**A Segurança da Informação: uma observação sobre os aspectos técnicos, humanos, sociais e jurídicos conhecidos**

**Anderson Julianelli do Nascimento**

Instituto Federal de Educação, Ciência e Tecnologia do Rio de Janeiro – IFRJ

**Djones Braz de Araujo Costa**

Instituto Federal de Educação, Ciência e Tecnologia do Rio de Janeiro – IFRJ,

djones.braz@gmail.com

**RESUMO**

Este artigo visa discutir o impacto dos aspectos técnicos, humanos, sociais e legais na área da Segurança da Informação como um todo. Buscaremos a compreensão sobre como esses fatores afetam a segurança dos dados digitais e como podemos nos preparar para minimizar os efeitos causados pelos riscos e ameaças aos quais estamos sujeitos em nosso dia a dia. Analisaremos também se o Brasil está preparado para atuar em casos de incidentes e o que vem fazendo para coibir os ataques cibernéticos. Já quanto à parte jurídica, por se tratar de uma matéria nova e que se modifica constantemente, observamos o estágio de adaptação da legislação brasileira à realidade atual. Por fim, concluímos sugerindo a adoção de métodos e padrões de combate a ataques cibernéticos.

**Palavras-Chave**:Segurança da Informação; Ameaças; Ataques; Melhores Práticas.

Data de Submissão: 17/10/2023

Data Aceito Publicação: 15/05/2024

**Information Security: an observation on the known technical, human, social and legal aspects.**

**ABSTRACT**

This article aims to discuss the impact of technical, human, social and legal aspects in the area of Information Security as a whole. We will seek to understand how these factors affect the security of digital data and how we can prepare to minimize the effects caused by the risks and threats to which we are subject in our daily lives. We will also analyze whether Brazil is prepared to act in cases of incidents and what it has been doing to curb cyber attacks. As for the legal part, as it is a new matter that is constantly changing, we observe the stage of adaptation of Brazilian legislation to the current reality. Finally, we will conclude by suggesting the adoption of methods and standards to combat cyber attacks.

**Key Words:** Best practices; Information security; Threats; Attacks.

**1. Introdução**

Este artigo propõe analisar as modificações nas ferramentas aplicadas para garantir a segurança da informação, considerando o desenvolvimento das técnicas e das tecnologias num recorte de 60 anos, de 1957 a 2017. Ao longo desse artigo, pretende-se também apontar como o comportamento humano e social impacta diretamente os sistemas cibernéticos, tanto para métodos de invasão como para procedimentos de defesa. Todavia, não podemos deixar de destacar os esforços empregados na elaboração de legislações específicas sobre ameaças cibernéticas e as aplicações das sanções cabíveis a estes criminosos.

O artigo pretende observar três frentes bem experimentadas, são elas: a visão tecnológica, o comportamento humano e social e as ferramentas legais disponibilizadas para o combate desses crimes. Em conjunto, essas frentes formam uma tríade bastante sólida capaz de nos dar informações relevantes sobre o comportamento destes criminosos e também de nós, usuários. Por conseguinte, estes dados serão analisados e, com base nestas análises, serão sugeridas novas metodologias de defesa, técnicas de prevenção, tecnologias para mitigação de ataques cibernéticos, políticas de segurança e dispositivos legais para dirimir inconveniências causadas por este tipo de infração.

Dentre a imensa variedade de dados que trafega pelo ciberespaço, destacamos as transações bancárias, responsáveis por inúmeros negócios, e que estão sujeitas a todos os tipos de ameaças imagináveis. Devemos estar sempre atentos e preparados para todo tipo de ameaça que possamos vir a sofrer, empregando todas as ferramentas conhecidas e atuando no desenvolvimento de novas ferramentas.

O tema escolhido para este artigo científico tem a sua relevância social, pois atualmente o mundo inteiro está conectado, ou seja, vivemos num cenário globalizado em que a rapidez e a facilidade para se comunicar com outras pessoas, empresas, governos, entre outros, e essa realidade se deve à concepção da internet. Essa rede global que interliga a todos sem distinção e que em um período tão curto, se comparado à revolução industrial, alcançou um patamar imensurável e indispensável para todos nós, haja vista que hoje seria impossível pensarmos em não haver trocas de informações em tempo real.

**2. Fundamentação teórica**

**2.1. Os fundamentos de segurança da informação**

Para entendermos o que tratamos como segurança da informação, primeiramente, devemos entender que a internet que conhecemos hoje está em constante transformação devido a velocidade dos avanços tecnológicos. Permitindo assim, em um futuro próximo, o surgimento da Web Semântica ou como a maioria dos especialistas estão chamando, Internet 3.0. Essa nova forma de uso da internet que está por vir, será capaz de organizar e usufruir de todo conhecimento adquirido e disponível na rede mundial de uma forma mais inteligente, onde dados de fontes distintas serão embaralhados de maneira imediata a partir de dados acessados e conectados entre si.

Garantir a segurança da informação em ambiente digital constitui, cada vez mais, uma preocupação à escala mundial, seja por parte de organismos públicos, privados, universidades, empresas e até pelos cidadãos, de forma individual ou coletiva. (PEREIRA, 2005, p.67).

Deste modo, com as possibilidades que surgirão a partir dessa nova internet, deveremos prestar mais atenção nos conteúdos disponibilizados na rede. A maneira como usamos essas informações e a segurança que deveremos empregar em nossas redes terão um papel cada vez mais importante no cenário cibernético.

Em seu artigo científico Canongia & Mandarino (2009) nos esclarecem que, em março de 2009 ocorreu a reunião da Organização para a Cooperação e o Desenvolvimento Econômico (OCDE), preocupados com os rumos que a nova sociedade da informação está tomando recentemente. Dentre os vários pontos explicitados nesta reunião, destaca-se a discussão sobre a cultura de segurança como um vetor estratégico das nações, onde os seguintes aspectos foram evidenciados:

* Cada parte envolvida tem um importante papel para assegurar a segurança em função de suas competências, e devem ser sensibilizados sobre os riscos associados à segurança de sistemas e redes de informação;
* As questões de segurança devem ser objeto de preocupação e responsabilidade de todos os atores, seja governamental, empresarial, e de outros (pesquisa e terceiro setor).

Segundo a International Communications Union (ITU), cybersecurity significa basicamente prover proteção contra acesso, manipulação, e destruição não autorizada de recursos críticos e bens. Para a promoção da cybersecurity, a ITU considera as seguintes áreas como foco principal:

1. Áreas de elevada atenção: Combate ao crime cibernético, Criação em nível nacional de CERTs/CSIRTs (*Computer Emergency Response Teams/Computer Security Incident Response Teams*); Aumento da cultura de segurança cibernética e suas atividades; e Promoção da educação;
2. Áreas com menos atenção: Pesquisa e Desenvolvimento; Avaliação e monitoramento; e Atendimento às pequenas e médias empresas (PMEs). (SUND, 2008).

Na esfera pública do Brasil, dois conceitos são empregados e dão sustentação à abordagem da segurança cibernética, são eles:

[...] “infraestrutura crítica da informação”, bem como “ativos de informação”. Para o governo federal brasileiro, considera-se “infraestrutura crítica da informação” o subconjunto de ativos de informação que afetam diretamente a consecução e a continuidade da missão do Estado e a segurança da sociedade. E, complementarmente, consideram-se “ativos de informação”, os meios de armazenamento, transmissão e processamento da informação, os sistemas de informação, bem como os locais onde se encontram esses meios, e as pessoas que a eles têm acesso. (BRASIL, Portaria n. 34.2009).

Os “Princípios para a Governança e Uso da Internet no Brasil”, criado em fevereiro de 2009, pelo Comitê Gestor da Internet no Brasil (CGI.br), tem o objetivo de normatizar a estabilidade, a segurança e a funcionalidade globais da rede. No entendimento do CGI.br, esses três pontos devem ser preservados de forma ativa através de medidas técnicas compatíveis com os padrões internacionais e estímulo ao uso das boas práticas.

Para assegurarmos uma boa segurança da informação, devemos nos ater as suas principais propriedades, a confidencialidade - é a necessidade de garantir que as informações sejam divulgadas somente para aqueles que possuem autorização para vê-las; integridade – é a necessidade de garantir que as informações não tenham sido alteradas acidentalmente ou deliberadamente, e que elas estejam corretas e completas e, disponibilidade – é a necessidade de garantir que os propósitos de um sistema possam ser atingidos e que ele esteja acessível àqueles que dele precisem.

**2.2. A importância da segurança cibernética e a prevenção de riscos e ameaças**

Um dos primeiros princípios para um bom serviço de segurança digital é o controle de acesso. Além disso, outros princípios são fundamentais para minimizar o risco de incidentes, sendo eles:

**Autenticação** é o serviço de segurança que pode ser utilizado para assegurar que as pessoas que acessam a rede sejam autorizadas;

**Confidencialidade** é o serviço de segurança que pode ser utilizado para assegurar que os dados, o software e as mensagens não sejam expostos a partes não-autorizadas;

**Integridade** é o serviço de segurança que pode ser utilizado para assegurar que partes não-autorizadas não modifiquem os dados, o software e as mensagens;

**Não-repúdio** é o serviço de segurança que pode ser utilizado para assegurar que as entidades envolvidas em uma comunicação não possam negar sua participação nesta comunicação. Especificamente, a entidade que envia não pode negar que tenha enviado uma mensagem (não-repúdio como prova de origem) e a entidade receptora não pode negar ter recebido uma mensagem [não-repúdio como prova de entrega] (BURNETT & PAINE, 2002, p.279).

Inúmeros autores, como os citados por Pereira (2005) em seu artigo, quando abordam a segurança da informação digital fazem uma primeira distinção entre a segurança física e a lógica. CARNEIRO (2002), quando discorre sobre segurança física da informação digital, propõe a sua subdivisão em 3 subgrupos: de pessoal, de equipamentos e de instalações.

**2.3. Os aspectos legais e normativos da segurança da informação**

Um documento digital só terá validade jurídica se cumprir com alguns requisitos, como os que já são feitos aos documentos tradicionais. Tanto para os documentos digitais quanto para os tradicionais são exigidas verificações de sua autenticidade, da integridade e da tempestividade. Para garantir a identificação e autenticidade das pessoas que assinam estes documentos eletrônicos, foram criadas as Autoridades Certificadoras, que intermediam a relação entre usuários por meio de um sistema cifrado de comunicação assimétrica. A medida provisória no. 2.200, de 28 de junho de 2001, dispõe sobre a infraestrutura de Chaves Públicas Brasileiras – ICP – Brasil, que instituiu o Comitê Gestor de Infraestrutura de Chaves Públicas Brasileira (CG ICP-Brasil), e cuja função é de autoridade gestora de políticas de certificação digital, ao qual garantirá a segurança e demais aspectos apresentados sobre os documentos digitais.

Atualmente, podemos nos pautar em padrões internacionais de segurança cibernética, como as normas ISO/IEC, específicas para as áreas de segurança da informação, para tentar dirimir ou até mesmo minimizar os efeitos causados por incidentes e/ou ataques sofridos diariamente. Pereira (2005) informa em seu artigo que:

A norma ISO/IEC 17799 é relativa à segurança da informação e procura contribuir para a segurança das organizações, dos seus colaboradores, instalações e, sobretudo, dos sistemas de informação, sendo o seu título ‘Tecnologias da Informação – Código de prática para a gestão da segurança da informação’”. PEREIRA (2005, p.75).

**2.4. Segurança cibernética: práticas e políticas adotadas no brasil**

A Administração Pública Federal (APF), o Gabinete de Segurança Institucional da Presidência da República (GSIPR), por meio de seu Departamento de Segurança da Informação e Comunicação (DSIC), desenvolveram em colaboração com vários órgãos da APF e seus representantes, e em conjunto ao Comitê Gestor de Segurança da Informação (CGSI), um conjunto de normas que visam garantir a segurança da informação e comunicações para o governo. Além disso, as normas também estão focadas em impulsionar a criação de grupos de trabalhos técnicos e na formação de recursos humanos capazes de tratar temas relativos à segurança cibernética.

A publicação da Instrução Normativa IN GSIPR No. 01/2008, possui relevância quanto ao tema segurança da informação, pois disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indiretamente. O documento define que “Segurança da Informação e Comunicações (SIC) são as ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações”, trazendo consigo uma nova ideia de inovação e ampliação do entendimento tradicionalmente adotado na segurança da informação.

Podemos identificar parâmetros e valores principais na SIC com relação aos conceitos descritos na IN GSIPR No.01/2008, são eles:

**Disponibilidade:** propriedade de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade;

integridade: propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;

**Confidencialidade:** propriedade de que a informação não esteja disponível ou revelada a pessoa física, sistema, órgão ou entidade não autorizada e credenciada; e,

**Autenticidade:** propriedade de que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado sistema, órgão ou *entidade*. (GSIPR, No.01/2008).

Destacamos também as seguintes publicações com relação ao desenvolvimento e implantação da SIC em órgão e entidades da APF, são elas:

* **NC 03/IN 01/DSIC/GSIPR** - “Diretrizes para Elaboração de Política de Segurança da Informação e Comunicações nos Órgãos e Entidades da Administração Pública Federal”, Portaria No. 29, publicada no D.O.U de No. 125, em 03 de julho de 2009;
* **NC 04/IN 01/DSIC/GSIPR** - “Gestão de Risco de Segurança da Informação e Comunicações – GRSIC nos Órgãos e Entidades da Administração Pública Federal”, Portaria No. 37, publicada no D.O.U de No. 156, em 17 de agosto de 2009; e,
* **NC 05/IN 01/DSIC/GSIPR** - “Criação de Equipes de Tratamento e Resposta a Incidentes em Redes Computacionais – ETIR nos Órgãos e Entidades da Administração Pública Federal”, Portaria No. 38, publicada no D.O.U No. 156, em 17 de agosto de 2009.

Diante de todo exposto, vimos que nosso país possui os instrumentos e mecanismos necessários para o desenvolvimento de nossa segurança da informação e comunicações. O Brasil possui normatizações próprias, adequadas à realidade de nosso país, e com reconhecimento internacional, capaz de atender qualquer eventualidade que possa surgir com relação às ameaças virtuais.

**3. Considerações finais**

Este artigo tem a intenção de discutir questões sobre Segurança da Informação abordando seus aspectos técnicos, humanos, sociais e legais e demonstrando como cada um destes influencia o desenvolvimento de novas técnicas e metodologias.

Durante a reflexão, detectamos que a nossa legislação ainda está em fase inicial, em se tratando especificamente de leis para combate aos crimes digitais. Contudo, temos que reconhecer que o primeiro passo no sentido de regulamentar esses crimes cometidos na esfera tecnológica já foi dado com a sanção da Lei 12.737/2012 (Lei Carolina Dieckman), a qual discorre sobre a tipificação criminal de delitos informáticos.

Além disso, devemos também uma parcela de atenção à nossa legislação penal em vigor, pois esta encontra-se desatualizada com relação à realidade dos dias atuais. Nosso código penal data da década de 40, portanto, não condiz com a realidade atual. É necessária uma grande reforma jurídica com a criação de leis específicas para o combate aos crimes digitais. Sem dispositivos legais que considerem o novo cenário virtual, atualmente adaptamos as leis existentes aos crimes cometidos na esfera digital.

**Referências**

ABREU, Karen Cristina Kraemer. História e usos da Internet. Artigo Científico. Disponível em: <http://www.bocc.ubi.pt/pag/abreu-karen-historia-e-usos-da-internet.pdf>. Acesso em: 16 agosto 2018.

BRASIL, Decreto n. 6.605, de 14 de outubro de 2008. O Comitê Gestor da Infraestrutura de Chaves Públicas Brasileira - CG ICP-Brasil exerce a função de autoridade gestora de políticas de certificação digital. Disponível em: <https://www.iti.gov.br/comite-gestor>. Acesso em: 25 out 2018.

\_\_\_\_\_\_, Decreto n. 6.703, de 18 de dezembro de 2008. Aprova a Estratégia Nacional de Defesa e dá outras providências. Disponível em: <http://www.fab.mil.br/portal/defesa/estrategia\_defesa\_nacional\_portugues.pdf>. Acesso em: 18 de agosto de 2018.

\_\_\_\_\_\_, Fundamentos de Segurança da Informação. Disponível em: <https://www.cert.br/docs/palestras/certbr-egi2014.pdf>. Acessado em: 24 setembro 2018.

\_\_\_\_\_\_, Lei n. 12.737, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei no 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil\_03/\_Ato2011-2014/2012/Lei/L12737.htm>. Acesso em: 25 out 2018.

\_\_\_\_\_\_, Segurança Cibernética: onde estamos e onde deveríamos estar? Disponível em: < https://www.cert.br/docs/palestras/certbr-painel-telebrasil2018.pdf>. Acessado em: 24 setembro 2018.

\_\_\_\_\_\_, Gabinete de Segurança Institucional da Presidência da República (GSIPR). Lei n. 10.683, de 28 de maio de 2003. Dispõe sobre a organização da Presidência da República e dos Ministérios, e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil\_03/LEIS/2003/L10.683.htm>. Acesso em: 18 de agosto de 2018.

\_\_\_\_\_\_, Norma Complementar 03/IN01/DISC/GSIPR. Diretrizes para Elaboração de Política de Segurança da Informação e Comunicações nos Órgão e Entidades da Administração Pública Federal. Diário oficial da União, n. 125, 03 jul 2009. Disponível em: < http://dsic.planalto.gov.br/legislacao/nc\_3\_psic.pdf>. Acesso em: 18 de agosto de 2018.

\_\_\_\_\_\_, Norma Complementar 04/IN01/DISC/GSIPR. Gestão de Risco de Segurança da Informação e Comunicações – GRSIC nos Órgão e Entidades da Administração Pública Federal. Diário oficial da União, n. 156, 17 ago 2009. Disponível em: <http://dsic.planalto.gov.br/legislacao/nc\_04\_grsic.pdf> Acesso em: 18 de agosto de 2018.

\_\_\_\_\_\_, Norma Complementar 05/IN01/DISC/GSIPR. Criação de Equipes de Tratamento e Resposta a Incidentes em Redes Computacionais nos Órgão e Entidades da Administração Pública Federal. Diário oficial da União, n. 156, 17 ago 2009. Disponível em: <http://dsic.planalto.gov.br/legislacao/nc\_05\_grsic.pdf> Acesso em: 18 de agosto de 2018.

\_\_\_\_\_\_, Portaria n. 34, de 05 de agosto de 2009. Institui Grupo de Trabalho de Segurança das Infraestruturas Críticas da Informação, no âmbito do Comitê Gestor de Segurança da Informação - CGSI. Diário oficial da União, n. 149, 06 ago 2009. Disponível em: <http://www.mctic.gov.br/mctic/opencms/legislacao/portarias/migracao/Portaria\_CGSIPR\_n\_34\_de\_05082009.html> Acesso em: 25 de agosto de 2018.

\_\_\_\_\_\_, Portaria n. 35, de 06 de agosto de 2009. Institui Grupo de Trabalho de Criptografia, no âmbito do Comitê Gestor de Segurança da Informação - CGSI. Diário oficial da União, n. 150, 07 ago 2009. Disponível em: < http://www.transportes.gov.br/images/Portaria\_223-2009.LLX.pdf> Acesso em: 25 de agosto de 2018.

BURNETT, Steve; PAINE, Stephen. Criptografia e Segurança: O Guia Oficial RSA. Rio de Janeiro: Campus, 2002.

CANONGIA, Claudia; MANDARINO JR., R. Segurança cibernética: o desafio da nova Sociedade da Informação. 2009. Artigo Científico – Parc. Estrat., Brasília-DF. v14. n 29. p. 21-46, 2009.

CARNEIRO, Alberto. Introdução à Segurança dos Sistemas de informação. Lisboa: FCA Editores, 2002. In: PEREIRA, Pedro Jorge Fernandes. Segurança da informação digital. Cadernos BAD 1. 2005. Lisboa: BAD. p.66-80, 2005.

DEPARTMENT OF HOMELAND SECURITY (DHS). National Infrastructure Protection Plan: partnering to enhance protection and resiliency. EUA: DHS, 2009. p.12.

GANDINI, João Agnaldo Donizeti; SALOMÃO, Diana Paola da Silva; JACOB, Cristiane. A SEGURANÇA DOS DOCUMENTOS DIGITAIS. 2011. Artigo Científico – Postado em: 03 mar 2011. No site: Portal de e-governo, inclusão digital e sociedade do conhecimento. Disponível em: <http://www.egov.ufsc.br/portal/conteudo/seguran%C3%A7a-dos-documentos-digitais>. Acessado em: 16 ago 2018.

INTERNATIONAL TELECOMMUNICATION UNION (ITU). Global Cybersecurity Agenda (GCA): framework for international cooperation. Switzerland: ITU, 2007. p.10. In: \_\_\_\_\_\_. Segurança cibernética: o desafio da nova Sociedade da Informação. 2009. Artigo Científico – Parc. Estrat., Brasília-DF. v14. n 29. p. 21-46, 2009.

LYRA, Maurício Rocha. Segurança e Auditoria em Sistemas de Informação. 2 ed. Rio de Janeiro: Ciência Moderna, 2017.

MANDARINO JR., R. Um estudo sobre a segurança e a defesa do espaço cibernético brasileiro. 2009. Monografia aprovada no Curso de Especialização em Gestão de Segurança da Informação e Comunicações. Brasília: Universidade de Brasília – UNB/Departamento de Ciência da Computação, jun 2009. p.29. In: \_\_\_\_\_\_. Segurança cibernética: o desafio da nova Sociedade da Informação. 2009. Artigo Científico – Parc. Estrat., Brasília-DF. v14. n 29. p. 21-46, 2009.

ORGANIZATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (OECD). Guidelines for the security of information systems and networks: towards a culture of security. Adopted as a Recommendation of the OECD Council at its 1037th Session on 25 july 2002. Paris: OECD, 2002. 28p. In: \_\_\_\_\_\_. Segurança cibernética: o desafio da nova Sociedade da Informação. 2009. Artigo Científico – Parc. Estrat., Brasília-DF. v14. n 29. p. 21-46, 2009.

\_\_\_\_\_\_, Recommendation of the council on the protection of critical information infrastructure: Adopted as a Recommendation of the OECD Council at its 1172th Session on 30 april 2008. Seoul, jun. 2008. In: \_\_\_\_\_\_. Segurança cibernética: o desafio da nova Sociedade da Informação. 2009. Artigo Científico – Parc. Estrat., Brasília-DF. v14. n 29. p. 21-46, 2009.

PEREIRA, Pedro Jorge Fernandes. Segurança da informação digital. Cadernos BAD 1. 2005. Lisboa: BAD. p.66-80, 2005.

SILVA, D. R. P. da; STEIN, Lilian Milnitsky. Segurança da informação: uma reflexão sobre o componente humano. 2007. Artigo Científico – Ciência & Cognição, 2007. Vol.10. p. 46-53. Pontifícia Universidade Católica do Rio Grande do Sul (PUCRS). Porto Alegre-RS, 2007.

SUND, Christine. Promoting a culture of Cybersecurity. In: ITU REGIONAL CYBERSECURITY FORUM FOR EASTERN AND SOUTHERN AFRICA, Lusaka, 25-28 Aug 2008, Lusaka: ITU, 2008. In: \_\_\_\_\_\_. Segurança cibernética: o desafio da nova Sociedade da Informação. 2009. Artigo Científico – Parc. Estrat., Brasília-DF. v14. n 29. p. 21-46, 2009.