REVISTA
GESTÃO DE RISCOS

b&a BRASILIANO & ASSOCIADOS

EDIÇÃO 99
JULHO 2016

Transparência meta da alta administração, será?

Os escândalos de corrupção continuam a produzir manchetes no mundo inteiro e as economias emergentes têm destaque nesse cenário.

Prof. Dr. Antonio Celso Ribeiro Brasiliano, CRMA, CES, DEA, DSE, MBS

Doutor em Ciência e Engenharia da Informação e Inteligência Estratégica pela Université East Paris - Marne La Vallée – Paris – França, Publisher da revista Gestão de Riscos, diretor-presidente da Brasiliano & Associados

abrasiliano@brasiliano.com.br

Seja a campanha anticorrupção do governo chinês, o grande escândalo de corrupção no Brasil ou as alegações de desvio de fundos envolvendo o primeiro- ministro da Malásia, o impacto da corrupção prejudica seriamente as economias emergentes em um momento na qual são fustigadas pela desaceleração do crescimento.

Apesar dos desafios da crise econômica e das consequências destrutivas dos escândalos de corrupção, as multinacionais de mercados emergentes continuam a ocupar um lugar importante nos mercados regionais e globais. Embora existam previsões negativas sobre o futuro de curto prazo dos mercados emergentes e das economias dos BRICS (Brasil, Rússia, Índia, China e África do Sul), especificamente, esses países ainda são responsáveis por 30% da produção mundial, sendo que suas empresas mais dinâmicas continuam a buscar oportunidades comerciais no mercado nacional e internacional. Assim como outras multinacionais importantes, elas devem desempenhar seu papel no combate à corrupção e elevar os padrões de integridade e transparência nos negócios.

Empresas bem administradas que operam com altos níveis de integridade e transparência estão mais propensas a manter a vantagem competitiva no mercado global, em que práticas comerciais desleais ou obscuras apresentam ameaças crescentes ao sucesso empresarial. No Brasil, as consequências do escândalo da Petrobras custaram não só sua reputação, como lucros cessantes estimados em US$ 1,5 bilhões.

A divulgação abrangente de informações públicas é um componente fundamental das medidas que as empresas devem empregar para enfrentar a corrupção e fornecer a transparência que forma a base de uma governança sólida e responsável. No entanto, os esforços voluntários são restritos e obrigações regulatórias e jurídicas realmente promovem uma maior transparência corporativa.

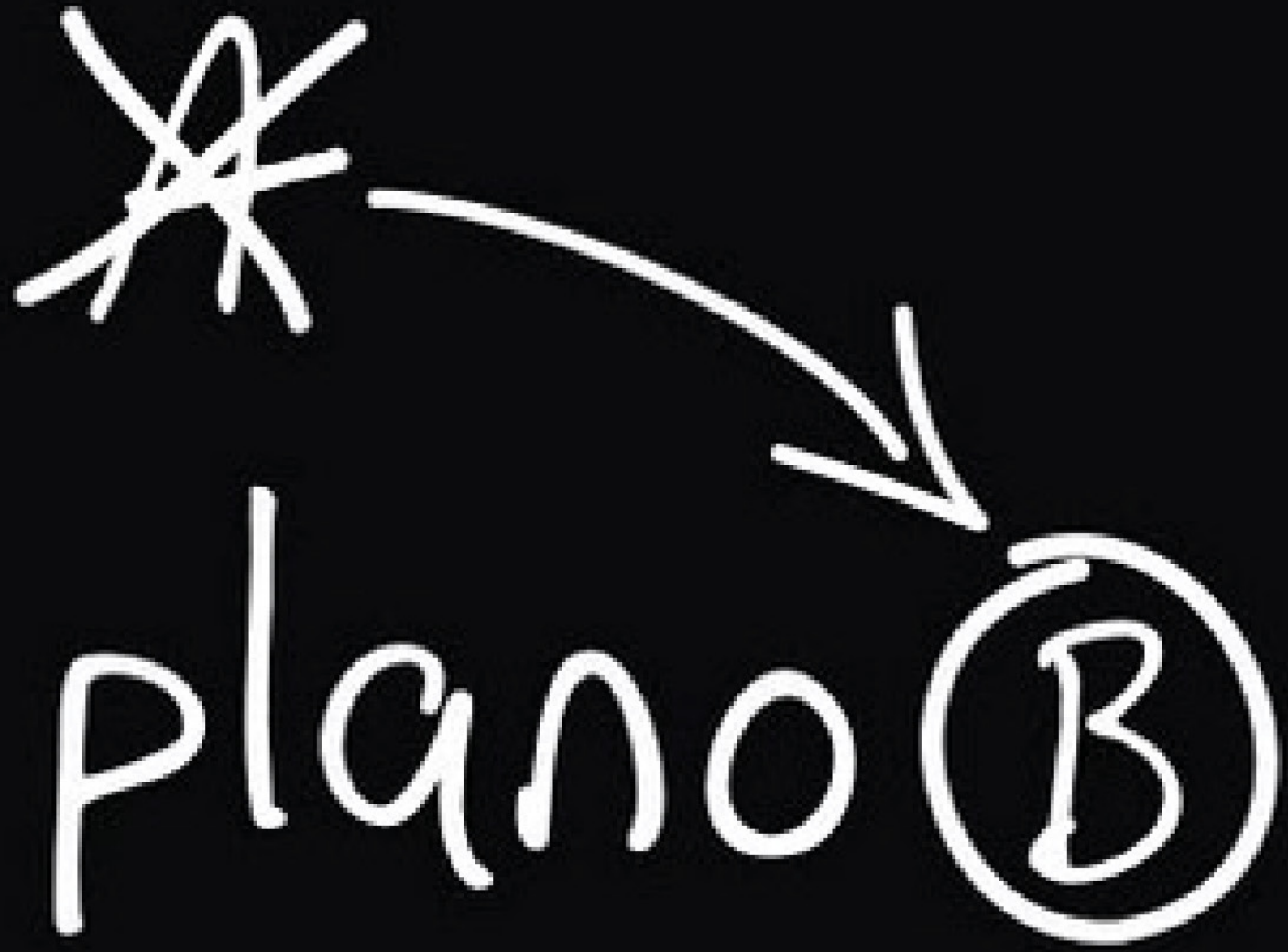
Como resultado da pressão exercida pela União Europeia, pelos EUA e por outros países, novas leis e novos regulamentos foram adotados. A finalidade dessa adoção é criar novos padrões globais obrigatórios de transparência, principalmente para as indústrias do setor extrativista, além de outros setores, tais como o setor financeiro e madeireiro. Na União Europeia, há propostas para expandir esses requisitos para todos os setores.

Essas alterações afetarão grandes empresas de economias desenvolvidas, mas muitas multinacionais de mercados emergentes não escaparão do impacto. Sendo assim, essas empresas têm interesse em se prepararem para uma nova era de transparência global. Os governos e os reguladores também devem desempenhar sua função na construção de uma demanda consistente pela transparência corporativa.

Desta forma é imperioso que os membros dos conselhos de administração e os diretores executivos estejam cientes das suas reais obrigações e responsabilidades, no que tange a cobrar o processo de Gestão de Riscos Corporativos, integrados com Controles Internos, Governança e Conformidade.

A aplicação do conceito maior das três linhas de defesa passa a ser pilar estratégico para que as empresas possam, de fato, possuírem uma real governança e transparência com os controles e riscos gerenciados. Basta a alta administração cobrar! Como sempre falo em minhas apresentações cenoura e nabo!

Sorte e sucesso para todos nós!! Boa Leitura!



revise seu plano de
contingência e emergência

www.brasiliano.com.br

b&a
BRASILIANO & ASSOCIADOS
GESTÃO DE RISCOS

Jocelia B. Oliveira

Aluna do Curso de Pós Graduação em Gestão de Riscos – MBA pela Faculdade de Engenharia de São Paulo e Brasiliano & Associados e trabalha na Net São Paulo.

A falta do compliance pode comprometer os objetivos estratégicos da empresa

É possível notar que nem todas as empresas veem a importância do Compliance dentro de seu universo empresarial. Muitas vezes, preferem remediar do que prevenir e acabam deixando a empresa vulneráveis aos riscos tendo altos prejuízos, comprometendo seus objetivos estratégicos.

Empresas que se sujeitam a travar longas brigas judiciais por leis trabalhistas que foram desrespeitas, arcar com multas pesadas da Receita Federal por falhas em sua prestação de contas ao Fisco ou até mesmo receber imposições por descumprimento às leis ambientais, acabam por enfraquecer a empresa no mercado, perdendo sua credibilidade, seus lucros e suas perspectivas de futuro.

Organizações que não valorizam o Compliance e a importância de atuar dentro das regras é o que explica, muitas vezes, os índices de falência de empresas com até 5 anos chegando aos 50% no Brasil. Conforme indicativos, menos de 20% das empresas chegam aos seus 10 anos de vida, por falta de controles internos, falhas de gestão, respeito às normas e regulamentação.

Por isso, é de vital importância que as organizações que desejam atingir seus objetivos estratégicos, implantem uma comissão de Compliance em suas organizações para que a empresa não fique vulneráveis aos riscos e comprometa seus objetivos.

Alinhando a função de compliance aos objetivos estratégicos,

MISSÃO E VISÃO

Devido ao aumento de pressões externas solicitadas pela adoção de padrões éticos, que gere valor a todos os membros da organização, bem como fornecedores, atacadistas, varejistas, etc., deve impulsionar as organizações para a criação de programas preventivos e de monitoramentos constantes. Através das ferramentas de compliance é possível que uma empresa possa alcançar com mais solidez seus objetivos estratégicos.

A sinergia da empresa com todas as normas, ditames de regulamentação e controles internos eficientes, representam maior qualidade na atividade empresarial economia de recursos, evitando gastos com multas, punições e cobranças judiciais e com isso, o fortalecimento da marca no mercado como empresa séria e ética.

Objetivos, papéis e responsabilidades da função de compliance na organização

Para a organização desempenhar adequadamente a função de compliance é necessário que esteja de acordo com os seguintes objetivos:

- Analisar meticulosamente os riscos operacionais;
- Gerenciar os controles internos, devendo o profissional atuar não só como um “xerife”, mas como um consultor orientando aos colaboradores sobre as normas e procedimentos da empresa;
- Desenvolver projetos de melhoria contínua e adequação às normas técnicas;
- Analisar e prevenir de fraudes à empresa, atuando o profissional como um consultor que irá orientar as áreas envolvidas;

A falta do compliance pode comprometer os objetivos estratégicos da empresa

- Monitoramento, junto aos responsáveis pela TI, no que se refere às medidas adotadas na área de segurança da informação;
- Realização de auditorias periódicas;
- Gerenciar e rever as políticas de gestão de pessoas, juntamente com os responsáveis pela área de Gestão de Recursos Humanos;
- Trabalhar na elaboração de manuais de conduta e desenvolver planos de disseminação do compliance na cultura organizacional;
- Fiscalização da conformidade contábil de acordo com as normas internacionais (International Financial Reporting Standards – IFRS);
- Interpretar leis e adequá-las ao universo da empresa.

Compliance e controles internos

É muito importante para a empresa, que além de interpretar as leis que regem suas atividades, com amparo de especialistas em assessoria jurídica, a empresa precisa da ajuda de outros profissionais de controles internos e análise de riscos, como parte integrante no processo de construção de um departamento nesse campo, no que tange a entendimento das leis e normas internas.

O profissional de Compliance necessita entender melhor as suas funções que vão além de elaborar e publicar normativos e procedimentos e estar direcionando as responsabilidades aos gestores de áreas. É necessário que este profissional entenda o que está sendo cobrado e como podem melhorar as atividades e proporcionar maiores índices de eficiência, eficácia e confiabilidade das informações, que é a base de toda decisão.

A atividade de prevenção a fraudes; segurança da informação; plano de continuidade de negócios; contabilidade internacional, fiscal e gerencial; gestão de riscos e de pessoas; atendimento a auditorias internas e externas; dentre outras, formam o leque de atribuições do profissional de compliance, que deverá dominar conhecimentos sobre o negócio, as metas e objetivos dos administradores.

Desta forma, os controles internos terão seu papel levado mais a sério nas organizações, independentemente de tamanho ou atividade econômica, as normas legais emanadas pelos órgãos reguladores serão cumpridas à risca e a auditoria interna poderá trabalhar com rapidez e eficiência.

Conforme pesquisa realizada pela empresa Deloitte as principais barreiras para a adequada implementação de um programa de anticorrupção são:

Externas:

1. Cultura do País;
2. Burocracia pública;
3. Postura dos fiscais governamentais.

Internas:

1. Forma de fazer negócios;
2. Segmento de atuação suscetível à corrupção;

3. Estrutura da empresa.

Essa mesma pesquisa realizada pela empresa Deloitte, relatou que as principais formas de corrupção no setor são:

1. Pagamentos indiretos (pagamentos a agentes, representantes, intermediários, ou outros terceiros contratados);
2. Presentes, brindes, hospitalidade, entretenimento e viagens inapropriadas;
3. Facilitação de licenças.

Empresas sem compliance, mesmo as pequenas estarão fora do mercado

O Compliance funciona como uma forma de dar transparência da conduta empresarial perante a sociedade e autoridade, pois caso a empresa seja atingida pela Lei Anticorrupção (Lei nº 12.846/2013), o Compliance, quando existente e efetivamente aplicado, tem a aptidão de atenuar a aplicação das gravosas penalidades mencionadas.

O Compliance e suas normas tem como objetivo guiar a organização em relação a todas as suas vertentes, atuações e relações internas e externas, tendo como função principal não só evitar atos de corrupção, mas organizar a padronizar a gerência, produção e forma de produção, emissão de relatórios, etc. Através do Compliance a empresa cria regras próprias que a deixam mais profissional e menos suscetível a erros, além de atos de corrupção, ou seja, trata-se de uma nova cultura empresarial, com governança corporativa adequada e aptas às exigências legais e sociais que dispomos atualmente.

Os pequenos empresários pensam que Compliance é necessário apenas para as grandes empresas, pois as pequenas empresas são muito simples para chamarem a atenção. Porém, a fiscalização governamental é muito ampla e, em grande parte, eletrônica e automática. A Receita Federal do Brasil monitora as relações das empresas entre si, os bancos estão obrigados a informar movimentações consideradas “elevadas” e até as operadoras de cartão de crédito são obrigadas a prestar informações de seus clientes, ou seja, ninguém mais está livre de fiscalização.

No entanto, o que o Compliance traz de importante e que refletirá nas pequenas empresas é o fato de que essas normas, por sua natureza, exigem regras e prova de probidade também para clientes, parceiros, fornecedores, todos que tenham qualquer tipo de relacionamento. Com isso, as grandes empresas, para contratar, exigirão que os parceiros tenham Compliance, como forma de resguardar a si própria caso ocorra algum ato lesivo ou mesmo de corrupção.

É importante observar que o Compliance não é algo padronizado e nem de imposição automática, é necessário que seja implantado na empresa não como uma quebra de paradigma, mas como uma consagração das boas práticas próprias já existentes, além de criação de novas. Mas, para isso exige-se preparação, adaptação e treinamento para que surtam efeitos práticos e traga benefícios reais à empresa, servindo também de escudo para os casos de corrupção.

Também, é importante destacar, que a manutenção do Compliance não exige que haja um aumento de custos ou contratação de pessoal, ou seja, a comissão do Compliance é um órgão dentro da empresa responsável pela fiscalização e manutenção desse tipo de conformidade e deverá ser composto por pessoas da própria empresa, em colaboração com a alta direção.

Conforme estudo da empresa Deloitte intitulado “Lei Anticorrupção - Um retrato das práticas de Compliance na era da empresa limpa”, indicou-se que 57% dos executivos concordam que corrupção é um custo intrínseco na forma de se fazer negócios no Brasil. “A demanda da sociedade por maior transparência é irreversível. As empresas e as instituições serão cada vez mais cobradas neste sentido”, afirma Camila Araújo, sócia-líder do Centro de Governança Corporativa da Deloitte. O Fórum Econômico Mundial calcula que o custo da corrupção equivale a US$ 2,6 trilhões por ano, ou em torno de 5% do Produto

Com o Compliance, verificamos que o maior investimento que se pode ter será o comprometimento de todos, resultando em uma empresa com governança corporativa responsável, atraindo parceiros e até mesmo investidores.

Futuramente, o Compliance será indispensável a qualquer empresa e aquelas que logo se adequarem estarão à frente no mercado, abrindo maiores oportunidades para contratações e inclusive, utilizando a existência do Compliance como fator de qualidade, agregando valor às suas prestações.

Curso Gestão de Risco Corporativos

A Brasiliano & Associados, através do seu Presidente Prof. DR. Antonio Celso Ribeiro Brasiliano, CRMA,CES,DEA,DSE,MBS, ministrou na Rumo Logística, Curitiba, Paraná, nos dias 11 a 13 de julho de 2016 o Curso Gestão de Corporativos, alinhado com a ISO 31000, para a Equipe de Segurança Empresarial e Prevenção de Perdas a nível Brasil.

Curso Gestão de Riscos Corporativos

O Prof. Dr. Antonio Celso Ribeiro Brasiliano, CRMA,CES,DEA, DSE, MBS, ministrou a aula, para o Curso da FIA - USP/Sicredi, Gestão de Riscos Corporativos , na cidade de Porto Alegre, RGS, para os Gerentes de Unidades no dia 19 de julho de 2016.

Palestra Controles Internos, Riscos e Prevenção a Fraudes

O Prof. Dr. Antonio Celso Ribeiro Brasiliano, CRMA,CES,DEA, DSE, MBS, ministrou, para o Sicredi, na cidade de Tapejara, RGS, Palestras versando sobre Controles Internos, Riscos e Prevenção a Fraudes para os Gerentes de Unidades, Diretores e Membros do Conselho da Regional do Sicredi, no período de 27 e 28 de julho de 2016.

Prof. Dr. Antonio Celso Ribeiro Brasiliano, CRMA, CES, DEA, DSE, MBS

Doutor em Ciência e Engenharia da Informação e Inteligência Estratégica pela Université East Paris - Marne La Vallée – Paris – França, Publisher da revista Gestão de Riscos, diretor-presidente da Brasiliano & Associados

A nova função do gestor de riscos corporativos: fornecer inteligência em riscos

O atual contexto de Gestão de Riscos Corporativos das organizações, no Brasil e no mundo, está cada vez mais complexo e dinâmico, exigindo um processo com alta flexibilidade e, mandando um nível elevado da área de gestão de riscos, bem como uma maior tempestividade na avaliação contínua e na resposta a potenciais cenários de riscos.

Isto significa que o gestor de riscos corporativos deve ser competente para poder integrar e interpretar as diversas informações das disciplinas de riscos da suas empresas com o objetivo de fornecer para a Alta Gestão Inteligência em Riscos. Este passa a ser o maior desafio deste século para os gestores de riscos das empresas!!.

Hoje em dia a visão e o escopo do gerenciamento de risco corporativo ficou muito mais amplo, muito mais holístico, abrangendo inúmeras disciplinas de riscos nas corporações, decorrentes das atividades desenvolvidas. A alta direção deve ter uma visão consolidada de suas exposições, sejam operacionais, legais, financeiras e ou estratégicas. Para este fim, é necessária a criação de uma área específica, com uma estrutura e recursos definidos.

As atividades de um departamento de gerenciamento de riscos corporativos, dentro do enfoque moderno, abrange inúmeras disciplinas. Muitas dessas atividades são comuns a uma ampla gama de funções administrativas. Por esta razão, é que este departamento deve possuir processo sistêmico e contínuo de identificação de exposição, medição, análise, controle, prevenção, redução, avaliação e financiamento de riscos. Esta nova função ajuda a integrar riscos financeiros e não financeiros tradicionais a seguros e responsabilidade legal. É uma área que possui uma grande abrangência, mas com muitas interações através de diferentes disciplinas e, portanto, com uma necessidade de uma abordagem integrada. Algumas das disciplinas de riscos que devem se interagir são:

1) Riscos estratégicos
2) Riscos operacionais – ligados a operação
3) Riscos nos processos
4) Riscos de tecnologia da informação
5) Riscos de meio ambiente
6) Riscos de saúde e segurança do trabalhador
7) Riscos de segurança empresarial
8) Riscos financeiros
9) Riscos legais
10) Riscos sociais
11) Riscos de sustentabilidade
12) Riscos de comunicação
13) Riscos de fraudes
14) Riscos na cadeia logística
15) Riscos no projeto
16) Outras tantas disciplinas

Estas disciplinas devem estar integradas com um único Framework e com Políticas integradas, visando a empresa falar uma mesma linguagem. Este é o principal desafio das empresas, integrar as disciplinas para que possam possuir a chamada Inteligência em Riscos Corporativos – IRC.

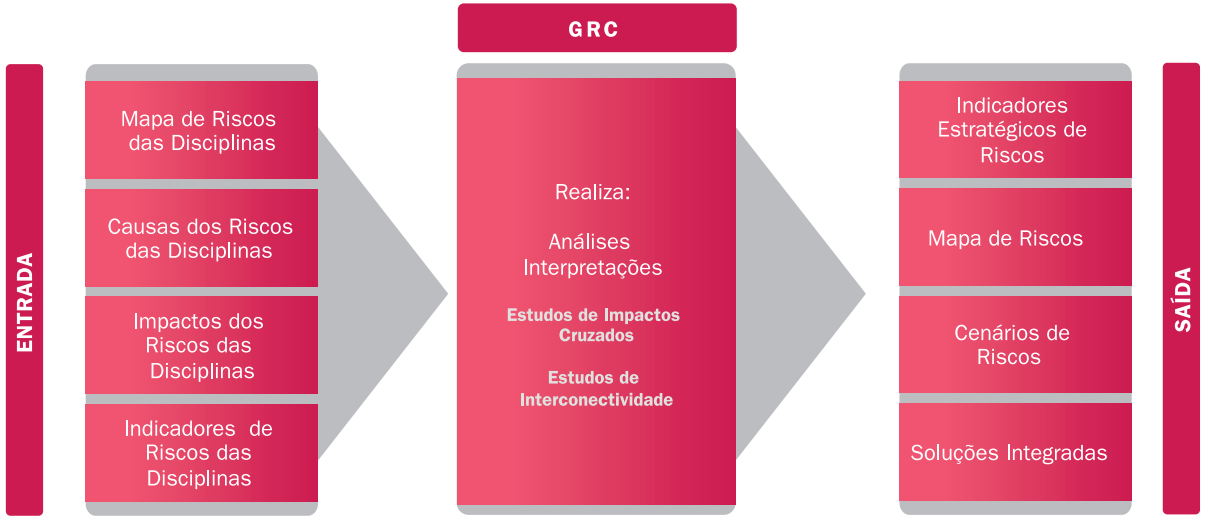
O gerenciamento de riscos, sob este enfoque, contribui para o fortalecimento e a eficácia operacional e financeira da empresa, na medida que proporciona mecanismos de alocação de recursos para o seu emprego mais eficiente e eficaz, atingindo de forma direta a efetividade.

Portanto a função do gestor de riscos é de integrar disciplinas e gerenciar as informações das inúmeras disciplinas de riscos. O gestor de riscos tem que relacionar os diversos riscos e verificar as interdependências entre eles. Hoje por si só não existe mais a possibilidade de só ter como ferramenta de gestão a Matriz de Riscos, mas deve também ter a Matriz de Impactos Cruzados para ver a motricidade entre riscos. Segundo o Fórum Econômico Mundial, em seu Relatório de Riscos Globais de 2015 ressalta: "A edição 2015 do relatório de Riscos Globais completa uma década destacando os riscos a longo prazo mais significantes ao redor do mundo, extraindo as perspectivas de especialistas e dos tomadores de decisões globais. Nesse tempo, a análise mudou da identificação dos riscos a pensar através das interconexões dos riscos e os potenciais efeitos-cascata que resultarão deles."

Podemos então afirmar que a função do gestor de riscos corporativos é possuir Inteligência em Riscos, levado para a alta administração os riscos considerados mais críticos, já com as conexões feitas. A figura ao ladomostra um modelo de gestão.

Com o modelo ao lado entendemos a Inteligência em Riscos em integrar soluções e indicadores, fornecendo para os decisores a visão holística dos riscos considerados críticos e as respectivas soluções integradas, com um farol de monitoramento de acompanhamento das evoluções. Desta forma a organização possuirá verdadeiramente condições operacionais de se antecipar de forma objetiva a possíveis riscos, trabalhando de forma preventiva, através de indicadores e cenários, e não mais de forma reativa. A organização ganha com isso velocidade e competitividade, fatores chaves de sucesso em um mundo com extrema volatidade.

A abrangência da área da Gestão de Riscos Corporativos é muito grande, deixando de ser somente uma abordagem financeira e regulamentar – trabalhista, tributária e de investimento. A tendência é que a área de gestão de riscos caminhe para fatores de interesse de seus stakeholders, com forte atenção à imagem e à reputação das organizações. Por esta razão a amplitude cresceu



e acabou abrangendo a organização como um todo, envolvendo as médias gerências como responsáveis na gestão de riscos corporativos. Desta maneira a área de riscos passa atuar como uma área de Inteligência em Riscos, ou seja, de interpretação das informações e utilização de ferramentas estratégicas. A figura ao lado demonstra esta abrangência nas áreas e processos das organizações, incluindo os fornecedores críticos/estratégicos.

Outro ponto a destacar na nova função do Gerenciamento de Riscos Corporativos e do seu Gestor é o foco de atuação do gestor de riscos, que tem que ser o da prevenção, o da antecipação, como resposta aos cenários de riscos. Tem que ter também estruturado o chamado plano "B", as respostas de emergências, descontinuidade de negócio e de crises. Atualmente o mercado identificou a necessidade de uma abordagem integrada a gestão de riscos, envolvendo temas como mercado, estratégia, modelo de negócio, segurança cibernética, anticorrupção e reputação corporativa. Essa abordagem demanda compreender e responder a interconectividade entre riscos de diferentes naturezas à medida que, e muito impulsionado pela tecnologia, os mais variados fatores podem gerar cenários de descontinuidade e de crises, impactando as operações e os res-

Abrangência da área de Gestão de Riscos Corporativos nas empresas.

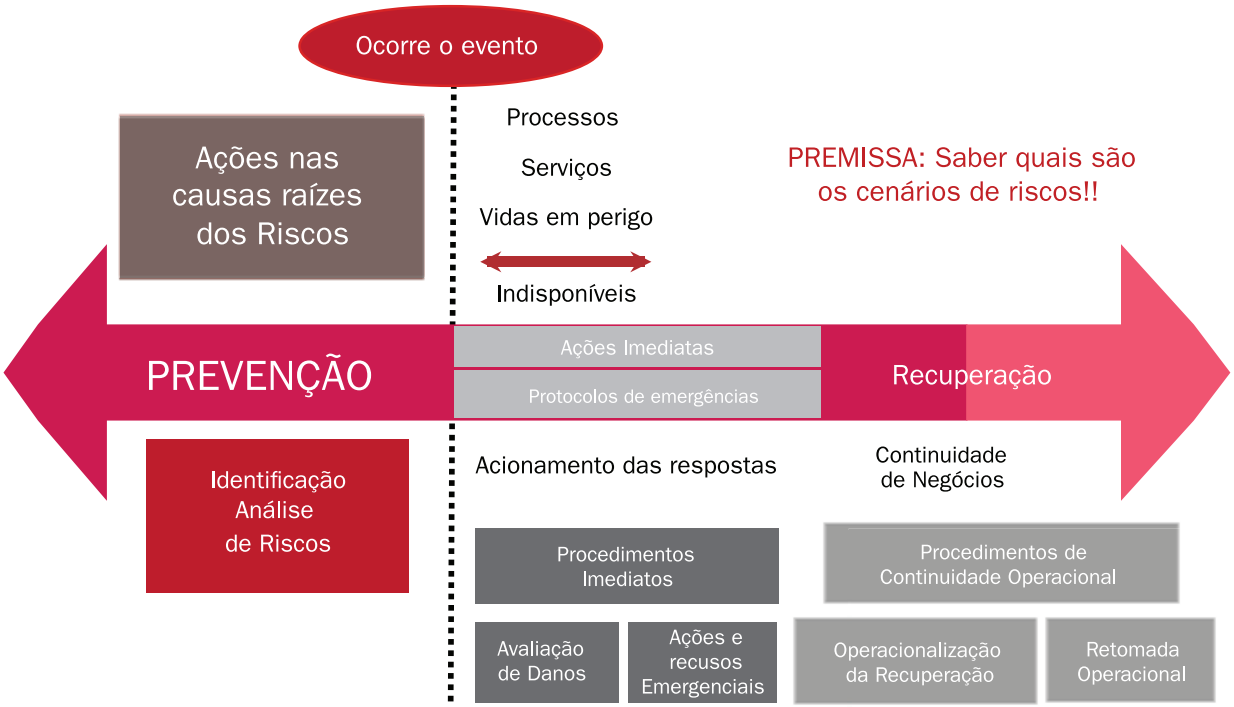
pectivos resultados das empresas no curto, médio e longo prazo.

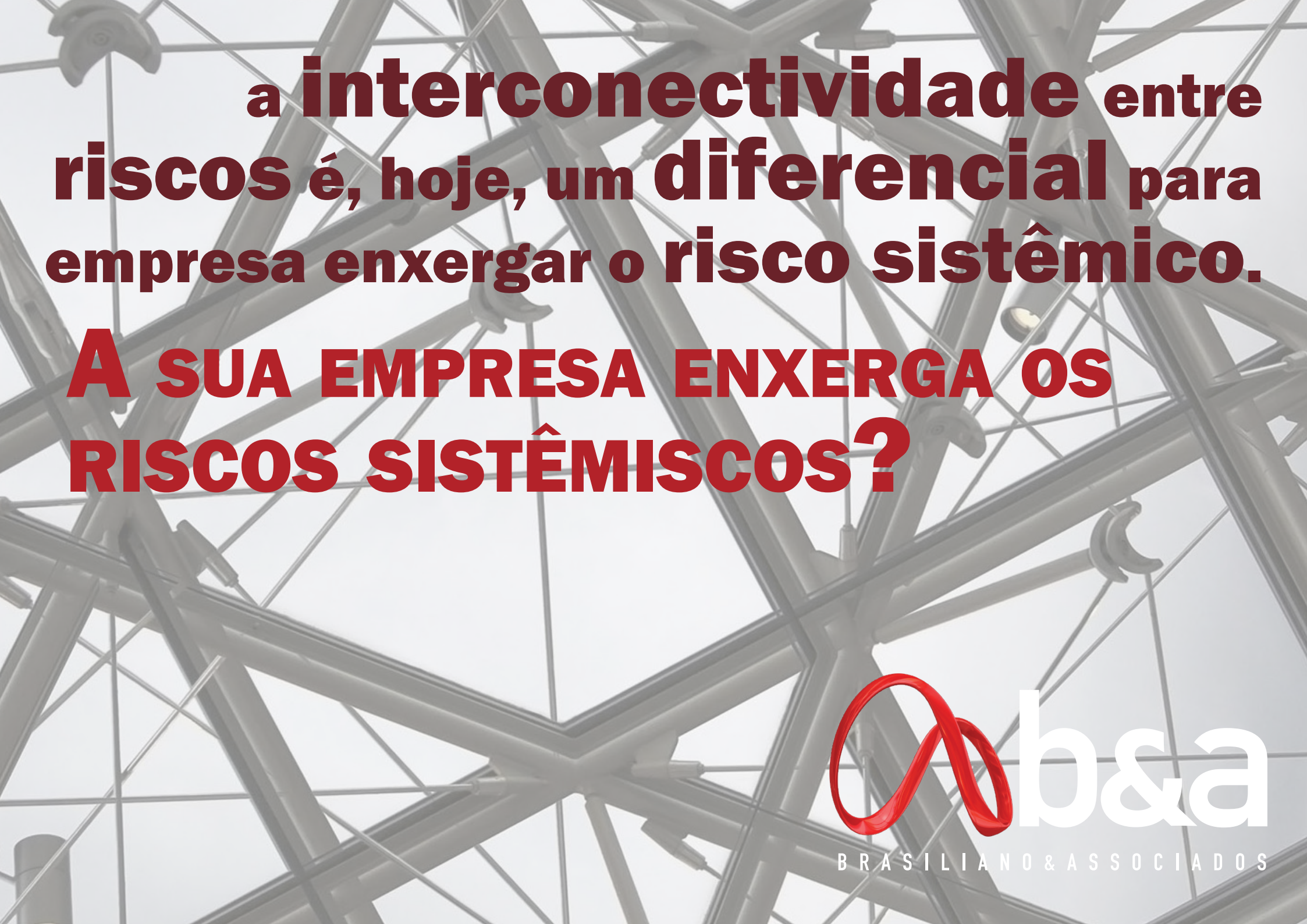
Frente a este novo contexto, mundo volátil, torna-se imperioso que as empresas intensifiquem esforços no aprimoramento nas estruturas integradas – Inteligência em Riscos – onde o gestor possa enxergar e trabalhar tanto a prevenção como as contingências. Na verdade a função do gestor de riscos é de um "chapéu de dois bicos": um lado a prevenção e do outro as respostas para as emergências, continuidade de negócio e crises empresariais. Tudo isso integrado em um único Framework.

A função da gestão de riscos, vista sob a ótica estratégica, atua no aumento da resiliência empresarial. Nesse sentido, a maturidade dessa função interfere diretamente na qualidade e entendimento global dos riscos, sejam eles internos e ou externos, que podem produzir relevantes cenários de descontinuidade e ou de crises.

O grande passo da gestão de riscos está relacionado com a definição e a qualificação de um panorama dos potenciais cenários de descontinuidade e de crise, que podem e ou devem serem gerados com base na avaliação geral de riscos operacionais, legais e estratégicos, levando em consideração a linguagem comum de riscos e o impacto para as operações e a reputação da empresa. Essa base de potenciais cenários de descontinuidade e ou de crises deverão orientar a estruturação dos planejamentos das respostas estruturadas e respectivas alternativas. É nesse momento que, deve se definir, com extrema clareza, o nível de complexidade e dimensão do impacto no contexto (empresa e sociedade como um todo).

No quadro abaixo podemos visualizar uma visão holística do processo preventivo e contingencial da função do gestor de riscos do século XXI.




a interconectividade entre riscos é, hoje, um diferencial para empresa enxergar o risco sistêmico.
A SUA EMPRESA ENXERGA OS RISCOS SISTÊMISCOS?
b&a
BRASILIANO&ASSOCIADOS

As vantagens da governança corporativa e compliance para as empresas da atualidade

Juliano Silamá Santolaia

aluno do Curso de Pós Graduação em Gestão de Riscos – MBA pela Faculdade de Engenharia de São Paulo e Brasiliano & Associados e trabalha na Hyundai.

Com o advento da Lei nº 12.846/13, também chamada Lei da Empresa Limpa ou Lei Anticorrupção Empresarial, vigente desde 29/01/14, faz-se necessária a implantação das melhores práticas de Governança Corporativa e de Compliance no ambiente interno, de acordo com o porte e segmento de negócios.

Está cada vez mais em evidência a responsabilidade dos agentes de governança, tais como sócios, administradores, conselheiros fiscais e auditores, diante de temas como sustentabilidade, corrupção, fraude, além da complexidade de relacionamentos que as organizações estabelecem com os mais variados públicos.

Pela definição dada pelo Instituto Brasileiro de Governança Corporativa (IBGC), 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. Ela se aplica a tomadas de decisão estratégicas, como iniciar um novo projeto ou até contextos de impasse entre sócios ou diretoria. Seu objetivo,

basicamente, é recuperar e/ou garantir a confiabilidade de uma empresa para os seus acionistas.

No Brasil a Governança Corporativa surgiu como resposta à crescente demanda por transparência na gestão das empresas. A Bolsa de Valores de São Paulo (Bovespa) implantou em dezembro de 2000 o Novo Mercado e os Níveis Diferenciados de Governança Corporativa (Nível 1 e Nível 2). Esses níveis são segmentos especiais de listagem que foram desenvolvidos com o objetivo de proporcionar um ambiente de negociação que estimulasse, ao mesmo tempo, o interesse dos investidores e a valorização das companhias (BOVESPA, 2009 citada por CASA et al, 2009).

Ainda conforme a Bovespa (2009): "Empresas listadas nesses segmentos proporcionam aos seus acionistas investidores avanço nas práticas de Governança Corporativa que expandem os direitos societários dos acionistas minoritários e aumentam a transparência das companhias, com divulgação de maior volume de informações e de melhor qualidade, facilitando o acompanhamento de seu desempenho".

Desta forma, as companhias com um sistema de Governança Corporativa protegem os seus investidores, divulgando informações sobre o rumo da empresa. Assim, as ações tendem a ser mais valorizadas porque os investidores reconhecem através da transparência da gestão que o retorno dos investimentos em longo prazo é viável e promissor.

A seguir são apresentados os princípios da Governança Corporativa, segundo o IBGC. Quanto mais fiel uma empresa for a essas diretrizes, melhor ela será vista pelo mercado. A sua adequada aplicação resulta em um clima de confiança tanto internamente como e, principalmente, nas relações externas.

a. Transparência: Consiste no desejo de disponibilizar para as partes interessadas as informações que sejam de seu interesse e não apenas aquelas impostas por disposições de leis ou regulamentos. Não deve restringir-se ao desempenho econômico-financeiro, contemplando também os demais fatores (inclusive intangíveis) que norteiam a ação gerencial e que condizem à preservação e à otimização do valor da organização.
b. Equidade: Caracteriza-se pelo tratamento justo e isonômico de todos os sócios e demais partes interessadas (stakeholders), levando em consideração seus direitos, deveres, necessidades, interesses e expectativas.
c. Prestação de Contas: Os agentes de governança devem prestar contas de sua atuação de modo claro, conciso, compreensível e tempestivo, assumindo integralmente as conseqüências de seus atos e omissões e atuando com diligência e responsabilidade no âmbito dos seus papeis.
d. Responsabilidade Corporativa: Os agentes de governança devem zelar pela viabilidade econômico-financeira das organizações, reduzir as externalidades negativas de seus negócios e suas operações e aumentar as positivas, levando em consideração, no seu modelo de negócios, os diversos capitais (financeiro, manufaturado, intelectual, humano, social, ambiental, reputacional, etc.) no curto, médio e longo prazos.

Outro ponto importante da Governança é o Compliance, manter a empresa em conformidade significa adotar um conjunto de medidas

internas de forma a atender aos normativos dos órgãos reguladores e seus próprios regulamentos e processos internos.

Empresas de todos os portes podem se beneficiar de um programa de Compliance. No entanto, os riscos – principalmente de ordem concorrencial – a que uma empresa está exposta variam de acordo com seu porte, posição de mercado, objetivos, etc. Por esta razão, não há um modelo único de programa de Compliance, cada programa deve respeitar as peculiaridades da empresa e ser revisto constantemente de modo a contemplar novos riscos que eventualmente possam surgir, como por exemplo da introdução de um novo produto no mercado.

Os elementos essenciais a um bom programa de Compliance buscam comprometimento, implementação, monitoramento/medição e melhoria contínua e se resumem a, segundo o Fórum ABBC (2011):

1. Padrões de conduta e política e procedimentos formalizados.
2. Designação de um CCO ou comitê.
3. Comunicação efetiva e preventiva.
4. Educação e treinamento para fornecer conhecimento efetivo.
5. Canal de comunicação anônima.
6. Monitoramento de não conformidades e ajuda na redução dos problemas relatados.
7. Ações disciplinares e corretivas.

Programas de Compliance requerem não apenas a elaboração de uma série de procedimentos, mas também (e principalmente) uma mudança na cultura corporativa. O programa de Compliance terá resultados positivos quando seus colaboradores entenderem a importância em fazer a coisa certa sempre. Eles necessitam também entender o que está sendo cobrado e como é possível melhorar as atividades e proporcionar maiores índices de eficiência, eficácia e confiabilidade das informações, que é a base de toda decisão. Uma vez que os funcionários de uma empresa podem apresentar diferentes motivações, o programa dita valores e objetivos comuns, garantindo sua observância permanente.

Tanto a Governança Corporativa quanto seus pilares, como a Compliance, representam um modelo de gestão empresarial fundamental, que aliam boas práticas, organização, métodos, disciplina, ética e procedimentos.

A Governança Corporativa é um novo modelo de gestão adotado por empresas que buscam competir de forma diferenciada no mercado, valorizando a transparência como princípio norteador das relações estabelecidas nos diversos segmentos de negócios, e está sendo inserida no contexto da gestão empresarial para superar conflitos, pois nem sempre os interesses do gestor estão alinhados com os do proprietário.

Empresas que contam com práticas de Governança Corporativa e de Compliance são mais bem vistas no mercado, seja porque demonstram maior transparência, seja porque contam com mecanismos internos de resolução de conflitos.

É importante que os nossos empresários percebam e entendam o que são e para o que servem esses conceitos e as ferramentas que os integram, para que utilizem as melhores práticas a favor de seus negócios e de suas empresas e alcancem maior rentabilidade, competitividade e sustentabilidade.

Cursos In Company e Palestras

Risco de Corrupção: como minimizar

- Lei anticorrupção
- Contexto das fraudes e corrupção nas 3 linhas de defesa.
- Framework ISO 31000, Coso

Solicite informações!

b&a
BRASILIANO & ASSOCIADOS
GESTÃO DE RISCOS

conteúdo delhado
www.brasiliano.com.br
ou entre em contato
11 5531 6171
asilva@brasiliano.com.br

Prof. Dr. Antonio Celso Ribeiro Brasiliano, CRMA, CES, DEA, DSE, MBS

Doutor em Ciência e Engenharia da Informação e Inteligência Estratégica pela Université East Paris - Marne La Vallée – Paris – França, Publisher da revista Gestão de Riscos, diretor-presidente da Brasiliano & Associados

Cyberataques um novo campo de batalhas para o gestor de riscos

Diante de um cenário cada vez mais complexo, dinâmico e interconectado, a virtualização é a palavra-chave para uma proteção mais inteligente e eficaz contra o cyberataques.

O atual cenário da Segurança da Informação está cada vez mais dinâmico e mutável. Todos os dias a mídia noticia algum caso de vazamento de dados, sequestro de informações, invasões maliciosas e ataques de cibercriminosos.

Isso porque os desafios da proteção corporativa no ambiente virtual estão mais complexos diante do surgimento de novas tecnologias, plataformas e aplicações. Internet das coisas, mobilidade, cloud computing e aplicações interconectadas impõem um ritmo completamente diferente aos gestores de Riscos, inclgindo a disciplina Segurança da Informação, exigindo novas formas de defesa cibernética.

Diante desse cenário, nenhum profissional de Gestão de Riscos em Tecnologia da Informação ignorar o fato de que o seu papel mudou e que a função de gerenciar os riscos de Tecnologia da Informação ficou extremamente relevante para as organizações.

A mudança do nível de relevância deve-se a proteção das informações críticas de negócio que as empresas tem que proteger, visando sua sobrevivência. Uma analogia que podemos traçar é com a história da guerra. Afinal, a complexidade da gestão dos riscos da tecnologia da informação fez com que houvesse mudado o campo de batalha, e, para isso, há a necessidade de entendeer muito bem suas características para se sair vitorioso.

Ataque e defesa

A corrida armamentista traz como característica as ações de ataque e defesa. Se um dos lados faz investimento tecnológico para atacar seu oponente, consequentemente o outro deve melho- rar a defesa. Esse tipo de guerrilha dá certo até um certo ponto, onde o aporte feito para a proteção traz resultados positivos, porém, com o passar do tempo, ele deixa de ser eficaz.

Não importa o esforço e aportes investidos, esse sistema simplesmente não funciona mais.

Geralmente isso acontece quando existe um descompasso muito grande entre as partes em termos de tecnologia, proporções de ações de guerrilha ou quando o campo de batalha muda de forma drástica. Aqui, soa um alerta para as empresas sobre a necessidade de mudar a estratégia de proteção. Essa analogia tem tudo a ver com o atual cenário de vulnerabilidades.

O campo de batalha mudou!! Hoje, a transformação digital pela qual as empresas do mundo todo estão passando tornou a luta contra ações cibercriminosas ainda mais complexa. Cada brecha de Segurança é aproveitada pelas quadrilhas de bandidos virtuais, seja uma porta semiaberta, um link despretensioso em um e-mail ou um simples pen drive, tudo pode servir de meio para um ataque virtual. Com esse novo campo de batalha, as empresas devem se armar com tecnologia e novas estratégias.

Cidade murada

Outra analogia do atual cenário de vulnerabilidades é ver o data center como uma cidade murada. Os grandes muros eram tidos como um dos mais antigos sistemas de defesa do mundo e servia de perímetro, uma linha de proteção onde os exércitos posicionavam as tropas e havia apenas uma entrada, geralmente a mais protegida.

Hoje, muitos data centers são tratados como uma cidade murada focada na segurança do perímetro, mas com controles internos mais brandos. Se um cibercriminoso conseguir invadir a porta de entrada, certamente contaminará a parte interna e isso é mais comum do que se imagina.

A estimativa de perdas globais de incidentes, invasões e ataques cibernéticos foi de US$ 500 bilhões, em 2015, número um pouco abaixo do mercado global de drogas, que gira em torno de US$ 600 bilhões. Isso mostra que o mundo do crime virtual dá dinheiro e a sua atratividade só aumenta. Ou seja a relação custo benefício é muito boa.

Os bandidos do cibercrime estão cada vez mais espertos e com a chegada de novas tecnologias como a computação na nuvem, internet das coisas e mobilidade, as políticas de segurança devem ir além da proteção do perímetro. Isso porque hoje vivemos um desalinhamento entre ataque e defesa, tanto em efetividade, quanto em eficiência e investimento.

Estratégia de combate

Os novos ambientes digitais trazem muita interação entre pessoas com múltiplos acessos, redes de comunicação, base de dados, servidores críticos e todo mundo tem que passar pelo portão central da cidade murada. Internamente, as empresas colocam pilhas e camadas de softwares e aplicações a fim de alinhar o controle de segurança.

Antigamente, não era tão complexo fazer as políticas de proteção corporativa, pois as aplicações eram monolíticas. Entretanto, o avanço tecnológico, aplicações altamente conectadas, nativas da nuvem e arquiteturas microsegmentadas exigem uma mudança na estratégia de combate. Os controles devem contemplar a segurança da empresa e de dados mais críticos, mas sem engessar o trabalho dos usuários.

O desafio é proteger a empresa de ataques virtuais modernos, pois os cibercriminosos aproveitam a complexidade que o atual momento traz para as empresas. Em algum momento, o atacante vai conseguir furar o bloqueio da cidade murada, seja por meios próprios ou usando um usuário interno. Uma vez lá dentro, o passo seguinte para o invasor é o movimento lateral, replicando-se continuamente. Aí, Segundo os especialistas, só o investimento em firewalls não é eficaz para a proteção da empresa.

O jogo não é justo, porque as empresas devem ser bem

sucedidas em todas as linhas de defesa, todas as frentes de proteção, enquanto que o atacante se tiver um ataque bem sucedido ele ganha. Existem muitos componentes conversando entre si em uma infraestrutura compartilhada e tudo isso cria um desalinhamento entre a proteção e a defesa.

Virtualização é a solução?

Mas não tem como as organizações continuarem a perder para os cibercriminosos. Como elas podem resolver esse dilema? Como manter seguros o hardware convergente, nuvens, ambientes híbridos e garantir a segurança além do perímetro?

A solução é simples: as empresas devem construir um data center para cada aplicação. Boa parte dos problemas de Segurança da Informação desa- parece quando se monta uma proteção assim. Mas quanto custa? Certamente, milhares de dólares!!

E para quem não tem um grande volume de dinheiro para investir, a melhor solução é a virtualização.

Virtualização é ajudar as empresas a reorganizar a linha de defesa com uma plataforma segura e virtualizada, que permite uma micro segmentação na porta de cada máquina virtual, seja desktop ou servidor. Esse modelo de segurança zero trust está alinhado aos controles internos e às aplicações mais críticas. Os controles de segurança não são mais ligados à rede, mas à uma plataforma com uma camada de abstração, que permite a inserção de serviços de proteção corporativa. Quando as empresas colocam uma máquina virtual para funcionar, a política de segurança já vem embarcada, desde a criação daquele ambiente e os gestores já podem inserir todos os pontos de controle da micro segmentação. A segurança passa a acompanhar a máquina virtual para onde ela for, seja em camadas ou pelos data centers.

A virtualização é a peça-chave para uma segurança inteligente e proativa, pois ela cria uma camada de abstração entre as aplicações e a infraestrutura. O campo de batalha está mudou. Não podemos mais fazer a segurança da forma antiga, colocando as políticas de segurança atreladas a uma porta ou ao um endereço IP. Isso ficou para trás. Hoje, as aplicações precisam de uma Segurança dinâmica e inteligente.

Lembram do mundo VUCA?

Já acontece.

Estamos preparados?

ler e saber

Sicurezza
EDITORA

16 de setembro
Lançamento

Cursos In Company e Palestras

A importância da 2ª Linha de Defesa na eficácia da Gestão de Riscos

Solicite informações!!

- Qual o papel da 2ª linha de defesa e sua responsabilidade?
- Como identificar riscos nos processos?
- Como controlar e monitorar Riscos?

b&a
BRASILIANO & ASSOCIADOS
GESTÃO DE RISCOS

conteúdo delhado
www.brasiliano.com.br
ou entre em contato
11 5531 6171
asilva@brasiliano.com.br

CURSOS ONLINE

otimize seu tempo

adquira no site www.sicurezzaeditora.com.br

REVISTA
GESTÃO DE RISCOS

b&a BRASILIANO & ASSOCIADOS

EDIÇÃO 99
JULHO 2016

Críticas e sugestões de pauta:
revista@brasiliano.com.br

www.brasiliano.com.br

Edição 99 - Julho 2016

ISSN 1678-2496N

A revista Gestão de Riscos é uma **publicação gratuita** eletrônica da Brasiliano & Associados

Rua Barão de Jaceguai, 1768. Campo Belo - São Paulo - SP, 04606-004, BRASIL

Publisher: Antonio Celso Ribeiro Brasiliano

Edição: Enza Cirelli

Edição de arte: Marina Brasiliano