Pontifícia Universidade Católica
do Rio de Janeiro

Ana Paula Conceição Teixeira Penna

Proposta de *Framework* para o uso de *Robotic Process Automation* nas Auditorias Internas de Bancos Brasileiros

Dissertação de Mestrado

Dissertação apresentada no Programa de Pós-graduação em Administração da PUC-Rio como requisito parcial para obtenção do grau de Mestre em Administração

Orientador: Prof. Leonardo Lima Gomes

Rio de Janeiro
Abril de 2020

Pontifícia Universidade Católica
do Rio de Janeiro

Ana Paula Conceição Teixeira Penna

Proposta de *Framework* para o uso de *Robotic Process Automation* nas Auditorias Internas de Bancos Brasileiros

Dissertação apresentada como requisito parcial para obtenção do grau de Mestre pelo Programa de Pós-graduação em Administração da PUC-Rio. Aprovada pela Comissão Examinadora abaixo.

Prof. Leonardo Lima Gomes
Orientador e Presidente
Departamento de Administração - PUC-Rio

Prof. Henrique Castro Martins
Departamento de Administração – PUC-Rio

Profa. Marta Corrêa Dalbem
Pesquisadora Independente

Rio de Janeiro, 08 de abril de 2020

Ana Paula Conceição Teixeira Penna

Graduou-se em Administração na UFRJ (Universidade Federal do Rio de Janeiro) em 1998. Cursou MBA em Finanças no IAG/PUC-Rio em 2011. Atuou como educadora corporativa na UniBB. É auditora do Banco do Brasil e Agente de Transformação do Programa iNovAudit. Responsável pela coordenação da proposta que deu origem às Células de Análise de Dados na Auditoria Interna do Banco do Brasil. Desenvolve trabalhos e pesquisas em *Business Intelligence* com foco em Auditoria Interna.

Ficha Catalográfica

Penna, Ana Paula Conceição Teixeira

Proposta de *Framework* para o uso de *Robotic Process Automation* nas Auditorias Internas de Bancos Brasileiros / Ana Paula Conceição Teixeira Penna; orientador: Leonardo Lima Gomes. – Rio de Janeiro: PUC, Departamento de Administração, 2020.

v., 102 f.; il.color. ; 29,7 cm

1.Dissertação (mestrado) – Pontifícia Universidade Católica do Rio de Janeiro, Departamento de Administração, 2020.

Inclui referências bibliográficas.

1. Administração – Teses. 2. Auditoria Interna. 3. Auditoria Contínua. 4. *Robotic Process Automation* 5. RPA. 6. Bancos Brasileiros I. Gomes, Leonardo L. (Leonardo Lima). II Pontifícia Universidade Católica do Rio de Janeiro. Departamento de Administração. III. Título.

CDD 658

À minha filha, Ana Cecilia, minha força e razão de existir e
a meu namorado, Marcelo, pelo apoio, amor e compreensão.

Agradecimentos

Ao Banco do Brasil, pela bolsa de estudos concedida, sem a qual esse trabalho não teria sido realizado.

À Comissão Examinadora pela aprovação do trabalho.

A todos os professores e funcionários do Departamento de Administração do IAG PUC-Rio pelos ensinamentos e pela ajuda.

A todos os amigos e colegas de trabalho que de uma forma ou de outra me estimularam ou me ajudaram.

A meu pai, minhas tias, minha avó e meus padrinho e madrinha pelo amor, carinho e inspiração.

Resumo

Penna, Ana Paula Conceição Teixeira; Gomes, Leonardo Lima. **Proposta de *Framework* para o uso de *Robotic Process Automation* nas Auditorias Internas de Bancos Brasileiros** Rio de Janeiro, 2020. 102 p. Dissertação de Mestrado - Departamento de Administração, Pontifícia Universidade Católica do Rio de Janeiro.

A Automação Robótica de Processos (RPA) surge como uma nova tecnologia advinda da indústria 4.0, focada na automação de tarefas humanas repetitivas, rotineiras e baseadas em regras. Ela promete eliminar esses processos que consomem mais tempo, sem substituir os sistemas de TI existentes. Consequentemente, reduziria custos e riscos operacionais; e melhoraria a eficiência, os processos internos e a experiência do cliente. Além disso, a RPA tem o potencial de revolucionar a auditoria tradicional, pois minimizaria as atividades tenocráticas, que apresentam baixo valor agregado, e permitiria que os auditores se concentrassem mais em atividades que exijam raciocínio analítico e julgamento profissional. Assim, levaria à ampliação da cobertura dos testes e do monitoramento de transações, aumentando a performance e a qualidade da auditoria contínua. Devido ao exposto, a RPA está sendo vista como um ativo estratégico para enfrentar os desafios da transformação digital.

Por ser uma nova tendência, a literatura científica sobre o tema ainda é escassa, mas está crescendo rapidamente. E, nos últimos dois anos, foi amplamente adotada em muitas organizações e instituições financeiras com sucessos e fracassos. Portanto, considerando o modelo das três linhas de defesa, este estudo tem como objetivo propor um *framework* para implantação da RPA na auditoria interna de bancos brasileiros.

Palavras-Chaves

RPA; *Robotic Process Automation*; Auditoria Interna; Auditoria Contínua; Modelo das Três Linhas de Defesa; bancos nacionais; indústria 4.0; transformação digital.

Abstract

Penna, Ana Paula Conceição Teixeira; Gomes, Leonardo Lima (Advisor). **Robotic Process Automation Framework Proposal for Internal Audit in Brazilian Banks**. Rio de Janeiro, 2020. 102p. Dissertação de Mestrado - Departamento de Administração, Pontifícia Universidade Católica do Rio de Janeiro.

Robotic Process Automation (RPA) emerges as a new 4.0 industry technology focused on the automation of repetitive, routine, rule-based human tasks. It promises to eliminate the most time-consuming processes without replacing existing IT systems. Consequently, reducing costs and operational risks as it improves efficiency, internal processes, and customer experience. Moreover, it has the potential to disrupt the traditional audit model as it minimizes mechanical low added value activities, enabling auditors to concentrate more on assignments that require thinking skills and professional judgment. Thus, it would lead to the expansion of testing and monitoring analytics coverage, enriching continuous audit quality and performance. Due to the above, RPA is being seen as a strategic asset to face the challenges of digital transformation.

Since it is a new trend, there is limited literature on the subject, but growing fast. And, in the last couple of years, it has been widely adopted in many industries and financial organizations with successes and failures. Therefore, considering the three lines of defense model, this paper aims to propose an RPA framework for internal audit in Brazilian banks.

Keywords

RPA; Robotic Process Automation; Internal Audit; Continuous Audit; Three Lines of Defense Model; Brazilian banks; 4.0 industry; digital transformation.

Sumário

Lista de Figuras

Lista de Tabelas

Abreviaturas & Símbolos

AICPA - American Institute of Certified Public Accountants
API - Application Programming Interface
Bacen – Banco Central do Brasil
BPA - Business Process Automation
BPM - Business Process Management
CA – Continuous Auditing
CAATS - Computer-assisted audit tools
CAE – Chief Audit Executive
CCM - Continuous Control Monitoring
CDA - Continuous Data Assurance
CEO - Chief Executive Officer
CICA - Canadian Institute of Chartered Accountants
CISR - Center for Information Systems Research
CoE - Center of Excellence
COMO - Continuous *Compliance* Monitoring
CPAS - Continuous Process Audit System
CRMA - Continuous Risk Monitoring and Assessment
CSF - Critical Sucess Factors
DBS - The Development Bank of Singapore Limited
DW – Data warehouse
ECIIA - European Confederation of Institutes of Internal Auditing
ERM - Enterprise Risk Management
Febraban - Federação Brasileira de Bancos
Ferma - Federation of European Risk Management Associations
GAAS - Generally Accepted Auditing Standards
GUI - Graphical User Interface
IA – Inteligência Artificial
IEEE - The Institute of Electrical and Electronics Engineers Standards Association
IIA® – Institute of Internal Audit
IPA - Intelligent Process Automation
IRPAAI – Institute for Robotic Process Automation & Artificial Intelligence
ISACA® - Information Systems Audit and Control Association
KPI - Key Performance Indicator
KRI - Key Risk Indicator
MIS – Management Information System
MIT - Massachusetts Institute of Technology
MVP – Minimum Viable Product
NPS – Net Promoter Score
PCAOB - Public Company Accounting Oversight Board
RPA – Robotic Process Automatization
RTA – Real Time Accounting
SLA - Service Level Agreement
SMACIT - social, mobile, analytic, cloud and internet of things
SoD - Segregation of Duties
SOX - Lei Sarbane-Oxley
SWOT - Strengths, Weaknesses, Opportunities and Threats
TI – Tecnologia da Informação
UX – User Experience
VUCA – volatility, uncertainty, complexity and ambiguity

Modern finance is complex, perhaps too complex. Regulation of modern finance is complex, almost certainly too complex. That configuration spells trouble. As you do not fight fire with fire, you do not fight complexity with complexity. Because complexity generates uncertainty, not risk, it requires a regulatory response grounded in simplicity, not complexity (HALDANE, 2012).[1]

[1] Economista-chefe e o Diretor Executivo de Análise e Estatística Monetária do Bank of England

1
Introdução

1.1.
O problema

Até a promulgação da Lei Sarbanes-Oxley - SOX, em 2002, as atividades da auditoria interna focavam, basicamente, as demonstrações contábeis de uma empresa. Devido, principalmente, à Seção 404 dessa norma, houve a ampliação do escopo nos trabalhos. Ela determinou que houvesse uma avaliação anual de todos os controles e procedimentos internos da organização previamente a emissão dos relatórios financeiros. Em função disso, esse tipo de auditoria passou a ser denominada integrada (PCAOB, 2007). Consequentemente, houve, também, um aumento nos pré-requisitos para a qualificação profissional de auditoria e nos custos desse processo. O setor financeiro, escopo desse estudo, foi o que mais sentiu o impacto dessa regulamentação.

Paralelamente, nesse período, houve uma sofisticação progressiva na tecnologia da informação subjacente aos processos de negócios. Isso gerou um volume de processamento de transações, que incorpora milhares de regras de negócios, distribuídas e configuradas em diversas linguagens; sistemas legados; e canais (TRELLES et al., 2011). Consequentemente, a auditoria tradicional tornou-se insuficiente para obtenção de relatórios tempestivos, abrangentes e de qualidade. Então, vários *softwares* de auditoria e análise de dados foram aperfeiçoados e passaram a oferecer soluções para esses problemas. Contudo, não é suficiente usar aplicativos de mineração de bases e/ou criar gatilhos com alertas para identificar possíveis irregularidades ou fraudes. Esse tipo de abordagem é míope e ignora outros riscos, às vezes mais relevantes. Além disso, geralmente, é custosa e, raramente, gera valor.

Isso ocorre porque a Alta Administração, normalmente, possui um conhecimento limitado sobre TI (RADOVANOVIĆ et al., 2010) e sobre Auditoria. Consequentemente, não é incomum, haver uma certa dificuldade em entender as iniciativas que precisam ser tomadas para adequação da organização (como um todo e não somente nessas áreas) ao processo de transformação digital que vivemos. E, assim, garantir a eficácia e a eficiência de suas estratégias, como também a perenidade da empresa.

Adicionalmente, até uma década atrás, os correntistas iam às agências bancárias para qualquer tipo de atendimento, como obter orientações sobre

investimentos e meios de financiamento. Com o advento do *machine learning*, da inteligência artificial, do *mobile banking,* da automação de fluxos e da robotização, como os *chatbots*, surgiu uma realidade sem precedentes para o sistema financeiro, na qual as plataformas digitais tornaram-se o grande ambiente de negócios (BACEN, 2018). Nela, há a criação constante de novos produtos e serviços, concomitantemente, a alterações cotidianas nos sistemas, devido a atualizações de programas e ao desenvolvimento de novas funcionalidades. Esse ambiente complexo e mutável pode ser muito vulnerável a riscos. E, esses podem causar perdas que precisam ser estimadas, avaliadas e mitigadas. Ademais, podem suscitar novos tipos de problemas operacionais, irregularidades e fraudes que necessitam ser previstos e coibidos.

Resta, ainda, mencionar outros fatores relevantes que vem impactando esse setor. O cenário econômico mundial está levando à diminuição dos *spreads* bancários. As *fintechs* vêm aumentando a competitividade na área. Particularmente no Brasil, os bancos de investimento e as corretoras têm ganho *market share*, principalmente, no segmento alta renda. Adicionalmente, há a regulamentação que é extensa. Quando não há uma nova norma, as antigas são revisadas, exigindo dos bancos mudanças recorrentes, em processos e controles, que demandam planejamento de médio e longo prazo. Amostras disso são a Lei Geral de Proteção ao Dados – LGPD (BRASIL, 2018) e Basileia III – Reformas pós-crise (Basileia 4) (COMMITTEE ON BANKING SUPERVISION, 2017). O *Openbanking*[2] já é uma realidade (BACEN, 2019). E, até o final de 2020, deve ser implantado o Sistema de Pagamentos Instantâneo no país. Há, também, diversas propostas em andamento para o uso de *Blockchain*.

Em pesquisa realizada por Fitzgerald (2013), 90% dos CEOs acreditavam que a transformação digital impactaria suas indústrias, mas menos de 15% estavam adotando uma estratégia digital. Logo, os profissionais de Auditoria Interna dessas organizações precisam entender esse novo ambiente; mapear os processos; identificar esses riscos; e, atuar de forma a incluí-los nos trabalhos de Auditoria. É necessário saber se os modelos e as abordagens em uso pela auditoria interna, no caso em estudo – o setor bancário brasileiro, são suficientes para compreender, analisar e avaliar essa nova realidade; e, assegurar o cumprimento das atribuições definidas à ela pelo Institute of Internal Auditors – IIA®.

[2] Open banking é um modelo de negócio que tem o propósito de compartilhar informações financeiras referentes a dados, produtos e serviços dos usuários.

Segundo essa instituição, a atividade de auditoria interna é independente e objetiva. Ela almeja: assessorar e dar consultoria à alta administração; agregar valor à empresa; colaborar na melhoria dos processos da organização; e, auxiliar ativamente na consecução de seus objetivos. Auditoria interna deve ainda, por meio de uma abordagem sistemática e disciplinada, avaliar a melhoria na eficácia do gerenciamento de riscos, dos controles internos e do processo de governança (Instituto de Auditores Internos [IIA], 2008).

Considerando o exposto, algumas questões necessitam de respostas: Em função do fenômeno transformação digital e seus impactos no setor bancário nacional, qual é a melhor abordagem para a Auditoria Interna? Que modelo deve adotar para assegurar o cumprimento das atribuições? Que mecanismos devem ser criados para tratar o volume e a velocidade de informações produzidas a serem auditadas?

1.2. O Objetivo

Este estudo objetiva responder as questões ora levantadas por meio da implantação de um framework para o uso da automação robótica de processos – *robotic process automation* (RPA), na Auditoria Contínua, considerando o modelo das três linhas de defesa e o planejamento estratégico integrado da auditoria interna nos bancos brasileiros.

1.2.1. Objetivos Intermediários

Para atingir o objetivo final proposto esse estudo prevê os seguintes objetivos intermediários a serem alcançados:

- Pesquisar as teorias relacionadas à transformação digital, à automação robótica de processos e à auditoria interna;
- Discorrer sobre o impacto da transformação digital nas organizações e as estratégias para adaptação à essas mudanças;
- Conceituar e caracterizar a automação robótica de processos;
- Sintetizar a evolução, as abordagens e os planejamentos da auditoria interna;
- Descrever o modelo de três linhas de defesa;
- Conceituar e descrever a evolução da auditoria contínua;

- Apresentar casos de estratégias de transformação digital, RPA e auditoria contínua envolvendo bancos;

1.3. A importância do estudo

Embora o termo automação remonte a linha de montagem industrial. O conceito de Automação Robótica de Processos (*Robotic Process Automation – RPA)* foi cunhado após 2000. E, apenas em 2017, *The Institute of Electrical and Electronics Engineers Standards Association* emitiu sua definição sobre essa nova tecnologia como tratado nesse estudo.

Seguindo essa tendência, no segundo trimestre de 2018, o *Journal of Emerging Technologies in Accounting*, uma revista reconhecida internacionalmente por focar temas de vanguarda envolvendo contabilidade, auditoria e TI, valeu-se da *Rutgers University*, centro de referência mundial nos estudos de auditoria, para escrever um editorial sobre o uso de RPA na Auditoria. As conclusões dos estudiosos Moffit, Rozario e Vasarhelyi, vinculados à essa instituição, envolviam os benefícios obtidos pela RPA com a redução do tempo empregado em tarefas repetitivas; e como seu uso nas atividades de auditoria melhoraria a qualidade dos dados e dos relatórios, o *compliance* e o valor dos negócios. Mas, também, salientava os riscos de sua implementação; e o fato de 30 a 50% dos projetos de RPA falharem. Um desses riscos seria um possível conflito com a área de TI, pois, um projeto de RPA poderia ser implementado por não técnicos. Logo, ainda não havia sido publicado um *framework* para a implementação do uso de RPA na Auditoria, que apresentasse as melhores práticas a serem adotadas visando mitigar seus riscos e maximizar seus resultados. Essa foi a inspiração do estudo ora apresentado, que se iniciou naquele momento.

Em novembro de 2019, quando essa pesquisa já estava em revisão, foi publicado o artigo *Applying robotic process automation (RPA) in auditing: A framework*, por Huang e Vasarhelyi. Os achados e constatações obtidos por mim, até então, estavam alinhados aos desses autores e foram devidamente citados nesse estudo. Contudo, a abordagem aqui apresentada enfoca outros aspectos não tratados por aqueles pesquisadores. Por exemplo, o uso do modelo das três linhas de defesa como arcabouço para a implementação da RPA e a integração entre os planejamentos estratégicos da organização, da auditoria interna e de TI.

Além disso, esse trabalho aborda os impactos da transformação digital e da indústria 4.0 nos bancos nacionais.

Portanto, esse estudo distingue-se por propor uma análise sobre o uso de uma tecnologia disruptiva e emergente, RPA, em todos os aspectos que envolvem as atividades da Auditoria Interna considerando o sistema bancário nacional. Sua relevância reside ainda na sugestão de um *framework* para a disseminação dessa nova ferramenta por toda a organização, de forma planejada e estruturada, visando à melhoria da eficiência operacional da empresa e a disponibilização dos auditores para as atividades que agreguem mais valor para os *stakeholders.* E, como a regulamentação, segundo Cooper et al.(2019), é o principal fator de atraso no uso de RPA pela auditoria, subsidiariamente, ajudará os reguladores e supervisores a entender melhor a automação robótica de processos e seus benefícios para esse setor, quiçá, mudando essa situação.

1.4. Delimitação do Estudo

Este estudo não pretende aprofundar questões relacionadas a estrutura de TI ou os processos específicos de auditoria nessa área, nas instituições financeiras nacionais. Embora relevante, também não se pretendeu comparar as características dos *softwares* de RPA oferecidos no mercado para a identificação da melhor escolha a ser usada na implementação da proposta de integração ora apresentada.

Cabe destacar, ainda, que a pesquisa se limitou a abordar o tema proposto a partir do ponto de vista do caso em particular, não sendo consideradas outras organizações. Desta forma, as conclusões apresentadas neste trabalho estão limitadas ao contexto específico da auditoria interna em bancos nacionais.

1.5. Estrutura do Trabalho

O presente trabalho encontra-se dividido em seis capítulos. O primeiro introduz o problema da pesquisa e seus objetivos. Aborda, ainda, a importância da análise e suas delimitações.

O segundo capítulo apresenta os estudos sobre o tema e expõe a lente teórica dos elementos que embasaram a proposta apresentada: transformação digital, RPA e auditoria interna, com suas abordagens e formas de planejamento.

Segue, explicando o modelo das três linhas de defesa. Finaliza, conceituando a auditoria contínua, explicando sua evolução e comentando suas perspectivas futuras.

No terceiro capítulo, é justificada e descrita a metodologia utilizada nesse estudo, com seus aspectos epistemológicos, ontológicos e limitações.

No quarto capítulo, há a contextualização da pesquisa com a apresentação de casos.

Em seguida, o quinto capítulo apresenta a proposta para o uso da RPA na auditoria contínua, considerando o modelo das três linhas de defesa, e como essa estrutura pode ser adotada para o planejamento da implementação da automação robótica de processos em toda organização.

Para, no sexto capítulo, concluir sobre a utilização dessa proposição no planejamento estratégico da auditoria interna em bancos nacionais; e, expor as devidas recomendações, implicações, limitações e sugestões para pesquisas futuras.

2
Referencial Teórico

Neste capítulo são apresentados os fundamentos teóricos que suportam o estudo. Inicialmente, são comentadas as pesquisas realizadas sobre os temas que serão tratados: transformação digital, RPA e auditoria interna. Em relação ao primeiro, será destacado seu aspecto fenomenológico, como consequência da indústria 4.0; e, as principais teorias desenvolvidas, até o momento, sobre as estratégias adotadas pelas organizações para lidar com essa nova realidade. Como constructo principal e consequente daquele, será conceituada a RPA, descrita suas características, seus benefícios e as dificuldades para sua implementação.

Na segunda seção, serão introduzidos os conceitos e as teorias que formam o arcabouço epistemológico da auditoria interna, incluindo o modelo das três linhas de defesa, e suas correlações com o planejamento estratégico da organização, a gestão de riscos, os controles internos e a governança. Ao final, será mostrada a evolução da Auditoria Contínua.

Essas discussões e desenvolvimentos teóricos são necessários para embasar as conclusões sobre a atuação da auditoria interna em bancos nacionais num ambiente de transformação digital e sobre a melhor forma de implementar um projeto de RPA nesse contexto.

2.1.
Os estudos que têm abordado o problema

Ao longo dos últimos 50 anos, os trabalhos de auditoria interna tiveram diferentes abordagens que foram desenvolvidas para atender as necessidades e as características específicas das empresas na medida em que novos negócios, novas tecnologias e novas escolas e visões administrativas surgiam (BYRNES et al., 2018). Um exemplo é a criação do planejamento estratégico de auditoria e sua integração ao planejamento estratégico da organização.

Um estudo sobre os principais temas pesquisados e publicados em auditoria na era pós-SOX (PORTE et al., 2018) analisou objetivos e hipóteses de 1.650 publicações na Web of Science® no período entre 2002 e 2014. Nele constatou-se que os temas mais abordados foram: relatório de auditoria e usuários das demonstrações contábeis; governança corporativa; mercado de auditoria; auditoria externa; dados socioeconômicos da empresa; regulamentação

internacional; e, risco de fraude e de auditoria. Portanto, observa-se que temas relacionados a auditoria contínua eram incipientes nesse período.

Segundo (MURCIA; SOUZA; BORBA, 2008), a maioria dos artigos que abordam tópicos relacionados a auditoria contínua são não-empíricos. Dos 57 artigos selecionados, na base Capes®, no período de 1998 a 2006, apenas um apresentou uma pesquisa empírica: um estudo de caso na Siemens (ALLES et al., 2006), que descreve o caso seminal sobre o tema. Cabe destacar ainda que aproximadamente 50% desses estudos não-empíricos adotam uma abordagem conceitual, definindo principalmente modelos e teorias de auditoria contínua; e, apresentando razões e oportunidades para seus usos.

Uma análise bibliométrica feita entre 2000 e 2016 na base Scopus® (MARQUES; SANTOS, 2017) identificou 207 publicações sobre auditoria contínua, sendo 65%, após 2010 e com crescimento ao longo dos anos. Além disso, 61% eram artigos em jornais e 27%, oriundos de conferências.

Considerando, agora, o outro pilar desse estudo, a automação robótica de processos, foi identificado apenas uma bibliometria, realizada por Syed et all (2019) e publicada no nº 115 do periódico da *Computers in Industry* . Nessa revisão literária nas bases de dados SpringerLink®, AISel®, ProQuest®, Elsevier®, AB/INFORMS®, IEEEXplore®, Web of Science®, Scopus® e Google Scholar®, foram identificados 125 artigos, sendo a maioria datada dos anos precedentes ao seu levantamento. Desses, 24 tentavam, explicitamente, definir o assunto. Demonstrando que se tratava de uma tecnologia incipiente e que seu conceito foi sendo forjado com o desenvolvimento de suas aplicações. Já as outras pesquisas identificadas sobre o tema eram, basicamente, lições, práticas e experiências aprendidas durante sua implementação nas organizações. Portanto, disseminaram os acertos, os erros e os pontos de melhoria que deveriam ser observados para as empresas que fossem adotar a RPA.

Em junho de 2019, foi publicado na *American Accounting Association*, revista especializada e sem acesso a público não filiado, o artigo *Robotic Process Automation in Public Accounting,* elaborado por Cooper et al., no qual foram entrevistados líderes das Big Four[3]. Esse foi o primeiro estudo a discutir os benefícios, as oportunidades e os desafios para implementação da RPA na auditoria externa.

Em abril de 2020, foi realizada uma consulta ao termo *Robotic Process Automation* como título, resumo ou palavra-chave na base Scopus representada

[3] Big Four designação dada às quatro maiores empresas contábeis especializadas em auditoria e consultoria do mundo: EY, PwC, Deloitte e KPMG.

na Figura 1. Foram identificados 129 artigos, sendo que as cinco primeiras publicações sobre o tema ocorreram apenas em 2016.

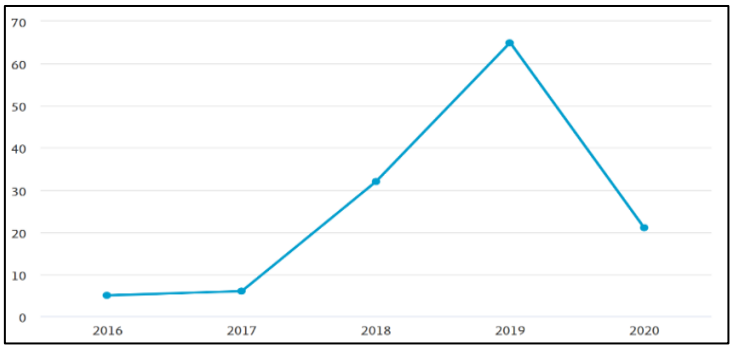

Figura 1 - Publicações sobre Robotic Process Automation
Fonte Scopus (2020)

Adicionalmente, foi elaborada uma busca, também em abril de 2020, nos sites supracitados, usando os termos RPA e "Audit" em título, resumo ou palavras-chaves. Nessa, foram identificados somente os dois artigos já mencionados, no item 1.3. importância do estudo, sobre o uso de *Robotic Process Automation* em auditoria, ambos de coautoria do Professor da *Rutgers University*, Miklos Vasarhelyi, precursor no estudo da auditoria contínua.

Mas como a era digital é uma realidade recente dentro de um mundo VUCA – volátil, incerto, complexo e ambíguo (BENNIS, 1985), muitas pesquisas estão sendo realizadas focando esse tema e, muitas vezes, utilizando-se de novas tecnologias. Logo, há uma tendência de crescimento nos estudos desses campos.

2.2. Transformação Digital

A indústria 4.0 impulsionada pelos *smartphones* e por diversas tecnologias disruptivas como robótica, inteligência artificial, realidade aumentada, *big data*[4], nanotecnologia, impressão 3D, biologia sintética e internet das coisas, traz desafios e oportunidades para as organizações e toda a economia mundial (SCHWAB, 2016).

Nesse contexto, surgiu a Transformação Digital. Segundo Mazzone (2014), TD é a evolução deliberada e contínua de uma empresa, um modelo de negócios, um processo de ideias ou uma metodologia para o digital, tanto estratégica quanto taticamente.

[4] Representam um volume de dados grande demais para ser processado numa única máquina, devido a gargalos no processador, na memória ou no disco. Como solução, usa-se algoritmos que executem análises bayesianas aproximadas distribuídas com comunicação mínima.

Ser digital não envolve apenas a adoção de tecnologias, como as citadas. Mas, a mudança pela qual as organizações devem passar para aproveitar as oportunidades criadas por essas tecnologias. Ela implica repensar a proposta de valor da empresa, não apenas suas operações. Uma empresa digital inova não somente para fornecer produtos e serviços, mas para melhorar seu desempenho e aprimorar o envolvimento com o cliente. Essas organizações são denominadas *Future Ready* (ROSS; WEILL; ROBERTSON, 2006).

Apesar do processo de transformação digital dos negócios ter se iniciado há cerca de 20 anos, Weill e Woerner (2018b), constataram que apenas 23% das empresas pesquisadas estavam Prontas Para o Futuro. Enquanto 51% delas não estavam. Essas foram chamadas Silos & Complexidade devido às deficiências na integração e na coordenação entre as áreas; e à ineficiência dos seus processos.

Assim, baseado no *framework* da transformação em negócios digitais representado na Figura 2, uma organização para ir do quadrante inferior esquerdo (Silos e Complexidade) para o superior direito (Pronta para o futuro) precisaria mudar em duas dimensões - experiência do cliente e eficiência operacional.

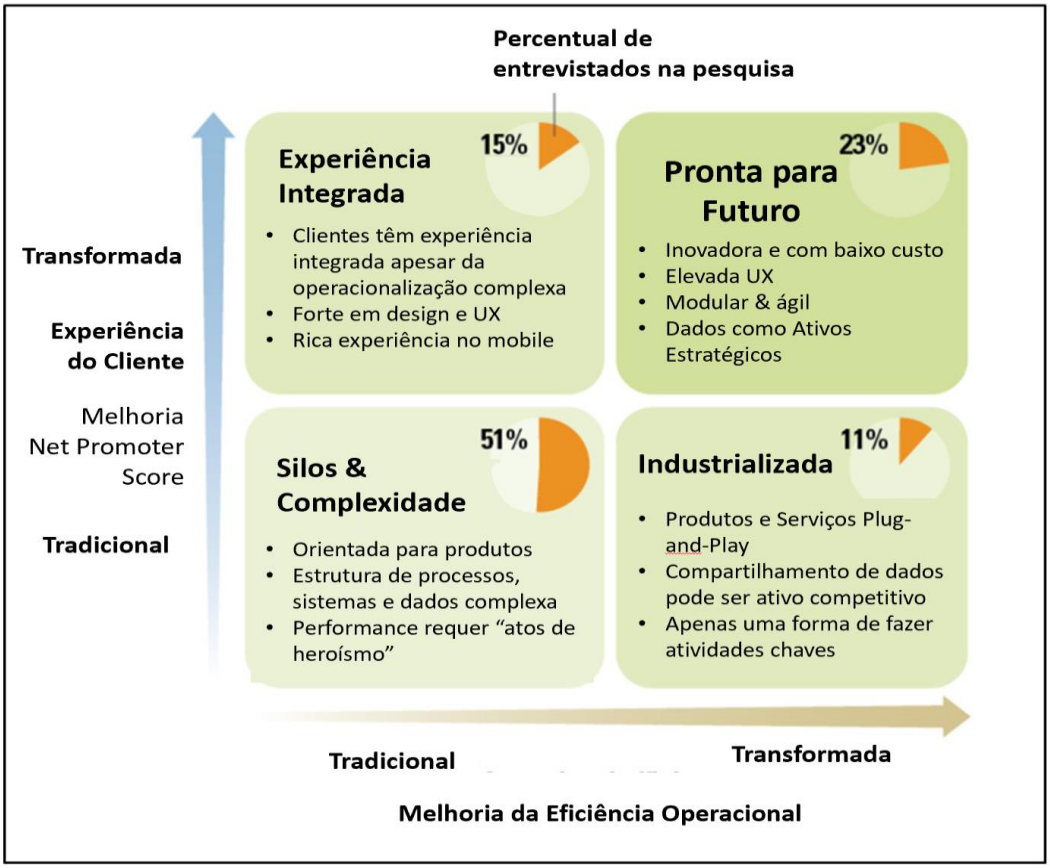

Figura 2 - Framework Digital Business Transformation
Adaptado de: WEILL, P.; WOERNER, S. L. **Is Your Company Ready for a Digital Future?** MIT Sloan Management Review, [s.l.], December 04, 2017.

Os pesquisadores constataram que esse processo vem ocorrendo de quatro formas:

1) Industrializando – essa opção foi considerada árida devido a reutilização dos serviços e a necessidade de digitização;

2) Integrando – essa escolha aumenta a *User Experience* - UX a um custo muito alto, pois os sistemas legados, quando criados, não foram projetados para integração;

3) *Stair steps* – essa alternativa causa exaustão devido a mudança de foco, ora melhorando o NPS, ora reduzindo custo. Ademais, necessita de uma governança madura, uma vez que, quando o topo decidir mudar a direção, a base ainda estará implementando a última diretriz;

4) *Give up* – ocorre quando a organização desiste de mudar e cria uma nova empresa com as características *Future Ready*. Essa opção causa demissão em massa e problemas de identificação da marca. Além disso, numa eventual fusão da empresa nova com a antiga, haveria dificuldades na integração entre os sistemas; e, um choque cultural entre os empregados.

Além disso, muitas empresas estão embarcando em uma jornada de transformação para negócios digitais sem saber, ao certo, como realizar esse processo e quais seriam os benefícios obtidos. Geralmente, optam pela filosofia *mobile first*, disponibilizando seus produtos e serviços em celulares e oferecendo aplicativos, sob a premissa que os sistemas de TI resolveriam qualquer problema (WEILL; WOERNER, 2018a). Mas na prática não resolvem.

Para construir uma arquitetura que aumente a lucratividade, melhore o tempo de comercialização e reduza os custos, é necessário o planejamento de uma infraestrutura de TI, que viabilize a integração dos processos, permitindo a digitização dos negócios e a automatização dos principais recursos da empresa. Nesse sentido, é fundamental identificar os processos essenciais ao negócio e rever as atividades que os compõem, de forma a simplificá-los e digitizá-los. Preferencialmente, começando por aqueles que já se executa bem (CODESSO et al., 2018).

A empresa preparada para o futuro é capaz de inovar não só para envolver e satisfazer os clientes, mas também para se tornar mais eficiente e eficaz. Seu objetivo deve ser atender às necessidades dos clientes, ao invés de empurrar os produtos. Em contrapartida, os clientes teriam a expectativa de uma boa experiência atendida, independentemente do canal de entrega escolhido. Em relação às operações, os recursos da empresa tornar-se-iam modulares e ágeis.

E, os dados, um ativo estratégico, que seria compartilhado e acessível a todos que precisassem deles (MAZZONE, 2014).

Considerando o exposto, evidencia-se que cabe a liderança das organizações determinar qual direcionamento seguir, para obter o melhor desempenho na economia digital, e quão agressivamente se mover, tendo por base um planejamento estratégico integrado à estrutura de TI; e à sua evolução em conjunto com os negócios, o mercado e as novas tecnologias, de forma a definir sua visão de futuro e alcançá-la (ROSS et al., 2016).

2.3. Robotic Process Automation

Segundo o IEEE, RPA:

> é a preconfiguração de uma rotina baseada em regras, completamente autônoma, num *software*, envolvendo processos, atividades, transações e tarefas, relacionadas a um ou vários sistemas, para a entrega de um produto ou serviço sem a intervenção humana (IEEE, 2017).

A origem do conceito subjacente a RPA remete a automação tradicional oriunda da linha de montagem. D.S. Harder cunhou esse termo, em 1936, quando trabalhava para a *General Motors Corporation*. Significava a transferência de peças de montagem entre as máquinas em um processo de produção, sem operação humana. Em 1946, como vice-presidente da *Ford Motor Company*, ele criou o Departamento de Automação (HARDER; DAVIS, 1953).

Até o surgimento da transformação digital, a automação ficou praticamente restrita ao gerenciamento de processos e à reengenharia desses, no ambiente mecânico-industrial. Mas, o aumento vertiginoso da capacidade de processamento e da criação de dados das últimas décadas fez com que as macros e os scripts, criados em *softwares* como Excel®, que apresentavam inúmeras restrições de processamento e compatibilidade, fossem substituídos por programas elaborados para a automação de processos de negócios (BPA – *Business Process Automation*), como mostrado na Figura 3. O objetivo era integrar sistemas e reestruturar tarefas para melhorar o fluxo de trabalho e minimizar custos. Nesse sentido, foi desenvolvida uma metodologia, BPM – *Business Process Management*, uma notação própria para os diagramas, BPMN – *Business Process Magement Notation*, e um guia de gestão de processos, o BPM CBOK – *Business Process Management Common Book of Knowledge.*

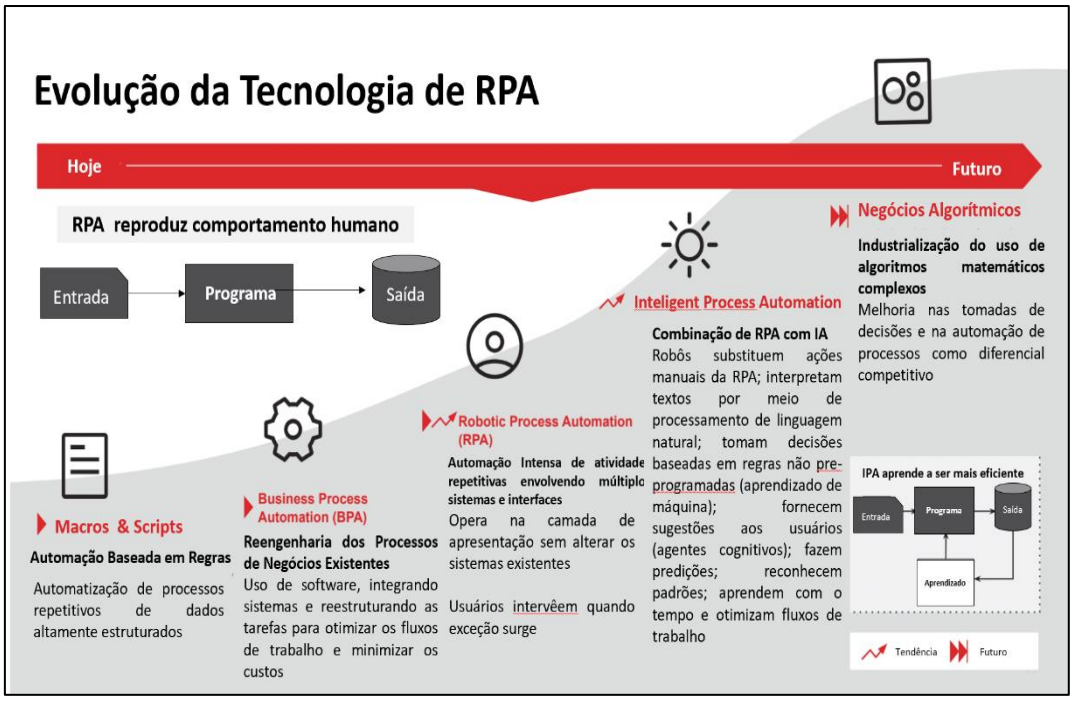

Figura 3 - Evolução da tecnologia RPA
Adapatado de: MENNIE, P. **AI and RPA in Internal Audit**. In: IIA Annual Conference. [s.l.]: [s.n.], 2019

A diferença dessas automações para a RPA reside no fato dela reproduzir a interação humana por meio de um *software* que "grava" as tarefas que seriam realizadas pelo funcionário ao executar uma atividade, como fazer login, ler e-mails, copiar e colar dados entre aplicativos ou criar relatórios. Ou seja, os *softwares* de RPA cadastram, em sequência, todas as ações realizadas pelos empregados ao executar cada tarefa, em cada interface gráfica utilizada pelo usuário (GUI), em um ou mais aplicativos, e, em seguida, executa a automação repetindo essas tarefas diretamente na GUI. Numa ferramenta tradicional de automação de fluxo de trabalho como BPA, um desenvolvedor de *software* programaria a lista de ações para automatizar cada tarefa e, também, uma interface com o sistema de *back-end* usando APIs (interfaces de programação de aplicativos internas) ou uma linguagem[5] de script[6]. Portanto, a RPA trouxe uma simplicidade e uma agilidade para a automação de (certos tipos) processos sem precedentes. Daí estar sendo adotada tão rapidamente por organizações no mundo todo. Isso não quer dizer que substitui a BPA. Ela permanece tendo sua função e, em alguns casos, são adotadas em conjunto (TECNODATA, 2019), como representado na Figura 4.

[5] Back-end é o sistema responsável pelas regras de negócios, webservices e APIs de uma aplicação.
[6] Linguagem de script é uma linguagem de computador com uma série de comandos em um arquivo que pode ser executado sem ser compilado. Exemplos Perl, PHP e Python.

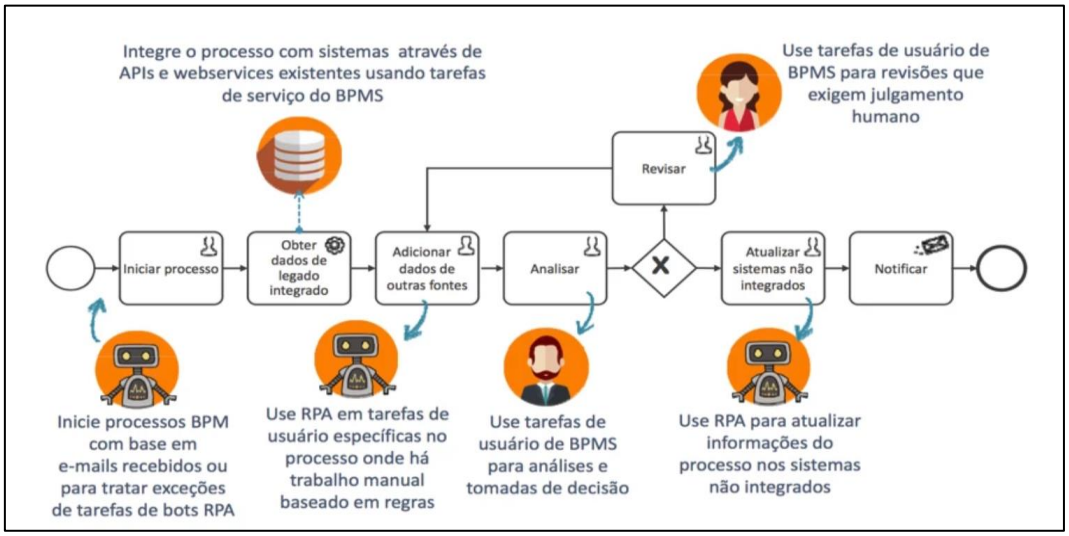

Figura 4 - Processo contendo BPA e RPA
Fonte: TECNODATA. **RPA vs. BPM - dois lados da mesma moeda**. 2019.

Outra grande vantagem da RPA é que funciona com praticamente qualquer aplicativo ou servidor. Ademais, podem ser monitoradas em tempo real por um usuário ou por outro robô (MOFFITT; ROZARIO; VASARHELYI, 2018).

Em função disso, já há ensaios sobre o uso de *Intelligent Process Automation* – IPA, que é a união de inteligência artificial à RPA. Essa seria uma tendência de vanguarda no mercado (SAS; INTEL; DELOITTE, 2018). E, há ainda estudiosos que vislumbrem a industrialização de algoritmos matemáticos complexos visando à melhoria nas tomadas de decisão; e, à automação de processos complexos.

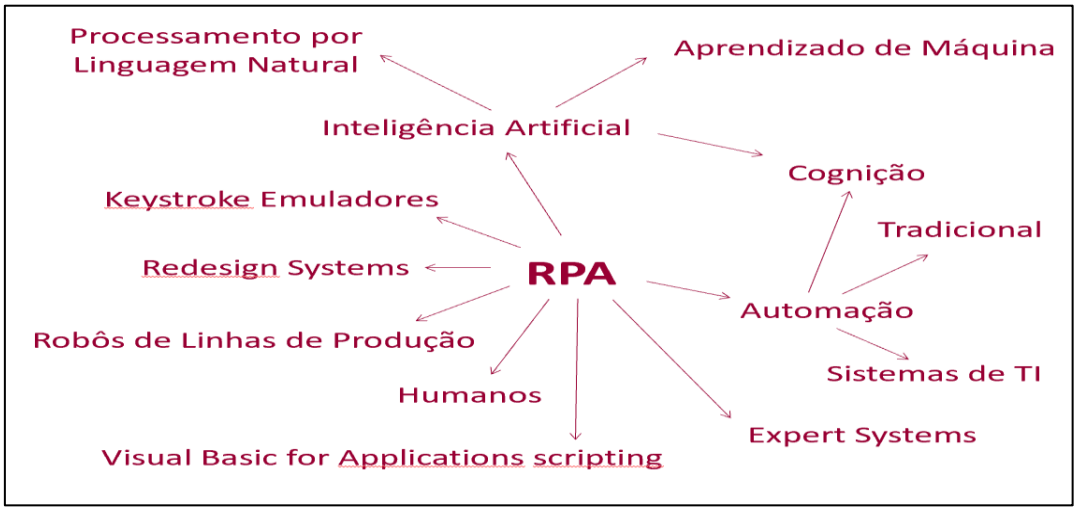

Figura 5 - Correlações entre RPA e demais tecnologias digitais
Adaptado de: SYED, R. et al. **Robotic Process Automation.** Contemporary Themes and Challenges. Computers in Industry, [s.l.], v. 115, p. 4, 2019

Além disso, a indústria 4.0 propiciou a revisão, a remodelagem e a integração de antigos e novos conceitos, levando a topografias de sistemas de TI multifacetados (BROCKE, VOM et al., 2018). Um resumo esquemático dessas correlações em relação a RPA é apresentado na Figura 5.

Mas, considerando o estágio atual, o uso da RPA é apropriado a atividades rotineiras, padronizadas e maduras. Ou seja, tarefas estáveis, em que o fluxo e os dados necessários para sua realização são conhecidos. Bem como, devem ser altamente manuais, repetitivas e baseadas em regras. A lógica de decisão precisa estar expressa nas regras de negócios e essas têm que ser inequívocas. Em função disso, as atividades devem ser bem documentadas, apresentarem baixo nível de tratamento de exceções e os dados, que utiliza, serem estruturados. Ademais, é comum interagirem com muitos sistemas (ACCENTURE, [s.d.])

Logo, ao realizar a avaliação sobre a automação de um processo deve-se, inicialmente, dividi-lo em atividades. Nesse momento, o uso de aplicativos de BPM auxiliam no mapeamento do fluxo de trabalho com suas etapas e características (ROMAO; COSTA; COSTA, 2019). Depois, verifica-se a necessidade do uso de dados não estruturados ou de uma análise subjetiva do conteúdo em alguma fase do processo. Se for o caso, o processo não é candidato à automação. Posteriormente, devem ser aferidos três aspectos: adequação, complexidade e valor. O primeiro, mede possíveis restrições a sua implementação e os benefícios relacionados aos controles do processo. Segundo, identifica-se o fluxo entre as atividades para determinar sua extensão e enredamento, pois, quanto mais excepcionalidades os robôs tiverem que tratar, maior será a automação. Em função disso, pode-se optar-se por segmentar a RPA ou adiá-la. E, o terceiro quantifica o montante economizado com a automação (MENNIE, 2019).

Considerando que a RPA, essencialmente, substitui o processo manual pelo automatizado, pois não há reengenharia nesses, nem alteração nos sistemas de TI existentes, os custos, o cronograma e o risco de implementação são relativamente pequenos, se comparados a outros procedimentos envolvendo os sistemas de uma organização ou outros tipos de automação. Assim, quanto menos complexo for o processo composto pelas atividades automatizadas, mais rápida será a entrega da RPA, menor será seu custo e, geralmente, maior o retorno (IRPAAI, 2016).

É importante frisar, também, que o uso da RPA não se restringe a melhoria da eficiência operacional, devido a redução do risco de erros transacionais e ao aumento da velocidade na execução das atividades. Esse tipo de automação

incrementa a qualidade dos serviços e dos trabalhos produzidos, facilita e torna mais ágil a integração com outros sistemas; e aprimora o gerenciamento de riscos e controles internos (SYED et al., 2019). Todas essas vantagens são muito relevantes e cobiçadas.

Todavia, segundo a *Ernest & Young* (2016), 30 a 50% dos projetos de implementação de RPA fracassam. E, de acordo com pesquisa realizada pela AI Multiple (2020), mais de 40% dos que não, apresentam resultados abaixo das expectativas quanto ao custos e ao tempo de implementação, a redução de despesas e os benefícios analíticos. Os principais problemas apontados para ocorrência dessa lacuna entre a realidade e as expectativas envolvem aspectos organizacionais, processuais e técnicos relacionados à implantação e à pós-implantação do projeto. Basicamente, os organizacionais abrangeram a falta de comprometimento das equipes e das lideranças locais em relação a solução apresentada. Como também, a carência do devido suporte das áreas de TI, de RH e de gestão de dados e *analytics*[7] para o êxito do projeto. Adicionalmente, ainda foi verificada a insuficiência na atribuição de responsabilidades e na divulgação e comunicação da estratégia escolhida para implementação das RPAs. Em relação aos processos foi constatada a escolha de atividades para automação que não atendiam aos pré-requisitos, como serem compostas por tarefas que mudam frequentemente; e/ou que envolvem alto grau de cognição; e/ou que se relacionam com muitas outras, tornando a cadeia do processo complexa. Adicionalmente, houve casos em que não era financeiramente interessante automatizar todo o processo (*end-to-end*); ou que havia alternativas melhores de robotização, ponderando todo o processo. Quanto a tecnicidade, constatou-se escolhas de soluções que exigiam intensa programação e/ou que não demonstravam escalabilidade. Além da ocorrência de falta de confiança na aquisição de serviços das empresas de RPA e de suas ferramentas. Em relação a implementação propriamente dita, observou-se o desenvolvimento de soluções intraorganizacionais sem que houvesse a capacitação técnica necessária para tal. E, depois, do projeto em operação, que não havia sido devidamente pensado sua escalabilidade e/ou como seria a estrutura para sua manutenção. Logo, a opção pela RPA embora extremamente atrativa, requer muito planejamento, integração, engajamento e liderança para que atenda as expectativas.

[7] Analytics é o uso aplicado de dados por meio de técnicas matemáticas e estatísticas, modelagem preditiva e aprendizado de máquina para encontrar padrões, prever cenários e ampliar o conhecimento sobre as interrelações entre os dados.

2.4.
Auditoria Interna

Embora tenha suas origens nas Ciências Contábeis, a Auditoria Interna, atualmente, fundamenta-se no pensamento complexo[8] (MORIN, 1995), que enfoca a complementaridade entre as visões linear[9] e sistêmica[10] do mundo. Nesse sentido, adota uma abordagem de integração, envolvendo a avaliação crítica (GRIFFITH et al., 2015), sincronizada, multidisciplinar e independente, para verificação do gerenciamento das inter-relações entre objetivos, riscos e controles associados aos processos corporativos.

Sua aceitação como disciplina acadêmica vem se fortalecendo na medida em que autores com diversas formações iniciaram o desenvolvimento de teorias próprias para a área, como Mautz e Sharaf (1961) e Tom Lee (1986). Todavia, foi David Flint (1988), que enunciou os sete postulados que norteiam essa profissão:

1. Existe uma relação de responsabilidade contábil que é pública.
2. A responsabilidade não pode ser demonstrada sem uma auditoria.
3. Uma auditoria exige independência e liberdade.
4. O assunto de auditoria é susceptível de verificação por meio de provas.
5. Os auditores são juízes qualificados que são capazes de medir e comparar o desempenho real em relação aos padrões de responsabilidade.
6. O significado, a significância e a intenção das declarações a serem auditadas devem ser claros.
7. Uma auditoria produz um benefício econômico ou social.

2.4.1.
Abordagens da Auditoria Interna

Segundo Moeller (2009), as abordagens da Auditoria Interna podem ser classificadas por gerações, pois o enfoque dado aos trabalhos foi sendo ampliando ao longo dos anos:

1ª) Baseada em Controle – é feita para determinar a conformidade em relação a: leis, regulamentos, políticas e padrões específicos; balanços, demonstrações financeiras, rubricas contábeis; ou, controles e procedimentos operacionais determinados.

2ª) Baseada em Processo - é feita para determinar a eficácia e a eficiência dos principais processos operacionais da organização.

[8] O pensamento complexo considera que não se deve ver o mundo sob uma única lente nem sobre múltiplas, mas ponderar que esses enfoques se complementam / se integram e para alcançar isso deve-se ter uma análise crítica.
[9] Visão linear = única e objetiva
[10] Visão sistêmica = múltipla e interrelacionada.

3ª) Baseada em Risco – é feita para determinar se os riscos-chaves estão mitigados de acordo com o nível de tolerância estabelecido.

4ª) Baseada na Gestão de Risco – é feita para determinar a eficácia das atividades de gestão de risco quanto à manutenção dos riscos-chaves no nível de tolerância determinado; e, prover, assim, a segurança que os objetivos estratégicos da organização serão alcançados.

Na Tabela 1, apresentada a seguir, há um resumo das principais abordagens quanto ao objetivo, ao foco, aos testes e às recomendações, visando uma comparação objetiva dos diferentes enfoques para melhor compreensão da evolução ocorrida.

Tabela 1 - Abordagens da Auditoria Interna

	I - Baseada em Controle	**II - Baseada em Processo**	**III - Baseada em Risco**	**IV - Baseada na Gestão do Risco**
Objetivo	Conformidades com as diretrizes fundamentais	Eficácia e eficiência de processos	Eficácia de controles e processos para mitigar os riscos-chaves	Eficácia na gestão do risco para o atingimento dos objetivos e mitigação dos riscos
Abordagem	Compreensão das diretrizes e da auditoria para conformidade	Comparação do processo atual com as melhores práticas	Identificação dos riscos-chave do negócio e avaliação dos controles para mitigar esses riscos	Compreensão dos objetivos, da identificação dos riscos, do nível de tolerância, da performance, das medidas de risco e da avaliação da eficácia da gestão de riscos.
Foco	Identificar omissões e erros na conformidade	Identificar desvios entre os processos atuais e as melhores práticas	Identificar controles e processos que não estão operando devidamente para mitigar os riscos-chaves	Identificar desvios entre o nível de eficácia da gestão de risco atual e a esperada.
Abordagem nos Testes	Preditivos, substantivos e de conformidade com base estatística	Consultivos e de conformidade focando na avaliação das práticas atuais em relação as melhores práticas	Combinação de testes substantivos e de conformidade focando somente nos riscos-chave	Combinação de testes substantivos e de conformidade focando somente nos objetivos estratégicos e seus respectivos riscos
Recomendações	Relacionadas às omissões ou erros nas diretrizes relevantes	Relacionadas aos desvios em objetivos operacionais específicos	Relacionadas às omissões ou erros nos riscos-chaves	Relacionadas aos desvios na eficácia da gestão de risco quanto aos riscos fundamentais e aos objetivos estratégicos dos negócios

Adaptado de MOELLER, Robert R. **Brink's Modern Internal Auditing**. John Wiley & Sons, 2009, capítulo 3.11

2.4.2.
Planejamento da Auditoria Baseado na Gestão de Riscos

O Planejamento da Auditoria Baseada na Gestão de Riscos permite que o auditor interno forneça segurança à Alta Administração que o processo de gerenciamento de risco é eficiente em relação ao apetite de risco estabelecido. Envolve desde a identificação, a avaliação, o reporte e a comunicação das informações relacionadas a todos os riscos incorridos pela organização.

Segundo Pickett (2006) o modelo apresenta quatro fases:

1) a avaliação da maturidade do risco, que determina a extensão da análise sobre a gestão e o monitoramento dos riscos (ERM - Enterprise Risk Management), fornecendo os parâmetros para o planejamento da auditoria;

2) a determinação dos objetivos da auditoria, que proporciona consultoria e análise profissional - independente, sistemática e segura, da eficácia da gestão de riscos, dos controles internos e do processo de governança; agregando valor à organização e auxiliando-a no alcance dos resultados esperados.

3) o plano de trabalho da auditoria (*Methods*), que identifica os parâmetros de segurança e consultoria para um período específico (geralmente anual); determina as priorizações indicadas pela Alta Administração (*Message*); analisa o processo de gestão de risco e os processos críticos (*Results*); e, especifica os registros e a comunicação de resultados focando nos riscos (*Audience*).

4) o planejamento de auditoria, que compreende os trabalhos de auditoria, os recursos que serão utilizados, os indicadores chave de desempenho e a estratégia de auditoria para os próximos três anos, considerando abordagens flexíveis e não cíclicas com posicionamento proativo.

Na Figura 6, há a representação esquemática dos elementos constituintes da auditoria baseada em riscos e suas fases, segundo Pickett (2006), juntamente com a demonstração que essa metodologia permite a migração do formato antigo de auditar, que envolve verificações, checagens e identificação de fraude e erros, com o novo que agrega assessoria, consultoria, aconselhamento e informação tempestiva e relevante.

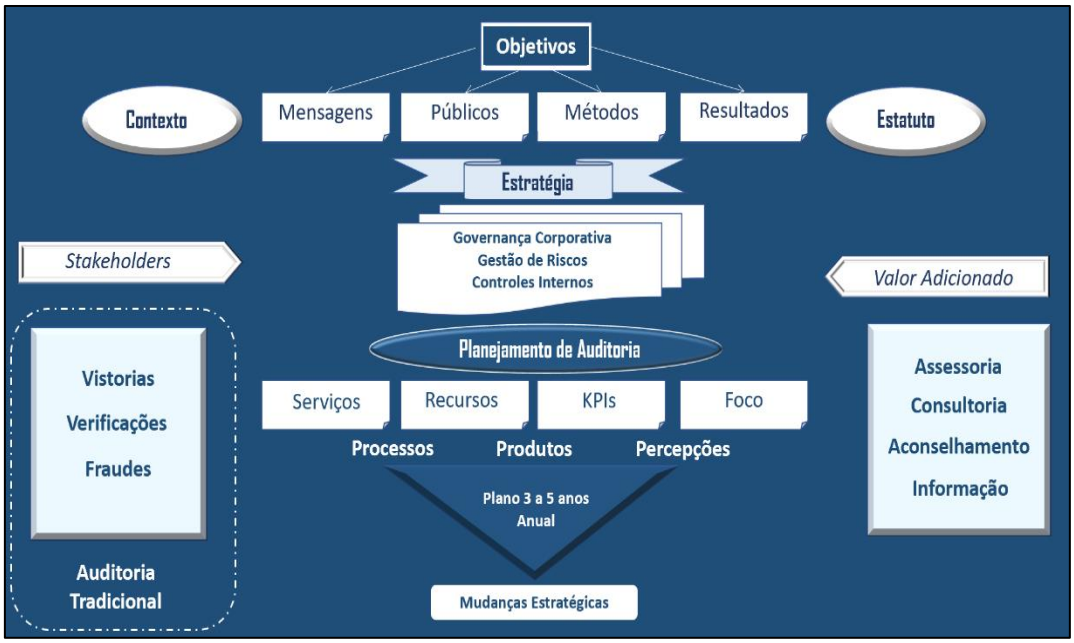

Figura 6 - Auditoria Baseada em Riscos
Adaptdo de: Pickett, K. **Audit Planning**. A Risk-based Approach. John Wiley &Sons, 2006, p.45

Nessa abordagem, cada processo é dividido em subprocessos, atividades, tarefas e passos, que são avaliados quanto aos respectivos objetivos e aos riscos e controles existentes, como representado na Figura 7, numa matriz de riscos. Essa, geralmente, é baseada em critérios como relevância financeira (materialidade), exposição da organização (vulnerabilidade), desempenho e criticidade. Também é considerado o grau de impacto (baixo/médio/alto) desses fatores nos resultados da organização. Dependendo da metodologia adotada podem ser incluídos pesos. O objetivo é concluir sobre o risco de um processo pela combinação dos riscos dos elementos que o compõe. Assim, é possível identificar aqueles que são mais críticos para o atingimento dos objetivos da organização; e otimizar os recursos da auditoria interna para avaliar e garantir que os riscos desses processos sejam devidamente mitigados.

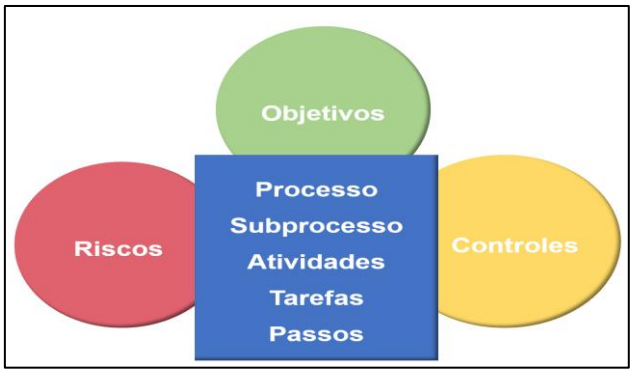

Figura 7 - Tríade da Auditoria Baseada em Riscos
Fonte: própria

Ademais, a Auditoria Baseada na Gestão de Riscos permite: a identificação e a avaliação dos processos corporativos e dos riscos acima e abaixo do apetite de risco estabelecido; a análise da efetividade das medidas corretivas para os riscos inerentes aos processos corporativos e aos riscos residuais (ambos em relação ao apetite de risco); e a classificação e a comunicação, apropriada, completa e precisa, das medidas corretivas e das ações adotadas em relação aos respectivos riscos.

2.4.3. Planejamento Estratégico de Auditoria Interna

Já o planejamento estratégico da auditoria interna é realizado conforme as diretrizes estabelecidas pela administração da organização por meio do alinhamento entre missões e objetivos dessa com aquela. Ele compreende os exames preliminares das áreas, atividades, produtos e processos da empresa, bem como, a análise do ambiente ético e do sistema de controles internos para definir a amplitude dos trabalhos e a época em que serão realizados.

Segundo o IIA® (IIA NETHERLANDS, 2015), trata-se de um processo sistemático e estruturado que se inicia com a Declaração da Visão de forma a articular a filosofia da atividade de auditoria interna com sua contribuição para a organização. A visão transcende objetivos, pois expressa o que é desejado para o futuro. Após, segue-se a Declaração de Missão, que é construída com base na declaração de visão e descreve o objetivo principal da atividade de auditoria; o que planeja alcançar no futuro; seus valores; e, como ele se integra ao plano estratégico da organização. A declaração de missão deve ressoar por todo o pessoal de auditoria interna e, também, pelas partes interessadas interna e externamente. É a partir da declaração da missão que o plano estratégico de auditoria interna é desenvolvido, determinando essencialmente como a missão será alcançada. A declaração de missão é comumente a primeira declaração no estatuto da auditoria interna.

De acordo com o IIA®, os três Ps dos fatores críticos de sucesso (CSFs[11]) devem responder as seguintes questões:

• Posicionamento - A atividade de auditoria interna está estrategicamente posicionada e suportada?

• Processos - Os processos da atividade de auditoria interna são ágeis e dinâmicos para atender às necessidades do negócio?

[11] Critical Sucess Factors

• Pessoas - A estratégia de pessoal da auditoria interna está adequada ao cumprimento de sua missão?

Em seguida, é necessário avaliar a situação da própria auditoria interna. Uma técnica comumente usada é a análise SWOT (REED et al., 2018). Seu objetivo é identificar os fatores-chaves internos (Forças & Fraquezas) e externos (Oportunidades & Ameaças) que são fundamentais para o alcance da estratégia a ser implementada. Nesse caso, o ambiente externo inclui os elementos da organização, além da atividade de auditoria interna, assim como os de fora da empresa.

Alguns aspectos que devem ser considerados na SWOT, são: a estrutura organizacional; as habilidades e os conhecimentos necessários à execução dos trabalhos; a tecnologia e as ferramentas disponíveis; e, a relação custo benefício, considerando os recursos e as características da empresa.

O planejamento deve considerar os fatores relevantes na execução dos trabalhos, especialmente os seguintes:

a) o conhecimento detalhado da política e dos instrumentos de gestão de riscos da organização, das atividades operacionais, dos sistemas contábil e de controles internos, e seu grau de confiabilidade;
b) a natureza, a oportunidade e a extensão dos procedimentos de auditoria interna a serem aplicados, alinhados com a política de gestão de riscos da organização;
c) a existência de empresas associadas, filiais e partes relacionadas que estejam no âmbito dos trabalhos da Auditoria Interna;
d) o uso do trabalho de especialistas;
e) os riscos de auditoria, quer pelo volume ou pela complexidade das transações e operações;
f) o conhecimento do resultado e das providências tomadas em relação a trabalhos anteriores, semelhantes ou relacionados;

Adicionalmente, o planejamento deve ser documentado e os planos de trabalho formalmente preparados, detalhando-se o que for necessário à compreensão dos procedimentos que serão aplicados, em termos de natureza, oportunidade, extensão, equipe técnica e uso de especialistas.

Ou seja, os planos de trabalho devem ser estruturados de forma a servir como um guia e como um meio de controle da execução do trabalho, devendo ser revisados e atualizados sempre que as circunstâncias o exigirem.

Seguindo ainda as orientações do IIA, o Chefe Executivo de Auditoria (CAE) deve coordenar os trabalhos com outras atividades de gestão de risco e

assessoria, alinhando recursos e prioridades. Ademais, deve estabelecer um plano de comunicação em que a Alta Administração e a Diretoria permaneçam informadas sobre a evolução dos trabalhos; os riscos e as limitações envolvidos; os achados; e; as ações corretivas com seus respectivos status.

O plano de desenvolvimento de pessoal também é incluído no planejamento estratégico. Devem ser especificadas as competências essenciais, o conhecimento, a experiência e as certificações necessárias à realização dos trabalhos e à ascensão profissional, de forma a viabilizar a prontidão dos auditores.

Para cada trabalho, é importante monitorar o prazo de execução; os objetivos desejados; as medidas de desempenho (qualitativa e quantitativa); e, os elementos SWOT associados. Além disso, o CAE e sua equipe podem realizar auto avaliações em relação a eficiência e a eficácia da execução do planejamento estratégico e divulgar essas informações por meio dos relatórios fornecidos as partes interessadas.

Então, na prática, como o planejamento estratégico de auditoria interna coexiste com o baseado em riscos? O planejamento de auditoria interna relacionado à estratégia organizacional pode ser dividido em dois aspectos: auditoria estratégica de riscos e auditoria de processos estratégicos (IIA NETHERLANDS, 2015). A auditoria estratégica de riscos foca aqueles relacionados a busca pelas metas organizacionais. Logo, reflete o alinhamento da auditoria interna aos objetivos estratégicos da organização. Em função disso, a auditoria atua dando consultoria e assessorando à Alta Administração para garantir que esses riscos estão mitigados, conforme o apetite a risco preestabelecido; e que não impedirão que as metas sejam alcançadas. Já a auditoria do processo estratégico ou corporativo envolve a avaliação do processo (incluindo subprocesso, atividade, tarefa e passo, quando relevantes), em relação aos objetivos, riscos, controles, *compliance* e governança, considerando o apetite de risco estabelecido. Ou seja, está relacionada ao *assurance* quanto à eficiência e à eficácia da gestão operacional e de riscos exigido pelos normativos e pelo IIA. E, o modelo geralmente adotado para realizar essas atribuições relativas à auditoria interna é o das três linhas de defesa.

2.4.3.1. Modelo das Três Linhas de Defesa

A SOX não foi a única legislação oriunda dos escândalos com empresas

como a Xerox e a Enron. Em 2006, a oitava Diretiva 84/253 do direito societário europeu, que trata das pessoas responsáveis pela revisão e aprovação das demonstrações financeiras nas organizações, foi alterada pela 2006/43. Em função disso, a *Federation of European Risk Management Associations* - Ferma e a *European Confederation of Institutes of Internal Auditing* - ECIIA emitiram orientações sobre a estrutura das linhas de defesa proposta para as companhias (FERMA / ECIIA, 2010), reproduzida na Figura 8. Além disso, reafirmaram os deveres dos auditores como independência, integridade, objetividade, capacitação, diligência e confidencialidade. Como também, ressaltaram a importância da aplicação de salvaguardas, no caso de ameaça incontornável na independência desse profissional.

Figura 8 - Modelo de Três Linhas de Defesa
Adaptado de: IIA. **IIA Position Paper:** The Three Lines Of Defense In Effective Risk Management And Control. Jan.2013, p. 2.

Consequentemente, em 2013, o IIA® publicou seu posicionamento em relação ao uso do modelo das três linhas de defesa para a gestão e controle eficaz de riscos (IIA, 2013). Em 2017, o *Chartered Institute of Internal Auditors* emitiu novo parecer sobre o tema e o revisou em 2019.

Na prática, esse modelo considera que o Conselho de Administração fornece orientações à Alta Administração quanto ao apetite de risco que a companhia está disposta a tolerar. Além disso, por meio da identificação dos principais riscos que a organização enfrenta, assegura-se que a Alta Administração os esteja gerindo, continua e adequadamente. Então, delega ao

CEO e à gerência sênior a responsabilidade pela gestão e controle de riscos operacionais, para que, liderem e orientem os funcionários das demais áreas, em relação a gestão de riscos e dos controles internos, em suas atividades cotidianas, conforme o nível de apetite aos riscos acordado. Para garantir a eficácia dessa estrutura, o Conselho e a gerência sênior precisam confiar que essas atribuições estão sendo monitoradas dentro da organização.

Assim, como esquematizado na Figura 9, a primeira linha de defesa é formada pelas gerências e respectivos funcionários, que realizam os processos da organização, sejam operacionais, táticos ou estratégicos. Eles são responsáveis por avaliar, controlar e mitigar riscos diretamente. Portanto, devem ter os conhecimentos, as habilidades, as informações e a autoridade necessárias para implementar as políticas e os procedimentos exigidos para o controle desses riscos. Isso requer um entendimento da empresa, de seus objetivos, do ambiente no qual operam e dos riscos que enfrentam.

Figura 9 – Resumo das atribuições no Modelo Três Linhas de Defesa
Adaptado de: LUBRUVIC R. **Strengthening the Three Lines of Defence in Terms of More Efficient Operational Risk Management in Central Banks**. Journal of Central Banking Theory and Practice.2017. v.6. p.35.

A segunda linha de defesa compreende as funções de supervisão, conformidade e gerenciamento de riscos. Ela fornece as políticas, as estruturas, as ferramentas, as técnicas e o suporte à conformidade, à governança e à gestão de riscos e de controles internos para a primeira linha de defesa. Ademais, realiza o monitoramento para avaliar a eficácia desse processo e das metodologias de mensuração dos riscos utilizadas.

A terceira linha de defesa precisa ser independente para poder avaliar de

forma isenta todos esses processos e atribuições. Logo, é representada pela auditoria interna. Uma de suas principais funções é assegurar que as duas primeiras linhas de defesa estejam operando em *compliance* e com eficiência e eficácia. Bem como, recomendar melhorias nos processos corporativos. Ela, ainda, é responsável por fornecer uma avaliação, por meio de uma abordagem baseada em riscos, sobre a eficácia da governança, do gerenciamento de riscos e dos controles internos aos órgãos reguladores, e à Alta Administração da organização.

Esse modelo é empregado em qualquer tipo de organização ou segmento econômico e é bem conhecido de todas as áreas das instituições financeiras nacionais e internacionais por estar associado a determinações regulamentares. Ademais, é considerado de fácil entendimento e aceitação quanto às atribuições de responsabilidades de cada segmento organizacional.

2.4.4. Auditoria Contínua

Paralelamente a tudo isso e acompanhando os avanços tecnológicos da época, a auditoria interna, não parou de evoluir. Em 1989, foi desenvolvido um sistema para a AT&T Bell (VASARHELYI; HALPER, 1991) que media, monitorava e analisava as informações de faturamento da empresa. Ele foi denominado Sistema de Auditoria de Processo Contínuo (CPAS). Nesse, foram introduzidos, pela primeira vez, KPIs, análises e alarmes relacionados aos dados em processamento. Assim, surgia a Auditoria Contínua, um processo de coleta e avaliação de evidências que visa determinar a eficiência e eficácia, em tempo real, dos sistemas contábeis na proteção de ativos; manter a integridade dos dados; e produzir informações financeiras confiáveis (REZAEE; ELAM; SHARBATOGHLIE, 2001).

Em função disso, o CICA / AICPA definiu a Auditoria Contínua como:

> Uma metodologia que permite uma avaliação por escrito baseada em relatórios emitidos concomitantemente aos eventos sob análise, ou num curto período depois da ocorrência desses (CICA / AICPA, 1999).

As principais vantagens da auditoria contínua são exigir menos custos de funcionamento e ser mais tempestiva, exata e compreensiva. O termo contínua tem caráter de evolução. Sua abordagem é dinâmica, pois concentra-se nas relações dos eventos que compõem o fluxo de trabalho, a partir do conhecimento da arquitetura dos processos organizacionais.

Cabe destacar que as informações resultantes da Auditoria Contínua retroalimentam a base de conhecimento da mesma forma que as demais produzidas pela Auditoria Interna; e, que sua abordagem antecipada não prejudica a identificação e o tratamento de achados.

Nessa época, a auditoria contínua não era vista como um novo tipo de auditoria. Mas, como uma técnica, análoga à entrevista, ao exame ou à circularização. Restringia-se a utilizar indicadores e alertas seletivos automatizados (gatilhos) para identificação de ocorrências diferentes dos padrões preestabelecidos. Ou seja, focava a auditoria por exceção. Além disso, era integrada e orientada para a produção de informação de auditoria por meio da análise de dados. Almejava pro atividade na detecção e na medição de eventuais riscos, reais ou potenciais, incluindo, fatores desencadeantes, para evitar a exposição além do limite tolerado pela empresa.

Dez anos depois, com os escândalos que envolveram a Enron, a Arthur Andersen e a WorldCom, as atenções voltaram-se para o sistema de controles internos das organizações. Contudo, esses controles não podem ser observados "visualmente", quando se utiliza ERPs (VASARHELYI; ALLES; WILLIAMS, 2010). E, a maioria das grandes empresas, principalmente no exterior, usam. Ademais, a seção 404 (SARBANES; OXLEY, 2002) exigiu que houvesse um monitoramento das métricas dos controles internos e que esses fossem avaliados quanto sua eficácia. Devido a isso, foi incorporado à Auditoria Contínua, o conceito de Monitoramento de Controle Contínuo[12] (CCM), que verifica atividades como: controles de acessos e autorizações; e configurações de sistemas e de processos, quase em tempo real. Assim, os procedimentos relacionados à verificação da gestão dos dados, das transações e das métricas chaves dos processos[13] - o antigo foco da auditoria contínua, passou a ser denominado Auditoria Contínua de Dados[14] (CDA) (ALLES, M.; KOGAN; VASARHELYI, 2008).

Em 2008, a crise do *subprime* evidenciou que a medição, a modelagem e a avaliação de riscos não estavam sendo devidamente fiscalizadas pelas empresas. Então, houve uma revisão do conceito de Apetite a Riscos e foi incorporada a Avaliação e o Monitoramento Contínuo dos Riscos[15] (CRMA) na Auditoria Contínua.

A CRMA envolve três categorias: operacional, ambiental e cisnes negros, que são riscos muito remotos, mas com grande impacto (TALEB, 2017). Em

[12] Continuous Control Monitoring (CCM)
[13] Key Process Metrics (KPM)
[14] Continuous Data Auditing (CDA)
[15] Continuous Risk Monitoring and Assessment (CRMA)

função disso, os riscos passaram a ser criteriosamente identificados pela auditoria. E, foram elaborados indicadores – KRIs[16], associados aos processos mais importantes da organização – Auditoria Baseada em Riscos, para cada uma dessas categorias. Como também, metodologias para detectar alterações significativas nesses riscos que, geralmente, utilizam variância, e podem incorporar heurísticas e pesos. Uma boa prática, comumente adotada, é atualizar a parametrização do modelo, ao fazer o planejamento anual de auditoria, e sempre que houver um evento relevante. Ademais, quando o monitoramento indica uma mudança significativa em algum risco, o algoritmo é rodado novamente. Se for confirmada a variação, o gestor responsável pela área vinculada ao risco é informado para que tome as providências cabíveis (BUMGARNER; VASARHELYI, 2015).

Considerando esse contexto e o fato que as regulamentações têm aumentando nos últimos anos, principalmente no setor bancário, esses autores propuseram a inclusão de mais uma perspectiva no framework da Auditoria Contínua: o Monitoramento Contínuo do *Compliance*[17] (COMO). Pois, apesar da abordagem tradicional sobre o *compliance* ser qualitativa, a automação dos sistemas vem permitindo o desenvolvimento de parâmetros quantitativos. Assim, a integração dessas visões em um único f*ramework* e em tempo próximo ao dos eventos tem a vantagem de melhorar os resultados das avaliações propostas, evitando a repetição de tarefas; e, de otimizar o uso das plataformas de TI. Baseado no exposto, a Auditoria Contínua, atualmente, poderia ser, resumidamente, representada pela equação a seguir e pela Figura 10 (PWC, 2020):

$$CA = CDA + CCM + CRMA + COMO$$

Onde:

CA = Auditoria Contínua

CDA= Auditoria Contínua de Dados

CCM = Monitoramento Contínuo de Controles

CRMA = Avaliação e Monitoramento Contínuo de Riscos

COMO = Monitoramento Contínuo do *Compliance*

Portanto, a auditoria contínua tornou-se o meio para realizar o planejamento estratégico integrado baseado em riscos num ambiente complexo, mutável e com

[16] Key Risk Indicator (KRI)
[17] Continuous Compliance Monitoring

fluxo crescente de dados. Mas a tecnologia usada atualmente é suficiente para atender o fator crítico de sucesso Processos (Os processos da atividade de auditoria interna são ágeis e dinâmicos para atender às necessidades do negócio?). E, os auditores estão suficientemente capacitados e atualizando-se para suprir o de Pessoas (A estratégia de pessoal da auditoria interna está adequada ao cumprimento de sua missão?)

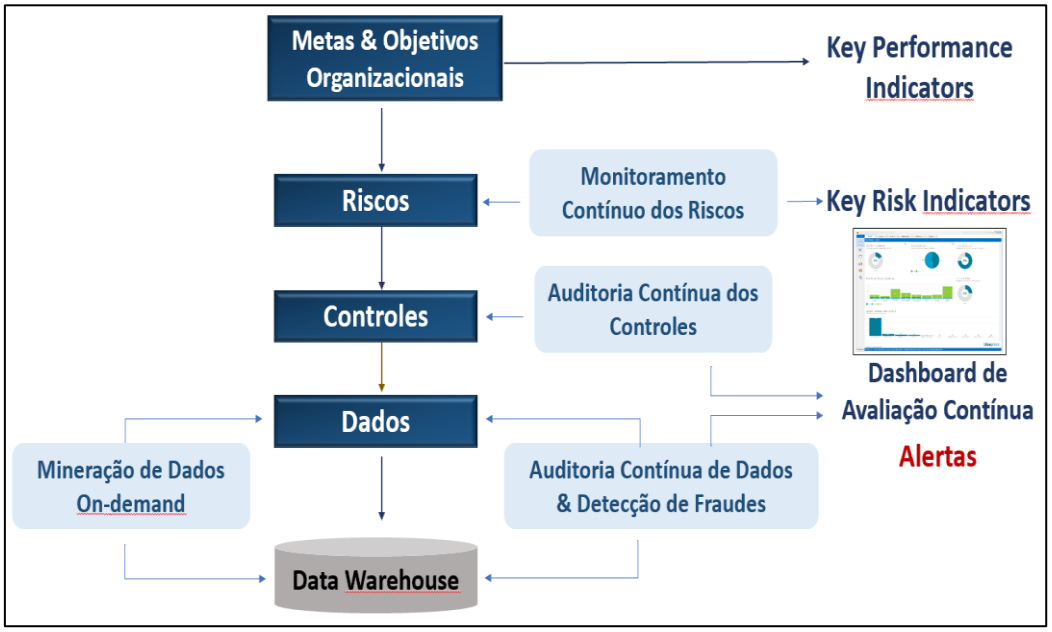

Figura 10 - Representação Simplificada da Auditoria Contínua
Adaptado de: PWC VIETNAM. **Continuous Audit & Monitoring**. 2020.

2.4.5.
A Auditoria na era da Transformação Digital

Segundo Jun e Vasarhelyi (2016), a década de 70, foi o berço da auditoria de TI, pois, nessa época, houve a expansão do uso de computadores por empresas em todos os segmentos econômicos e portes. Contudo, ainda em 2010, a habilitação em TI requeria melhorias (PROTIVITI, 2010). Essa distorção pode ser parcialmente atribuída ao conservadorismo e a rigidez da profissão, que são reforçados pelas orientações dos institutos de auditoria, como também pela regulamentação cada vez mais obsoleta (LIU; VASARHELYI, 2014) em relação à dinâmica evolutiva dos processos e tecnologias, que ocorre atualmente. Outro aspecto a se considerar, era a falta de ferramentas de qualidade que permitissem aos auditores, sem treinamento em TI, automatizar suas atividades (BROWN-LIBURD; ISSA; LOMBARDI, 2015).

Nessa época, nos bancos, a maioria das informações financeiras e evidências de auditoria tornaram se eletrônicas - *Real Time Accounting* (RTA)

(REZAEE; ELAM; SHARBATOGHLIE, 2001). As que, hoje, ainda não o são, como contratos e cheques, passaram a ser digitalizadas. Ademais, o fato dos dados serem eletrônicos ou digitalizados não altera o objetivo ou os padrões de auditoria geralmente aceitos (GAAS - *Generally Accepted Auditing Standards*).

Em função disso, os procedimentos de auditoria precisaram ser adaptados aos novos fluxos de processos e de dados levando ao surgimento da Auditoria Contínua e a sua evolução, como já mencionado. E, com ela, o desenvolvimento de *softwares* especializados em auditoria como Arbutus *Software*®, Shelter EAS®, ACL®, IDEA® e CaseWare® (HARDY, 2015). Seguindo essa tendência, outros *softwares* passaram a ser adaptados aos trabalhos de auditoria, como Excel®, Easy Trieve®, SQL+® e SAS®. Como esses produtos suportam automação, as técnicas e programas utilizadas para avaliar controles pela extração e análise de dados foram denominadas *Computer-Assisted Audit Tools* – CAATs (CHARTERED INSTITUTE OF INTERNAL AUDITORS, 2019).

Essas ferramentas, juntamente com a criação de papéis de auditoria eletrônicos e de seu gerenciamento em plataformas próprias, melhoram a eficiência e a eficácia dos trabalhos realizados. Todavia, a automação observada até então restringia-se a tarefas ou testes específicos, sem que houvesse integração ou coordenação entre os diferentes sistemas ou aplicativos. De forma que os auditores permaneciam executando um grande volume de rotinas para conciliar os dados resultantes desses trabalhos em análises e reportes. Mas, devido aos avanços computacionais, a RPA veio ajudar a resolver esse problema (HUANG; VASARHELYI, 2019).

Assim, observa-se uma Reestruturação de Processo Tecnológico – RPT, ou seja, a reconsideração de métodos e processos de uma área devido ao advento de uma tecnologia disruptiva. Destarte, a auditoria está começando a se valer dessa e de outras, como *cloud, block chain, smart contracts, large data stores e big data*. Há trabalhos, por exemplo, com IA sendo utilizada para detecção, previsão, meta-controles / meta-processos, medição exógena, identificação rápida de fenômenos, integração de evidências e *deep learning* [18]em auditoria (ISSA; SUN; VASARHELYI, 2016).

Contudo, os padrões, regulamentos e legislações tendem a ser afetados mais lentamente que processos, principalmente, em se tratando de auditoria. Segundo Li e Vasarhelyi (2018), atualmente, a ferramenta de apoio à decisão mais usada para o brainstorming feito durante o planejamento da auditoria ainda é a

[18] *Deep learning* é um ramo do *machine learning* que treina computadores para realizar tarefas complexas como reconhecimento de fala e identificação de imagem.

lista de verificação (BELLOVARY; JOHNSTONE, 2007), que apresenta inúmeras limitações (SEOW, 2011). Em função disso, os autores propõem melhorar a eficácia desse processo por meio do uso de um assistente cognitivo, como descrito na Figura 11, devidamente nutrido com o cabedal de conhecimentos necessários à realização de um planejamento de auditoria. Assim, ofereceria suporte às decisões e auxiliaria na avaliação de riscos entre outras colaborações.

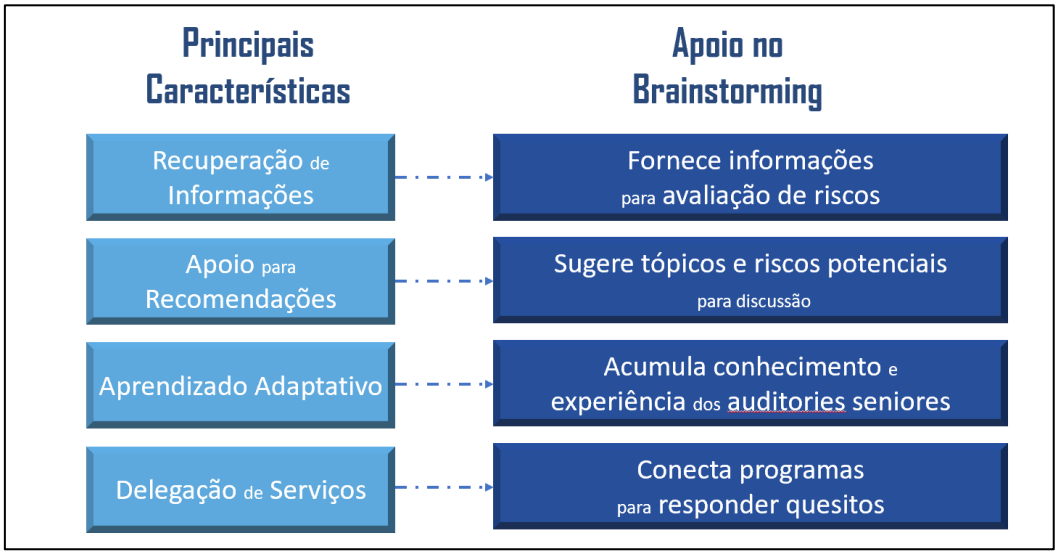

Figura 11 - Assistente Cognitivo para Brainstorming de Planejamento da Auditoria
Adaptado de LI, Q.; VASARHELYI, M. **Developing a cognitive assistant for the audit plan brainstorming session.** International Journal of Digital Accounting Research, v. 18, January, p.123

Há ainda casos do uso de modelos preditivos baseados em aprendizagem de máquina, regressão logística e árvores de decisão, visando à identificação de anomalias relacionadas, por exemplo, a vendas de cartão de crédito, de forma a alertar a organização sobre possíveis fraudes (KUENKAIKAEW, 2013). Contudo, cabe à Alta Administração a decisão de inibir, mesmo que momentaneamente, a realização de uma operação diante de um indício de irregularidade. Essa escolha envolve seu apetite a risco; a análise da relação custo/benefício para a implementação dessa sistemática; e a ponderação sobre um eventual impacto negativo na satisfação do cliente e em sua imagem, se a ocorrência for falsa-positiva.

Essa análise realizada antes da ocorrência do evento caracteriza o conceito de Auditoria Preventiva, que é o que há de mais desafiador, no momento, nessa profissão.

Outros tipos de auditoria também foram concebidos nesse contexto, menos revolucionárias e com enfoque mais tradicional, como a auditoria de inovação. Essa objetiva descobrir os pontos fortes e fracos da organização relacionados aos

recursos, processos e práticas de inovação conforme seus objetivos estratégicos; e orientar as pessoas e os departamentos no alcance das melhorias necessárias ao atingimento desses (CHIESA; COUGHLAN; VOSS, 1996). Outro caso é auditoria de *marketing* digital, que avalia o desempenho das empresas nos canais digitais e apresenta recomendações para melhorias.

De forma análoga, mas mais conservadora, os institutos de auditoria vêm incorporando em suas práticas esses conceitos. Em 2017, o da Escócia definiu como *Digital Auditing*, o uso de ferramentas e tecnologias digitais para apoiar e executar o trabalho de auditoria; e como *Auditing Digital,* a abordagem flexível baseada em riscos para realizar auditorias financeiras e de desempenho nos meios digitais (AUDIT SCOTLAND, 2017).

Diante dessa nova realidade, Dai e Vasarhelyi (2016), conceberam o que seria a Audit 4.0, representada na Figura 12.

> A Auditoria 4.0, apoiaria-se nas tecnologia da Indústria 4.0, para analisar, modelar, e visualizar dados, objetivando a descoberta de padrões; a identificação de anomalias; a extração de informações úteis; e o fornecimento de garantia eficaz, eficiente e em tempo real. Basicamente, faria uma sobreposição dos processos de gestão de negócios da Indústria 4.0 e usaria uma infraestrutura semelhante, mas para fins de validação.

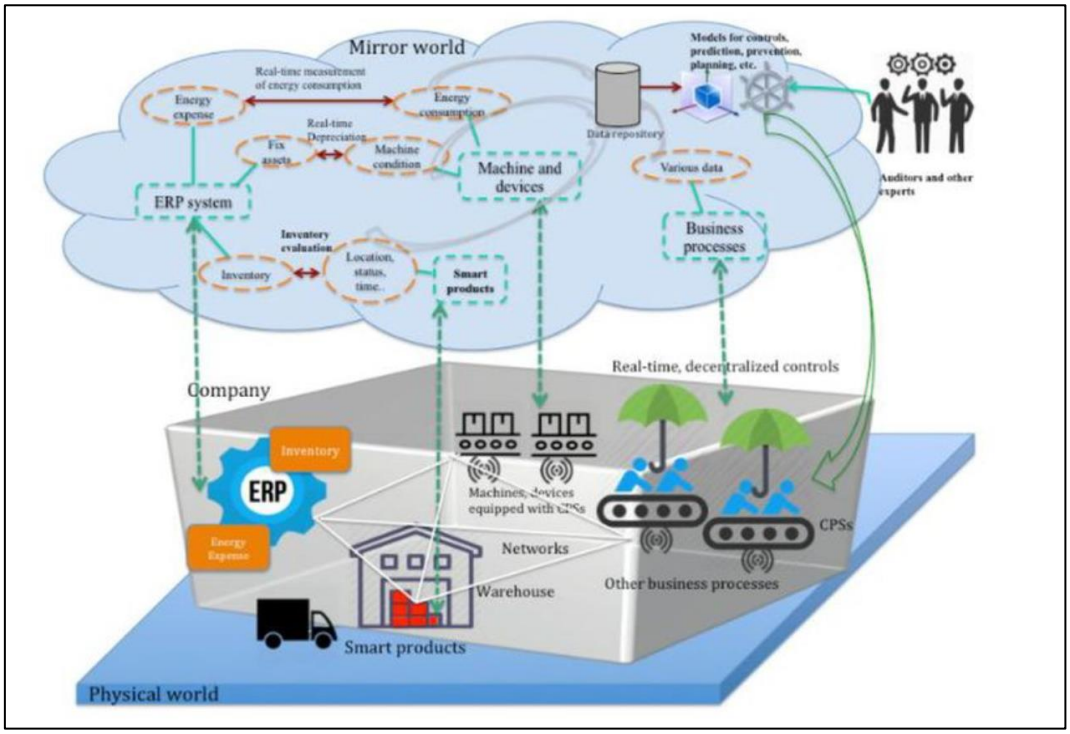

Figura 12 - Representação da Audit 4.0
Fonte: DAI, J.; VASARHELYI, M. A**. Imagineering audit 4.0**. Journal of Emerging Technologies in Accounting, [s.l.], v. 13, no 1, p. 11, 2016.

Nela, as organizações usariam equipamentos que captariam dados interna e externamente (fornecedores, clientes, mídia, entre outros), quase

instantaneamente, por meio de uma rede de sensores, computadores embarcados e módulos de *software*. Esses alimentariam modelos analíticos que monitorariam a qualidade dos produtos e serviços, identificariam falhas, trariam eficiência operacional e auxiliariam na tomada de decisões. O processo de auditoria seria baseado numa representação espelhada do mundo real (*mirror world*) relacionadas a questões financeiras e, especialmente, não financeiras. Assim, concluíram que a auditoria por exceção (VASARHELYI; HALPER, 1991) seria extremamente automatizada e usada para destacar problemas mais relevantes em todas as esferas da organização. Consequentemente, essa abordagem reequilibraria substancialmente os conceitos de linhas de defesa.

Contudo, esse modelo só se tornará real para as empresas que efetivamente criarem um ecossistema de auditoria integrado aos processos, sob uma visão de riscos e monitoramento contínuo, e com a automatização das rotinas conforme os objetivos estratégicos da organização. E, atualmente, uma das formas mais vantajosas de realizar essa robotização é por meio da RPA.

3
Metodologia

3.1.
Aspectos epistemológicos e ontológicos

Segundo Heidegger (1927), a ontologia é o conhecimento do ser dos entes e a explicação do próprio ser. Nesse sentido, o presente trabalho visa aprofundar o entendimento sobre o uso da automação robótica de processos pela auditoria interna e pelos bancos nacionais.

Para isso, inicialmente, foi realizada uma pesquisa sobre os estudos que abordam as lentes teóricas utilizadas - transformação digital, RPA e auditoria interna, objetivando, sucintamente, salientar os aspectos epistemológicos mais relevantes sobre esses temas, que se alinhavam à proposta desse estudo. Em relação a auditoria interna, houve, ainda, a preocupação de evidenciar a evolução de sua gnose, numa abordagem singela e prática, almejando demonstrar a complementariedade dos enfoques desenvolvidos ao longo dos anos; e a mudança de uma abordagem passiva, tecnocrata e proforma, para uma ativa, estratégica e de vanguarda. Bem como, de explicar o modelo das três linhas de defesa, posto que esse foi escolhido, devido a sua simplicidade, clareza, objetividade e conhecimento prévio pela organização, para ser um dos pivôs do *framework* que será apresentado.

Cabe, aqui, salientar que o conhecimento da auditoria contínua (ontologia da auditoria) advém de sua metodologia, esquematizada na Figura 13. Essa envolve o mapeamento do inventário de dados referentes aos processos corporativos (ontologia dos processos), por meio de sua classificação, sua validação, seu fluxo e seu reuso (ontologia dos domínios) para aplicação das regras e dos testes de auditoria. Pois, desses procedimentos originam-se os relatórios e as exceções para averiguação. Como também, os *insights* para a formação da convicção; para o assessoramento dos setores nos diversos níveis da organização; e para a tomada de decisão. E, é esse método, composto pela auditoria contínua de dados; pelo monitoramento contínuo de controles; pela avaliação e monitoramento contínuo de riscos; e pelo monitoramento contínuo do *compliance*, que estará subliminarmente presente na análise e na proposta de *framework* que será descrita. Só que, agora, ele terá a inclusão da automação robótica de processos (RPA) com a prévia avaliação e modelagem desses.

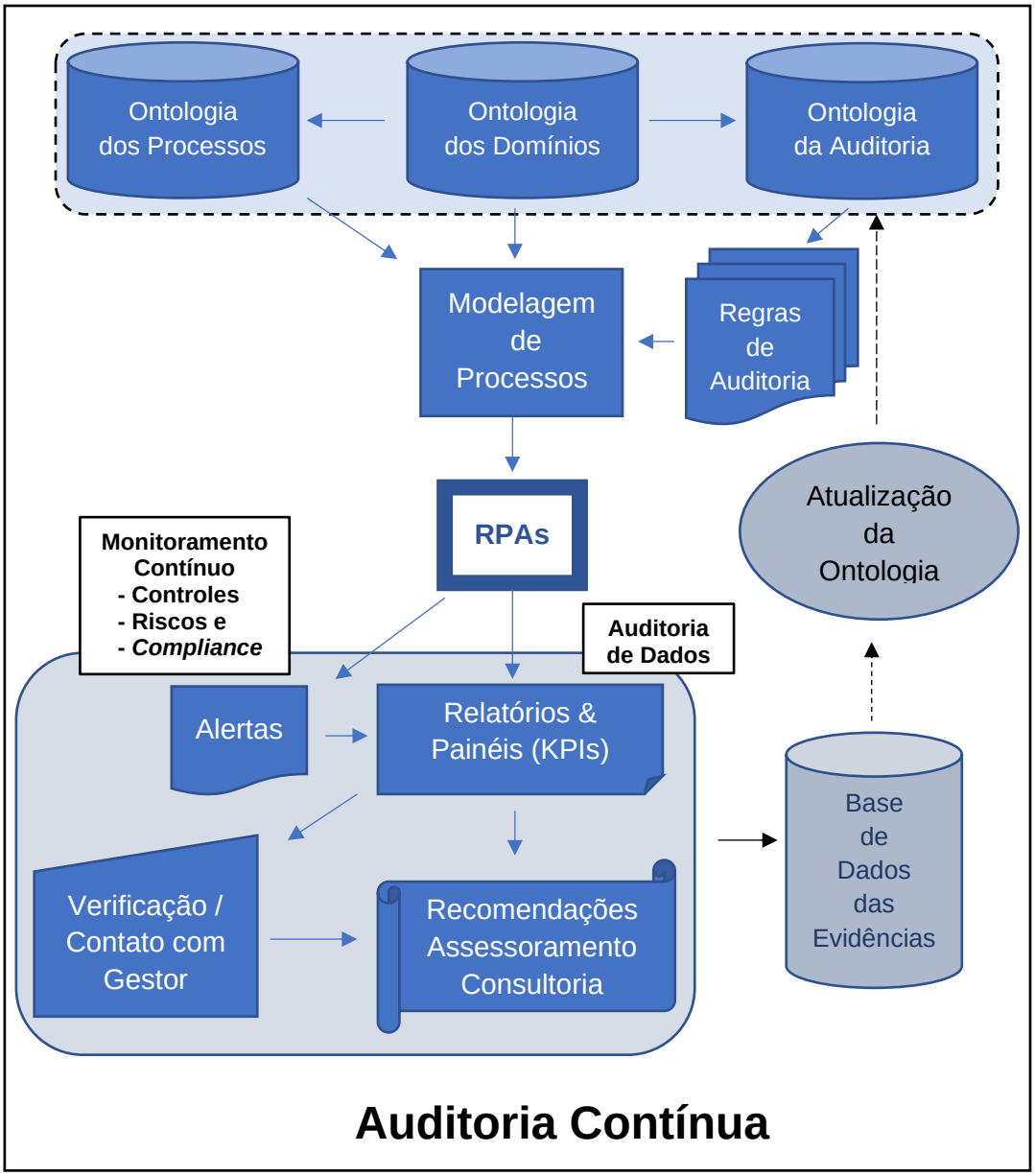

Figura 13 - Modelo ontológico e epistemológico proposto
Fonte própria

Depois, para melhor entendimento desses fenômenos, buscou-se contextualizá-los, refletindo-se sobre o impacto da indústria 4.0 e da transformação digital no macro e no microambiente que envolvem as instituições financeiras mundiais e nacionais, considerando uma avaliação crítica das inter-relações entre os elementos desse novo ambiente em relação aos objetivos estratégicos dessas empresas, de forma a certificar-se que a ferramenta em questão não é um "*modismo*" ou o produto de uma boa estratégia de *marketing*. Ou seja, optou-se pelo enfoque do pensamento complexo, característico da metodologia da auditoria interna, que apoia-se na complementaridade entre as visões linear e sistêmica do mundo, pois não é incomum observar-se estudos

sobre novas ferramentas, sem a visão do seu papel e do seu valor no planejamento organizacional ou na estrutura existente – benefícios, resultados esperados, capacitação requerida, riscos, objetivos, controles; como é feita a integração dessa com sistemas, pessoas, processos e áreas; e como garantir que as expectativas com a adoção dessa ferramenta sejam atingidas e renovadas.

Após, houve a convergência dos casos para a auditoria interna de bancos nacionais e foram apresentadas perspectivas para essa função, diante do impacto da transformação digital e do novo ambiente de negócios, no *assurance* e na gestão dos riscos, dos controles internos, do *compliance* e da governança.

Uma vez exploradas e analisadas essas informações, foram identificados os pontos de correlação entres os referenciais teóricos, as pesquisas, os casos e as experiências positivas e negativas descritas, de forma a compreender a interconectividade desses fenômenos para, então, começar a reconhecer as práticas que melhor garantiriam o êxito na implementação de um projeto de RPA na auditoria interna de um banco nacional, a escalabilidade desse e a expansão para toda organização.

É importante frisar que, no contexto dos robôs, almejou-se, principalmente, entender as relações entre o(s) dispositivo(s) físico(s); as regras de negócio; as abordagens de inteligência usadas para racionalizar as tarefas que seriam executadas; e o ambiente em que essas seriam realizadas (SCHLENOFF et al., 2012). Bem como conhecer os riscos envolvidos; a metodologia de avaliação dos processos para automação; a estrutura para o desenvolvimento de MVPs e para escalabilidade das RPAs; as lacunas de capacitação, tanto dos usuários como do *dev team;* as ações necessárias num eventual contingenciamento; e os métodos de trabalho e de planejamento mais adequados.

Uma vez adquirida essa cognição, objetivou-se pragmaticamente, incorporá-la à Auditoria Contínua, como meio de torná-la uma prova de conceito, visando à expansão do uso de RPA por toda organização.

Para isso, optou-se por usar o modelo das três linhas de defesa – proprietários do risco, supervisores dos riscos e avaliadores independentes, mas de forma diferente. Ao invés de identificar, numa estrutura existente, as linhas de defesa e suas respectivas responsabilidades, como geralmente ocorre. Elas tornar-se-iam linhas de “ataque” (MARKS, 2015), pois as RPAs já seriam desenvolvidas, controladas, supervisionadas e avaliadas numa estrutura que atenda o *compliance* regulatório e que, previamente, seguisse as atribuições de cada segmento desse modelo dentro dos bancos.

3.2.
Tipo de pesquisa

Como este estudo objetiva propor um *framework* para o uso da RPA no planejamento estratégico da auditoria interna dos bancos brasileiros sob o enfoque do modelo das três linhas de defesa, optou-se por uma pesquisa exploratória aplicada (CRESWELL, 2010), pois envolve uma tecnologia incipiente que está sendo adotada exponencialmente, com sucessos e fracassos. Então, é imprescindível ter uma maior compreensão sobre o fenômeno da automação robótica de processos e como a auditoria interna pode participar ativamente nessa mudança. Não somente adotando esse paradigma, mas assessorando toda a organização em sua implantação e manutenção. De forma a colaborar na adaptação dos bancos nacionais à transformação digital; e, no desenvolvimento de diferenciais competitivos visando à perenidade da instituição.

3.3.
Abordagem da pesquisa

Este trabalho foi estruturado como uma pesquisa qualitativa bibliográfica documental prospectiva (GERHARDT; SILVEIRA, 2009), na qual houve uma intensiva leitura, em diversas fontes, dos temas que envolveram o estudo, de modo a analisar as teorias, os casos, as *surveys*, as situações descritas e concluir sobre as melhores práticas para a implementação de um projeto de RPA, considerando o planejamento estratégico integrado, a auditoria interna, a auditoria contínua, o modelo das três linhas de defesa e sua adoção por bancos nacionais.

3.4.
Justificativa da abordagem da pesquisa

A pesquisa bibliográfica documental é a que mais se adequa a proposta desse estudo, posto que visa compilar o conhecimento explícito relacionado aos temas, como exigências legais, normativas e regulatórias, internas e externas, que envolvem a auditoria interna e os bancos nacionais, com os achados e as conclusões dos trabalhos acadêmicos e dos relatórios de empresas e órgãos especializados ou supervisores sobre transformação digital, RPA e auditoria. Permitindo, assim, a sintetização das conclusões sobre as diretrizes a serem adotadas em relação aos diversos aspectos que envolvem um projeto de implementação de uma ferramenta num ambiente complexo como o bancário.

3.5.
Limitações da abordagem de pesquisa

Devido a abordagem documental dessa pesquisa exploratória aplicada, não foram aprofundadas questões relacionadas as ferramentas de RPA; ou os riscos relacionados à privacidade e à segurança; ou a estrutura de TI subjacente à robotização. Tampouco foram avaliadas outras tecnologias que estão sendo utilizadas pela auditoria contínua, como *blockchain* e IA. Posto que esses esclarecimentos são próprios de um trabalho descritivo, cujo tema já é conhecido, e não de um de vanguarda, como o apresentado.

Em função disso, ainda não há literatura específica, experimentos e estudos de casos suficientes para a construção de um arcabouço epistemológico que embase uma pesquisa explicativa sobre todo o fenômeno.

Logo, o trabalho se limitou a abordar o tema proposto a partir do ponto de vista do caso em particular, não sendo considerados outros setores econômicos. Assim, as conclusões apresentadas neste trabalho estão limitadas ao contexto específico da auditoria interna em bancos nacionais e não devem ser correlacionadas a outras situações sem a devida análise e ponderações específicas.

4
Contextualização

Neste capítulo, inicialmente, serão apresentados casos sobre as estratégias adotadas por instituições financeiras para enfrentar a nova realidade trazida pela indústria 4.0 e a transformação digital. E, em seguida, o impacto dessas mudanças no sistema bancário nacional. Após, será abordado o grau de automação robótica de processos nas empresas e sua adoção em bancos. Depois, serão apresentados os modelos de atuação das auditorias internas em bancos nacionais.

Essas informações são relevantes para contextualizar o setor bancário internacional e nacional. E, para demonstrar o impacto da escolha de suas estratégias (seja melhorando a experiência do cliente, a eficiência operacional, as duas, ou desistindo) e da forma como optaram realizá-la, na performance da organização. Posto que, as estratégias não tão bem sucedidas ou os fracassos ocorridos dificilmente são conhecidos. Mas, o fato de não alcançarem desempenho semelhante aos casos de sucesso apresentados, ou perderem *market share*, são evidências que estão tendo dificuldades. E, essas, geralmente estão relacionadas aos processos e a integração desses com os sistemas de TI.

4.1.
Transformação Digital em instituições financeiras

No caso das instituições financeiras, a escolha da estratégia para enfrentar a transformação digital tem sido diversa.

O banco australiano *Westpac*, em 2014, seguiu a estratégia *mobile first* e desenvolveu mais de 40 aplicativos para atendimento aos clientes e para a venda de produtos. No primeiro ano, 20% dos produtos mais simples (cartões, certificados de depósitos bancários, empréstimos simplificados) estavam sendo oferecidos nesse canal; e 7,5% dos clientes os estavam adquirindo. Em 2019, a instituição declarou que estava tentando reformular, rapidamente, sua infraestrutura e serviços de tecnologia; e preparando-se para lançar uma nova plataforma bancária totalmente digital (BAJKOWSKI, 2019).

Esse caso deixa evidente que, para cada tecnologia, há uma estratégia e um custo. E, não necessariamente há integração entre elas, levando ao desperdício e ao não atingimento dos resultados projetados (ROGERS, 2016).

Já o BBVA - Banco Bilbao Vizcaya Argentaria que possui 135 mil funcionários e atua em 34 países (BBVA, 2020), optou pelo foco em UX. Sua

eficiência digital é percebida desde o momento em que o cliente abre a conta pelo celular, pois o processo leva apenas cinco minutos. Além disso, é possível adquirir 7 produtos em um minuto cada; e, é necessário apenas um dia para a contratação de um financiamento imobiliário.

Em relação a integração com sistemas legados, o Danske - Banco Dinamarquês, é um exemplo de eficiência. Fundado em 1871 e atuando em 12 países, adquiriu seis bancos desde 2010 e reduziu o custo operacional em 20% com a criação de uma nova plataforma de negócios (DUREVALL, 2014).

No mercado nacional, o Bradesco lançou em 2017, um banco digital chamado Next, adotando a estratégia *give up* (SALOMÃO, 2017). Ele é controlado por aplicativo, foca o público jovem e oferece três cestas de serviços, sendo que nenhuma é gratuita. No 3º trimestre de 2019, o Next alcançou a marca de 1,4 milhão de contas. Destas, cerca de 79% não eram de clientes do Bradesco (BRADESCO, 2019).

Finalmente, um dos destaques em estratégia digital no mercado financeiro é o DBS - *The Development Bank of Singapore Limited*. Um grupo líder de serviços financeiros na Ásia, sediado em Cingapura e fundado há 50 anos, com mais de 280 filiais em 18 mercados, com presença crescente na Grande China, no Sudeste Asiático e no Sul da Ásia. Suas classificações de crédito "AA" e "Aa1" estão entre as mais altas do mundo (DBS BANK, [s.d.]). Ademais, em 2016, 2018 e 2019, foi nomeado “Melhor Banco Digital do Mundo” pela *Euromoney* (EUROMONEY, 2016, 2018 e 2019).

Mas, esse resultado só foi obtido devido a uma mudança de paradigma ocorrida em 2009. Devido à crise financeira global, o DBS decidiu se concentrar no segmento asiático. Na época, o índice de satisfação do cliente estava bem abaixo da média do setor. Em função disso, ficaram seis meses trabalhando com clientes, colaboradores e especialistas. Então, obtiveram 96 ideias sobre o que o serviço asiático realmente significava. Em agosto de 2010, as 50 principais pessoas do DBS se reuniram por dois dias e destilaram essas ideias em três conceitos: respeito, facilidade e confiabilidade - RED. O vermelho é uma cor que representa sucesso nas culturas asiáticas; uma das cores da empresa; e, um adjetivo, que rapidamente se tornou parte do vocabulário da companhia, causando uma mudança comportamental, pois adotaram uma abordagem que abrangia tanto o *hardware* como o "*heartware*"[19]. Ademais, tiveram o apoio do CEO e

[19] *Heartware* é um neologismo relacionado ao estímulo das pessoas ao engajamento por meio da associação das iniciativas com emoções e valores.

utilizaram *hackathons*[20] e ferramentas de *lean startup*[21] para criar o conceito de "banco invisível", que passou a moldar toda abordagem de digitização da organização (SIA; SOH; WEILL, 2016).

Paralelamente a isso, devido ao aumento nos requisitos de *compliance* pelos órgãos reguladores, como a Comissão de Supervisão Financeira de Taiwan, em 2014, foi implementada a auditoria contínua com o uso de CAATs e a construção de uma *Audit Data Warehouse*, começando pelo banco em Cingapura (LIANG; ZHENG, 2016).

Ou seja, em 2016, o DBS tornou-se o melhor banco digital, pois promoveu uma revolução cultural interna por meio da conscientização e do engajamento do CEO e de todos os funcionários. E, pela adoção de métodos ágeis para digitizar a empresa, isto é, promoveram a eficiência operacional por meio da integração dos sistemas legados e dos processos. É importante frisar que ao adotarem a auditoria contínua, CAATs e um *Data Warehouse*[22], garantiram a manutenção dessa eficiência; e, ainda a melhoraram a gestão dos riscos, dos controles internos, do *compliance* e da governança. Assim, conseguiram melhorar a satisfação dos clientes e atingir o objetivo principal da estratégia de transformação digital que é a melhoria da UX. Mas, é importante frisar que toda essa mudança de paradigma até o reconhecimento levou sete anos. Logo, foi necessário um sólido planejamento estratégico de longo prazo e uma governança muito forte.

4.1.1. Efeitos da Transformação Digital no Sistema Bancário Brasileiro

A indústria 4.0 vem trazendo novos entrantes ao mercado bancário brasileiro como Neon®, PicPay®, Ame Digital®, Next® e Original®. Atualmente, a startup Nubank®, fundada em 2013, com a proposta de resolver problemas financeiros usando tecnologia, é a principal *fintech* da América Latina com mais de 5 milhões de clientes (NUBANK, 2020). Destarte, em um ano, teve seu valor aumentado de 1 bilhão para dez bilhões de dólares.

Em 2019, a Stone®, com apenas sete anos de existência, já possuía um *market share* de 6% e o dobro de valor de mercado da Cielo®, que tem 25 anos

[20] *Hackathon* é uma maratona de programação, na qual especialistas se reúnem por horas, dias ou até semanas, a fim de explorar dados, códigos e sistemas lógicos; discutir novas ideias e desenvolver projetos de software ou hardware.
[21] *Lean Startup* é uma metodologia para o desenvolvimento de negócios e produtos que visa reduzir seus ciclos de desenvolvimento e descobrir, rapidamente, se a proposta de um modelo de negócios é viável.
[22] *Data Warehouse* é o armazenamento das informações relativas às atividades de uma organização, na forma de um banco de dados consolidado.

no ramo e 38% de participação. Naquele ano, a notícia de que o Facebook® criaria sua moeda, Libra, causou furor internacional e preocupação dos governos, caso os 2 bilhões de usuários da rede aderissem a tal sistema monetário. Ademais, aumentaram as preocupações, já comuns, do uso de criptomoedas para transações ilegais. Na China, 90% dos pagamentos são realizados por meio de aplicativos. Um dos mais usados é o Alipay®, uma plataforma de pagamento do Alibaba Group® (CIRNE, 2019).

Em pesquisa realizada pelo The World Bank®, no ano de 2017, o principal meio de pagamento dos brasileiros, ainda, era o dinheiro em espécie. E, 30% da população, cerca de 48 milhões de pessoas, não possuía conta bancária, devido, principalmente, à dificuldade de comprovação de renda. Esse segmento movimenta cerca de 670 bilhões de reais ao ano, sendo que 60% dessas pessoas têm acesso a celular e a internet (DEMIRGÜÇ-KUNT et al., 2017). Em função disso, esse mercado também está sendo visado pelas *fintechs.* Consequentemente, agora, as instituições financeiras de varejo vêm analisando estratégias para atender esse público de forma segura e rentável.

Segundo a 27ª Pesquisa de Tecnologia Bancária (FEBRABAN, 2019), da qual participaram 20 bancos brasileiros ou com atuação no Brasil, que representam 91% dos ativos da indústria bancária no País:

> O setor de serviços financeiros, no Brasil e no mundo, passa atualmente por um ponto de inflexão. Para lidar com a evolução de um segmento que atravessa profundas transformações tecnológicas, regulatórias e de mercado, os bancos se deparam com a necessidade de conduzir mudanças estratégicas em seus modelos de negócios e operacionais (FEBRABAN, 2019).

Essa fonte relata que, em 2018, seis em cada dez transações bancárias foram realizadas por *mobile* ou *internet banking*. Além disso, foi observado que o uso dos canais digitais continua crescendo devido, principalmente, à praticidade, à segurança e à conveniência que apresentam. Mas que o *mobile* já representa o dobro de transações em relação ao internet banking. Em função disso, os esforços de *marketing* e vendas vêm sendo direcionados mais intensamente para o primeiro. Na Figura 14, há a reprodução desses resultados.

Foi observado que, no mundo, os bancos são o segundo setor que mais destinam recursos para tecnologia atrás apenas do setor público. Contudo, em 2018, no país, pela primeira vez, seus gastos equipararam-se ao daquele. As instituições financeiras aplicaram R$ 19,6 bilhões em tecnologias, um crescimento de 3% em relação a 2017. Esses recursos foram usados, principalmente, em *softwares*, pois permitem o desenvolvimento de novas funcionalidades que

melhoram a experiência do consumidor bancário. Mas, para alcançar esse objetivo, investiu-se, também, em segurança e capacidade de processamento. Houve, ainda, significativos investimentos em ferramentas de comunicação e relacionamento com os clientes, devido ao aumento expressivo das interações realizadas entre os bancos e os usuários. Em 2018, as feitas por *chats*, operadas por atendentes, tiveram um crescimento de 364%, chegando ao volume de 138,3 milhões. E, as por *chatbots*, que são automatizadas por robôs e utilizam linguagem natural como forma de aperfeiçoamento, 2.585%, equivalendo a 80,6 milhões contatos.

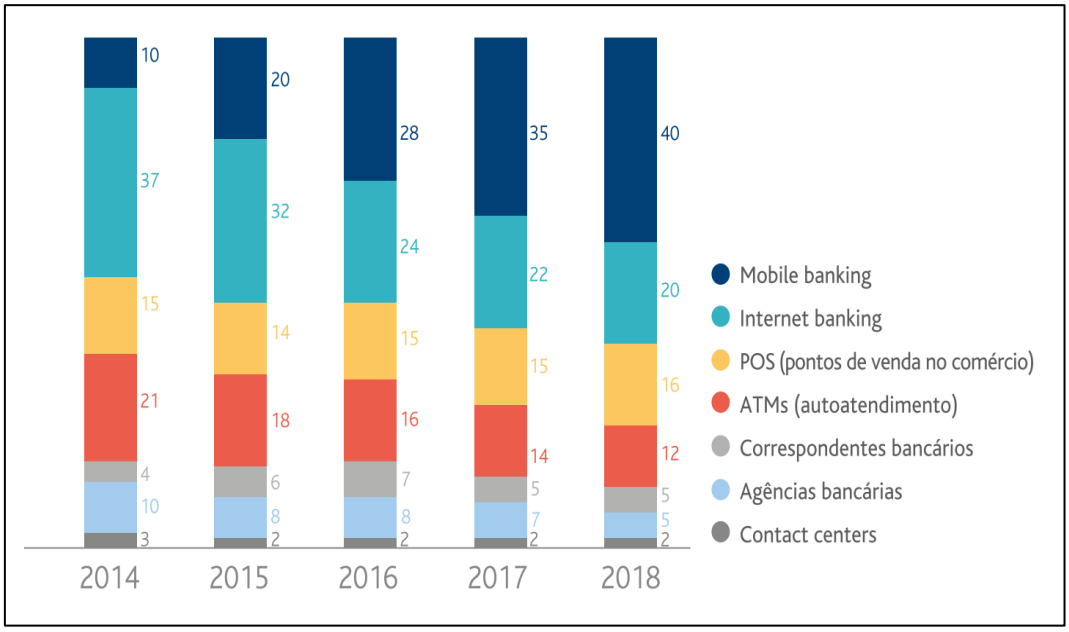

Figura 14 - Composição das Transações Bancárias por Canal (em %)
Fonte: FEBRABAN. **27ª Pesquisa FEBRABAN de Tecnologia Bancária**.2019. p 11

Destarte, constataram que as tecnologias mais empregadas foram *big data, analytics*, inteligência artificial e computação cognitiva. E, as que mais receberam investimentos, além das citadas, foram *blockchain,* robótica e *openbanking / marketplacebanks.*

Logo, evidencia-se que todas essas tecnologias dependem da disponibilidade de dados abundantes, acessíveis, claros e integrados. Para alcançar essa sinergia tecnológica, é necessário um planejamento estratégico claro e preciso que elabore um novo modelo operacional de longo prazo. Esse deverá primar pela integração entre sistemas, plataformas, *softwares* e ferramentas.

4.2.
RPA nas organizações

Segundo a Gartner® (2019), em 2018, a receita obtida por softwares de RPA cresceu 63,1%, totalizando US $ 846 milhões e tornando-se o segmento que mais cresce no mercado global de *software* corporativo. Ademais, projetou que, em 2019, essa receita atingiria US$ 1,3 bilhão. Naquele ano, os cinco principais fornecedores de RPA controlavam 47% do mercado.

Embora a RPA possa ser aplicada em qualquer organização, os principais usuários tem sido bancos, seguradoras, empresas de telecomunicações e empresas de serviços públicos, porque, tradicionalmente, têm muitos sistemas legados e as soluções com RPA garantem a integração entre eles. Além disso, apresenta um ciclo de implantação mais rápido, em comparação com outras alternativas, como as plataformas de BPM ou a terceirização de processos de negócios[23].

Em 2018, foi realizada uma pesquisa com 549 empresas líderes de mercado na Europa, cujos detalhes estão reproduzidos na Figura 15 (INFORMATION SERVICES GROUP, 2019). Nessa verificou-se que, a maioria, 42%, ainda não tinha iniciado o processo de implantação de RPA, ou tinha realizado apenas uma Prova de Conceito. A Projeção para 2020 era que a maioria, 54%, estaria na fase avançada, com 10 ou mais de 25 processos automatizados.

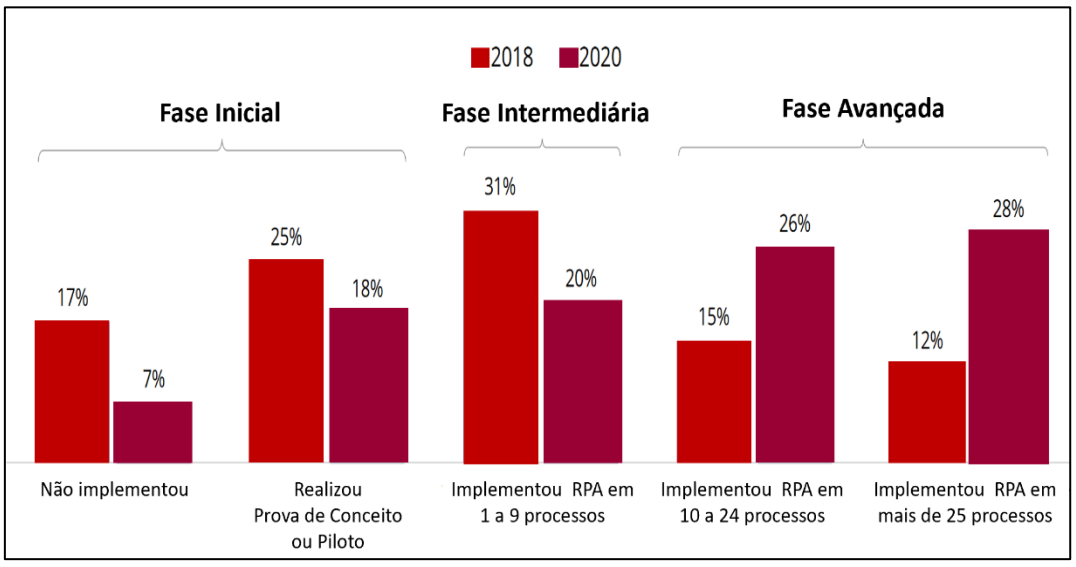

Figura 15 - Pesquisa sobre RPA na Europa
Adaptado de ISG. **RPA in Europe**. Enterprise plans, budgets and organization impact. 2018

[23] Terceirização de processos de negócios é a subcontratação por terceiros de operações relacionadas a negócios da empresa.

Porém, o mesmo relatório revelou que as principais preocupações relacionadas a essa mudança de paradigma são a segurança na governança, na gestão de riscos, no *compliance* e na TI. Como também, a resistência a mudanças pela empresa como um todo; e a falta de orçamento para implementação, mesmo sendo relativamente baixo, posto que o retorno do investimento, geralmente, ocorre em um ano. Outros aspectos salientados foram: a falta de suporte de TI e do comprometimento da Alta Administração; as limitações dos *softwares* de RPA disponíveis atualmente no mercado; a falta de capacitação para a implementação; e a exaustiva lista de processos disponíveis para automação.

Portanto, evidencia-se que a adoção da RPA deve seguir um framework integrado ao planejamento estratégico da empresa e as preocupações apresentadas devem ser tratadas. Mas, principalmente, deve-se engajar os *stakeholders* e implementar uma linha de comunicação que prepare os usuários finais para uma mudança nos papéis que passarão a desempenhar no dia-a-dia. (ERNST & YOUNG, 2016).

4.2.1. RPA em instituições financeiras

Estima-se que os bancos desembolsem quase US$ 270 bilhões por ano, apenas em conformidade e que esse valor represente mais de 10% do custo operacional dessas organizações. Com a automação robótica de processos, os bancos poderiam reduzir as atividades manuais, melhorar a conformidade, atenuar riscos, aprimorar a experiência do consumidor e incrementar os resultados devido à diminuição dos custos operacionais. Além disso, não há requisitos adicionais associados à infraestrutura e sua abordagem é, basicamente, *low-code*. Ou seja, não há a codificação linha por linha, e, sim, a elaboração de um fluxograma (MARUTI TECHLABS, 2019).

Em função disso, a RPA vem sendo experimentada em diversas instituições financeiras com sucessos e fracassos. Esses, dificilmente, são noticiados. Além disso, há a preocupação de não divulgar informações estratégicas. Então, mesmo, nas publicações oficiais, não há detalhes sobre essas iniciativas, com sua real abrangência e seus resultados específicos.

Um caso de sucesso do uso da RPA, no setor bancário, é o Banco Popular®, que é um dos 50 principais bancos dos EUA em ativos. Sediado em Porto Rico e fundado em 1893, possui aproximadamente 8.000 funcionários e cerca de 880 agências (em Porto Rico, Ilhas Virgens Americanas, Ilhas Virgens Britânicas, Nova

York, Chicago e Flórida). Em 2014, assinou um contrato com a IBM e, em 2018, foram implementadas as soluções IBM® *Business Process Manager* e IBM® *Robotic Process Automation* com *Automation Anywhere*®, executada em nuvem e dimensionada conforme a necessidade da empresa (IBM, 2018). Note que, nesse caso, a solução envolveu a união de BPA com RPA.

Na Figura 16, há a reprodução de um processo padrão de emissão de faturas com a robotização feita pela IBM® para o Banco Popular®.

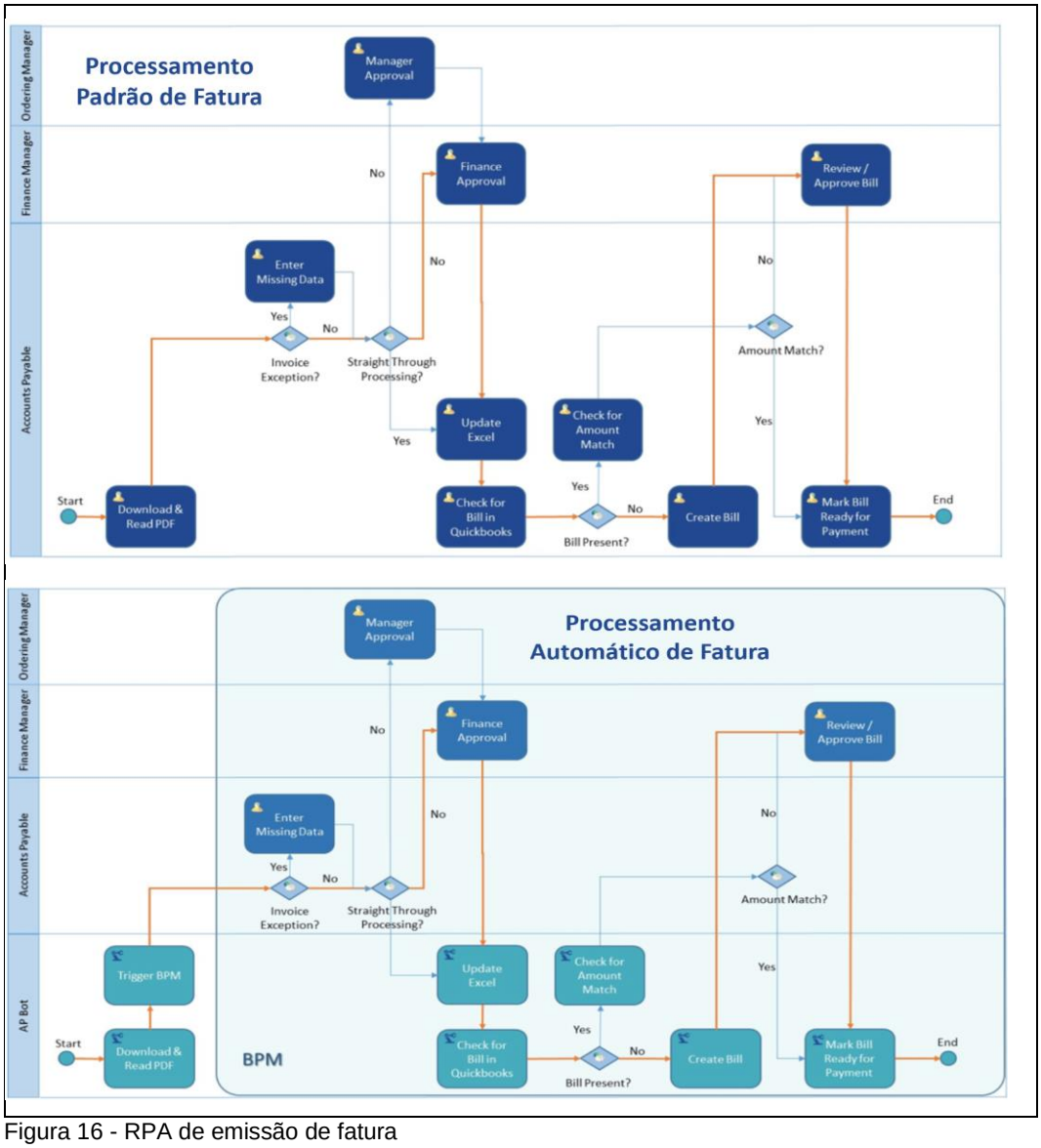

Figura 16 - RPA de emissão de fatura
Fonte: IBM. **Invoice processing in the digital world, powered by BPM and RPA - Cloud computing news**.2018.

Outro uso da RPA, foi desenvolvido, em 2016, no BNY Mellon® com apoio da BluePrism®. No final daquele ano, 150 robôs estavam em produção, englobando processos de liquidação de transações financeiras, comerciais e de custódia. Além disso, os robôs pesquisavam as negociações e resolviam

discrepâncias. Nesse caso, a grande vantagem adveio do tempo gasto na reconciliação de uma falha, numa transação financeira, que deixou de ocupar de 5 a 10 minutos de um funcionário, para ser executada num quarto de segundo. Adicionalmente, o banco obteve uma melhoria de 88% nos tempos de processamento das transações e das validações de fechamento de contas de negociação, que são realizadas em cinco sistemas diferentes, à uma taxa de precisão de 100%. Em função disso, os funcionários do BNY Mellon® ficaram com tempo disponível para dedicarem-se ao controle de qualidade operacional e a evetuais *outliers*. E, devido a isso, em 2017, a instituição ganhou o prêmio NOVA para inovações em tecnologia (BNY MELLON, 2017).

O Danske Bank® desenvolveu um robô que transfere automaticamente as informações coletadas durante uma reunião entre um consultor bancário e um cliente. Antes, o funcionário levava de 20 a 30 minutos para inserir esses dados em duas plataformas e, agora, a RPA, leva segundos. No Sumitomo Mitsui®, a automação bancária permitiu, que essa instituição financeira japonesa, reduzisse 400.000 horas em trabalho manual dos empregados (PHANEUF, 2019).

Em 2017, o Citigroup Inc®. lançou um piloto da RPA que automatizava os pagamentos de importação comercial na Índia e na China, o que resultou numa redução significativa dos processos manuais e numa grande melhoria no tempo de resposta das tarefas básicas (CITI, 2017). Essa entre outra iniciativas relacionadas a centenas de processos que tiveram o tempo de execução reduzido, como a abertura de uma conta de corretagem, a executação de pagamentos ou o tratamento de uma contestação no cartão de crédito, levou-o, entre outros fatores, a ser nomeado, naquele ano, o melhor banco digital do mundo pela Euromoney® (EUROMONEY, 2017).

O OCBC - *Oversea-Chinese Banking Corporation®,* é o banco mais antigo de Cingapura. Ele foi formado em 1932, a partir da fusão de três bancos locais, o mais antigo havia sido fundado em 1912. Atualmente, é o segundo maior grupo de serviços financeiros do sudeste da Ásia, em ativos, e um dos bancos com classificação mais alta do mundo, com rating Aa1 da Moody's®. Em 2015, foi implementado o uso de RPA na Central de Atendimento dos clientes. Em 2017, os robôs já estavam na segunda geração – seus nomes: Bob e Zac. Bob ajuda no processamento de pedidos de reestruturação de empréstimos para habitação. Ele conseguiu reduzir o tempo de reavaliação desses de 45 minutos para apenas um. Além disso, verifica a elegibilidade do cliente para fazes jus a reavaliação de seu empréstimo à habitação, recomenda opções de reprecificação e, até, elabora o e-mail de recomendação. Já Zac auxilia a equipe de Finanças e colabora na

elaboração de relatórios diários de desempenho de vendas. As tarefas realizadas por ambos não requerem processamento cognitivo ou tomada de decisão de nível superior e os funcionários anteriormente envolvidos nessas atividades, agora, realizam outras de maior valor, focadas em oferecer um serviço melhor ao cliente (OCBC BANK, 2017). Adicionalmente, em parceira com a Pega Systems® foi desenvolvido o ROME - *Relationship Opening Made Easy*, uma solução de RPA para abertura de contas que realiza todas as 150 tarefas desse processo, criando uma experiência perfeitamente integrada para o cliente e os empregados. Dessa forma, alcançaram um aumento de 40% na satisfação dos clientes, um incremento significativo no NPS e o crescimento de mais de 10% nas vendas durante a abertura de contas (PEGASYSTEMS, 2019).

Ao experimentar a RPA, o DBS® percebeu que poderia haver um aumento nos riscos do negócio, se não houvesse a padronização do projeto de automação. Pois, a instituição possui diferentes perfis de empregados e diversas áreas de atuação, que poderiam usar diferentes ferramentas RPA, ou procedimentos diferentes no mesmo software, aumentando, em ambos os casos, a possibilidade de falhas operacionais (CHANDEL, 2019). Também percebeu que era necessário o estabelecimento de diretrizes para informar as equipes comercial e técnica sobre a aplicabilidade e as limitações da RPA. Devido a isso, em fevereiro de 2017, fez uma parceria com a IBM *Global Business Services*® e com a IBM *Global Technology Services*® para dimensionar um Centro de Excelência (CoE), pois almejava expandir as RPAs para além das operações de *back-end* e implementá-la em toda instituição. Apenas cinco meses depois, o DBS® já havia otimizado mais de 50 processos de negócios complexos. E, em 2018, ainda utilizando-se da parceria com a IBM®, combinou IA com RPA para oferecer uma resposta mais rápida aos alertas relacionados a lavagem de dinheiro. (IBM SERVICES, 2018).

No Brasil, o uso da automação robótica de processos em bancos também é recente. Em 2018, o Itaú iniciou o uso de RPA na carteira de crédito imobiliário, por ser um processo que envolve grande quantidade de documentos. Assim, trouxe mais agilidade e controle aos atendimentos prestados; e direcionou o tempo de trabalho dos empregados, economizado pela robotização, para oferta produtos (*cross sell*) (SANTOS, 2018). Também em 2018, o Bradesco® declarava que suas inciativas em RPA extrapolavam a área de TI e envolviam, além dos negócios, o redesenho de processos (FINANTECH, 2018). A instituição utiliza ferramentas da Automation Anywhere® (FERRAZ, 2019). Ainda nesse ano, o Santander® fez uma parceria com a Automation Anywhere® visando colocar a RPA como componente principal de sua estratégia de negócios com o consumidor

(AUTOMATION ANYWHERE, 2019). Em função disso, o Santander Brasil®, em maio de 2019, contratou 400 especialistas em TI, sendo uma das principais posições a de arquiteto de BPM/RPA (PATI, 2019). Já em agosto de 2019, o Banco Safra divulgou a contratação de desenvolvedor de automação para programação de RPA em .NET e Selenium®; e para realizar pesquisas com Uipath® e Cypress®, entre outras atribuições (CECCHI, 2019).

4.3. Auditoria Interna em Bancos Brasileiros

Segundo ALLES et al. (2009):

> A indústria bancária brasileira é mais avançada do que na maioria dos países emergentes…Esses bancos utilizam-se de sistemas de TI de grande porte e seu pessoal está capacitado para entender e implementar novas tecnologias como a auditoria contínua.

Contudo, em pesquisa realizada na internet sobre as auditorias internas dos cinco maiores bancos brasileiros - Banco do Brasil®, Itaú-Unibanco®, Bradesco®, Caixa Econômica Federal® e Santander® (MARTELLO, 2019), foi constatada a divulgação dos documentos que legalmente devem ser disponibilizados ao público em geral, como regimento interno e pareceres em relatórios sobre gestão de risco, controles internos*, compliance* e governança. Não foi verificada qualquer menção sobre a metodologia de trabalho desses órgãos ou pesquisas acadêmicas sobre o tema nessas instituições, provavelmente por questões de sigilo, excesso de zelo e/ou conservadorismo. À exceção do uso de auditoria contínua nas duas primeiras, cujo teor, resumimos a seguir. Além disso, em nenhuma não foi evidenciado o uso de RPA como proposto nesse estudo.

4.3.1. Auditoria Interna do Banco do Brasil

Em 2010, a Auditoria Interna do Banco do Brasil® iniciou, gradativamente, o emprego da auditoria contínua em seus trabalhos e, assim, vem ampliando sua eficiência na avaliação dos processos corporativos com foco em riscos. Um exemplo do uso dessa técnica é o desenvolvimento do Painel de Auditoria Contínua – Agências (AUDITORIA INTERNA DO BANCO DO BRASIL, 2015), reproduzido na Figura 17.

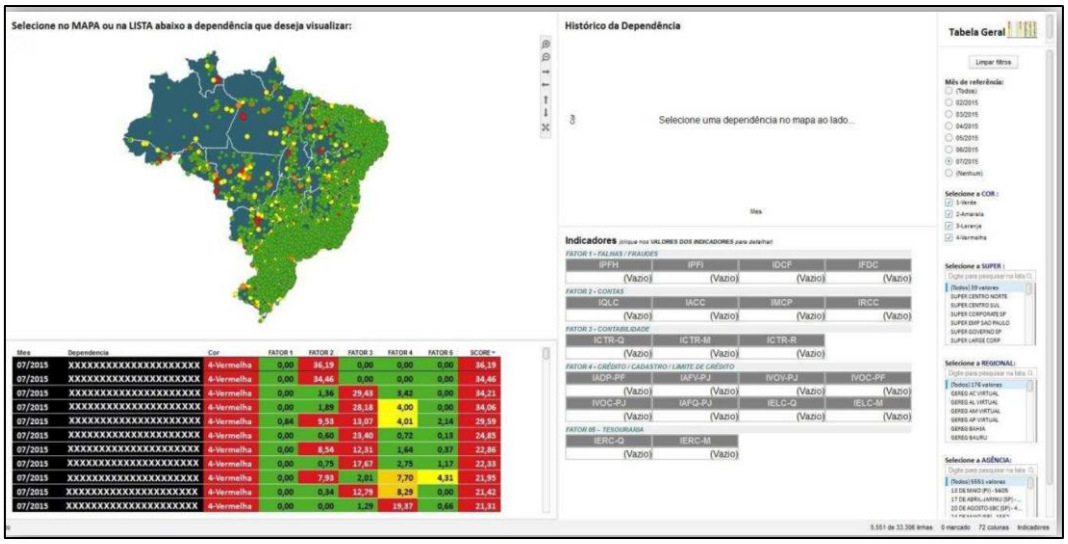

Figura 17 - Painel de Auditoria Contínua – Agências do Banco do Brasil
Fonte: AUDITORIA INTERNA DO BANCO DO BRASIL. **III Concurso de Boas Práticas da CGU**. 2015

Ele permite o monitoramento remoto e de forma comparativa do risco operacional em agências da rede do Banco do Brasil®, por meio de indicadores capazes de sinalizar comportamentos sugestivos de anomalias. O somatório dos desvios, observados em cada um dos indicadores utilizados, possibilita a classificação das agências em escala cromática (verde, amarela, laranja ou vermelha), como demonstrado na Figura 18, de forma a apontar o nível de desvio no comportamento de cada unidade em relação às demais agências do seu agrupamento (*cluster*).

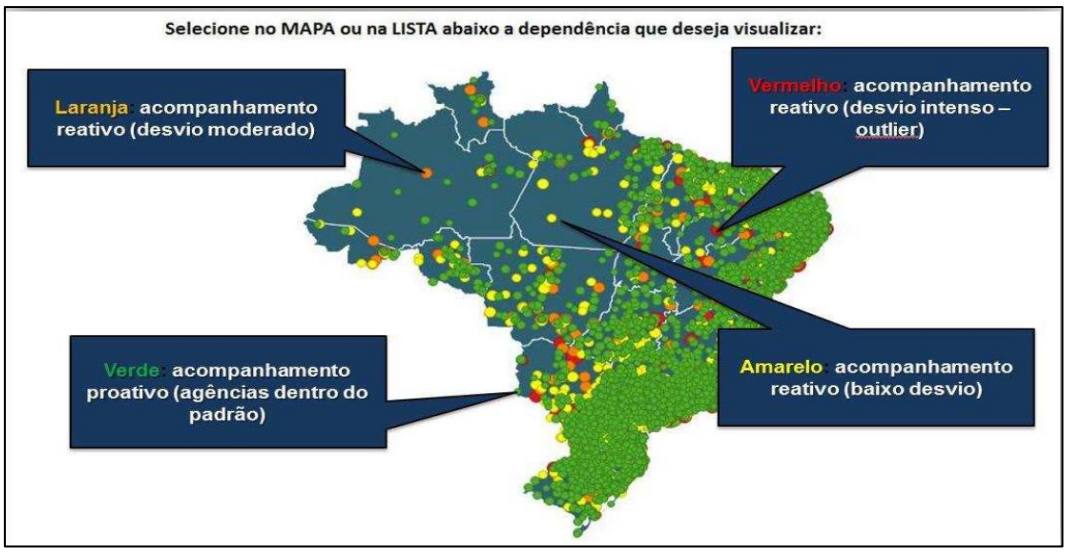

Figura 18 - Escala cromática Painel de Auditoria Contínua – Banco do Brasil
Fonte: AUDITORIA INTERNA DO BANCO DO BRASIL. **III Concurso de Boas Práticas da CGU**. 2015

Todas as etapas da construção do Painel de Auditoria Contínua – Agências, assim como, sua atualização e manutenção, foram realizadas diretamente pela auditoria interna do Banco do Brasil®, desde a elaboração do modelo de agrupamento de agências (*cluster*) e a concepção dos indicadores de auditoria contínua, até o desenvolvimento da ferramenta, disponibilizada para toda a rede de gerências de auditoria espalhadas pelo Brasil.

A utilização de ferramentas especializadas em extração, tratamento e análise de dados, como o SAS® e o Spotfire®, diminuiu a complexidade de implementação da solução e trouxe celeridade e baixo custo, pois não concorreu com demandas voltadas para o negócio principal da empresa; não onerou a área de TI da instituição; e não precisou da instalação de infraestrutura local para aplicação, uma vez que as informações estão disponíveis em ambiente *web* mediante concessão de acesso.

O uso de indicadores, como detalhado na Figura 19, permite que a auditoria tenha uma atuação mais ampla, abrangente e assertiva. Bem como, que haja o direcionamento de recursos para avaliações de situações com maior potencial de exposição ao risco. Ademais, abrange todo o universo de ocorrências e possibilita a escolha, baseada em modelo científico, dos elementos amostrais com indicativo de desvio para uma análise mais detalhada.

Figura 19 - Detalhes de Indicador do Painel de Auditoria Contínua – Banco do Brasil
Fonte: AUDITORIA INTERNA DO BANCO DO BRASIL. **III Concurso de Boas Práticas da CGU**. 2015

Em função disso, há a diminuição dos deslocamentos dos auditores para trabalhos em loco, com consequente redução dos custos; e a geração de

subsídios para avaliação, no segmento estratégico, dos processos corporativos da empresa.

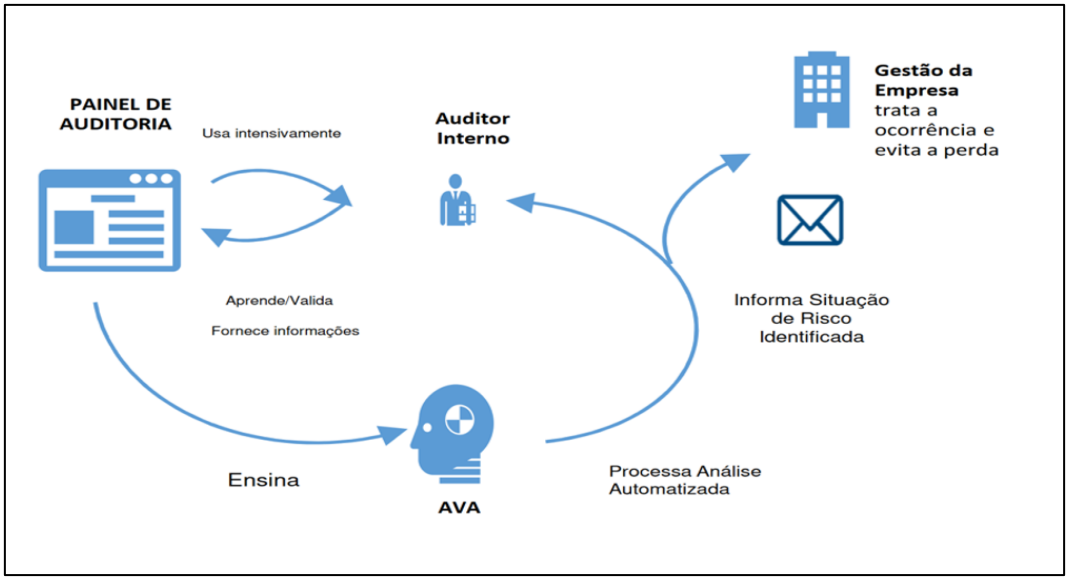

Figura 20 - Fluxo dos Assistentes Virtuais de Auditoria do Banco do Brasil
Fonte: AUDITORIA INTERNA DO BANCO DO BRASIL. **Relatório Anual de Atividades de Auditoria Interna 2018**. 2019

Seguindo no processo de evolução da auditoria contínua, em 2018, foram desenvolvidas ferramentas, denominadas Assistentes Virtuais de Auditoria – AVA, utilizando *Robotic Process Automation* – RPA (AUDITORIA INTERNA DO BANCO DO BRASIL, 2019), que visam identificar, de forma preventiva e ininterrupta, situações ou operações que não estejam em conformidade com as normas e padrões admitidos pelo banco, cujo fluxo é representado na Figura 20.

4.3.2. Auditoria Interna do Itau-Unibanco

Em 2008, o Itau-Unibanco® estabeleceu uma parceria com a *Rutgers University* para o desenvolvimento de projetos abordando várias técnicas de análise de dados como *clustering*, correlações, sumarização de dados, análise lógica e sequencial e técnicas de visualização. Em função disso, em 2009, foi criada a Gerência de Auditoria Contínua, que vem evoluindo desde então, como mostrado na Figura 21. A capacitação em estatística e em análise e interpretação de dados, foi sendo aprimorada por meio de treinamentos com o Professor Miklos Vasarhelyi e pela realização de cursos em ACL® e SAS®. Destarte, em 2014, houve a revisão do dashboard com o cancelamento de 64 indicadores, inclusão de 78 e manutenção de 7.

Figura 21 - Timeline Auditoria Eletrônica e Contínua do Itau-Unibanco
Fonte ITAU-UNIBANCO**. Auditoria Eletrônica**: Automatização de procedimentos de auditoria através do uso de ferramentas de análise de dados. 12th CONTECSI 34th WCARS.mai.2015

A instituição distingue as atividades realizadas como auditoria eletrônica e as como auditoria contínua, salientando que a primeira se refere a automatização de procedimentos de auditoria por meio de ferramentas de análise de dados (CAATS); e, a segunda, a avaliação de risco de forma perene, por meio de uso de indicadores ou técnicas de monitoramento. Na visão da empresa, os objetivos e benefícios da Auditoria Eletrônica e Contínua são aumentar a abrangência dos testes, o "*timing*" das análises e a eficiência na execução dos testes; identificar novos riscos por meio da análise de dados; e permitir o acesso rápido a dados confiáveis e íntegros.

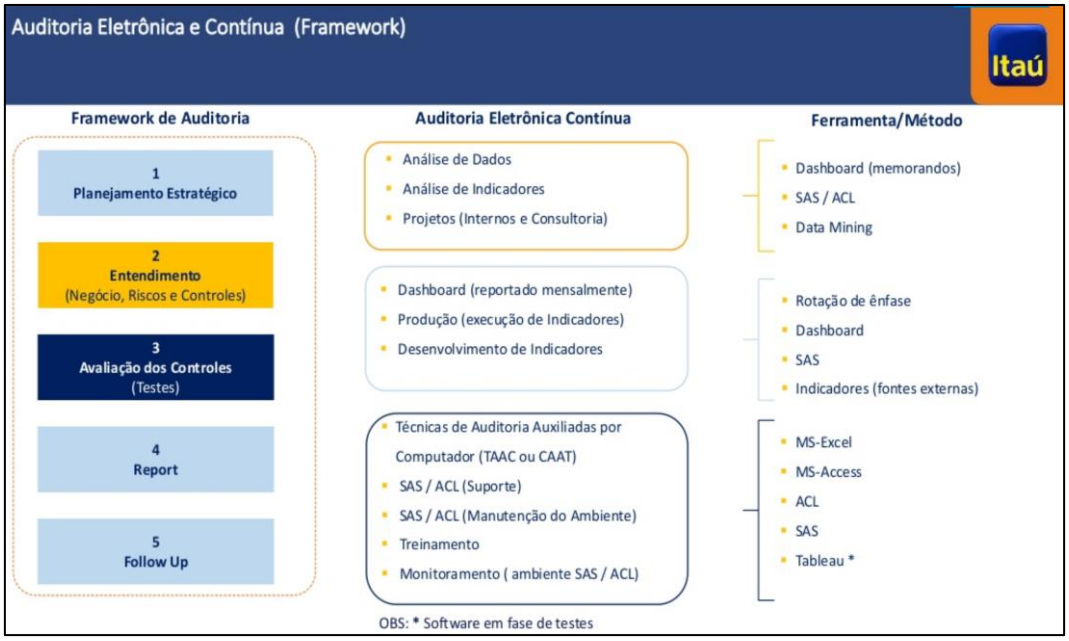

Figura 22 - Framework Auditoria Interna do Itau-Unibanco
Fonte ITAU-UNIBANCO. Auditoria Eletrônica: Automatização de procedimentos de auditoria através do uso de ferramentas de análise de dados. 12th CONTECSI

Nesse sentido, o framework da auditoria interna do Itau-Unibanco®, apresentado na Figura 22, demonstra a integração da auditoria eletrônica e contínua, com as ferramentas utilizadas e as atividades realizadas, ao planejamento estratégico integrado da unidade. Essa estrutura permite a atualização da visão dos riscos em relação às mudanças no ambiente de controle. Além disso, viabiliza o alinhamento entre a segunda e a terceira linha de defesa; e facilita a sinergia entre as diversas estruturas de monitoramento da empresa.

O trabalho da auditoria eletrônica e contínua é feito por uma equipe, formada por desenvolvedores e analistas de dados, com foco na criação de indicadores e CAATS complexas, por meio do uso de ferramentas como ACL®, SAS® e Tableau® (Figura 23). O monitoramento contínuo é priorizado, pois visa à identificação: de *outliers*; da integridade dos dados; e de não conformidades, em relação às políticas, normativos, resoluções e leis. Nele, a elaboração das CAATs e o suporte são descentralizados. Além disso, o setor presta treinamento e apoio à análise de dados aos demais departamentos da organização.

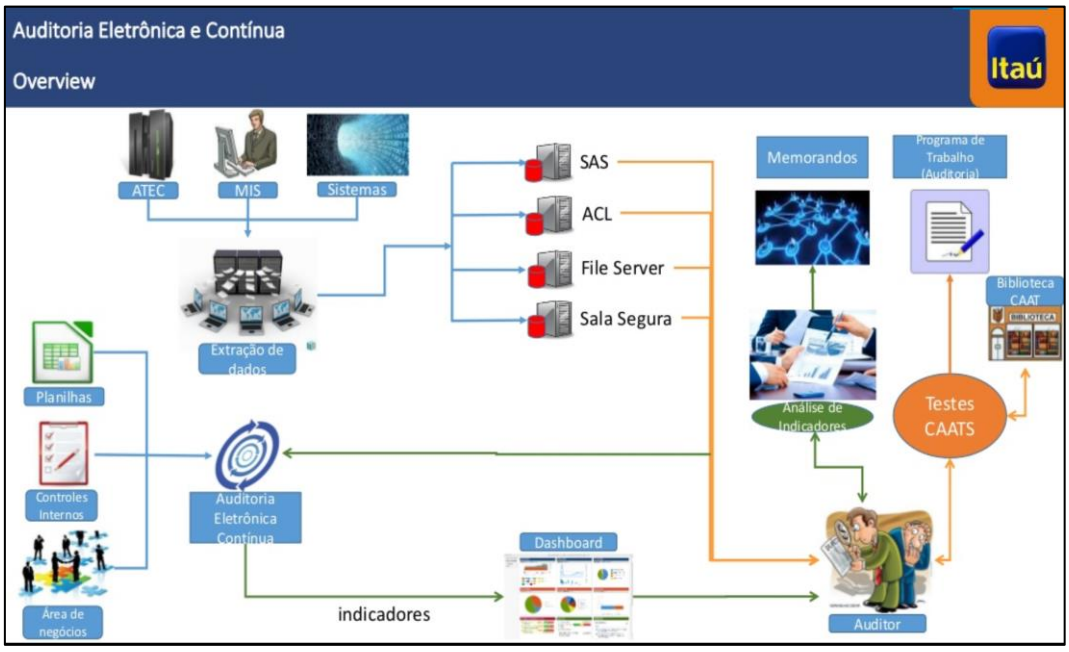

Figura 23 - Overview da Auditoria Eletrônica e Contínua do Itaú-Unibanco
Fonte: ITAU-UNIBANCO. **Cenário atual da Auditoria Contínua em Bancos no Brasil**. 12th CONTECSI 34th WCARS.mai.2015

Dessa forma, o Itaú-Unibanco® almeja obter análises ainda mais profundas e assertivas, em tempo real, para a identificação automática de exceções, tendências e correlações. Assim, o esforço do auditor fica concentrado na análise desses casos. Em função disso, os principais desafios, segundo a instituição, para o avanço nessa área são:

a) a obtenção de dados de forma rápida e com conteúdo fidedigno (preferencialmente nessa ordem) da área de tecnologia, de relatórios sistêmicos ou dos departamentos de MIS - DW[24], com validação prévia dos dados para esse último;
b) o custo de replicação das bases e a manutenção de sua segurança física e lógica;
c) a integração dos métodos de utilização dos dados; e
d) a mudança do "*mindset*" do auditor tradicional para um com as seguintes competências: excelente pensamento crítico-analítico, grande poder de persuasão, personalidade inquisitiva e mentalidade globalizada.

4.3.3. Perspectivas para Auditoria Interna

Em 2016, na reunião da Rede Europeia de Lideranças de Comitês de Auditoria (EUROPEAN AUDIT COMMITTEE LEADERSHIP NETWORK, 2017) foi discutido o impacto da transformação digital na função de auditoria interna. Três assuntos se destacaram: seu efeito em relação ao gerenciamento de riscos e controles internos, no novo cenário de negócios; como as tecnologias digitais fortalecem e desafiam a auditoria interna; e a preocupação dos CAEs com a inovação e o *assurance*.

Foi evidenciado que será necessário rever o framework de gestão de risco e de controles internos, visando avaliar, proativamente, os pontos de verificação que surgiram (e surgirão) nos processos organizacionais dentro desse novo cenário. Além disso, foi observado que as tecnologias digitais, como a RPA e a análises avançada de dados, estão ajudando a auditoria interna a melhorar seu desempenho. Pois, permitem uma economia significativa de custos na execução de tarefas rotineiras. Além disso, deixam que os auditores se concentrem nas tarefas que requerem julgamento humano.

Mas, foi destacado que, para alcançar esses benefícios, seria necessário o desenvolvimento de novas habilidades e competências. Como também, a adoção de abordagens mais flexíveis para o planejamento da auditoria. Já os CAEs expressaram sua apreensão quanto ao impacto dessas novas tecnologias nas três linhas de defesa, posto que podem causar o sombreamento de responsabilidades. Além disso, destacaram que a colaboração entre as linhas é importante, mas a independência e a objetividade da auditoria interna devem ser mantidas.

[24] MSI - DW = *Management Information System – Data warehouse.* Sistema de informações gerencias de uma organização armazenado num banco de dados consolidado.

5
Análise & Proposta

5.1.
Framework para o uso de RPA na Auditoria Contínua

A principal vantagem do uso da RPA, na auditoria interna, é a consequente disponibilização de tempo para os auditores tratarem de análises que necessitem de seu julgamento e expertise, devido à redução do trabalho empreendido em processos altamente repetitivos.

Outros benefícios são a confiabilidade; as trilhas de auditoria perfeitas; o baixo custo de implementação; e o aprimoramento na segurança e na qualidade do processo, em função da ausência de interação humana (MCCLIMANS, 2016). Uma pesquisa recente nas principais empresas de contabilidade mostra que a precisão da RPA atinge 99,9%, enquanto a humana, 90% (COOPER et al., 2019).

Ademais, o custo de funcionamento de um *software* de RPA é cerca de onze vezes menor do que o de empregar um ser humano. E, esses "robôs" podem funcionar 24 horas por dia, 7 dias por semana (BURGESS, 2016). Além disso, oferecem flexibilidade e escalabilidade, pois executam vários tipos de processos e podem ser reatribuídos a outros.

Apesar disso, o uso da RPA, na prática de auditoria, ainda é tímida, dado ao conservadorismo da profissão e aos riscos de sua implementação. Pois, a configuração de um ecossistema automatizado e controlado para o uso da RPA envolve fatores que vão além da simples programação do fluxo de trabalho num *software*. Tampouco requer automatizar freneticamente todos as atividades "robotizáveis". É primordial, antes, rever todas as tarefas que compõem o processo e seu fluxo, identificando seus dados, documentos, sistemas, interações e estruturas. Depois, analisar como pode ser melhorado, inclusive considerando o uso de novas tecnologias (LOWERS et al., 2016). Ou seja, verificar se o processo realmente é passível de automação do jeito que é hoje; senão, se deve ser automatizado, após ser remodelado; ou, se deve ser subtituido por outro / extinto (HAMMER, 1990). Nesse momento, é primordial o uso de técnicas de *Design Thinking*[25].

Logo, a automação na auditoria deve ser realizada sistematicamente incorporando a reengenharia em seus processos manuais, não num sentido

[25] *Design Thinking* é um conjunto de técnicas para o desenvolvimento de ideias e insights utilizado na abordagem de problemas, aquisições de informações, análise de conhecimento e propostas de soluções.

estrito, mas numa abordagem adaptada às novas tecnologias e adotando uma metodologia que garanta o atingimento dos objetivos propostos nessas mudanças (ALLES, M.; KOGAN; VASARHELYI, 2008).

Nesse sentido, primeiramente, deve se ter em mente que a governança e a estratégia de TI são essenciais para essa empreitada (ACKERMAN, 2009). Então, é fundamental conhecer o universo de TI da organização. Esse, geralmente, é divido em:

1) Infraestrutura - controla o fluxo e o processamento de informações de toda empresa. Compreende servidores, roteadores, comunicações, *desktops*, etc;

2) Operações - faz a manutenção do sistema por meio de aplicativos de segurança e de recuperação de desastres; e dos planos e acordos de nível de serviço (*Service Level Agreement* - SLAs); e

3) Aplicativos - são os *softwares* usados para registrar e armazenar transações, como banco de dados; e as ferramentas de inteligência de negócios.

Adicionalmente, há três elementos-chave para maximizar os resultados oriundos das tecnologias digitais (ROSS et al., 2016) : definir uma estratégia com a proposta de valor que a integração, no caso da RPA na auditoria interna, pretende alcançar; uma estrutura operacional, que forneça recursos de excelência; e, uma de serviços digitais que permita a rápida resposta aos planos de ação.

Figura 24 - Principais *softwares* de RPA do mercado
Fonte: FORRESTER. **Forrester Wave Robotic Process Automation, Q2 2018**. Forrest Research. 2018.

Deve-se escolher, se os auditores de TI desenvolverão toda automação, ou se serão usados, no todo ou em parte, *softwares* de mercado, sejam eles pagos, gratuitos ou de código aberto, como por exemplo a finlandesa *Robot Framework*. Para isso, é necessário avaliar as características de cada produto para identificar aquele(s) que melhor atende(m) aos objetivos estabelecidos, principalmente quanto a custo, segurança, escalabilidade e curva de aprendizagem em sua programação e utilização. No relatório da *Forrester Wave*® de junho de 2018, foram identificadas 32 marcas de *softwares* para RPA (FORRESTER, 2018). As quinze com maior representatividade no mercado são apresentadas na Figura 24.

Adicionalmente, a escolha da ferramenta deve focar a capacidade, a eficiência e a eficácia de automação das atividades de auditoria. Na Tabela 2, há uma comparação entre as ferramentas de automação e os possíveis usos nas rotinas de auditoria. Nela, evidencia-se que, dependendo do trabalho a ser realizado, não haveria necessidade do uso de um *software* de RPA, pois uma ferramenta comum como o Excel®, ou um programa em python® ou R®, poderia fazê-lo. Portanto, é fundamental ter sempre isso em mente quando o assunto é automação.

Tabela 2 - Comparação entre ferramentas para automação em auditoria

Ferramenta	**Execução**	**Atividades de Auditoria**
Macros do Excel®	Funções baseadas em regras	Reconciliações
IDEA®	Cálculos	Análise de Procedimentos
		Testes de Controles Internos
		Testes de Atributos
python®	Funções baseadas em regras	Reconciliações
R®	Cálculos	Análise de Procedimentos
	Pesquisas na web	Teste de Controles Internos
Softwares de RPA	Importação de dados	Testes de Atributos
	Exportação de Dados	Levantamento de Dados
		Compilação dos resultados dos testes de auditoria

Adaptado de: MOFFITT, K. C.; ROZARIO, A. M.; VASARHELYI, M. A. **Robotic process automation for auditing.** Journal of Emerging Technologies in Accounting, [s.l.], v. 15, no 1, p. 4, 2018.

Um exemplo disso é o MVP para automação dos testes substantivos de um plano de benefícios dos funcionários de uma empresa de contabilidade, feito pela *Rutgers Continuous Audit and Reporting Laboratory* (CARLab), que basicamente

consistiu numa combinação do uso de SQL® (*Structured Query Language*) e uma RPA para coletar evidências de auditoria e executar os testes no Access® (COHEN; ROZARIO; CHANYUAN, 2019).

Mas, independentemente disso, para que a RPA seja escalável, é fundamental a realização do mapeamento dos domínios de informações nos sistemas legados visando à padronização nos dados, para não incorrer em problemas de interpretação entre fontes, objetos e seus respectivos rótulos, como proposto pela AICPA *Assurance Services Executive Committee Audit Data Standard* - ADS (AICPA, 2020).

Atendidos os pré-requisitos, inicia-se o plano de ação para a implementação da RPA, cujo framework está esquematizado na Figura 25. Esse deve garantir uma transição tranquila entre a auditoria repleta de atividades manuais para a essencialmente analítica (SEASONGOOD, 2017). Assim, deve-se avaliar, quais processos de auditoria podem ser automatizados, considerando que os procedimentos, que os compõem, precisam ser segmentados em etapas, tarefas e atividades repetitivas, volumosas, maduras, com regras de negócios específicas e dados estruturados – Modularização (ABDOLMOHAMMADI; USOFF, 2001). Nesse momento, é oportuno analisar se os dados, que não estiverem estruturados, podem ser digitizados. Isso requer o profundo conhecimento de cada um dos processos em verificação.

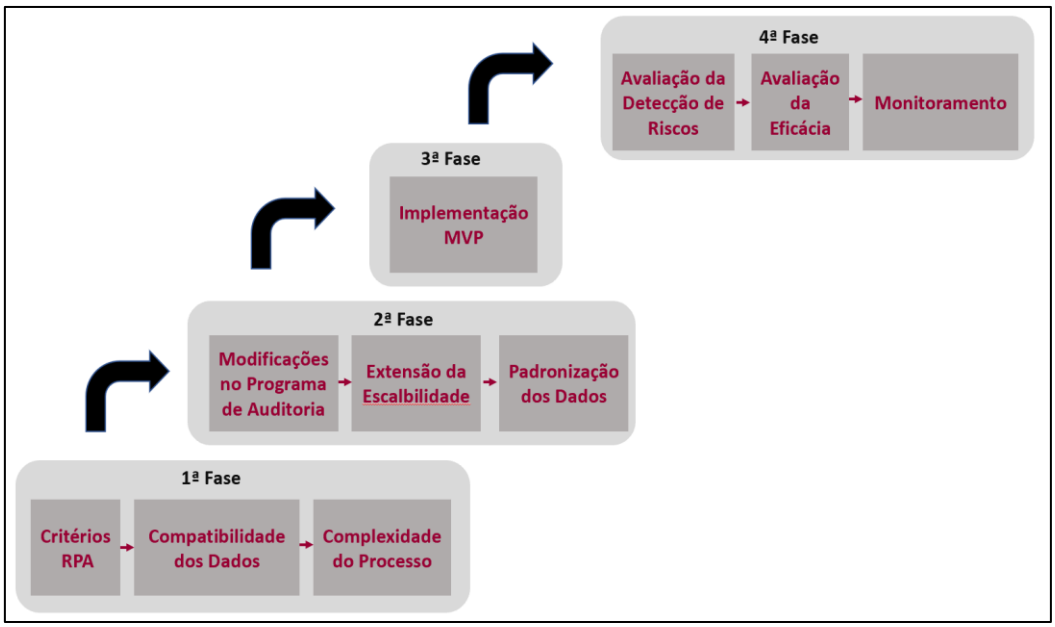

Figura 25 - Framework da implantação de uma RPA
Adaptado de: HUANG, F.; VASARHELYI, M. A. **Applying robotic process automation (RPA) in auditing**: A framework. International Journal of Accounting Information Systems, [s.l.], v. 35, p. 4, 2019.

E, ainda, apreciar os resultados e o valor agregado dessa automação. Pois, pode ocorrer do processo ser baseado em regras e, portanto, automatizável, mas, suas entradas podem não ser transformadas em conteúdo digital de maneira eficiente. Ou seja, o *software* comercial de RPA pode ser capaz de extrair e interpretar informações textuais de fontes não estruturadas como imagens, mas os dados podem ficar imprecisos (VINUTHA, 2017). Ou, a automatização do processo pode gerar altos níveis de sobrecarga que diminuiriam os benefícios obtidos.

Feita essa avaliação, seriam utilizados métodos ágeis, como SCRUM, em todo plano de ação. Assim, antes da RPA ser usada em trabalhos reais de auditoria, haveria um *Minimum Viable Product - MVP* visando aferir possíveis necessidades de refinamento e/ou inclusão ou modificação das regras existentes. Portanto, o processo de auditoria automatizado precisaria ser executado manualmente e de forma independente da RPA, para que haja a comparação dos resultados e a avaliação de sua eficácia e eficiência. Se for verificado que o programa precisa de ajustes ou melhorias, os feedbacks da prototipação, seriam incorporados ao projeto para a elaboração da prova de conceito (PoC), antes da implementação em processos mais complexos. Pois, mesmo depois de aprovado e funcionando, devem ser avaliados os casos em que a RPA realmente traria ganhos de escala (DELOITTE, 2018). O *roadmap* aqui descrito está representado na Figura 26:

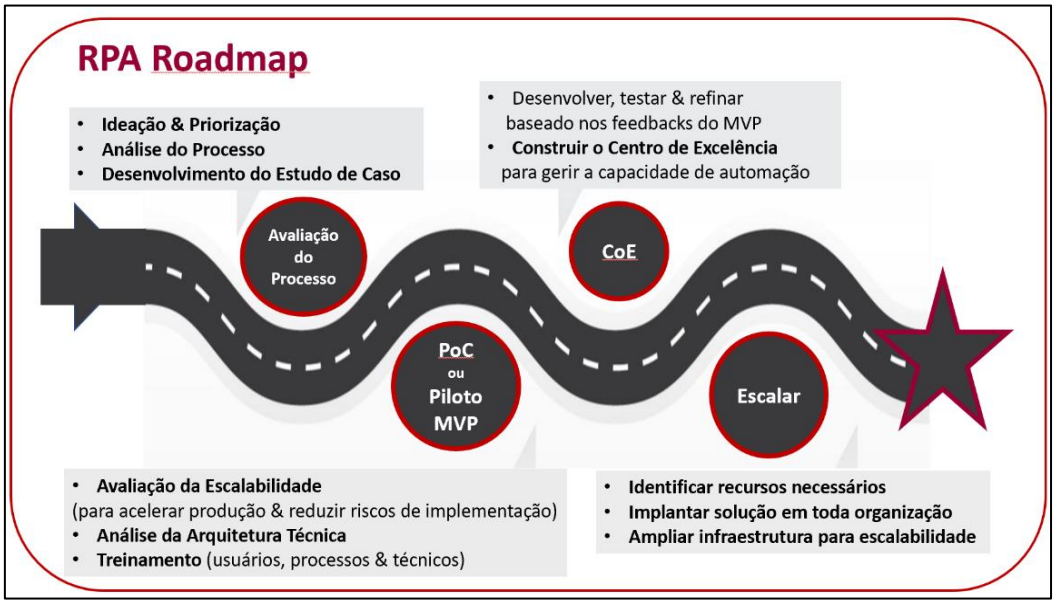

Figura 26 - RPA Roadmap
Adapatado de: DELOITTE. **The Path Forward : Operationalizing RPA to Automate the Digital Supply Network**. [s.l.]: [s.n.], 2018.

Destarte, as licenças dos *softwares* de RPA precisariam ser adquiridas para que os programas fossem desenvolvidos pela própria auditoria interna. Assim, o risco de implementação seria reduzido, haveria maior controle e as informações confidenciais estariam mais protegidas (LACITY; WILLCOCKS; CRAIG, 2015).

Consequentemente, haveria a capacitação dos auditores. Nos estudos sobre o tema, esse aspecto não foi considerado como uma preocupação, uma vez que foi relatado que a curva de aprendizado para utilização e codificação dos aplicativos mais populares, no nível de usuário, é rápida. De forma que, apenas os processos mais complexos requereriam programadores mais experientes (WILLCOCKS; HINDLE; LACITY, 2019).

Assim, as RPAs seriam monitoradas e administradas continuamente por meio de um painel de desempenho, como mostrado na Figura 27, que conteria informações sobre a precisão, como taxas de erro e exceções identificadas; e a eficiência dos programas, como tempo de processamento, de ociosidade e de manutenção (BHARADWAJ, 2019).

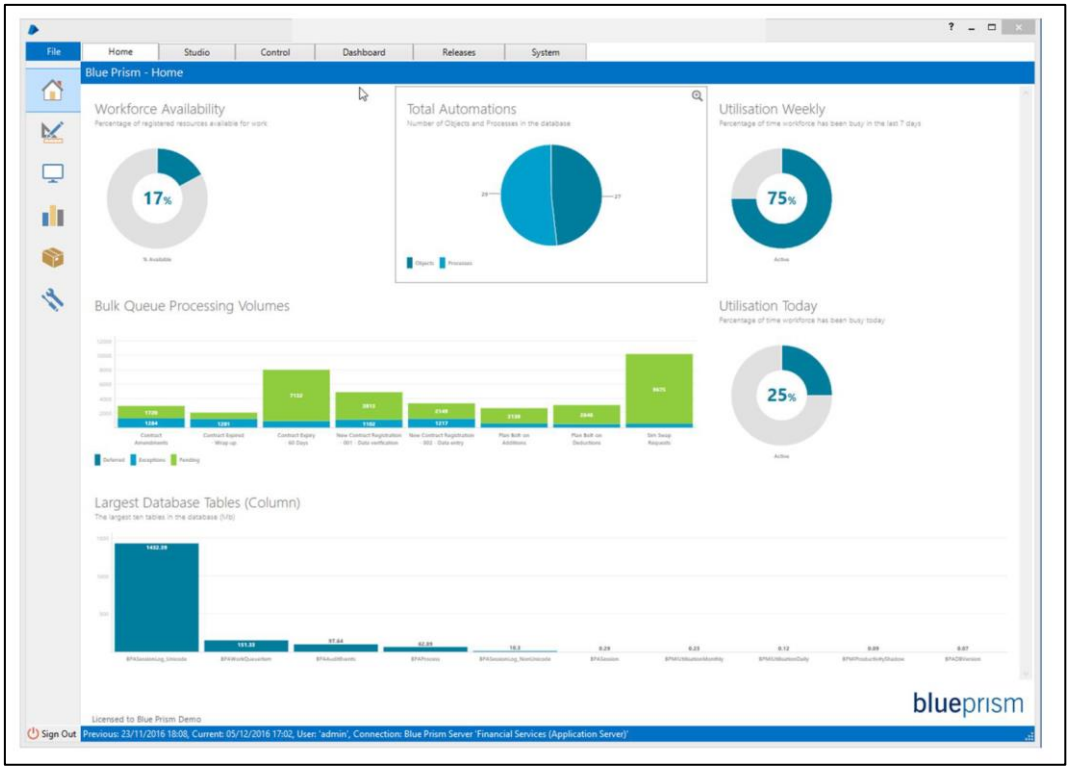

Figura 27 - Dashboard de Monitoramento de RPAs (Blueprism)
CHAPPELL, D. **Introducing Blue Prism Robotic Process Automation for the Enterprise**. [s.l.], p. 21, 2017.

Um dos indicadores chave de desempenho (KPI) usado para avaliar a implementação de RPA é o número de horas de trabalho humano reduzidas por mês devido a automação. Essa métrica pode suscitar questionamentos quanto a

adesão ao projeto, pois supostamente implicaria em desemprego. Apesar do discurso das empresas de *softwares* apregoarem que os robôs liberam os trabalhadores das tarefas tediosas e repetitivas para que executem atividades mais complexas e criativas, a partir do momento que a organização consegue se expandir sem contratar mais funcionários, esse risco existe (CHAPPELL, 2017). Ademais, a fusão da RPA com tecnologias cognitivas tende a aumentar as atividades que serão automatizadas. Portanto, é imprescindível clarificar e comunicar a política da organização sobre esse tema antes de iniciar o plano de ação para que haja engajamento no projeto.

Uma vez começado o plano de automação, deve-se avaliar os riscos inerentes a essa nova realidade. Se essa mudança ocorrer de forma descentralizada, os robôs podem não ficar sujeitos a padrões e/ou se tornarem muitos. A auditoria interna deve avaliar se há uma estrutura de governança sólida que verifique a adequação dos robôs aos padrões de desenvolvimento definidos pelo Centro de Excelência de RPA. Além disso, deve-se verificar se foram devidamente identificados os objetos, os riscos e os controles. Como também, se esses são eficazes. Deve-se ainda, determinar a periodicidade e a forma de supervisão dos robôs. Essas medidas evitam que haja a diminuição da eficácia de algum controle devido à automação de um processo; e o consequente aumento de seu risco. Adicionalmente, precisa-se avaliar, se a proliferação de robôs, não está tornando o ambiente tecnológico mais vulnerável e fragmentado, prejudicando os benefícios da RPA em relação aos custos e à segurança. Nesse sentido, a auditoria interna deve mapear cada processo automatizado, incluindo a qualidade e o ciclo de vida dos dados (ICAEW, 2019).

Mesmo havendo a prototipagem e a prova de conceito, pode haver erros num ambiente ativo. Devido a isso, rotinas de monitoramento e tratamento de erros devem ser incorporadas ao processamento para garantir que problemas e anomalias operacionais sejam detectadas antecipadamente e respondidas, sempre que possível, automaticamente. Ademais, a supervisão do painel de RPAs deve ser humana para evitar que, caso uma anomalia não seja detectada prontamente, não haja tempo para que cause danos ou que esses sejam minimizados (AI MULTIPLE, 2020).

Dependendo do risco, os robôs exigirão níveis variados de supervisão humana, podendo, inclusive, utilizar-se de métricas específicas. Assim, a auditoria interna deve testar, num cenário problemático, a eficácia dos alertas e dos interruptores do robô; analisar os registros de problemas e reclamações para avaliar se podem ser atribuídos ao seu desempenho; revisar se os indicadores de

risco (KRIs) existentes são suficientes para assegurar a eficiência e a eficácia da gestão de riscos de cada processo; avaliar a precisão dessas métricas; e fornecer novos *insights* e sugestões de melhoria sobre a operacionalização de cada processo (PWC, 2018).

Outro aspecto a cuidar são as atualizações necessárias das regras da RPA, devido, por exemplo, a mudanças no modelo de negócios, do ambiente operacional ou da legislação. Nesse caso, valem as medidas tomadas para sua implementação: avaliar se ainda é passível de automação; revisar todo o processo para verificar se basta alterar uma parte dele, ou se é melhor refazê-lo totalmente; e testar antes de colocá-la em uso. Pois, a simples alteração dos requisitos pode prejudicar sua eficácia e / ou incorrer em erros. Em função disso, a auditoria interna deve assegurar que haja um processo estruturado de gerenciamento de mudanças incluindo os responsáveis por essas atividades; os testes e as aprovações devidas; os logs de alterações, os *backups* de versões anteriores; e as notificações aos usuários impactados (ICAEW, 2019).

É importante destacar que o uso generalizado de robôs pode criar uma dependência que torne os processos vulneráveis, se esses ficarem desabilitados. E, nesse caso, pode não haver funcionários suficientes para operar os processos manualmente. Preventivamente, a auditoria interna deve revisar o Plano de Continuidade de Negócios para certificar-se de que há: procedimentos de *backup* das fontes de dados; definição de como as atividades serão retomadas; testes de capacidade do sistema conduzidos regularmente; e medidas para garantir que as áreas impactadas, a jusante, sejam notificadas da incapacidade do(s) robô(s). Outras possíveis vulnerabilidades são a privacidade, o vazamento de dados e os riscos cibernéticos. Portanto, é preciso garantir a precisão, a segurança e a integridade dos dados armazenados durante todo o seu ciclo de vida; e, que todos os riscos e aspectos relacionados à implementação e à utilização de RPAs identificados sejam devidamente tratados (SESHADRI; SHARMA, 2018).

Finalmente, cabe aprender com a experiência daqueles que já vivenciaram essa mudança, inclusive dos que falharam. Uma pesquisa da *Knowledge Capital Partners* (WILLCOCKS; HINDLE; LACITY, 2019), observou que cerca de 30% a 50% dos projetos de RPA não atingem os objetivos propostos. Nessa, foram identificados oito fatores críticos de sucesso: estratégia, recursos, seleção de ferramentas, estimativas de tempo do projeto, operações e execução, gerenciamento de mudanças, maturidade e participação das partes interessadas. Quanto a essa última, há o risco de um conflito potencial com o departamento de TI, quando a automatização é feita por representantes dos *softwares* adquiridos

ou por iniciativas isoladas dentro da organização, pois se tornam soluções não sancionadas ou não suportada pela TI. Essa ausência de integração é arriscada, porque muitas vezes é mal documentada e o conhecimento de como usar as ferramentas pode ser perdido à medida que os funcionários envolvidos no projeto de automação são transferidos. É recomendável que haja uma parceria entre a TI e os Centros de Excelência de RPA, permitindo inclusive, que aqueles participem ativamente dos projetos como consultores ou *dev team*. Além disso, é fundamental o engajamento e a liderança da Alta Administração, principalmente, nos estágios iniciais da automação.

Portanto, o desenvolvimento de um projeto de RPA é um processo extenso, que exige treinamento robusto dos funcionários, entradas estruturadas e governança. No entanto, uma vez configurados e implementados corretamente, esses robôs podem assumir o controle completo dos sistemas mediante o devido monitoramento. Resumidamente, as ameaças ao framework proposto para a RPA estão identificadas na Figura 28:

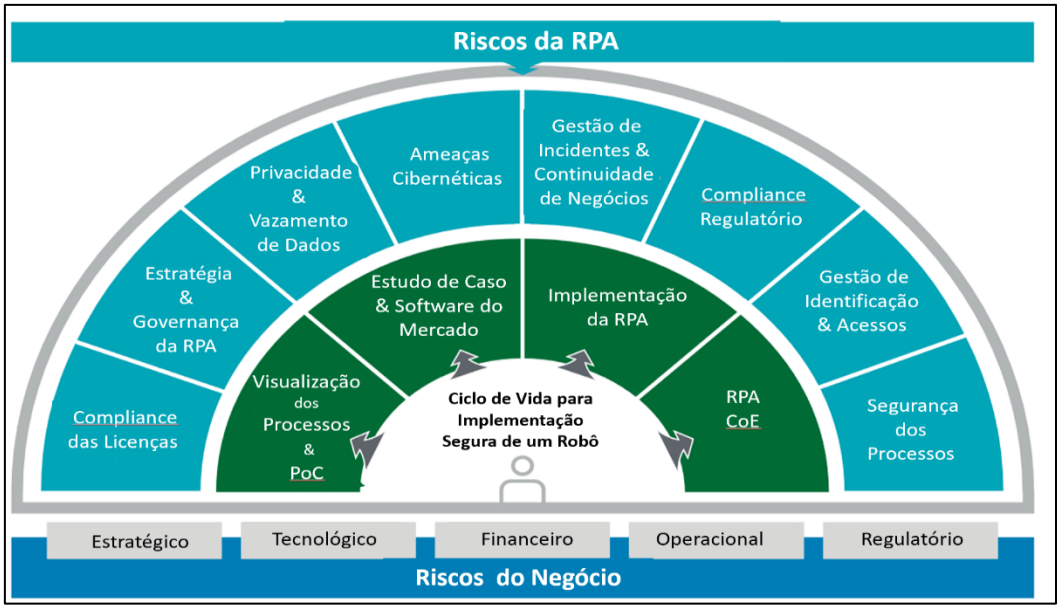

Figura 28 - Riscos para implementação de RPA
Adaptado de: SESHADRI, D.; SHARMA, A. **Auditing the RPA environment Our approach towards addressing risks in a BOT environment Risk Advisory**. [s.l.]: [s.n.], 2018.p.3

Apesar dos riscos descritos ao adotar a RPA, o risco de auditoria, a princípio, não sobre alteração, pois é função do risco inerente, do risco de controle e do risco de detecção (PCAOB, 2010). Como os riscos inerentes e de controle são determinados principalmente pela natureza dos negócios e pelo ambiente de controle, é pouco provável que sejam afetados pela automatização proposta nesse *framework*. Portanto, a auditoria precisa avaliar o efeito dos robôs no risco

de detecção, que é o risco dos procedimentos de auditoria não detectarem a anomalia, seja apontando falsos negativos ou não identificando as irregularidades, de forma que não haja um incremento nos riscos dos processos. Um exemplo disso é a norma AU-C 315.31 (AICPA, 2019), que determina que para alguns riscos, o auditor pode julgar que não é possível ou praticável obter evidência de auditoria apropriada e suficiente apenas a partir de testes substantivos. Tais riscos podem estar relacionados ao registro impreciso ou incompleto de transações rotineiras ou saldos contábeis, cujas características, geralmente, permitem processamento altamente automatizado com pouca ou nenhuma intervenção manual. Nesses casos, é relevante para a auditoria compreender o impacto desses riscos e os controles internos existentes. Logo, os auditores precisam ter convicção de que o *framework* está zelando pelo alcance de suas atribuições, o atingimento dos objetivos estratégicos e a perenidade da organização.

Uma representação gráfica do *framework* de RPA descrito para implementação na auditoria continua é apresentada na Figura 29 :

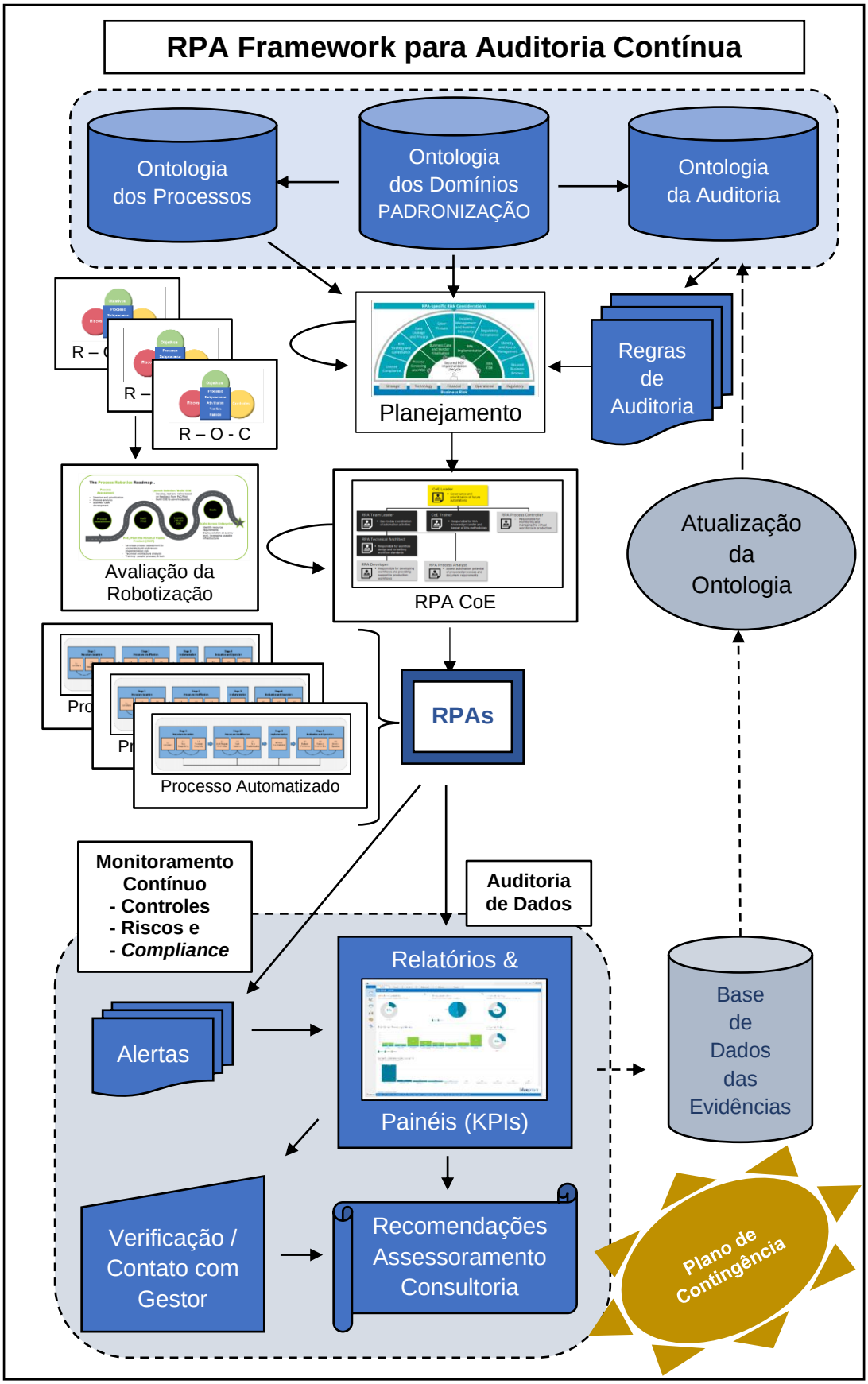

Figura 29 - RPA Framework para Auditoria Contínua
Fonte própria

5.2.
Modelo das Três Linhas de Defesa para implantação de RPA

A implantação da RPA pela auditoria interna, dificilmente seria uma iniciativa isolada dentro de uma organização. Geralmente, quando algum setor está dando os primeiros passos numa nova tecnologia, outros também estão iniciando sua jornada.

No caso específico da robotização, há relatos de sucesso e fracasso nessa empreitada em empresas de todos os setores. Logo, a experiência da Auditoria Interna poderia ser útil no assessoramento à Alta Administração, visando à escolha da melhor tática para seu uso em toda a empresa.

Todavia, cabe lembrar que os bancos já veem adotando a estratégia de integração para aumentar a UX, por meio do enriquecimento da experiência com o *mobile*. Apesar desta ser feita por meio de operações complexas, que geram altos custos. Isso ocorre porque, quando os sistemas legados foram criados, não foram projetados para integração.

Então, a RPA tornar-se-ia se uma alternativa valiosa a ser incluída nesse planejamento corporativo, uma vez que faria a interação entre os sistemas legados e as ferramentas das tecnologias emergentes e/ou dos sistemas que as suportam. Pois, sua instalação e operacionalização não altera os sistemas de TI existentes. Assim, as desvantagens da estratégia de incremento da UX seriam minimizadas, tornando a mais eficaz e eficiente; e deixando-a “Pronta para o Fututo”.

Mas, esse processo não deve ser feito sem um plano e uma metodologia. Uma forma eficiente de estruturar a implantação de robôs, como módulos de integração por toda a organização, é o modelo das três linhas de defesa, considerando-o sob um novo enfoque, como uma estratégia de “ataque” (MARKS, 2015). Com essa abordagem, seria possível alcançar o diferencial competitivo que traria melhores resultados à estratégia de UX.

Ou seja, a automação seria segregada entre os proprietários dos riscos - primeira linha; os supervisores dos riscos – segunda linha; e os avaliadores dos riscos – terceira linha. Então, nesse *framework*, cabe à auditoria interna, a avaliação objetiva e independente da gestão dos riscos, dos controles e da governança da organização, em relação à adoção da estratégia de RPA; e a comunicação e o acompanhamento das oportunidades de melhoria identificadas. As atribuições de cada linha, em relação a RPA, estão resumidas na Figura 30:

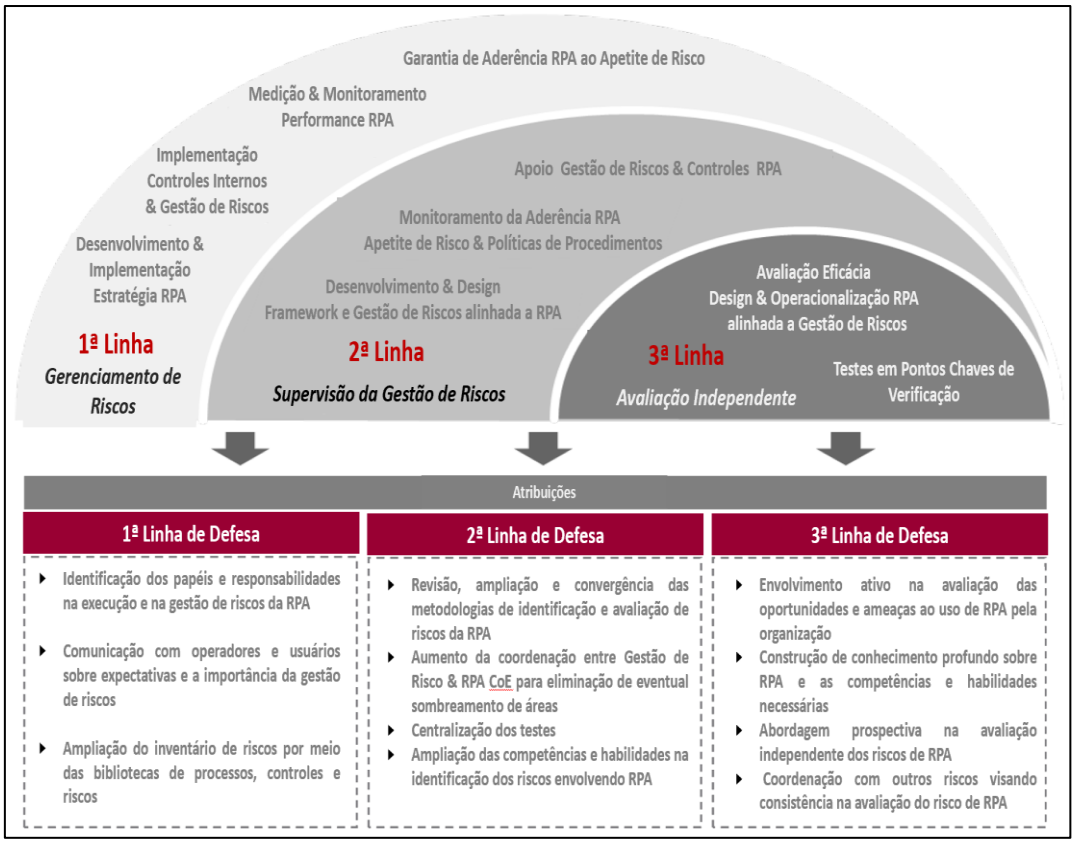

Figura 30 - Modelo das Três Linhas de Defesa para implantação de RPA
Adaptado de: DAMIANIDES, M. Robotics Process Automation (RPA) and Artificial Intelligence (AI): A New World Order. In: Ernst & Young Partner. Los Angeles: ISACA, 2018.

Em função disso, a auditoria interna deve compreender as oportunidades e riscos que envolvem a adoção de RPAs numa empresa. Verificar como está sendo planejada sua implementação e desenvolvido o ecossistema que dará suporte a esse projeto. Se a automação será feita unicamente pela TI da organização, se utilizará algum tipo de consultoria ou serviço tercerizado, ou se adquirirá licenças de *softwares* de automação, ou, ainda, se adotará alguma combinação dessas opções. Necessita também focar na governança, na capacitação dos usuários e desenvolvedores, na comunicação do programa de automação, nas mudanças necessárias à criação de uma cultura de RPA e no Centro de Excelência. Ou seja, fazer o mapeamento desse novo "processo corporativo" identificando e avaliando objetos, riscos, controles, pontos de verificação, responsáveis, alçadas, segregação, matriz de criticidade, competências, suporte e plano de contigência. Pois, precisa considerar o efeito da robotização nos processos; nos controles; e na confiabilidade e na precisão dos dados. Como ainda, seu impacto na disponibilidade e na coleta de evidências de auditoria para as análises. Um exemplo de matriz de responsabilidade para avaliação do ambiente de controle, considerando as linhas de defesa, está esquemetizado na Figura 31:

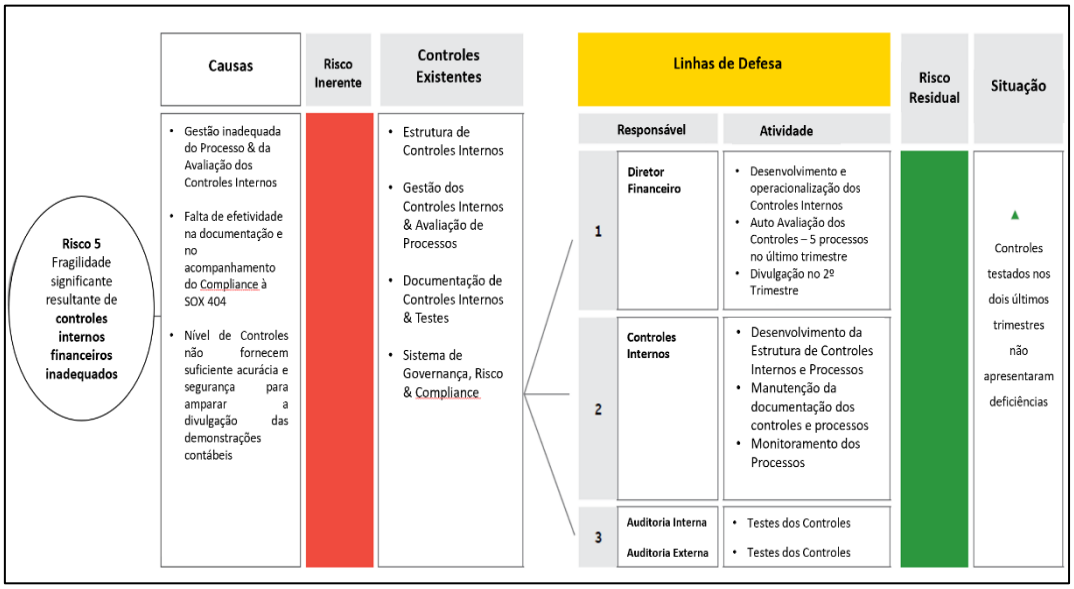

Figura 31 - Matriz de Responsabilidade e Avaliação de Controle
Adpatado de ERNST & YOUNG GLOBAL LIMITED. **Maximizing value from your lines of defense**. A pragmatic approach to establishing and optimizing your LOD model. [s.l.]: [s.n.], 2013

É importante frisar que a adoção da RPA, na auditoria interna, não se restringe a automação de testes para verificação da eficiência dos controles internos. Outras principais utilizações são: o rastreamento e o monitoramento dos principais indicadores de risco (KRIs); a criação de relatórios e painéis automatizados; e a modelagem de *scorecards* (PWC 2017). Como também, a avaliação da qualidade das informações usadas pela organização em reportes e dashboards, em relação a base de dados; e a avaliação da governança, por meio da verificação dos arquivos de *log*, das validações nos sistemas e dos acessos e concessões desses (GOTTHARDT et al., 2019).

Independentemente do tipo de trabalho realizado, há, inicialmente, um planejamento, que requer diversas tarefas tecnocráticas. Então, poderia desenvolver, por exemplo em python®, as regras que regem essas atividades e análises. Depois, configurar a RPA para executá-la. E apresentar os resultados aos auditores para suas contribuições (que são as mais relevantes). Um protótipo dessa automação, em estudo na *Rutgers University*, realizou a parte repetitiva do processo de planejamento, que pode levar mais de um dia, em cerca de 3 minutos (CALABRESE et al., 2020).

Um exemplo de robôs, que poderiam ser usados pela terceira linha de defesa, seriam módulos de monitoramento, baseados nos testes de auditoria, que corroborariam inclusive com a detecção de fragilidades; e o acompanhamento e a certificação de recomendações, cujo fluxo é reproduzido na Figura 32:

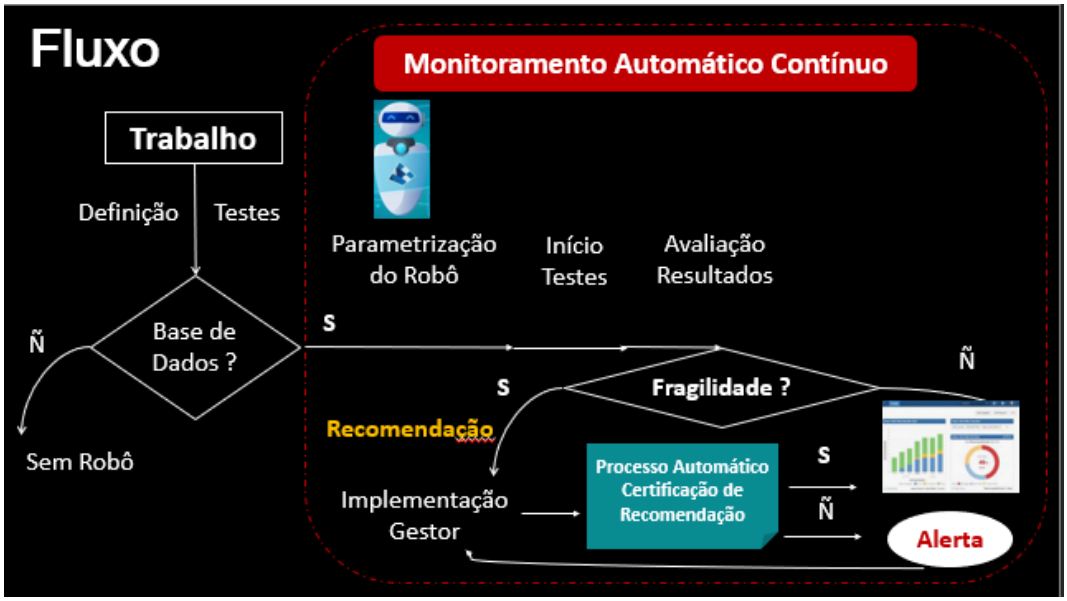

Figura 32 - Fluxo Automação Monitoramento Contínuo e Certificação de Recomendação
Fonte própria

Já a segunda linha de defesa, deve avaliar se os riscos provenientes de cada tipo de robô implementado e do ecossistema de TI, que os suportam, estão alinhados com o apetitie de risco estabelecido pala Alta Administração da organização, de forma a determinar se os riscos foram mitigados. É importante detectar, também, se surgiu algum novo risco com a implementação da RPA, além daqueles inerentes a sua criação, manutenção e revisão. Adicionalmente, deve monitorar a aderência dos negócios, nesse sistema automatizado, às políticas e aos procedimentos estabelecidos na estrutura de riscos e implementar medidas mitigantes.

Precisaria ainda compreender as implicações da automação em relação aos reguladores, que no caso do sistema bancário são muitos. Principalmente, atentar para a Lei Geral de Proteção de Dados Pessoais – LGPD. E, caso a instiuição tenha escritórios ou filiais na Europa e nos Estados Unidos, precisa considerar a *General Data Protection Regulation* – GDPR e a California *Consumer Privacy Act* – CCPA, respectivamente. Além disso, é necessário desenvolver habilidades, competências e técnicas para capacitar os funcionários à supervisão de um ambiente automatizado (ANDRIOLE, 2018).

Para isso, a TI precisa estabelecer uma estrutura de governança com funções e responsabilidades para a segurança das RPAs, configurando seu CoE e o modelo operacional que será adotado. E, em conjunto com o CoE, deve estabelecer as políticas e os controles, criando uma estratégia e os requisitos de segurança. Além de alinhar essa governança com as demais áreas da

organização de forma a estabelecer protocolos para o gerenciamento das RPAs com as atividades (como por exemplo ALM ou precificação de ativos) e com as funções corporativas (1ª, 2ª e 3ª linha de defesa). Assim, desenvolveria uma gestão de riscos baseada em RPAs e ampliaria a conscientização entre os desenvolvedores e usuários sobre os riscos da automação.

Considerando que é comum o uso de *softwares* de mercado, como Uipath®, Blueprism® ou Aumation Anywhere®, seria fundamental analisar o risco da arquitetura de segurança do produto selecionado em relação à criação, ao controle e á execução de robôs. Adicionalmente, deve-se identificar possíveis falhas da arquitetura de segurança nas conexões entre os vários ambientes, nas metodologias de virtualização e nas falhas de autorização. É essencial, também, garantir que o *design* seja seguro para a manipulação de informações confidenciais, incluindo a análise do fluxo de dados, para confirmar se os controles de segurança estão integrados à autenticação, à autorização e à entrada de validação dos robôs (credenciais de acesso). E, ainda, implementar varredura de segurança e testes de vulnerabilidade. Esse procedimento deve ser integrado ao processo de criação do robô por meio de testes dinâmicos ou de tecnologia de difusão (EY, 2018).

Uma vez estabelecida a governança e o *software*, resta determinar como seria feita a segurança em relação ao acesso dos desenvolvedores e dos usuários aos robôs. O gerenciamento de privilégios de acesso precisaria conter as segregações de tarefas. Nesse sentido, deve-se separá-las para minimizar a sobreposição de regras de segregação. Assim, a matriz de segurança autorizaria os robôs a executar apenas as tarefas que lhe forem atribuídas. Logo, seria essencial a centralização do gerenciamento criptografado das credenciais de acesso e seu uso frequente nas sessões das RPAs (ROBOTICSBIZ, 2019).

Para proteger essa estrutura, é fundamental o monitoramento do manuseio dos dados confidenciais, incluindo o processo de registro dos robôs e a avaliação da conformidade em relação às políticas de uso. É importante, também, verificar a integridade dos códigos por meio de testes de regressão robustos e avaliar o impacto da mudança na integração dos sistemas nas operações dos robôs. Adicionalmente, deve-se controlar as tarefas manuais sujeitas a erros para que não aumentem os riscos e/ou gerem não conformidades. Ademais, deve-se monitorar possíveis acessos inadequados ou desvios de regras de SoD[26], reunindo dados dos funcionários reponsáveis pelo uso e controle dos robôs, suas

[26] Segregation of Duties

trilhas de auditoria e atividades, principalmente os picos anormais. E, estabelecer a segurança da infraestrutura da pilha (*stack*) de forma a avaliar as vulnerabilidades da plataforma de automação por meio de exercícios de ameaça para identificar pontos fracos ou lacunas no processo (DAMIANIDES, 2018).

Considerando a operacionalização dos *softwares*, apesar dos robôs existirem na infraestrutura interna por trás de múltiplas camadas, firewalls baseados em rede, sistemas de detecção de intrusão, antimalware e servidores de log externos são controles de segurança padrão tão relevantes para a implantação de RPA quanto para qualquer outra infraestrutura (AUTOMATION ANYWHERE, 2018). O diagrama da Figura 33 mostra, de forma lógica, onde esses componentes são colocados na implantação da RPA. Além disso, os dados devem ser criptografados em repouso ou em trânsito, evitando "espionagem", "adulteração" ou "falsificação de mensagens". E, é preciso um banco de dados seguro, com criptografia reversível e chave armazenada separadamente, para os *login* usados nos robôs, de maneira que somente os funcionários autorizados possam recuperá-los. Aqui, cabe sopesar o uso de *hashing*[27] e salientar que Automation Anywhere® é a única ferramenta, atualmente, que possui essa opção. Outro recurso, é o mascaramento de dados para informações sensíveis. Assim, se o robô for invadido, o *hacker* não conseguirá roubá-las.

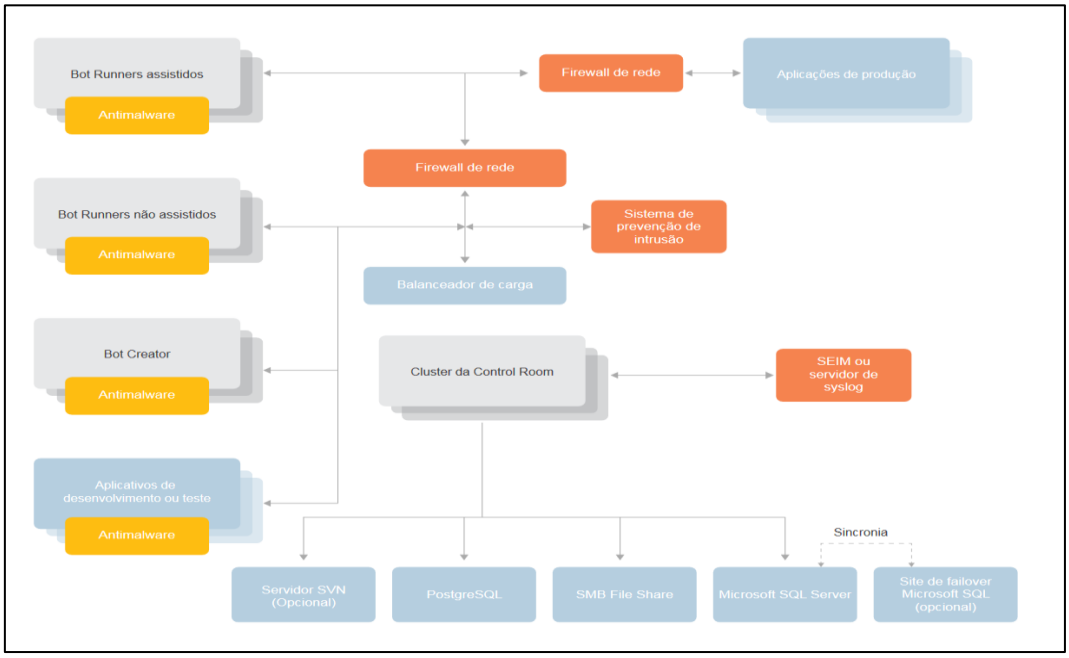

Figura 33 - Posicionamento de Firewalls para implantação de RPA
Fonte: AUTOMATION ANYWHERE. **Segurança de nível empresarial para Automação Robótica de Processos**. [s.l.]: [s.n.], 2018, p.9

[27] *Hash* é um algoritmo que mapeia dados grandes e de tamanho variável, resumindo-o em pequenos dados de comprimento fixo.

Um exemplo de RPA, que poderia ser usada pela segunda linha de defesa, seria uma que usasse uma macro em SAS®, baseada na Lei de Benford, para avaliar possíveis fraudes no uso de cartão de crédito; e, que apresentasse esses resultados num dashboard no Spotfire® (SMITH, 2018), como reproduzida na Figura 34:

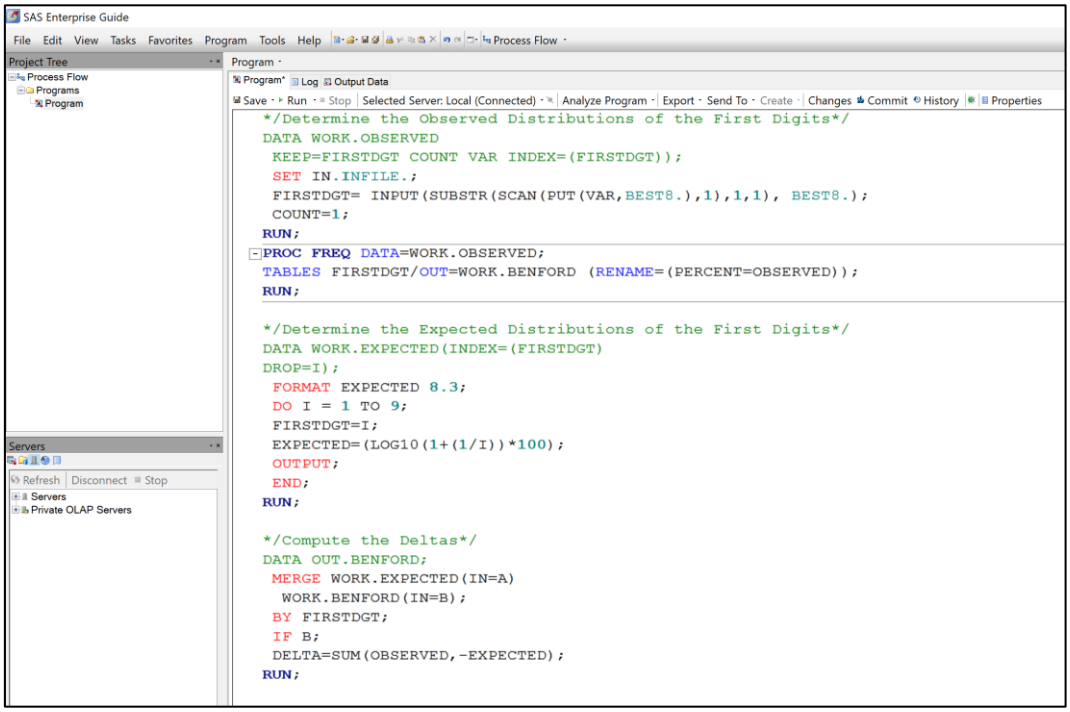

Figura 34 - Macro baseada na Lei de Benford
Fonte Própria

Enfim, a primeira linha de defesa, necessita compreender os riscos potenciais relacionados às alterações nos processos que serão alvo da RPA; estabelecer meios para educar e conscientizar os desenvolvedores e usuários dos benefícios dessa nova tecnologia; esclarecer os impactos dessas mudanças no negócio, como é conhecido atualmente (*Business as Usual* – BAU), e na cultura de *compliance* e gestão de riscos. Além disso, precisa verificar se os novos controles serão suficientes para acompanhar os fatores chaves de riscos e sua gestão; documentar os novos processos por meio de mapas; e verificar a efetividade do ambiente de controle (ERNST & YOUNG GLOBAL LIMITED, 2013).

O projeto de automação da organização deve ser planejado num Comitê, composto pelas áreas de negócios, para que decidam, juntamente com a TI, e conforme as políticas e os direcionadores do planejamento estratégico, os processos que serão priorizados.

A TI como responsável pelo gerenciamento, desenvolvimento e operacionalização do meio ambiente, precisa estabelecer a padronização dos dados e as metodologias que serão utilizadas. Ademais, deve verificar a melhor forma de integração entre *softwares* próprios ou adquiridos; a arquitetura e a infraestrutura; os peritos nos negócios e o CoE. De forma que, o *dev team* da RPA seja escolhido entre os membros do CoE, em função de suas competências, visando a maximização da proposta de valor esperada pelo gestor (*Product Owner*) com a automação do processo (BRACHIO, 2018). Uma estrutura para o Centro de Excelência de RPA é sugerida na Figura 35.

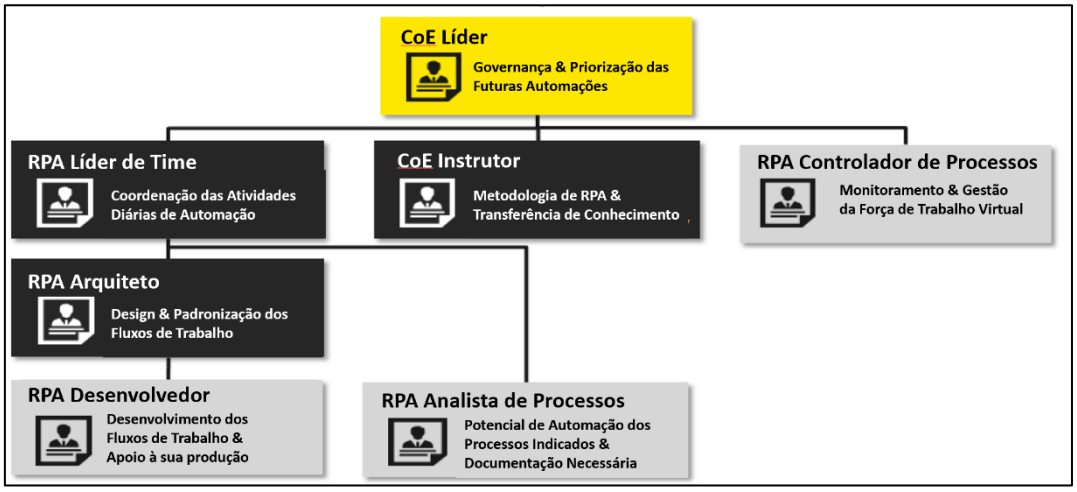

Figura 35 - Estrutura do Centro de Excelência de RPA
Adaptado de DAMIANIDES, M. **Robotics Process Automation (RPA) and Artificial Intelligence (AI): A New World Order**. In: *Ernst & Young Partner*. Los Angeles: ISACA, 2018.p.30

Todo esse processo precisa ser controlado por meio de um painel com dashboards para cada indicador de desempenho. Os KPIs mais comuns envolvem a produção de um robô ou grupos de RPAs por período (horas) trabalhado; a taxa de SLA[28], para avaliar o nível de serviço quanto a possíveis inoperâncias; a eficiência dos processos automatizados, medido pelo tempo economizado com a automação; os benefícios financeiros alcançados, que quantifica, principalmente, a diminuição com os custos de mão de obra; e de criação de RPAs pelos desenvolvedores, podendo ser ponderado por tipos e/ou complexidade.

Um exemplo de robô, que poderia ser usado pela primeira linha de defesa, para o gerenciamento do orçamento e/ou pagamento dos serviços prestados por terceiros a um banco, seria o de leitura de faturas utilizando o UiPath Studio®, como apresentado na Figura 36:

[28] SLA = *Service Level Agreement*

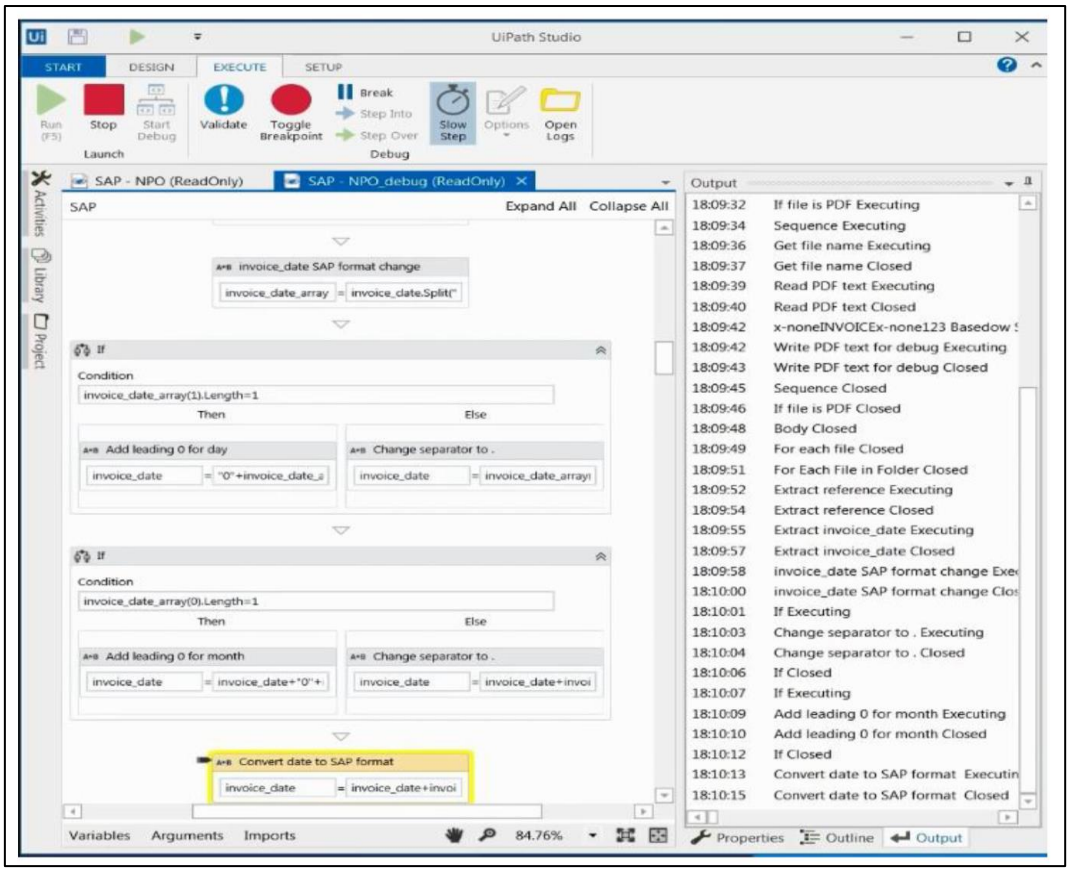

Figura 36 - RPA para extração e conversão de dados no UiPath Studio
Fonte: GOTTHARDT, M. et al. **CURRENT STATE AND CHALLENGES IN THE IMPLEMENTATION OF ROBOTIC PROCESS AUTOMATION AND ARTIFICIAL INTELLIGENCE IN ACCOUNTING AND AUDITING**. *Journal of Finance & Risk Perspectives*, [s.l.], v. 8, p. 31–46, 2019.

Considerando todo o exposto, o alinhamento estratégico entre o planejamento da organização e o da auditoiria, com o desenvolviemnto de RPAs por essa; a consultoria no planejamento de TI; e o assessormento na implantação do projeto de RPA integrado em toda a empresa, estão represeantodos na Figura 37.

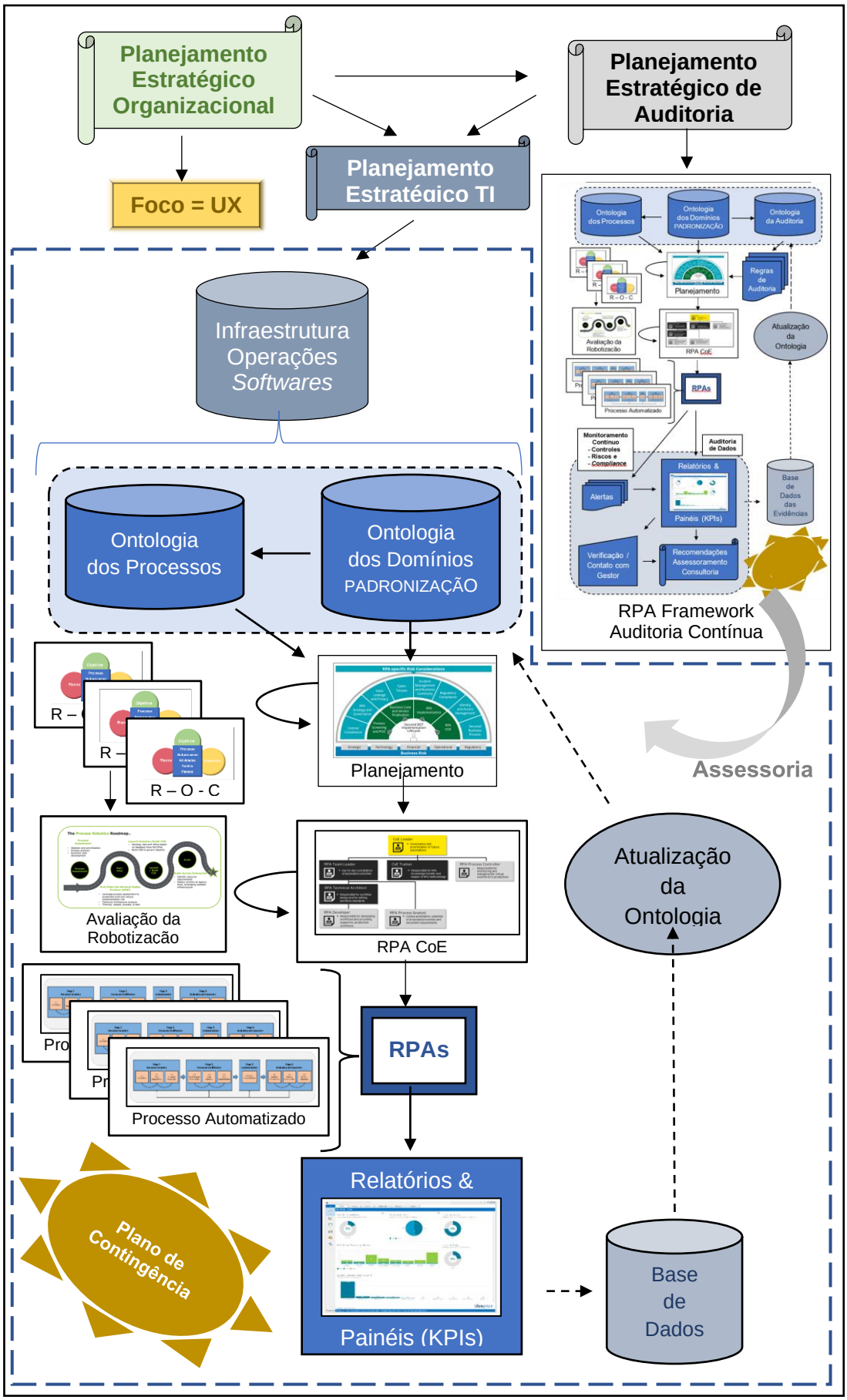

Figura 37 - Alinhamento entre Planejamentos & Programas de RPA
Fonte Própria

6
Conclusão

Com o advento da indústria 4.0, os mercados, o ambiente de negócios, a concorrência e as necessidades dos clientes vêm mudando rapidamente. Um dos segmentos que mais vem sendo afetado por essas mudanças é o financeiro. Para se defender da evasão de clientes para os novos entrantes, os bancos tradicionais, como Itaú, Banco do Brasil, Bradesco, Santander e Caixa Econômica Federal, têm investido em tecnologia; digitizado seus processos; e adotado ferramentas disruptivas. A estratégia escolhida para enfrentar a transformação digital é melhorar a experiência dos correntistas, principalmente no *mobile.* Ou seja, os bancos vêm optando pela integração (WEILL; WOERNER, 2018b), que implica no desenvolvimento de ambientes com *design* intuitivos e ágeis. Contudo, essa opção traz um custo muito alto e operações complexas, pois os sistemas legados, quando criados, não foram projetados para integração. Ademais, sendo a estratégia igual a todos, descaracteriza-se com tal e se torna um preceito. Logo, as instituições que não perceberem isso estarão míopes e fadadas a perdas significativas.

Então, onde estará o diferencial competitivo que agregará valor e permitirá o alcance das metas? Justamente em como é feita essa integração. Pois, a verdadeira estratégia digital deve almejar desenvolver um ambiente de negócios integrado, que forneça acessibilidade ampla e imediata às tecnologias SMACIT[29]; e que se adapte às constantes mudanças do segmento de atuação da organização (ROSS et al., 2016).

Além disso, as mudanças no ecossistema tecnológico e de processos nos bancos está acontecendo tão rápido que muitos riscos distintos dos usuais estão surgindo. Portanto, precisam ser identificados e mapeados, inclusive em função de alterações constantes nas legislações as quais os bancos são impostos. Esse cenário tem feito as organizações se preocuparem, ainda mais, com segurança e recorrerem à Auditoria Interna como meio de assegurar que a governança e o gerenciamento dos riscos e dos controles internos estejam condizentes com o apetite de risco estabelecido e que não prejudicarão o alcance dos objetivos estratégicos.

Logo, a evolução na atuação da auditoria interna depende que seus processos estejam altamente automatizados, com dados confiáveis, completos e

[29] social, mobile, analytic, cloud and internet of things.

precisos; e que os testes sejam realizados, continuamente, logo após a ocorrência dos eventos sob análise (auditoria contínua). Em função disso, é necessário criar e manter um *data warehouse* que sustente essas atividades e mantenha as informações dos relatórios de auditoria acessíveis e atualizadas, preferencialmente, em forma de painel. Como também, verificar se os controles internos são eficientes e eficazes. E, ainda, comunicar, eletronicamente, os resultados dos procedimentos de auditoria com as devidas evidências. De forma a entender rapidamente as causas de eventuais anomalias e erros, identificar sua origem e discutir ações corretivas em conjunto com o gestor do produto / serviço.

Embora a arquitetura do sistema e os componentes de *software* sejam extremamente importantes, a capacitação do auditor, o ambiente ético-cultural da empresa e o perfil da Alta Administração também são fundamentais para o êxito dessa mudança.

Considerando o exposto, as respostas aos questionamentos apresentados inicialmente nesse estudo estão sintetizadas nas recomendações a seguir.

6.1. Recomendações

Esse estudo evidenciou que, em função do fenômeno transformação digital e seus impactos no setor bancário nacional, a melhor abordagem para a Auditoria Interna é elaborar um Planejamento de Auditoria Interna estratégico, contínuo, integrado, baseado em riscos, alinhado com o planejamento estratégico da organização e ao de TI. Além disso, que a melhor forma de tratar o volume e a velocidade de informações produzidas a serem auditadas é a automação robótica de processos. E, que o modelo que deve ser adotado para assegurar o cumprimento das atribuições da auditoria interna e do sucesso na implantação da RPA é o das três linhas de defesa, considerando-o como a base dos desenvolvimentos dos robôs e da determinação de atribuições.

Ou seja, os auditores de bancos nacionais devem elaborar um Planejamento de Auditoria Interna estratégico, contínuo, integrado, baseado em riscos, com foco na automação de processos, fundamentado no modelo das três linhas de defesa e alinhado com o planejamento estratégico da organização e da TI, para enfrentar os desafios trazidos pela transformação digital e tornar a organização “Pronta para o Futuro”. Pois, as instituições financeiras estão adotando as ferramentas da indústria 4.0, como *machine learning, big data, blockchain*, para, entre outros usos, reter e fidelizar seus clientes; atender a legislação crescente dos órgãos

supervisores; e criar novos produtos e serviços. Mas, se não houver foco na integração entre TI, processos, gestores, áreas intervenientes e pessoas, capitaneada pela Alta Administração, com assessoria da Auditoria Interna; e amparada por uma cultura de inovação, essas ferramentas, e a automação delas, não trarão vantagem competitiva. Afinal todo o segmento, inclusive os novos entrantes (*fintechs* e bancos de investimento) estão fazendo isso.

Baseado nas evidências desse trabalho, as orientações metodológicas e estruturais para implantação da RPA, na auditoria interna, devem ser estendidas à toda empresa. E, principalmente, devem ser seguidas as atividades e as responsabilidades do processo de robotização atribuídas a cada segmento, conforme o modelo das três linhas de defesa. Isso deve ser feito não somente para a melhoria na gestão dos controles internos, dos riscos e da governança. Ou pelo fato desse novo ambiente virtual gerar riscos, que precisam ser mapeados; e possibilitar a ocorrência de novos tipos de fraudes e irregularidades, que necessitam ser previstas e mitigadas pela auditoria interna. Mas, sobretudo, para dirimir qualquer questão associada ao sombreamento de atividades, evitando a perda de foco e de eficiência; e para maximizar a integração vertical e horizontal. Além disso, o framework é simples e seu conceito é de fácil entendimento e aceitação.

Adicionalmente, é importante frisar que os profissionais de auditoria precisarão desenvolver diversas habilidades e competências para implementar o framework proposto, como em BPM, RPA, computação em nuvem, tecnologias emergentes, métodos ágeis e segurança cibernética.

6.2. Implicações

Nas últimas duas décadas, os 37 maiores bancos americanos foram reduzidos a 4, devido a fusões e incorporações ocasionadas, principalmente, por crises financeiras e o consequente arrocho regulatório (CALEIRO, 2016). Esses impactos repercutiram no sistema bancário nacional e nas atribuições das auditorias internas. E, a agora, há preocupações em relação ao futuro dos bancos e da auditoria interna, como conhecemos hoje, devido à transformação digital.

Esse fenômeno criou um novo ambiente para a atração e o relacionamento com os clientes; para a melhoria da eficiência operacional; e para a busca de vantagens, num setor já conhecido pela pressão da competitividade. Em função disso, é necessário o constante desenvolvimento de competências e de estudos

sobre essas novas tecnologias para escolha da melhor estratégia. Pois, os impactos dessas mudanças afetam as operações de *front e back-office* e causam questionamentos sobre as regulamentações nos mercados financeiros.

Além disso, está surgindo um ecossistema de dados, tratados analiticamente, que necessita de supervisão para evitar possíveis problemas éticos relacionados à privacidade e à portabilidade. Nesse cenário, surgem novos riscos relacionados à aplicação de algoritmos de inteligência artificial que desafiam os auditores a repensarem seus padrões de trabalho e a buscarem, na combinação desses mesmos recursos com a RPA, uma forma de garantir que suas responsabilidades sejam cumpridas, enquanto terceira linha de defesa.

Adicionalmente, há uma outra preocupação, que remonta os primórdios da industrialização - a substituição de humanos por máquinas. Mas, apesar da crescente robotização; e da perspectiva do incremento dessa, com sua fusão a tecnologias cognitivas, ainda não há um consenso sobre suas consequências. Contudo, caso isso ocorra num futuro próximo, pode haver grupos que prefiram se relacionar com organizações *robot-free*, de forma análoga a atual busca por produtos naturais, feita por nichos de mercado.

Independentemente desses fatores, a literatura recente enfatiza a necessidade dos auditores aproveitarem as vantagens das tecnologias emergentes para automatizar os mais diversos procedimentos, como a mineração de texto em contratos, para a avaliação de riscos e para a geração de evidências de auditoria; e o uso de drones na fiscalização de bens financiados.

Considerando que os avanços nesse campo têm sido exponenciais, a RPA em conjunto com o *big data*, poderiam ser usados para transformar a auditoria de *post factum* em preventiva (KUENKAIKAEW, 2013). E, a virtualização de dados na nuvem permitiria o acesso e a disponibilidade de informações a qualquer momento, o que tornaria a auditoria um serviço (AaS).

Portanto, a indústria 4.0 está gerando a auditoria 4.0 e, quiçá, o banco 4.0.

6.3. Deficiências no estudo sobre o tema

Na visão de Byrnes et al. (2018), a evolução da auditoria chegou num momento crítico no qual necessita optar por uma abordagem de vanguarda. Isso exigirá dos auditores, reguladores e normatizadores ajustes significativos, como a diminuição do intervalo de tempo entre auditorias; a capacitação em novas tecnologias e em métodos analíticos; a adoção somente do exame populacional

completo; o reexame de conceitos como materialidade e independência; e, a obrigatoriedade da padronização dos dados de auditoria. Portanto, há um campo fértil a ser arado; e, as pesquisas, até o momento, sobre essa nova forma de atuação da Auditoria, foram basicamente exploratórias.

Além disso, embora haja o aumento no uso de *machine learning* e da robotização, o julgamento analítico e a tenacidade, inerentes às habilidades do auditor, não são passíveis de automação. Aquela ocorrerá em aspectos pontuais das atividades críticas de cada processo relevante ao longo do ano, ao invés de apenas uma vez no período, deixando os auditores focados nas questões mais urgentes e necessária à sua opinião especializada. Logo, há grande deficiência na literatura e muito a pesquisar sobre as atividades que podem e devem ser automatizadas, de forma a produzir insumos para *insights* sobre os processos, visando, assim, a melhoria na eficácia da gestão de riscos, dos controles internos, da governaça; e, do assessoramento e da consultoria à Alta Administração pela auditoria interna.

6.4.
Limitações desse estudo e Sugestões para Futuras Pesquisas

O presente estudo foi descritivo-proposito e restringiu-se a apresentar um *framework* para do uso da RPA nas auditorias internas de bancos nacionais, considerando o modelo das três linhas de defesa, de forma a assegurar que essa mudança de paradigma seja exitosa. Mas, à medida em que a auditoria evolui, acompanhando a transformação digital, surgem diversas questões que precisam ser respondidas. Nesse sentido, novas pesquisas poderiam abordar: os meios de identificação das ferramentas mais adequadas à proposta de valor determinada no plano de ação da RPA; os critérios de determinação da melhor combinação entre elas; os principais desafios na implementação de RPAs e como tratá-los; os casos concretos do uso da RPA em testes de auditoria; as metodologias para avaliação da estrutura das RPAs; os riscos relacionados à privacidade e à segurança; ou, se nesse novo cenário, haveria mudança nos papéis das linhas de defesa.

7
Referências

ABDOLMOHAMMADI, M. J.; USOFF, C. A. **The Assessment of Task Structure, Knowledge Base, and Decision Aids for a Comprehensive Inventory of Audit Tasks**. In: BOOKS, Q. (Org.). [s.l.]: [s.n.], 2001.

ACCENTURE. **Robotic Process Automation**. [s.d.]. Disponível em: <https://www.accenture.com/dk-en/insight-financial-services-robotic-process-automation>. Acesso em: 19/jan./20.

ACKERMAN, M. **IT Strategic Audit Plan**. *Journal of Technology Research*, [s.l.], v. 1, p. 10, 2009.

AI MULTIPLE. **20 RPA Pitfalls & the Checklist for Avoiding Them [2020 update]**. 2020. Disponível em: <https://blog.aimultiple.com/rpa-pitfalls/>. Acesso em: 26/jan./20.

AICPA. **Understanding the Entity and Its Environment and Assessing the Risks of Material Misstatement**. 2019.

_____. **Audit Data Standards**. 2020. Disponível em: <https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/auditdatastandards.html>. Acesso em: 26/jan./20.

ALLES, M. G. et al. **Continuous Auditing: the USA Experience and Considerations for its Implementation in Brazil**. *Journal of Information Systems and Technology Management*, [s.l.], v. 3, nº 2, p. 211–224, 2009. ISBN: 1807177520060, DOI: 10.4301/s1807-17752006000200007.

ALLES, M.; KOGAN, A.; VASARHELYI, M. **Audit automation for implementing continuous auditing: Principles and problems**. *Ninth International Research …*, [s.l.], p. 1–24, 2008. ISSN: 0001-0782, DOI: http://doi.acm.org/10.1145/129875.129878.

ANDRIOLE, S. J. **Skills and Competencies for Digital Transformation**. *IT Professional*, [s.l.], v. 20, nº 6, p. 78–81, 2018. ISSN: 1941045X, DOI: 10.1109/MITP.2018.2876926.

AUDIT SCOTLAND. **Digital Audit Strategy 2017**. [s.l.]: [s.n.], 2017. Disponível em: <https://www.audit-scotland.gov.uk/uploads/docs/um/digital_audit_strategy_2017.pdf>.

AUDITORIA INTERNA DO BANCO DO BRASIL. **Relatório Anual de Atividades de Auditoria Interna - 2018**. [s.l.]: [s.n.], 2019. Disponível em: <https://www.bb.com.br/docs/portal/pub/Raint2018.pdf>.

AUTOMATION ANYWHERE. **Segurança de nível empresarial para Automação Robótica de Processos**. [s.l.]: [s.n.], 2018. Disponível em: <https://www.automationanywhere.com/images/enterprise-class-security/Enterprise-class-Security-RPA-042519-pt.pdf>.

_____. **Robotic Process Automation is a major component of Santander Consumer Bank's Business Strategy | Aut**. *april*. 2019. Disponível

em: <https://resources.automationanywhere.com/watch/robotic-processing-automation-is-a-major-component-of-santander-consumer-banks-business-strategy>. Acesso em: 28/fev./20.

BACEN. **Relatório de Cidadania Brasileira**. In: *Banco Central do Brasil*. [s.l.]: [s.n.], 2018. Disponível em: <https://www.bcb.gov.br/content/cidadaniafinanceira/documentos_cidadania/RIF/Relatorio Cidadania Financeira_BCB_16jan_2019.pdf>. ISSN: 2595-4865.

_____. **Requisitos fundamentais para a implementação, no Brasil, do Sistema Financeiro Aberto (Open Banking).** 2019. Disponível em: <https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Comunicado&numero=33455>. Acesso em: 13/jan./20.

BAJKOWSKI, J. **Westpac to build new pure play digital bank -**. *iTnews*. 2019. Disponível em: <https://www.itnews.com.au/news/westpac-to-build-new-pure-play-digital-bank-533398>. Acesso em: 15/jan./20.

BBVA. **The digital bank of the 21st century**. 2020. Disponível em: <https://www.bbva.com/en/>. Acesso em: 15/jan./20.

BHARADWAJ, R. **Robotic Process Automation (RPA) in Finance – Current Applications**. *Emerj*. 2019. Disponível em: <https://emerj.com/ai-sector-overviews/robotic-process-automation-rpa-finance-current-applications/>. Acesso em: 26/jan./20.

BNY MELLON. **BNY Mellon's Automation Efforts Draw Industry Accolades**. 2017. Disponível em: <https://www.bnymellon.com/us/en/newsroom/news/press-releases/bny-mellons-automation-efforts-draw-industry-accolades.jsp>. Acesso em: 28/fev./20.

BRACHIO, A. **How internal audit can help make RPA implementation a success**. *EY Global*. 2018. Disponível em: <https://www.eylaw.com.hk/en_gl/advisory/how-internal-audit-can-help-make-rpa-implementation-a-success>. Acesso em: 25/jan./20.

BRADESCO. **Bradesco - Relações com Investidores**. 2019. Disponível em: <https://www.bradescori.com.br/siteBradescoRI/Paginas/obradesco/202_presencaeinovacao_.aspx?termo=presença>. Acesso em: 15/jan./20.

BRASIL. Câmara dos Deputados do Brasil e Senado Federal do Brasil. **Lei Geral de Proteção de Dados Pessoais**. 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 13/jan./20.

BROCKE, J. VOM et al. **Future Work and Enterprise Systems**. *Business and Information Systems Engineering*, [s.l.], v. 60, nº 4, p. 357–366, 2018. ISSN: 18670202, DOI: 10.1007/s12599-018-0544-2.

BROWN-LIBURD, H.; ISSA, H.; LOMBARDI, D. **Behavioral implications of Big Data's impact on audit judgment and decision making and future research directions.** *Accounting Horizons 29 (2): 451–468.*, [s.l.], v. Vol. 29, nº No. 2, p. 451-468., 2015.

BUMGARNER, N.; VASARHELYI, M. A. **Continuous Auditing—A New View**. *Continuous Auditing: Theory and Application*. [s.l.]: [s.n.], 2015. p. 7–51. DOI: https://doi.org/10.1108/978-1-78743-413-420181002.

BURGESS, A. **Time to Talk - RPA and AI In Contact Centers**. 2016. Disponível em: <https://blog.symphonyhq.com/time-to-talk-robots-and-ai-in-contact-centres>. Acesso em: 26/jan./20.

BURKE, W. W. **Leaders: The strategies for taking charge, by Warren Bennis and Burt Nanus. New York: Harper & Row, 1985, 244 pp., $19.95**. *Human Resource Management*, [s.l.], v. 24, nº 4, p. 503–508, 1985. ISSN: 00904848, DOI: 10.1002/hrm.3930240409.

BYRNES, P. E. et al. **Evolution of Auditing: From the Traditional Approach to the Future Audit**. *Continuous Auditing*, [s.l.], p. 285–297, 2018. ISBN: 9781787434134, DOI: 10.1108/978-1-78743-413-420181014.

CALEIRO, J. P. **Veja em um diagrama como 37 bancos se tornaram 4 em 20 anos**. *EXAME*. 2016. Disponível em: <https://exame.abril.com.br/economia/veja-em-um-diagrama-como-37-bancos-se-tornaram-4-em-20-anos/>. Acesso em: 26/jan./20.

CECCHI, A. **Desenvolvedor de automação no Banco Safra**. *GitHub*. 2019. Disponível em: <https://github.com/backend-br/vagas/issues/1419>. Acesso em: 28/fev./20.

CHANDEL, A. S. **Making banking "invisible" with digital transformation**. *April*. 2019. Disponível em: <https://www.ibm.com/blogs/client-voices/banking-invisible-digital-transformation/>. Acesso em: 28/fev./20.

CHAPPELL, D. **Introducing Blue Prism Robotic Process Automation for the Enterprise**. [s.l.], p. 24, 2017.

CHARTERED INSTITUTE OF INTERNAL AUDITORS. **Computer assisted audit techniques**. In: *Chartered Institute of Internal Auditors*. [s.l.]: [s.n.], 2019. Disponível em: <https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=21&cad=rja&uact=8&ved=2ahUKEwiCl67plIvnAhWyH7kGHWDEChsQFjAUegQIAhAB&url=https%3A%2F%2Fwww.iia.org.uk%2Fresources%2Fdelivering-internal-audit%2Fcomputer-assisted-audit-techniques-caats%2F%3Fdown>. ISSN: 0353-359X.

CHIESA, V.; COUGHLAN, P.; VOSS, C. A. **Development of a Technical Innovation Audit**. *Journal of Product Innovation Management*, [s.l.], v. 13, nº 2, p. 105–136, 1996. ISSN: 0737-6782, DOI: 10.1111/1540-5885.1320105.

CIRNE, N. **Indústria 4.0: uma revolução no setor financeiro e nos meios de pagamento**. *ecommercebrasil*. 2019. Disponível em: <https://www.ecommercebrasil.com.br/artigos/industria-40-revolucao-setor-financeiro/>.

CITI. **AI and robotics can create an opportunity for new, more innovative jobs in banks|**. *eFinancialCareers*. 2017. Disponível em: <https://news.efinancialcareers.com/sg-en/292742/citi-ai-robotics-technology-sc>. Acesso em: 28/fev./20.

CODESSO, M. M. et al. **Continuous audit model: data integration framework**. *Revista Contemporânea de Contabilidade*, [s.l.], v. 15, nº 34, p. 144–157, 2018. ISSN: 1807-1821, DOI: 10.5007/2175-8069.2018v15n34p144.

COHEN, M.; ROZARIO, A. M.; CHANYUAN, Z. **Exploring the Use of Robotic Process Automation (RPA) in Substantive Audit Procedures -**. *The CPA Journal*, [s.l.], 2019.

COMMITTEE ON BANKING SUPERVISION, B. **Basel Committee on Banking Supervision Basel III: Finalising post-crisis reforms**. [s.l.]: [s.n.], 2017. ISBN: 9789292590222.

COOPER, L. et al. **Robotic process automation in public accounting.** [s.l.]: [s.n.], 2019. Disponível em: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3193222>. DOI: http://dx.doi.org/10.2139/ssrn.3193222.

CRESWELL, J. W. **Projeto de pesquisa : métodos qualitativo, quantitativo e misto**. 3. ed. ed. São Paulo: Sage, 2010. 296 p. ISBN: 8536323000.

DAI, J.; VASARHELYI, M. A. **Imagineering audit 4.0**. *Journal of Emerging Technologies in Accounting*, [s.l.], v. 13, nº 1, p. 1–15, 2016. ISSN: 15587940, DOI: 10.2308/jeta-10494.

DAMIANIDES, M. **Robotics Process Automation (RPA) and Artificial Intelligence (AI): A New World Order**. In: *Ernst & Young Partner*. Los Angeles: ISACA, 2018.

DBS BANK. **Live more, Bank less**. [s.d.]. Disponível em: <https://www.dbs.com/default.page>. Acesso em: 15/jan./20.

DELOITTE. **The Path Forward : Operationalizing RPA to Automate the Digital Supply Network**. [s.l.]: [s.n.], 2018.

DEMIRGÜÇ-KUNT, A. et al. **The Global Findex Database 2017**. *Journal of Chemical Information and Modeling*. [s.l.]: [s.n.], 2017. v. 53, 151 p. ISBN: 9788578110796, ISSN: 1098-6596, DOI: 10.1017/CBO9781107415324.004.

DUREVALL, H. **Danske Bank – A case study in delivering a digital strategy**. *Mapa Research*. 2014. Disponível em: <https://www.maparesearch.com/danske-bank-a-case-study-in-delivering-a-digital-strategy/>. Acesso em: 15/jan./20.

ERNST & YOUNG. **Get Ready For Robots**. In: *Ernst & Young*. [s.l.]: [s.n.], 2016. Disponível em: <https://www.ey.com/Publication/vwLUAssets/Get_ready_for_robots/$FILE/ey-get-ready-for-robots.pdf>. ISSN: 1099274X.

ERNST & YOUNG GLOBAL LIMITED. **Maximizing value from your lines of defense. A pragmatic approach to establishing and optimizing your LOD model**. [s.l.]: [s.n.], 2013. Disponível em: <ey.com/GRCinsights>.

EUROMONEY. **World's best digital bank 2016: DBS**. *july*. 2016. Disponível em: <https://www.euromoney.com/article/b12kq6p8mv5rh3/world39s-best-digital-bank-2016-dbs>. Acesso em: 15/jan./20.

_____. **World's best digital bank 2017: Citi**. *july*. 2017. Disponível em: <https://www.euromoney.com/article/b13pwgqqmt2fy6/world39s-best-digital-bank-2017-citi>. Acesso em: 28/fev./20.

_____. **World's best digital bank 2018: DBS**. *july*. 2018. Disponível em: <https://www.euromoney.com/article/b18k8wtzv7v23d/world39s-best-digital-bank-2018-dbs>. Acesso em: 15/jan./20.

_____. **World's best bank 2019: DBS**. *july*. 2019. Disponível em: <https://www.euromoney.com/article/b1fmmkjyhws0h9/world39s-best-bank-2019-dbs>. Acesso em: 15/jan./20.

EUROPEAN AUDIT COMMITTEE LEADERSHIP NETWORK. **The impact of digital technologies on internal audit**. [s.l.], nº January, p. 1–12, 2017.

EY. **How do you protect the robots from cyber attack ? Securing robotic process automation platforms and enabling cybersecurity through orchestration and cognitive learning**. [s.l.]: [s.n.], 2018. Disponível em: <https://www.ey.com/Publication/vwLUAssets/ey-how-do-you-protect-robots-from-cyber-attack/$FILE/ey-how-do-you-protect-robots-from-cyber-attack.pdf>.

FEBRABAN. **27ª Pesquisa FEBRABAN de Tecnologia Bancária**. In: *Federação Brasileira de Bancos*. [s.l.]: [s.n.], 2019. Disponível em: <https://uc584f91371099789ca1a46c377d.previews.dropboxusercontent.com/p/orig/AApW71SPLfoKfjK_Ry-yldbkFEkpV67jv0cRf2dDmGotzEntWcsIBnGd9QF0EwRWMd_vGLlVOjltroMtrjJQ2zfjRN3YNKdtKI44wtWTrkaFazgGOLnTKUSjP0QDC7eyI8tq0Y16-jbp5L8rh7sF0PSIycHPFgGteB6vcnRu6TsqUdWl1D>.

FERMA / ECIIA. **Guidance on the 8 th EU Company Law Directive**. *Guidance for boards and audit committees*, [s.l.], p. 11, 2010.

FERRAZ, K. **Como a Automation Anywhere pretende democratizar a robótica no Brasil | Computerworld**. *Computer world*. 2019. Disponível em: <https://computerworld.com.br/2019/05/21/como-a-automation-anywhere-pretende-democratizar-a-robotica-no-brasil/>. Acesso em: 28/fev./20.

FINANTECH. **Robotização minimiza gargalos operacionais e complexidade no setor de seguros**. 2018. Disponível em: <http://cantarinobrasileiro.com.br/blog/robotizacao-minimiza-gargalos-operacionais-e-complexidade-no-setor-de-seguros/>. Acesso em: 28/fev./20.

FLINT, D. **Philosophy and principles of auditing : an introduction**. [s.l.]: Macmillan Education, 1988. 191 p. ISBN: 9780333311165.

FORRESTER. **Forrester Wave Robotic Process Automation, Q2 2018**. *Forrest Research*. 2018. Disponível em: <https://www.uipath.com/company/rpa-analyst-reports/forrester-wave-2018-robotic-process-automation>. Acesso em: 01/fev./20.

GARTNER. **Gartner Says Worldwide Robotic Process Automation Software Market Grew 63% in 2018**. *june*. 2019. Disponível em: <https://www.gartner.com/en/newsroom/press-releases/2019-06-24-gartner-says-worldwide-robotic-process-automation-sof>. Acesso em: 28/fev./20.

GERHARDT, T. E.; SILVEIRA, D. T. **Metodologia de Pesquisa**. [s.l.]:

Universidade Federal do Rio Grande do Sul, 2009. 120 p. ISBN: 9788538600718.

GOTTHARDT, M. et al. **Current State and Challenges in the Implementation of Robotic Process Automation and Artificial Intelligence in Accounting and Auditing**. *Journal of Finance & Risk Perspectives*, [s.l.], v. 8, p. 31–46, 2019.

GRIFFITH, E. E. et al. **Auditor mindsets and audits of complex estimates**. *Journal of Accounting Research*, [s.l.], v. 53, nº 1, p. 49–77, 2015. ISSN: 1475679X, DOI: 10.1111/1475-679X.12066.

HALDANE, A. G. **The dog and the frisbee**. [s.l.]: [s.n.], 2012. Disponível em: <https://www.bis.org/review/r120905a.pdf?frames=0>.

HARDER, D. S.; DAVIS, D. J. **The Automatic Factory?** In: *Society of Automotive Engineers*. New York: [s.n.], 1953. Disponível em: <https://saemobilus.sae.org/content/530060/>.

HARDY, C. A. **Business analytics and continuous assurance: Theoretical matters, practice issues, and future directions**. *Proceedings of the Annual Hawaii International Conference on System Sciences*, [s.l.], v. 2015-March, p. 4732–4741, 2015. ISBN: 9781479973675, ISSN: 15301605, DOI: 10.1109/HICSS.2015.563.

HEIDEGGER, M. **Ser e Tempo**. [s.l.]: [s.n.], 1927.

HUANG, F.; VASARHELYI, M. A. **Applying robotic process automation (RPA) in auditing: A framework**. *International Journal of Accounting Information Systems*, [s.l.], v. 35, p. 100433, 2019. ISSN: 14670895, DOI: 10.1016/j.accinf.2019.100433.

IBM. **Banco Popular**. 2018. Disponível em: <https://www.ibm.com/case-studies/banco-popular>. Acesso em: 19/jan./20.

IBM SERVICES. **Wake-up call | Anand Singh Chandel: A father's son transforms an industry**. *june*. 2018. Disponível em: <https://www.ibm.com/blogs/services/2018/06/26/wake-up-call-anand-singh-chandel-a-fathers-son-transforms-an-industry/>. Acesso em: 28/fev./20.

ICAEW. **How do you audit a robot?** 2019. Disponível em: <https://www.icaew.com/technical/audit-and-assurance/assurance/what-can-assurance-cover/internal-audit-resource-centre/how-do-you-audit-a-robot>. Acesso em: 25/jan./20.

IIA NETHERLANDS. **Strategy-related Auditing**. *The Institute of Internal Auditors Netherlands*, [s.l.], nº June, 2015.

IRPAAI. **What is Robotic Process Automation?** 2016. Disponível em: <https://irpaai.com/what-is-robotic-process-automation/>. Acesso em: 20/jan./20.

ISSA, H.; SUN, T.; VASARHELYI, M. A. **Research ideas for artificial intelligence in auditing: The formalization of audit and workforce supplementation**. *Journal of Emerging Technologies in Accounting*, [s.l.], v. 13, nº 2, p. 1–20, 2016. ISSN: 15587940, DOI: 10.2308/jeta-10511.

KUENKAIKAEW, S. **Predictive Audit Analytics: Evolving to a New Era**.

147 p. 2013. Disponível em: <https://rucore.libraries.rutgers.edu/rutgers-lib/41494/>.

LACITY, M. C.; WILLCOCKS, L. P.; CRAIG, A. **Robotic process automation at telefónica O2**. *MIS Quarterly Executive*, [s.l.], v. 15, nº 1, p. 21–35, 2015. ISSN: 15401979.

LEE, T. A. **Company auditing**. 3rd ed. ed. [s.l.]: Chapman & Hall, 1986. ISBN: 0412437201.

LIANG, F. S.; ZHENG, Z. W. **Innovation in assurance: doing more, and more effectively, with less**. *Singapore Business Review*, [s.l.], 2016.

LIU, Q.; VASARHELYI, M. A. **Big questions in AIS research: Measurement, information processing, data analysis, and reporting**. *Journal of Information Systems*, [s.l.], v. 28, nº 1, p. 1–17, 2014. ISSN: 15587959, DOI: 10.2308/isys-10395.

LOWERS, P. et al. **Automate this - The business leader's guide to robotic and intelligent automation**. In: *Deloitte LLP*. [s.l.]: [s.n.], 2016. Disponível em: <https://www2.deloitte.com/content/dam/Deloitte/us/Documents/process-and-operations/us-sdt-process-automation.pdf>.

MARKS, N. **The Three Lines of Defense model is the Wrong model**. 2015. Disponível em: <https://normanmarks.wordpress.com/2015/01/25/the-three-lines-of-defense-model-is-the-wrong-model/>. Acesso em: 03/fev./20.

MARQUES, R. P.; SANTOS, C. **Research on continuous auditing: A bibliometric analysis**. *Iberian Conference on Information Systems and Technologies, CISTI*, [s.l.], p. 1–4, 2017. ISBN: 9789899843479, ISSN: 21660735, DOI: 10.23919/CISTI.2017.7976048.

MARTELLO, A. **Cinco maiores bancos comerciais detinham 84,8% do mercado de crédito no fim de 2018, revela BC**. *Economia G1*. 2019. Disponível em: <https://g1.globo.com/economia/noticia/2019/05/28/cinco-maiores-bancos-comerciais-detem-848percent-do-mercado-de-credito-no-fim-de-2018-revela-bc.ghtml>. Acesso em: 26/jan./20.

MARUTI TECHLABS. **RPA in Banking — Use-cases, Benefits and Steps**. *nov*. 2019. Disponível em: <https://medium.com/@MarutiTech/rpa-in-banking-use-cases-benefits-and-steps-8b97312a7d4f>. Acesso em: 28/fev./20.

MAUTZ, R. K.; SHARAF, H. A. **The philosophy of auditing**. *Published in 1961 in Sarasota Fla by American Accounting Association*, [s.l.], 1961.

MAZZONE, D. **Digital or Death: Digital Transformation—The Only Choice forBusiness to Survive Smash and Conquer.** 1st ed. ed. Mississauga, Ontario: SmashboxConsulting Inc, 2014.

MCCLIMANS, F. **Welcoming our Robotic Security Underlings**. [s.l.]: [s.n.], 2016. Disponível em: <https://www.hfsresearch.com/pointsofview/welcoming-our-roboticsecurity-%0Aunderlings>.

MENNIE, P. **AI and RPA in Internal Audit**. In: *IIA Annual Conference*. [s.l.]: [s.n.], 2019. Disponível em: <https://www.uaeiaa.org/writereaddata/Portal/ConferencesDownloads/642f94b6-

0451-4331-b48f-14a1e952b482.pdf>.

MOFFITT, K. C.; ROZARIO, A. M.; VASARHELYI, M. A. **Robotic process automation for auditing**. *Journal of Emerging Technologies in Accounting*, [s.l.], v. 15, nº 1, p. 1–10, 2018. ISSN: 15587940, DOI: 10.2308/jeta-10589.

MORIN, E. **Introdução ao pensamento complexo**. 2 ed. ed. Lisboa: Instituto Piaget, 1995.

MURCIA, F.; SOUZA, F.; BORBA, J. **Continuous Auditing : A Literature Review Auditoria Contínua : uma revisão da literatura**. *Organizações em Contexto*, [s.l.], v. 7, p. 1–17, 2008.

NUBANK. **O que é o Nubank? - Fala, Nubank**. 2020. Disponível em: <https://blog.nubank.com.br/nubank-o-que-e-confiavel/>. Acesso em: 27/jan./20.

PATI, C. **Santander abre mais de 400 vagas para profissionais de tecnologia**. *Exame*. 2019. Disponível em: <https://exame.abril.com.br/carreira/santander-abre-mais-de-400-vagas-para-profissionais-de-tecnologia/>. Acesso em: 28/fev./20.

PCAOB. **Auditing Standard No. 5**. 2007. Disponível em: <https://pcaobus.org/Standards/Archived/PreReorgStandards/Pages/Auditing_Standard_5.aspx>. Acesso em: 13/jan./20.

_____. **Auditing Standard No. 8**. 2010. Disponível em: <https://pcaobus.org/Standards/Archived/PreReorgStandards/Pages/Auditing_Standard_8.aspx>. Acesso em: 31/jan./20.

PEGASYSTEMS. **OCBC Sets New Standard for Customer Accounts**. 2019. Disponível em: <https://www.pega.com/customers/ocbc-bank-sales-automation>. Acesso em: 28/fev./20.

PHANEUF, A. **Robotic Process Automation (RPA) in Banking**. *Business Insider*. 2019. Disponível em: <https://www.businessinsider.com/rpa-banking-examples-use-cases>. Acesso em: 28/fev./20.

PORTE, M. et al. **Research in auditing: main themes**. *Revista Contabilidade & Finanças*, [s.l.], v. 29, nº 76, p. 41–59, 2018. ISSN: 1808-057X, DOI: 10.1590/1808-057x201804410.

PROTIVITI. **2010 Internal Audit Capabilities and Needs Survey**. [s.l.]: [s.n.], 2010. Disponível em: <https://www.yumpu.com/en/document/read/30871270/2010-internal-audit-capabilities-and-needs-survey-protiviti>.

PWC. **Robotic process automation : A primer for internal audit professionals**. [s.l.], p. 1–4, 2018.

PWC. **Continuous Audit & Monitoring**. 2020. Disponível em: <https://www.pwc.com/vn/en/services/consulting/continuous-audit-monitoring.html>. Acesso em: 09/fev./20.

RADOVANOVIĆ, D. et al. **IT Audit in Accordance with COBIT Standard**. In: *The 33rd International Convention MIPRO*. [s.l.]: [s.n.], 2010.

REED, B. et al. **Élaborer le Plan Stratégique de L'Audit Interne**. [s.l.]: [s.n.], 2018. DOI: 10.4000/books.puv.221.

REZAEE, Z.; ELAM, R.; SHARBATOGHLIE, A. **Continuous auditing: The audit of the future**. *Managerial Auditing Journal*, [s.l.], v. 16, nº 3, p. 150–158, 2001. ISSN: 02686902, DOI: 10.1108/02686900110385605.

ROBOTICSBIZ. **Best practices to secure your robotic process automation (RPA)**. 2019. Disponível em: <https://roboticsbiz.com/best-practices-to-secure-your-robotic-process-automation-rpa/>. Acesso em: 01/fev./20.

ROGERS, D. L. **Digital Transformation Playbook: Rethink Your Business for the Digital Age**. New york: Columbia Business School, 2016.

ROMAO, M.; COSTA, J.; COSTA, C. J. **Robotic process automation: A case study in the banking industry**. *Iberian Conference on Information Systems and Technologies, CISTI*, [s.l.], v. 2019-June, nº June, p. 19–22, 2019. ISBN: 9789899843493, ISSN: 21660735, DOI: 10.23919/CISTI.2019.8760733.

ROSS, J. W. et al. **Designing and executing digital strategies**. In: *International Conference on Information Systems, ICIS*. [s.l.]: [s.n.], 2016. ISBN: 9780996683135.

ROSS, J. W.; WEILL, P.; ROBERTSON, D. C. **Enterprise Architecture As Strategy: Creating a Foundation for Business Execution**. [s.l.]: Harvard Business School Press, 2006.

SALOMÃO, K. **Bradesco lança banco digital Next**. *EXAME*, [s.l.], 2017.

SANTOS, C. **Grandes empresas adotam RPA na busca de eficiência**. *TI inside*. 2018. Disponível em: <https://tiinside.com.br/14/05/2018/grandes-empresas-adotam-rpa-na-busca-de-eficiencia/>. Acesso em: 28/fev./20.

SARBANES, P.; OXLEY, M. Senate and House of Representatives of the United States of America in Congress assembled. **SARBANES-OXLEY ACT**. federal law. 2002.

SAS; INTEL; DELOITTE. **Combining Robotic Process Automation Title and Machine Learning**. [s.l.]: [s.n.], 2018. Disponível em: <https://www.sas.com/en/whitepapers/combining-robotic-process-automation-machine-learning-110369.html>.

SCHWAB, K. **A Quarta Revolução Industrial**. Geneva, Switzerland: [s.n.], 2016. Disponível em: <https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=15&cad=rja&uact=8&ved=2ahUKEwiM6bbjrffmAhXwHbkGHe1RDBEQFjAOegQICBAC&url=https%3A%2F%2Fedisciplinas.usp.br%2Fpluginfile.php%2F4212041%2Fmod_folder%2Fcontent%2F0%2FSchwab%2520%25282016%2529%2520A>.

SEASONGOOD, S. **Not Just for the Assembly Line: A Case for Robotics in Accounting and Finance**. *FEI*. 2017. Disponível em: <https://www.financialexecutives.org/Topics/Technology/Not-Just-for-the-Assembly-Line-A-Case-for-Robotic.aspx>. Acesso em: 26/jan./20.

SESHADRI, D.; SHARMA, A. **Auditing the RPA environment Our approach towards addressing risks in a BOT environment Risk Advisory**.

[s.l.]: [s.n.], 2018.

SIA, S. K.; SOH, C.; WEILL, P. **How DBS bank pursued a digital business strategy**. *MIS Quarterly Executive*, [s.l.], v. 15, nº 2, p. 105–121, 2016. ISSN: 15401979.

SMITH, C. A. . **Detecting Anomalies in Your Data Using Benford ' s Law**. *Statistics and Data Analysis*, [s.l.], v. paper 249-, nº sas, p. 6, 2018.

SYED, R. et al. **Robotic Process Automation: Contemporary Themes and Challenges**. *Computers in Industry*, [s.l.], v. 115, p. 103162, 2019. ISSN: 0166-3615, DOI: 10.1016/j.compind.2019.103162.

TALEB, N. N. **The black swan: The impact of the highly improbable**. *The Black Swan: The Impact of the Highly Improbable*. New York: Random House, 2017. 1–401 p. ISBN: 9781351351195, ISSN: 0733-4273, DOI: 10.4324/9781912281206.

TECNODATA. **RPA vs. BPM - dois lados da mesma moeda**. 2019. Disponível em: <https://www.atstecnologia.com.br/post/rpa-vs-bpm-dois-lados-da-mesma-moeda>. Acesso em: 27/fev./20.

THE INSTITUTE OF INTERNAL AUDITOR. **IIA Position Paper : The Three Lines of Defense in Effective Risk Management and Control**. In: *IAA*. [s.l.]: [s.n.], 2013. Disponível em: <https://www.theiia.org/3-lines-defense>.

TRELLES, O. et al. **Big data, but are we ready?** *Nature Reviews Genetics*, [s.l.], v. 12, nº 3, p. 224, 2011. ISSN: 14710056, DOI: 10.1038/nrg2857-c1.

VASARHELYI, M. A.; ALLES, M. G.; WILLIAMS, K. T. **Continuous Assurance for the Now Economy: A Thought Leadership Paper for the Institute of Chartered Accountants in Australia**. [s.l.], nº February, p. 1–70, 2010.

VASARHELYI, M. A.; HALPER, F. B. **The Continuous Audit of Online Systems**. *Continuous Auditing*, [s.l.], p. 87–104, 1991. DOI: 10.1108/978-1-78743-413-420181004.

VINUTHA. **Image Recognition – The heart of sophisticated RPA**. 2017. Disponível em: <https://www.nalashaa.com/image-recognition-rpa/>. Acesso em: 26/jan./20.

WEILL, P.; WOERNER, S. **What's Your Digital Business Model?: Six Questions to Help You Build the Next-Generation Enterprise**. [s.l.]: Harvard Business Review, 2018a.

WEILL, P.; WOERNER, S. L. **Is Your Company Ready for a Digital Future?** *MIT Sloan Management Review*, [s.l.], nº December 04, 2017, 2018b.

WILLCOCKS, L.; HINDLE, J.; LACITY, M. **KEYS TO RPA: How Blue Prism Clients Are Gaining Superior Long Term Business Value**. [s.l.]: [s.n.], 2019. Disponível em: <https://assets-eb99.kxcdn.com/uploads/resources/white-papers/KCP_Summary-Executive_Research_Report_Final.pdf>.