RICI Revista Ibero-Americana de Ciência da Informação

ISSN 1983-5213

Ciber Proteção:

a segurança dos sistemas de informação no espaço cibernético

Eduardo Wallier Vianna
eduardowallier@hotmail.com

Renato Tarciso Barbosa de Sousa
Universidade de Brasília, Faculdade de Ciência da Informação, Brasília, DF, Brasil
renasou@unb.br

Resumo: Os avanços dos meios de comunicação da informação e a inovação tecnológica colocam a sociedade, dita globalizada, com responsabilidades desafiadoras no que tange à segurança na era digital. O estudo pretende discutir a segurança da informação no espaço cibernético de interesse nacional, buscando, assim, contribuir com a otimização das medidas de salvaguarda dos sistemas de informação governamentais e dos ativos de informação nas infraestruturas críticas estratégicas. Considera-se que as atividades inerentes à proteção cibernética estão imbricadas no escopo abrangente e multidisciplinar da Ciência da Informação. Ressalta-se, ainda, a importância do ciberespaço no contexto de um Estado-Nação, assim como a necessidade de a proteção cibernética atuar em rede, por meio de ações colaborativas interagências e do trabalho cooperativo. Dentre as contribuições possíveis, propõe-se o conceito de Ciber Proteção construído a partir da Teoria do Conceito de Ingetraut Dalhberg. Considera-se a Ciber Proteção inserida no contexto da Soberania Nacional, bem como alinhada à complementariedade matricial das atividades de segurança com as ações de defesa no ciberespaço. Consolida, no contexto da Ciber Proteção, de forma gráfica, o relacionamento entre segurança, preservação, sistemas e ativos de informação digital com a defesa cibernética e as infraestruturas críticas.
Palavras-chave: Ativos de informação; Ciberespaço; Defesa cibernética; Infraestruturas críticas estratégicas; Segurança cibernética; Segurança da Informação.

ARTIGOS

Cyber Protection: the security of information systems on the cybernetic space
Abstract: The advances of information media and technological innovation put the globalized society the challenging responsibilities about security in the digital age. The study aims to contribute to the necessary optimization of information security in cyberspace, as well as the protection of systems and information assets in the national strategic infrastructure. It is considered that the activities related to cyber security are embedded in the comprehensive and multidisciplinary context of Information Science. It is emphasized also the importance of cyberspace in the strategic context of national defense and the necessity of cyber protection act in a network through collaborative action interagency and the cooperative work. Among the possible contributions, we propose the concept of Cyber Protection or Cybersecurity Protection as part of the Information Science and built on the theory of Ingetraut Dalhberg Concept. It is considered the Cyber Protection into the context of Sovereignty National, as well as aligned with the matricial complementarity of security activities with defense actions in cyberspace. Consolidates graphically the relation between information security, cyber defense and the strategic infrastructure to cyber protection.
Keywords: Cyberspace; Cyber defense; Cyber security; Information assets; Information security; National critical infrastructure.

Ciber protección: la seguridad de los sistemas de información en el espacio cibernético
Resumen: Los avances de los medios comunicacionales de la información y la innovación tecnológica colocan a la sociedad, dicha globalizada, con responsabilidades y desafíos en el que se refiere a la

seguridad en la era digital. El estudio pretende discutir la seguridad de la información en el espacio cibernético de interés nacional, busca así, contribuir con la optimización de las medidas de salvaguarda de los sistemas de información gubernamentales y de los activos de información en las infraestruturas críticas estratégicas. Se considera que las actividades inherentes a la protección cibernética están vinculadas en el enfoque amplio y multidisciplinar de la Ciencia de la Información. Se resalta, aún, la importancia del ciberespacio en el contexto de un Estado-Nación, así como la necesidad de la protección cibernética activa en red, por medio de acciones colaborativas inter-agencias y de trabajo cooperativo. De entre las contribuciones posibles, se propone el concepto de ciber protección construido a partir de la teoría del concepto de Ingetraut Dalhberg. Se considera la ciber protección insertada en el contexto de la Soberanía Nacional, así como alineada a complementar la matriz de la actividad de seguridad con la acción de defensa en el ciberespacio. Consolida, en el contexto de la ciber protección, de forma gráfica, la relación entre seguridad, preservación, sistemas y activo de información digital con la defensa cibernética y las infraestructuras críticas.
Palabras clave: Activo de información; Ciberespacio; Defensa cibernética; Infraestructuras críticas estratégicas; Seguridad cibernética; Seguridad de la información.

1 Introdução

Este artigo pretende discutir a segurança da informação no espaço cibernético de interesse nacional, buscando, assim, contribuir com a otimização das medidas de salvaguarda dos sistemas de informação governamentais e dos ativos de informação nas infraestruturas críticas estratégicas.

O presente trabalho propõe o conceito de Ciber Proteção no âmbito da Ciência da Informação, inserido no espectro da Soberania e da Defesa Nacional, bem como alinhado à complementariedade matricial das atividades de segurança com as ações de defesa cibernética.

A estratégia metodológica, deste estudo exploratório, teve início com a pesquisa documental no contexto da denominada era digital, particularmente, sobre ciberespaço, gestão dos documentos, preservação digital, segurança da informação e defesa nacional. Em segundo momento, fez-se uso de evidências coletadas por meio de observação participante junto às atividades desenvolvidas pelo Centro de Tratamento de Incidentes de Segurança de Redes de Computadores da Administração Pública Federal (CTIR Gov) da Presidência da República, no período de 2008 a 2012; pelo Centro de Defesa Cibernética (CDCiber) do Ministério da Defesa, durante a realização dos Grandes Eventos internacionais ocorridos entre 2012 e 2014 no Brasil e pela Rede Nacional de Segurança da Informação e Criptografia (RENASIC) de 2015 a 2016. Finalizando, utilizou-se como modelo a Teoria do Conceito de Ingetraut Dalhberg para estruturar a análise qualitativa dos dados levantados e compor o conceito de Ciber Proteção (proteção cibernética).

Os avanços dos meios de comunicação da informação e a inovação tecnológica parecem colocar a sociedade, dita globalizada, com responsabilidades desafiadoras, no que tange à segurança das informações. Especialmente quando se trata das informações inerentes ao contexto do ciberespaço ou espaço cibernético, ou seja, aquelas produzidas e armazenadas nos

sistemas de informação automatizados ou que trafegam em redes de dados locais e pela Internet. Em 2016, o foco do Fórum Econômico Mundial (World Economic Forum - WEF) foi a denominada "4ª Revolução Industrial", que vem causando profundas consequências políticas, econômicas e sociais na era digital[1], devido à maneira peculiar de compartilhar, analisar e processar as informações baseadas na acelerada e "irreversível" interconectividade global.

O Brasil está inserido nos desafios e oportunidades desse contexto, como acenou, em 2015, a Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética (ESIC), da Administração Pública Federal (APF):

> o cenário de uso da Internet e, consequentemente, de uso das Tecnologias de Informação e Comunicação (TIC) permanece crescente e sem dúvida além de qualquer expectativa e prospecção, operando-se em cifras bastante expressivas no mundo e no País, especialmente frente aos avanços do uso de dispositivos móveis, da computação em nuvem e da evolução da chamada "internet das coisas" (BRASIL, 2015).

Como exemplo de expansão no uso, Levantamentos de Governança de Tecnologia da Informação realizados pelo Tribunal de Contas da União (TCU), realizados no âmbito da APF, vêm registrando um crescimento significativo do número de organizações governamentais que têm disponibilizado aos cidadãos um volume cada vez maior de acervo de páginas, documentos, dados, aplicações e serviços *on-line* via Internet, passando o percentual de 49%, em 2012, para 88%, em 2014 (BRASIL, 2014).

Tal crescimento parece ser aderente à Política de Governança Digital[2], instituída no início de 2016, onde se destacam os seguintes princípios e diretrizes:

> a) priorização e oferta de serviços públicos disponibilizados em meio digital para o maior número possível de dispositivos e plataformas;
>
> b) autosserviço [3] como a forma prioritária de prestação de serviços públicos disponibilizados;
>
> c) disponibilização de dados em formato aberto, amplamente acessível e utilizável por pessoas e máquinas;
>
> d) garantia à segurança e à privacidade [grifo nosso] (BRASIL, 2016).

Não obstante os benefícios do uso intensivo das Tecnologias de Informação (TI), o Relatório final da Comissão Parlamentar de Inquérito, denominada CPI da Espionagem, apontou

[1]Disponível em <http://www.segs.com.br/info-ti/2677-privacidade-de-dados-dominou-discussao-sobre-4-revolucao-industrial-no-forum-economico-mundial-de-2016-em-davos.html>. Acesso em: 11 mar. 2016.

[2] Governança digital: utilização pelo setor público de recursos de tecnologia da informação e comunicação com o objetivo de melhorar a disponibilização de informação e a prestação de serviços públicos, incentivar a participação da sociedade no processo de tomada de decisão e aprimorar os níveis de responsabilidade, transparência e efetividade do governo (BRASIL, 2016).

[3] Serviço público disponibilizado em meio digital que pode ser utilizado pelo próprio cidadão, sem auxílio do órgão ou da entidade ofertante do serviço (BRASIL, 2016).

fragilidades do Brasil diante da espionagem eletrônica internacional, evidenciando a vulnerabilidade do sistema de telecomunicações brasileiro. O denominado "caso Snowden" (nome do delator do esquema de monitoramento - Edward Snowden) revelou o *modus operandi* de um esquema de espionagem, onde, entre outros fatos, o governo americano obteve acesso aos correios eletrônicos (*e-mails*), fotos e ligações dos usuários de serviços de empresas como *Google*, *Microsoft* e *Facebook* (BRASIL. SENADO FEDERAL, 2014).

Corroboram com o relatório da CPI, os últimos Encontros do WEF que, em suas análises sobre os riscos tecnológicos globais, vêm destacando (WEF, 2015, 2016):

a) mau uso das tecnologias;

b) colapso das infraestruturas críticas da informação;

c) ataques cibernéticos;

d) fraudes e roubos de dados;

e) ameaça à interconectividade mundial (Internet);

f) preocupação crescente com a privacidade dos dados corporativos e individuais.

A ESIC, alinhada com os dados acima, reforçou que as ameaças cibernéticas são crescentes, diferenciadas e apresentam elevado grau de sofisticação, exigindo dos governos ações transversais, integradoras, interdisciplinares e multissetoriais (BRASIL, 2015).

No intuito de fortalecer o argumento em questão e favorecer a discussão a respeito, este artigo compõe-se de cinco seções, além da introdução. A seção 2 apresenta breves considerações sobre informação, preservação digital e documento arquivístico no ciberespaço. A seção 3 relaciona a informação e as infraestruturas críticas por meio dos ativos de informação. A seção 4 aborda a segurança da informação e os seus desdobramentos em segurança e defesa cibernéticas. A seção 5 desenvolve o conceito de Ciber Proteção e seu relacionamento com a Ciência da Informação, bem como exemplifica, graficamente, o relacionamento da mesma com a segurança e a preservação da informação digital, a defesa cibernética e as infraestruturas críticas. A seção 6 apresenta as considerações finais do trabalho e sugere estudos para aprimoramento da pesquisa.

2 A informação no ciberespaço

Segundo a norma internacional ISO/IEC 27032 (2012, tradução nossa), ciberespaço ou espaço cibernético é entendido como "um ambiente complexo resultante da interação de pessoas, *software* e serviços existentes na Internet, conectados entre si por meio de dispositivos de tecnologia e redes, o qual não existe como forma física". Não obstante, questiona-se a suposta inexistência na forma física, pois o ciberespaço existe considerado como infraestrutura,

bem como tem muitos de seus efeitos concretamente sentidos no mundo real, e não apenas informacional e cognitivo (VIANNA; FERNANDES, 2015).

As informações geradas, comunicadas e armazenadas no ciber espaço possuem características peculiares como seu suporte, formas de recuperação e comunicação. Assim, optou-se pela abordagem objetiva da informação, alinhada, principalmente, as seguintes categorizações: (i) informação como um recurso de Sandra Braman (1989, 2006, 2014)[4] e (ii) Informação-como-coisa de Michael K. Buckland (1991)[5]. Resgata-se, também, o ponto de vista etimológico latino da palavra informação: *informatio* – ação de formar, modelar, esboço. Assim, estruturas informacionais externas ao indivíduo (objetos físicos) afetam objetivamente o ambiente individual e social ao compartilhar informação.

Em relação à representação do conhecimento no ciberespaço, Alvarenga (2001) considera que o documento não se acha fisicamente em outro espaço, mas no próprio meio que lhe proporciona materialidade, e acrescenta que, no novo contexto de produção, organização e recuperação de objetos digitais, as metas de trabalho do profissional de Ciência da Informação não se restringem à criação de representações simbólicas dos objetos físicos constantes de um acervo, mas compreendem estabelecimento dos denominados metadados[6], extraídos dos próprios objetos e chaves de acesso a serviço dos internautas. Não obstante seu formato digital, no entendimento da autora, a parte substancial dos documentos que se refere a seu conteúdo, à sua atinência, ao seu significado e aos enunciados que compõem os conceitos neles contidos, tudo isso continua invariável.

Na busca por fundamentos para o conceito de "gestão de documentos", em contexto amplo e globalizado, José Maria Jardim (2015) compilou vários conceitos e definições do referido termo em diversas línguas e "tradições arquivísticas", a saber: inglês, espanhol, francês e português.

O quadro 1 resume o levantamento do autor, grupando seus aspectos teóricos e práticos, no que tange à frequência de termos associados ao objeto, às ações e aos objetivos inerentes à gestão de documentos, por língua/tradição arquivística.

[4] A autora delineia seis categorias/definições para informação: (i) como um recurso, (ii) como uma mercadoria, (iii) como uma percepção de padrão, (iv) como uma força social constitutiva, ((v) como um agente, e (vi) como um recipiente de possibilidade .

[5] O autor identifica três principais usos da palavra "informação": (i) Informação-como-processo; (ii) informação-como-conhecimento; e (iii) informação-como-coisa.

[6] Metadados: dados estruturados que descrevem e permitem encontrar, gerenciar, compreender e/ou preservar documentos arquivísticos ao longo do tempo (CONARQ, 2011).

Quadro 1: Gestão de documentos

LÍNGUAS	OBJETO	AÇÕES	OBJETIVOS
INGLESA (EUA, Inglaterra, Canadá e Austrália)	Produção, manutenção, uso e destinação de documentos	Planejamento, controle e direção	Economia e eficiência
FRANCESA (França, Canadá [Quebec e Montreal])	Produção, conservação, uso e destinação de documentos	Controle	Eficácia
ESPANHOLA (Colômbia, Costa Rica, Espanha, México)	Produção, uso, manutenção, controle físico e intelectual de documentos íntegros, autênticos e confiáveis	Controle, planejamento, e a análise da produção, tramitação, uso e informação contidas nos documentos	Eficiência e estabelecimento de normas
PORTUGUESA (Brasil e Portugal)	Produção, tramitação, classificação, uso, avaliação e arquivamento	Controle	Eficácia, eficiência e racionalização

Fonte: adaptado de Jardim (2015).

Ao analisar o quadro resumo de gestão de documentos, a luz da segurança da informação no espaço cibernético, percebe-se que:

1) o “uso” e a “produção” são comuns a todas as línguas no quesito Objeto, sendo também, essenciais para o estabelecimento de medidas preventivas de Ciber Proteção;

2) o “controle”, berço e essência da Cibernética, encontra-se presente em todas as línguas no que se refere as Ações;

3) a busca pela efetividade (eficiência + eficácia) alinha-se perfeitamente com o objetivo de redução das vulnerabilidades em Tecnologia da Informação da Ciber Proteção.

No presente estudo, o documento digital (informação registrada, codificada em dígitos binários e acessível por meio de sistema computacional) pode também ser considerado arquivístico, ou seja, acumulado (produzido ou recebido) no curso de uma atividade prática, como instrumento ou resultado dessa atividade e retido para ação ou referência, bem como incorporado a um sistema de arquivos [sistema de informação automatizado] (CONARQ, 2011).

Neste contexto, inerente à segurança dos documentos digitais, destacam-se os quesitos:

1) controle de acesso - físico e lógico;

2) acessibilidade - garantia de localização, recuperação, apresentação e interpretação;

3) autenticidade - transmissão e preservação sem adulteração/corrupção;

4) preservação digital - conjunto de ações gerenciais e técnicas exigidas para superar as mudanças tecnológicas e as fragilidades [vulnerabilidades] dos suportes.

No que tange à preservação da informação digital, a mesma é analisada como um dos objetivos norteadores da Ciber Proteção, sendo reconhecida como um conjunto de práticas imprescindíveis ao funcionamento administrativo da Organização que produziu a informação/documento, bem como base fundamental para as relações econômicas, sociais e históricas (Memória) de um Estado soberano.

Luciana Duranti (2015, p. 12), fundadora e diretora do Projeto InterPARES, ao abordar as ameaças futuras ou que ainda persistem sobre o impacto das Tecnologias da Informação (digitais) nos princípios e práticas arquivísticas, elencou diversas inquietações. Dentre aquelas intrinsicamente relacionadas com o tema do presente artigo, destacam-se três: (i) o impressionante volume de dados e de documentos arquivísticos, bem como sua avaliação e destinação; (ii) a necessidade de manutenção e preservação de ambientes híbridos e (iii) a crescente adoção pelas instituições de políticas que permitem aos empregados usarem seus próprios dispositivos e suas próprias nuvens[7] no ambiente de trabalho.

Para Vint Cerf (WCTI, 2016), considerado "um dos pais" da Internet, a preservação é uma questão fundamental que pode afetar o futuro da Internet, levando a uma situação de perda de memória, a qual denominou de "A era negra da Internet". No seu entendimento, diversas atividades já deveriam estar em curso, de forma global e cooperativa, visando, basicamente, assegurar:

> a) a disponibilidade de mecanismos de "leitura";
>
> b) que os arquivos digitais antigos possam "rodar" nos novos *softwares* que serão desenvolvidos;
>
> c) a emulação de *hardware*, sistemas operacionais e *softwares* em máquinas virtuais;
>
> d) um padrão mundial de documentos digitais que perdure por décadas;
>
> e) a continuidade dos domínios de conteúdos na Internet, que atualmente não são *links* permanentes e podem ser alterados.

3 As infraestruturas críticas estratégicas e os ativos de informação

No campo político nacional, a segurança das Infraestruturas Críticas (também conhecidas como "Infraestruturas Estratégicas") vem sendo tratada no âmbito do Conselho de Defesa Nacional (CDN) e da Câmara de Relações Exteriores e Defesa Nacional (CREDEN). As

[7] Computação em nuvem (*cloud computing*) - modelo computacional que permite acesso por demanda, e independente da localização, a um conjunto compartilhado de recursos configuráveis de computação (rede de computadores, servidores, armazenamento, aplicativos e serviços), provisionados com esforços mínimos de gestão ou interação com o provedor de serviços (BRASIL, 2012b).

Infraestruturas Críticas (IC) compreendem as instalações, serviços, bens e sistemas que, se forem interrompidos ou destruídos, provocarão sério impacto social, econômico, político, internacional ou à segurança do Estado e da sociedade (BRASIL, 2009).

Christopher J. Furlow, veterano da Casa Branca (EUA), na área de segurança, alertou que as motivações para os ataques cibernéticos hoje são diversificadas, variando de organizações bem financiadas, organizadas e articuladas, até ações de *hackers* solitários, recomendando que, como uma forma de vencer esse desafio, as empresas e o governo identifiquem quais são os ativos mais importantes que precisam defender e quais são as vulnerabilidades antes de desenvolver um plano de ação (WCTI, 2016).

Em 2009, o CDN instituiu, no âmbito do Comitê Gestor de Segurança da Informação (CGSI), o Grupo de Trabalho de Segurança das Infraestruturas Críticas da Informação (GT-SICI). O GT-SICI publicou o *Guia de Referência para a Segurança das Infraestruturas Críticas da Informação*, a qual se refere à proteção do subconjunto de ativos de informação que afetam diretamente a consecução e a continuidade da missão do Estado e a segurança da sociedade (BRASIL, 2010).

Conforme consta no referido *Guia* (Brasil, 2010), as instituições responsáveis pelas infraestruturas críticas nacionais são orientadas a realizar, no mínimo: (i) mapeamento de seus ativos de informação para a identificação daqueles que são críticos; (ii) gestão de risco, com identificação de potenciais ameaças e vulnerabilidades; e (iii) estabelecimento de método de geração de alerta de segurança das infraestruturas críticas da informação.

Nesse contexto, os ativos de informação são os meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso. A proteção dos ativos de informação implica na definição de investimentos para um melhor posicionamento das instituições governamentais em relação à produção e custódia, principalmente, às informações dos cidadãos brasileiros e do Estado (BRASIL, 2015).

Assim sendo, reforça-se a inserção indissociável e transversal dos sistemas de informação nas Infraestruturas Críticas, consolidando a informação como mais uma área prioritária para o país. Destaca-se, ainda, que a manutenção e a proteção das IC inserem-se no contexto da Segurança Nacional, por afetar diretamente a soberania e a defesa do Estado brasileiro.

4 Segurança da informação

No âmbito da área do conhecimento da Ciência da Informação (CI), segurança da informação seria assegurar que a produção, seleção, organização, interpretação, armazenamento, recuperação, disseminação, transformação e uso da informação estivessem livres de perigos e incertezas (CAPURRO, 2003; RAMOS, 2006).

Segundo Cunha e Cavalcanti (2008), compilando-se, por meio da interdisciplinaridade, para as áreas de informática, redes de computadores, Biblioteconomia e Arquivologia, pode-se definir segurança da informação como um conjunto de procedimentos para proteção do acervo informacional de uma organização contra o acesso à informação ou ao seu uso por pessoas não autorizadas.

De acordo com o Conselho Nacional de Arquivos - Conarq (2011), segurança é um dos requisitos para sistemas informatizados de gestão arquivística de documentos e caracteriza-se pela preservação de diversos atributos, tais como:

> a) confiabilidade - credibilidade de um documento arquivístico como afirmação de um fato. Existe quando um documento arquivístico pode sustentar o fato ao qual se refere, sendo o atributo confiabilidade estabelecido pelo exame da completeza, da forma do documento e do grau de controle exercido no seu processo de criação;
>
> b) integridade - estado dos documentos que se encontram completos e não sofreram nenhum tipo de corrupção ou alteração não autorizada nem documentada;
>
> c) disponibilidade - prontidão de atendimento de um sistema;
>
> d) autenticidade - credibilidade de um documento como documento, isto é, a qualidade de um documento ser o que diz ser e de que está livre de adulteração ou qualquer outro tipo de corrupção.

Sintetizando, segurança da informação zela por manter íntegros os processos informacionais que servem à organização em um determinado contexto, seguindo os requisitos gerados pela mesma e também aqueles emanados dos indivíduos usuários dos sistemas de informação.

4.1 Segurança cibernética

A princípio, poder-se-ia supor que segurança cibernética (SegCiber ou ciber segurança), também conhecida como segurança digital ou do mundo virtual ou ,ainda, do espaço cibernético, seria uma evolução de segurança da informação. Para a presente pesquisa, segurança cibernética encontra-se inserida no contexto mais amplo e multifacetado da

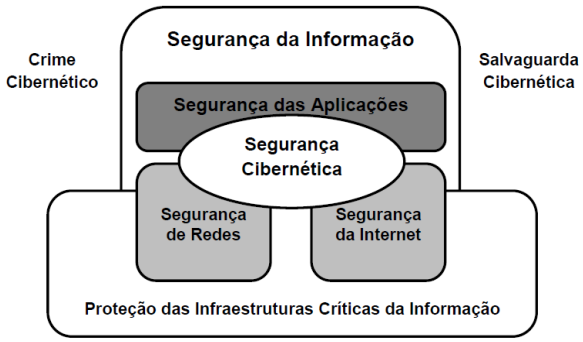
segurança da informação (VIANNA, 2015). Nesta linha de abordagem, emerge o entendimento da Organização dos Estados Americanos:

> o conceito de “ciber segurança” costuma ser usado como um termo amplo para se referir a diversos temas, desde a segurança da infraestrutura nacional e das redes pelas quais os serviços de internet são prestados, até a segurança ou integridade dos usuários. No entanto, desenvolvimentos posteriores sugerem a necessidade de limitar o conceito exclusivamente à proteção dos sistemas [de informação] e dados de informática. [...] essa abordagem mais restrita permite uma melhor compreensão do problema e uma adequada identificação das soluções necessárias para proteger as redes interdependentes e a infraestrutura da informação (OEA, 2013, p. 56).

A ISO/IEC 27032 - *Guidelines for cybersecurity* - Diretrizes para a segurança cibernética, alinhada com o "espírito" de segurança da informação inerente à família das normas internacionais 27000, define segurança cibernética (c*ybersecutity* ou c*yberspace secutity*) como preservação da confidencialidade, da integridade e da disponibilidade da informação no espaço cibernético. Adicionalmente, outras propriedades, tais como: autenticidade, responsabilidade, não repúdio e confiabilidade, podem, também estar envolvidas nesse contexto (ISO/IEC 27032, 2012, tradução nossa).

A Figura 1, extraída da norma ISO/IEC 27032, exemplifica uma forma de inserção da segurança cibernética no campo da segurança da informação.

Figura 1: Relacionamento entre segurança cibernética e outras seguranças



Fonte: Vianna (2015)

Não obstante, quando particularizada no contexto do ciberespaço, do mundo virtual ou digital, a segurança da informação passa a ser, também, conhecida como segurança cibernética ou ciber segurança.

4.2 Defesa Cibernética

Edição conjunta da Política de Defesa Nacional (PND) com a Estratégia Nacional de Defesa (END) destaca a necessidade de uma Defesa Nacional moderna, fundada em princípios democráticos, capaz de atender às necessidades de uma nação repleta de riquezas e inserida num mundo turbulento e imprevisível como o atual, ressaltando, ainda, que a Defesa não deve ser assunto restrito aos militares ou ao governo e sim uma preocupação de toda a sociedade. Nesta edição, ratificam-se três setores essenciais para a defesa nacional: o espacial, o **cibernético**[8] [grifo nosso] e o nuclear (BRASIL, 2012a).

No contexto estratégico nacional, pode-se definir o termo Defesa Cibernética (ciber defesa) como:

> o conjunto de ações defensivas, exploratórias e ofensivas, realizadas no ciberespaço, com as finalidades de proteger os nossos **sistemas de informação** [grifo nosso], obter dados para a produção de conhecimento de inteligência e causar prejuízos aos sistemas de informação do oponente (BRASIL, 2007).

É possível, então, inferir que a ciber defesa pode ser considerada como um vetor militar, ou seja, tem-se uma quinta e nova dimensão - a cibernética, ao lado das dimensões bélicas tradicionais: terrestre, marítima, aérea e espacial. Como atividade especializada, com métodos, procedimentos, características e vocabulário que lhe são peculiares, a ciber defesa pode desdobrar-se em ações de guerra cibernética (*ciber war*), que se desenvolve em ambiente totalmente artificial – o ciberespaço criado pelo homem- fazendo parte do contexto mais abrangente e conhecido da guerra da informação.

Na guerra da informação, onde a própria informação é considerada alvo e arma, podendo sua ausência ou excesso causar paralisia e derrota, busca-se afetar a informação disponível ao oponente, de maneira a degradar, interromper, enganar, negar ou destruir sua capacidade de perceber uma dada situação e exercer o comando efetivo. Para tanto, esforços devem ser direcionados na consolidação de um amplo espectro de capacidades governamentais, civis e militares com a finalidade de explorar o ambiente global de informação e assegurar domínio estratégico.

[8] O termo cibernético deriva do grego *kybernetike* e significa aquele que conduz, possui o leme, timoneiro, governador ou piloto. No campo científico, Wiener (1965), partindo de análises comportamentais, apresenta cibernética como o estudo da comunicação e controle das máquinas, seres vivos e grupos sociais. Considera-se que, do ponto de vista da transmissão da informação, não há distinção entre máquinas e seres humanos (VIANNA; FERNANDES, 2015).

5 A proteção da informação no ciber espaço

Uma das abordagens centrais deste estudo é baseada na necessidade de se discutir o conceito de Ciber Proteção (proteção cibernética) devidamente adequado à realidade brasileira, buscando-se um incremento do diálogo entre a proteção dos recursos informacionais no espaço cibernético e a Ciência da Informação.

Outro aspecto fundamental a ser considerado, é que, na prática, em operações reais e de alto risco, observou-se que ações de defesa e segurança do ciberespaço ocorrem simultaneamente, com a participação e interação de diversos atores dos diversos níveis governamentais (federal, estadual e municipal) e das instituições públicas e privadas, bem como da sociedade civil. Tal fato foi evidenciado durante a realização dos chamados "Grandes Eventos" internacionais, ocorridos no Brasil: em 2012 com a Conferência das Nações Unidas sobre Desenvolvimento Sustentável, Rio+20; em 2013 com a Copa das Confederações e a Jornada Mundial da Juventude; e, em 2014 com a Copa do Mundo de Futebol (FIFA)[9]. Não obstante, os grandes eventos vêm contribuindo para evidenciar a importância e a necessidade imprescindível da proteção do espaço cibernético como vetor de sustentabilidade do Estado brasileiro nas ações operacionais de segurança pública e de defesa nacional, assim como na salvaguarda dos serviços essenciais à população como energia elétrica, mobilidade urbana, abastecimento de água, entre outros, gerenciado pelos estados e municípios, ou pela iniciativa privada.

Aspecto igualmente crítico dessa discussão é reconhecer que os documentos e as informações circulantes no espaço cibernético são recursos tangíveis materializados por *bits.* Não obstante, os mesmos são reconhecidos em conceitos, passíveis de serem capturados e explicitados, que na essência traduzem o pensamento humano.

5.1 Construindo o conceito de Ciber Proteção

Considera-se como fundamento teórico, a fim de subsidiar o processo analítico-sintético de conceituar Ciber Proteção, a Teoria do Conceito de Ingetraut Dalhberg, que, em essência, visa a dar uma versão fidedigna à representação da informação. A autora reconhece conceito como unidade do conhecimento, definindo-o como a síntese de características essenciais de um referente [objeto de interesse] que é representado por designações (termos, nomes, códigos)[10] [ou qualquer outro signo] (DALHBERG, 1978a, 1978b, 2009).

Campos (2001), ao analisar diversas teorias relacionadas com sistemas de conceitos, no contexto das linguagens documentárias, conclui que a Teoria do Conceito de Dalhberg oferece o

[9] Informações adicionais em Vianna (2013) e Vianna; Fernandes (2015).

[10] A knowledge unit (concept) is the synthesis of the essential characteristics of a referent to be represented by designations (terms, names, codes).

melhor suporte teórico-metodológico para a recuperação da informação, possibilitando a representação do conhecimento e, em consequência, comunicações mais precisas nas áreas relativas à ciência e tecnologia.

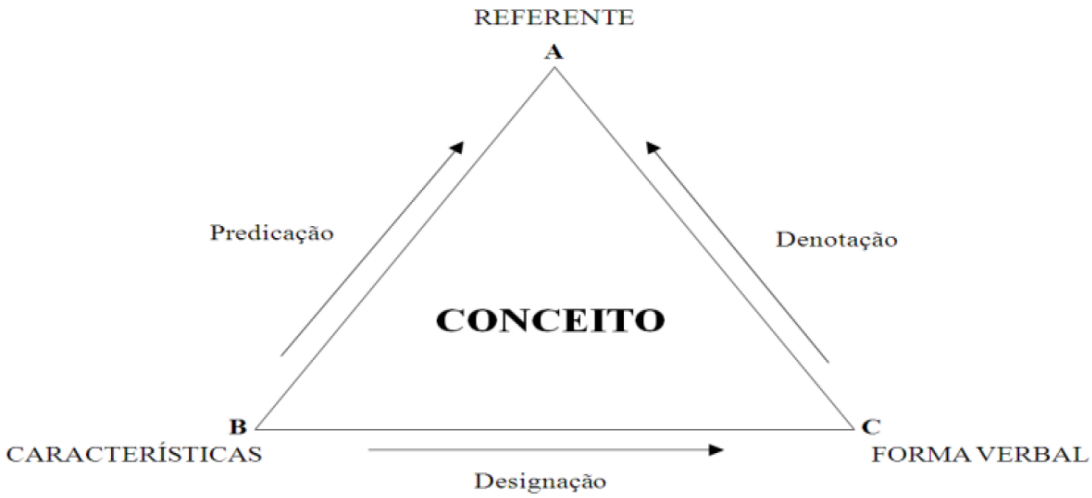
O Triângulo do Conceito proposto por Dahlberg, representado na Figura 2, sintetiza a Teoria do Conceito e divide-se em três partes:

a) item de referência (*Referent*) - componente que mantém relações sobre as afirmações verdadeiras e a forma verbal, chegando ao referente por meio da predicação (asserção de alguma coisa sobre um sujeito);

b) características (*Characteristics*) - afirmações, proposição enunciada como verdadeira (asserções) que expressam atributos sobre o item de referência;

c) formal verbal (*Verbal forms*) - termo/nome que sintetiza o conceito com o propósito de representação.

Figura 02: Triângulo do Conceito



Fonte: Adaptado de Dahlberg (1978a, p. 171)

Utilizando como base o Triângulo do Conceito, podem-se agrupar os componentes do conceito de Ciber Proteção de acordo com o Quadro 2.

Quadro 02: Quadro síntese do conceito de Ciber Proteção

ELEMENTOS	DESCRIÇÃO
REFERENTE	Proteção dos Sistemas de Informação no Espaço Cibernético de interesse nacional
CARACTERÍS-TICAS / PROPRIE-DADES DECLARADAS	- estabelece uma rede colaborativa interagências com os responsáveis pela segurança e defesa do espaço cibernético de interesse, buscando atuação integrada e essencialmente cooperativa; - participa da construção de comunidades horizontais de proteção do espaço cibernético, exercendo coordenação centralizada e intervenção descentralizada, favorecendo a consciência situacional; - participa do planejamento da preservação das informações de interesse à soberania e ao poder nacional no espaço cibernético; - acompanha as atividades de salvaguarda nos sistemas e ativos de informação nas Infraestruturas críticas, cooperando na mitigação de vulnerabilidades, na análise de riscos e no fortalecimento da resiliência cibernética (continuar operando mesmo na presença de falhas ou ataques); - analisa cenários e ameaças futuras, focando atenção especial à prevenção de ameaças externas (P. ex.: ciber terrorismo); - relaciona-se com os serviços de inteligência nacionais e dos países amigos; - favorece o intercâmbio e a interoperabilidade entre as equipes de tratamento de incidentes em redes de computadores, formulando estratégias para gestão de incidentes de segurança; - funciona como ferramenta de coesão social e coletiva da sociedade brasileira para a salvaguarda da cibercultura nacional; - coopera na formação e disponibilização de recursos humanos vocacionados e altamente capacitados (P. ex.: Hacking); - abrange tanto a internet das coisas (IoT) como os equipamentos de uso militar, por meio da avaliação de sistemas de segurança físicos ou lógicos, bem como podendo desenvolver e implantar soluções de hardware, software, processos e metodologias; - opera alinhada com as necessidades e anseios da Sociedade, organizando-se em prol dos objetivos estratégicos de um estado-nação; - atua em diferentes realidades e ambientes (P. ex.: a atual Sociedade em Rede constituída por indivíduos, empresas e Estado); podendo operar em campo local, nacional e internacional, incluído a “nuvem” (cloud); - pode demandar ações de guerra cibernética, objetivando a obtenção de informações, exploração e medidas de defesa ativa em sistemas de informação de interesse nacional, não respeitando fronteiras geográficas definidas.
FORMA VERBAL	Ciber Proteção, Proteção Cibernética e Proteção da informação no espaço cibernético

Fonte: elaboração própria (2016).

Dessa forma, entende-se que o conceito de Ciber Proteção possui características típicas da complexidade[11] , onde o termo Ciber Proteção designa um conceito geral dentro de um universo de discurso pretendido, destacando-se os seguintes relacionamentos:

a) com a Ciência da informação, em particular, por intermédio das suas disciplinas: Segurança da Informação e Organização da Informação;

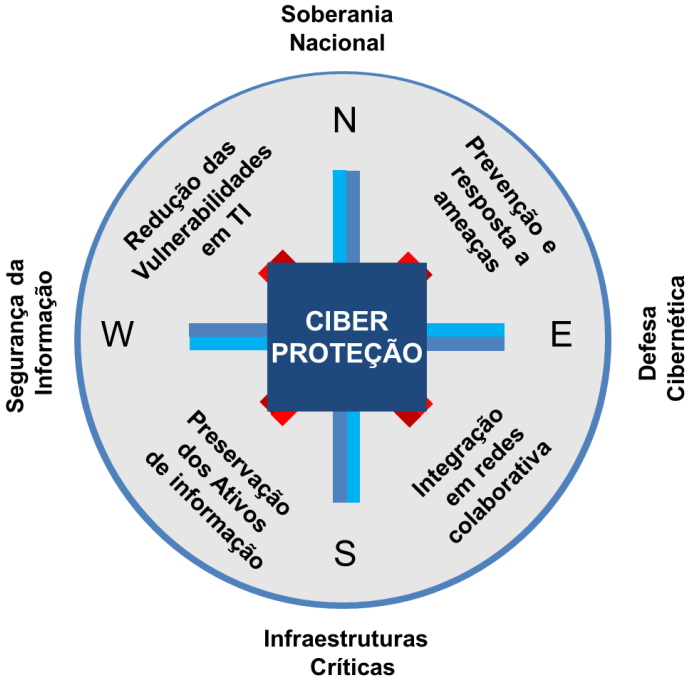
b) com a Ciência da Computação, por meio das especialidades em segurança de equipamentos (*hardware*), das aplicações (*software*) e das redes de comunicação de dados;

c) com as infraestruturas críticas nacionais, públicas ou privadas;

d) com instituições relacionadas com a governança da rede mundial de computadores - Internet;

e) com os órgãos envolvidos diretamente com a segurança e a defesa cibernéticas.

Figura 3: Bússola da Ciber Proteção



Fonte: elaboração própria (2016).

[11] Complexidade: possui aspectos científicos, filosóficos e tecnológicos, tornando difícil a formulação do comportamento geral de um sistema, mesmo quando seu funcionamento e inter-relacionamentos parecem ser compreendidos. Possui como características propriedades gerais transdisciplinares como: não linearidade, não determinismo, auto-organização e emergência (LEMOS *et al*, 2007).

5.2 Características da Ciber Proteção

A Ciber Proteção, norteada pelas demandas da soberania nacional, relaciona-se com a Ciência da Informação, atuando, particularmente, nos ativos de informação das infraestruturas críticas.

Dessa forma, busca preservar a informação (documentos digitais) nos sistemas informacionais de interesse nacional, bem como contribuir para a redução das fragilidades e vulnerabilidades inerentes às tecnologias de informação, englobando também a Internet, as aplicações para dispositivos móveis e os serviços via *Web.* Estrategicamente; pode colaborar com a prevenção de ameaças (regionais ou globais) e com a resposta aos ataques, não descartando medidas ativas sobre elementos hostis internos ou externos ao país.

A Ciber Proteção apresenta o entendimento colaborativo, de articulação em rede e cooperação interagências, vitais ao desenvolvimento da Sociedade de um Estado-Nação. A Figura 3 pretende sintetizar, graficamente, o conceito de Ciber Proteção.

5.3 A Ciência da Informação e a Ciber Proteção

Para fins deste estudo, considera-se que atividades inerentes à proteção cibernética estão imbricadas no contexto abrangente e multidisciplinar da Ciência da Informação (CI), vinculadas, particularmente, pelas áreas de estudo inerentes à segurança da informação, gestão de documentos e preservação da informação digital.

Levando-se em conta a complexidade e a dinâmica do tema no cenário atual, nacional e mundial, bem como a soberania e a segurança do Estado brasileiro, percebe-se a necessidade do crescimento da interação entre as áreas de atuação da Ciência da Informação (CI)[12] e a proteção do ciberespaço, particularmente, no que tange às denominadas "soluções de segurança" centradas no uso massivo das TI. As mesmas possuem riscos inerentes e são incompletas, necessitando, no mínimo: (i) de **pessoas** qualificadas para adequá-las ao ambiente e às necessidades de segurança institucionais, em condições de responder as falhas ou incidentes indesejados que possam comprometer a informação organizacional e (ii) de **processos** peculiares para a organização da Informação e do conhecimento com segurança.

Paradoxalmente ao inexorável desenvolvimento tecnológico, o ser humano detém papel essencial no controle e na segurança do espaço cibernético (onde, invariavelmente, circula

12 No contexto da Ciência da Informação, pode-se, por exemplo, citar a realização do mapeamento das necessidades informacionais dos profissionais que atuam na gestão da segurança da informação do ciberespaço (VIANNA, 2015).

grande parte da informação em tempo real), devendo sua capacidade profissional ser objeto de constante estudo e aperfeiçoamento[13]. Sobre a importância do fator humano na Ciber Proteção, o lendário *Hacker* Kevin Mitnick traça interessante analogia:

> a medida que os especialistas contribuem para o desenvolvimento contínuo de melhores tecnologias de segurança, tornando ainda mais difícil a exploração de vulnerabilidades técnicas, os atacantes se voltarão cada vez mais para a exploração do elemento humano. Quebrar o "firewall humana" quase sempre é fácil, não exige nenhum investimento além do custo de uma ligação telefônica e envolve um risco mínimo (MITNICK e SIMON, 2003).

Considerando-se os "processos", argumenta-se que a Ciber Proteção possui um significativo componente informacional, associado com: (i) a representação da informação, sua organização intelectual e encadeamentos; (ii) busca e recuperação; (iii) a qualidade, o valor e o uso da informação - todos tradicionalmente tratados pela Ciência da Informação.

No caso, entende-se a CI como um campo de questões a serem estudadas, englobando, tanto a pesquisa científica quanto a prática profissional, pelos problemas que propõe e pelos métodos que escolheu, ao longo do tempo, para solucioná-los (SARACEVIC, 1996).

Dentre as contribuições que a Ciber Proteção pode adicionar ao campo de atuação da CI, em especial à segurança dos sistemas de informação de interesse nacional, destacam-se:

> a) o incremento de fatores como resiliência dos ativos de informação a ataques;
> b) coordenação e cooperação em rede em favor da mitigação de vulnerabilidades relacionadas às "soluções de segurança" cibernéticas;
> c) detecção e prevenção de ameaças cibernéticas, com ações ativas sobre elementos/sistemas potencialmente hostis internos ou não nacionais.

Considera-se, também, em relação aos processos informacionais, a percepção pelo autor (construída a partir das atividades profissionais desenvolvidas no período de 2008 a 2016) de lacunas e oportunidades de melhoria, no que tange ao tratamento e organização da informação e do conhecimento pelas instituições imbricadas com a segurança e a defesa cibernéticas.

6 Considerações finais

A implementação massiva e ininterrupta de TI nas organizações geraram novas necessidades na administração dos recursos, alavancadas pelas inúmeras possibilidades de inovação no trato da informação institucional. É fato que as (r)evoluções da TI, os tempos e movimentos da era digital, acontecem mas rapidamente do que outras áreas do conhecimento

[13] Sobre os perfis e procedimentos realizados pelos agentes responsáveis pela segurança da Informação no espaço cibernético da APF ver Vianna e Fernandes (2015).

conseguem acompanhar, particularmente no contexto da necessidade de proteção da informação e do ciberespaço.

Os sistemas e os ativos de informação intrínsecos e necessários ao funcionamento e controle dos serviços essenciais à sociedade, públicos ou privados, tornam-se cada vez mais automatizados e dependentes tecnologicamente. À medida que esses sistemas se tornam interligados a uma rede de comunicação de dados e podem ser acessados remotamente, aumenta a insegurança e amplia-se o rol de ameaças e de vulnerabilidades, particularmente quando conectados à Internet.

O gerenciamento da preservação da Informação digital remete a estratégias diversificadas que se estendem a processos, *hardware, software*, redes de dados, ambientes heterogêneos de armazenamento e produção, entre outros, envolvendo atividades complexas de segurança. Não obstante, almeja-se ampliar a capacidade de assegurar o funcionamento adequado dos sistemas e dos ativos de informação, em instituições governamentais de áreas diversificadas e níveis políticos-administrativos distintos, assim como nas infraestruturas críticas estratégicas nacionais a cargo da iniciativa privada.

Portanto, no âmbito da área de conhecimento da Ciência da Informação, torna-se primordial avançar em estudos amplos e diversificados, como promover o debate e o desenvolvimento de procedimentos de segurança da informação digital, particularmente em um espaço informacional típico, como o cibernético.

O estudo de Ciber Proteção, estruturado a partir da Teoria do Conceito e suportado pela multidisciplinaridade tão cara a CI, busca proporcionar um corpo de conhecimento consistente teoricamente, respaldado na prática de atividades operacionais de segurança e defesa cibernéticas, bem como aderente a realidade nacional.

Argumentou-se, também, que a proteção da informação no ciberespaço tem impactos relevantes na sustentação da sociedade, na construção da cidadania e no desenvolvimento econômico. A Ciber Proteção, sendo vocacionada para a coordenação e integração de uma massa sistêmica heterogênea, poderá ampliar as suas características típicas como: atuação em rede, ações colaborativas e trabalho cooperativo, em prol da proteção dos ativos de informação críticos para preservação da soberania nacional.

Assim sendo, de forma não exaustiva, pode-se afirmar que a proteção do espaço cibernético é complexa politicamente, heterogênea na sua operacionalização e envolve diversos segmentos governamentais, acadêmicos e da sociedade em geral.

Neste contexto, e na busca de ações efetivas, sugere-se a organização de um Conselho de Estado, supra governamental, voltado à proteção da informação no espaço cibernético. Dessa forma, o "Conselho Nacional de Proteção Cibernética" seria responsável pela formulação de políticas públicas, englobando as áreas de segurança cibernética, gestão de incidentes em redes de computadores, defesa cibernética, infraestruturas críticas, entre outras.

Como primeira ação concreta, o “Conselho Nacional de Proteção Cibernética" (CNPCiber) proposto ficaria encarregado de revitalizar o Decreto Presidencial n. 3.505, de 13 de junho de 2000, que instituiu a Política de Segurança da Informação (PSI), por meio da elaboração de uma “Política Nacional de Proteção da Informação no Ciberespaço”.

Estudos futuros poderiam englobar a organização da informação e a gestão do conhecimento nas instituições relacionadas com a Ciber Proteção; e, igualmente, a estruturação de um órgão de caráter executivo integrado ao CNPCiber.

Referências

ALVARENGA, L. A Teoria do Conceito Revisitada em Conexão com Ontologias e Metadados no Contexto das Bibliotecas Tradicionais e Digitais. **DataGramaZero**: Revista de Ciência da Informação, v. 2, n. 6, dez. 2001.

BRAMAN, Sandra. Poder, privacidade e segurança: discussões sobre acesso, controle e uso da informação. **O Debatedouro**, v. 12, n. 01, 84. ed., Belo Horizonte, 2014. Disponível em: <https://odebatedouro.files.wordpress.com/2014/05/debat84_v1.pdf>. Acesso em: 29 ago. 2016.

BRAMAN, Sandra. **Change of State:** information, policy and power. Cambridge: MIT Press, 2006.

BRAMAN, Sandra. Defining information: An approach for policy-makers. **Telecommunications Policy**, v. 13, p. 233-242, September 1989.

BRASIL. MINISTÉRIO DA DEFESA. **Glossário das Forças Armadas** – MD35-G-01. Apresenta definições de termos comuns às Forças Armadas. Brasília, 2007. Disponível em: <https://www.defesa.gov.br/arquivos/File/legislacao/emcfa/publicacoes/md35_g_01_glossario_fa_4aed2007.pdf>. Acesso em: 09 jun. 2013.

BRASIL. MINISTÉRIO DA DEFESA. **Política Nacional de Defesa (PND) e a Estratégia Nacional de Defesa (END)**. Brasília, DF, 2012a. Disponível em: <http://www.defesa.gov.br/arquivos/estado_e_defesa/END-PND_Optimized.pdf. Acesso em: 15 jul. 2015.

BRASIL. MINISTÉRIO DO PLANEJAMENTO. Decreto n. 8.638, de 15 de janeiro de 2016. Institui a Política de Governança Digital no âmbito dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional. **Diário Oficial [da] República Federativa do Brasil**. Brasília, DF, 18 de janeiro de 2016.

BRASIL. PRESIDÊNCIA DA REPÚBLICA. **Livro Branco da Defesa Nacional**. Brasília, DF, 2012b. Disponível em: < http://www.defesa.gov.br/arquivos/2012/mes07/lbdn.pdf>. Acesso em: 04 mar. 2016.

BRASIL. PRESIDÊNCIA DA REPÚBLICA. Gabinete de Segurança Institucional. **Guia de referência para a segurança das infraestruturas críticas da informação.** Brasília, 2010. Disponível em <http://dsic.planalto.gov.br/documentos/publicacoes/2_Guia_SICI.pdf>. Acesso em: 10 ago. 2015.

BRASIL. PRESIDÊNCIA DA REPÚBLICA. Gabinete de Segurança Institucional. Portaria n. 45, de 8 de setembro de 2009. Institui, no âmbito da Câmara de Relações Exteriores e Defesa Nacional (CREDEN), o Grupo Técnico de Segurança Cibernética e dá outras providências. **Diário Oficial [da] República Federativa do Brasil**, Brasília, DF, 9 set. 2009.

BRASIL. PRESIDÊNCIA DA REPÚBLICA. Gabinete de Segurança Institucional. **Estratégia de segurança da informação e comunicações e de segurança cibernética da administração pública federal 2015-2018**: versão 1.0 Brasília: Presidência da República, 2015.

BRASIL. SENADO FEDERAL. **Em Discussão!**. Brasília, n.21, jul. 2014. Disponível em: <http://www.senado.gov.br/noticias/jornal/emdiscussao/espionagem/>. Acesso em: 29 nov. 2014.

BRASIL. TRIBUNAL DE CONTAS DA UNIÃO. **Acórdão n. 3117/2014 – TCU – Plenário. Relatório de Levantamento. Avaliação da governança de tecnologia da Informação na administração pública federal.** Brasília: TCU, 2014.

BUCKLAND, M.K. Information as thing. **Journal of the American Society for Information Science** (JASIS), v. 45, n. 5, p. 351-360, 1991.

CAMPOS, M. L. de Almeida. **Linguagem documentária**: teorias que fundamentam sua elaboração. Niterói: Editora UFF, 2001.

CAPURRO, Rafael. Epistemologia e ciência da informação. In: ENCONTRO NACIONAL DE PESQUISA EM CIÊNCIA DA INFORMAÇÃO, 5., 2003, Belo Horizonte. [**Anais]** do Encontro**...** Belo Horizonte: Associação Nacional de Pesquisa e Pós-Graduação em Ciência da Informação e Biblioteconomia, 2003. Disponível em <http://www.capurro.de/enancib_p.htm>. Acesso em: 02 mar. 2014.

CONSELHO NACIONAL DE ARQUIVOS (CONARQ). **e-ARQ Brasil**: Modelo de Requisitos para Sistemas Informatizados de Gestão Arquivística de Documentos. Rio de Janeiro: Arquivo Nacional, 2011.

CUNHA, M. B. da; CAVALCANTI, C. R. de O. **Dicionário de biblioteconomia e arquivologia.** Brasília: Briquet de Lemos, 2008.

DAHLBERG, I. **Concepts and terms**: ISKO's major challenge. **Knowledge Organization**, v. 36, n. 2-3, p. 169-177, 2009.

DAHLBERG, I. A referent-oriented, analytical concept theory for interconcept. **International Classification**., v. 5, n. 3, p. 142-151, 1978a.

DAHLBERG, I. Teoria do conceito. **Ciência da Informação**, Rio de Janeiro, v. 7, n. 2, p. 101-107, 1978b.

DURANTI, Luciana. InterPARES Trust. In: **Acervo**: revista do Arquivo Nacional, Rio de Janeiro, v. 28, n. 2, p. 11-18, jul./set. 2015. Disponível em: <http://revista.arquivonacional.gov.br/index.php/revistaacervo/article/view/607>. Acesso em: 25 set.2016.

INTERNATIONAL STANDARD ORGANIZATION. **ISO/IEC 27032** - Information technology - Security Techniques - Guidelines for cybersecurity. 2012.

JARDIM, Jose Maria. Caminhos e perspectivas da gestão de documentos em cenários de transformações. In: **Acervo**: revista do Arquivo Nacional, Rio de Janeiro, v. 28, n. 2, p. 19-50, jul./set. 2015. Disponível em: <http://revista.arquivonacional.gov.br/index.php/revistaacervo/article/view/607>. Acesso em: 25 set.2016.

LEMOS, R. T. S.; FRANKLIN B. L.; ALVES, J. B. M.; KERN, V. M. Tecnontologia & complexidade. **Ciências & Cognição**, v. 11, 2007. Disponível em: <http://www.cienciasecognicao.org/revista/index.php/cec/article/view/664>. Acesso em 28 mar. 2016.

MITNICK, Kevin D.; SIMON, William L. **A arte de enganar:** controlando o fator humano na segurança da informação. São Paulo: Pearson Education, 2003.

ORGANIZAÇÃO DOS ESTADOS AMERICANOS. Comissão Interamericana de Direitos Humanos. **Liberdade de expressão e internet**. 2013. Disponível em: <http://www.oas.org/pt/cidh/expressao/docs/publicaciones/2014%2008%2004%20Liberdade%20de%20Express%C3%A3o%20e%20Internet%20Rev%20%20HR_Rev %20LAR.pdf>. Acesso em: 25 set. 2016.

RAMOS, Anderson *et al.* (Orgs.). **Security Officer – 1:** Guia Oficial para Formação de Gestores em Segurança da Informação**.** 2. ed., Porto Alegre, RS: Zouk, 2006.

SARACEVIC, T. Ciência da Informação: origem, evolução e relações. **Perspectivas em Ciência da Informação**, v. 1, n. 1, p. 41-62, jan./jun., 1996. Disponível em: <http://portaldeperiodicos.eci.ufmg.br/index.php/pci/article/view/235>. Acesso em: 02 mar. 2016.

VIANNA, Eduardo Wallier. **Análise do comportamento informacional na gestão da segurança cibernética da Administração Pública Federal**. 2015. 115 f., il. Dissertação (Mestrado em Ciência da Informação) - Universidade de Brasília, Brasília, 2015.

VIANNA, Eduardo Wallier. A Segurança Cibernética na Conferência das Nações Unidas para o Desenvolvimento Sustentável. In: NAKAIAMA M. K. *et al.* (Orgs.). **Ciência, tecnologia e inovação**: pontes para a segurança pública. Florianópolis: FUNJAB, 2013. cap. 5. p. 127-156.

VIANNA, Eduardo Wallier; FERNANDES, J. H. C. O gestor da segurança da informação no espaço cibernético governamental: grandes desafios, novos perfis e procedimentos, **Brazilian Journal of Information Science: research trends,** v. 9, n. 1, 2015. Disponível em: <http://www2.marilia.unesp.br/revistas/index.php/bjis/article/view/5216/3668>. Acesso em: 12 ago. 2015.

WORLD CONGRESS ON INFORMATION TECHNOLOGY- **WCIT 2016**. Brasília, 2016. Disponível em: <http://www.wcit2016.com/home/>. Acesso em: 18 out. 2016.

WORLD ECONOMIC FORUM – **Report of WEF/2015**, 2015. Disponível em: <http://reports.weforum.org/global-risks-2015/. Acesso em: 18 out. 2016.

WORLD ECONOMIC FORUM – **Report of WEF/2016**, 2016. Disponível em: <http://reports.weforum.org/global-risks-2016/. Acesso em: 11 mar. 2016.

WIENER, Norbert. **Cybernetics – 2nd Edition**: or the control and Communication in the animal and the machine. Boston: MIT Press. 1995.

Recebido/Recibido/Received: 2016-05-31
Aceitado/Aceptado/Accepted: 2017-03-07