E-BOOK GESTÃO DE RISCOS

2019

Eduardo Person Pardini

WWW.CROSSOVERBRAZIL.COM

CONTEÚDO

EDIÇÃO 1 – SÃO PAULO – BRASIL - 2019

PUBLICAÇÃO: Crossover Consulting & Auditing

1. INTRODUÇÃO

Contar com um bom e estruturado processo de gerenciamento de riscos é fundamental para a consolidação de uma gestão pautada em boas práticas de governança.

Sabemos que a gestão de riscos aumenta a capacidade da organização em alcançar seus objetivos estratégicos que, se estiverem alinhados a sua missão, possibilitará a organização criar valor às partes relacionadas.

Atualmente uma grande gama de normas, regulamentos e leis estabelecem a obrigatoriedade do gerenciamento de riscos pelas organizações, como exemplo: Instrução Normativa Conjunta MP/CGU 01, Circular Susep 521, Lei 13.303, sem falar as normas do Banco Central, CVM e outras, o que está motivando uma onda de implementação nas organizações do setor privado e público.

É valido mencionar ainda que o gerenciamento de riscos para uma empresa do setor privado ou uma empresa do setor público segue a mesma estrutura, o que muda são alguns requisitos legais e a natureza do negócio, do resto, são semelhantes.

Vamos abordar os principais fatores que devem ser observados para se ter um processo estruturado e integrado de gerenciamento de riscos, elemento chave para uma efetiva governança corporativa.

2. A IMPORTÂNCIA DA GESTÃO DE RISCOS

Todas as organizações, sem exceção, têm como marco estratégico a criação de valores para as partes relacionadas, o qual é traduzido na missão da organização. Para alcançar a missão, é definida a estratégia e por consequência os objetivos de negócio.

As organizações contam com 4 tipos básicos de recursos: Financeiros, Humanos, Tecnológicos e Materiais. Para direcionar estes recursos, de forma otimizada, no processo de execução das ações necessárias para cumprir com os objetivos estratégicos, a empresa se organiza em ciclos de negócio, que por sua vez são compostos por processos operacionais, cada um com sua camada de objetivos, que devem estar sempre relacionados com os objetivos estratégicos.

Está claro que o risco está sempre presente em qualquer corporação, seja o risco de não alcançar os objetivos estratégicos, ou o risco de não alcançar os objetivos operacionais. O grande desafio da gestão é definir quanto de riscos ela está disposta correr para criar valor às partes relacionadas.

"O grande desafio da gestão é definir quanto de risco ela está disposta correr para criar valor as partes relacionadas"

Justamente neste ponto é que entra a importância de a empresa contar com um processo de gerenciamento de riscos integrado à sua cultura e ao ambiente interno, e não apenas um processo de elaborar planilhas. Ele deve estar presente nas atividades diárias de gestão, fazendo parte das decisões operacionais ou estratégicas.

Não é possível ter uma efetiva governança corporativa sem que haja uma boa consciência e gestão de riscos, que por sua vez necessita de um eficaz sistema de controles internos.

A gestão de riscos aumenta a capacidade da organização em alcançar seus objetivos, possibilitando a visualização de oportunidades que impactaram positivamente a organização como um todo.

O COSO, em sua revisão da estrutura de boas práticas, indica alguns benefícios de se ter uma boa gestão de riscos. Vejam alguns que entendo como prioritários:

- Permite às entidades melhorar sua capacidade de identificar riscos e definir as respostas adequadas, diminuindo surpresas e os custos ou prejuízos correspondentes e tirando proveito dos demais desdobramentos favoráveis.

- Diminuição da oscilação da performance,
- Melhor distribuição dos recursos,
- Aumento da resiliência da empresa.

O risco em síntese trás impacto negativo, entretanto, o processo de gerenciamento de riscos deve ser visto com um fato positivo, uma vez que dá origem a oportunidades estratégicas e a importantes competências diferenciadoras, como pontua o COSO.

3. CONCEITO DE RISCO

Muitas são as conceituações do risco, muitas conceituam o risco como sendo a incerteza de alcançar os resultados planejados. Outros definem com sendo eventos que impactam positivamente ou negativamente a corporação.

Prefiro conceituar risco como:

> "Probabilidade de ocorrência de eventos associados a perda ou um efeito adverso que impacta negativamente a capacidade da organização em alcançar os objetivos estabelecidos, sejam eles operacionais ou estratégicos."

É importante salientar, que, em minha opinião, eventos que trazem impacto positivo são considerados oportunidades, as quais uma vez identificadas devem ser transferidas para a gestão do planejamento estratégico.

Risco está sempre presente e pode ser medido de forma matricial, isto é: Probabilidade de ocorrência e seu impacto se ocorrer, por isso também não é uma incerteza. As respostas para as incertezas, se existirem, serão subjetivas, por sua vez, as respostas para os riscos serão sempre objetivas, pois conseguimos medir o risco objetivamente.

Posso dizer também que risco é a forma negativa de se olhar para uma situação, o que nos ajuda a reconhecer a presença da ameaça que pode em certo momento, se existir a exposição, se materializar em um evento de risco.

O termo "ameaça" também tem sido utilizado como sinônimo de risco, então vamos rever isto:

- Ameaça – é o evento que pode ocorrer sob certa circunstância e pode causar uma perda.
- Risco – é a probabilidade da ameaça se materializar e causar um efeito adverso ou uma perda a organização.
- Exemplo: O risco de destruição do data center corporativo aumenta quando um furacão (ameaça) se aproxima.

O risco faz parte de qualquer tipo de operação, não existe nenhuma iniciativa sem risco, ele está sempre presente e é inerente ao negócio. Isto também é uma verdade para nossa vida particular, vivemos sempre à mercê de eventos que podem impactar negativamente nossa capacidade de alcançar os nossos objetivos profissionais ou particulares.

Risco está sempre associado ao objetivo. A análise dos riscos aumenta nossa capacidade de não ser "pego de surpresa".

4. GESTÃO DE RISCOS COMO SEGUNDA LINHA DE DEFESA

O modelo das três linhas de defesa surgiu com a publicação em 21 de setembro de 2010 pelas FERMA e ECIIA no *Guidance on the 8th EU Company law* como recomendação da implementação dos requisitos da lei para o monitoramento da efetividade do sistema de controles internos, auditoria interna e gerenciamento de riscos.

Como salienta a declaração de posicionamento do IIA sobre o tema:

"O modelo de Três Linhas de Defesa é uma forma simples e eficaz de melhorar a comunicação do gerenciamento de riscos e controle por meio do esclarecimento dos papéis e responsabilidades essenciais".

O ponto significativo neste modelo é a transparência sobre quais são as responsabilidades de cada uma das partes interessadas na condução dos negócios e operação da organização, de forma a organizar o processo para que não existam lacunas devido a não compreensão das reais responsabilidades de cada um neste processo de governança.

Adaptação da *Guidance on the 8th EU Company Law Directive* da ECIIA/FERMA, artigo 41

De uma forma resumida, a primeira linha de defesa são os gestores que tem como responsabilidade o gerenciamento de riscos de seus processos, a supervisão e o alinhamento do sistema de controle interno com os riscos inerentes, tecnologia e fraude.

Como segunda linha de defesa estão as áreas de apoio ou staff que auxiliam os gestores a executar suas responsabilidades. Estão as áreas de controle interno, compliance, gestão de riscos e outros.

E como terceira linha de defesa temos a auditoria interna a qual tem a responsabilidade de realizar um monitoramento periódico através de uma avaliação independente do processo de governança, gestão de riscos e sistema de controles internos que os gestores da primeira linha de defesa são responsáveis.

Costumo dizer que o setor de controles internos não faz controle, mas ajuda o gestor a ter um sistema de controles internos efetivo e otimizado. O mesmo acontece com a área de gestão de riscos; ela não faz gestão de riscos, mas apoia os gestores a fazerem a análise de riscos de seus processos.

5. PARADIGMAS DE BOAS PRÁTICAS

Sempre é importante nos apoiarmos em estruturas reconhecidas como de boas práticas de forma a auxiliar, seja na avaliação da maturidade do gerenciamento de riscos existente ou seja para o desenvolvimento e implantação de um processo estruturado de análise de riscos.

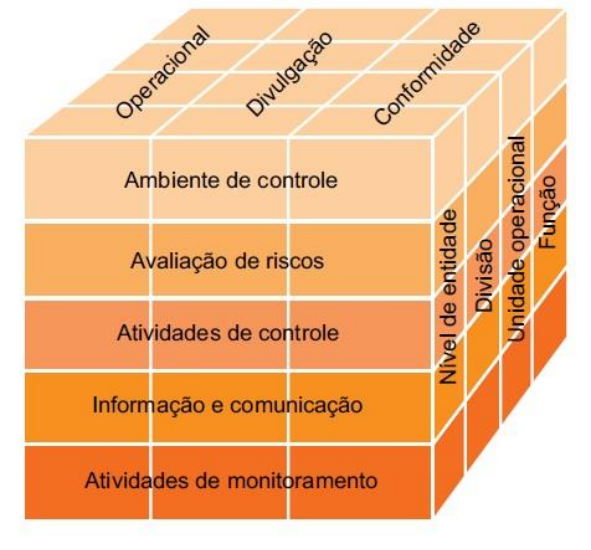
Existem duas estruturas do COSO – *Committee of Sponsoring Organizations of the Treadway Commission* são elas:

COSO Internal Control framework, atualizado em 2013, onde tem seu foco na parte operacional da organização. Ela indica que um sistema de controles internos existe para mitigar três tipos de riscos básicos:

- Operacional – Risco de Eficiência e eficácia, incluindo salvaguarda dos ativos e conformidade com políticas e procedimentos da organização.

- Divulgação - Risco de perda da consistência e integridade das informações e dados transacionados nos diversos sistemas operacionais, sejam eles financeiros e não financeiros.

- Conformidade – Risco da não conformidade com Leis, regulamentos, normas regulatórias, sejam da União, Estado, Município ou agencia e órgão regulador.



Esta estrutura trabalha com cinco componentes importantes para a definição de um sistema de controles internos baseado em riscos. Observem que o ambiente de controle está no topo da estrutura devido sua significativa importância, pois mais importante do que ter um processo de avaliação de riscos é ter a cultura e consciência de riscos e controle de forma que exista comprometimento da gestão com estas boas práticas.

Importante salientar é que antes de definir um controle é necessária uma avaliação de riscos; a comunicação e informação é a base do processo e deve fluir consistentemente de cima para baixo e vice-e-versa. O monitoramento deve ser continuo, responsabilidade da gestão, e também periódico pela auditoria interna.

Este processo deve acontecer em todos os níveis da organização, sem exceção.

COSO Enterprise Risk Management Framework, atualizado em 2017, integrando o gerenciamento de riscos com a estratégia e com o desempenho. Ele ressalta a importância de se considerar o risco tanto no processo de definição das estratégias como também na melhoria do desempenho.

Cada vez que fazemos uma escolha no caminho para atingir um objetivo tem seus riscos, e lidar com estes riscos nessas escolhas faz parte do processo decisório. Segundo o COSO esta nova estrutura e forma de analisar os riscos fornece a alta gestão possibilidades reais de lidar com a crescente volatilidade, complexidade e ambiguidade do mundo, principalmente do mundo dos negócios.

Os dois grandes pontos nesta estrutura é que anteriormente, a gestão de riscos estava baseada na analise dos riscos de não alcançar os objetivos estratégicos. Agora a gestão de riscos sobe um nível, o Conselho passa a ser parte da gestão de riscos e não mais um usuário.

Eles devem, de forma objetiva, avaliar se a estratégia definida está alinhada à missão da organização e também precisa avaliar se esta estratégia está dentro do apetite a risco da corporação e se existem recursos para a sua execução.

Para mim, com certeza, esta são as mudanças mais significativas deste novo framework, e que muda completamente o posicionamento da gestão de riscos na organização.

Diferente da estrutura anterior, que trabalhava em cubo com oito componentes e quatro grandes objetivos, está nova estrutura trabalha com cinco componentes para o processo de gerenciamento, os quais tem como objetivo aperfeiçoar o processo e melhorar o valor criado as partes relacionadas.

Ela segue o mesmo processo da estrutura COSO ICF, e define vinte princípios que norteiam o entendimento dos cinco componentes.

É importante mencionar que o COSO não excluiu o CUBO, deixando o profissional à vontade para continuar utilizando-o, até mesmo, como ele menciona, isto não é uma lei e sim uma melhor prática, que pode ou não ser utilizada pelas corporações.

Uma outra estrutura semelhante é a ISO 31000:2019 elaborada pelo Technical Management Board Working Group on Risk Management, a qual busca definir e padronizar conceitos e processos do gerenciamento de riscos. No meu entendimento ela se equivoca quando afirma que risco é um desvio em relação ao esperado, podendo ser positivo ou negativo. Entretanto fora isto, sua estrutura fornece diretrizes genéricas para o gerenciamento de riscos que pode ser aplicada também para todo e qualquer tipo de organizações.

Um outro modelo que também me chama atenção, e de alguma forma, na minha visão vem complementar as estruturas mencionadas anteriormente é o Orange Book publicado pelo HM Treasury of United Kingdom em 2001 e atualizado no ano de 2004. Um dos pontos que gosto e que é bem significativo é que o componente

comunicação e aprendizado não é uma etapa do processo, mas está inserida nele, de forma que a cada ciclo o processo vai amadurecendo através do monitoramento e feedback.

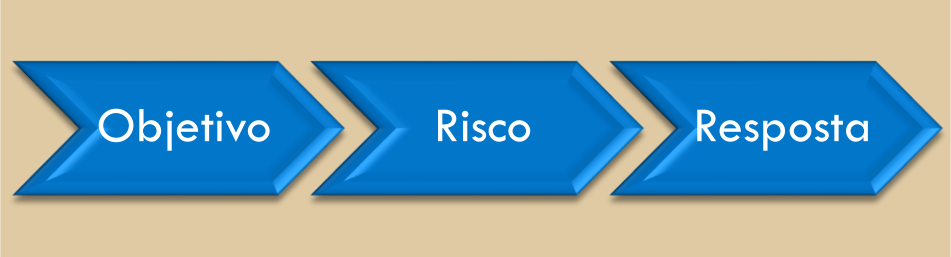
Existem estruturas base para o gerenciamento de riscos as quais podem ser utilizadas como parâmetros, mas as principais são as acimas mencionadas. Para alguns setores existe legislação sobre este processo, como por exemplo a IN conjunta MP/CGU n°1 de 16 que estabelece os parâmetros para as entidades federais; Circular SUSEP 521; Lei 13303/16 para empresas mistas e públicas; CVM, Banco Central e outras.

Fora aquelas empresas que estão em setores regulamentados, as demais devem escolher o paradigma que melhor se adequar à sua cultura e complexidade operacional.

Algumas vezes me perguntam se não existe algum requisito legal, se é imperativo para a qualidade do processo tomar uma destas estruturas como paradigma, e minha resposta é que não, não é necessário, entretanto, é recomendável que se tenha sim um parâmetro de boa prática, pode ser mais efetivo e econômico.

6. O PROCESSO DE ANÁLISE DE RISCOS

Para que exista uma gestão de negócio baseada em riscos, esta deverá trabalhar com a seguinte visão:



O risco está intimamente relacionado com os objetivos, isto é, se não tivermos ou conhecermos os objetivos, não temos como identificar, de forma objetiva, os riscos inerentes, isto é, aqueles riscos que se relacionam diretamente com o objetivo.

De uma forma simples, risco é todo o evento que impacta negativamente a capacidade de alcançarmos o objetivo. Então uma vez que já temos a consciência de que o risco existe precisamos de um processo para poder identifica-lo e trata-lo, de forma a aumentar as chances da organização de alcançar os objetivos pré-estabelecidos.

Conceitualmente, a gestão de riscos é o processo que antecipa o que pode impactar negativamente a capacidade da organização alcançar os objetivos, promovendo a possibilidade de executar ações mitigatórias ou contingenciais.

O oposto da gestão de riscos é a gestão de crise.

Basicamente o processo é simples. Ele é composto por três etapas básicas: etapa da identificação dos riscos, depois avaliação de sua magnitude, e no final o tratamento dos riscos, e se necessário, dependendo da magnitude do risco, a criação de um plano de contingência.

Observem que este processo visa que a empresa, uma vez conhecendo seus riscos brutos (riscos sem nenhum processo mitigatório) possa tomar as ações necessárias para reduzi-lo ao máximo economicamente possível, permitindo que o risco residual (risco remanescente após as ações mitigatórias) esteja alinhado ao seu apetite a risco.

Desta forma, definir e conhecer o apetite a risco é primordial para a efetividade da gestão de riscos. Apetite a riscos é a quantidade de riscos que a organização se sente confortável em correr para criar valor as partes relacionadas.

Vejamos o processo na figura seguinte:

Vejamos cada uma destas atividades para avaliação dos riscos de um processo operacional:

a. Identificação dos Riscos

Nesta etapa precisamos antes de mais nada definir os objetivos do processo que será avaliado. Quanto mais detalhado for a definição do objetivo, melhor será para iniciar a identificação dos riscos inerentes. O risco inerente nada mais é a do que a negativa do objetivo, exemplo: Se o objetivo do processo for comprar apenas serviços e produtos necessários para a operação, os riscos inerentes serão: Não comprar ou Comprar o que não for necessário. A forma mais utilizada para identificação dos riscos é o "Brainstorm", o qual poderá ser apoiado por algumas outras ferramentas para auxiliar na formalização e organização, como: Ishikawa, Bowtie e outros.

É importante que nesta etapa também, tomando como base o COSO ICF, possamos identificar os riscos de conformidade legal, da aplicação da tecnologia da informação no processo e também o risco de fraude. O processo é o mesmo, com pequenas diferenças na definição dos objetivos.

Uma vez que os riscos foram identificados, precisamos identificar suas causas, conhecido também como fatores de riscos. Vocês vão perceber que a resposta ou tratamento não é no risco em si, mas em sua causa.

A formalização desta etapa pode ser em uma matriz simples, onde na primeira coluna são definidos os objetivos do objeto sob avaliação, na segunda coluna são identificados os riscos para cada um dos objetivos e uma terceira coluna

onde serão identificados os fatores de riscos para cada um dos riscos identificados. Ao final desta etapa já teremos três colunas da matriz de riscos preenchidas (objetivo, risco e fator de risco)

b. Avaliação da Magnitude

O risco pode ser medido e isto é realizado de forma matricial através da leitura da probabilidade de ocorrência e seu impacto na organização.

Neste ponto é fundamental que a empresa tenha uma métrica (régua) para a medição da probabilidade e outra para a medição do impacto, de maneira a realizar a medição da magnitude de forma mais objetiva, mesmo sabendo que existe uma grande subjetividade neste processo.

O desafio aqui é ser o mais simples possível, dentro da complexidade da operação.

De nada adianta ter modelos matemáticos sofisticados se no final o gestor ou especialista terá que ter uma posição subjetiva, ou então fica tão complexo que o gestor gasta boa parte do tempo trabalhando no cálculo, deixando de lado o que tem real significado que são as ações para trazer o risco bruto ao apetite a risco da corporação.

Para a formalização desta medição, sugerimos que sejam acrescidas três colunas na planilha utilizada para a formalização dos riscos acima identificados, sendo: uma para a probabilidade, outra para o impacto e uma para a magnitude (resultado da probabilidade x impacto).

c. Tratamento dos riscos

O risco poderá ser tratado somente após sua magnitude ser conhecida, pois para que se possa definir uma resposta adequada, o apetite e a tolerância ao risco deverão ser considerados. Tenha em mente que não é qualquer resposta, mas sim aquela que consegue fazer com que o risco residual esteja alinhado ao apetite a risco.

Existem quatro formas básicas de respostas:

- Aceitar o risco,
- compartilhar o risco,
- evitar o risco e
- mitigar o risco.

Quando falamos em mitigar o risco operacional, estamos falando em definir um controle interno para dar resposta a probabilidade de ocorrência, de forma a

detectar a perda antes e sua ocorrência. Dependendo da magnitude, será necessário também ter um plano de contingência.

A ideia é que a atividade controle interno é trazer o risco residual para o nível de apetite a risco da organização. Aqui sugerimos a elaboração de uma matriz de controle onde todos os controles internos identificados no fluxo do processo sejam relacionados quanto ao seu objetivo, responsável, evidencia, tipo, natureza, periodicidade, etc.

d. Contingência

Como disse, dependendo da magnitude do risco será necessário, além da definição da resposta, a criação de um plano de contingência.

Sabemos que um controle interno não é absoluto, ele pode falhar, e por isso é necessário ter um plano para reduzir o impacto do evento, resultado da falha do controle.

Quando a resposta for diretamente no impacto, em casos de fatores externos, a mitigação não será um controle, mas sim, um plano contingencial para redução do impacto se o evento se materializar.

7. CONCLUSÃO

Como podem observar a estruturação do processo de gerenciamento de riscos é relativamente simples, entretanto, sua implementação não é tão simples, pois afeta diretamente a cultura e a forma de gerir os processos decisórios.

Em uma pesquisa de maturidade do processo de gestão de riscos no Brasil realizado pela empresa de auditoria KPMG os cinco obstáculos mais citados para implantação da gestão de riscos são:

- 65% - Ausência de cultura em gestão de riscos
- 56% - Existência de outras prioridades
- 52% - Falta de clareza em relação aos benefícios potencias
- 45% - Falta de apoio dos executivos
- 36% - Resistencia às mudanças no âmbito do Conselho de Administração e diretoria

Outro dado interessante é que somente 19% das empresas participantes possuem apetite a risco formalizado e implementado. Este dado por si só já demonstra a falta de efetividade da gestão de riscos das empresas no Brasil.

Como vocês podem ver, as dificuldades para a implantação do processo são inúmeras, então procurem ser o mais simples possível, dentro da complexidade da organização, na definição do processo, principalmente na medição da magnitude. Não interessa saber dez casas após a virgula, o que precisamos saber é se a magnitude do risco é 3 ou 4, não se é 3,2785.

O que precisa ser trabalhado é a ação que será tomada sobre a leitura do risco, e não a forma e acuracidade de como está sendo medido. Fujam de soluções “one fits all” ou complexas, perderão tempo, dinheiro e credibilidade.

Busque a simplicidade que além de melhorar o desempenho é economicamente muito mais efetiva.

8. BIBLIOGRAFIA

Guide to the CICS Common Body of Knowledge, version 7.1 – Internal Control Institute, USA

Framework COSO ICF 2013 e ERM 2017 – Committee of Sponsoring Organizations of the Treadway Commission, USA

The Orange Book, Management of Risk – Principles and Concepts, HM Treasury, UK

Pesquisa Maturidade do Processo de Gestão de Riscos no Brasil, 1ª edição, KPMG, Brasil

ABNT – Associação Brasileira de normas técnicas, NBR ISO 31000:2019, Brasil

MP/CGU - Instrução normativa conjunta nº1 de 2013, Brasil

9. SOBRE O AUTOR

EDUARDO PERSON PARDINI

Bacharel em Ciências Contábeis pela FACESP – Faculdade de Ciências Econômicas de São Paulo. Pós-graduado em Administração concentração em Finanças. Especialização em Estratégia pela Wharton Business School. Especialização sobre Governance, Bribery and fraud pela Milliken University, Certificado CICP – Certified Internal Control Institute USA.

Auditor externo na Coopers & Lybrand, Gerente na Price Waterhouse, Diretor de Auditoria Internacional Latin America da Grand Metropolitan PLC, Chief Financial Officer Latin America da ISP International Specialty Products, Diretor Financeiro da Iochep Maxion, Chief Financial Officer LA da Milliken Corp.

Sócio principal da Crossover Consulting & Auditing Corporation, Diretor executivo do Internal Control Institute Brasil. Palestrante e professor de Gerenciamento de riscos, governança, auditoria interna e controles internos pela Crossover Brazil, ICI Brasil, e professor de MBA na Trevisan Escola de Negócio.

10. SOBRE A CROSSOVER

CROSSOVER
CONSULTING & AUDITING

Somos uma empresa com 10 anos de sólida experiencia em Gestão Empresarial, Auditoria Interna, Controles Internos, Riscos e Governança Corporativa.

CROSSOVER
CONSULTING & AUDITING

Governança

Gestão	Controles internos Auditoria Interna Gestão Riscos Compliance	Capacitação
• Mentoria • Estratégia • Fluxo Financeiro • Diagnóstico • Otimização de custos • Organização • Interin Mgmt.	• Mentoria • Diagnóstico • Mapeamento • Implantação • Co-sourcing • Outsourcing • Comitê • Quality review	• Auditoria • Riscos • Compliance • Controles internos • TI • Fraudes • Contábil

Nossos Serviços


CROSSOVER
CONSULTING & AUDITING
Presença Nacional e Internacional
Fort Lauderdale
São Paulo
Curitiba
Porto Alegre


CROSSOVER
CONSULTING & AUDITING
Internal Control Institute
Brasil
Nossos escritórios
Brasil
São Paulo
Rua Alexandre Dumas, 1711 - 5° Andar
Chácara Santo Antonio, SP - SP
Fone 55+11+2599 8360
Curitiba
Rua Pasteur, 463 - 13° Andar
Agua Verde, Curitiba - PR
Fone 55+41+2101 1622
Porto Alegre
Rua Dr. Alcaraz Caldas, 90 - 8° Andar
Praia de Belas, Porto Alegre - RS
Fone 55+51+3533 8566
Estados Unidos
Corporate Office
460 Jefferson Dr. Bld 29 #203
Deerfiled Beach, FL 33442-9562
email: corporateusa@crossoverbrazil.com