Revista Eletrônica de Estratégia & Negócios

ISSN 1984-3372
DOI: 10.19177/reen.v12e3201975-96

GOVERNANÇA, RISCOS E CONFORMIDADE: MODELO INTEGRADO UTILIZANDO A MODELAGEM DE PROCESSOS DE NEGÓCIOS

GOVERNANCE, RISKS AND COMPLIANCE: INTEGRATED MODEL USING BUSINESS PROCESS MODELING

GOBERNANZA, RIESGOS Y CUMPLIMIENTO: MODELO INTEGRADO UTILIZANDO MODELOS DE PROCESO EMPRESARIAL

Daniel Massiére Birchal
Mestre em Engenharia e Gestão de Processos e Sistemas no IETEC
Coordenador de planejamento da DF+ Engenharia no Instituto de Educação Tecnológica (IETEC)
Endereço: R. General Andrade Neves, n. 840, Grajaú, CEP: CEP 30431-128. Belo Horizonte, MG, Brasil
Telefone: (31) 9 8464-4413
E-mail: danielbirchal@gmail.com

Fernando Hadad Zaidan
Doutor em Ciência da Informação
Professor e pesquisador do Mestrado no Instituto de Educação Tecnológica (IETEC)
Endereço: R. Gonçalves Dias, n. 750, CEP: 30.140-091. Belo Horizonte, MG, Brasil
Telefone: (31) 9 8822-5523
E-mail: fhzaidan@gmail.com

José Luis Braga
Doutor em Informática Pontifícia Universidade Católica (PUC-Rio)
Professor Orientador IETEC Instituto de Educação Tecnológica (IETEC)
Endereço: R. dos Timbiras, n. 63, CEP 30140-130. Belo Horizonte, MG, Brasil
E-mail: zeluisbraga@gmail.com

Artigo recebido em 01/05/2019. Revisado por pares em 10/05/2019. Reformulado em 11/05/2019. Recomendado para publicação em 15/12/2019. Publicado em 23/12/2019. Avaliado pelo Sistema *double blind review*.

RESUMO

Devido as novas regulações, Governança, Riscos e Conformidade (GRC) tornou-se pauta prioritária nas empresas. O objetivo deste artigo é apresentar um modelo de GRC integrado utilizando a modelagem de processos de negócio. Foi utilizada a *Design Science Research* (DSR) como método. Para este fim, foi realizada uma revisão bibliográfica para obter modelos correlatos que serviram como base para a fundamentação deste trabalho. Como resultado, conceberam-se modelos em cada um dos domínios da GRC, os quais, em seguida, foram validados por meio de comparações com modelos encontrados na literatura. Finalmente, os modelos foram integrados, permitindo uma visão holística do processo.

Palavras-chave: Governança; Riscos e Conformidade (GRC); GRC integrado; Modelo de processo de negócios; BPMN.

ABSTRACT

Due to the new regulations, Governance, Risks and Compliance (GRC) has become a priority in companies. The objective of this article is to present an integrated GRC model, using business process modeling. Design Science Research (DSR) was used as a method. For this purpose, a bibliographic review was carried out to obtain correlated models that served as a basis for the foundation of this work. As a result, models were designed in each of the GRC domains, then validated through comparisons with models found in the literature. Finally, the models were integrated allowing a holistic view of the process.

Keywords: Governance, Risks and Compliance (GRC); Integrated GRC; Business process model; BPMN.

RESUMEN

Debido a las nuevas regulaciones, Gobernanza, Riesgos y Conformidad (GRC) se hizo una pauta prioritaria en las empresas. El objetivo de este artículo es presentar un modelo de GRC integrado, utilizando el modelaje de procesos de negocios. Fue utilizada la Design Science Research (DSR) como método. A este fin, fue realizada una revisión bibliográfica para obtener modelos correlatos que sirvieron como base para la fundamentación de este trabajo. Como resultado, concibieron modelos en cada uno de los dominios de la GRC, en seguida fueron validados por medio de comparaciones con modelos encontrados en la literatura. Finalmente, los modelos fueron integrados, permitiendo una visión holística del proceso.

Palabras clave: Gobernanza, Riesgos y Conformidad (GRC); GRC integrado; Modelo de proceso de negocios; BPMN.

1 INTRODUÇÃO

Historicamente, a Gestão de Riscos Corporativos (do inglês, *Enterprise Risk Management* – ERM), a Governança Corporativa e a Conformidade foram tratadas como atividades totalmente independentes e sem nenhuma interação. Da integração dessas atividades surge o conceito de Governança, Riscos e Conformidade (GRC), que integra esses esforços promovendo ganho de eficiência e economia a partir de sinergia, compartilhamento de informações e aumento de eficiência.

Assim como aconteceu com o Planejamento de Recursos Empresariais (do inglês, *Enterprise Resource Planning* – ERP), segundo Gill e Purushottam (2008), a GRC está constantemente ganhando importância nas corporações. Isso ocorre principalmente devido à globalização, a crescentes demandas por transparência e a novas regulações, como o Acordo de Basileia, a Lei Sarbanes-Oxley, leis de prevenção à lavagem de dinheiro e, no caso brasileiro, à Lei 13303/16, que dispõem sobre novos padrões de GRC para empresas públicas, sociedades de economia mista e suas subsidiárias.

Embora sejam significativas, pesquisas científicas sobre iniciativas de GRC integradas são insuficientes (RACZ *et al*., 2010). Além disso, a literatura existente sobre implementação de GRC indica que muitos aspectos ainda não foram investigados (SPANAKI; PAPAZAFEIROPOULOU, 2015).

Diante desse contexto, o objetivo deste artigo é apresentar um modelo de GRC integrado utilizando a modelagem de processos de negócios por meio da notação *Business Process Model and Notation* (BPMN), que é uma notação que fornece uma simbologia simples e robusta para modelar aspectos de processos de negócio. O modelo foi baseado no modelo conceitual para GRC integrado proposto por Vicente e Silva (2011) e facilita o planejamento de implantação do GRC em organizações através da visualização de seus processos, interações e sequência. Para elaboração dos modelos de GRC será utilizado o método *Design Science Research* (DSR), que orienta a construção do conhecimento enfatizando a solução de problemas (WIERINGA, 2009).

Além desta introdução, o artigo apresenta a elucidação dos conceitos, no Referencial Teórico; a descrição do percurso metodológico; o detalhamento do desenvolvimento da

modelagem, bem como a validação e, por fim, as considerações finais e a lista de referências utilizadas.

2 REFERENCIAL TEÓRICO

A seguir serão apresentados trabalhos que embasarão a pesquisa.

2.1 MODELO CONCEITUAL PARA GRC INTEGRADO

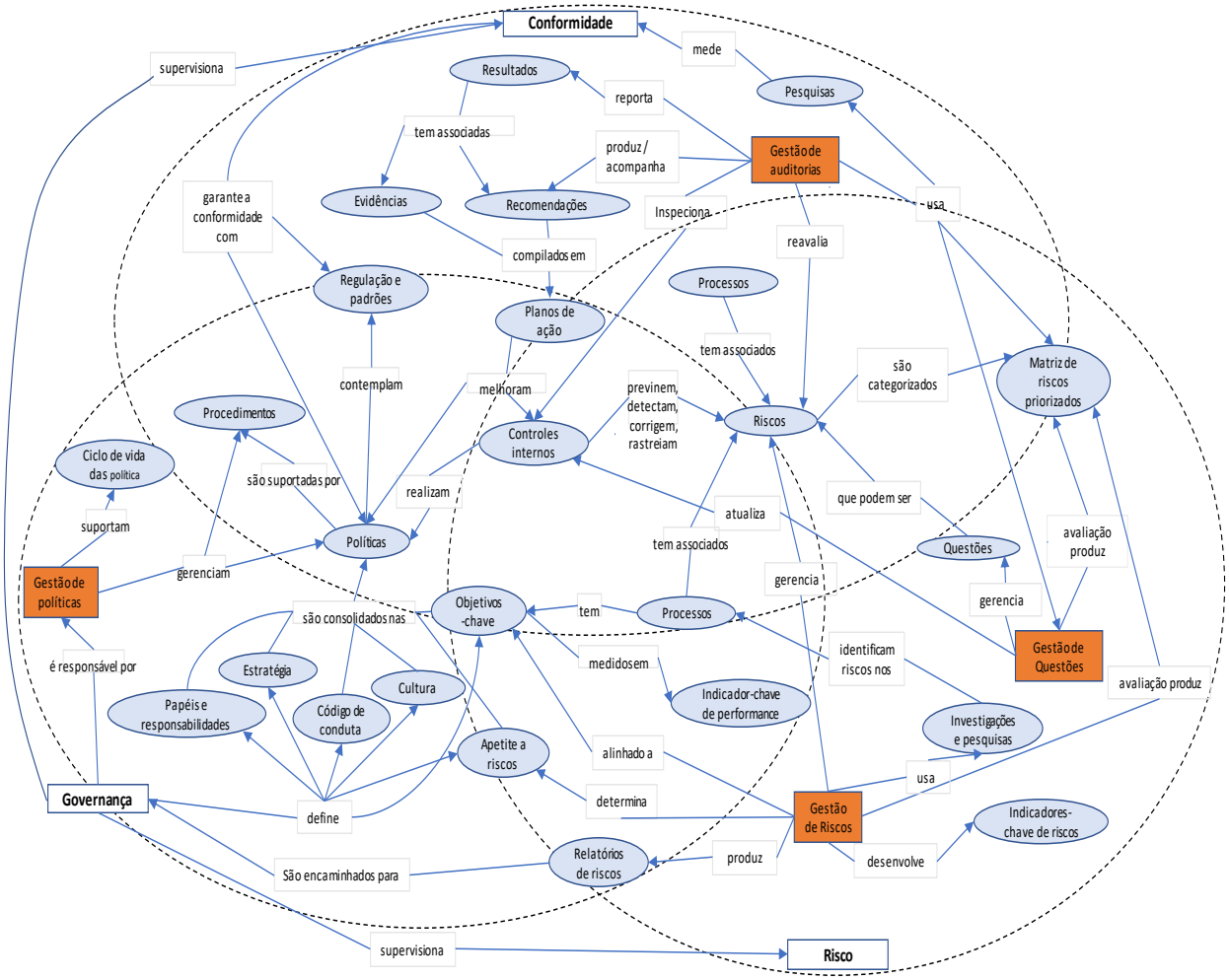
Nesta seção será apresentado o modelo conceitual para GRC integrado proposto por Vicente e Silva (2011). Inicialmente, os autores definiram três domínios – Governança, Riscos e Conformidade – e desenvolveram um modelo conceitual para cada um deles, destacando as quatro principais funcionalidades do GRC: gestão de auditorias, gestão de políticas, gestão de questões e gestão de riscos (FIG. 1). Essas atividades foram representadas por retângulos laranjas. Os conceitos em retângulos brancos também representam funcionalidades importantes, mas estas normalmente são automatizadas. Os conceitos modelados em elipses azuis representam informações que são gerenciadas por essas funções ou são de responsabilidade de pelo menos uma das áreas do GRC.

Segundo Vicente e Silva (2011), a Governança é responsável pela supervisão da Gestão de Riscos Corporativos e da Conformidade. As políticas definidas pela Governança são fundamentais para a GRC, uma vez que representam a visão da alta administração de como a organização deve ser dirigida e definem como a organização deve trabalhar, descrevendo o que é aceitável e o que não é.

Uma Gestão de Riscos Corporativos bem estruturada deve ser alinhada e ligada à Governança e Conformidade a fim de obter informações vantajosas para o processo de gestão de riscos. Além disso, a ERM não deve se restringir a apenas identificar e responder a riscos, mas deve agir proativamente prevendo e evitando riscos, bem como reduzindo a possibilidade de que eventos inesperados ocorram.

A Conformidade deve garantir que a organização esteja operando dentro dos padrões estabelecidos pela Governança além das exigências da legislação. A priorização de riscos elaborada pela ERM ajuda a Conformidade a atingir esse objetivo, uma vez que os riscos são alinhados aos objetivos corporativos.

Figura 1 – Modelo GRC integrado



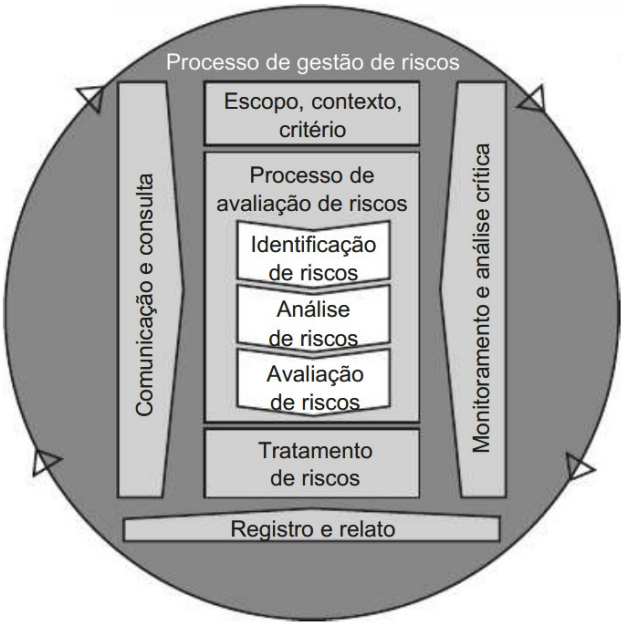
Fonte: Vicente e Silva, 2011.

Como pode ser observado na Figura 1, os controles internos exercem um papel central, haja vista que são fundamentais para as atividades de GRC.

2.2 ABNT NBR ISO 31000:2018 – Gestão de riscos: diretrizes

A NBR ISO 31000:2018 divide a ERM em seis processos principais. Inicia-se com o estabelecimento do contexto, seguido pelo processo de avaliação de riscos, o processo de tratamento de riscos e o processo de registro e relato. Os processos de comunicação e consulta e monitoramento e análise crítica devem ser executados em paralelo durante todo o processo de gestão de riscos. Adicionalmente, o processo de avaliação de riscos pode ser dividido em três etapas: identificação de riscos, análise de riscos e avaliação de riscos (ABNT, 2018). O processo de gestão de riscos proposto pela NBR ISO 31000:2018 pode ser visto na Figura 2.

Figura 2 – Processo de gestão de riscos

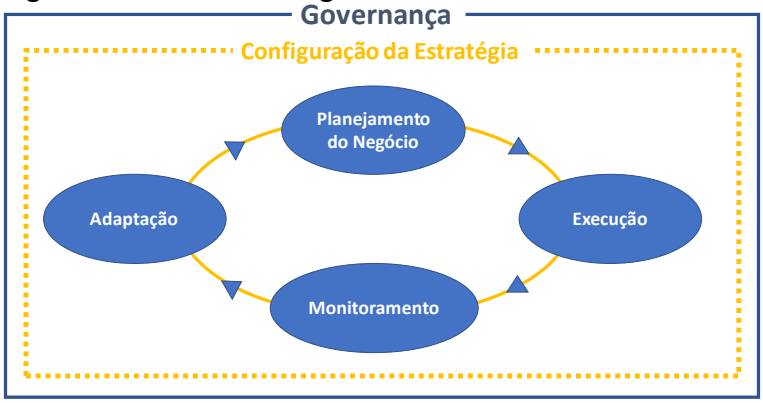


Fonte: ABNT, 2018.

2.3 MODELO DE NEGÓCIO CONCEITUAL DE GOVERNANÇA COSO

O *Committee of Sponsoring Organizations of the Treadway Commission* (COSO) desenvolveu um modelo de negócio conceitual com uma visão holística dos processos de Governança e gerenciais baseado no ciclo PDCA, do inglês, *Plan/Do/Check/Act*, conforme apresentado na Figura 3, a seguir.

Figura 3 – Modelo de negócios contextual COSO



Fonte: DELOACH; THOMSON, 2014, adaptada pelos autores, 2019.

Nesse modelo, o processo se inicia com o planejamento estratégico definindo a visão e a missão da empresa seguido pela configuração da estratégia. Esta, por sua vez, define o contexto para o planejamento do negócio por meio de um plano de alto nível para o que a organização quer atingir no horizonte de planejamento. A etapa de planejamento do negócio

formaliza os objetivos ou *roadmaps* de como a gestão de operação vai contribuir para alcançar os objetivos estratégicos. Já a execução consiste na operação cumprindo as atividades para realizar esse plano de negócio. A etapa de monitoramento é composta basicamente por atividades da gerência de supervisão e controle da operação. A última etapa é a adaptação, que se refere à adoção de ações corretivas que resultam em mudanças na estratégia, plano de negócios ou plano tático.

2.4 FRAMEWORK INTEGRADO DE CONTROLE INTERNO COSO

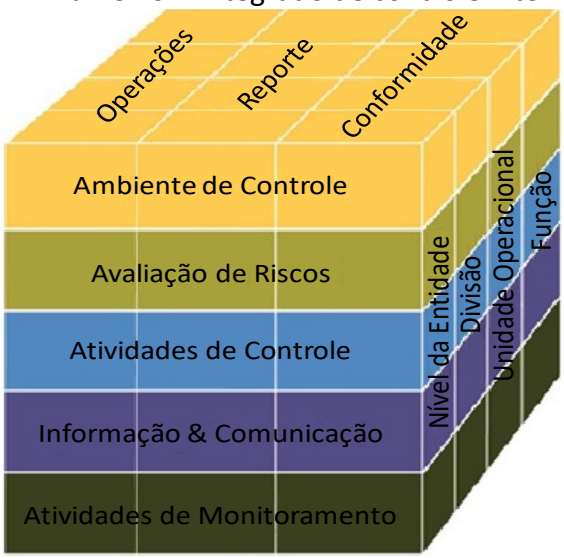
O COSO (2013) sugere que há três categorias de objetivos – operacionais, de reporte e de Conformidade – e define o controle interno como um processo projetado para prover garantias razoáveis de atingimento desses objetivos.

O controle interno é composto por cinco componentes: ambiente de controle; avaliação de riscos; atividades de controle; informação e comunicação; e atividades de monitoração.

Avaliações contínuas, avaliações separadas ou uma combinação das duas são utilizadas para certificação de que cada um dos cinco componentes dos controles internos está presente e funcionando. Avaliações contínuas são embutidas no processo e entregam informação em tempo real, enquanto avaliações separadas são conduzidas periodicamente e com escopo e frequência em função da avaliação de riscos, efetividade das avaliações contínuas e outras considerações gerenciais.

Segundo o COSO (2013) há uma relação direta entre os objetivos, os componentes do controle interno e a estrutura organizacional. Essa relação pode ser representada na forma de um cubo, conforme a Figura 4.

Figura 4 – Framework integrado de controle interno COSO

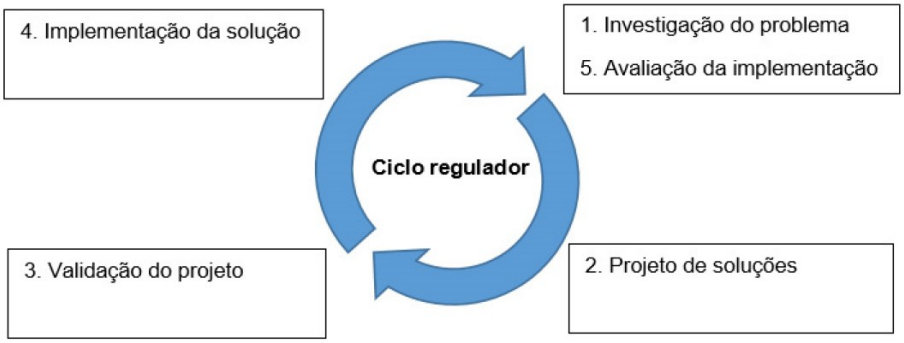


Fonte: COSO, 2013.

3 PERCURSO METODOLÓGICO

Esta pesquisa utiliza a metodologia DSR para desenvolvimento dos modelos. O ciclo regulador proposto por Wieringa (2009), autor seminal que defende a DSR, envolve a investigação do problema, o projeto da solução, a validação, a implementação e a avaliação, e é adequado às necessidades deste projeto.

Figura 5 – Ciclo regulador de Wieringa



Fonte: ZAIDAN, 2015. (Adaptada de WEIRINGA, 2009).

Relacionando as etapas propostas pelo ciclo regulador às necessidades desta pesquisa obtém-se o Quadro 1.

Quadro 1 – Relação entre as etapas do ciclo regulador e as atividades da pesquisa

Etapas do ciclo regulador	**Atividade do projeto**
1) Investigação do problema	Revisão bibliográfica
2) Projeto de soluções	Proposição do modelo
3) Validação do projeto	Validação comparando o modelo obtido com modelos relacionados

Etapas do ciclo regulador	Atividade do projeto
4) Implementação da solução	Realização de adequações advindas do processo de validação
5) Avaliação da implementação	Avaliação do modelo final

Fonte: Elaborado pelos autores, 2019.

4 CONSTRUÇÃO DOS MODELOS

Esta proposta de *framework* sequencia as atividades mapeadas no modelo conceitual proposto por Vicente e Silva (2011) de acordo com os processos de ERM propostos pela NBR ISO 31000:2018 e o modelo de negócios contextual proposto pelo COSO.

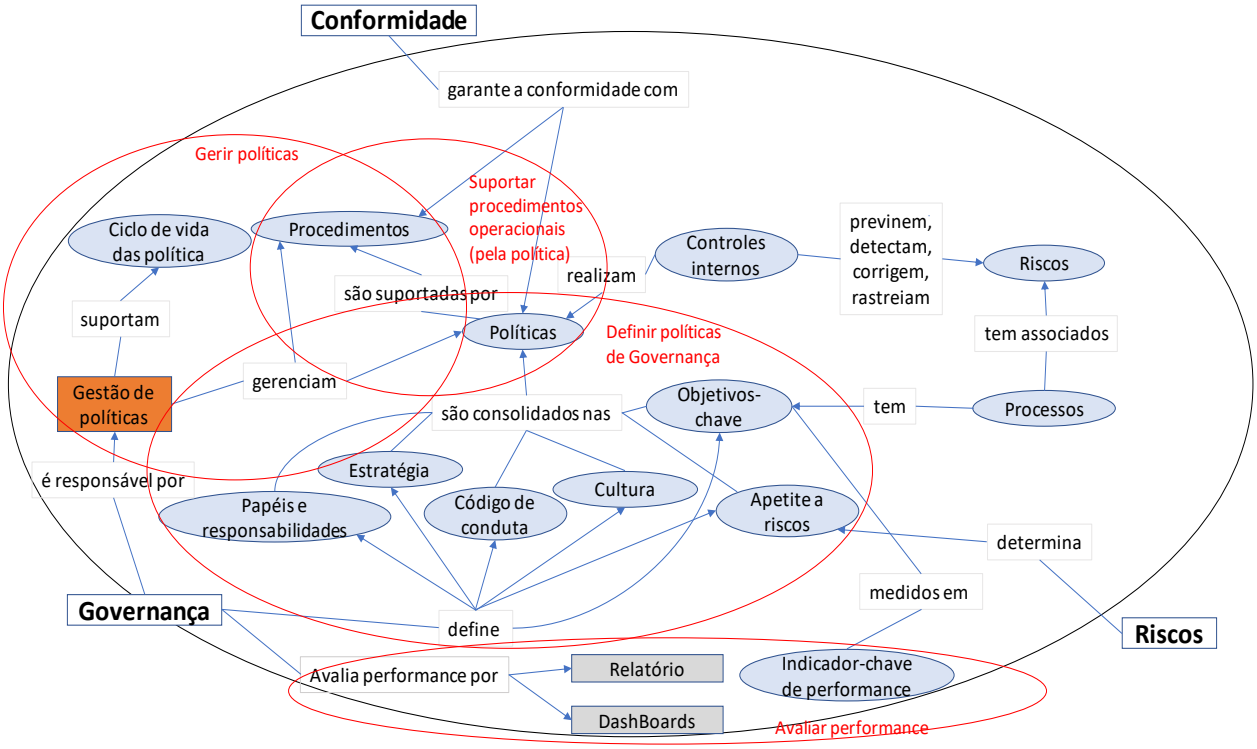
4.1 GOVERNANÇA

Do modelo conceitual de Governança proposto por Vicente e Silva (2011), conforme a Figura 6, é possível extrair os seguintes processos principais da Governança:

a) Definir políticas de Governança;
b) Consolidar políticas;
c) Supervisionar ERM e Conformidade;
d) Suportar procedimentos operacionais (pela política);
e) Avaliar performance;
f) Gerir políticas.

As demais atividades de Governança serão modeladas como subprocessos destes.

Figura 6 – Modelo de Governança



Fonte: VICENTE e SILVA (2011), adaptada pelos autores, 2019.

Como o modelo proposto por Vicente e Silva (2011) modela apenas relações, o modelo de negócios contextual proposto pelo COSO será utilizado para estabelecer a sequência das atividades e validar o modelo, conforme Quadro 2. Uma abordagem análoga também será utilizada na construção dos modelos de ERM e Conformidade.

Quadro 2 – Atividade *versus* fase em que o processo ocorre

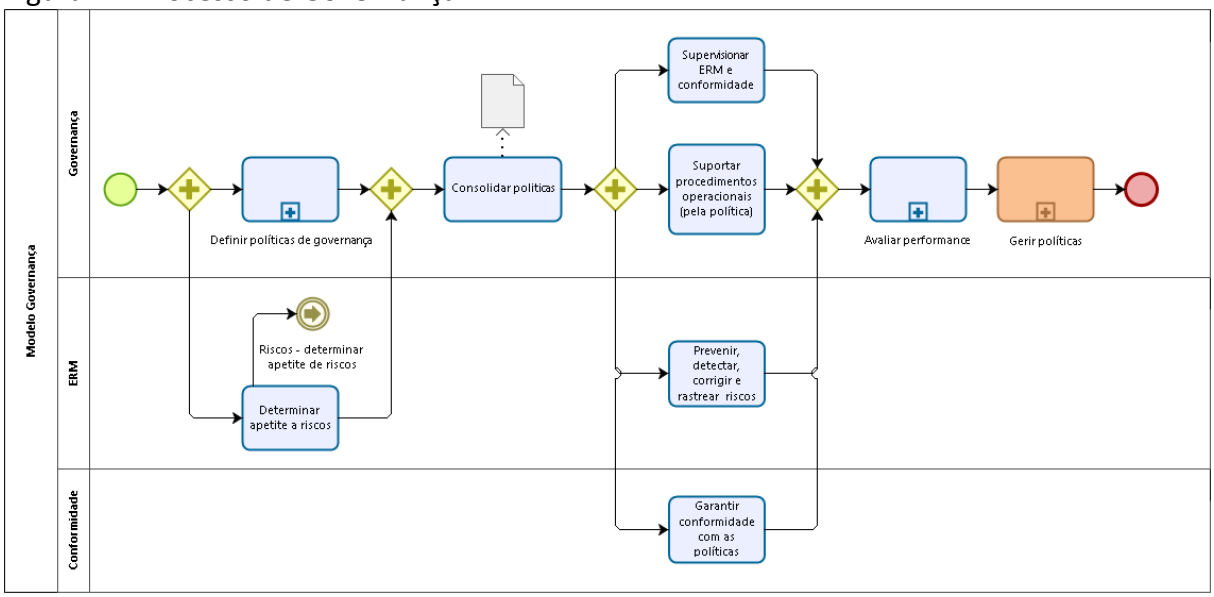
Atividades principais identificadas (Governança)	**Fase correspondente no modelo proposto pelo COSO**
Definir políticas de Governança	Configuração da estratégia / planejamento do negócio
Consolidar políticas	Planejamento do negócio
Supervisionar ERM e Conformidade	Execução
Suportar procedimentos operacionais	Execução
Avaliar performance	Monitoramento
Gerir políticas	Adaptação

Fonte: Elaborado pelos autores, 2019.

A Figura 7 ilustra o processo de Governança e suas principais relações com o ERM e a Conformidade modelados utilizando a metodologia BPMN. O processo é iniciado com o processo definir políticas e, em seguida, ocorre o processo de consolidação das políticas. Na sequência, o processo de supervisão à ERM e à Conformidade ocorre paralelamente ao

suporte aos procedimentos operacionais. Posteriormente estão os processos de avaliação de performance e gestão das políticas.

Figura 7 – Processo de Governança

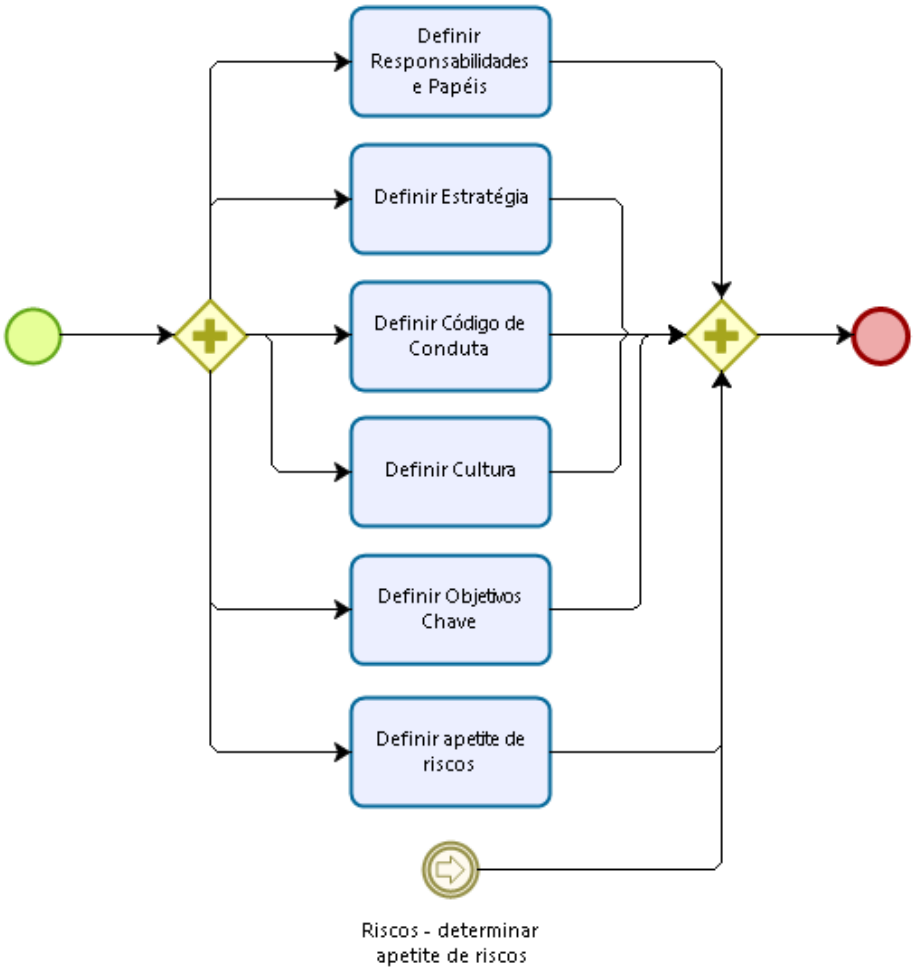


Fonte: Elaborado pelos autores, 2019.

4.1.1 Processo de definição das políticas de Governança

O processo de definição das políticas de Governança tem como subprocessos: definir responsabilidades e papéis, definir estratégia, definir códigos de conduta, definir cultura, definir objetivos-chave e definir apetite de riscos, conforme demonstrado na Figura 8. Adicionalmente, a ERM determina o apetite de riscos. O processo de definição das políticas de Governança consiste nas definições de responsabilidades e papéis, estratégia, código de conduta, cultura, objetivos-chave, apetite de riscos, além da definição do apetite de riscos que é efetuado pela ERM.

Figura 8 – Processo de definição das políticas de Governança

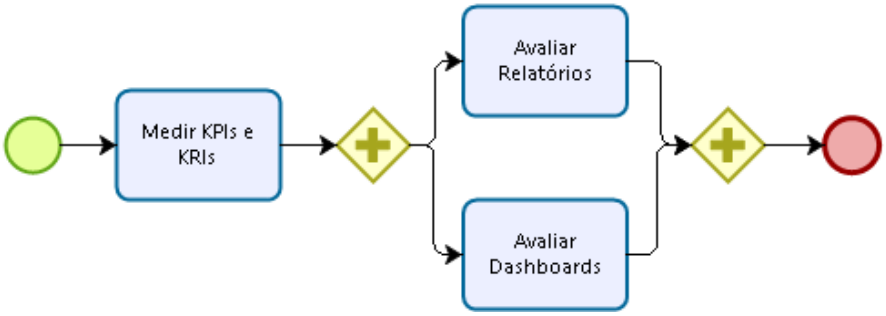


Fonte: Elaborado pelos autores, 2019.

4.1.2 Processos de avaliação da performance e processo de gestão de políticas

Por serem atividades integrantes deste processo, as atividades medir indicadores-chave de performance (KPIs) e indicadores-chave de riscos (KRIs), avaliar relatórios e avaliar *dashboards* foram modeladas como subprocessos do processo de avaliação de performance, conforme a Figura 9.

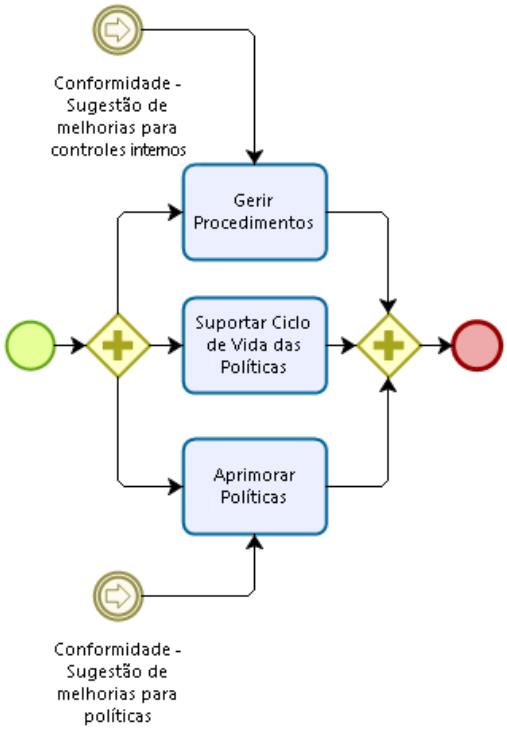
Figura 9 – Processo de avaliação de performance



Fonte: Elaborado pelos autores, 2019.

Analogamente, como pode ser visto na Figura 10, as atividades gerir procedimentos, suportar ciclo de vida das políticas e aprimorar políticas foram modeladas como subprocessos do processo de gestão de políticas. Tanto o processo de gestão de procedimentos quanto o processo de aprimoramento de políticas recebem *feedback* da Conformidade com sugestão de melhorias dos controles internos e melhorias para as políticas, respectivamente.

Figura 10 – Processo de gestão de políticas

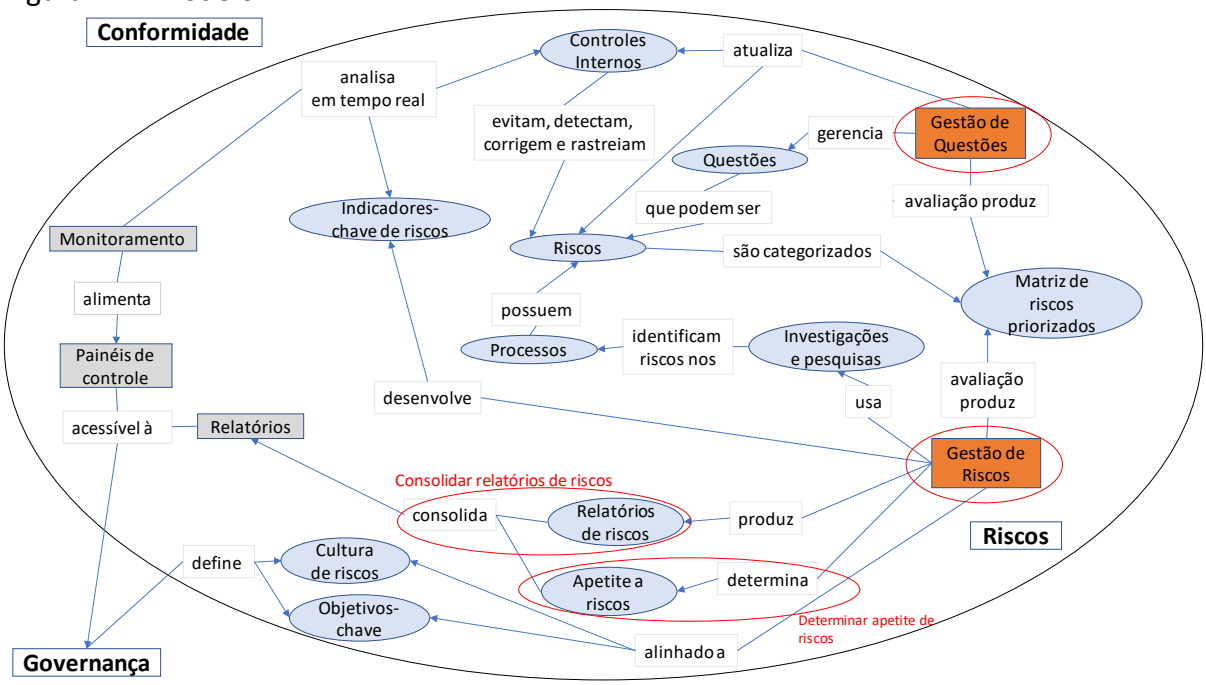


Fonte: Elaborado pelos autores, 2019.

4.2 GESTÃO DE RISCOS CORPORATIVOS (ERM)

É possível identificar quatro processos principais no processo de gestão de riscos corporativos proposto por Vicente e Silva (2011), conforme apresenta a Figura 11.

Figura 11 – Modelo ERM



Fonte: VICENTE e SILVA (2011), adaptada pelos autores, 2019.

Analogamente ao que foi feito no processo de Governança, as demais atividades presentes no modelo serão modeladas como subprocessos dessas atividades principais e o modelo proposto pela NBR ISO 31000:2018 foi utilizado para o sequenciamento dessas atividades e validação do modelo, conforme o Quadro 3.

Quadro 3 – Correspondência entre atividades principais identificadas no modelo de Vicente e Silva (2011) e a NBR ISO 31000:2018

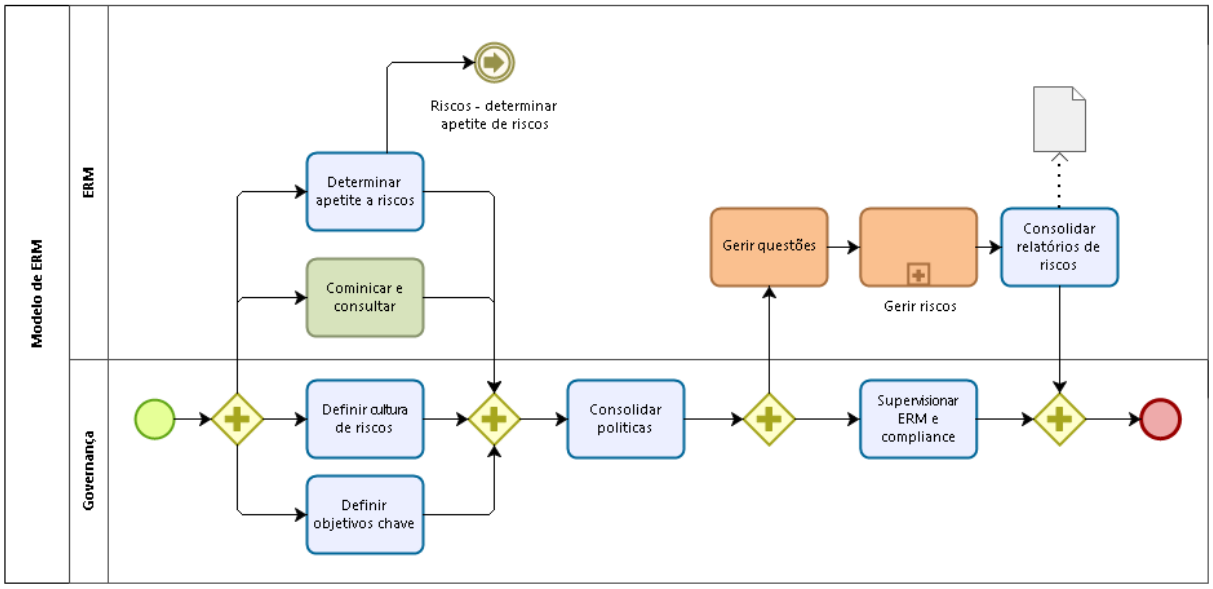
Atividades principais identificadas (ERM)	**Fase correspondente no modelo proposto pela NBR ISO 31000:2018**
Determinar apetite a riscos	Escopo, contexto e critérios
Gerir questões	Identificação de riscos
Gerir riscos	Processo de avaliação de riscos / Tratamento de riscos
Consolidar relatórios de riscos	Registro e relato
Sem atividade correspondente	Comunicar e consultar

Fonte: Elaborado pelos autores, 2019.

Como pode ser observado no Quadro 3, não há uma atividade correspondente ao processo comunicar e consultar que é proposto pela NBR ISO 31000:2018. Como essa é uma atividade fundamental da prática de gestão de riscos, ela será incluída no modelo BPM proposto.

A Figura 12 ilustra o processo de ERM modelado utilizando a metodologia BPMN e devidamente sequenciado de acordo com a NBR ISO 31000:2018, bem como suas principais relações com a Governança.

Figura 12 – Processo ERM



Fonte: Elaborado pelos autores, 2019.

4.2.1 Processo de gestão de riscos

Do modelo de ERM proposto por Vicente e Silva (2011) podem-se destacar as seguintes atividades pertencentes ao processo de gestão de riscos: identificar riscos, analisar indicadores-chave de riscos, categorizar riscos, desenvolver indicadores-chave para riscos, produzir a matriz de prioridades, executar ações corretivas e atualizar controles internos.

Correlacionando essas atividades ao modelo proposto pela NBR ISO 31000:2018 obtém-se o Quadro 4.

Quadro 4 – Correspondência entre atividades de gestão de riscos identificadas no modelo de Vicente e Silva (2011) e a ABNT ISO 31000:2018

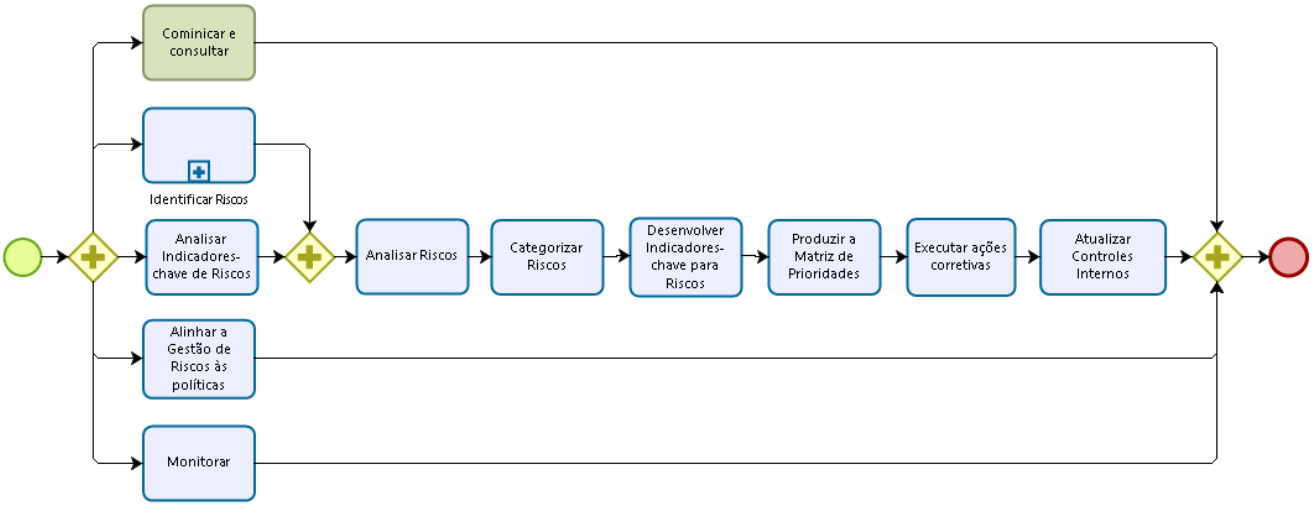
Atividades principais identificadas (Gerir riscos)	**Fase correspondente no modelo proposto pela NBR ISO 31000:2018**
Identificar riscos	Identificação de riscos
Analisar indicadores-chave de riscos	Identificação de riscos
Alinhar a gestão de riscos às políticas	Monitoramento e análise crítica
Monitorar	Monitoramento e análise crítica
Analisar riscos	Análise de riscos
Categorizar riscos	Análise de riscos
Desenvolver indicadores-chave para riscos	Análise de riscos

Atividades principais identificadas (Gerir riscos)	Fase correspondente no modelo proposto pela NBR ISO 31000:2018
Produzir a matriz de prioridades	Avaliação de riscos
Executar ações corretivas	Tratamento de riscos
Atualizar controles internos	Registro e relato
Sem atividade correspondente	Comunicar e consultar

Fonte: Elaborado pelos autores, 2019.

Mais uma vez não há uma atividade correspondente para o processo comunicar e consultar proposto pela NBR ISO 31000:2018. Acrescentando-se essa atividade e modelando conforme a sequência obtida pela correlação dos dois modelos, o processo de gestão de riscos obtido é demonstrado na Figura 13.

Figura 13 – Processo gerir riscos

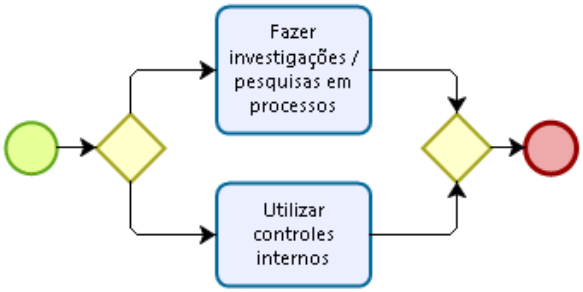


Fonte: Elaborado pelos autores, 2019.

4.2.2 Processo de identificação de riscos

Por serem partes integrantes do processo de identificação de riscos, os processos fazer investigações/pesquisas em processos e utilizar controles internos foram modelados como subprocessos deste.

Figura 14 – Processo de identificação de riscos

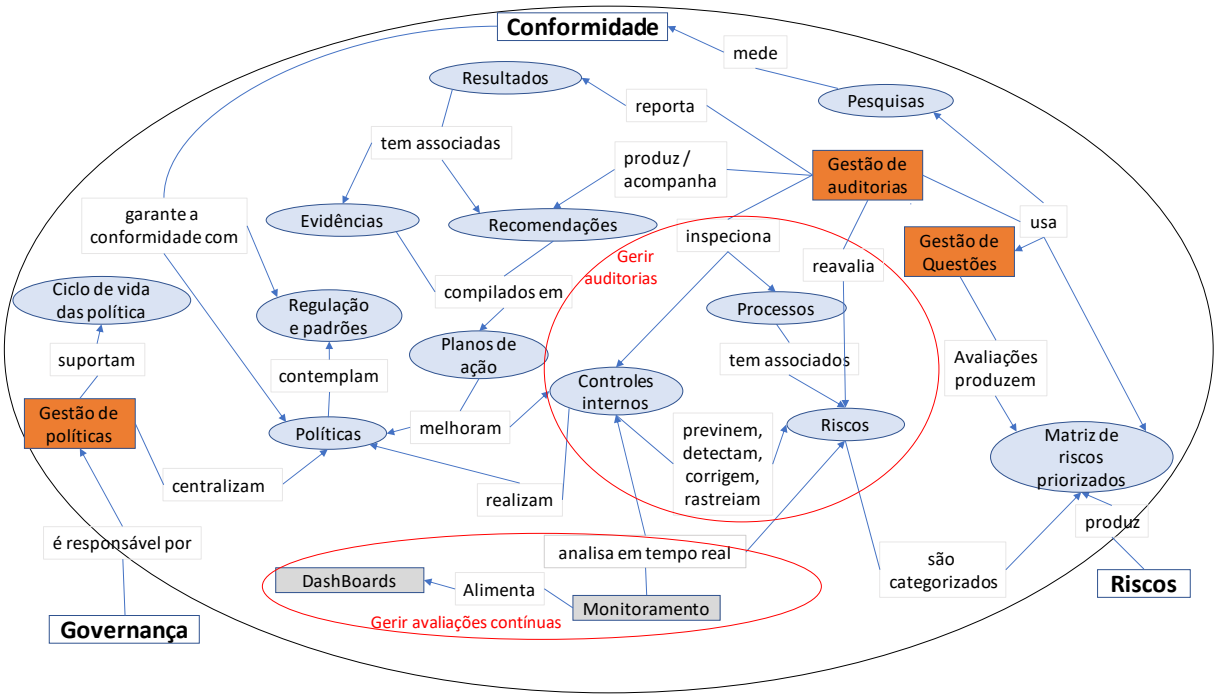


Fonte: Elaborado pelos autores, 2019.

4.3 CONFORMIDADE

Segundo o modelo proposto por Vicente e Silva (2011), a Conformidade é definida por quatro processos principais: gerir auditorias, reportar conclusões, compilar evidências e recomendações em planos de ação e fazer *follow up.* A Figura 15 ilustra esse modelo e as demais atividades serão modeladas como subatividades desta.

Figura 15 – Modelo Conformidade



Fonte: VICENTE e SILVA (2011), adaptada pelos autores, 2019.

Correlacionando as atividades obtidas com o *framework* integrado de controle interno obtém-se o Quadro 5. É importante ressaltar que devido ao fato de o *framework* extrapolar os limites de domínio da Conformidade, parte de suas atividades deve ser representada por atividades da Governança ou ERM.

Quadro 5 – Correspondência entre atividades Conformidade identificadas no modelo de Vicente e Silva (2011) e o framework integrado de controle interno do COSO

Atividades identificadas no modelo da Conformidade	**Atividade correspondente no *framework* integrado de controle interno do COSO**
Atividades do domínio da Governança	Ambiente de controle
Subatividade reavaliar riscos e atividades do ERM	Avaliação de riscos
Fazer *follow up* e atividades executadas pela Governança	Atividades de controle
Reportar conclusões	Informação e comunicação

Gerir auditorias e gerir avaliações contínuas	Atividades de monitoramento

Fonte: Elaborado pelos autores, 2019.

O sequenciamento das atividades no modelo avaliando-se os pré-requisitos de cada uma das atividades é demonstrado no Quadro 6.

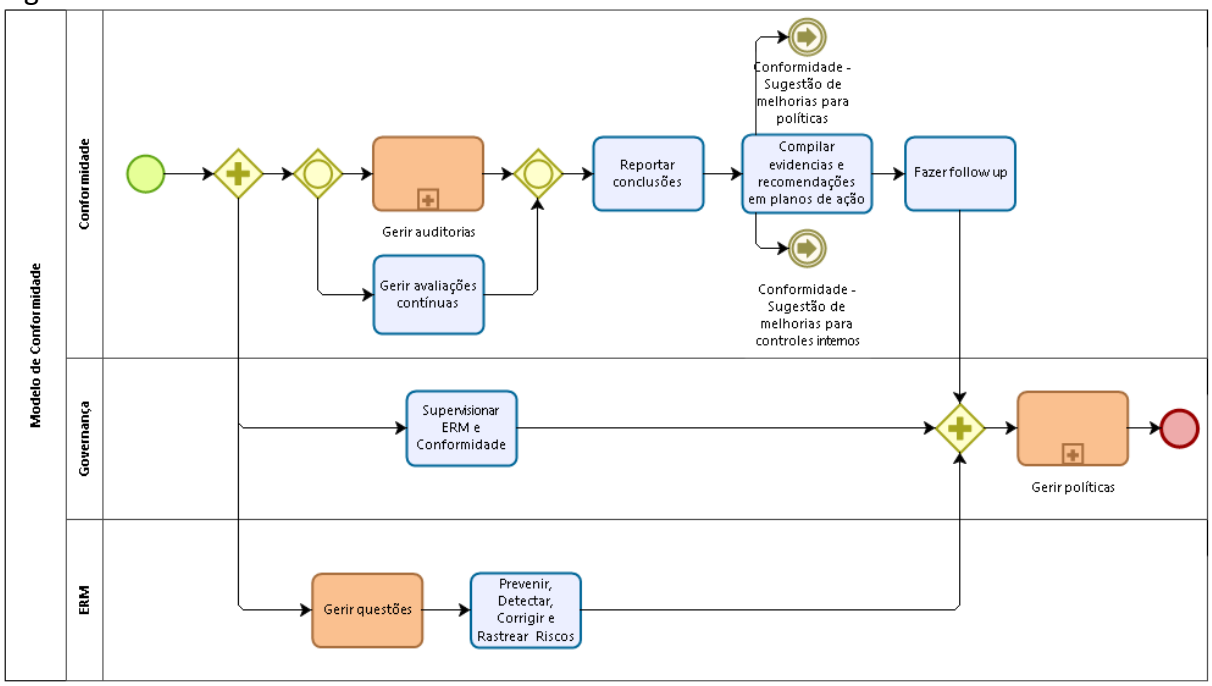
Quadro 6 – Avaliação de pré-requisitos das atividades do modelo da Conformidade

Atividades identificadas no modelo da Conformidade	**Pré-requisito**	**Atividade necessariamente predecessora**
Gerir auditorias	Nenhum	Nenhuma
Compilar resultados de avaliações contínuas	Nenhum	Nenhuma
Reportar conclusões	Realização de auditoria / avaliações contínuas	Gerir auditorias / compilar resultados de avaliações contínuas
Compilar evidências e recomendações em planos de ação	Realização de auditoria / avaliações contínuas	Gerir auditorias / compilar resultados de avaliações contínuas
Fazer *follow up*	Sugestão de planos de ação	Compilar evidências e recomendações em planos de ação

Fonte: Elaborado pelos autores, 2019.

Uma vez que é prática comum o reporte de conclusões e validação das ações corretivas a serem tomadas com a administração da empresa e com a finalidade de simplificar o fluxo neste trabalho, a atividade reportar conclusões será posicionada entre as atividades gerir auditorias e compilar evidências e recomendações em planos de ação. Dessa forma, o fluxo de processos resultante pode ser observado na Figura 16.

Figura 16 – Processo de Conformidade

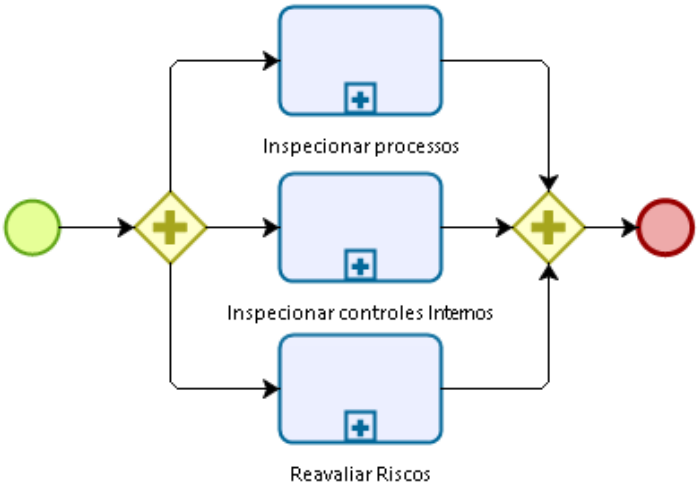


Fonte: Elaborado pelos autores, 2019.

4.3.1 Processo gerir auditorias

O processo de gestão de auditorias consiste em três subprocessos, conforme Figura 17, que devem ser executados periodicamente, e seus escopos e frequências variarão em função da efetividade das avaliações contínuas, avaliação de riscos e outras considerações gerenciais.

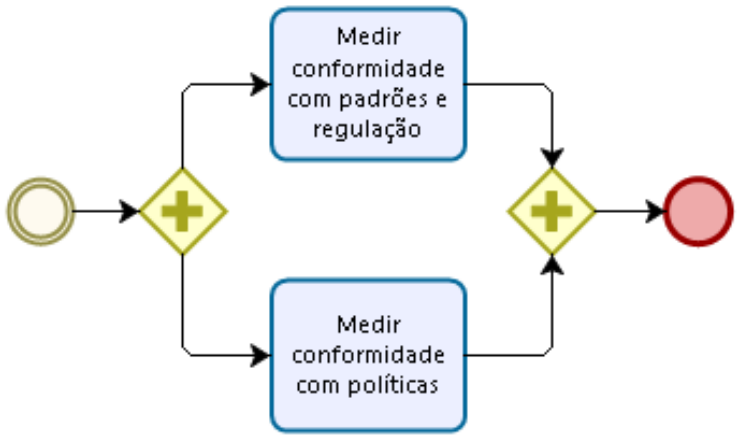
Figura 17 – Processo de gerir auditorias



Fonte: Elaborado pelos autores, 2019.

Os subprocessos inspecionar processos e inspecionar controles internos são idênticos e foram modelados conforme a Figura 18.

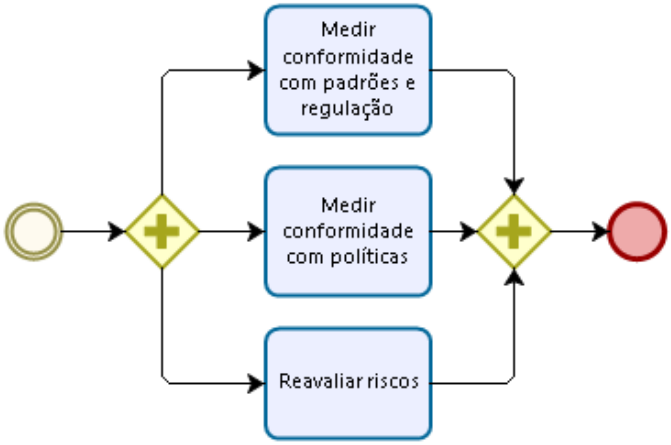
Figura 18 – Subprocessos inspecionar processos e inspecionar controles internos



Fonte: Elaborado pelos autores, 2019.

Analogamente, o processo reavaliar riscos é ilustrado na Figura 19.

Figura 19 – Subprocesso reavaliar riscos

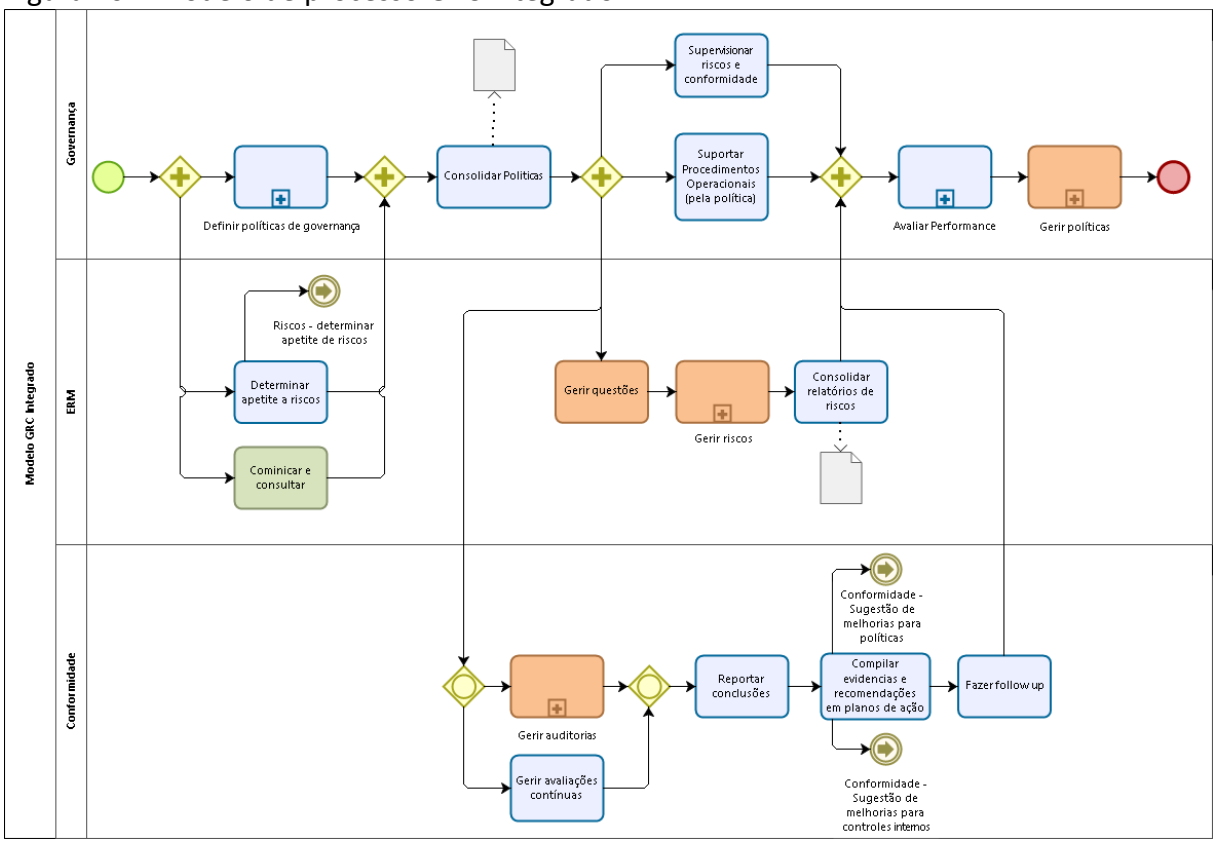


Fonte: Elaborado pelos autores, 2019.

4.4 MODELO GRC INTEGRADO

Nesta seção é apresentada a integração dos modelos de Governança, ERM e Conformidade. Conforme pode ser observado na Figura 20, o processo se inicia no domínio da Governança, definindo as políticas de Governança. Essa atividade também requer a participação da equipe ERM para determinação do apetite de riscos da empresa, que é parte integrante das políticas de Governança. Após a consolidação das políticas de Governança, processos nos três domínios do GRC são executados em paralelo. No domínio da Governança, a supervisão à ERM e Conformidade e o suporte aos procedimentos operacionais com base nas políticas; no domínio de ERM, os processos de gestão de questões e gestão de riscos são finalizados e todos os processos do domínio da Conformidade são finalizados. Posteriormente, os processos de avaliação de performance e gestão de políticas completam o ciclo do processo GRC.

Figura 20 – Modelo de processo GRC integrado



Fonte: Elaborado pelos autores, 2019.

5 CONSIDERAÇÕES FINAIS

Devido ao pouco material científico sobre o tema optou-se por tratar cada um dos domínios do GRC separadamente. Dessa forma, a princípio, cada um dos modelos propostos por Vicente e Silva (2011) foram analisados e suas atividades foram mapeadas. Seguindo a orientação da DSR, posteriormente os modelos de cada um dos domínios foram comparados com outros modelos, processo ou *frameworks* extraídos da literatura com o objetivo de validá-los, assegurar sua coerência e garantir a abrangência dos domínios de forma satisfatória.

Para tanto, foi realizada uma extensa pesquisa na literatura e foram escolhidos o modelo de negócios contextual proposto pelo COSO para a Governança, o processo de gestão de riscos descrito pela NBR ISO 31000:2018 para o ERM e o *framework* integrado de controles internos, também proposto pelo COSO, para a Conformidade. Em seguida, os modelos foram integrados, permitindo uma visão completa dos processos do GRC e de suas interações.

Apesar da pouca documentação científica disponível sobre o tema GRC integrado foi possível a elaboração de modelos de processo de negócios para Governança, ERM,

Conformidade e GRC integrado desenvolvidos segundo as diretrizes do DSR e utilizando a notação BPMN.

Cabe destacar que a avaliação dos impactos da implantação desse modelo em um processo não está no escopo deste trabalho e deve ser considerada como uma oportunidade para trabalhos futuros.

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT. **NBR ISO 31000**: gestão de riscos: diretrizes. 2. ed. Rio de Janeiro, 2018.

COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION. COSO. **Internal control:** integrated framework. Durham: COSO, 2013.

DELOACH, J.; THOMSON, J. **Improving organizational performance and governance:** how the COSO frameworks can help. Durham: COSO, 2014.

GILL, S.; PURUSHOTTAM, U. Integrated GRC: is your organization ready to move? **SETLabs Briefings**, v. 6, n. 3, p. 37-46, 2008.

RACZ, N. *et al*. Governance, risk & compliance (GRC) status quo and software use: results from a survey among large enterprises. In: AUSTRALASIAN CONFERENCE ON INFORMATION SYSTEMS, 21., 2010, Brisbane. **Proceedings [...]**. Brisbane: ACIS 2010.

SPANAKI, K.; PAPAZAFEIROPOULOU, A. Analysing the governance, risk and compliance (GRC) implementation process: primary insights. In: EUROPEAN CONFERENCE ON INFORMATION SYSTEMS, 21., 2013, Utrecht, Netherlands. **Proceedings [...]**. Utrecht: ECIS 2013 Completed Research, 2013. Paper 58.

VICENTE, P.; SILVA, M. M. A conceptual model for integrated governance, risk and compliance. In: INTERNATIONAL CONFERENCE ON ADVANCED INFORMATION SYSTEMS ENGINEERING, 23., 2011, London. **Proceedings [...]**. London, UK: Springer-Verlag, 2011. p. 199-213.

WIERINGA, R. Design science as nested problem solving. In: INTERNATIONAL CONFERENCE ON DESIGN SCIENCE RESEARCH IN INFORMATION SYSTEMS AND TECHNOLOGY, 4., 2009, Philadelphia. **Proceedings [...]**. Philadelphia, PA, USA ACM, 2009 p. 8.

ZAIDAN, F. H. **Aportes da arquitetura corporativa para o ambiente dos sistemas informatizados de gestão arquivística de documentos:** aplicação em companhia de energia elétrica. 2015. 176f. Tese (Doutorado) – Universidade Federal de Minas Gerais, Escola de Ciência da Informação, Belo Horizonte, 2015.