RECITE
Revista Carioca de Ciência, Tecnologia e Educação

TRANSFORMAÇÃO DIGITAL E COMPLIANCE: GESTÃO DO TRABALHO COM ERP NUMA ORGANIZAÇÃO QUE APRENDE

Ana Carolina de Gouvea Dantas Motta
Doutora em Engenharia de Produção - COPPE/ UFRJ. Universidade Santa Úrsula (USU)
https://orcid.org/0000-0001-5918-6274

Fernando Cesar Almeida Silva
Mestre em Sistemas de Gestão. Universidade Federal Fluminense (UFF)
https://orcid.org/0000-0002-9236-7170

Emiliano Carlos Serpa Castor
Mestre em Gestão do Trabalho pela Qualidade do Ambiente Construído. Universidade Santa Úrsula (USU)
https://orcid.org/0000-0003-2976-704

Data de submissão: 08/09/2020
Data de aprovação: 26/10/2020

RESUMO

Este trabalho baseou-se na pesquisa bibliográfica de informações em livros de referência e em documentações específicas relativas às instituições competentes responsáveis por *frameworks*, padrões e práticas de mercado e às legislações em vigor. Também foram consultadas políticas, normas e notas técnicas corporativas com o intuito de levantar as aplicações práticas de conceitos teóricos em uma empresa de grande porte e âmbito nacional. O objetivo geral deste trabalho é mostrar que é possível elevar a qualidade dos serviços prestados e atender aos marcos regulatórios impostos pela legislação e pelas auditorias internas e externas, por meio de Sistemas de TI concebidos especificamente para este fim. A pesquisa permitiu identificar como resultado que o *Cloud Identity Access Governance (IAG)* se apresenta como o próximo passo na gestão da *Compliance* dos Sistemas SAP, em substituição à suíte Governança, Riscos e Conformidade (GRC), pois ele implementa atributos de controle de acesso, gestão de riscos, controles internos, governança e integridade em sistemas SAP que se utilizam da Computação em Nuvem (*in cloud*). Por fim, destaca-se que, com o IAG, é possível mitigar riscos associados a conflitos de segregação de funções (*SoD)* e ao acesso crítico para soluções locais (*on premise*) e na nuvem (*in cloud*). Tais soluções possuem a característica de residirem em *sites* fora das fronteiras físicas das organizações. E, para isto, a estratégia de *Compliance* deve ser diferente da tradicional. Como este assunto extrapola o escopo deste trabalho de conclusão de curso, é recomendado, como continuação do estudo deste tema, o levantamento dos métodos que são aplicados para estabelecer a gestão da conformidade em ambientes SAP *in cloud* com o suporte do SAP IAG.

Palavras-chave: Ética. SAP. GRC. Lei Sarbanes-Oxley. Organização que aprende.

DIGITAL TRANSFORMATION AND COMPLIANCE: ERP WORK MANAGEMENT IN AN LEARNING ORGANIZATION

ABSTRACT

This work was based on the bibliographic search for information in reference books and specific documentation related to the competent institutions responsible for frameworks, standards and market practices and the laws in force. Corporate policies, standards and technical notes were also consulted in order to survey the practical applications of theoretical

concepts in a large company and nationwide. The general objective of this work is to show that it is possible to raise the quality of the services provided and meet the regulatory frameworks imposed by legislation and by internal and external audits, through IT Systems designed specifically for this purpose. The research allowed us to identify as a result that Cloud Identity Access Governance (IAG) presents itself as the next step in managing SAP Systems Compliance, replacing the Governance, Risk and Compliance (GRC) suite, as it implements access control attributes, risk management, internal controls, governance and integrity in SAP systems that use Cloud Computing (in cloud). Finally, it is noteworthy that, with the IAG, it is possible to mitigate risks associated with segregation of duties (SoD) conflicts and critical access to local solutions (on premise) and in the cloud (in cloud). Such solutions have the characteristic of residing on sites outside the physical boundaries of organizations. And, for this, the Compliance strategy must be different from the traditional one. As this subject goes beyond the scope of this course conclusion work, it is recommended, as a continuation of the study of this theme, to survey the methods that are applied to establish compliance management in SAP in cloud environments with the support of SAP IAG.

***Keywords**: Ethic. SAP. GRC. Sarbanes–Oxley Act. Learning organization.*

TRANSFORMACIÓN DIGITAL Y COMPLIANCE: GESTIÓN DEL TRABAJO CON ERP EN UNA ORGANIZACIÓN QUE APRENDE

RESUMEN

Este trabajo se basó en la investigación bibliográfica de informaciones de libros de referencia y documentación específicos relacionados con las instituciones competentes responsables por frameworks, estándares y prácticas de mercado y las leyes vigentes. También se consultaron políticas, normas y notas técnicas corporativas con el fin de relevar las aplicaciones prácticas de conceptos teóricos en una gran empresa y a nivel nacional. El objetivo general de este trabajo es mostrar que es posible elevar la calidad de los servicios prestados y cumplir con los marcos regulatorios impuestos por la legislación y por las auditorías internas y externas, a través de Sistemas de TI diseñados específicamente para tal fin. La investigación permitió identificar como resultado que Cloud Identity Access Governance (IAG) se presenta como el siguiente paso en la gestión de Compliance de los Sistemas SAP, reemplazando el Gobierno, Riesgo y Cumplimiento (GRC), ya que implementa atributos de control de acceso, gestión de riesgos, controles internos, gobernanza e integridad en sistemas SAP que utilizan Cloud Computing (en la nube). Finalmente, se destaca que, con el IAG, es posible mitigar los riesgos asociados a los conflictos de segregación de funciones (SoD) y el acceso crítico a soluciones locales (en la premisa) y en la nube (en la nube). Tales soluciones tienen la característica de residir en sitios fuera de los límites físicos de las organizaciones. Y, para ello, la estrategia de Compliance debe ser diferente a la tradicional. Dado que este asunto va más allá del alcance de este trabajo de conclusión del curso, se recomienda, como continuación del estudio de esta temática, relevar los métodos que se aplican para establecer la gestión del cumplimiento en ambientes SAP en la nube con el apoyo de SAP IAG.

***Palabras clave**: Ética. SAP. GRC. Ley Sarbanes-Oxley. Organización que aprende.*

1 INTRODUÇÃO

A necessidade de integrar conceitos de governança, riscos e conformidade aos processos corporativos das companhias, devido à legislação e aos altos padrões de gestão corporativa e regulação adotados atualmente, serviu como motivação para que os sistemas de informação (*softwares*) provessem suporte para que estes conceitos se concretizassem na realização das atividades cotidianas das empresas. Neste contexto, a empresa SAP apresenta a suíte GRC - Governança, Riscos e Conformidade, que serve como um guarda-chuva e que, além de proteger o SAP ERP - *Enterprise Resource Planing*, proporciona a extensão de diversas habilidades no sentido de atender às melhores práticas de mercado com foco na produtividade e na simplicidade da obtenção de informações relativas à gestão da conformidade. Desta forma a organização aprende de maneira orgânica e integrada.

Este trabalho aborda a implementação da conformidade nos sistemas do landscape SAP por meio de sistemas de apoio que garantem a governança e a gestão de riscos corporativos. Estes sistemas de apoio também suportam a criação de controles internos eficazes. Esse tema está em voga, visto que empresas que publicam seus demonstrativos financeiros na bolsa de valores de Nova York devem estar em conformidade com as auditorias externas relativas às legislações em vigor. Além disso, evidencia a necessidade da criação de mecanismos para a detecção e prevenção de fraudes e corrupção em resposta a recentes denúncias em grandes empresas do cenário nacional e internacional.

Existem diferentes formas de realizar atividades relacionadas com Governança, Riscos e Conformidade (GRC). A empresa SAP auxilia seus clientes e parceiros a realizar esta gestão no seu *landscape* de TI. Com o intuito de preservar a performance do ERP e evitar que realize atividades que não fazem parte do seu escopo, foram criados sistemas de apoio que assumem a tarefa de gerir a GRC. Cada uma dessas atividades pode ser suportada por um sistema correspondente que provê soluções estruturadas e que atende às exigências legais, bem como a necessidades específicas do cliente, pois, dependendo de sua área econômica de atuação, determinados critérios são mais ou menos relevantes, variando de acordo com a situação.

Desta forma, o objetivo geral deste trabalho é mostrar que é possível elevar a qualidade dos serviços prestados e atender aos marcos regulatórios impostos pela legislação e pelas auditorias internas e externas, por meio de sistemas de TI concebidos especificamente para este fim. Como consequência, espera-se a elevação do nível de satisfação do cliente e a segurança em temas referentes à GRC.

A decomposição do objetivo geral deste estudo é indicada nos seguintes itens: apresentar as legislações e os temas referentes à GRC; apresentar o framework de referência; identificar sistemas SAP que auxiliam na gestão dos temas apresentados e o seu papel no *landscape* SAP. Este trabalho não pretende esgotar o assunto e, por isso, faz-se importante delimitar um escopo. Será desenvolvida pesquisa bibliográfica das informações necessárias para redigir este texto. A abrangência do levantamento será mundial para a pesquisa bibliográfica.

A relevância desse tema se apresenta tanto do ponto de vista teórico como prático. A alta gestão de uma organização pode melhorar a qualidade de seus processos de gestão da conformidade, e, como consequência, melhorar seu reconhecimento e boa reputação perante parceiros, stakeholders e acionistas, além de atender aos padrões e obrigações amplamente difundidos e adotados mundialmente. A melhoria contínua da gestão, na prática, já é suportada por diversos sistemas disponíveis no *landscape* SAP. A gestão da

conformidade é fator de vantagem competitiva que eleva o patamar de uma organização, tornando-a referência por adotar as melhores práticas de mercado e atender às legislações em vigor. Esse tipo de diferenciação atrai clientes e parceiros interessados em obter as vantagens resultantes de processos de gestão claros e que fluam com agilidade, eficiência e eficácia.

2 REFERENCIAL TEÓRICO

2.1 Lei Sarbanes-Oxley

Após os escândalos financeiros corporativos ocorridos em 2001, alguns meses após a queda das Torres Gêmeas, o mercado de capitais foi seriamente abalado por uma profunda crise de confiança nas empresas que publicam ações na bolsa de valores de Nova York (NYSE). A repercussão no mercado financeiro foi imediata e as bolsas caíram no mundo inteiro.

Esta crise foi iniciada por escândalos contábeis em grandes empresas dos Estados Unidos, tais como WorldCom, Enron e Arthur Andersen. As duas primeiras, uma do ramo de gás natural e a outra do ramo da telefonia, inflaram seus dados contábeis, passando para o mercado a impressão de que seus negócios estavam em crescimento, aumentando, assim, seu valor na bolsa de valores e, desta forma, atraindo cada vez mais investidores. A terceira era tida como empresa-modelo na área de auditoria e considerada uma das *Big Five (*Arthur Andersen, Price water house Coopers, Deloitte Touche Tohmatsu, Ernst & Young e KPMG formavam o grupo das maiores empresas de consultoria do mundo), na época., mas, pelo fato de ter corroborado com as maquiagens contábeis da Enron, teve sua reputação seriamente abalada, o que levou à sua falência.

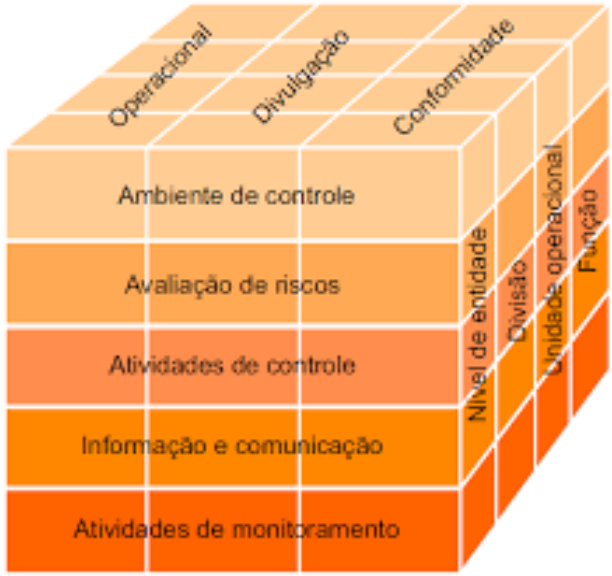
Por consequência destes fatos, foi criada a lei Sarbanes-Oxley, que segundo Borgerth (2007, p. XVI), seu grande objetivo era “restaurar o equilíbrio dos mercados por meio de mecanismos que assegurem a responsabilidade da alta administração de uma empresa sobre a confiabilidade da informação por ela fornecida”.

> A princípio, acreditava-se que a lei SOX iria atingir apenas empresas norte-americanas, ou empresas estrangeiras que comercializassem seus papéis no mercado dos Estados Unidos. No entanto, o que se verifica é um grande interesse nos efeitos desta lei por parte dos principais mercados internacionais (BORGERTH, 2007, p. XVI).

2.2 Coso

Conforme Singleton *et al.* (2008), o *Commitee of Sposoring Organizations of Treadway Commision* (COSO) indica as áreas de interesse que são relevantes para a auditoria de sistemas. Segundo Campos e Santos (2012, p. 37), este *Framework* pode ser utilizado na mitigação de riscos e auxiliar na eficácia dos controles internos. O COSO é um processo. Esse processo é constituído por cinco ambientes que estão inter-relacionados entre si. Conforme a Figura 1, os cinco elementos do COSO são: (a) Ambiente de controle; (b) Avalição de Riscos; (c) Atividades de Controle; (d) Informação e Comunicação; e (e) Atividades de Monitoramento.

Figura 1 - Modelo COSO I – Controle Interno – Estrutura Integrada

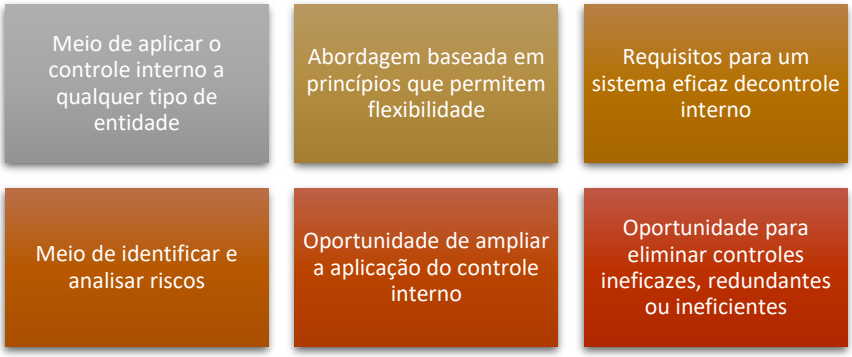


Fonte: COSO (2013).

> O controle interno auxilia as entidades a alcançar objetivos importantes e a sustentar e melhorar o seu desempenho. O material *Internal Control – Integrated Framework* (Estrutura) do COSO permite que as organizações desenvolvam, de forma efetiva e eficaz, sistemas de controle interno que se adaptem aos ambientes operacionais e corporativos em constante mudança, reduzam os riscos para níveis aceitáveis e apoiem um processo sólido de tomada de decisões e de governança da organização (COSO, 2013, p. 4).

Para a administração e a estrutura de governança, o *framework* COSO proporciona os benefícios apresentados na Figura 2.

Figura 1 - Benefícios do framework COSO



Fonte: COSO (2013).

2.3 Governança

Segundo o IBGC (2018)

> a governança corporativa é o sistema pelo qual as empresas e demais organizações são dirigidas, monitoradas e incentivadas, envolvendo os relacionamentos entre sócios, conselho de administração, diretoria, órgãos de fiscalização e controle e demais partes interessadas. As boas práticas de governança corporativa convertem princípios básicos em recomendações objetivas, alinhando interesses com a finalidade de preservar e otimizar o valor econômico de longo prazo da organização, facilitando seu acesso a recursos e contribuindo para a qualidade da gestão da organização, sua longevidade e o bem comum (IBGC, 2018, p. 20).

Os princípios da governança corporativa estão descritos na Figura 3.

Figura 2 - Princípios básicos da Governança corporativa

Fonte: ELETROBRAS (2017).

2.4 Risco

Pode-se entender o Risco como uma medida de incerteza, uma vez que pode representar oportunidades ou ameaças ao alcance dos objetivos do negócio. Um bom gerenciamento de riscos é

> um processo que visa identificar e mensurar eventos que possam causar perdas ou desvios de objetivos da organização, de maneira a mitigá-lo pelo emprego balanceado de recursos materiais, tecnológicos, alocação e capacitação de capital intelectual, criação e/ou redefinição de normas e procedimentos, estabelecimento de mecanismo de controle e de gestão, gerando o desenvolvimento de uma cultura organizacional robusta e compatível com o “Apetite ao Risco” da organização (ELETROBRAS, 2018).

Segundo o COSO - *Enterprise Risk Management* (ERM) (2014, p. 5), o gerenciamento de riscos envolve tanto o entendimento “das implicações da estratégia e a possibilidade de seu eventual desalinhamento, como o gerenciamento dos riscos associados aos objetivos de negócios”. A Figura 4 ilustra essas considerações no contexto de missão, visão e valores fundamentais, como determinantes dos direcionadores estratégicos e da performance da entidade.

Figura 3 - Missão, visão e valores fundamentais do COSO ERM

Fonte: COSO (2013).

A gestão do risco consiste no “emprego coordenado dos recursos e ferramentas de governança e de gestão para alinhar objetivos, ações e processos com as práticas de gestão de riscos. Tais práticas são capazes de proporcionar resultados alinhados com as expectativas dos acionistas e da organização em termos de apetite e ‘tolerância ao risco’“

(ELETROBRAS, 2018). Uma das ferramentas utilizadas é a Matriz de risco, mostrada na Figura 5.

Figura 4 - Matriz de Riscos

		PROBABILIDADE				
		INCOMUM	OCASIONAL	COMUM	FREQUENTE	QUASE CERTA
IMPACTO	CATASTRÓFICA	MÉDIO	ALTO	ALTO	ALTO	ALTO
	CRÍTICA	MÉDIO	MÉDIO	ALTO	ALTO	ALTO
	MODERADA	BAIXO	MÉDIO	MÉDIO	MÉDIO	ALTO
	BAIXA	BAIXO	BAIXO	MÉDIO	MÉDIO	MÉDIO
	DESPREZÍVEL	BAIXO	BAIXO	BAIXO	MÉDIO	MÉDIO

Fonte: ELETROBRAS (2018).

> As falhas originadas de riscos operacionais devem ser registradas em base de dados única para identificação, análise das principais causas de perdas operacionais e monitoramento, permitindo uma atuação objetiva na correção dos problemas e nos reportes aos responsáveis pelo processo e à Alta Administração (ABRAPP, 2010).

Uma área de gestão de riscos é responsável pelo processo da análise dos riscos, por suas grandezas e impactos sobre as atividades, permitindo o desenvolvimento de planos de ação para a correção de eventual ocorrência de perda (ABRAPP, 2010).

2.5 Conformidade (*Compliance*)

O termo *compliance*, traduzido para o português como ‘conformidade’, explicita o “quanto a organização está adequada a normas, legislações, procedimentos e boas práticas, recomendáveis ou obrigatórias”. “Gerenciar *compliance* é estar apto a manter a organização adequada a estes requisitos através da implantação, do monitoramento e da auditoria de controles, de modo a garantir e comprovar a adequação a eles” (ELETROBRAS, 2018).

Segundo Serat (2017, p.58), uma organização que aprende valoriza o papel que a aprendizagem pode desempenhar no desenvolvimento da eficácia organizacional. Um importante desafio para as organizações, na chamada 4ª revolução industrial, é desenvolver habilidades referentes à conformidade, à ética, e sobre as tecnologias que provêm suporte a tais competências empresariais. Desta forma, o conceito de organização que aprende é desenvolvido por meio de pensamento sistêmico, e é possível aprimorar os processos produtivos, com o objetivo maior de manter a empresa perene e competitiva frente ao mercado com base em valores que trazem benefícios para a sociedade em geral.

Uma área responsável pela conformidade empresarial deve realizar ações contínuas para a promoção da ética e para o cumprimento de leis e regulamentos estabelecidos para o negócio e para as atividades empresariais. Para manter a empresa em conformidade, é necessário que esta previna e detecte discrepâncias entre as leis e regulamentações, internas ou externas, que existam nos processos da empresa e em seus negócios, resultantes da ação de seus empregados ou outros agentes (ELETROBRAS, 2015).

A Figura 6 sugere alguns princípios que regem as políticas relativas à implantação da conformidade em uma organização.

Figura 5 - Princípios que regem as políticas de conformidade

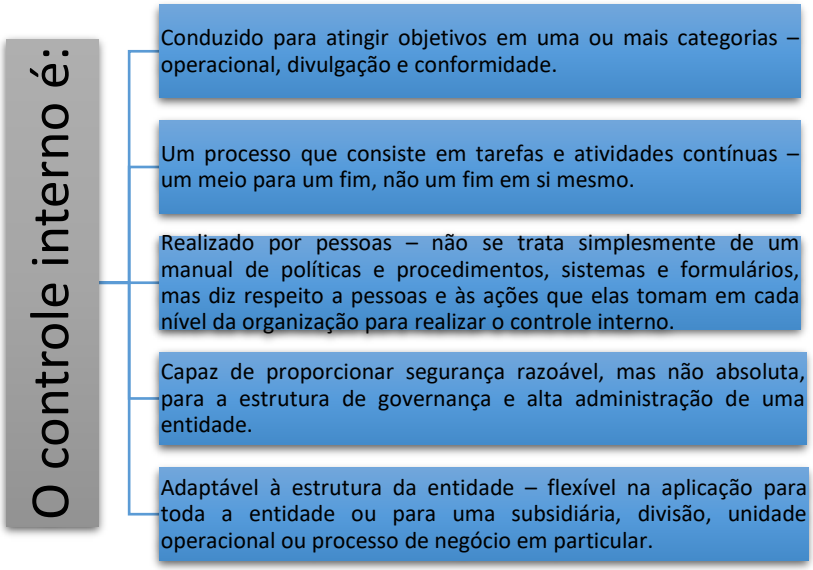
Princípios
Repudiar ações de fraude e corrupção direta ou indireta
Repudiar atos em desacordo com as Leis Anticorrupção
Utilizar critérios e mecanismos éticos e íntegros para estabelecer os relacionamentos com terceiros
Agir com transparência nas relações com órgãos de controle e fiscalização
Assegurar a integridade dos livros, registros e contas contábeis
Incentivar o reporte imediato de desvios éticos e de integridade
Assegurar a não retaliação aos denunciantes
Proibir doações para candidatos e partidos políticos

Fonte: ELETROBRAS (2015).

2.6 Controles Internos

Segundo o COSO (2013, p. 7), controle interno é um “processo conduzido pela estrutura de governança, pela administração e por outros profissionais da entidade”, e desenvolvido “para proporcionar segurança razoável no que diz respeito à realização dos objetivos relacionados a operações, divulgação e conformidade”. A Figura 7 demonstra alguns conceitos fundamentais.

Figura 6 - Conceitos fundamentais de Controles Internos segundo o COSO 2013



Fonte: COSO (2013).

Atividades de controle são “ações estabelecidas por meio de políticas e procedimentos que ajudam a garantir o cumprimento das diretrizes determinadas pela

administração para mitigar os riscos à realização dos objetivos". A segregação de funções é necessária desenvolvimento das atividades de controle. Nos casos em que a segregação de funções seja impraticável, a administração deverá desenvolver atividades alternativas de controle (ELETROBRAS, 2018).

2.7 Integridade corporativa

Segundo a CGU (2015, p. 8), um programa de integridade corporativa é um "conjunto de medidas que objetiva prevenir, detectar e remediar a ocorrência de fraude e corrupção nas empresas", pensado e implementado de forma sistêmica, com aprovação da alta direção, e sob coordenação de uma área ou pessoa responsável. Portanto, visando à realização de tais atividades e ao estabelecimento de políticas, medidas e normas relativas ao tema, foram criadas, para a alta direção, seus colaboradores, intermediários, fornecedores e prestadores de serviço, estruturas organizacionais em empresas Estatais. Um programa de integridade corporativa é composto por 5 passos relacionados (Figura 8).

Figura 7 - Visão integrada de um Programa de Integridade

Fonte: CGU (2015).

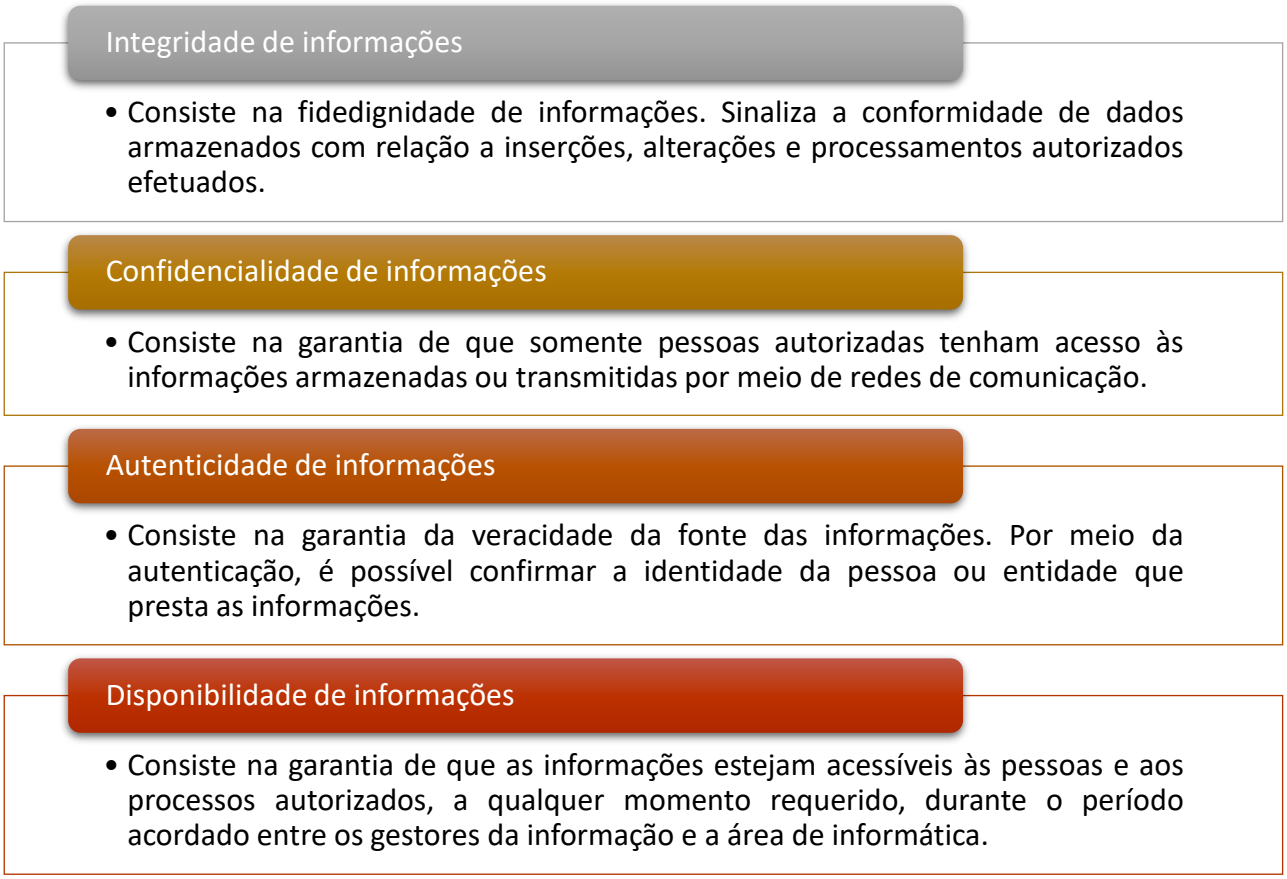
Desta forma, é possível prestar apoio ao gestor em questões de integridade e estabelecer uma boa governança que confere às outras atividades empresariais legitimidade, confiabilidade e eficiência. O objetivo é que existam instrumentos para identificar e reparar atos ilícitos e desvios de conduta, evitando, assim, danos à imagem da empresa e prevenindo perdas financeiras antes que desvios aconteçam.

2.8 Segurança da informação

> É importante zelar pela segurança de informações, pois a informação é um ativo muito importante para qualquer instituição, podendo ser considerada, atualmente, o recurso patrimonial mais crítico. Informações adulteradas, não disponíveis, sob o conhecimento de pessoas de má-fé ou de concorrentes, podem comprometer significativamente não apenas a imagem da instituição perante terceiros, como também o andamento dos próprios processos institucionais. Pode-se inviabilizar a continuidade de uma instituição se não for dada a devida atenção à segurança de suas informações (TCU, 2012, p. 10).

Segundo o TCU (2012, p. 9), a segurança de informações "visa garantir a integridade, a confidencialidade, a autenticidade e a disponibilidade das informações processadas pela instituição". A Figura 9 contém detalhes destes conceitos.

Figura 8 - Conceitos da Segurança da Informação



Fonte: TCU (2012).

Os controles de acesso lógico são um conjunto de procedimentos e medidas que possuem o objetivo de proteger dados, programas e sistemas contra tentativas de acesso não autorizadas realizadas por pessoas ou outros programas de computador.

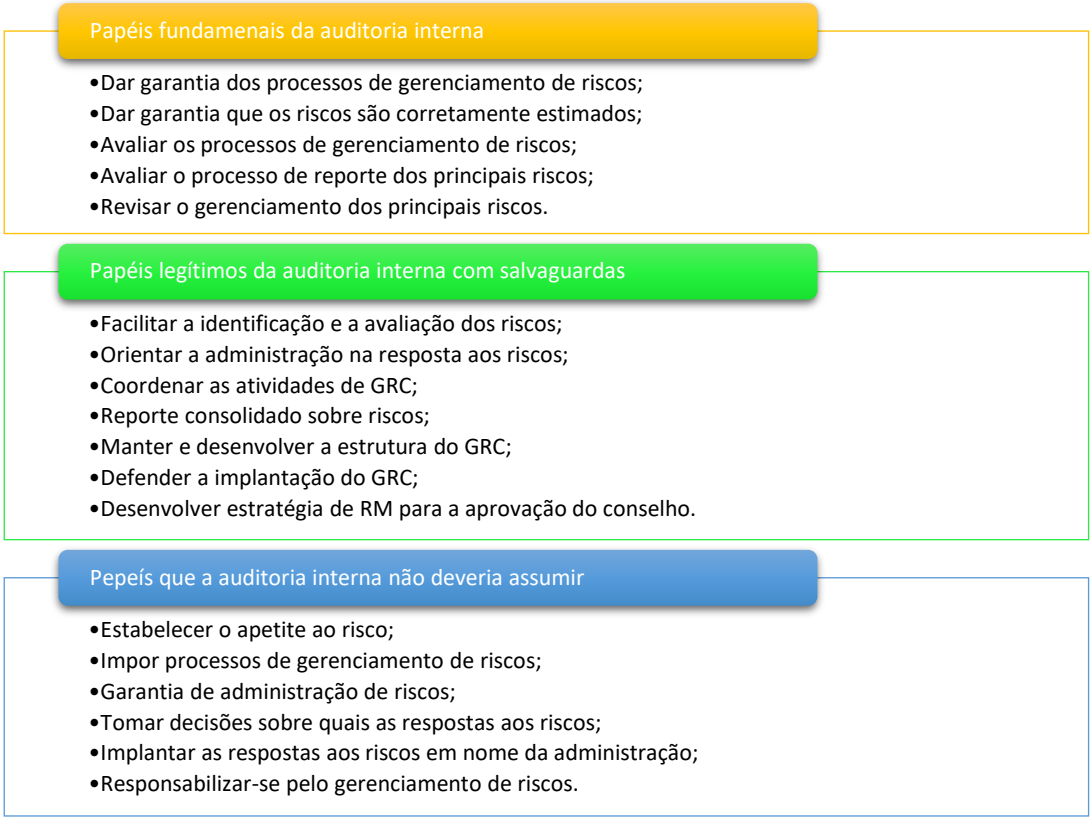
> A proteção aos recursos computacionais baseia-se nas necessidades de acesso de cada usuário, enquanto a identificação e a autenticação do usuário (confirmação de que o usuário realmente é quem ele afirma ser) são feitas normalmente por meio de um identificador de usuário (ID) e uma senha durante o processo de *logon* no sistema (TCU, 2012, p. 17).

Política de segurança de informações é um "conjunto de diretrizes estabelecidas que determinam as linhas mestras que devem ser seguidas pela instituição para que sejam assegurados seus recursos computacionais e suas informações" (TCU, 2012, p. 10).

2.9 Auditoria interna

Segundo o IAA (2009, p. 4), a auditoria interna é uma atividade independente de avaliação (*assurance*) e de consultoria. Seu papel fundamental em relação ao *Governance Risk Compliance* (GRC) é "fornecer avaliação objetiva (*objective assurance*) ao conselho quanto à eficácia do gerenciamento de riscos". Os diversos papéis que a auditoria interna pode assumir são os descritos na Figura 10.

Figura 9 - O papel da auditoria interna no GRC



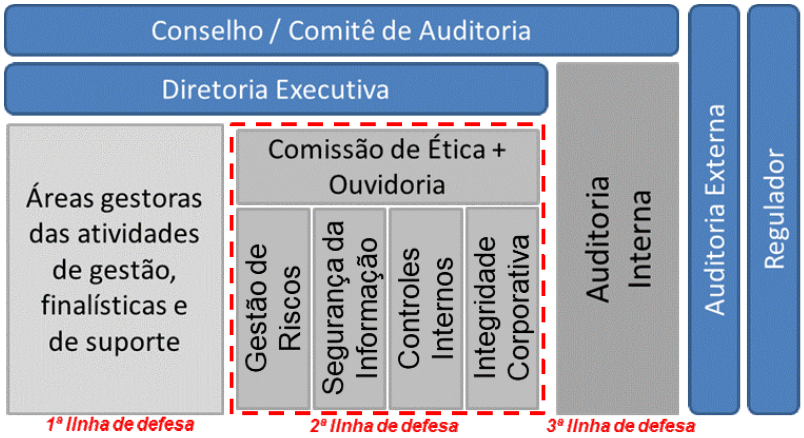
Fonte: IAA (2009).

> A auditoria interna pode prestar serviços de consultoria que melhorem os processos de governança, gerenciamento de riscos e controle de uma organização. A extensão da consultoria por um auditor interno no GRC irá depender dos outros recursos, internos e externos, disponíveis ao conselho e da maturidade de risco da organização (IAA, 2009, p. 5).

2.10 As três linhas de defesa

O modelo de 3 Linhas de Defesa é uma “forma simples e eficaz de melhorar a comunicação do gerenciamento de riscos e controles por meio do esclarecimento dos papéis e responsabilidades essenciais”. O modelo, representado na Figura 11, apresenta “um novo ponto de vista sobre as operações, ajudando a garantir o sucesso contínuo das iniciativas de gerenciamento de riscos, e é aplicável a qualquer organização, não importando seu tamanho ou sua complexidade” (ELETROBRAS, 2018, p. 29).

Figura 10 - As três linhas de defesa



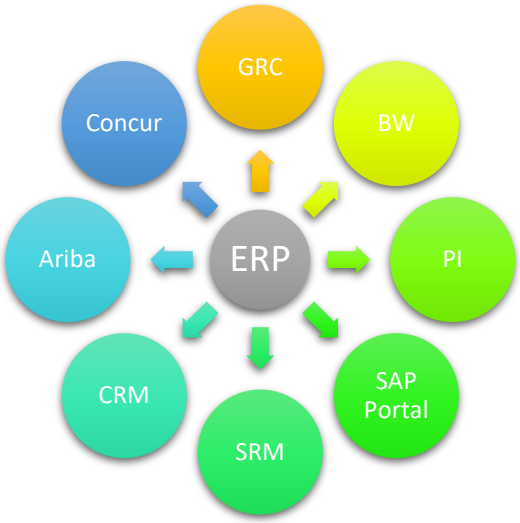
Fonte: ECIIA/FERMA (2010).

> Embora os órgãos de governança e a alta administração não sejam considerados dentre as 3 “linhas” desse modelo, nenhuma discussão sobre sistemas de gerenciamento de riscos estaria completa sem considerar, em primeiro lugar, os papéis essenciais dos órgãos de governança (i.e., conselho de administração e órgãos equivalentes) e da alta administração (ELETROBRAS, 2018, p. 29).

2.11 SAP - Governança, risco e conformidade

O sistema de gestão empresarial SAP, também conhecido como *Enterprise Resource Planing* - ERP SAP, é um *software* de sistema integrado de gestão, de origem alemã, criado no início da década de 1970, com o propósito de dar suporte a diversos processos de negócio das organizações. Ao longo do tempo, foram surgindo diversos outros sistemas para auxiliar e até mesmo estender as funcionalidades do ERP. Com isso, surgiu a arquitetura *Netweaver (*Plataforma computacional principal tecnologia da empresa de *software* **SAP***),* que serve de base para todo o ecossistema de *softwares* que realiza desde atividades de gestão da segurança até plataformas localizadas na nuvem, conforme exemplificado na Figura 12.

Figura 11 - Landscape SAP

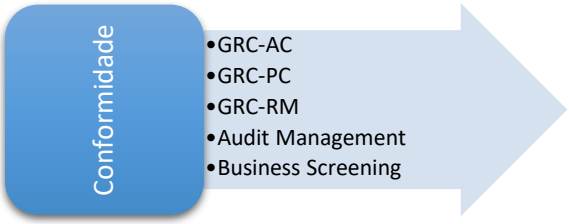


Fonte: ECIIA/FERMA (2010).

Hoje em sua última versão, o ERP da SAP é chamado de S/4 e é suportado por uma tecnologia de banco de dados *in memory (*Computação em memória*)* chamado HANA (*High Performance Analytic Appliance*). Com o advento desta tecnologia, foi possível aumentar em grande escala a velocidade de processamento dos novos sistemas, possibilitando o uso da tecnologia em aplicações de *Big Data* e *Cloud.* Uma das primeiras aplicações SAP a se beneficiar dessa inovação foi o sistema de *Business Warehouse* - ferramenta usada para *Business Intelligence* da SAP. Hoje, a empresa foca seus esforços em oferecer serviços na nuvem e aplicações voltadas para o acesso na internet com um novo desenho de *front-end (*Interface de interação entre o usuário e o sistema*),* que leva em consideração uma boa experiência de interação com usuário.

Conforme os conceitos apresentados nas outras seções, torna-se evidente que as áreas que são responsáveis pela *compliance* das empresas necessitam de suporte e automatização para realizar a gestão adequada dos processos relativos a controles internos, segurança da informação, auditoria interna, integridade corporativa, governança, risco e conformidade. Os sistemas SAP estão aderentes aos conceitos de conformidade, uma vez que o ERP é suportado por outros sistemas que cumprem este papel. A Figura 13 exemplifica essa realidade.

Figura 12 - Conformidade aplicada ao landscape SAP



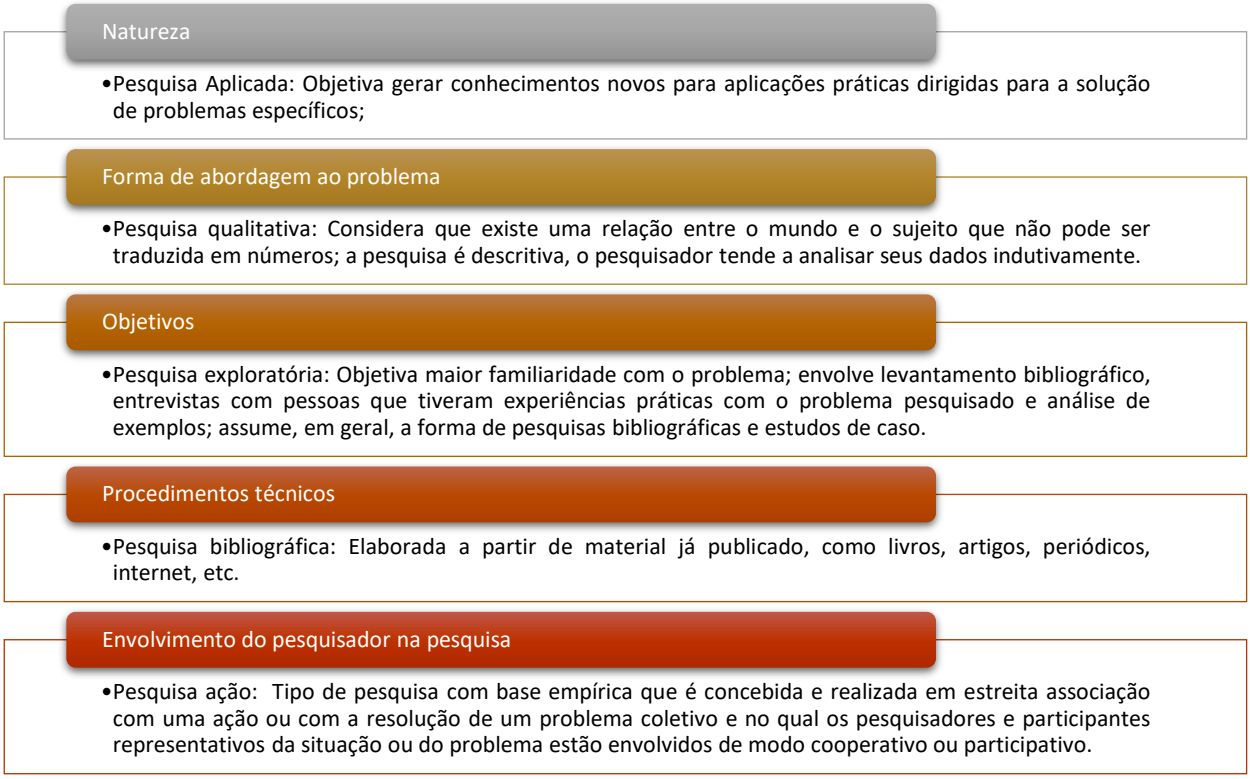
Fonte: ECIIA/FERMA (2010).

3 METODOLOGIA

Este trabalho baseou-se na pesquisa bibliográfica de informações em livros de referência e em documentações específicas relativas às instituições competentes responsáveis por *frameworks*, padrões e práticas de mercado e às legislações em vigor. Também foram consultadas políticas, normas e notas técnicas corporativas com o intuito de levantar as aplicações práticas de conceitos teóricos em uma empresa de grande porte e âmbito nacional. Por fim, foram realizadas buscas no Google acadêmico e consultada a documentação da SAP.

Segundo Gil (2002, p. 57), pode-se definir pesquisa como o "procedimento racional e sistemático que tem como objetivo proporcionar respostas aos problemas que são propostos". As classificações do tipo de pesquisa adotada neste trabalho têm o objetivo de contextualizar o leitor na busca pelo conhecimento e balizar seus objetivos quanto ao que está sendo apresentado pelo autor. Portanto, esta pesquisa está classificada conforme a Figura 14 a seguir:

Figura 13 - Classificação do tipo de pesquisa



Fonte: GIL (2002).

A SAP possui a suíte GRC, que proporciona ao seu *landscape* a gestão de acesso lógico baseada em perfis de acesso, e a identificação de riscos de ação crítica e de segregação de funções (SoD), bem como sua mitigação por meio da associação de controles compensatórios.

Esta suíte também pode realizar a gestão de processos corporativos e a gestão dos riscos nos níveis estratégicos e operacionais tanto de forma qualitativa quanto de forma quantitativa.

A gestão das atividades de Auditoria também é contemplada nesta suíte. Com uma fonte de informações única, é possível estabelecer sinergia e a redução de tempo, custos e recursos humanos nesta atividade, principalmente em empresas públicas e que possuem controles SOX em seus processos de negócio.

Adicionalmente, há ainda um sistema que pode realizar a predição de atividades fraudulentas, baseadas em regras pré-determinadas pela área de negócio.

A implementação do SAP GRC Access Control visa instituir e/ou aperfeiçoar controles para o estabelecimento de governança e conformidade contínua no ambiente sistêmico, no que tange ao processo de administração de usuários e perfis de acesso.

Composto de quatro módulos, o Access Control suporta processos de gestão da conformidade relativos à concessão de acesso, à segregação de funções, ao acesso emergencial e à Manutenção de perfis de acesso, conforme a Figura 15.

Numa implementação do AC, conforme apresentado, seria mais recomendado que a área de segurança da informação fosse sua gestora, devido às características de atividade de controle de acesso lógico aos sistemas SAP.

Os benefícios esperados com a adoção do *Access Control* serão explicitados a seguir:

- aderência dos processos a padrões estabelecidos com o uso de fluxo de aprovação, que pode ser configurado com base nos requerimentos e políticas vigentes de TI, *compliance*,
- controles internos e/ou gestão de riscos, de forma a padronizar as solicitações de acessos nas áreas de negócio;
- mitigação dos riscos de acesso ao ambiente;
- redução de custo de operação para a área de TI, pois o processo de aprovação que de ser manual;
- suporte às áreas de auditoria e de negócio por meio de relatórios e *dashboards*;
- definição de papéis e responsabilidades na organização, pois há diversos papéis (*profile owner/risk owner/control owner*) que necessitam estar configurados no sistema.

Todos estes fatores otimizam o tempo de trabalho das áreas de auditoria e de controles internos, 2ª e 3º linhas de defesa das empresas.

Figura 14 - Processos básicos do GRC-AC

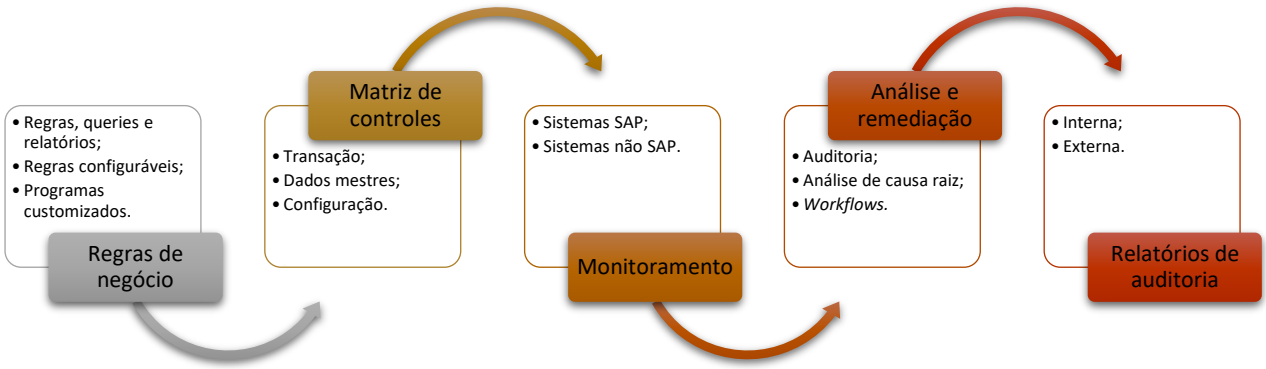
Fonte: ECIIA/FERMA (2010).

O GRC PC possibilita a implementação de um processo de controle automatizado e eficiente, e está baseado em conceitos de monitoramento contínuo de controles. Normalmente, a gestão destes controles fica a cargo da área de controles internos das empresas.

Após a identificação dos riscos relevantes para uma companhia, pode ser configurada a automação de alguns controles-chave dentro dos processos críticos, que sejam objetos das políticas e regulamentações da empresa.

Tendo como base este conjunto de riscos e controles automatizados, há a possibilidade de monitorar configurações, dados mestres e transacionais dos sistemas SAP, tendo como padrão um conjunto lógico de critérios e/ou regras de negócio, a fim de identificar exceções e possibilitando o encaminhamento dos planos de ação num ciclo ao longo do ano. A Figura 16 descreve uma proposta do processo de gestão dos controles.

Figura 15 - Processo básico do GRC-PC



Fonte: ECIIA/FERMA (2010).

A aplicação básica do PC é a gestão de todos os controles compensatórios corporativos, sendo eles da matriz de objetivo e controle SOX ou não, relativos aos riscos levantados nos processos de negócio. Desta forma, há ganhos de escala na qualidade e na acurácia das informações que estão disponíveis para que a alta gestão tome decisões mais precisas.

As áreas de gestão de riscos das companhias possuem um aliado para a gestão dos seus processos. O SAP GRC Risk Management possibilita maior controle dos principais componentes do modelo de gerenciamento de riscos: governança de riscos, gestão de riscos, integração de riscos e desempenho do processo de negócio. O processo de gestão dos riscos prevê as atividades de planejamento, identificação, análise, resposta e monitoração, conforme a Figura 17.

Figura 16 - Processo básico de gestão do risco no GRC-RM

Fonte: ECIIA/FERMA (2010).

Com o RM, é possível controlar o ciclo de vida dos riscos corporativos por meio de um *workflow* customizável para atender aos processos de qualquer empresa. Há a automatização do processo de avaliação dos riscos com o uso de pesquisas colaborativas e *Key Risk Indicators* (*KRI*) -Indicadores Chave de Risco, em conjunto com a simulação de riscos e com o acompanhamento realizado via mapa de riscos (*heatmap* - Representação gráfica de dados onde os valores individuais contidos em uma matriz são representados como cores). Os riscos podem ser configurados com seus objetivos

corporativos e suas atividades relacionadas, bem como com sua classificação, seus limiares de tolerância, estratégia de resposta, etc.

O GRC AM permite adotar uma forma mais simples para criar, rastrear e gerenciar as atividades típicas das áreas de Auditoria das companhias. Com esta ferramenta, é possível capturar a documentação de auditoria instantaneamente, até mesmo com dispositivos móveis e ferramentas de arrastar e soltar. O AM disponibiliza relatórios padronizados com modelos pré-estabelecidos e do rastreamento automatizado de pontos de auditoria. A Figura 18 representa o processo básico de gestão automatizada da Auditoria.

Figura 17 - Processo básico de gestão da auditoria no GRC-AM

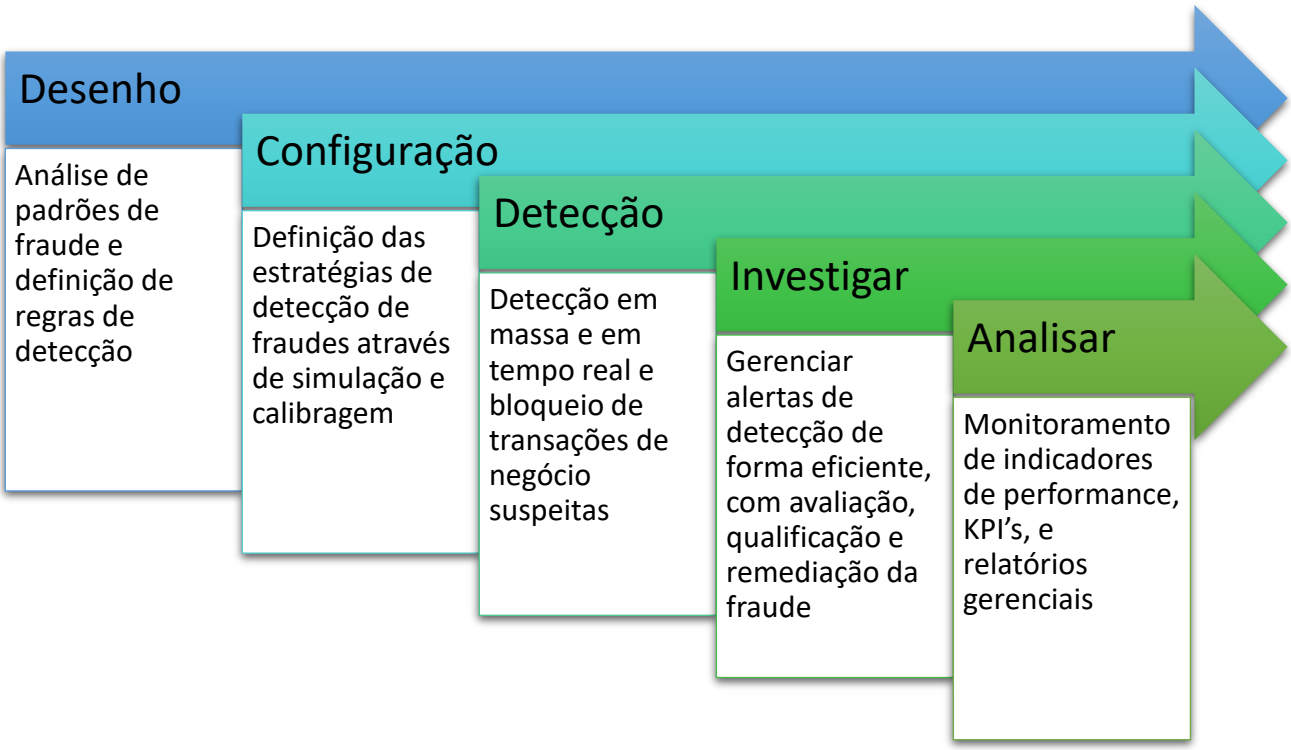
Fonte: TCU (2014).

Com o uso do *Audit Management*, os auditores internos podem fornecer avaliações abrangentes aos órgãos de governança e à alta administração de forma mais rápida, precisa e simples, baseadas nas informações disponíveis no sistema, aumentando seu nível de independência e objetividade dentro da organização.

O GRC BIS (*Business Integrity Screening*) provê, para as áreas de Integridade Corporativa, meios para a detecção de padrões suspeitos mais comuns, bem como de violações de políticas internas das organizações. Com esta ferramenta, é possível descobrir

situações de conflitos de interesse, a existência de fornecedores fantasmas, a realização de pagamentos suspeitos, a existência de faturas duplicadas e o fracionamento intencional de pedidos de compra etc. A Figura 19 exemplifica o processo típico de detecção de fraudes do BIS.

Figura 18 - Processo básico de gestão da integridade no GRC-BIS



Fonte: TCU (2014).

4 ANÁLISE E DISCUSSÃO DOS RESULTADOS

O objetivo geral foi alcançado, pois este estudo apresentou de forma ampla os conhecimentos mínimos para que o leitor possa entender as origens da necessidade do estabelecimento de um processo de gestão de governança, dos riscos e da conformidade (GRC). Além disso, demonstramos que os sistemas SAP são suportados por uma suíte que oferece um arcabouço de funcionalidades.

O primeiro objetivo específico foi abordado e atingido com um levantamento bibliográfico centrado na apresentação de conceitos em legislações, manuais e códigos, nos quais se visitam os motivos da obrigatoriedade da gestão da *compliance*. Isso se dá tanto por motivos de imposição do governo, como dos mercados de valores e, até mesmo, por uma questão de ética, transparência e sustentabilidade econômica, que são valores relevantes no ambiente empresarial.

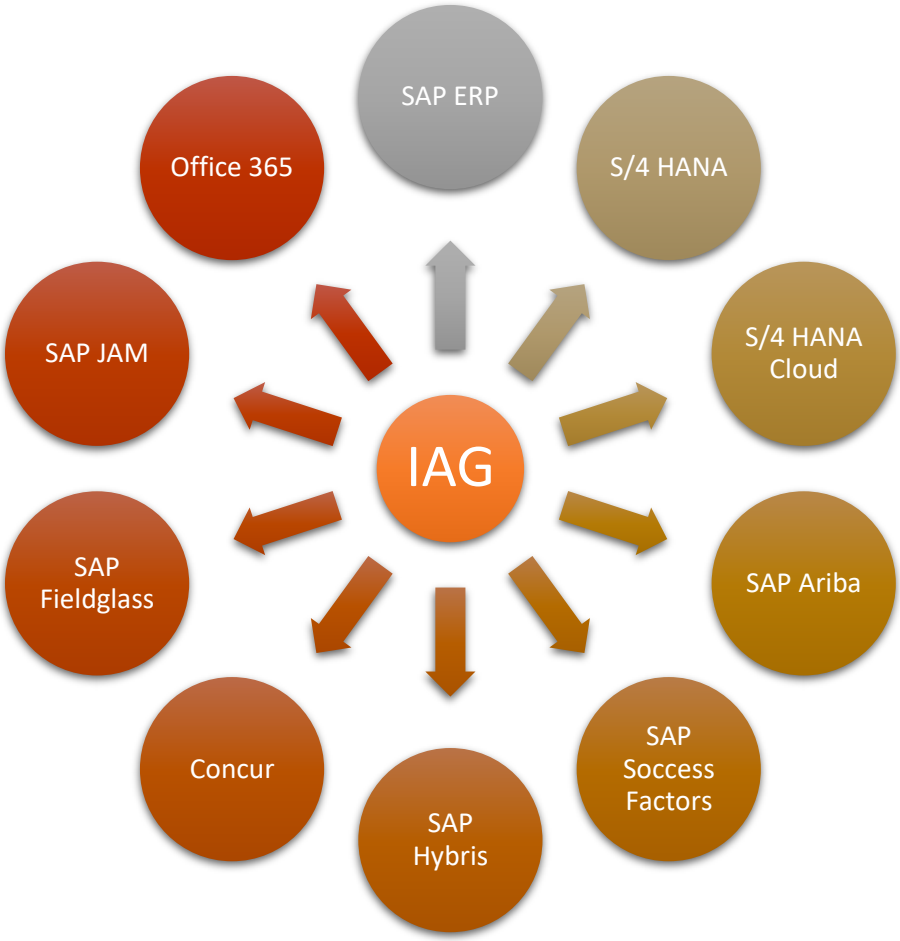
O segundo objetivo específico é coberto pela apresentação do COSO e do COSO-ERM, que são as bases para a implementação da cultura de gestão de controles internos e de riscos. COSO e COSO-ERM favorecem os trabalhos das auditorias internas e das auditorias externas, corroborando para um ambiente de conformidade maduro e estável nas organizações.

O terceiro objetivo, que é identificar sistemas SAP que auxiliam na gestão dos temas apresentados, é realizado por meio da apresentação da suíte GRC, formada pelos sistemas GRC-AC, GRC-PC, GRC-RM, GRC-AM e BIS. Com estes sistemas, é possível dar suporte

a todos os processos de uma área de conformidade de forma integrada. Cada um deles possui um processo interno que ajuda a estruturar as atividades das áreas de Segurança da Informação, Controles Internos, Gestão de Riscos, Auditoria e Conformidade. Há uma relação direta entre a aplicação destas ferramentas, o processo e a solução de diversos *gap*[i] identificados em controles existentes nas Matrizes de objetivos e controles das empresas que são auditadas sob os critérios da SOX.

O IAG (*Cloud Identity Access Governance)* se apresenta como o próximo passo na gestão da *Compliance* dos sistemas SAP, em substituição à suíte GRC, pois ele implementa atributos de controle de acesso, gestão de riscos, controles internos, governança e integridade em sistemas SAP que se utilizam da Computação em Nuvem (*in cloud*) - utilização da memória e da capacidade de armazenamento e cálculo de computadores e servidores compartilhados e interligados por meio da Internet. Além das funcionalidades de *Single Sign On* (SSO) – Recurso computacional que possibilita que um usuário tenha acesso a mais de um serviço sem necessitar preencher um cadastro completo a cada nova aplicação – basta autenticar e utilizar um cadastro que já exista anteriormente., de criação de usuários e de atribuição de perfis, o IAG suporta as conexões descritas na Figura 20.

Figura 19 - Conexões do IAG com outros



Fonte: COSO (2013).

5 CONSIDERAÇOES FINAIS

Este estudo ocorre em um momento do nosso país em que a corrupção e as fraudes tomaram grande vulto na mídia, devido a diversos escândalos financeiros nos quais

políticos, a troco de propinas oriundas de grandes empresas, oferecem vantagens utilizando a máquina pública em benefício próprio.

Neste cenário caótico, onde há uma séria crise de confiança nas instituições governamentais, a existência de sistemas que propiciam a gestão da conformidade de forma eficaz e transparente torna-se matéria de grande relevância, visto que estes sistemas auxiliam a alta gestão das empresas, em especial das empresas estatais, a se manterem no caminho da licitude.

A gestão do acesso lógico, dos riscos, da conformidade e dos controles internos faz parte das linhas de defesa que estão disponíveis para oferecer robustez e eficiente combate aos processos empresariais escusos. Sob a ótica do conceito da organização que aprende e através destas ferramentas, é possível estabelecer uma cultura de *compliance,* que é disseminá-la por toda a companhia, além de estabelecer, em suas relações internas e externas, ética e integridade por meio da governança preconizada por políticas e normas internas e externas. Portanto, a união destes três fatores – pessoas, processos e sistemas computacionais – formam três pilares que propiciam a elevação no nível de maturidade da gestão da conformidade nas empresas no Brasil.

Com o IAG, é possível mitigar riscos associados a conflitos de *SoD* e ao acesso crítico para soluções locais (*on premise*) e na nuvem (*in cloud*). Tais soluções possuem a característica de residirem em *sites* fora das fronteiras físicas das organizações. E, para isto, a estratégia de *Compliance* deve ser diferente da tradicional. Como este assunto extrapola o escopo deste trabalho de conclusão de curso, é recomendado, como continuação do estudo deste tema, o levantamento dos métodos que são aplicados para estabelecer a gestão da conformidade em ambientes SAP *in cloud* com o suporte do SAP IAG.

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DAS ENTIDADES FECHADAS DE PREVIDÊNCIA COMPLEMENTAR (ABRAPP). **Manual de Controles Internos/Comissão Técnica Nacional de Governança.** São Paulo: 2010.

BRASIL. Tribunal de Contas da União. **Boas práticas em segurança da informação.** 4. ed. – Brasília : TCU, Secretaria de Fiscalização de Tecnologia da Informação, 2012. Disponível em: http://www4.planalto.gov.br/cgd/assuntos/publicacoes/2511466.pdf. Acesso em: 10 out. 2018.

BORGUERTH, V. M. C. **SOX**: Entendendo a Lei Sarbanes-Oxley: Um caminho para a informação transparente. São Paulo: Cengage Learning, 2008.

CAMPOS, F. C.; SANTOS, G. S. **Governança na Oferta de Serviço**: modelo de *outsourcing* para provedores de tecnologia da informação. São Paulo: Atlas, 2012.

COMMITTEE OF SPONSORING ORGANIZATIONS (COSO). **Internal Control:** Integrated Framework. New York, 2013.

COMMITTEE OF SPONSORING ORGANIZATIONS (COSO). **Enterprise Risk Management:** Integrated Framework. California, 2013.

CONTROLADORIA-GERAL DA UNIÃO (CGU). **Guia de Implantação de Programa de Integridade nas Empresas Estatais.** Brasília, 2015. Disponível em: http://eletrobrasalagoas.com/wp-content/uploads/arquivos/Guia%20de%20Implantacao%20de%20Programa%20de%20Integridade%20nas%20Empresas%20Estatais.pdf . Acesso em: 10 out. 2018.

ELETROBRAS. **Manual de *Compliance* Referente às Leis Anticorrupção.** Rio de Janeiro, 2015. Disponível em: < https://www.eletronuclear.gov.br/Quem-Somos/Governanca/Documents/Manual-do-Programa-de-Compliance.pdf> . Acesso em 11 jul. 2018.

ELETROBRAS. **Manual de Melhores Práticas da Certificação SOX da ELETROBRAS**. Rio de Janeiro: 2017.

ELETROBRAS. **Política Anticorrupção das Empresas ELETROBRAS.** Rio de Janeiro: 2018. Disponível em: http://eletrobras.com/pt/Paginas/Conformidade-e-Praticas-Anticorrupcao.aspx. Acesso em: 14 nov. 2018.

GIL, Antônio Carlos. **Como elaborar projetos de pesquisa**. 4. ed. São Paulo: Atlas, 2002.

INSTITUTO BRASILEIRO DE GESTÃO CORPORATIVA (IBGC). **Código das melhores práticas de governança corporativa.** São Paulo: 2015. Disponível em: https://conhecimento.ibgc.org.br/Paginas/Publicacao.aspx?PubId=21138. Acesso em: 6 ago. 2018.

THE INSTITUTE OF INTERNAL AUDITORS. **Declaração de Posicionamento do IIA:** O Papel da Auditoria Interna no Gerenciamento de Riscos Corporativo**.** Flórida: 2009. Disponível em: https://iiabrasil.org.br/korbilload/upl/ippf/downloads/declarao-de-pos-ippf-00000001-21052018101250.pdf. Acesso em: 14 out. 2018.

SERAT, O. **Knowledge Solutions Tools, Methods, and Approaches to Drive Organizational Performance.** Mandaluyong: Asian Development Bank, 2017.

SINGLETON, T.W. The COSO Model: How IT Auditors Can Use IT to Measure the Effectiveness on Internal Controls. **Information Systems Control Journal**, v. 1, p. 9-10, 2008.

TRIBUNAL DE CONTAS DA UNIÃO (TCU). **Referencial básico de governança aplicável a órgãos e entidades da administração pública /** Tribunal de Contas da União. 2 ed. Brasília: Secretaria de Planejamento, Governança e Gestão, 2014. Disponível em: https://portal.tcu.gov.br/lumis/portal/file/fileDownload.jsp?inline=1&fileId=8A8182A24F0A728E014F0B34D331418D. Acesso em: 08 set. 2018.

[i] Resultados dos levantamentos das diferenças entre os controles existentes no processo de elaboração dos relatórios financeiros e os controles da estrutura de controle interno (p.ex., COSO) selecionada pela Alta Administração da Empresa.