FACULDADE DE TECNOLOGIA DE AMERICANA

Curso Superior de Tecnologia em Segurança da Informação

Alisson Rogério Rodrigues Cinque

Americana, SP
2018

FACULDADE DE TECNOLOGIA DE AMERICANA

Curso Superior de Tecnologia em Segurança da Informação

Alisson Rogério Rodrigues Cinque

Segurança da Informação em Inteligência Artificial

Artigo desenvolvido em cumprimento à exigência curricular do Curso Superior de Tecnologia em Segurança da Informação, sob a orientação do (a) Prof. Dr. Renato Kraide Soffner.

Área de concentração: Tecnologias de Redes de computadores.

Americana, SP

2018

Segurança da Informação em Inteligência Artificial

Trabalho de graduação apresentado como exigência parcial para obtenção do título de Tecnólogo em **Segurança da Informação** pelo CEETEPS/Faculdade de Tecnologia – FATEC/ Americana.
Área de concentração: Tecnologias de Redes de computadores.

Americana, 03 de Dezembro de 2018.

Banca Examinadora:

Renato Kraide Soffner
Doutor
Fatec Americana

Márcio Roberto Baldo Taglietta
Especialista
Fatec Americana

Acácia de Fátima Ventura
Doutora
Fatec Americana

RESUMO

A Inteligência Artificial é um campo abrangente e que cresce na busca de se saber até onde o homem é capaz de representar sua própria inteligência na máquina, a fim de utilizar a tecnologia em seu favor e, assim, transformar os processos do mundo que afetam a qualidade de vida da humanidade. Vivemos dias de profunda transformação da informação digital, e a Inteligência Artificial é parte desse processo. Mesmo com este nível de tecnologia, temos que estar atentos às preocupações decorrentes da Segurança da Informação, pois, através das politicas de segurança será possível trabalhar e desenvolver novas aplicações e dispositivos utilizando a Inteligência Artificial. E o objetivo deste artigo é tratar destes dois assuntos, que está em fase de crescimento e apresentar os pontos de conexão entre eles.

Palavras Chaves: Inteligência artificial; Segurança da Informação; Tecnologia Digital.

ABSTRACT

Artificial Intelligence is a broad field that grows in the quest to know how far man is able to represent his own intelligence in the machine in order to utilize the technology in his favor and thus transform the processes of the world that affect quality of life of humanity. We live days of deep transformation of digital information, and Artificial Intelligence is part of this process. Even with this level of technology, we have to be attentive to the concerns of Information Security, because through security policies it will be possible to work and develop new applications and devices using Artificial Intelligence. And the purpose of this article is to address these two issues, which is in the growth phase and present the connection points between them.

Key Words: Artificial Intelligence; Information security; Digital Technology.

LISTA DE ABREVIATURAS

IA - **Inteligência Artificial**

SI - **Segurança da Informação**

TI - **Tecnologia da Informação**

SO - **Sistema Operacional**

PSI - **Politicas de Segurança da Informação**

1. Introdução

O presente artigo apresenta as relações entre a Inteligência Artificial (IA) e a área de Segurança da Informação (SI). A Inteligência Artificial é uma área em grande crescimento nas ciências e em engenharia. Surgiu após a Segunda Guerra Mundial, com as ideias de Alan Turing sobre uma máquina inteligente.

Atualmente está inserida em ampla variedade de aplicações abrangendo aprendizagem e percepção, calibragem, decisão – e até em trabalhos específicos, como jogos de xadrez, teoremas matemáticos, diagnóstico de doenças, e carros autônomos - que hoje estão em desenvolvimento e em teste nas ruas e estradas.

O objetivo deste trabalho é buscar os pontos de contato entre a Inteligência Artificial e a Segurança da Informação, e mostrar como estes dois campos da tecnologia estão trabalhando juntos para garantir inovação e agilidade de processos, que devem ser confiáveis e seguros. Para isso, utilizou-se a metodologia qualitativa de pesquisa bibliográfica.

Visando a necessidade de trabalhar cada dia mais com os pilares da Segurança da Informação, que são Confidencialidade, Disponibilidade e Integridade, justifica-se fazer esse estudo para abranger as vantagens de trabalhar com a Inteligência Artificial, e como a Segurança da Informação se alinha com essa tecnologia juntamente com os seus pilares para manter a ferramenta segura.

2. Inteligência Artificial

Segundo Minsky (1986), Inteligência Artificial é

> O ato de forçar definições para as coisas que nós não entendemos completamente geralmente causa mais danos do que benefícios. Além disso, apenas em lógica e matemática é que as definições detêm perfeitamente os conceitos. As coisas com as quais lidamos na vida prática são frequentemente muito complicadas para permitirem uma representação clara baseada em expressões compactas. Em todo caso, não podemos nos privar de buscar uma definição para as coisas, no sentido de entender o que elas são.

O estudo da Inteligência Artificial (IA) iniciou-se em 1940 e era utilizada apenas para encontrar novas utilidades para os computadores. Com a segunda Guerra Mundial, existiu a necessidade de encontrar novas formas para melhorar e desenvolver os armamentos utilizados na guerra. Não podemos deixar de citar Alan Turing um dos percursores da área, responsável por acelerar a quebra do código da máquina Enigma, máquina essa utilizada para mandar informações criptografadas durante a Segunda Guerra. (CIRIATO, 2018, p.1)

Após muitos anos surgiram várias linhas de estudo, uma delas é o estudo das redes neurais onde queriam desenvolver máquinas para imitar um ser humano, e foi nos anos 60 que o nome Inteligência Artificial foi criada, pois os pesquisadores acreditavam na possibilidade de máquinas serem criadas para realizar atividades que humanos realizavam. Essa é uma área da computação que visa estudar e criar equipamentos que simulem o ser humano, tais como raciocinar, perceber, tomar decisões e resolver problemas. Essa é impulsionada pelo grande desenvolvimento das tecnologias, principalmente, as voltadas para a tecnologia da informação, que permitem que novos estudos sejam introduzidos à IA (CIRIATO, 2018, p.2)

> Na Figura 1.1 podemos visualizar oito definições de IA dispostas ao longo de duas dimensões. Em linhas gerais, as que estão na parte superior da tabela se relacionam a processos de pensamento e raciocínio, enquanto as definições da parte inferior se referem ao comportamento. As definições do lado esquerdo medem o sucesso em termos de fidelidade ao desempenho humano, enquanto as definições do lado direito medem o sucesso comparando-o a um conceito ideal de inteligência, chamado de

racionalidade. Um sistema é racional se "faz a coisa certa", dado o que ele sabe. Historicamente, todas as quatro estratégias para o estudo da IA têm sido seguidas, cada uma delas por pessoas diferentes com métodos diferentes. Uma abordagem centrada nos seres humanos deve ser em parte uma ciência empírica, envolvendo hipóteses e confirmação experimental. Uma abordagem racionalista1 envolve uma combinação de matemática e engenharia. Cada grupo tem ao mesmo tempo desacreditado e ajudado o outro. Vamos examinar as quatro abordagens com mais detalhes. (RUSSELL, 2013, p.25)

Figura 1.1 Algumas definições de Inteligência Artificial, organizadas em quatro categorias

Pensando como um humano	**Pensando racionalmente**
"O novo e interessante esforço para fazer os computadores pensarem (...) *máquinas com mentes*, no sentido total e literal." (Haugeland, 1985) "[Automatização de] atividades que associamos ao pensamento humano, atividades como a tomada de decisões, a resolução de problemas, o aprendizado..." (Bellman, 1978)	"O estudo das faculdades mentais pelo uso de modelos computacionais." (Charniak e McDermott, 1985) "O estudo das computações que tornam possível perceber, raciocinar e agir." (Winston, 1992)
Agindo como seres humanos	**Agindo racionalmente**
"A arte de criar máquinas que executam funções que exigem inteligência quando executadas por pessoas." (Kurzweil, 1990) "O estudo de como os computadores podem fazer tarefas que hoje são melhor desempenhadas pelas pessoas." (Rich and Knight, 1991)	"Inteligência Computacional é o estudo do projeto de agentes inteligentes." (Poole *et al*., 1998) "AI... está relacionada a um desempenho inteligente de artefatos." (Nilsson, 1998)

Fonte: (RUSSEL,2013, p.25)

A tecnologia tem focado na exploração do estudo da capacidade de raciocínio humano e com o desenvolvimento de algorítmos matemáticos de resolução de problemas em modo geral. A ideia de construir uma máquina capaz de raciocinar e realizar algumas tarefas como humano é muito estimulante, essas áreas tem sido estudadas e alguns resultados são vistos nos dias de hoje com os jogos, tradução de idiomas, diagnósticos de falhas, robótica, e carros autônomos que já estão evoluindo e já se encontram em testes nas ruas de algumas grandes cidades.

3. Segurança da Informação

Com o crescimento das tecnologias conectadas a redes de computadores como forma de trabalho e até entretenimento, está havendo um despertar para manter a Segurança da Informação mais atualizada e, com isso, diminuir as suas vulnerabilidades.

Segundo Laureano (2004), o crescimento das redes de computadores e a internet fizeram com que o tratamento das informações fosse alterado, já que a utilização dessas informações é muito mais ampla quem em sistemas privados. Por esse motivo é muito importante manter as formas de segurança nos sistemas de informação sempre atualizados e que os mesmos sejam projetados a garantir de que acessos não autorizados venham ocorrer.

Para melhor definir o conceito de Segurança da Informação será necessário citar três destaques.

> 1) Preservação da confidencialidade, integridade e disponibilidade da informação; adicionalmente, outras propriedades, tais como autenticidade, responsabilidade, não repúdio e confiabilidade, podem também estar envolvidas. (ABNT NBR ISO/IEC 27002: 2005)
>
> 2) Podemos definir a Segurança da Informação como uma área do conhecimento dedicada à proteção de ativos da informação contra acessos não autorizados, alterações indevidas ou sua indisponibilidade. (Sêmola, 2003, p. 43).
>
> 3) A segurança de informação é caracterizada pela aplicação adequada de dispositivos de proteção sobre um ativo ou um conjunto de ativos visando preservar o valor que este possui para as organizações. A aplicação destas proteções busca preservar a confidencialidade, a integridade e a disponibilidade (CID), não estando restritos somente a sistemas ou aplicativos, mas também informações armazenadas ou veiculadas em diversos meios além do eletrônico ou em papel. (BASTOS & CAUBIT, 2009, p. 17).

Em todos os conceitos citados acima existe algo em comum, todos definem que a confidencialidade, integridade e disponibilidade como sendo os 3 principais pilares da Segurança da Informação, Segundo Lyra (2008, p.4):

> Quando falamos em Segurança da Informação, estamos nos referindo a tomar ações para garantir a confidencialidade, integridade, disponibilidade e demais aspectos da segurança das informações dentro das necessidades do cliente.

3.1. Conceitos dos Pilares

Vejamos agora os conceitos sobre os três pilares da Segurança da Informação

Confidencialidade: "Garantia de que o acesso à informação é restrito aos seus usuários legítimos." (BEAL, 2008, p. 1), o acesso à informação deverá ser permitido apenas para o usuário ou grupo de usuários através de identificação e autenticação.

Integridade: "Toda informação deve ser mantida na mesma condição em que foi disponibilizada pelo seu proprietário, visando protegê-las contra alterações indevidas, intencionais ou acidentais" (SÊMOLA, 2003, p. 45), a informação deve sempre estar protegida para que não haja alterações e com isso manter a integridade da informação.

Disponibilidade: "Garantia de que a informação e os ativos associados estejam disponíveis para os usuários legítimos de forma oportuna" (BEAL, 2008, p. 1), a informação deverá sempre estar disponível para o acesso.

Com os três itens descritos acima, haverá um suporte para que as empresa e ou organizações consigam atingir os objetivos e consigam garantir que as suas informações sejam mais seguras e, com isso, garantir um ambiente seguro e mais organizado trazendo benefícios e um aumento da produtividade dos usuários, pois haverá mais controle sobre os equipamentos e informações que estarão trabalhando.

Segundo Lyra (2008, p.4), a segurança precisa de mais alguns itens complementares para garantir a real Segurança da Informação.

- Autenticação: "Garantir que um usuário é de fato quem alega ser".
- Não repúdio: "Capacidade do sistema de provar que um usuário executou uma determinada ação".
- Legalidade: "Garantir que o sistema esteja aderente à legislação".

- Privacidade: “Capacidade de um sistema de manter anônimo um usuário, impossibilitando o relacionamento entre o usuário e suas ações”.
- Auditoria: “Capacidade do sistema de auditar tudo o que foi realizado pelos usuários, detectando fraudes ou tentativas de ataque”.

Trabalhando com os conjuntos de Segurança da Informação como definição/elaboração de processos, políticas de Segurança da Informação (PSI), procedimentos, treinamento de profissionais, o uso de ferramentas de monitoramento e controle, será possível alcançar os objetivos de manter os ativos da informação protegidos.

3.2. Vulnerabilidades

A vulnerabilidade é uma fragilidade ou ponto fraco de um ativo, e pode ser definida como sendo um erro de procedimento na elaboração de um sistema de informação, falha ou má configuração em um equipamento ou aplicativos de segurança de extrema importância para uma empresa ou organização. Esse tipo de erro ou falha pode ocorrer propositalmente ou não, com isso gerando ou criando uma vulnerabilidade de um processo ou informação. Segundo Beal (2008, p. 14) o conceito para vulnerabilidade é tratado como uma “fragilidade que poderia ser explorada por uma ameaça para concretizar um ataque”, e segundo Lyra (2008, p.06) “Essas vulnerabilidades poderão ser exploradas ou não, sendo possível que um ativo da informação apresente um ponto fraco que nunca será efetivamente explorado”.

Assim que as falhas são detectadas é necessário entrar com algumas providencias, e a primeira dela é identificar onde aconteceu ou esta acontecendo e corrigi-la da melhor maneira, abaixo citaremos algumas vulnerabilidades segundo Sêmola (2003, p.48).

> Físicas - Instalações prediais fora do padrão; salas de CPD mal planejadas; falta de extintores, detectores de fumaça e de outros recursos para combate a incêndio em sala com armários e fichários estratégicos; risco de explosões, vazamento ou incêndio.
>
> Naturais - Computadores são suscetíveis a desastres naturais, como incêndios, enchentes, terremotos, tempestades, e outros,

como falta de energia, acúmulo de poeira, aumento umidade e de temperatura etc.

Hardware - Falha nos recursos tecnológicos (desgaste, obsolescência, má utilização) ou erros durante a instalação.

Software - Erros na instalação ou na configuração podem acarretar acessos indevidos, vazamento de informações, perda de dados ou indisponibilidade do recurso quando necessário.

Mídias - Discos, fitas, relatórios e impressos podem ser perdidos ou danificados. A radiação eletromagnética pode afetar diversos tipos de mídias magnéticas.

Comunicação - Acessos não autorizados ou perda de comunicação.

Humanas - Falta de treinamento, compartilhamento de informações confidenciais, não execução de rotinas de segurança, erros ou omissões; ameaça de bomba, sabotagens, distúrbios civis, greves, vandalismo, roubo, destruição da propriedade ou dados, invasões ou guerras."

4. Considerações Finais

A Inteligência Artificial e a Segurança da Informação são áreas de TI que já trabalham juntas, mas sendo a IA uma área em constante desenvolvimento ainda gera insegurança e incerteza sobre as garantias dessa tecnologia. Teme-se, inclusive, o que uma máquina poderá fazer para o ser humano, com o medo de nos tornarmos reféns além do receio de perdermos o trabalho para a dimensão máquina.

O tema dos chamados "carros autônomos" é comprovação de tal receio com as novidades da IA, pois esse tem sido o maior foco em desenvolvimento da tecnologia e o seu crescimento tem sido constante.

Segundo o Grupo Gartner (2018), haverá aproximadamente 250 milhões de veículos conectados e rodando nas ruas e rodovias em dois anos, com o retorno de mais de US$900 bilhões até 2035. Esses carros geram muitas informações e são repletos de sensores dentro e fora, passando a sensação de segurança. Mas a segurança de que estamos falando vai além das seguranças físicas. Sabe-se que os carros autônomos e os futuros robôs irão gerar muitos dados, e é com esse tipo de segurança que devemos nos preocupar. Esses dados poderão ser utilizados para gerar informações e com isso buscar novas formas de gerar economia e agilidade em algumas de nossas rotinas, por exemplo, os carros aprenderem sua rotina e escolher qual o melhor caminho para ir ao trabalho. Com a Inteligência Artificial algumas de nossas responsabilidades passarão a ser das máquinas (MATIAS NETO, 2017). Essa responsabilidade vem acompanhada de preocupações em relação à segurança dos dados gerados, e em como a integridade, confidencialidade, disponibilidade deverão manter os equipamentos e as informações longes das pessoas mal intencionadas, como os crackers e hackers.

Devemos nós preocupar com o avanço e interesses das pessoas más intencionadas e que estão em busca de conseguir informações com grandes ataques, como aconteceu em maio de 2017, pudemos ver que os ataques do wannacry, em que atingiu mais de 150 países e que gerou um alerta em várias organizações, foi evidente que esse ataque foi em busca de prejuízos financeiros, nesse tipo de situação é possível recuperar-se, mas e se o caso fosse um ataque a algum carro autônomo ou robô, em que será colocado à vida humana em risco. Com isso devemos procurar avançar nos estudos sobre a Segurança da Informação e sempre buscar novas alternativas que mantenham as

tecnologias seguras, pois a vulnerabilidades e falhas sempre existirão e será com elas que deveremos nos preocupar, pois de várias que existem, uma delas é o fator humano, sendo esse o mais perigoso e falho que existe, pois não sabemos as intenções das pessoas por trás de uma maquina.

Referências

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27001:2005** Tecnologia da informação: técnicas de segurança. Rio de Janeiro, 2006.

BASTOS Alberto; CAUBIT, Rosângela. **Gestão de Segurança da Informação. ISO 27001 e 27002 Uma Visão Prática**. Rio Grande do Sul. Zouk, 2009.

BEAL, Adriana. **Segurança da Informação. Princípios e Melhores Práticas para a Proteção dos Ativos de Informação nas Organizações**. São Paulo. Atlas, 2005

CIRIATO, Douglas. **"O que é Inteligência Artificial?"**; tecmundo.com.br. Disponível em <http://ceavi.udesc.br/arquivos/id_submenu/487/o_que_e_inteligencia_artificial.pdf>. Acesso em:25 Mar 2018

GARTNER GROUP. **Gartner Says By 2020, a Quarter Billion Connected Vehicles Will Enable New In-Vehicle Services and Automated Driving Capabilities**. Disponível em <https://www.gartner.com/newsroom/id/2970017>, Acesso em: 29 Abril 2018.

INTERNATIONAL STANDARDIZATION ORGANIZATION. **ISO/IEC 27035:2011**. Disponível em: <https://www.iso.org/standard/44379.html>. Acesso em: 23 de Maio de 2018.

LYRA, Maurício Rocha. **Segurança e Auditoria em Sistemas de Informação**. Rio de Janeiro: Ciência Moderna, 2008.

MINSKY, Marvin. **The society of mind**. New York: Simon & Schuster, 1986

NETO, José Matias. **Cibersegurança em um mundo com Inteligência Artificial**. Disponível em < http://cio.com.br/opiniao/2017/06/12/cibersegurança-em-um-mundo-com-inteligencia-artificial/> Portal CIO, 2017. Acesso em: 25 Abril 2018.

PORTAL GLOBO.COM. **A Inteligência Artificial pode ser usada em ciberataques?** Disponíivel em: <https://epoca.globo.com/tecnologia/experiencias-digitais/noticia/2017/09/inteligencia-artificial-pode-ser-usada-em-ciberataques-diz-pesquisador.html>, acesso em: 29 de Abril de 2018.

PORTAL TI ESPECIALISTAS. **As previsões de TI para 2018: Inteligência Artificial, segurança cibernética e IoT**. Disponível em <https://www.tiespecialistas.com.br/as-previsoes-de-ti-para-2018-inteligencia-artificial-seguranca-cibernetica-e-IoT/>, Acesso em: 25 Abril 2018.

RUSSEL, Stuart; NORVIG, Peter **Inteligência artificial**. Tradução Regina Célia Simille. Rio de Janeiro: Elsevier, 2013

SANTOS, Marco Aurélio da Silva. **Inteligência Artificial**. Brasil Escola. Disponível em <https://Brasilescola.uol.com.br/informatica/inteligencia-artificial.htm>. Acesso em: 25 Mar de 2018.

SÊMOLA, Marcos. **Gestão da segurança da informação**: uma visão executiva. Rio de Janeiro: Elsevier, 2003

SUNDMAEKER, H.; GUILLEMIN, P.; FRIESS, P.; WOELFFLÉ, S. **Vision and challenges for realising the Internet of Things**. Volume 20, EUR-OP, 2010.