contrário, essa mudança de interpretação pode tornar a ontologia inconsistente, invalidando relacionamentos ou conceitos que deixam de existir no mundo real. É importante dizer que nenhuma ontologia é completa ou totalmente correta, mas deve ser validada constantemente frente a requisitos estabelecidos. Esses foram os fundamentos que Martimiano (2006) utilizou para a produção da OntoSeC.

As seguintes definições foram assumidas por Martimiano (2006) para o desenvolvimento da OntoSeC:

- Domínio: “incidentes de segurança em sistemas computacionais”;

- Objetivo principal: “estabelecer uma estrutura única para representar informações sobre incidentes de segurança, possibilitando relacionar esses incidentes”;
- Usuários: “administradores de segurança e ferramentas de auxílio ao gerenciamento de segurança, como IDS (*Intrusion Detection Systems*) e firewalls”;
- Tarefas: aquelas descritas e definidas pelas metodologias Methontology (Fernandez-Lopez et al. 1997) e 101 (Noy e McGuinness 2001), como, por exemplo, definição e hierarquização de classes; e
- Recursos: “ferramenta computacional para modelar a ontologia, linguagem para formalizá-la e recursos humanos para o processo de desenvolvimento”.

Foram, então, identificadas e analisadas as diversas fontes de incidentes de segurança. Dois principais dicionários foram utilizados: Glossary of Computer Security (Russell e Gangemi 1991) e Request for Comments RFC2828-Internet Security Glossary (Shirey 2000). Foi também utilizada a taxonomia de Howard (1997) para a análise de incidentes de segurança e as informações de segurança gerenciadas pelo CERT para a definição de alguns dos tipos de incidentes que a OntoSeC representa.

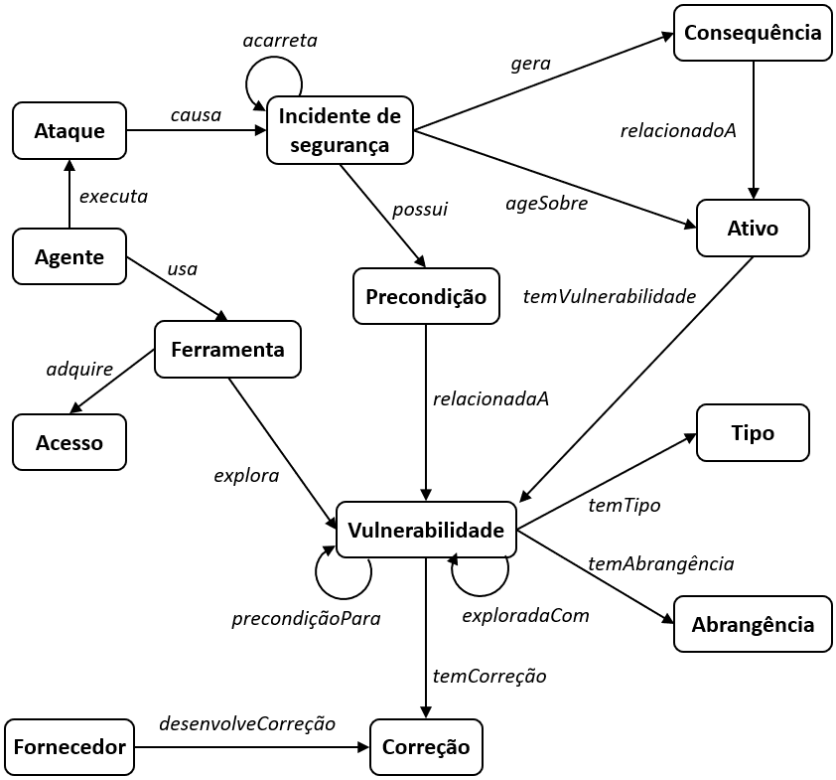
As questões de competência da OntoSeC, ou seja, as perguntas que ela deveria responder foram:

- Quais os tipos de incidentes mais frequentes?
- Quais as consequências de um determinado incidente?
- Quais as pré-condições para a ocorrência de um determinado incidente?
- Que ativos do sistema podem ser alvos de um incidente?
- Que ativos são mais atacados e sofrem incidentes?
- Que ferramentas são utilizadas para executar um ataque?
- Que tipos de acesso são utilizados para se realizar um ataque?
- Quais os tipos de ataques mais comuns?
- Que incidentes precedem ou antecedem um incidente?

- Quais as possíveis correções de uma vulnerabilidade?
- Quais os tipos de vulnerabilidade mais frequentes?
- Quais as vulnerabilidades de um ativo?
- Que vulnerabilidades são exploradas em conjunto?
- Que vulnerabilidades são exploradas durante um incidente?
- Que vulnerabilidades são precondições para outra vulnerabilidade?
- Em que período ocorrem mais incidentes?

Parte significativa dos conceitos de mais alto nível da OntoSeC e suas relações podem ser descritos da seguinte forma: um *Agente* executa um *Ataque* que pode causar um *Incidente de Segurança*. Para executar ataques, um *Agente* pode explorar uma *Vulnerabilidade* com uma *Ferramenta* e adquirir *Acesso* a um sistema. Um *Incidente de Segurança*, por sua vez, gera uma *Consequência*, age sobre um *Ativo* e possui uma *Precondição*. Essa *Precondição* pode estar relacionada a uma *Vulnerabilidade*. Uma *Consequência* pode ainda estar relacionada a um *Ativo*. Além disso, um *Incidente de Segurança* pode ocorrer antes ou após outros incidentes. Uma *Vulnerabilidade* em um *Ativo* é caracterizada por uma *Abrangência* e um *Tipo*, e envolve uma *Correção*. Uma *Correção* é realizada pela Gestão da Segurança da Informação (*Fornecedor* da correção). Uma *Vulnerabilidade* pode ainda se relacionar com outras vulnerabilidades quando esta for *Precondição* para que outra seja explorada, ou uma *Vulnerabilidade* é explorada em conjunto com outras. A Figura 1 representa essas relações conceituais. A partir dessa estrutura conceitual básica, a OntoSeC pode ser especializada. A abordagem utilizada para esse processo foi a *middle-out*, proposta por Uschold e Gruninger (1996). Ou seja, à medida que surge a necessidade, a ontologia tem alguns de seus conceitos incorporados a superclasses ou especializados em subclasses.

Figura 1 – Fragmento da ontologia OntoSeC



Fonte: os autores

5.1.2 Ontologia da Gestão de Risco à Informação – InfoSecRM

InfoSecRM (Gualberto 2012) é uma ontologia para compartilhamento e estruturação dos processos e conceitos na área de Gestão de Riscos à Segurança da Informação. Essa ontologia foi adequada e incorporada à prática do PNPC que, desde 2010, desenvolvia uma metodologia de análise de riscos para a APF, em particular para tratar de vulnerabilidades da TI no contexto da APF. No DSIC/GSI, essa iniciativa foi incorporada à Segurança Cibernética na APF (Canongia e Mandarino Júnior 2010; Albuquerque e Andrade 2014).

A estrutura da InfoSecRM considera a arquitetura das informações no domínio da Segurança da Informação sob a ótica de Schumacher (2003). Para ele, a segurança da informação direcionada apenas a engenheiros e especialistas em segurança não atende às necessidades de segurança da Internet. São propostos cenários que refletem questões de segurança relevantes para os níveis empresarial, arquitetônico e operacional. O objetivo é apoiar o compartilhamento e o processamento do conhecimento no domínio da segurança da informação. Com isso, podem-se

estabelecer representações semânticas passíveis de serem processadas pelos agentes relacionados ao contexto, facilitando não só o compartilhamento e aquisição de conhecimento sobre este domínio, mas também a institucionalização dos processos gerenciais envolvidos no plano estratégico (Albuquerque e Andrade 2014). A InfoSecRM descreve o conhecimento relacionado ao processo de gestão de riscos de segurança da informação nos moldes do que preconiza a norma ISO/IEC 27005.

Na elaboração da InfoSecRM foram utilizadas três abordagens: (1) a metodologia Methontology (Fernández-Lopez et al. 1997), como o processo que define o arcabouço das atividades a serem realizadas; (2) o método 101 (Noy e McGuiness 2001), que define "como fazer'' algumas destas atividades (na conceituação, por exemplo); e (3) os princípios, métodos e aplicações de validação propostos por Uschold e Gruninger (1996), com a utilização de cenários de motivação e com a definição de questões de competência.

Na fase de planejamento e especificação da InfoSecRM, foram definidas as atividades, os recursos a serem utilizados, o escopo e os objetivos. Para isso, foram elencados os seguintes cenários:

- O conhecimento em segurança da informação deriva de diversas fontes e é uma conceitualização que representa os conceitos inerentes a este domínio de forma padronizada e que pode facilitar o compartilhamento deste conhecimento em ambientes corporativos;
- A Gestão de Riscos de Segurança da Informação (GRSI) é um dos principais elementos em um processo de GSI; neste contexto, uma ontologia que permita operar sobre os conceitos e atividades deste tipo de processo pode auxiliar a identificação das necessidades e prioridades de segurança da informação de uma organização;
- A utilização de processos padronizados para a gestão de riscos, como o proposto pela família de normas ISO/IEC 27000, auxilia no mapeamento dos conceitos e atividades relevantes a serem descritas pela conceitualização proposta pela ontologia.

A partir destes cenários foram definidos:

- Domínio: especificamente a GRSI, porém, como este processo está inserido em um domínio maior, de forma pontual descreve-se também a GSI;
- Objetivo: estabelecer uma estrutura de representação para informações e atividades relacionadas à GRSI;
- Usuários: responsáveis pela segurança da informação e tecnologia da informação em organizações, e estudiosos e especialistas neste domínio;
- Tarefas: aquelas indicadas pelas três metodologias utilizadas (Fernandez-Lopez et al. 1997; Noy e McGuiness 2001; Uschold e Gruninger 1996);
- Recursos: o framework Protégé (Musen 2015), a máquina de inferência Pellet (Sirin et al. 2007), as linguagens OWL-DL, RDF e SPARQL (Motik et al. 2009; Prud'hommeaux e Seaborne 2008), e as normas da família ISO/IEC 27000.

A aquisição do conhecimento relacionado ao domínio escolhido foi feita a partir de bibliografia técnico-científica, padrões e glossários de termos, sobretudo das normas da família ISO 27000. Além dessas fontes, o conhecimento representado pela ontologia recebeu contribuições de especialistas em GSIC.

Além das pesquisas realizadas para o desenvolvimento da InfoSecRM, houve atividades que contemplaram a elaboração das seguintes questões de competência:

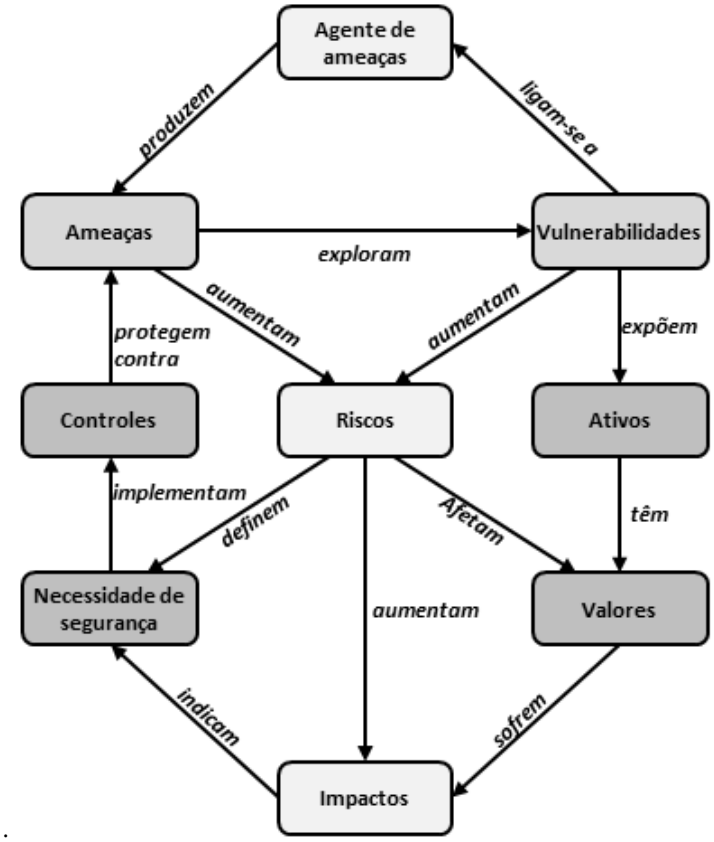
- Quais os riscos de nível alto a que uma organização está sujeita?
- Que cenários de incidentes de segurança da informação, caso se concretizem, podem impactar na reputação da organização?
- Qual o perfil de riscos de segurança da informação de uma organização?
- Qual a probabilidade de ocorrência de um cenário de incidente de segurança da informação?
- Qual o nível de impacto de um cenário de incidente de segurança da informação?

5.2 Combinação de ontologias no contexto de proteção do conhecimento de inteligência

A proteção do conhecimento de Inteligência e salvaguarda das IC nacionais é atribuição estratégica da Abin que, por meio do PNPC, realiza o PPC. O PPC procura disponibilizar o conhecimento para antecipar fatos, situações e relações de causa e efeito na identificação de ameaças e oportunidades que possam impactar a segurança do Estado e da sociedade brasileira. Essa ação tática configura-se em diretivas técnicas e legais para a elaboração de projetos e recomendações sobre como agir frente aos fatores adversos estrangeiros ou internos. O CEPESC é instrumentalizado pela elaboração de criptografia de estado e ontologias para a prospecção e proteção do conhecimento de Inteligência. O CEPESC desenvolve ontologias próprias no âmbito da prospecção de conhecimento da Inteligência e da proteção ao conhecimento na Contrainteligência e, servindo-se de técnicas e ferramentas de engenharia de ontologias, reusa as ontologias elaboradas pelos parceiros do SISBIN.

Por meio da engenharia de ontologias, o CEPESC realiza uma avaliação de riscos e vulnerabilidades que aponta elementos de segurança e proteção a serem incorporados nos sistemas de TI considerados críticos para a Segurança Cibernética. A combinação das ontologias proporciona oportunidade e qualidade na obtenção do conhecimento de Inteligência, tanto pela reunião de fragmentos isolados de informação como, principalmente, pela eliminação de conflitos semânticos do conhecimento obtido também pelos parceiros do SISBIN em cenários de Inteligência e Contrainteligência. A Figura 2 representa o modelo mental da ontologia resultante da combinação das ontologias InfoSecRM e OntoSeC. Os conceitos em tons claro, escuro e médio são oriundos das ontologias OntoSeC, InfoSecRM e da combinação entre elas, respectivamente. Esta combinação mostra-se efetiva como apoio ao processo decisório estratégico da Inteligência ao reunir conhecimentos de gestão da informação e de proteção para a IC distribuídos de forma não homogênea na APF. Daí a relevância de metodologias para a combinação de ontologias que contemplem a abordagem doutrinária da Inteligência e da Contrainteligência. Ressalta-se o ganho com o conjunto de diretivas relacionadas à segurança e proteção ao conhecimento obtido pelo processo de combinação das ontologias originais.

Figura 2 – Modelo mental da ontologia combinada



Fonte: os autores

A Engenharia de Ontologias, e mais especificamente a combinação de ontologias, é uma das formas com as quais o CEPESC promove, no âmbito do SISBIN, a proteção de IC da APF no contexto da Segurança Cibernética.

6 Conclusões

Este artigo relata a experiência de reuso de ontologias, como uma estratégia de gestão da proteção do conhecimento institucional, na perspectiva da Inteligência de Estado e no contexto da Segurança da Informação e Comunicação. Várias metodologias e ferramentas de Engenharia de Ontologias vêm sendo utilizadas para a combinação de ontologias na obtenção de dados negados e na proteção do conhecimento no âmbito do CEPESC.

A combinação de ontologias no contexto do PNPC vem fornecendo, em um ambiente cooperativo e compartilhado, uma estrutura formal e padronizada para a representação de informações e conhecimentos na Segurança da Informação e Comunicação, habilitando a proteção da infraestrutura de TI da APF. A produção de conhecimento com orientação à combinação de ontologias e foco em informações relevantes resulta em conhecimento com significativo ganho potencial para apoio ao processo decisório de mais alta ordem (estratégico) em relação à visão muitas vezes fragmentada da ação operacional de Inteligência. O esforço em compatibilizar a terminologia dos sistemas e a geração de conhecimento emergente a partir de ontologias legadas podem auxiliar em situações como:

- Criação de cenários para ação usando-se uma estrutura sem os conflitos semânticos das ontologias fragmentadas;
- Utilização destes cenários para a obtenção de uma visão estratégica para a proteção do conhecimento e das IC; e
- Implementação de um conjunto de instrumentos para apoiar o processo decisório na escolha de cursos de ação a partir da avaliação de resultados potenciais.

Com isto, são agregadas melhorias na comunicação entre os especialistas comprometidos com a gestão e tratamento dos riscos e no tempo de resposta tático-operacional naqueles cenários adversos para a IC da APF, podendo induzir novas políticas ou aprimorar os controles técnicos e de gestão. Do ponto de vista estratégico, a Engenharia de Ontologias mostra-se um meio para se aproveitar oportunidades e reduzir ameaças, auxiliando a Inteligência de Estado nas atividades de construção do seu conhecimento estratégico. Destaca-se também o ganho do ponto de vista cognitivo e metodológico obtido pelo trabalho colaborativo na gestão do conhecimento para a Inteligência de Estado no SISBIN, em particular no desenvolvimento de outras ontologias em domínios correlatos.

O caráter inovador da proposta relaciona-se com a oferta de resposta inédita à necessidade de reuso de ontologias em nível conceitual e em grau de aproximação para as necessidades da engenharia de ontologias.

Referências

Afonso, L. S. “Fontes abertas e inteligência de estado”. *Revista Brasileira de Inteligência*, vol. 2, no. 2, 2006, pp. 49-62.

Agência Brasileira de Inteligência. *Atividade de inteligência no Brasil*. Abin, 2019.

Agência Brasileira de Inteligência. *Doutrina Nacional da Atividade de Inteligência*: fundamentos doutrinários. Abin, 2016.

Albuquerque, C. E. P., e Andrade, F. S. “O emprego da análise de risco como ferramenta de inteligência estratégica”. *Revista Brasileira de Inteligência*, vol. 4, no. 2, 2014, pp. 107-121.

Almeida, M. B. *Ontologia em Ciência da Informação:* teoria e método. Editora CRV, 2020.

Associação Brasileira de Normas Técnicas. *ISO Guia 73 – Gestão de riscos – Vocabulário – Recomendações para uso em normas*: NBR ISO/IEC Guide 73. ABNT, 2005.

Associação Brasileira de Normas Técnicas. *NBR ISO/IEC 27002 – Tecnologia da informação – Técnicas de segurança – Código de prática para controles de segurança da informação*. ABNT, 2013.

Associação Brasileira de Normas Técnicas. *NBR ISO/IEC 27005 – Tecnologia da informação - Técnicas de segurança – Gestão de risco da segurança da informação*. ABNT, 2019.

Balué, I. G., e Nascimento, M. S. O. “Proteção do conhecimento: uma questão de Contrainteligência de Estado”. *Revista Brasileira de Inteligência*, vol. 2, no. 3, 2006, pp. 93-94.

Brasil. Ministério da Defesa. *Glossário das Forças Armadas*. 5 ed., Ministério da Defesa, 2015.

Brasil. Presidência da República. *Estratégia Nacional de Inteligência*. Gabinete de Segurança Institucional, 2017.

Brasil. Presidência da República. “Livro verde: segurança cibernética no Brasil”. *Gabinete de Segurança Institucional*, org. por R. Mandarino Junior e C. Canongia, 2010.

Britto, A. C. P. *Estudo do gerenciamento de projeto baseado no PMBOK para a implantação da Gestão da Segurança da Informação e Comunicação na Administração Pública Federal*, 2008. Universidade de Brasília, Monografia de Especialização.

Campos, M. L. A. “A problemática da compatibilização terminológica e a integração de ontologias: o papel das definições conceituais”. *Anais do 6º Encontro Nacional de Pesquisa em Ciência da Informação*: Florianópolis, ENANCIB, 2005.

Campos, M. L. A. “Integração de ontologias: o domínio da Bioinformática”. *Revista Eletrônica de Comunicação, Informação & Inovação em Saúde*, vol. 1, no. 1, 2007, pp. 117-121.

Canongia, C., e Mandarino Júnior, R. "Segurança cibernética: o desafio da nova sociedade da informação". *Parcerias Estratégicas*, vol. 14, no. 29, 2010, pp. 21-46.

Charmaz, K. *Construção da Teoria Fundamentada:* guia prático da análise qualitativa. Artmed, 2009.

Euzenat, J., and Shvaiko, P. *Ontology Matching*. Springer, 2013.

Fernandes, A. A., e Abreu, V. F. *Implantando a governança de TI:* da estratégia à gestão dos processos e serviços. 2 ed., Brasport, 2008.

Fernández-López, M., et al. "METHONTOLOGY: from ontological art towards ontological engineering". *Proceedings of the Spring Symposium Series on Ontological Engineering*: Palo Alto, AAAI, 1997.

Ferreira, F. G. *Um framework de alinhamento ontológico entre a TI e o negócio de uma organização*. Universidade de Brasília, Dissertação de Mestrado, 2007.

Gruber, T. R. "A translation approach to portable ontology specifications". *Knowledge Acquisition*, vol. 5, no. 2, 1993, pp. 199-220.

Gruber, T. R. "Ontology". *Encyclopedia of Database Systems*. Edited by L. Liu and M. T. Özsu. Springer-Verlag, 2009. pp. 1963-1965.

Gualberto, E. S., et al. "InfoSecRM: uma abordagem ontológica para a gestão de riscos de segurança da informação". *Revista Brasileira de Sistemas de Informação*, vol. 6, 2012, pp. 30-43.

Guarino, N. "Formal ontology in information systems". *Proceedings of the First International Conference in Formal Ontology in Information Systems*: Trento, IOS Press, 1998.

Guarino, N. "The ontological level". *Philosophy and the Cognitive Science*. Organized by R. Casati, et al. Holder-Pivhler-Tempsky, 1995.

Howard**,** J. D. *An analysis of security incidents on the internet: 1989-1995*, 1997. Carnegie Mellon University, PhD Thesis.

Keet, C. M. *An introduction to ontology engineering*. 2020, https://people.cs.uct.ac.za/~mkeet/files/OEbook.pdf. Acessado 14 set. 2021.

Klein, M. "Combining and relating ontologies: an analysis of problems and solutions". *17th International Join Conference on Artificial Intelligence*: Seattle, AAAI, 2001.

Kul, G., and Upadhyaya, S. "Towards a cyber ontology for insider threats in the financial sector". *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, vol. 6, 2015, pp. 64-85.

Leite, S. S. "O emprego das fontes abertas no âmbito da atividade de inteligência policial". *Revista Brasileira de Inteligência*, vol. 5, no. 1, 2014, pp. 11-45.

Lima-Marques, M. *Ontologias:* contribuição à arquitetura da informação. Editora Thesaurus, 2005.

Martimiano, L. A. F. *Sobre a estruturação de informação em sistemas de segurança computacional: o uso de ontologias*. Universidade de São Paulo, Tese de Doutorado, 2006.

Mitra, P., et al. "A Graph-Oriented Model for Articulation of Ontology Interdependencies". *Lecture Notes in Computer Science*, v. 1777, Springer, 2000.

Motik, B., et al. *OWL 2 Web Ontology Language: Structural Specification and Functional-Style Syntax*, 2009, http://www.w3.org/TR/owl2-syntax. Acessado 14 ago. 2020.

Musen, M. A. "The Protégé Project: a look back and a look forward". *AI Matters*, vol. 1, no. 4, 2015, pp. 4-12.

Nakamura, E. T., e Lima, M. B. *Estratégia de proteção da infraestrutura crítica da informação*. 2 ed., Novatech, 2004.

Noy, N. F., e McGuinness, D. L. *Ontology Development 101: A guide to creating your first ontology*. Knowledge Systems Laboratory, 2001.

Patrício, J. S. "A representação do conhecimento de inteligência". *Revista Brasileira de Inteligência*, no. 6, 2005, pp. 47-53.

Probst, G., et al. "Preservando o conhecimento". *Gestão do conhecimento: os elementos construtivos do sucesso*. Editado por G. Probst, Bookman, 2002, pp. 175-193.

Project Management Institute. *Um guia do conjunto de conhecimentos do gerenciamento de projetos*. PMI, 2008.

Prud'hommeaux, E., e Seaborne, A. *SPARQL Query Language for RDF*, 2008, http://www.w3.org/TR/rdf-sparql-query. Acessado 04 nov. 2020.

Raposo, A. C. *Metodologia para diagnóstico de segurança em sistemas de informação*. Abin, 2010.

Roratto, J. M. "Acepções e conceitos de inteligência de estado". *Revista Brasileira de Inteligência*, no. 7, 2012, pp. 31-40.

Russell, D., and Gangemi, G. T. *Computer security basics*. O'Reilly Media Inc., 1991.

Schumacher, M. *Security engineering with patterns:* origins, theoretical models, and new applications. Springer, 2003.

Sfetcu, N. *Ontology of intelligence*, PhilArchive, 2019. doi:10.13140/RG.2.2.25163.54569. Acessado 20 out. 2020.

Shirey, R. *Internet Security Glossary*. Internet Engineering Task Force (IETF), 2000, https://datatracker.ietf.org/doc/rfc2828. Acessado 11 out. 2020.

Sirin, E., et al. “Pellet: A Practical OWL-DL Reasoner”. *SSRN Electronic Journal*, 2007. doi:10.2139/ssrn.3199351. Acessado 12 jan. 2021.

Strauss, A. L., e Corbin, J. *Pesquisa Qualitativa:* Técnicas e Procedimentos para o Desenvolvimento de Teoria Fundamentada. Artmed, 2008.

Swenson, R. G., e Hughes, F. J. *Projeto de Pesquisa*. Abin, 2006.

Tarapanoff, K. “Inteligência social e inteligência competitiva”. *Encontro Bibli: Revista Eletrônica de Biblioteconomia e Ciência da Informação*, vol. 9, no. 1, 2004, pp. 11-26.

Uschold, M., e Gruninger, M. “Ontologies: principles, methods and applications”. *The Knowledge Engineering Review*, vol. 11, no. 2, 1996, pp. 93-136.

Vieira, T. M. *Direito à privacidade na sociedade da informação*. Sergio Antonio Fabris Editor, 2007.

Whetten, D. A. “Desenvolvimento de teoria. O que constitui uma contribuição teórica?”. *Revista de Administração de Empresas*, vol. 43, no. 3, 2003, pp. 69-73.

Dados da pesquisa

Devido à natureza do trabalho, não há dados da pesquisa a serem compartilhados.

Received: 16/07/2021 Accepted: 07/10/2021