DOI: 10.5748/16CONTECSI/DSC-6195

APLICAÇÃO DE ALGORITMOS DE INTELIGÊNCIA ARTIFICIAL PARA PREDIÇÃO DE ASSALTOS A BANCOS NO ESTADO DO CEARÁ

A tecnologia atingiu altos níveis de disponibilidade, armazenamento, processamento e grande redução nos custos de operação, possibilitando o uso com qualidade de algoritmos de Inteligência Artificial (IA). O objetivo desta pesquisa é aplicar técnicas modernas de computação para combater os crimes de assaltos a bancos no estado do Ceará, utilizando modelos preditivos de IA. A metodologia utilizada é a quantitativa para apresentar os resultados estatísticos apurados pelos algoritmos de IA. Foram utilizadas também a pesquisa bibliográfica e a pesquisa aplicada, pois buscamos usar os resultados desta pesquisa em benefício da segurança pública do Ceará, podendo ser replicada para outros estados do Brasil. Os resultados apurados mostram um padrão de assalto dos criminosos: 54,6% dos assaltos são em localidades com menos de 30 mil habitantes, 46,2% usam explosivos, 61% durante a madrugada e 93% em dias úteis, sendo 45,4% nos primeiros cinco dias ou nos últimos cinco dias do mês e 77% dos casos em agências do Banco do Brasil ou Bradesco. Quando aplicamos os modelos preditivos obtivemos um nível de acurácia de 85,43% mais ou menos 3,25% de erro. Concluindo, podemos inferir que um em cada quatro assalto a banco no estado do Ceará apresentará um padrão conhecido e que a aplicação das técnicas corretas nos dados oficiais trará maior assertividade às nossas predições.

Palavras-chaves: Inteligência Artificial; Criminalidade; Predição; Algoritmos.

APPLICATION OF ARTIFICIAL INTELLIGENCE ALGORITHMS FOR BANK ROBBERIES PREDICTION IN THE STATE OF CEARÁ

Technology has reached high levels of availability, storage, processing and a great reduction in the operating costs, allowing the use with quality of Artificial Intelligence (AI) algorithms. The objective of this research is to apply modern computational techniques to combat the crimes of bank robberies in the state of Ceará, using predictive AI models. The quantitative methodology is used to present the statistical results obtained by the IA algorithms. We also used bibliographical research and applied research, as we sought to use the results of this research for the benefit of public security in Ceará, and could be replicated to other Brazilian states. The results show an assault pattern from criminals: 54.6% of assaults are in locations with less than 30,000 inhabitants, 46.2% use explosives, 61% during the night and 93% in working days, being 45.4% % in the first five days or in the last five days of the month and 77% in Banco do Brasil or Bradesco branches. When we applied the predictive models we obtained a 85.43% level of accuracy with a margin of error of 3.25% (plus or minus) . In conclusion, we can infer that one in four bank robbery in the state of Ceará will present a known pattern and that the application of correct techniques in the official data will bring greater assertiveness to our predictions.

Keywords: Artificial Intelligence; Crime; Prediction; Algorithms.

INTRODUÇÃO

Para os pesquisadores de criminalidade no Brasil, somente nos anos de 1980 é que a violência como problema social ganha visibilidade nas grandes cidades e nos meios de comunicação de massa, passando a ser relevante para os governantes. Embora este fenômeno ganhasse destaques em matérias de jornais e telejornais no início dos anos de 1970, é somente

na década de 1980 que passa a ser debatido e considerado um fator constitutivo do cotidiano VENTURA, 1992).

Com o crescimento das cidades fora do eixo das capitais nos anos 1970 e 1980, cresce o interesse de interiorização pelas instituições financeiras, que passam a ter grandes redes de agências espalhadas pelo Brasil, atraindo o interesse de criminosos para essas regiões, consideradas "menos protegidas" pela segurança pública. Já nos anos 2000, passamos a ver cidades pacatas do interior brasileiro sendo atacadas por bandos bem organizados e fortemente armados.

Segunda a pesquisa de Aquino (2018), olhando pelo lado do criminoso: os assaltos contra instituições financeiras são operações sofisticadas, resultantes de elaborados planos e que mobilizam uma complexa infraestrutura. Eximindo-se da ênfase sobre sua dimensão criminosa e violenta, são elementos significativos para seus protagonistas, que vivenciam a organização de um assalto como atividade econômica e "trabalho" de alto risco. O desempenho dramático ou as performances acionadas diante dos seus reféns, com o intuito de amedrontá-los e levá-los a colaborar com o roubo, constituem habilidades relevantes e denotativas de competências, entre estes "profissionais do crime".

A segurança pública, assim como a saúde e a educação, faz parte dos três grandes desafios que do Brasil tem para os próximos anos. A organização de grupos criminosos e facções criminosas aterrorizam as pequenas localidades do interior do Brasil, em especial para este estudo nos estados do Ceará, Piauí, Paraíba e Rio Grande do Norte na região Nordeste.

O Gráfico 1 apresenta a evolução dos assaltos a bancos ocorridos no estado do Ceará no período de 2015 a 2018, dados públicos apurados no site do Sindicato dos Bancários do Estado do Ceará. Neste gráfico podemos observar que 2016 foi o pior ano com 76 assaltos, média de 1,4 assaltos por semana, mas esses delitos reduziram nos últimos dois anos para uma média de 0,83 assalto por semana em 2018, que ainda configura um número assustador que nos permite inferir que praticamente toda semana haverá um assalto a banco no Ceará.

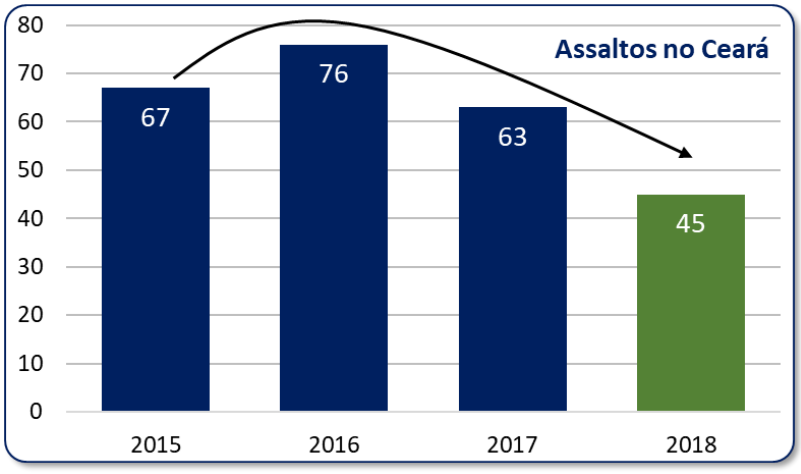

Gráfico 1 – Evolução dos assaltos a bancos no estado do Ceará de 2015 a 2018.
Fonte – Sindicato dos Bancários do estado do Ceará (2018).

Como informativo e para uso comparativo, o Jornal "O Estado de São Paulo", divulgou no dia 12/fev/2019 a seguinte nota: "SOROCABA - Em dois anos, foram registrados 202 ataques com explosivos a bancos no Estado de São Paulo. Foram 100 ataques em 2017 e 102 em 2018, segundo dados da Secretaria de Segurança Pública do Estado. Os alvos foram os caixas eletrônicos ou os cofres das agências. Os números deste ano ainda não estão disponíveis, mas as quadrilhas continuam agindo, principalmente em cidades pequenas

do interior do Estado". Nessa nota podemos verificar que o problema é nacional e São Paulo pela sua dimensão e volume financeiro circulando, apresentou mais que o dobro de ataques em relação ao estado do Ceará.

As pequenas localidades coerentemente só possuem pequenas guarnições de segurança pública, capazes de cuidar do dia a dia dessas populações, mas incapazes de confrontar grandes grupos bem organizados e com armamentos pesados, sendo esta uma função de um grupamento de elite da polícia, mais preparado, mais organizado e que utilize inteligência estratégica para detectar e combater as ações criminosas contra as instituições financeiras instaladas nessas localidades.

As ações criminosas desses grupos visam pequenas localidades com policiamento reduzido e agências bancárias que efetuam pagamento de benefícios sociais, normalmente nos últimos dias do mês. Neste contexto os meliantes invadem as cidades, explodem as agências bancárias, fazem reféns e "tocam o terror" por toda comunidade, roubando os recursos sociais, deixando ainda como consequência, essa localidade passar vários meses sem instituição bancária funcionando, e eventualmente para sempre, quando a instituição decide fechar a agência definitivamente por falta de segurança.

A Figura 1 apresenta o estado de destruição da agência do Banco do Brasil de Farias Brito, localidade no interior do Ceará, após o uso de explosivos em ação de criminosos no dia 13/set/2018.

Figura 1 – Agência do Banco do Brasil de Farias Brito, interior do Ceará.
Fonte – Jornal G1/CE do dia 13/09/2018.

Nos últimos anos o mundo vem passado por uma revolução tecnológica, que até mesmo os mais otimistas não teriam imaginado esse nível de evolução. Estamos vendo, a cada dia, o poder dos algoritmos e da Inteligência Artificial em várias atividades do nosso dia a dia sem percebermos, e não demora muito para que estas tecnologias mudem a forma que vivemos e como vemos o mundo. É usando estes recursos tecnológicos que este projeto de pesquisa inovador se propõe a gerar conhecimento tático e estratégico de segurança pública no combate aos crimes de assalto à bancos, que levam o dinheiro, a dignidade e o sossego das comunidades interioranas em todo território nacional.

A evolução tecnológica computacional tem origem nas décadas de 50 e 60 com os Mainframes, que eram disponíveis só para grandes organizações públicas e privadas. Somente na década de 80 chega a democratização da tecnologia com os PCs (Personal Computers) e a

TV por assinatura. Na década de 90 a internet, a telefonia móvel e a privatização das telecomunicações no Brasil. Todo esse caminho foi necessário para que a partir de 2010 pudéssemos assistir à popularização das tecnologias com a chegada da computação em nuvem, smartphones modernos, mobilidade, e assim criar um ambiente tecnologicamente adequado para processar grandes volumes de dados com capacidade para manipular textos, fotos, vídeos, TVs, links, tudo em alta velocidade e disponibilidade. É neste contexto que a IA (Inteligência Artificial) se desenvolve, possibilitando que qualquer instituição possa se beneficiar dos seus poderosos recursos de geração de conhecimento a partir de grandes volumes de dados.

A inteligência Artificial começou a ser estudada no pós-guerra na década de 50, mas ficou adormecida por várias décadas a espera das condições ideais para o seu desenvolvimento, que encontramos agora, como: computação em nuvem, algoritmos complexos, Big Data e alto poder dos computadores atuais em armazenar e processar grandes volumes de dados em curto espaço de tempo e com alta disponibilidade.

Segundo Luger (2013), a Inteligência Artificial (IA) revela um campo de estudo jovem e promissor, onde o principal interesse é encontrar um modo efetivo de entender e aplicar técnicas inteligentes para a solução de problemas e para o planejamento de uma gama de problemas práticos.

Objetivos da pesquisa

O projeto proposto visa atuar na área da Segurança Pública apoiada em tecnologias modernas, como BIGDATA e os algoritmos de Inteligência Artificial (IA): Redes Neurais Artificiais e K-Means para predizer e quando necessário classificar os assaltos à bancos nas localidades do interior dos estados do Ceará, gerando assim conhecimento tático e estratégico para a atuação otimizada de combate a ações dessa natureza pela Segurança Pública do estado.

Objetivos Específicos

Aplicar técnicas e ferramentas de IA (Inteligência Artificial) para beneficiar a comunidade em que estamos inseridos, usando os conhecimentos adquiridos na academia para atingir os seguintes objetivos específicos:

a) Especificar uma solução tecnológica replicável para outras regiões do país;

b) Levantar os requisitos e ferramentas necessárias para essa pesquisa;

REFERENCIAL TEÓRICO

Para melhor explicar a pesquisa proposta, algumas técnicas e conceitos precisam ser descritos e detalhados para o melhor entendimento do projeto.

A criminalidade

Quando se deseja pesquisar a criminalidade, já dispomos de considerável bibliografia referente ao universo do crime, ambientes prisionais, conflitos e políticas de segurança pública. mas temas vinculados à violência não só se consagram como objetos de estudo relevantes nas ciências sociais, mas também têm desencadeado pesquisas capazes de orientar políticas estatais de assistência social e de segurança pública; que discutem motivações e causas de atos e práticas violentas, direcionando a atuação de organizações não governamentais e movimentos sociais (AQUINO, 2018).

Nesses estudos, a maior parte se baseiam em dados secundários e enfatizam as relações entre crime e pobreza ou entre crime e desigualdade social. Quase sempre essas discussões concluem que o crime e a violência no país são resultantes da ineficiência de políticas estatais, sendo frequente apontar a violência como obstáculo aos direitos humanos e ao exercício da cidadania (AQUINO, 2018).

São vários os tipos de crimes que preocupam a população e seus governantes, entre eles: assalto a banco; tráfico de drogas; tráfico de armas; formação de milícias; roubo de cargas; crimes virtuais e homicídios entre outros. Toda essa criminalidade abala o crescimento do país aumentando os custos de segurança pública para patrulhar e investigar, da saúde pública para tratar os feridos dessas guerras, das organizações devido aos roubos de cargas e custos de segurança e da população que vive em o stress diário da segurança pessoal.

As instituições financeiras e seguradoras de valores amargam constantes ataques dos bandos e facções que buscam dinheiro vivo em ataques aos pontos de atendimentos bancários e aos carros de transporte de valores. Segundo o Anuário de Segurança Pública 2018 com dados até 2017, os estados com mais ataques às instituições financeiras foram Rio de janeiro e São Paulo, conforme o Gráfico 2.

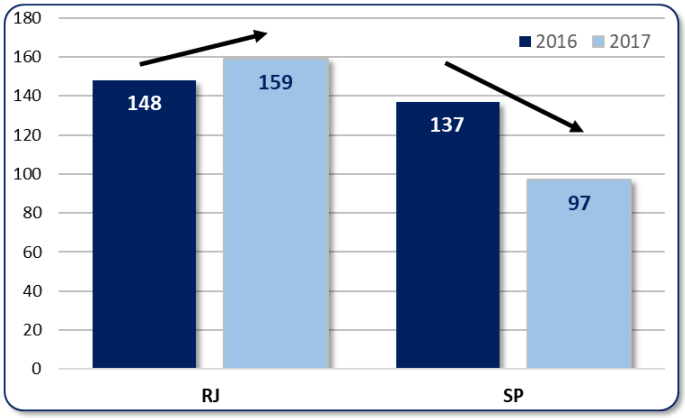

Gráfico 2 – Ataques no Rio de Janeiro e São Paulo em 2016 e 2017.
Fonte – Anuário de Segurança Pública 2018.

No gráfico acima que compara 2016 e 2017, podemos observar um aumento de 7,4% no Rio de Janeiro e uma significativa redução de 29,2% em São Paulo.

Inteligência Artificial (IA)

A Inteligência Artificial tem como objetivo principal entender e aplicar técnicas inteligentes na solução de problemas complexos para as mais variadas aplicações que usam computadores ou máquinas inteligentes. Seguem algumas definições de inteligência artificial usadas na literatura.

> "IA é a parte da Ciência da Computação que se preocupa em desenvolver sistemas computacionais inteligentes, isto é, sistemas que exibem características, as quais nós associamos com a inteligência no comportamento humano - por exemplo: Compreensão da linguagem, aprendizado, raciocínio, resolução de problemas, etc." (BARR; FEIGENBAUM, 1981).

> "IA é o estudo de faculdades mentais através do uso de modelos computacionais" (CHARNIAK; McDERMOTT, 1987).

> "IA é a arte de criar máquinas que executam funções que requerem inteligência quando executadas por pessoas" (KURZWEIL, 1990).

> "IA é o estudo de como fazer os computadores realizarem coisas que, no momento, as pessoas fazem melhor" (RICH; KNIGHT, 1990).

Combinando todos os conceitos acima, chegamos ao conceito mais usado na academia: "IA é o campo da Ciência da Computação que está preocupado com a automação do comportamento inteligente".

Embora um computador não possa ter experiências, estudar e aprender como um ser humano consegue, ele pode utilizar os conhecimentos dos especialistas humanos. Esses conhecimentos podem ser fatos, conceitos, teorias, métodos heurísticos, procedimentos e relacionamentos. O conhecimento também é informação organizada e analisada para torná-la compreensível e aplicável à solução de problemas ou à tomada de decisão (TURBAN et. al., 2010).

Redes Neurais

De acordo com Haykin (2001), uma rede neural é um processador maciçamente e paralelamente distribuído, constituído de unidades de processamento simples, que têm a propensão natural para armazenar conhecimento experimental e torná-lo disponível para uso. A rede neural se assemelha ao cérebro em dois aspectos:

1) O conhecimento é adquirido pela rede a partir de seu ambiente através de um processo de aprendizagem.

2) Forças de conexão entre neurônios, conhecidas como pesos sinápticos, são utilizadas para armazenar conhecimento adquirido.

Um neurônio é uma unidade de processamento de informação fundamental para a operação de uma rede neural (HAYKIN, 2001). O processo utilizado para se obter o conhecimento é chamado de algoritmo de aprendizagem, conforme mostra a Figura 2.

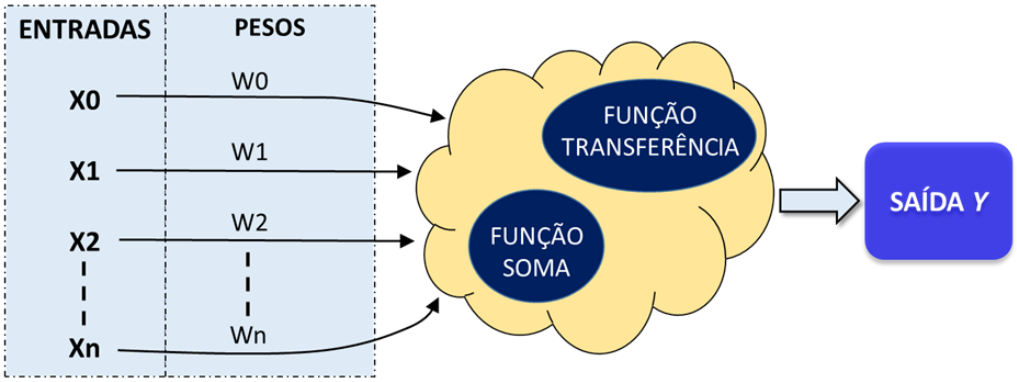

Figura 2 – Modelo de neurônio artificial de McCulloch e Pitts.
Fonte – Adaptação do autor.

De acordo com Braga, Carvalho e Ludemir (2007), o neurônio artificial criado por McCulloch e Pitts é uma simplificação do neurônio biológico como este era conhecido à época. Sua descrição matemática propiciou um modelo com "n" nodos de entrada (correspondente aos dendritos) que recebem os valores X1, X2 até Xn (que correspondem as ativações dos neurônios anteriores), e um neurônio de saída "y" (que corresponde ao axônio). O comportamento das sinapses dos neurônios biológicos, são representados no modelo artificial pelos pesos W1, W2 até Wn, que se referem aos valores de entrada através do

produto destes pelos valores de entrada. Esses pesos podem assumir valores positivos ou negativos correspondendo às sinapses excitatórias ou inibitórias, respectivamente.

Um neurônio dispara quando a soma ponderada dos valores XiWi é confrontado com um limiar (threshold) que determinará sua excitação ou não, correspondente à soma dos impulsos que dispara a sinapse no modelo biológico. A ativação do neurônio de saída é obtida através de uma função de ativação, normalmente uma função logística, sendo as mais comuns a sigmoide e degrau, conforme a Gráfico 3 (BRAGA; CARVALHO; LUDEMIR, 2007).

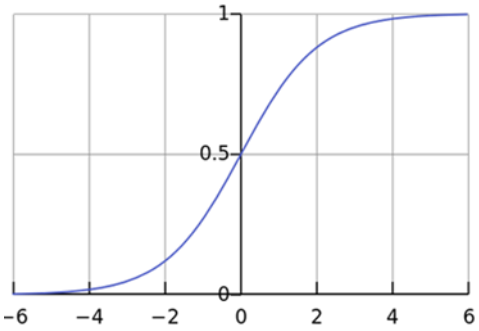

Gráfico 3 – Função Sigmoide.
Fonte – Adaptação do autor.

Agrupamento ou Clusterização

Técnica que segmenta uma base de dados em subconjuntos ou clusters, de forma que os elementos de um cluster compartilhem propriedades comuns que os diferenciem dos elementos dos outros clusters. O objetivo é maximizar a similaridade "Intracluster" e minimizar a similaridade "Intercluster" (FAYYAD; PIATETSKY-SHAPIRO; SMYTH, 1996).

Exemplos de uso: A área de Marketing das empresas usa para segmentar os clientes, agrupando clientes com as mesmas características. A Netflix já usou para prever preferências dos usuários com base nos usuários similares;

A Gráfico 4 apresenta um exemplo fictício de agrupamento de dados em 03 (três) *clusters*.

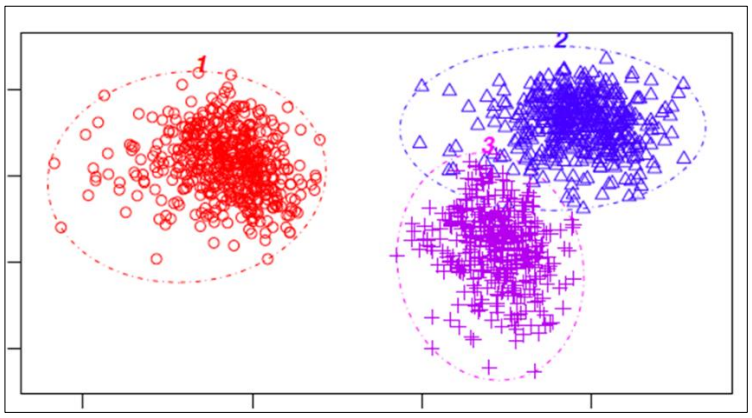

Gráfico 4 – Exemplo fictício de clusterização de dados.
Fonte – Adaptação do autor.

No gráfico acima os *clusters* foram representados por figuras e cores, mas cada um possui um centroide que agrupa ao seu redor todos os componentes com mais características semelhantes a ele.

METODOLOGIA

A metodologia de pesquisa utilizada é a quantitativa, quando utilizamos recursos estatísticos para explicar os fatos, causas e consequências. Será utilizada também a pesquisa aplicada, quando o resultado da pesquisa pode ser aplicado no ambiente real em benefício de um grupo ou comunidade.

A pesquisa quantitativa é um meio para testar teorias objetivas, examinando a relação entre as variáveis. Tais variáveis, por sua vez, podem ser medidas tipicamente por instrumentos, para que os dados numéricos possam ser analisados por procedimentos estatísticos, permitindo aos pesquisadores desta forma de investigação deduzir teorias, explicar alternativas, generalizar e replicar os achados (CRESWELL, 2010).

Também foi utilizado como método a pesquisa bibliográfica, composta de estudos através dos livros, artigos, teses, dissertações, anais de congressos e etc. Visando criar um conteúdo completo e seguro sobre o tema estudado.

A pesquisa bibliográfica procura explicar um problema a partir de referências teóricas publicadas em artigos, livros, dissertações e teses. Pode ser realizada independentemente ou como parte da pesquisa descritiva ou experimental. Em ambos os casos, busca-se conhecer e analisar as contribuições culturais ou científicas do passado sobre determinado assunto, tema ou problema (CERVO; SILVA; BERVIAN, 2007).

Nesta pesquisa foi considerado assalto a banco os casos de explosões de agências, explosões de caixas eletrônicos, arrombamentos e os ataques aos carros-fortes de transportadoras durante o trajeto ou no momento do abastecimento de cédulas.

Os dados coletados para os primeiros resultados foram extraídos do site do Sindicato dos Bancários do estado do Ceará que publica em forma de notícia todos os eventos criminosos nas instituições financeiras do estado. Foram coletados os eventos ocorridos entre 2015 e 2018 no Estado do Ceará. Na continuação da pesquisa ainda serão utilizados os dados da Paraíba e do Rio Grande do Norte, estes dados serão solicitados oficialmente das respectivas secretarias de segurança pública. O estado do Ceará servirá de modelo da pesquisa.

Para utilizar estas informações foi utilizado um processo com os seguintes passos: [1] Identificação das variáveis (atributos) para o banco de dados; [2] Digitação de todos os eventos criminosos no banco de dados; [3] Categorização dos dados; [4] Transformação dos dados categóricos em quantitativos; [5] Aplicação de estatística descritiva; [6] Aplicação dos algoritmos de clusterização; [7] Aplicação dos algoritmos de Redes Neurais; [8] Avaliação e divulgação dos resultados;

Os modelos preditivos e os *clusters* foram gerados a partir do tratamento dos dados coletados onde foram aplicados algoritmos de Inteligência Artificial. As ferramentas tecnológicas utilizadas foram preferencialmente de uso público e gratuito, são elas:

- Software livre: ECLIPSE/NetBeans para desenvolvimento de programas em JAVA e Software livro ANACONDA para usar PYTHON com biblioteca PANDAS e KERAS;

- Linguagens de programação livre: JAVA 8 update 191, PYTHON 3 e R 3.5.1 ;

- Uso de Banco de Dados livre MYSQL 8.0.

Um modelo preditivo pode ser descrito como uma função matemática que aplicada a um grande volume de dados é capaz de identificar padrões e oferecer uma previsão do que pode ocorrer. O modelo preditivo utiliza métodos quantitativos e qualitativos para estabelecer previsões, recomendar otimizações e simular modelos que sejam úteis a uma linha de pesquisa (WALLER; FAWCETT, 2013).

Resultados esperados

Geração de conhecimentos estratégicos que auxiliem à tomada de decisão na área da Segurança Pública voltada para ao combate aos assaltos à bancos em todas as suas formas conhecidas.

O uso de redes neurais artificiais é uma ferramenta riquíssima de geração de conhecimento estratégico, estruturado e útil para a tomada de decisões, que já vem sendo utilizado por grandes corporações pelo mundo para a identificação de padrões de comportamentos.

A natureza interdisciplinar dessa pesquisa, permite a utilização de técnicas da Ciência da Computação com os conhecimentos da Segurança pública, possibilitando gerar conhecimentos não detectados e não padronizados, como: estatísticas, grafos, padrões, relatórios e gráficos, pertinentes ao tema explorado.

LEVANTAMENTO DOS DADOS E RESULTADOS

Para entender melhor esse tema, foi usada a estatística descritiva nos dados relativos aos 251 assaltos a bancos no estado do Ceará de 2015 a 2018.

Nas primeiras análises percebemos que as menores localidades são as preferidas pelos criminosos, provavelmente porque possuem os menores efetivos policiais. Localidades com até 20.000 habitantes são as mais visadas com 34,3% dos crimes, quando somamos todas as localidades até 30.000 habitantes esse volume sobe para 54,6% dos crimes, isto é, mais da metade dos casos, conforme apresenta o Gráfico 5.

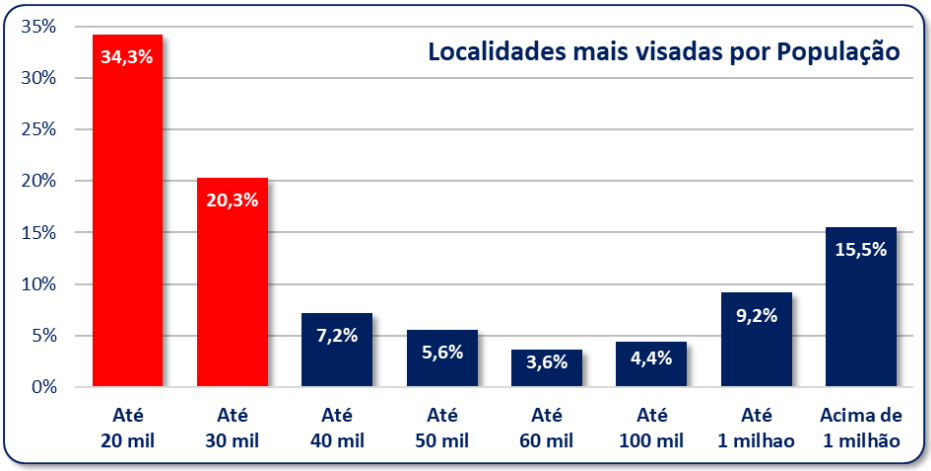

Gráfico 5 – Distribuição dos eventos nas localidades por tamanho da população.
Fonte – Adaptação do autor.

O Gráfico 6 apresenta a distribuição dos assaltos durante os dias da semana. Neste gráfico é possível observar que a “quarta-feira” é dia preferido com 18,7% dos crimes e os

finais de semana são os dias menos atrativos para os criminosos, principalmente o “domingo” que participa com apenas 8% dos crimes.

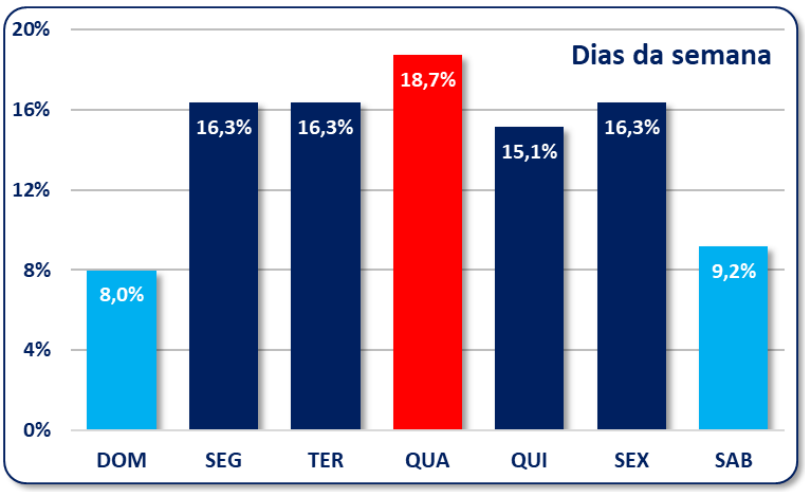

Gráfico 6 – Distribuição dos eventos .nos dias da semana.
Fonte – Adaptação do autor.

Quando avaliamos o horário preferido para os ataques, percebemos uma incidência destacada de 61% dos crimes nas “madrugadas”, quando as cidades dormem, poucas pessoas nas ruas e os tiros e explosões provocados apavoram os moradores destas localidades dentro de suas casas, que evitam sair nas ruas. O Gráfico 7 nos mostra essa preferência destacada pela “madrugada” com 153 assaltos no período estudado.

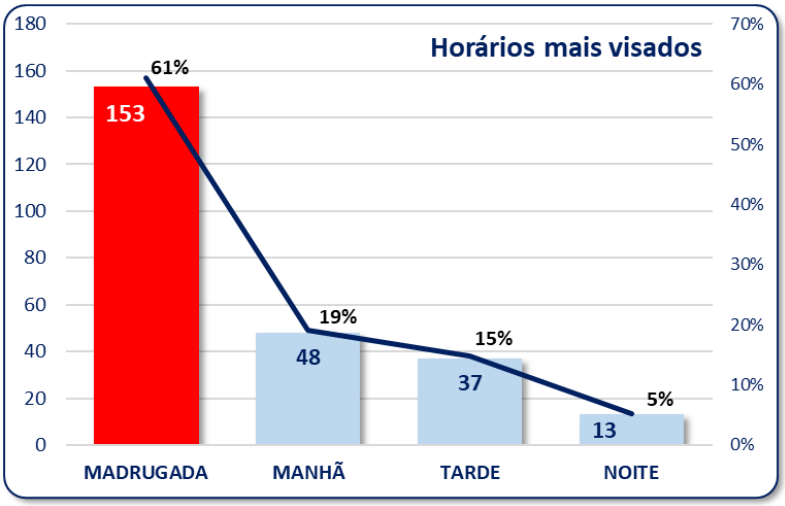

Gráfico 7 – Distribuição dos eventos nos horários do dia.
Fonte – Adaptação do autor.

Quando avaliamos os dias do mês, observamos uma concentração de ataques nos primeiros dias do mês ou nos últimos dias do mês, nos permitindo inferir que esses ataques visam as remessas de papel moeda para as agências bancárias no período de pagamento de salários, aposentadorias e benefícios sociais que se concentram nessas duas épocas do mês. O Gráfico 8 nos mostra essa distribuição onde podemos observar que mais de 45% dos casos se concentram nos dias de 01 a 05 ou de 26 a 31.

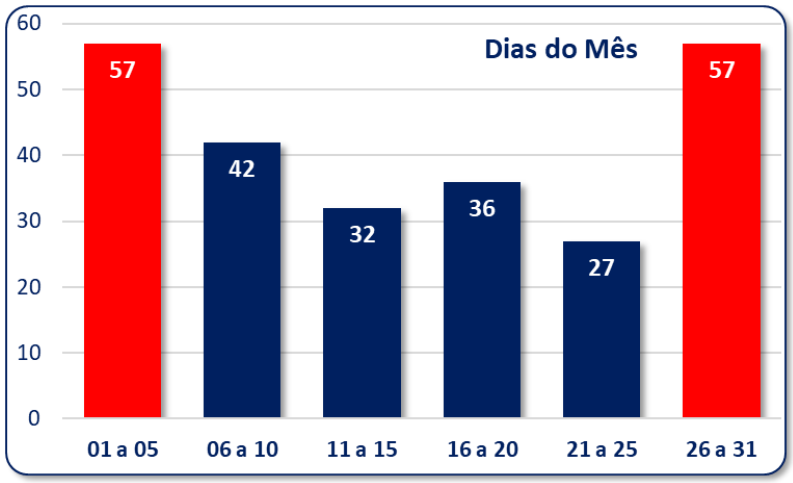

Gráfico 8 – Distribuição dos eventos por dias do mês.
Fonte – Adaptação do autor.

Quanto às instituições financeiras mais visadas podemos dizer que não temos muitas surpresas, pois o Banco do Brasil e o Bradesco são as instituições com maior capilaridade nas cidades do interior do Brasil e no Ceará não é diferente, mas os números são preocupantes. Analisando o Gráfico 9, podemos observar que 77% dos ataques foram direcionados para as agência do Banco do Brasil e Bradesco, e o Banco do Brasil sofreu 44% dos ataques, representando quase a metade de todos os assaltos no período estudado.

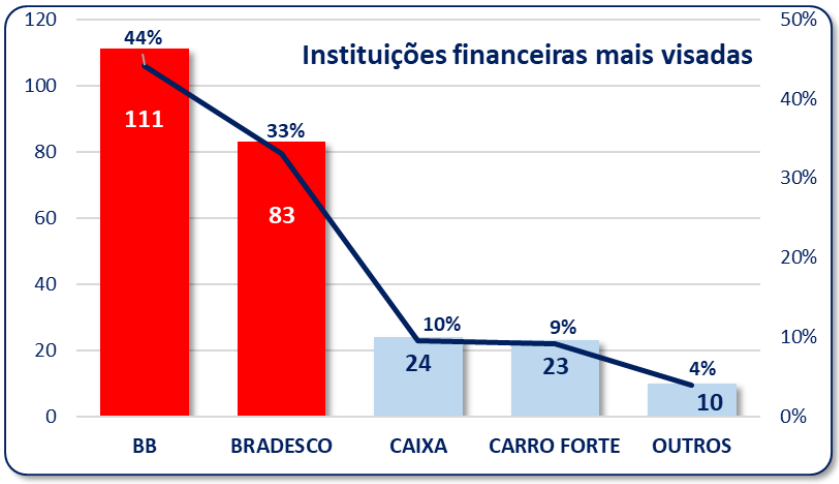

Gráfico 9 – Distribuição das Instituições financeiras mais visadas.
Fonte – Adaptação do autor.

Quanto ao *modus operandi* dos criminosos, ou seja, como foram executados os crimes, destaca-se o uso de explosivos com 46,2% das ações. Este tipo de ataque além de causar grande pavor na população, deixa muita destruição nas agências bancárias atacadas e em prédios vizinhos, causando grandes transtornos para a população, que fica sem os serviços bancários da agência atacada por vários meses e dependendo dos prejuízos causados a instituição bancária opta por não reabrir a agência. O Gráfico 10 mostra as principais ações dos criminosos.

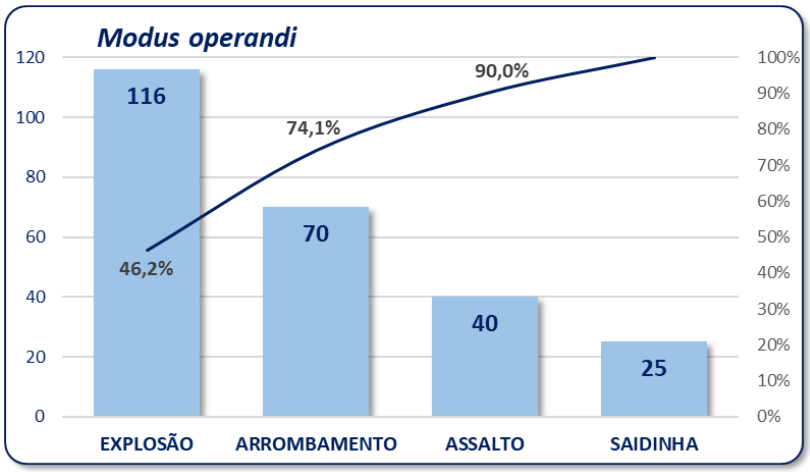

Gráfico 10 – *Modus operandi* dos criminosos.
Fonte – Adaptação do autor.

Os gráficos apresentados já nos permite inferir um padrão de comportamento dos criminosos: Preferencialmente atacam localidades com menos de 30.000 habitantes, durante a madrugada em dias úteis, nos últimos dias do mês ou nos primeiros dias do mês subsequente e preferem as agências do Banco do Brasil ou Bradesco, conforme apresenta a Figura 3.

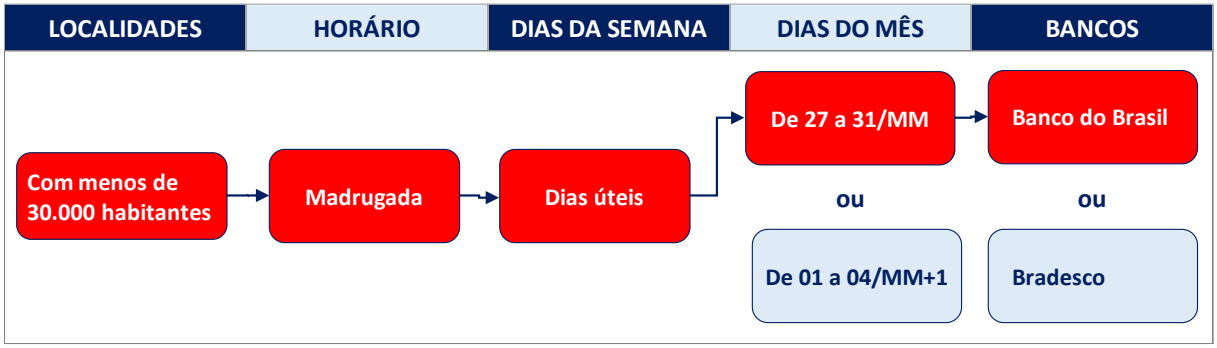

Figura 3 – Padrão baseado na estatística descritiva.
Fonte – Adaptação do autor.

Geração dos Modelos Preditivos

Para geração dos modelos preditivos foi utilizado um processo de preparação, tratamento, processamento e avaliação dos dados, conforme as fases descritas abaixo na Figura 4.

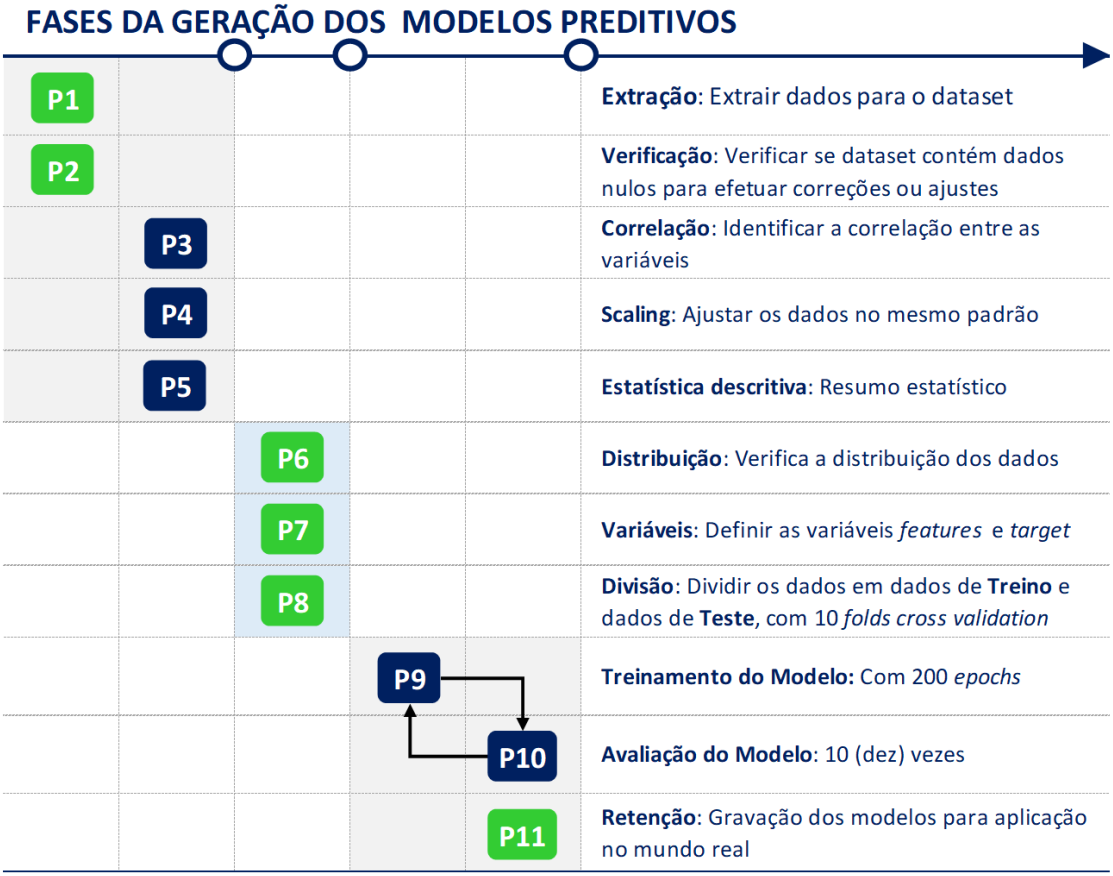

Figura 4 – Fases para geração dos modelos preditivos
Fonte – Adaptação do autor.

A partir do processo desenhado acima, iniciamos o processamento dos dados coletados e armazenados no nosso banco de dados. É do nosso conhecimento que nossos dados podem apresentar viés de qualidade das informações, pois não tivemos acesso aos dados oficiais, utilizamos os dados divulgados pelo Sindicato dos bancários do estado do Ceará em seu site institucional.

A execução do nosso processo obteve os seguintes resultados:

Fase I: Foram extraídos os dados para um *DataSet* com 460 (quatrocentos e sessenta) eventos de “assaltos” e “não assaltos”.

Fase II: Foi executado um algoritmo para verificar se o *DataSet* continha valores nulos em sua formação. Este processo retornou o resultado *FALSE*.

Fase III: Foi executado um algoritmo para identificar a correlação entre as variáveis do *DataSet*. Os resultados não apresentaram nenhum valor significativo para divulgação.

Fase IV: Os dados foram ajustados em *Scaling* para que todos os dados estivessem na mesma proporção de valores, isto é, nenhuma variável tinha um *Range* muito diferente das demais.

Fase V: Resumo estatístico de todas as variáveis utilizadas, detalhando a Média, Desvio Padrão, Mínimo, Máximo, Primeiro Quartil (25%), Segundo Quartil (50%) e o Terceiro Quartil (75%).

Fase VI: Verificação da distribuição dos dados em Total de casos positivos (251) e Total de casos negativos (209), com Percentual de 54.565217391304344% de Casos Positivos e 45.43478260869565% de Casos Negativos.

Fase VII: Nesta fase são identificadas as variáveis explicativas, ou seja, as características dos eventos que explicam as variáveis *targets* ou alvos. No nosso processo a variável target era binária (0 – Não houve assalto e 1 – Houve assalto).

Fase VIII: Nesta fase os dados foram divididos em dados para o treinamento e dados para os testes, na proporção de 70% por 30%. Utilizamos também a técnica que utiliza 10 (dez) *folds* em *cross validation* (Validação cruzada), isto é, misturando os dados de treino e teste em grupos diferentes e cruzando-os.

Fase IX: Nesta fase iniciamos o processo de treinamento com 200 (duzentas) épocas, isto é, o modelo de aprendizado foi executado duzentas vezes para a base de dados, e esse processo repetido por 10 (dez) vezes, obtendo os seguintes resultados, conforme a Tabela 1.

TREINAMENTO	PERDA	ACURÁCIA	ACURÁCIA DO TESTE
1º	0,0208	99,52%	87,23%
2º	0,0195	100,00%	89,13%
3º	0,0221	99,76%	86,96%
4º	0,0338	99,28%	86,96%
5º	0,0272	99,76%	78,26%
6º	0,0609	98,31%	82,61%
7º	0,0309	99,28%	89,13%
8º	0,0323	99,03%	82,61%
9º	0,0315	99,28%	86,96%
10º	0,0253	99,52%	84,44%

Tabela 1 – Resultados obtidos em 10 treinamento com 200 épocas cada.
Fonte – Adaptação do autor.

Fase X: Nesta fase são feitas as avaliações do modelo. Os dados obtidos na avaliação do modelo usando os dados retidos para testes, isto é, que não foram utilizados no treinamento do modelo, apresentaram resultados satisfatórios, com o menor valor de acuraria de 78,26% no quinto teste e o melhor valor de acurácia de 89,13% no segundo e sétimo testes.

Fase XI: Agora todos os modelos estão treinados e testados, logo devemos armazenar os pesos dos treinamentos realizados para posterior aplicação no mundo real. Ao final de todos os treinamentos e testes, chegamos ao valor médio da acurácia de 85,43% com erro de mais ou menos 3,25%.

CONCLUSÕES

Os valores obtidos nos permite inferir que a rede neural funcionou muito bem para predizer os eventos de assaltos a banco, embora os dados utilizados não sejam os ideais, pois não ter o rigor dos dados oficiais de polícia e investigação criminal.

As oportunidades que tivemos de usar esse modelo para prever o futuro, sito é, usar o treinamento para prever o que ainda vai acontecer, nos mostrou que a técnica é válida e pode agregar valor estratégico para a nossa inteligência policial.

Em dois casos testados no mundo real, obtivemos o seguinte resultado: A predição nos mostrou três localidades que ocorreriam um assalto com explosão e no dia seguinte realmente uma das localidades tinha sido assaltada com explosão da agência bancária. Em outra oportunidade das três localidades que estavam previstas para ocorrer um assalto, no dia seguinte não ocorreu nenhum assalto a banco nestas localidades, mas uma localidade com características semelhantes foi assaltada no estado do Paraíba, distante 50% das localidades indicadas, isto é, nessa oportunidade descobrimos que nosso projeto precisa envolver os estados da Paraíba e do Rio Grande do Norte que possuem características sócio demográficas muito semelhantes as localidades do estado do Ceará.

Como proposta e continuidade desta pesquisa, enviaremos ofícios para as secretarias de segurança pública dos três estados para que definitivamente possamos usar tecnologia com inteligência e a inteligência artificial em benefícios das nossas comunidades. É a academia levando conhecimentos e soluções para a gestão pública.

REFERÊNCIAS

ANUÁRIO DE SEGURANÇA PÚBLICA, São Paulo: Fórum Brasileiro de Segurança Pública, 2018.

AQUINO, Jania Perla D. Performance e Perigo nos Assaltos contra instituições financeiras. 26ª Reunião brasileira de Antropologia, Porto Seguro – BA, 2018.

BARR A; FEIGENBAUM E. A. The Handbook of Artificial Inteligence, volume I-II. Willian Kaufmann Inc., Los Altos, California, 1981.

BRAGA, Antônio de P.; CARVALHO, André P. L.; LUDEMIR, Teresa B. Redes Neurais Artificiais: Teoria e Aplicações. Rio de Janeiro: Ed. LTC, 2007.

CERVO, Amado L.; SILVA, Roberto da; BERVIAN, Pedro A. Metodologia Científica. 6ª ed. São Paulo: Ed. Pearson Prentice Hall, 2007.

CHARNIAK, Eugene; McDERMOTT, Drew. Introduction to artificial intelligence. Addison-Wesley Logman Publishing Co., Boston, USA, 1987.

CRESWELL, John W. Projeto de pesquisa: Métodos qualitativo, quantitativo e misto. 3ª ed. Porto Alegre: Artmed, 2010.

FAYYAD U.; PIATETSKY-SHAPIRO G.; SMYTH P. From Data mining to Knowledge Discovery: An Overview, Knowledge Discovery and Data mining, Menlo Park: AAAI Press; 1996.

HAYKIN, Simon. Redes neurais: princípios e prática. 2ª edição. Porto Alegre: Ed. Bookman, 2001.

KURZWEIL, Raymond. The age of Intelligent Machines. MIT Press, USA, 1990.

LUGER, George F. Inteligência Artificial. 6ª ed. São Paulo: Pearson Education do Brasil, 2013.

RICH, Elaine; KNIGHT, Kavin. Artificial Intelligence. McGraw-Hill Higher Education, USA, 1990.

TURBAN, Efraim; LEIDNER Dorothy.; MCLEAN Ephraim.; WETHERBE James. et al. Tecnologia da informação para a gestão, 6ª ed. Porto Alegre: Ed. Bookman, 2010.

VENTURA, Zuenir. Cidade Partida. São Paulo: Companhia das Letras, 1992.

WALLER, M. A.; FAWCETT, S. E. Data Science, Predictive Analytics, and Big Data: A Revolution That Will Transform Supply Chain Design and Management. Journal of Business Logistics, 34(2), 77–84. 2013.