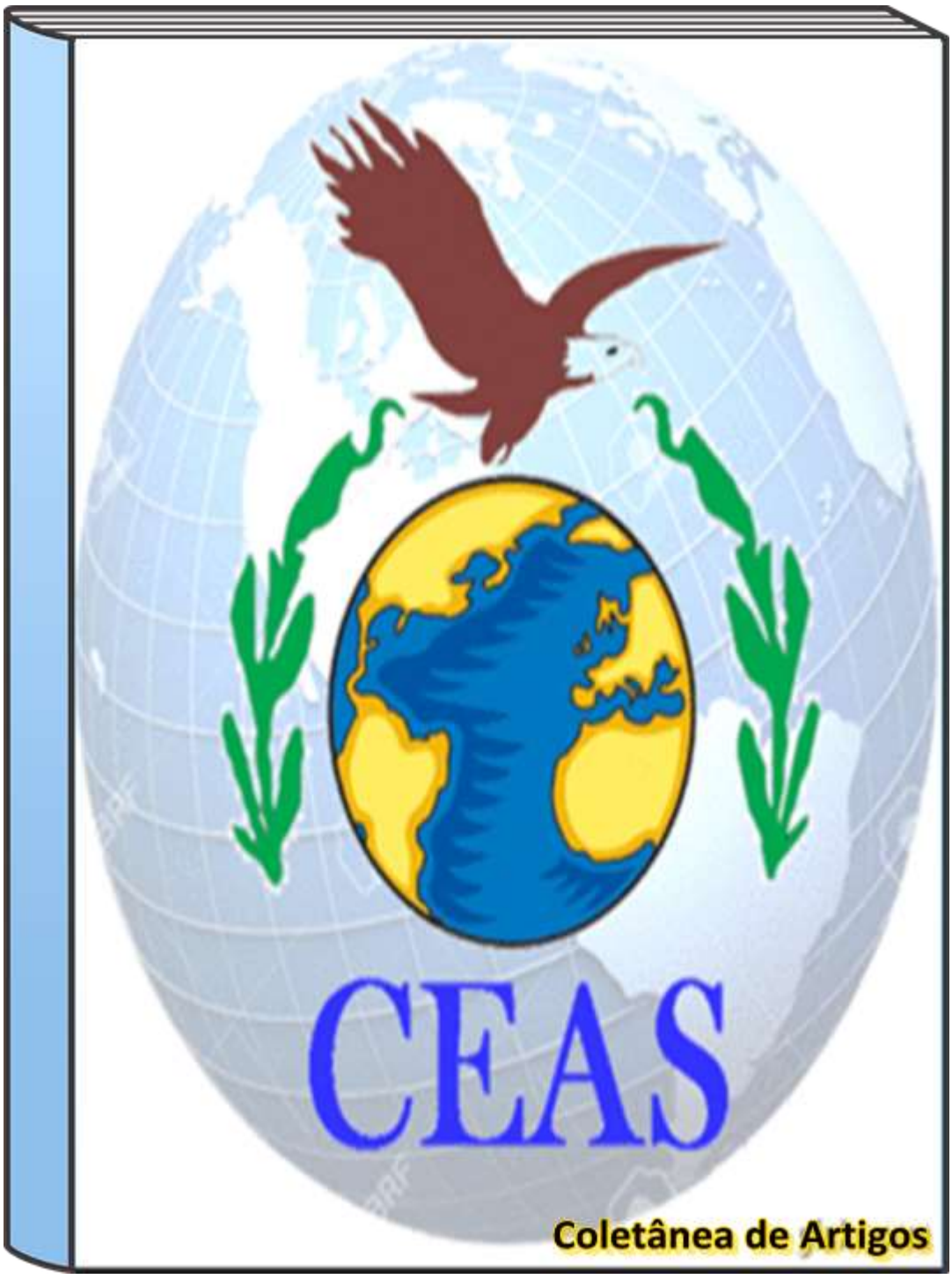


Edição V – 2022

Corporación Euro-Americana de Seguridad

CEAS INTERNACIONAL

CEAS BRASIL

“Formamos profissionais e líderes em segurança integral.”

“ENSINANDO SEGURANÇA INTELIGENTE”

www.ceasbrasil.com.br
contato@ceasbrasil.com.br

SUMÁRIO

INTRODUÇÃO

A importância de artigos ligados à área de segurança para todos os profissionais da área.

A regulamentação da atividade de segurança privada foi iniciada no Brasil a partir do Decreto-Lei 1034/69, à época, com o intuito de prover segurança às instituições financeiras. Passadas cinco décadas, muitas conquistas foram alcançadas, novas áreas de negócio foram contempladas e passaram a compor o acervo de especialidades em segurança.

Apesar da crescente procura por pessoas que almejam engajar-se nesta área, e da oferta de vagas oferecidas por um mercado consolidado, ainda observamos uma carência grande de literatura voltada à área de segurança, inclusive no ambiente acadêmico, de cursos stricto sensu relacionados à área de segurança.

Atento a esse cenário, CEAS Brasil tem proporcionado, aos profissionais de segurança, excelentes oportunidades de crescimento profissional, oferecendo artigos com conteúdos ricos em conhecimento e atualização sobre as melhores práticas do mercado, cursos de aperfeiçoamento e certificações nacionais e internacionais voltados à área de segurança.

Este e-book é um verdadeiro oásis no meio da escassez de materiais orientados à área de segurança, está acessível e põe em nossas mãos um material robusto, técnico e aprofundado. Privilégio de poucos, nós associados, nos sentimos verdadeiramente assistidos, o que nos confere um diferencial competitivo no mercado brasileiro de segurança.

Esta coletânea, disponibilizada pela biblioteca da CEAS BRASIL, nos auxilia na complexa tarefa de capacitação profissional, a compreender a estrutura de gerenciamento, controle, implementação e operação da segurança nas organizações. O mercado é dinâmico, novas tecnologias e cenários nos são apresentados e cada vez mais a aceleração do ritmo da evolução tecnológica amplifica o acesso à tecnologia e encurta, de forma drástica, o ciclo das transformações.

Portanto, é preciso assumirmos riscos diante de tamanha rapidez com que as mudanças acontecem. Nosso tempo de resposta aos problemas que nos são apresentados está cada vez mais curto e precisamos tomar decisões rápidas e certeiras para não ficarmos “a pé”. Assim, o papel que CEAS Brasil tem desempenhado em termos de serviços prestados para os profissionais da segurança tem sido essencial e os artigos publicados pelos associados muito nos têm orgulhado devido à qualidade técnica que os caracteriza.

É mister que nos empenhemos em prestigiar esses trabalhos que tanto têm colaborado com nosso crescimento profissional, atualização e renovação de conhecimentos. Para isso, precisamos manter os contatos apropriados com o grupo de associados, fortalecer a classe de profissionais da segurança, participar de webinars, ler os artigos e participar de fóruns especializados.

Mariana da Silveira, CEGRC, CIGR, CISI, MBA em GRC, MBCR, DPO, CISO

Gerente de Gestão de Riscos, ex-aluna do MBA e MBCR do Prof. Dr. Antonio Celso Ribeiro Brasiliano.

CIBERSEGURANÇA TEM O MESMO SIGNIFICADO DE CIBER RESILIÊNCIA? VOCÊ SABE A DIFERENÇA?

Prof. Dr. Antonio Celso Ribeiro Brasiliano, DICS, MCRC, CIEAI, CEGRC, CIEAC, CIEIE, CPSI, CIGR, CRMA, CES, DEA, DSE, MBS

A pandemia de Covid-19 e sobretudo o aumento no número de ataques virtuais em escala global, transformaram a cibersegurança em prioridade para líderes corporativos. De acordo com o relatório Global Cybersecurity Outlook 2022, produzido pelo Fórum Econômico Mundial de Davos, o número de ataques de ransomware teve um acréscimo de151% somente no primeiro semestre de 2021.

Os ataques cibernéticos de ransomware estão entre as 3 principais preocupações dos grandes executivos globais quando o assunto é cibersegurança. Outras preocupações estão integradas com a do ransomware, tais como a engenharia social e o phishing, que são a porta de entrada para os grandes ataques cibernéticos.

As atividades maliciosas internas abrangem situações em que colaboradores atuais ou antigos, ou mesmo parceiros de negócios, utilizam informações privilegiadas para prejudicar a empresa.

Seja qual for a situação de risco que a empresa enfrenta, o consenso entre os participantes do Fórum de Davos é de que tem de haver uma maior integração entre os profissionais da área de fraudes corporativas com os da segurança física e lógica, tanto na iniciativa privada quanto nos órgãos governamentais.

A integração entre os profissionais de segurança e os das demais áreas de negócios é um dos principais desafios das empresas, já que contraria o paradigma de que a área de segurança da informação é a única responsável pela prevenção de ataques cibernéticos. Segundo o relatório Global Cybersecurity Outlook 2022, 92% dos executivos concordam que a segurança cibernética está integrada às estratégias de gestão de riscos corporativos e, em consequência, acha-se integrada ao modelo de negócio e a suas estratégias comerciais. No entanto, apenas 55% dos líderes com foco em segurança concordam com essa afirmação. Muitos desses líderes alegam, por exemplo, não serem consultados em decisões relacionadas à segurança dos negócios. Isso acaba tornando as empresas – ou os órgãos de governo – mais vulneráveis.

Do lado dos executivos, é preciso garantir o envolvimento de profissionais de segurança da informação em decisões estratégicas da empresa e reservar orçamento para a área. Os profissionais de cibersegurança, por outro lado, precisam investir tempo e energia na integração com as áreas de negócios e no treinamento e retenção de talentos.

O relatório liberado pela equipe de Davos mostra que 59% de todos os entrevistados consideram difícil responder de forma eficaz a um incidente de segurança cibernética devido à falta de pessoal capacitado no âmbito de suas equipes.

Cibersegurança X ciber-resiliência

Para muitas empresas, cibersegurança e ciber-resiliência são conceitos iguais ou até sinônimos, o que é um grande equívoco. Vejamos: cibersegurança é a atividade que consiste em proteger sistemas e dados de possíveis ataques, construindo barreiras para manter as ameaças cibernéticas afastadas dos sistemas e processos críticos da empresa; já a ciber-resiliência é a capacidade da empresa em ultrapassar eventos

cibernéticos no âmbito da organização e de seu ecossistema. A empresa deve possuir visão de antecipação para, mantendo-se em condições de suportar, recuperar e adaptar-se. Ou seja, o objetivo é garantir formas de continuidade para manter a operação rodando.

Portanto a área de Cibersegurança contará necessariamente com três características:

1a – contar com controles de segurança para detectar sintomas de ataques;

2a – após haver detectado, de forma antecipada, os ataques, ter condições de barrá-los ou isolá-los;

3a – ter capacidade de se recuperar desses ataques e, ao mesmo tempo, adaptar-se ao contexto do ataque.

O Fator Crítico de Sucesso é a colaboração entre diferentes equipes de cibersegurança para permitir a troca de conhecimentos e experiências. O desafio é convencer as empresas da necessidade de compartilhar informações para que o mercado como um todo aprenda e torne-se mais seguro. É essencial o estabelecimento de parcerias público-privadas com essa finalidade. Infelizmente, no Brasil, ainda estamos longe dessa realidade.

O Fórum de Davos lançou o Centro para Cibersegurança, que reúne mais de mil organizações de todo o mundo, cujos objetivos são fortalecer a colaboração global, entender o futuro da área de cibersegurança e construir uma cultura voltada à ciber-resiliência. É importantíssima a participação das empresas nessa jornada.

Como disse Jeremy Jurgens, managing diretor do Fórum Econômico Mundial:

“O ciberespaço transcende fronteiras. Precisamos, portanto, mobilizar uma resposta global para lidar com desafios de cibersegurança”

Conseguiremos? Desafio que depende de quebra de paradigmas e de acultaramento!

Prof. Dr. Antonio Celso Ribeiro Brasiliano, DICS, MCRC, CIEAI, CEGRC, CIEAC, CIEIE, CPSI, CIGR, CRMA, CES, DEA, DSE, MBS, Doctor en Ciencias de la Información e Ingeniería e Inteligencia Estratégica pela Universidad Paris-Est (Marne La Vallée, Paris, França); Doctor Internacional en Ciencias de la Seguridad, pela CEAS – Internacional – Madrid – Espanha, presidente da Brasiliano INTERISK. abrasiliano@brasiliano.com.br

CRITÉRIOS DE ANÁLISE DE RISCOS LEGAIS

Flavio Fleury de Souza Lima, CIEAC, CISI, CIGR

Uma organização deve, através da adaptação de técnicas apropriadas de gestão de riscos, identificar de forma proativa seus riscos legais. No presente texto, abordaremos os critérios a serem adotados para a análise desses riscos.

A norma ABNT NBR ISSO 31000:2018, em seu tópico 6.3.4, estabelece que é conveniente para uma organização especificar a quantidade e o tipo de riscos que ela pode ou não assumir em relação aos seus objetivos.

Neste contexto, a referida norma determina que é conveniente à organização que sejam estabelecidos critérios para avaliar a importância dos riscos e auxiliar nos processos de tomada de decisões. Desta forma, devem ser estabelecidos os critérios de riscos que estejam alinhados à estrutura de gestão de riscos e sejam padronizados para o propósito específico e o escopo da atividade em consideração.

Tais critérios de riscos devem refletir os valores, objetivos e recursos da organização e ser consistentes com as políticas e declarações sobre gestão de riscos. Convém, ainda, que os critérios de riscos sejam estabelecidos levando em consideração as obrigações da organização e os pontos de vista das partes interessadas.

Esses critérios devem ser estabelecidos no início do processo de avaliação de riscos, devem ser dinâmicos e continuamente analisados de maneira crítica e alterados sempre que necessário.

É conveniente que tais critérios de riscos considerem:

• a natureza e o tipo de incertezas que podem afetar resultados e objetivos, tanto tangíveis quanto intangíveis;

• como as consequências (tanto positivas quanto negativas) e as probabilidades serão definidas e medidas;

• os fatores relacionados ao tempo;

• a consistência no uso de medidas;

• como o nível de risco será determinado;

• como as combinações e sequências de múltiplos riscos serão levadas em consideração;

• a capacidade da organização para suportar o risco materializado.

Em determinadas situações, como nos casos em que a organização é obrigada por lei a realizar, seguir ou aprovar algo; ou em casos relacionados à política ou ao contrato em que é obrigada por lei a adotar uma decisão que somente ela pode tomar legalmente; ou, ainda, em ações judiciais e acordos “fora do curso normal dos negócios” em que o valor envolvido ou a questão apresentada envolvem um ou mais dos fatores apresentados, dentre outros, podem ser requeridas a aplicação de critérios de riscos legais.

Neste contexto, a norma ABNT NBR ISSO 31022:2020, que complementa a norma mencionada acima, estabelece a conveniência de a organização considerar que os critérios de riscos legais:

• constituem um subgrupo dos critérios de riscos organizacionais;

• são medidas identificadas e definidas para avaliar um nível significativo e aceitável de um risco legal ou de um grupo de riscos legais;

• devem refletir os objetivos, valores, recursos, preferências e tolerâncias gerais da gestão de riscos em relação aos riscos legais;

• devem ser analisados criticamente de maneira regular e ao início de qualquer grande projeto de atualização de critérios e processos de gestão de riscos legais;

• podem surgir, ou derivar, da aplicação de leis ou deveres contratuais ou obrigações;

• são dinâmicos e, uma vez definidos, pertencem à função responsável pela gestão de riscos legais;

• devem estar alinhados com a abordagem geral e/ou política da organização em relação à gestão de riscos legais (convém que a organização desenvolva e ajuste seus critérios de riscos legais de acordo com situações reais).

Na determinação dos critérios de riscos legais devem ser considerados os seguintes fatores:

• objetivos e prioridades organizacionais;

• governança, incluindo níveis hierárquico das autoridades e a alocação das responsabilizações, papéis, e responsabilidades da gestão de riscos legais na organização;

• relacionamentos com terceiros;

• escopo e objetivos da gestão de riscos legais e as categorias de riscos legais;

• princípios adotados para determinar o nível de riscos legais;

• status das políticas, protocolos, estruturas, processos e metodologias da gestão de riscos legais;

• aceitação de riscos legais ou nível de tolerância de riscos legais das partes interessadas;

• mensurações para classificação de níveis de risco.

O estabelecimento de critérios de riscos legais deve ser orientado por processos, sendo requerido que tais riscos sejam caracterizados e medidos de maneira que possam ser quantificados e que o tratamento de risco ideal seja adotado.

Uma resposta adequada aos riscos legais deve estar em concordância com os critérios adotados tanto no nível da direção quanto na organização como um todo. Os critérios de riscos, se indevidamente restritos, podem resultar no isolamento dos proprietários desses riscos do contexto maior de risco operacional, desconectando-os, assim, da organização como um todo.

Critérios restritos demais ou que não se integram aos critérios gerais de riscos adotados pela organização podem oferecer uma abordagem equivocada do problema.

Como resultado, é possível que os responsáveis pela área jurídica da empresa somente se envolvam no processo numa fase mais avançada, de agravamento da crise. Nesse caso, esses profissionais não teriam a oportunidade de atuar de forma precoce, de modo a mitigar tais riscos em um estágio inicial, quando estariam em posição de oferecer um tratamento mais adequado aos riscos legais.

Flavio Fleury de Souza Lima, CIEAC, CISI, CIGR
Especialista nas áreas de IRPJ, CSLL, PIS e COFINS. Formado pelo CPOR/SP, é graduado em administração de empresas pelo Mackenzie e cursou direito na UNIP. Atualmente trabalha como Diretor Associado da Divisão de Risco Tributário na Brasiliano INTERISK.

12 erros frequentes que tornam a gestão de riscos míope

Marcos Alves Junior

No âmbito de tudo que abrange uma Gestão de Riscos estruturada, existem fatores que ganham destaques por serem cruciais. Um deles é o conceito das Três linhas de Defesa, no qual a 1ª Linha, responsável pela gestão operacional, precisa avaliar e reportar perfeitamente os riscos do negócio. A 2ª Linha de Defesa inclui as funções de Gerenciamento de Riscos, orientando e supervisionando as áreas de negócios para auxiliar os profissionais da 1ª Linha. Desse modo, a área de Gestão de Riscos Corporativos se torna essencial para que a organização assuma uma posição de antecipação diante dos riscos.

Outro fator de suma importância no processo de Gestão de Riscos é representado pelos principais padrões de mercado e metodologias nacionais e internacionais, tais como: ISO 31000:2018 - Gestão de riscos - Diretrizes, COSO ICIF:2013 - Committee of Sponsoring Organizations of the Treadway Commission - Internal Control - Integrate Framework e o COSO ERM:2017 - Committee of Sponsoring Organizations of the Treadway Commission - Enterprise Risk Management – Integrating with Strategy and Performance (Integrado com Estratégia e Performance). É importante ressaltar que esses padrões são apenas orientadores, ou seja, cabe a cada organização assimilar as diretrizes e implementá-las, levando sempre em consideração a cultura organizacional e as suas necessidades.

Tendo em vista os fatores acima expostos, cabe aos gestores entenderem a responsabilidade e a importância de ter um processo estruturado. Evitando uma análise de riscos míope e mediante a estruturação dos processos, um erro pode ser identificado e corrigido com maior agilidade. Tendo esses conceitos claros, vejamos quais são os 12 erros acometidos com maior frequência em uma análise de riscos míope:

1. O não envolvimento das partes interessadas, por exemplo, a área de Gestão de Riscos (segunda linha) não envolve o Dono do Processo (primeira linha), presumindo que a primeira linha não tem tempo e condição técnica para identificar e analisar os riscos. Detalhe que deveria ser alinhado em um treinamento especializado;

2. A falta de integração da área de Controle Interno com a área de Gestão de Riscos, o que não se justifica, pois só existe controle devido à condição do risco;

3. A falta de independência das áreas de Gestão de Riscos e Auditoria Interna, pois em algumas empresas essas áreas respondem para o mesmo Diretor, ou seja, algumas empresas que possuem uma Auditoria com a função adicional da Gestão de Riscos e em alguns casos a área de Gestão de Riscos está ligada ao Diretor Financeiro, podendo também gerar conflito de interesse;

4. A Mensuração da probabilidade do risco, somente pelo critério de Frequência, ou seja, o histórico pode deixar uma visão errônea de probabilidade;

5. A Mensuração do impacto (consequência) do risco, somente pelo critério Financeiro, sendo necessário minimamente considerar os critérios Financeiro, Imagem, legal e Operacional;

6. A falta de estruturação na matriz de riscos;

7. Deixar de identificar os fatores de riscos (causas dos riscos);

8. Não possuir uma Política de Gestão de Riscos Corporativos, deixando claros as responsabilidades e o apetite ao risco;

9. Não monitorar os riscos e indicadores de desempenho;

10. Dispensar o uso de tecnologias que tornam a Gestão de Riscos e Auditoria Interna baseada em riscos mais eficientes e integradas;

11. Áreas que atuam com o tema de Gestão de Riscos trabalhando como ilhas, por exemplo: Cibernético, Segurança do Trabalho, Segurança Empresarial, Meio Ambiente, entre outras;

12. A Alta Gestão não dar a devida importância para o tema de Gestão de Riscos (top-down). O assunto precisa fazer parte da rotina, estabelecendo uma cultura efetiva de gestão de riscos.

Tendo em vista todos esses erros cometidos pelos gestores, é importante citar que o processo de gestão de riscos não é uma ferramenta para que os gestores tenham aversão aos riscos. A gestão de riscos tem como objetivo prover a confiança para que os gestores possam aceitar riscos, em níveis pré-definidos, e alavancar oportunidades para a organização.

Quando a empresa tem uma cultura de aversão aos riscos, cria-se uma gestão inflexível, com a construção de bloqueios que podem prejudicar o desempenho da organização no cumprimento dos seus objetivos. Por outro lado, quando a empresa

tem uma aceitação de riscos desproporcionais a sua capacidade de geri-los, isso pode ocasionar impactos significativos.

A Brasiliano INTERISK conta com o Software INTERISK, uma ferramenta que atende às melhores práticas, aliando tecnologia e conceito, garantindo que as disciplinas de riscos trabalhem em sincronia, em um único framework. Atualmente o INTERISK conta com 13 módulos, abrangendo as diferentes áreas da organização. Dessa forma ele auxilia o desenvolvimento de todas as áreas de forma holística, assegurando a otimização dos processos como um todo.

Para saber mais sobre outros diferenciais do sistema INTERISK e sobre a otimização de processos que ele pode proporcionar a sua organização, acesse nosso site no link abaixo e solicite uma demonstração com um de nossos especialistas. (Link) (Obs: Imagem acima será alterada)

Marcos Alves Junior

Redator, Editor de texto, Criador de vídeos. Cursou Gestão Empresarial na Anhanguera. Formado pela Uninove – Universidade Nove de Julho em Comunicação Social – Jornalismo. Atualmente trabalha como Assistente de Comunicação e Marketing na Brasiliano INTERISK.

Diversidade na Estrutura Corporativa – Mais que Modismo, uma Necessidade

Décio Luís Schons, CIEAI, CEGRC, CIGR, CISI

Anos atrás, quando frequentei determinado curso de nível intermediário na carreira militar, um antigo instrutor nos ilustrava sobre o exercício da chefia e da liderança, ao tempo em que nos brindava com valiosas noções sobre a prática do assessoramento. Em determinado momento, ele nos chamou a atenção para a existência de dois tipos extremos de assessor, ambos nocivos, ambos daninhos à coesão e ao espírito de corpo da unidade: o “assessor do eterno sim” e o “assessor do eterno não”.

A primeira categoria, explicou-nos, é constituída pelos assessores que sempre concordam com o chefe, pelo menos da boca para fora. Alguns deles, mais requintados, chegam mesmo a desenvolver a capacidade de adivinhar o pensamento do chefe para antecipar-se a suas ideias. – “Que ideia genial, chefe!” – é uma das expressões mais frequentes em seu vocabulário.

Já os assessores da segunda categoria comportam-se de maneira diametralmente oposta: sempre de mal com a vida, eles são os “do contra”. Qualquer solução apresentada por outro integrante da equipe é considerada horrorosa, embora nem sempre os “assessores do eterno não” tenham algo melhor a apresentar em relação àquilo que já foi colocado sobre a mesa.

De todo o conteúdo do curso, aquela foi uma das aulas que mais me marcaram. Ao longo de quase meio século de vida profissional, tive ocasião de conviver, em algumas oportunidades, com as duas variantes de assessores. Algumas vezes cheguei a me questionar sobre qual das duas seria mais prejudicial ao trabalho em equipe e ao desempenho da unidade. Submeti o assunto à consideração de chefes e companheiros e percebi que não havia unanimidade com relação a esse quesito.

Hoje, fazendo um balanço da minha experiência, chego à conclusão de que a primeira variante é muito mais perniciosa que a segunda. E quando me questiono sobre que tipo de assessores escolheria se fosse constituir uma equipe para levar a cabo fosse qual fosse a tarefa ou a missão, afirmo sem medo de errar que preferiria ver nela contestadores a bajuladores. Gostaria de contar com uma equipe diversificada, em que pontos de vista diferentes fossem debatidos exaustivamente, até que soluções, não necessariamente de consenso, mas pelo menos aceitáveis por parte de todos, fossem levadas ao chefe para a tomada da decisão. Nesse grupo de trabalho, a diversidade seria o grande fator diferencial.

Li uma vez que o chefe que se deixa assessorar por um time em que as opiniões são parecidas ou coincidentes, particularmente quando a mediana do pensamento explicitado coincide com as opiniões do próprio chefe, melhor faria se não tivesse assessor nenhum. Assim economizaria o tempo e os recursos gastos em um processo cujo desfecho já seria de antemão conhecido. “Se você pensa exatamente como eu sobre esse tema, não há porque estarmos aqui a debatê-lo. Passemos adiante.”

Se mudarmos o foco para a área da gestão corporativa, veremos que a diversidade está mais que nunca na ordem do dia, especialmente quando se trata da vertente social da Agenda ESG (*Environmental, Social & Governance* – ou Ambiental, Social & Governança, em português). Contrariamente a uma visão ainda comum no ambiente empresarial, esse aspecto, como todos os outros relacionados à Agenda ESG, não deve ser encarado como apenas mais um ônus para as empresas. Na verdade, os encargos e os custos gerados poderão ser amplamente compensados a partir do aproveitamento das oportunidades que a colocação em prática da Agenda ESG irá ensejar, desde que essa agenda seja encarada de forma proativa, como algo suscetível de criar valor para a organização.

Voltando ao tema diversidade, parece evidente que a presença no ambiente de trabalho, especialmente nos espaços destinados ao assessoramento e à tomada de decisões, de pessoas com origens, formações e *backgrounds* diferenciados acrescentará muito à qualidade dos processos ali desenvolvidos.

Vale a pena recordar que **Diversidade** é apenas um componente de um aspecto mais abrangente chamado **Inclusão**. O outro componente, tão importante quanto o primeiro, é a **Equidade**. Equidade carrega o senso de justiça, de distribuição equilibrada dos encargos, como também dos bônus e das recompensas. Contraria o princípio da Equidade, por exemplo, a velha prática de oferecer remuneração inferior às mulheres apenas porque são.... mulheres. Como será trabalhar em um ambiente em que você se sente discriminado por não pertencer ao sexo, à etnia, à nacionalidade ou seja, a um grupo social que não é considerado “correto”, “adequado”, “aceito”, pela corrente dominante no local? Aí estava (vamos ser otimistas e usar o verbo no pretérito), em última análise, a expressão cristalina do preconceito que durante tanto tempo balizou as relações sociais em nosso país.

Convenhamos, não é nada fácil mudar, quebrar paradigmas em estruturas tradicionais, consolidadas e lucrativas. “Em time que está ganhando, não se mexe” – esse é o mote que temos ouvido por anos e anos. Só faltou alguém dizer que era preciso mexer no time para continuar ganhando. O caso da Kodak é emblemático, ao

exemplificar o fracasso decorrente da resistência à inovação (no caso, a revolução trazida pelas câmeras digitais) para não pôr em risco a gigantesca estrutura destinada à fabricação de câmeras analógicas e filmes fotográficos. Em razão dessa dificuldade em efetuar mudanças em organizações estruturadas e consolidadas, as quebras de paradigmas costumam ocorrer nas bordas, nos locais em que não há esse compromisso e esse temor da mudança. Startups são exemplos dessa realidade.

Empresas antigas e muito bem estabelecidas precisam estar atentas às oportunidades de transformação, seguindo outro aforisma bem conhecido: “As mudanças devem ser efetuadas antes que se tornem necessárias.” A popularização da Agenda ESG oferece uma excelente oportunidade para praticar a inovação, não apenas em tecnologias, mas sobretudo em gestão corporativa e em maneiras de encarar os desafios. A análise das estruturas e dos processos à luz dos padrões ESG poderá trazer *insights* valiosos, desde que a estrutura decisória tenha olhos para ver e ouvidos para ouvir.

Neste breve texto, procuramos nos deter sobre o tema Inclusão, no âmbito do aspecto Social da Agenda ESG. Nossa intenção é, na medida do possível, estimular o debate sobre esse assunto tão momentoso para todo o setor empresarial em nosso país.

Nós, da Brasiliano INTERISK, colocamos a gestão de riscos ESG como uma prioridade em nosso portfólio, exatamente por entender a importância do tema, tanto na conjuntura atual quanto em situações futuras. É voz corrente que o Brasil se encontra décadas atrasado em relação a alguns outros países no que diz respeito a esse assunto. Em razão disso, podemos afirmar que já é tempo de levarmos a Agenda ESG a sério, de modo a transformar riscos em oportunidades, para o bem de nossas empresas e de nosso país.

Décio Luís Schons, CIEAI, CEGRC, CIGR, CISI

General-de-Exército da Reserva, é Vice-Presidente de Operações de Consultoria da empresa Brasiliano INTERISK.

A CONTRAINTELIGÊNCIA E A SUA CONTRIBUIÇÃO PARA O GERENCIAMENTO DE RISCO EM PROJETOS

Maurilio Eduardo Freitas Rosa, CPSI, CIPP, CIGR, CISI, DIDS

1. INTRODUÇÃO

Por intermédio do gerenciamento de risco podemos identificar e assinalar as ameaças e as oportunidades e planejar as respostas e as contramedias, mediante estratégias bem definidas, formatadas e adaptadas para direcioná-las, bem como garantir o sucesso dos projetos que gerenciamos.

O conceito de risco está relacionado com a incerteza e a variabilidade, enquanto a sua gestão envolve tudo que uma organização faz ou fornece.

A gestão de riscos refere-se à arquitetura implantada internamente em uma organização para gerenciar os riscos de maneira eficaz, objetivando a redução de eventos que impactem negativamente seus objetivos estratégicos.

A gestão de riscos, por meio de um enfoque estruturado e da melhor compreensão das inter-relações e interdependência entre os diversos riscos, alinha estratégia, processos, pessoas e tecnologia, objetivando a preservação e a criação de valor para a organização e as Partes Interessadas.

Numa visão abrangente podem-se considerar riscos para as organizações humanas:

a. Especulativos relacionados à possibilidade de ganho ou chance de perda.
b. Administrativos dependentes de decisões gerenciais:
1. de mercado;
2. financeiros; e
3. de produção.
c. Políticos, vinculados a leis, decretos, portarias, regulamentação, etc.
d. De inovação, relacionados a novas tecnologias, novos produtos, etc.

A figura a seguir demonstra a natureza e abrangência dos riscos, por intermédio de uma matriz vetorial de riscos:

Figura 1: Matriz vetorial de riscos

Fonte: https://br.answers.yahoo.com/question/index?qid=20070508201039AAgXAzU

Com relação às influências organizacionais, conforme pontua o Guia PMBOK® — QUINTA EDIÇÃO (2013, p. 19):

> [...] projetos e seu gerenciamento são executados em um ambiente mais amplo que o do projeto propriamente dito. A compreensão deste contexto mais amplo ajuda a garantir que o trabalho seja conduzido em alinhamento com as metas e gerenciado de acordo com as práticas estabelecidas pela organização. [...] ***as influências organizacionais afetam os métodos*** usados na mobilização de pessoal, gerenciamento e execução do projeto. Ela discute a influência das partes interessadas no projeto e em sua governança, a estrutura e constituição da equipe do projeto e as várias abordagens das fases e relacionamento das atividades no ciclo de vida do projeto [...] (Grifo nosso)

O presente artigo tem sua justificativa e originalidade na percepção da constatação da falta de uma proposta metodológica referente à contribuição da contrainteligência para o gerenciamento de risco em projetos.

Quanto às fontes para a produção deste artigo, a primeira constatação foi que é exígua a produção literária acadêmica brasileira com relação especificamente ao gerenciamento de risco em projetos com a contribuição da contrainteligência para este gerenciamento.

A metodologia utilizada foi o levantamento bibliográfico, utilizando-se para isso os recursos existentes e disponibilizados a partir de materiais publicadas em livros, artigos, dissertações e teses, e, também, através de acesso a fontes disponibilizadas na rede mundial de computadores (internet). Uma pesquisa exploratória (bibliográfica), sendo norteada pelo objetivo de identificar a contribuição da Contrainteligência para o gerenciamento de riscos em projetos.

2. DESENVOLVIMENTO

Em um mundo onde a competição, o conhecimento, a evolução e a mudança desempenham papéis importantes para a inovação e o desenvolvimento de organizações, o gerenciamento de projetos é elemento fundamental para o sucesso das instituições e empresas.

Dentre as diversas áreas de conhecimento que são elencadas pelo gerenciamento de projetos, uma que direciona as ações, visando de forma pontual e macro a segurança, é o gerenciamento de risco, iniciado com a implementação de um processo de análise de risco.

Cada vez mais as organizações, seus sistemas de informação e planejamento estratégico são colocados à prova por diversos tipos de ameaças, incluindo de forma bem pontual aquelas oriundas de seus Fatores Ambientais e Ativos de Processos Organizacionais.

A análise de riscos tem por objetivo:

- Mapear e tratar adequadamente as ameaças e vulnerabilidades do ambiente interno e externo, e o próprio projeto;

- Identificar os riscos;

- Quantificar o impacto das ameaças; e

- Conseguir um equilíbrio financeiro entre o impacto do risco e o custo da contramedida.

Mas o que é “RISCO” dentro do escopo do PMI®?

Risco do projeto, conforme o GUIA PMBOK® — Quinta Edição (2013, p. 310):

> [...] é um evento ou condição incerta que, se ocorrer, provocará um efeito positivo ou negativo em um ou mais objetivos do projeto tais como escopo, cronograma, custo e qualidade [...]

Em continuidade, o risco é o efeito da incerteza nos objetivos, de tudo que pode comprometer ou contribuir para o alcance dos objetivos. (ISO 31000).

Para a exata delimitação do risco, devem-se identificar seus três componentes, a saber: causa (ou fonte), evento e consequência (ou efeito).

A figura 2, a seguir descreve de forma gráfica, o risco identificando seus três componentes:

Figura 2: Descrevendo Riscos

Fonte: https://br.answers.yahoo.com/question/index?qid=20070508201039AAgXAzU

Nos termos da norma ABNT NBR ISO 31000:2009, um evento é a ocorrência ou mudança em um conjunto específico de circunstâncias. Causa é a fonte do risco ou vulnerabilidade existente na organização e que dá origem a um evento, enquanto consequência é o resultado de um evento que afeta os objetivos.

Mas como a Atividade de Inteligência, por meio do seu ramo Contrainteligência, contribui para o gerenciamento de risco em projetos?

O que vem a ser a Contrainteligência?

O acesso indevido (não autorizado) a conhecimentos sensíveis e/ou sigilosos – aqueles que, pela importância, natureza e necessidade de proteção, exigem medidas especiais de segurança – sempre foram grande fonte de atenção e medidas cautelares dos Governos, das grandes empresas e das Instituições, tendo sido suas técnicas de obtenção (BUSCA), por um lado, e neutralização (PROTEÇÃO), por outro, compiladas, formatadas, organizadas e transformadas, respectivamente, nas Atividades do Ramo Inteligência e do Ramo Contrainteligência.

As atividades de Inteligência, em seus dois ramos, Inteligência e Contrainteligência, estão presentes em todas as grandes decisões nacionais, seja proporcionando segurança aos governantes ou garantindo grau de competitividade e capacidade de inovação às empresas.

Do ponto de vista da geopolítica e da história, as atividades de Inteligência e de Contrainteligência sempre foram de uso exclusivo dos ambientes militares, e agentes do Estado. Mas na história recente seus conceitos, formatação e métodos vêm sendo empregados por diversas organizações empresariais, motivadas que estão com o acirramento da concorrência, vazamento ou fuga de informações, competências e defesa de seu patrimônio, seja tangível (físico, digital), e por valores

intangíveis tais como o capital intelectual, a gestão do conhecimento ou a imagem, bem como a credibilidade junto à opinião pública (Partes Interessadas).

Portanto, neste primeiro momento, podemos afirmar que ambos os ramos, estão envolvidos com a Gestão de Riscos (Visão Macro, Sistêmica), e no Gerenciamento do Risco (Operacionalização), seja nos procedimentos formatados para proteção de áreas e instalações, na proteção de documentos e materiais, na segurança das pessoas, dos processos e em tecnologias confiáveis, pontualmente nos sistemas de comunicação e informações, digitais ou não.

Assim, é importante a formatação de uma Cultura e de uma Política de produção, aquisição e proteção do conhecimento, quer a nível Estratégico, Tático e Operacional objetivando garantir o controle de ativos e recursos de Informação, Imagem de Mercado e Conformidade Legal (“Compliance”).

2.1 GERENCIAMENTO DE RISCO

A figura de número 3, a seguir, visualiza o impacto que o risco causa aos objetivos:

Figura 3: Riscos (Impacto)

Fonte: https://br.answers.yahoo.com/question/index?qid=20070508201039AAgXAzU

O processo de planejamento do gerenciamento de risco do PMBOK é definido da seguinte forma:

a. Entradas;

- *Fatores organizacionais*;
- Atitude e tolerância com relação ao risco;
- *Processos organizacionais*;
- Categorias de risco;
- Definição de conceitos e termos;
- Papéis e responsabilidades;
- Níveis de autoridade para tomada de decisão;

- Escopo do projeto;
- Plano de gerenciamento do projeto;

b. Ferramentas e técnicas;

- Reuniões e análises;

c. Saída;

- Plano de gerenciamento de risco.

A estrutura do plano do gerenciamento de risco segue o seguinte formato:

- Metodologia;
- Papéis e responsabilidades;
- Investimento;
- Cronograma;
- Categorias de risco (RBS);
- Definição da probabilidade e impacto do risco;
- Matriz de probabilidade e impacto;
- Tolerância dos stakeholders;
- Formato dos relatórios;
- Auditoria.

A figura de Gerenciamento de Riscos - GUIA PMBOK® — Quinta Edição, abaixo, demonstra os processos pertinentes à área de Riscos:

Figura 4: Gerenciamento de Riscos - GUIA PMBOK® — Quinta Edição
Fonte: https://br.answers.yahoo.com/question/index?qid=20070508201039AAgXAzU

Assim, o gerenciamento de riscos, dentro de sua dimensão maior, a da Gestão de Riscos, é o processo de planejar, organizar, dirigir e controlar os recursos (humanos e materiais) de uma organização, no sentido de minimizar ou aproveitar os riscos e incertezas sobre essa organização.

E o gerenciamento de riscos, especificamente, na sua dimensão, como área de conhecimento para o Gerenciamento de Projetos objetiva:

a. Aumentar a probabilidade e o impacto dos eventos positivos e reduzir a probabilidade e o impacto dos eventos negativos no projeto.

b. Combater as incertezas presentes nos projetos, especialmente nas estimativas e premissas.

Em ambas as dimensões, as incertezas representam riscos e oportunidades, com potencial para destruir ou agregar valor. O gerenciamento de riscos implementa maiores possibilidades aos gestores de tratarem com eficácia as incertezas, bem como os riscos e as oportunidades a elas associadas, a fim de melhorar a capacidade de gerar valor.

Esta geração de valor é potencializada e maximizada quando a organização estabelece estratégias e objetivos para alcançar o equilíbrio ideal e/ou possível, entre as metas de crescimento, e de retorno de investimentos e os riscos a elas associados, e para explorar os seus recursos com eficácia e eficiência na busca dos objetivos da organização.

Segundo a definição do que é gerenciamento de riscos o ISO 31.000, pontua que uma gestão de risco eficaz deve atender os seguintes princípios:

a. Proteger e criar valor para as organizações.

b. Ser parte integrante de todos os processos organizacionais.

c. Ser considerada no processo de tomada de decisão.

d. Abordar explicitamente à incerteza.

e. Ser sistemática, estruturada e oportuna.

f. Basear-se nas melhores informações disponíveis.

g. Estar alinhada com os contextos internos e externos da organização e com o perfil do risco.

h. Considerar os fatores humanos e culturais.

i. Ser transparente e inclusiva.

j. Ser dinâmica, interativa e capaz de reagir às mudanças.

k. Permitir a melhoria contínua dos processos da organização.

Em continuidade, as principais finalidades do gerenciamento de riscos norteados pelo ISO 31.000 estão elencadas a seguir:

a. Alinhar o apetite a risco com a estratégia adotada – os gestores avaliam o apetite a risco da organização ao analisar as estratégias, definindo os objetivos a elas relacionados e desenvolvendo mecanismos para gerenciar esses riscos.

b. Fortalecer as decisões em resposta aos riscos – o gerenciamento de riscos, em sua dupla dimensão, possibilita o rigor na identificação e na seleção de alternativas de respostas aos riscos – Como evitar, reduzir, compartilhar e aceitar os riscos.

c. Reduzir as surpresas e prejuízos operacionais – as organizações adquirem melhor capacidade para identificar eventos em potencial e estabelecer respostas a estes, reduzindo surpresas e custos ou prejuízos as Parte Interessadas.

d. Identificar e administrar riscos múltiplos e entre empreendimentos – toda organização enfrenta um espectro de riscos que podem afetar diferentes áreas da organização. O gerenciamento de riscos, em sua dupla dimensão, possibilita uma resposta eficaz a impactos inter-relacionados, interdependentes e, também, respostas integradas aos mesmos.

e. Aproveitar oportunidades – pelo fato de considerar todos os eventos em potencial, a organização posiciona-se para identificar e aproveitar as oportunidades de forma proativa.

f. Otimizar o capital – a obtenção de informações adequadas e oportunas a respeito de riscos possibilita à organização conduzir uma avaliação crítica e eficaz das necessidades de capital como um todo e aprimorar a alocação desse capital.

A seguir a figura de número 5, demonstra graficamente os relacionamentos entre os princípios da Gestão de Riscos, sua estrutura e processo:

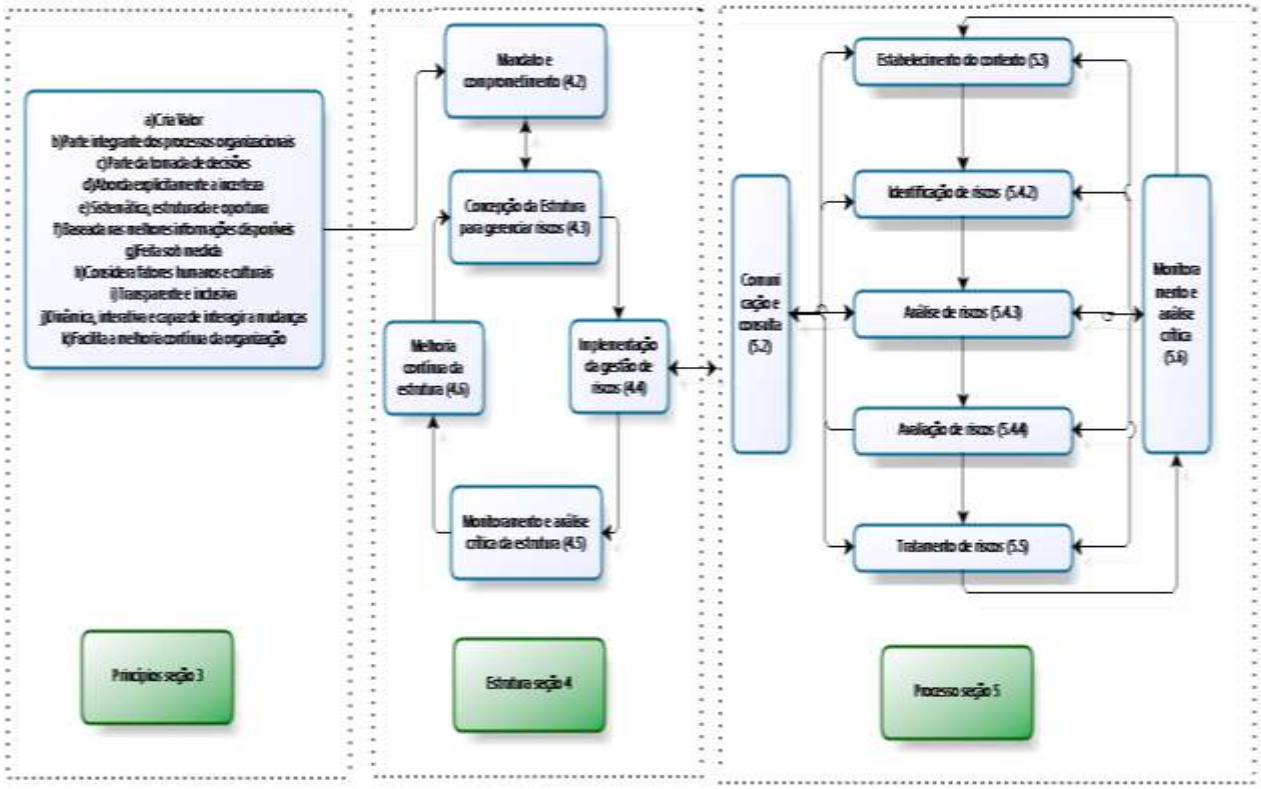


Figura 5: Relacionamentos entre os princípios da GR, estrutura e processo.
Fonte: Adaptado de ABNT, 2009a

2.2 ATIVIDADE DE INTELIGÊNCIA

A atividade de Inteligência, ainda, desconhecida da maioria das pessoas, bem como das organizações empresariais, encontra, eventualmente, reações contrárias nos mais variados níveis decisórios, fruto do preconceito e da falta de flexibilização de raciocínio para visualizar uma contribuição desta Atividade para o planejamento estratégico nas empresas, por meio de uma política de Inteligência.

Para CASTELLO BRANCO (2013, p.42):

> [...] O que é “a Atividade de Inteligência (Atv Intlg)”? Para que serve? Como funciona? Qual sua participação no processo decisório do Poder Executivo? Onde mais pode ser utilizada? Suas técnicas de produção e proteção do conhecimento podem ser aplicadas na área privada? São “sigilosas”?

Basicamente no levantamento bibliográfico realizado a definição do que é Inteligência não é consenso entre os diversos autores que estudam e tratam do assunto. Assim neste sentido PEREIRA (2009, p 19) expõe:

> [...] inteligência não é consenso entre os diversos autores que estudam e tratam do assunto. De um lado, há os que defendem a ideia de que a atividade está baseada no segredo, conferindo-lhe um sentido mais estrito. De outro, aqueles que entendem a atividade de inteligência de forma mais ampla, isto é, como um instrumento que possibilita, por meio de técnicas e métodos próprios, a transformação de dados e informações em conhecimento, com vistas a subsidiar a tomada de decisão.

A lei nº. 9.883 de 07 de dezembro de 1999, que criou o Sistema Brasileiro de Inteligência (SISBIN), apresenta a seguinte conceituação:

> [...] § 2º Para os efeitos de aplicação desta Lei, entende-se como inteligência a atividade que objetiva a obtenção, análise e disseminação de conhecimentos dentro e fora do território nacional sobre fatos e situações de imediata ou potencial influência sobre o processo decisório e a ação governamental; e sobre a salvaguarda e a segurança da sociedade e do Estado. § 3º Entende-se como contrainteligência a atividade que objetiva neutralizar a inteligência adversa.

Segundo CASTELLO BRANCO (2013, p.46):

> [...] A Atv Intlg, em um sentido amplo, caracteriza-se pela identificação de fatos e situações que, de modo real ou potencial, signifiquem obstáculos (problemas) ou oportunidades (melhorias) à consecução de interesses nacionais (ou locais, ou empresariais), bem como o processamento desses insumos, com vistas a subsidiar decisões governamentais (empresariais etc.).

Assim, é competência singular da Atividade de Inteligência, em seu ramo Inteligência e no ramo Contrainteligência identificar, analisar, sondar as ameaças e também as oportunidades no ambiente externo e as vulnerabilidades, fraquezas no ambiente interno das organizações, sejam elas públicas ou privadas.

As ameaças são os agentes, os “atores sociais”, quer de origem interna ou externa às Instituições que por qualquer motivação, realizam ações hostis com forte probabilidade de comprometer a segurança dos ativos organizacionais (recursos humanos, das informações, do material e das áreas e instalações) por intermédio das vulnerabilidades identificadas.

Normalmente essas ameaças, aproveitam as oportunidades geradas pelo relaxamento dos responsáveis pela “salvaguarda” de dados e conhecimentos, e pela não implementação e/ou desconhecimento das medidas decorrentes e uma política (gestão) focada na Atividade de Inteligência.

Ao consultarmos alguns estudiosos do assunto Atividade de Inteligência, no âmbito acadêmico, verificamos que o tema, suscita interpretações diversas. Mas havendo um entendimento que no mundo globalizado em que vivemos a Atividade de Inteligência, no seu ramo Inteligência e no ramo Contrainteligência produzem os conhecimentos que são fundamentais para subsidiar decisões precisas e oportunas, e minimizar os riscos decorrentes das diversas ações empreendidas na sociedade.

A Inteligência desdobra-se, portanto, em dois ramos com características distintas, mas que atuam de forma simbiótica. O ramo Inteligência e o ramo Contrainteligência.

Em continuidade a figura de número 6 demonstra graficamente a forma de atuação simbiótica dos Ramos Inteligência e Contrainteligência:

Figura 6: Atividade de Inteligência

Fonte: ttps://www.google.com.br/search?q=imagens+dos+ramos+intelig_AUIBigB

2.2.1 Contrainteligência

Ramo da atividade de Inteligência responsável pela proteção dos ativos organizacionais, constituído por bens tangíveis (pessoal, material, áreas, instalações, documentos, projetos, programas e portfólios) e intangíveis (conhecimentos, informações, ideias, inovações), agregando suporte metodológico para identificar e gerenciar riscos.

Na figura de número 7 são identificadas as ameaças no escopo da atuação da Contrainteligência:

Figura 7: Ameaças

Fonte: https://br.answers.yahoo.com/question/index?qid=20070508201039AAgXAz

Subdivide-se em:

a. Segurança Orgânica.

b. Segurança Ativa.

2.2.1.1 Segurança Orgânica

Conjunto de medidas preventivas e proativas adotadas para proteger um determinado sistema organizacional de ameaças de qualquer natureza que possam causar efeitos negativos sobre os recursos humanos, o material e a documentação, a informação, as áreas e instalações e as comunicações.

Sendo um conjunto de medidas que objetiva prevenir e obstruir ações adversas de Serviços de Inteligência, elemento ou grupo de qualquer natureza e dirigidas contra a organização.

A segurança orgânica é responsável pelo estabelecimento dos parâmetros de segurança para uma organização, além da elaboração e formatação das normas de segurança, com base em regras previamente definidas, conforme a sua política de Inteligência.

As normas de segurança devem ser particularizadas para cada conjunto de medidas, como segurança de recursos humanos, segurança de áreas e instalações, segurança do material e segurança da informação.

Aqui, há de se destacar que a “INFORMAÇÃO” constitui-se em um importante ativo nas empresas. Assim, a chamada “sociedade do conhecimento”, a informação assume valor exponencial e, é considerado um vetor diferencial entre as organizações de projeção, quer no segmento público ou privado. A sua importância e a sua alta complexidade, dentro de uma visão macro, sistêmica em contrainteligência fazem com que as medidas de segurança desdobrem-se em:
- Segurança da informação no pessoal:
- Segurança da informação na documentação; e
- Segurança da informação nas áreas e instalações.

A figura a seguir, de número 8 descreve o desdobramento da Segura Orgânica:

Figura 8: Segurança Orgânica

Fonte: Livro digital, logística, ações e operações de Inteligência, pag. 87.

2.2.1.2 Segurança Ativa

Conjunto de medidas de natureza repressiva que visa eliminar e/ou neutralizar as ameaças que venham a incidir sobre as organizações (Ativos de Processos Organizacionais, Fatores Ambientais da Empresa), bem como as atividades ilícitas que possam comprometer as atividades operacionais, quer de Inteligência, quer de produção e/ou processos organizacionais.

Atua ofensivamente sobre tais ameaças, usando: Contraespionagem, Contraterrorismo, Contrassabotagem, Contrapropaganda e Desinformação.

a. Contraespionagem:

Tratam-se de medidas de segurança implementadas para evitar a espionagem realizada por entidades e atores adversos. Normalmente se constituem por:

- controle de pessoal;

- controle de comunicações;

- acompanhamento da conjuntura;

- rede de informantes; e

- acompanhamento de atividades sensíveis.

b. Contrassabotagem:

Medidas de segurança voltadas para neutralizar os atos de sabotagem de atores hostis. Elas são desenvolvidas para proteger equipamentos, instalações, pessoas, documentos e sistemas da organização.

c. Contraterrorismo:

As medidas que visam contrapor-se as ações de terrorismo ou outras ameaças tipologicamente assemelhadas, quer de origem doméstica ou internacional, no plano exterior à empresa, ou de origem interna da organização, plano interno desta. Devem ser desenvolvidas em caráter permanente, consubstanciadas em ações específicas de proteção, vinculadas à segurança orgânica e ações específicas ofensivas, para identificação e neutralização de células e organizações sabotadoras.

d. Contrapropaganda e Desinformação:

Destinam-se a neutralizar a propaganda adversa. Algumas organizações amplificam este conceito, estendendo as medidas de segurança para contra-ações

psicológicas, abrangendo, dessa forma, todo tipo de ação psicológica (operações psicológicas).

A figura de número 9, a seguir identifica o conjunto de medidas de natureza repressiva, que atuam ofensivamente na Segurança Ativa:

Figura 9: Segurança Ativa

Fonte: Livro digital, Logística, ações e operações de Inteligência, pag. 90.

3. CONTRIBUIÇÃO DA CONTRAINTELIGÊNCIA

As organizações estão descobrindo que elas nunca serão maiores, ou melhores, do que a capacidade de seus colaboradores em gerar valor. Estão a cada dia tomando consciência que a tecnologia, as máquinas, os processos e as metodologias são ferramentas importantes, mas não funcionarão sem as pessoas bem preparadas. Pois sozinhas não trazem nem a capacidade de criação, nem o poder de tornarem as empresas ágeis, inovadoras, seguras e competitivas.

Essa crescente e importante valorização das pessoas, entendidas com recursos e/ou RH, também traz novos desafios. As ferramentas empregadas necessitam estar balizadas por uma metodologia que dê suporte para o exaltado entendimento do risco que envolve as atividades da organização e das atividades estruturantes do gerenciamento de projetos, em que ambas o cerne é o fator HUMANO.

A contrainteligência por intermédio de uma Análise de Risco, que é processo de decomposição do todo em partes para melhor identificar, assinalar os problemas e implementar soluções, com o fim de neutralizar ou mitigar os efeitos provenientes dos riscos reais e/ou potenciais que possam gerar impactos negativos sobre determinada organização e/ou projeto.

Em continuidade, o Estudo de Situação que é o diagnóstico, é fase da análise de rico que objetiva comparar a situação atual (vigente) com os riscos que possam configurar como ameaças contra as vulnerabilidades do sistema organizacional em estudo.

Entre os componentes que estruturam o processo de análise de risco de um sistema organizacional, existem diferenças fundamentais, a saber: Risco x Perigo x Ameaça.

a. Risco

O risco deve ser considerado sob a ótica da proatividade, pois sugere um fenômeno futuro.

b. Perigo

Traduz o efeito gerado pelo risco. A Contrainteligência estuda os riscos para neutralizar e/ou mitigar os efeitos (impactos) gerados pelos perigos.

c. Ameaça

É o fenômeno que gera impacto a um determinado sistema organizacional, desde que seja composta pelos seguintes elementos:

- ATOR + MOTIVAÇÃO + AÇÃO HOSTIL.

Ex: - um **desenvolvedor** de uma equipe de projetos de TI**,** motivado pela **ambição** de ficar bem na equipe e ser promovido, **sabota** os pacotes de trabalho de outro desenvolvedor (chefe), ao saber que o mesmo está para ser promovido ao final do projeto.

d. Análise comparativa:

- Risco: pacotes de trabalho não serem entregues.

- Ameaça: desenvolvedor + ambição + sabotagem.

- Perigos: demissão, e não é promovido.

Em continuação, na análise de risco, as vulnerabilidades são fraquezas inerentes a um sistema e seus processos organizacionais, cujo conhecimento possa gerar vantagens significativas à configuração de ameaças e a consequente geração de perigos à organização.

Assim, as medidas de Contrainteligência a serem adotas, como práticas metodológicas para suporte ao gerenciamento de risco podem ser elencadas como se segue:

a. Segurança dos Recursos Humanos

1) Estabelecer normas para a operação dos dispositivos de controle de acesso.

2) Regular a recepção de visitantes.

3) Estabelecer normas relativas à entrada na organização.

4) Regular a realização de treinamento especializado para o pessoal da segurança.

5) Estabelecer critérios para o recrutamento e seleção de pessoal.

b. Segurança da Documentação e do Material

1) Estabelecer normas para reforçar as medidas de segurança das dependências da organização.

2) Regular a instalação de câmeras de vigilância no interior da organização.

3) Regular o funcionamento do CFTV a ser implantado, cujo funcionamento deverá ser em regime de 24 horas ininterruptos.

4) Explicitar as normas de segurança que devem ser seguidas pelos prestadores de serviços terceirizados.

5) Intensificar as medidas de controle de abastecimento de combustíveis pelos veículos funcionais e /ou alugados (gestão de frota).

6) Controlar e vistoriar os materiais conduzidos por visitantes.

7) Controlar a circulação de veículos particulares no interior da organização.

8) Controlar o acesso e a circulação de fornecedores que atendem aos funcionários.

9) Estabelecer uma rotina de segurança exclusiva por ocasião da permanência de empresas de segurança de valores no interior da organização.

c. Segurança das Áreas e Instalações

1) Regular a segurança perimetral das instalações da empresa/organização com obstáculos físicos e dispositivos eletrônicos capazes de detectar a presença de pessoas estranhas às atividades.

2) Restringir os locais de acesso de pessoal e veículos no interior da organização.

3) Regular a instalação de barreiras físicas nos tetos e janelas das instalações sensíveis e/ou sigilosas.

4) Regular o uso do estacionamento de veículos particulares.

5) Regular o local de instalações de serviços terceirizados como lanchonetes, postos bancários, dentre outros.

6) Regular a restrição de acesso ao interior das repartições da organização.

7) Regular a restrição ao manuseio das caixas de distribuição de energia elétrica, de ramais telefônicos e o sistema sanitário (esgoto).

8) Regular a utilização de meios que permitam a comunicação necessária ao serviço de segurança orgânica.

d. Segurança da Informação dos Recursos Humanos

1) Regular o credenciamento (LEVANTAMENTO DE SEGURANÇA) do pessoal previsto para ocupar cargo sensível antes da assunção da função.

2) Regular a segurança dos meios de comunicações por meio do estabelecimento de normas claras quanto a utilização dos meios disponíveis.

3) Regular o controle de todo pessoal que adentrar a organização.

4) Regular o acesso ao interior das repartições da organização.

5) Regular auditorias mensais em todos os setores da organização a fim de detectar possíveis falhas na Segurança Orgânica e corrigi-las.

6) Regular o processo de desligamento do pessoal de cada função sensível.

e. Segurança da Informação do Material

1) Regular o acesso de funcionários aos servidores.

2) Regular a restrição de acesso de pessoas ao local diferente de sua estação de trabalho.

3) Regular o acesso aos locais de permanência de seguranças.

f. Segurança da Informação de Áreas e Instalações

1) Estabelecer normas para conscientizar os colaboradores sobre a necessidade de compartimentação da informação, por meio da restrição do acesso a locais que não dizem respeito a determinado público, em detrimento do vazamento de dados ou conhecimentos a respeito de um documento e (ou) matéria.

2) Orientar quanto à autorização de filmagens e fotografias de áreas sensíveis.

3) Orientar quanto à documentação envolvida na identificação, no controle de entrada, no trânsito, no acesso a instalações sensíveis e sigilosas e no controle de saída (crachá de acordo com cada universo e destino).

g. Segurança da Informação da Documentação

1) Guardar cópias das chaves e segredos dos cofres.

2) Protocolar toda documentação que entra e sai, física e eletronicamente.

3) Guardar a documentação sigilosa em local seguro.

4) Impedir o acesso de pessoas não autorizadas a documentos sensíveis.

5) Controlar a reprodução de documentos sensíveis.

6) Atribuir a classificação sigilosa correta aos documentos produzidos.

7) Destruir os rascunhos utilizados na elaboração de documentos sigilosos.

8) Acondicionar corretamente os documentos sigilosos a serem difundidos.

9) Selecionar a documentação sigilosa e/ou sensível que deve ser destruída.

10) Controlar a custódia de documentos sigilosos e/ou sensível.

11) Estabelecer uma rotina para situações de emergência de evacuação e/ou destruição de documentação sigilosa e/ou sensível.

h. Segurança da Informação Digital

1) Armazenar os arquivos em um único computador (servidor de rede).

2) Estabelecer procedimentos de segurança rígidos que restrinjam o uso de dispositivos de gravação de arquivos eletrônicos.

3) Fazer o back up das informações semanalmente e guardar em cofre.

4) Trocar periodicamente as senhas de acesso.

5) Confeccionar normas que disciplinem o uso dos computadores.

6) Disponibilizar uma sala segura para a gerência da rede e para os “switches”.

7) Manter redes distintas para assuntos sigilosos e assuntos administrativos.

8) Estabelecer normas para auditar mensalmente o protocolo eletrônico de documentos.

i. Segurança da Informação das Comunicações

1) Regular a troca periódica dos indicativos e frequências da rede rádio em uso pelo pessoal da segurança orgânica.

2) Definir os assuntos e a forma de veiculação de informação pelas redes rádio.

3) Controlar a documentação que entra e sai da empresa.

4) Restringir a utilização de telefones com linhas externas (comerciais) apenas à necessária para o bom andamento do serviço.

5) Fazer a seleção e o acompanhamento de todo pessoal envolvido no protocolo geral e expedição de documentos da empresa (Serviço de correios/protocolo).

6) Formatação de normas para a utilização de celulares.

A presente figura, de número 10, dá uma visão sistêmica das diversas ações a nível de Segurança Orgânica e Segurança Ativa e sua interdependência:

Figura 10: Visão Sistêmica das Atividades de Contrainteligência

Fonte: https://br.answers.yahoo.com/question/index?qid=20070508201039AAgXAzU

3. CONCLUSÃO

O gerenciamento de risco deve tratar de uma forma cada vez mais integrada as diferentes visões do risco.

Para tanto, o grande desafio está na sistematização de um gerenciamento de risco, que seja capaz de efetivar essa integração por meio de uma comunicação eficaz, na qual todas as partes envolvidas entendam e estejam comprometidas com os objetivos do gerenciamento de risco e da sua gestão.

Outro grande desafio é a sistematização da forma como o gerenciamento deve ser realizado, o que envolve o uso de diferentes metodologias para cada elemento do gerenciamento de risco.

É possível concluir através da pesquisa, dentro do nosso objetivo norteador, qual seja, de identificar a contribuição da Contrainteligência para o gerenciamento de riscos em projetos, que este ramo da Atividade de Inteligência, como uma metodologia estruturada, pode perfeitamente atender às necessidades de conhecimento e adotar as medidas de Segurança, quer Orgânica e/ou Ativa necessárias à proteção da organização (Gestão de Risco) e do projeto (Gerenciamento de Risco).

Portanto, a Contrainteligência tem caráter permanente e integrador por considerar que todas as atividades devem ser pensadas e praticadas constantemente por quem, direta ou indiretamente, desenvolve suas ações no âmbito das organizações e dos projetos.

REFERÊNCIAS

ABRAIC, Associação Brasileira dos Analistas de Inteligência Competitiva. *Perguntas Frequentes*. Disponível em: < http://www.abraic.org.br/site/faqs.asp> Acesso em 02 abr. 2008

ALMEIDA NETO, Wilson Rocha de. Inteligência e contra-inteligência no Ministério Público. Belo Horizonte: Dictum, 2009.

ABNT. Gestão de Riscos – Princípios e diretrizes. NBR ISO 31000. Associação Brasileira de Normas Técnicas. 2009.

ANTUNES; Priscila; CEPIK, Marco. Profissionalização da Atividade de Inteligência no Brasil: Critérios, Evidências e Desafios Restantes. Disponível em: <http://issuu.com/abressan/docs/profissionaliza__o_da_atividade_de_intelig_ncia/1> Acesso em 23 nov. 2013.

AZEVEDO, Daniel Lorenz. Atividade de Inteligência na prevenção do crime organizado. In: SEMINÁRIO ATIVIDADES DE INTELIGÊNCIA NO BRASIL: CONTRIBUIÇÕES PARA A SOBERANIA E A DEMOCRACIA. Brasília, 2002. Coletânea de textos apresentados no... Brasília: Abin, 2003. p. 463-481.

BÍBLIA. Bíblia On Line. Disponível em: <http://www.bibliaon.com/envio_de_exploradores_a_canaa/>. Acesso em: 05 set. 2012.

BRASIL. Lei n° 9.883, de 7 de Dezembro de 1999. Institui o Sistema Brasileiro de Inteligência, cria a Agência Brasileira de Inteligência - ABIN, e dá outras providências. Diário Oficial da União, Brasília, de 8 dez.1999. Disponível em: <www.planalto.gov.br/ccivil_03/Leis/L9883.htm>. Acesso em: 20 out. 2013.

_____. Constituição da República Federativa do Brasil de 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm>. Acesso em: 20 out. 2013.

_____. Decreto 4.376, de 13 de setembro de 2002. Dispõe sobre a organização e funcionamento do Sistema Brasileiro de Inteligência, instituído pela Lei 9.883, de 07 de dezembro de 1999. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto/2002/D4376.htm>. Acesso em: 20 out. 2013.

CASTELLO BRANCO, André Haydt. Inteligência: estratégia de segurança privada: livro digital / André Haydt Castello Branco; design instrucional Flavia Lumi Matuzawa. – Palhoça: UnisulVirtual, 2013.

COLPANI, Clóvis Lopes. Sistema nacional de segurança: livro digital / Clóvis Lopes Colpani; design instrucional Lis Airê Fogolari. – Palhoça: UnisulVirtual, 2011.

FARAH, Camel André de Godoy. Logística, ações e operações de inteligência: livro digital / Camel André de Godoy Farah; design instrucional Rafael da Cunha Lara. –

1. ed. – Palhoça: UnisulVirtual, 2012.

GONÇALVES, Joanisval Brito. O Controle da Atividade de Inteligência em Regimes Democráticos: os casos de Brasil e Canadá. Tese. Brasília: UNB, 2008.

MASP - Metodologia de Análise e Solução de Problemas. Disponível em: <http://www.gepeq.dep.ufscar.br>. Acesso em: 12 abr. 2010.

PEREIRA, Cláudia Vieira. A atividade de Inteligência como Instrumento de Eficiência no Exercício do Controle Externo pelo Tribunal de Contas da União. Disponível em: < portal2.tcu.gov.br/portal/pls/portal/docs/2054618.PDf>. Acesso em: 21 dez 13

PMI. Um guia do conhecimento em gerenciamento de projetos. Guia PMBOK®5a. ed. – EUA: Project Management Institute, 2013.

VARGAS,Ricardo V. Gerenciamento de Projetos: Estabelecendo Diferenciais Competitivos 6ª Edição. Rio de Janeiro: Brasport, 2005.

MAURILIO EDUARDO FREITAS ROSA, CPSI, CIPP, CIGR, CISI, DIDS

ÁREAS DE ATUAÇÃO

Segurança Empresarial: Gestor de Riscos, Gestor de Contratos de Vigilância Patrimonial e Segurança Eletrônica, Prevenção de Perdas. Instrutor credenciado e autorizado pelo Departamento de Polícia Federal. Auditoria e Apuração de Ilícitos. Gestão de Pessoas. Gestor e consultor de Inteligência, Contrainteligência e Operações de Inteligência (Investigação Corporativa). Gestor de Gerenciamento de Riscos em Projetos.

RESUMO DAS QUALIFICAÇÕES

Sólida experiência em gestão estratégica de equipes, vivência com planejamento estratégico, bem como sólida experiência em atividades desenvolvidas na área de Segurança, Inteligência, Contrainteligência e Operações de Inteligência. Estruturado conhecimento em análise e apuração de incidentes de segurança e Segurança da Informação e das Comunicações. Gerenciamento do Plano de Contingência e Crises. Monitoramento, identificação, comunicação, análise e tratamento de riscos operacionais. Elaboração e implementação de políticas, procedimentos e treinamentos de Segurança, Inteligência e contrainteligência. Experiência consolidada em Controle e Coordenação de Operações de Inteligência (Investigação Corporativa). Bem como competência técnica em Segurança e Proteção de Autoridades e Dignitários (VIP). Controle e acompanhamento de Metas e Indicadores. Conhecimento em Auditoria interna, controle e gestão de riscos. Gestão e controle de orçamento otimizando sua efetividade. Relacionamento com autoridades da área de segurança Publica e Inteligência e integração com outros órgão de segurança. Conhecimentos plenos para a elaboração e implementação de Gerenciamento de Projetos (MBA). Inglês básico (cursando). Segurança Empresarial: Gestor de Riscos, Gestor de Contratos de Vigilância Patrimonial e Segurança Eletrônica, Prevenção de Perdas. Auditoria e Apuração de Ilícitos. Gestão de Pessoas. Gestor e consultor de Inteligência, Contrainteligência e Operações de Inteligência. Gestor de Projetos (MBA). Consultor Internacional Segurança Integral. Instituição: LA CORPORACIÓN EURO AMERICANA DE SEGURIDAD, (CEAS). Certificação: CONSULTOR INTERNACIONAL EM SEGURANÇA INTEGRAL, GESTÃO DE RISCOS E PREVENÇÃO DE PERDAS
– (CISI).

O Desafio de Implantação da Gestão de Riscos ESG

Décio Luís Schons, CIEAI, CEGRC, CIGR, CISI

Recém-saído da pandemia e ainda sob seus impactos, o setor empresarial defronta-se com novos desafios, dentre os quais sobressaem a correta gestão dos riscos relacionados à agenda ESG(1), ou simplesmente riscos ESG. Não há como negar que o mundo mudou e um dos aspectos que caracterizam essa mudança é uma preocupação mais pronunciada com a sustentabilidade em todos os seus aspectos. As mudanças climáticas, mais que nunca presentes e evidentes, associadas a uma nova consciência social, motivam a prática de métodos de governança que atendam às expectativas de *stakeholders*(2) bem-informados e participantes do processo de tomada de decisões, graças à ampla conscientização proporcionada pelas mídias sociais. A adequada gestão de riscos é inerente a essa nova forma de encarar os negócios.

Por onde começar?

Os riscos ESG decorrem principalmente da inexistência de um programa ESG devidamente implantado na empresa. Assim sendo, a primeira tarefa daqueles que se dispõem a assessorar a implantação do sistema de gestão de riscos ESG em uma organização é verificar a existência e funcionamento do programa ESG. Caso ele não exista ou seja ainda incipiente, a equipe poderá muito bem colaborar na sua implantação ou aperfeiçoamento.

O ponto de partida para qualquer iniciativa exitosa visando resultados no que diz respeito à Agenda ESG é, sem dúvida, a Governança, com o engajamento responsável da alta liderança, ou seja, do Conselho de Administração (CA) e dos executivos da organização.

O Comitê ESG, ou Comitê de Sustentabilidade, deverá ser necessariamente vinculado ao CA e suas reuniões terão, em princípio, uma frequência mensal. É aconselhável que o líder do comitê seja um dos integrantes do CA com conhecimento do assunto. É desejável também que se incluam outros membros do CA, o CEO e outros ocupantes de cargos no mesmo nível entre os integrantes do Comitê ESG.

Capilaridade e Conscientização

Condição indispensável ao sucesso do programa ESG é a capacitação em todos os níveis, com prioridade para os detentores de cargos mais elevados, mas sem esquecer o chão de fábrica. Essa é a maneira de dar capilaridade ao conhecimento do assunto, gerando a criação de uma cultura comum, com uma linguagem própria

que facilite a comunicação sobre os assuntos relacionados à agenda ESG. Além disso, na medida em que o corpo de colaboradores adquire a consciência do que significa a agenda ESG e de como todos podem ser beneficiados no médio e longo prazo pela sua prática esclarecida, haverá um natural comprometimento de todos. Assume elevada importância, nesse ponto, o aspecto liderança da parte da alta administração da empresa na condução do processo.

É natural que os investidores e demais donos de ações se mantenham preocupados com os resultados financeiros e com a gestão dos riscos e oportunidades mais tradicionais, mas a empresa não pode, em nenhuma hipótese, perder de vista o impacto por ela provocado sobre o meio ambiente natural e social, sob pena de sofrer sérias consequências em futuro próximo.

Determinação dos Aspectos Relevantes

A confecção da matriz de materialidade ou relevância é uma das medidas basilares no processo de implantação da agenda ESG. Mediante uma série de entrevistas e reuniões, os aspectos mais importantes são identificados e tabulados segundo sua importância para o conjunto das partes interessadas e para os resultados financeiros da empresa.

A partir da determinação dos aspectos relevantes, será elaborada a política ESG da empresa, que definirá, em grandes linhas, o que fazer para chegar aos objetivos estabelecidos. É essencial que sejam determinados os pontos de aderência entre a realidade objetiva da empresa e os objetivos estabelecidos no contexto da Agenda ESG. A partir daí, trata-se de manter o foco sobre os objetivos a conquistar e, após conquistados, manter. A direção da empresa precisa saber muito bem o que quer e perseverar, mesmo a despeito de mudanças momentâneas na percepção da importância relativa de cada um desses aspectos considerados mais relevantes.

Determinação dos Riscos ESG

Os riscos ESG são aqueles relacionados aos aspectos ambientais, sociais e de governança e que podem impactar negativamente o desempenho econômico-financeiro da organização. Muito provavelmente, os riscos ligados à agenda ESG terão uma característica de menor urgência em relação aos demais riscos enfrentados pela empresa (riscos patrimoniais, riscos de segurança da informação, riscos cibernéticos e assim por diante). Não se deve perder de vista, porém, que os riscos ESG, ao serem materializados, podem exercer um forte impacto, a ponto de colocar em xeque a própria sobrevivência da organização. Essencial é estabelecer uma

priorização entre os riscos ESG detectados, tomando como ponto de partida uma classificação baseada nos aspectos probabilidade e impacto.

Governança deve sempre ser o foco

Tornou-se praticamente um lugar-comum, quando se aborda a agenda e os riscos ESG, encarar o assunto sob o ponto de vista da sustentabilidade, com prioridade para os pilares Meio Ambiente e Social. Essa, na verdade, é uma visão míope, pois, como já ressaltado anteriormente, a Governança é a coluna mestra de toda o sistema. Deve-se eleger, de início, pelo menos um objetivo correspondente a cada pilar ESG. No pilar Governança, é natural que um dos aspectos selecionados seja aquele que diz respeito à gestão de riscos corporativos, gestão essa que a partir de então englobará obrigatoriamente os riscos ESG.

Conclusão

Tudo que se fala e se debate ultimamente sobre a agenda ESG reflete a necessidade de investidores, especialmente os de grande porte, terem dados confiáveis sobre a saúde financeira das empresas em que pretendem apostar suas fichas. Nesse particular, o assunto Gestão de Riscos, em particular aqueles relacionados à sustentabilidade, vem assumindo uma importância cada vez maior.

Assim é que todo empresário ou administrador que tenha em mente colocar sua organização em lugar de destaque no ambiente de negócios precisa entender que a maneira mais lógica e prática de atingir tal objetivo é construir uma governança em que os riscos ESG ocupem o devido lugar. A correta prevenção ou mitigação dessa categoria de riscos poderá assegurar a perenidade do negócio, porque assentada nos pilares que, comprovadamente, determinam a longevidade de qualquer organização: o Ambiente natural e social em que ela se encontra, as Pessoas que a integram e que são a sua essência e a Governança Corporativa no sentido mais amplo da expressão. Marcas que apresentem a sustentabilidade como propósito e não apenas como instrumento de propaganda (*greenwashing*[3]), obterão o respeito do público e tenderão a gerar resultados compensadores para os *shareholders*[4] e para os *stakeholders* em geral.

[1] *Environment, Social and Governance* na sigla em inglês, ou Meio Ambiente, Social e Governança.

[3] *Greenwashing*: literalmente, lavagem verde, é a expressão utilizada para designar ações que agridem o meio ambiente, mas são maquiadas para parecer sustentável.

(2) *Stakeholders*: partes interessadas no negócio da empresa – acionistas, colaboradores, dirigentes, clientes, fornecedores, população vizinha, agências estatais etc.

(4) *Shareholders*: acionistas da empresa.

Décio Luís Schons, CIEAI, CEGRC, CIGR, CISI

General-de-Exército da Reserva, é Vice-Presidente de Operações de Consultoria da empresa Brasiliano INTERISK.

A relação entre a tecnologia blockchain e a segurança cibernética

Mariana da Silveira
CEGRC, CIGR, CISI, MBA em GRC, MBCR, DPO, CISO

No início da década de 1990, o físico *W. Scott Stornetta* e o cientista da computação *Stuart Haber*, pesquisadores norte-americanos pioneiros da tecnologia *blockchain*, mencionaram pela primeira vez a arquitetura *blockchain*, em uma publicação de 1991 intitulada *"How to Time-Stamp a Digital Document"*, em tradução livre "Como registrar um carimbo de data e hora em um documento digital".

A publicação tratava de um sistema de hierarquia digital chamado "cadeia de blocos", que permite a ordenação de arquivos gravados de modo único e seguro, possibilitando a gestão de documentos digitais livre de modificações ou manipulações. No ano seguinte, os estudiosos realizaram melhorias em seu sistema e incorporaram “árvores *Merkle*[1]”, com aumento de eficiência, permitindo a coleta de um maior número de documentos em um único bloco.

No entanto, apenas em 2008 o *blockchain* viria a ganhar notoriedade, com a publicação do artigo “*Bitcoin: A Peer-to-Peer Electronic Cash System*”, em tradução livre, “*Bitcoin*: um sistema financeiro eletrônico de pessoa para pessoa”. Esse texto, de autoria atribuída a *Satoshi Nakamoto*, codinome de uma pessoa ou grupo, trouxe a público a existência do *Bitcoin* como a primeira aplicação da tecnologia de contabilidade digital.

Temos acompanhado nos últimos anos a evolução da tecnologia *blockchain* e o surgimento de suas mais diversas aplicações, tais como transações com moedas digitais, sistemas de pagamentos, contratos inteligentes (*smart contracts*), registros

médicos no segmento da saúde, cadeia de suprimentos, registros acadêmicos no segmento da educação, com atuação na segurança cibernética mediante a mitigação de vulnerabilidades e neutralização de ameaças.

Blockchain é o encadeamento de blocos que contêm informações criptografadas para criar um banco de dados. Ele atua como um tipo de livro-razão (*ledger*) distribuído (descentralizado), que rastreia, verifica, processa e registra as transações de ativos em rede, permitindo a localização do registro e possibilitando, por meio da mineração (processo de validação e inclusão de novas transações), a determinação exata das transações.

A mineração ocorre por resolução de cálculos matemáticos complexos de criptografia, para dar sequência ao encadeamento em blocos (contendo o histórico das transações), em que cada bloco possui um *hash* (registro único) criptográfico, registrado no *ledger*, de um bloco anterior da cadeia. Por se tratar de tecnologia descentralizada, a alteração de um bloco por parte de um minerador deve ser confirmada pelos demais, em toda a rede.

Tal tecnologia torna o bloco de transações confiável, único, inalterável (é possível adicionar novos dados, nunca alterar ou excluir dados pré-existentes) e compatível com o bloco anterior. Sua atualização é sequencial,
mantendo uma trilha histórica perpétua. Destacam-se a transparência, com a visualização das transações e a descentralização, já que é desnecessária a validação por parte de autoridades certificadoras, sendo a fidedignidade garantida pela redundância das informações em diversos computadores distribuídos na internet.
[1]https://pt.theastrologypage.com/merkle-tree

As vantagens oferecidas pelo *blockchain* são inúmeras. Dentre elas, podemos destacar a proteção, a rastreabilidade do processamento de dados, que gera a integridade na transferência de dados e a confidencialidade do usuário, além da descentralização, uma vez que a falha de um único computador não afeta toda a rede. Isso provoca uma maior disponibilidade das informações e facilita a mitigação dos riscos relacionados ao comportamento humano na rede.

Quanto às desvantagens, é importante ressaltar que existem diferentes tipos de *blockchain*: públicos, privados e híbridos. Nas estruturas não permissionadas (públicas), qualquer nó (computador) da rede pode ler e gravar transações. Já nas estruturas permissionadas (privadas), as ações são restritas aos nós autorizados. Portanto, ao se falar em *blockchain*, os níveis de vulnerabilidade e ameaças estão relacionados à sua respectiva tipologia.

Assim, podem ser citadas como desvantagens o comprometimento dos nós validadores, gerando a falsificação de transações; o gerenciamento de chaves privadas que, se perdidas, são irrecuperáveis; os bancos de dados e APIs; vulnerabilidades na infraestrutura subjacente; vulnerabilidades de autenticação; exposição de dados armazenados; acesso aos dados no bloco e roubo de chave; alto custo de implantação e manutenção; dificuldades de escalabilidade em razão do processamento de dados excessivo; e consumo elevado de energia.

Um ponto importante, quanto à aplicabilidade dessa tecnologia, é a ausência de mecanismos de privacidade e proteção de dados pessoais, devido à transparência oferecida pelo registro em *blockchain*, que permite que todos os detalhes dos registros das transações sejam conhecidos. Ele impede inclusive que dados registrados sejam alterados, o que fere a autodeterminação informativa do titular dos dados pessoais,

negando-lhe a possibilidade de alterar informações, a retirada de consentimento, o direito ao esquecimento, dentre outros.

Sob as mesmos condições encontram-se os *smart contracts*, que são acessíveis devido à transparência, possuem valor, despertam o interesse de atacantes, e são imutáveis mesmo diante de um erro de segurança. O grande benefício dos contratos inteligentes é que o acordo entre as partes é realizado por um padrão único, conferindo maior transparência, já que todas as partes envolvidas possuem acesso aos dados em tempo real.

O ambiente cibernético é composto pelos usuários e pela cultura na qual estão inseridos; pela infraestrutura, governança e serviços de TIC (Tecnologia da Informação e Comunicação), máquinas, equipamentos, componentes periféricos, redes de comunicação, sistemas lógicos, gestão organizacional estratégica; e pela segurança do ambiente físico.

Toda essa complexidade expõe a *blockchain* a riscos cibernéticos, já que não existem tecnologias, pessoas, equipamentos ou processos que estejam imunes a ameaças e vulnerabilidades cibernéticas no ambiente de rede. Por isso, é mister envidar esforços para que a segurança cibernética na organização seja tratada em âmbito estratégico e não apenas no nível tático, isto é, aquilo que se refere a questões relacionadas à unidade organizacional de TIC.

Um grande desafio apresentado é que, apesar de haver pujantes soluções em *blockchain* disponíveis no mercado, ainda existe a falta de profissionais qualificados para manter uma rede protegida e em funcionamento, uma vez que para isso são exigidas diferentes linguagens de programação e ferramentas. Ressalta-se, inclusive, o choque de gerações tecnológicas como fator dificultador da implantação do *blockchain*, pela frequência na troca dos sistemas que rodam na rede, de modo a garantir a performance.

Ainda que a *blockchain* seja reconhecidamente uma tecnologia revolucionária, ela não é impenetrável e não está livre de ataques cibernéticos. Em razão da garantia do anonimato, é conferido um baixo risco ao atacante cibernético e uma alta recompensa associada aos fatores de sucesso. Por essa razão, são crescentes os esforços para a exploração de quaisquer vulnerabilidades no ambiente de *blockchain*.

Nesse diapasão, podemos citar ataques como o DDoS, que pode tornar os recursos de um sistema indisponíveis para seus utilizadores. A tecnologia *blockchain* consegue mitigar o sucesso desse tipo de ataque pela descentralização das entradas de Sistemas DNS (Sistema de Nomes de Domínios). Temos também o ataque de gasto duplo, tentativa de modificar a organização da cadeia *blockchain*, ou afetar o *hash power*, que compromete o poder computacional e a segurança de uma rede *blockchain*.

Percebe-se que a maioria dos problemas de segurança cibernética enfrentados durante as implementações de *blockchain* não estão diretamente relacionados ao *blockchain* em si, mas a questões clássicas de segurança da informação. Assim, independentemente da utilização de tecnologias mais modernas e confiáveis, as organizações não podem negligenciar as medidas técnicas, físicas e organizacionais, sob a tríade da confidencialidade, integridade e disponibilidade.

Dessarte, a tecnologia *blockchain* exige uma reflexão sobre os aspectos mais básicos da segurança da informação, tais como comportamento do usuário na rede,

engenharia social; aplicação de medidas técnicas em camadas de proteção, utilização de antivírus, *firewall*, sistema operacional e sistemas devidamente licenciados, atualizados, ativos em todos *endpoints* (equipamentos), utilização de anonimização, pseudonimização, criptografia; segurança física, proteção de perímetros de segurança; medidas organizacionais como elaboração de políticas, normas e procedimentos.

A realização de testes de segurança nos planos de recuperação de desastre e de resposta a incidente é primordial para assegurar a adequação, o treinamento e o aperfeiçoamento dos planos e da equipe envolvida, em um processo de melhoria contínua. A segurança cibernética precisa estar alinhada com todas essas medidas técnicas, físicas e organizacionais para alcançar sua eficácia.

A busca por uma solução integrada deve ser o objetivo a ser alcançado em qualquer organização. Não existe uma única tecnologia ou solução que contemple todas as funcionalidades e ainda elimine todos os riscos, vulnerabilidades e ameaças cibernéticos. Risco zero implica custo infinito e por isso surge a necessidade de uma solução em segurança cibernética cuja metodologia ofereça as condições necessárias e suficientes para permitir aos gestores a visão prospectiva dos riscos da empresa, permitindo uma análise e avaliação dos riscos com maior precisão.

A solução deve contemplar, pelo menos: indicadores estratégicos; realização de *walkthrough* (avaliação dos controles existentes); análise da cadeia de valor da organização; identificação de processos, sistemas e informações críticos do negócio; avaliação da maturidade das pessoas responsáveis; identificação das vulnerabilidades; levantamento da maturidade em segurança cibernética da organização; identificação da motricidade dos fatores de riscos cibernéticos; e avaliação de riscos cibernéticos inerentes e residuais.

Porém, a gestão de riscos cibernéticos não pode encerrar-se nesse estágio. É preciso elaborar e avaliar cenários de ataques cibernéticos, conforme as avaliações dos riscos cibernéticos e os perfis dos atacantes, de acordo com suas próprias características. Isso permite à organização preparar uma solução de inteligência em riscos, com ações preventivas e mitigatórias, com crises suportadas com base na relação custo x benefício e com a mensuração dos impactos no negócio da organização.

Isso posto, a tecnologia *blockchain* oferece a segurança que a criptografia oferece ao registro das transações e ao rastreamento de ativos em rede, o que mitiga os riscos cibernéticos consideravelmente. Contudo, essa tecnologia também possui vulnerabilidades e por isso é preciso que a organização compreenda a dimensão estratégica da segurança cibernética como pasta da alta direção, realize os investimentos necessários em soluções cibernéticas e institua a cultura de segurança cibernética.

Mariana da Silveira
CEGRC, CIGR, CISI, MBA em GRC, MBCR, DPO, CISO
Gerente de Gestão de Riscos, ex-aluna do MBA e MBCR do Prof. Dr. Antonio Celso Ribeiro Brasiliano

22 previsões de segurança para 2022. Um ano de novos desafios e exigências

Manuel Sánchez Gómez-Merelo
Consultor Internacional de Seguridad

Vivemos em meio a uma incerteza especial derivada do COVID-19. No que diz respeito às vulnerabilidades e segurança, vale destacar: ataques à cadeia de suprimentos, aumento de incidentes cibernéticos, aumento da pressão sobre ataques a sistemas operacionais e dados pessoais, etc. Tudo isso fez com que as organizações, públicas e privadas, percebessem que, em sua cadeia de segurança, elas são tão fortes quanto seu elo mais fraco.

Um capítulo à parte são os ataques a infraestruturas críticas em todo o mundo, já que, principalmente, os ciberdelinquentes aumentaram os ataques contra órgãos governamentais e serviços essenciais, como transporte, saúde, entidades financeiras etc.

Agora é hora de fazer um balanço do que foi o ano de 2021 e tentar prever o que acontecerá em 2022.

A parte positiva é que estamos dispostos a reconfigurar e redefinir nossos recursos de detecção, resposta e resiliência de ameaças, para identificar novos vetores de ataque, porque você não pode proteger o que não pode ver.

Jogando com os anos que passamos neste século XXI, resumimos esses novos vetores em 22 previsões que devem nos encontrar preparados para atender sua abordagem e neutralização:

1. **A segurança na cadeia de suprimentos será priorizada**

As organizações precisarão analisar e priorizar a resiliência da cadeia de suprimentos e o fornecimento responsável.

Os autores de ameaças, principalmente os ciberdelinquentes, estão cada vez mais visando os produtores e fornecedores mais vulneráveis ou menores, tornando quase inevitáveis as violações da cadeia de suprimentos ou de terceiros.

2. **A legislação global de privacidade será acelerada**

Os funcionários do governo precisarão acelerar as mudanças nas leis e regulamentos de privacidade globalmente.

Como a proteção de dados continua sendo um dos componentes mais importantes da segurança das organizações e dos cidadãos, espera-se que novas leis globais de privacidade cubram as informações pessoais de uma grande porcentagem da população, conforme estabelecido no GDPR (Regulamento Geral Europeu de Proteção de Dados), a localização e a proteção de dados continuarão a ser um componente importante.

3. **A contratação de compliance officer será aumentada**

O que é um Compliance Officer?

O Compliance Officer é o profissional responsável por garantir que todos os procedimentos da organização sejam cumpridos. Este executivo tem como objetivo assegurar a governança corporativa. Eles são responsáveis por desenvolver programas de conformidade, revisar as políticas da companhia e aconselhar a administração sobre possíveis riscos

Diante do desenvolvimento de novas legislações e normativas nacionais e internacionais, vai se produzir nas organizações uma demanda de responsáveis por cumprimento que ajudem a navegar pelos novos requisitos complexos e em constantes mudanças.

4. **A gestão dos sistemas e serviços de segurança será consolidada**

Os sistemas de segurança e a gestão de fornecedores de produtos e serviços especializados exigirão uma nova abordagem à sua gestão e garantias.

Com a mudança dos principais processos de negócios das organizações para ambientes de nuvem complexos, haverá uma demanda crescente para agilizar o gerenciamento de produtos e sistemas de segurança do fornecedor.

5. **Os gastos com detecção e resposta a ameaças aumentarão**

Com a proliferação de grandes campanhas de ataque de malware, como as vistas em 2021 (incluindo ransomware e spearphishing), os responsáveis por cybersegurança precisarão se concentrar em ficar à frente dos invasores cibernéticos para proteger suas atividades com o aumento resultante em investimentos e gastos.

6. **Os prêmios de seguro e seguro cibernético serão aumentados**

Como consequência do aumento dos ataques, os prêmios de seguro de segurança e segurança cibernética ficarão mais caros e dispararão, dado o grande impacto dos recentes ataques cibernéticos. O seguro cibernético já é muito mais caro, pois os custos dispararam e os prêmios provavelmente continuarão subindo.

7. **A falta de competências em segurança cibernética aumentará**

Apesar do grande número de programas de treinamento e certificações existentes para demonstrar competência como profissional especializado em segurança cibernética, a oferta será superada pela demanda por novos empregos que terão que ser preenchidos.

8. **A legislação e os regulamentos de segurança serão atualizados**

Como consequência dos atrasos decorrentes da pandemia, principalmente em relação às atualizações, a legislação e os regulamentos atuais das diferentes matérias e competências de segurança devem ser atualizados para avançar no caos causado desde o início de 2020 por outros compromissos exigidos no curto prazo.

9. **A liderança dos profissionais de segurança será reinventada**

A liderança em segurança é um aspecto chave para promover a nova cultura de prevenção e proteção que os novos desafios de segurança nos exigem para todo o tipo de atividades e setores e, principalmente, para aquelas infraestruturas operacionais críticas ou de funcionamento essencial.

É necessário implantar um novo modelo de gestão a ser seguido, motivando as pessoas a trabalhar com segurança, mostrando envolvimento e comprometimento com a conformidade e premiando o desempenho satisfatório.

10. As chaves para promover uma cultura preventiva serão atualizadas

Dadas as incidências e consequências derivadas do desenvolvimento da pandemia em 2021, deve-se atualizar os aspectos conceito-chave que sirvam para promover a necessária nova cultura de prevenção e proteção, tanto para pessoas como para organizações, nas distintas atividades de serviços, industriais e comerciais.

11. O envolvimento do pessoal na segurança será reforçado

A participação e envolvimento dos trabalhadores na segurança das organizações é um elemento eficaz na geração de uma cultura de prevenção e proteção, necessária a todos os membros da organização para gerir a saúde e segurança. Este envolvimento de todos os níveis da organização na identificação dos riscos e nas propostas para o seu controle e gestão, contribui para que os colaboradores sintam como “seus” os procedimentos implementados.

12. Será promovida uma formação especializada contínua e sistemática

Os novos desafios e exigências de segurança exigirão cada vez mais, com novos programas de formação contínua e especializada, aprendizagem sistemática e permanente, que é um elemento vital para o sucesso da prevenção e proteção numa organização. Uma cultura de treinamento baseada em ampla participação aumenta a capacidade da organização de identificar e alterar situações de risco ou ameaça.

13. Ataques de ransomware e crimes cibernéticos aumentarão

Muitos ataques complexos e suas consequências foram sofridos durante 2021, especialmente prejudiciais à cadeia de suprimentos, sistemas de saúde, transporte e logística.

As táticas de ransomware e crimes cibernéticos continuarão a evoluir e aumentar ao longo de 2022. O modelo de “duplo shakedown”, onde os dados são bloqueados e o adversário simultaneamente ameaça liberá-los, persistirá.

14. Confiança e identidade serão priorizados em projetos de segurança

As organizações públicas e privadas, de todos os setores de atividade, continuarão desenvolvendo e implementando a transformação digital, e a tendência se acelerará. Pesquisas mostram que estabelecer a confiança e a identidade das empresas globais de segurança serão priorizadas nos projetos de implementação.

15. Todos os tipos de ameaças se consolidarão e evoluirão

As previsões para 2021 incluíam uma ampla variedade de ameaças à segurança que estavam diretamente relacionadas ao desdobramento da pandemia do COVID-19. Prevê-se que, embora a incidência da pandemia se reduza lentamente, essas ameaças continuarão e se consolidarão.

16. A segurança cibernética será reforçada através da automação

Novos sistemas de controle e automação impulsionarão especialmente as melhorias de segurança cibernética. À medida que as organizações trabalham para se adaptar a “nova normalidade”, a eficiência das tecnologias de segurança será impulsionada para garantir a continuidade dos negócios.

17. Novas demandas de segurança serão criadas à medida que a soberania da nuvem aumentar

Em um mundo global cada vez mais integrado à nuvem, as abordagens de segurança tradicionais baseadas na proteção de perímetro são obsoletas. Prevemos que os desafios de segurança cibernética se tornarão ainda mais exigentes à medida que os serviços em nuvem se tornarem mais especializados e globais.

18. Será dada prioridade à estratégia/cultura de segurança nas organizações

Será dada prioridade às organizações que trabalham com rigor e responsabilidade para fortalecer uma cultura de segurança e segurança cibernética - segurança física e lógica - liderada por níveis superiores e em modelos de participação público-privada.

19. Se evoluirá para a segurança integral e integrada

Como vem estabelecendo-se nos últimos anos, evoluíra-se de forma importante para colocações de segurança global, com sistemas de prevenção e proteção integral e integrados.

20. Inovação em sistemas de segurança será priorizada

Perante os novos desafios e exigências de proteção de pessoas, bens e atividades ou serviços, as soluções assentarão e priorizarão a implementação de sistemas e produtos inovadores de segurança física e segurança cibernética.

21. Ele evoluirá para a identificação de riscos de segurança cibernética

Derivado das consequências do aumento dos ataques dos ciberdelinquentes em 2021, evoluirá para uma necessária e rigorosa identificação de novos riscos em termos de segurança lógica ou segurança cibernética.

22. Novos paradigmas serão definidos para planos de segurança

Os novos desafios e requisitos de segurança vão exigir uma mudança de paradigmas de segurança em todos os tipos de Planos de Segurança e Contingência, independentemente dos setores de atividade e da dimensão das organizações.

Resumindo

As previsões indicam claramente que, em 2022, a gestão de riscos em segurança física e segurança cibernética e o planejamento para gerenciar a incerteza e a resiliência serão priorizados.

A realidade é que o mundo e os tempos em que vivemos estão cada vez mais rápidos, com novos ataques e novos desafios para o funcionamento das organizações que devem manter-se flexíveis e adaptáveis a novas situações.

Você precisa planejar a incerteza, planejar a resiliência e, assim como os procedimentos de ataque, a segurança precisa evoluir constantemente. 2022 será um ano de mudança e conscientização para uma nova cultura de gestão de risco e segurança.

Por outro lado, também terá um certo impacto a recente aprovação da Estratégia Nacional de Segurança 2021 na Espanha, que contempla a inovação tecnológica como chave para a recuperação económica, a coesão social e a transição ecológica como caminhos para um país moderno com visão de futuro e progresso.

Especificamente, no capítulo sobre riscos e ameaças, o texto apresenta campanhas de desinformação aliadas a tecnologias e estratégias híbridas como elementos transversais ao conjunto de riscos para a segurança nacional. Um dos principais objetivos definidos é desenvolver capacidades de prevenção, detecção e resposta contra ameaças cibernéticas e favorecer a dimensão de segurança das novas ferramentas digitais.

Da mesma forma, a nova estratégia propõe a articulação de uma política preventiva que se baseará no estabelecimento de um sistema de alerta precoce,

baseado em tecnologia, que forneça indicadores para todas as áreas da segurança nacional.

Por fim, indicam que 2022 será o ano de uma evolução significativa dos profissionais de saúde e segurança. Finalmente, as organizações começaram a perceber a importância desses trabalhadores, que, em tempos difíceis, souberam se elevar acima de suas qualificações e responsabilidades, sempre que necessário.

Manuel Sánchez Gómez-Merelo
Presidente · Director General de ET. Estudios Técnicos, s.a.
Director de Programas de Protección de Infraestructuras Críticas del Instituto Universitario General Gutierrez Mellado IUGM-UNED
http://www.manuelsanchez.com

A importância da gestão sistêmica nas organizações

Prof. Dr. André Vicente dos Anjos, CIGR

Todas as organizações foram pensadas para ter êxito no cumprimento de seus objetivos sendo salutar, não só para o empregador, mas para os colaboradores que a empresa cresça, pois, esse movimento pode gerar novas oportunidades de desenvolvimento para todos os membros do time. É fato que, quando uma organização atinge suas metas e tem sucesso, todos são beneficiados, crescendo mutuamente.

Partindo desta premissa, observando a importância do cumprimento das metas para o alcance dos objetivos organizacionais, considera-se relevante que qualquer empresa tenha um planejamento focado no objetivo macro, sem deixar de considerar a situações adversas. Correção de possíveis falhas, caso elas ocorram. Esse gerenciamento deve ter seu foco na mitigação de riscos que possam ser impeditivos ao cumprimento do macro objetivo. Desconsiderar os riscos, seus impactos e sua correta forma de tratamento tem sido uma das principais deficiências de empresas em diferentes segmentos e tamanhos.

As falhas, em sua maioria, impactam nos processos das empresas, em maior ou menor intensidade por não serem observadas de forma analítica e ainda preteridas no contexto do planejamento, sendo muito comum perceber a inexistência inclusive, de um plano que possibilite uma resposta assertiva, tanto para ações preventivas como para as corretivas, que visam diminuir os impactos.

Segundo Falconi (2009), (...) “problema é um resultado indesejável, contudo, em uma visão mais moderna do sistema preventivo de segurança de uma organização, observa-se a existência de problemas bons e ruins. O primeiro é estimulado pelo gestor quando identifica lacunas em sua área de responsabilidade, com o objetivo de mitigar as falhas que possam impactar o negócio. O segundo corresponde a desvios e inconsistências em processos administrativos ou operacionais e devem ser resolvidos imediatamente.

Obviamente, se estamos falando aqui de gestão, é importante trazer à baila alguns importantes conceitos, um deles, atribuído a Edwards Deming. “Não se gerencia o que não se mede. Não se mede o que não se define. Não se define o que não se entende e não há sucesso no que não se gerencia”. (DEMING, 1990). Ainda nesta linha, os

autores do método Balanced Scorecard (BSC) assim apregoaram. “medir é importante: o que não é medido não é gerenciado” (KAPLAN; NORTON, 1997).

Dentro deste contexto de gerenciamento com métricas, outros importantes nomes como Drucker e Kotler, por exemplo, também dedicaram linhas em suas obras, pautando as métricas e controles como ferramentas importantes e fatores de sucesso dentro de um sistema organizacional.

Mesmo diante de um modelo de gerenciamento bem estruturado implantado, é possível que um ou mais riscos se materializem, inclusive de forma recorrente, dependendo do tipo de negócio. Para este cenário, a depender do risco materializado e seus impactos, é salutar a existência de todo o arcabouço sistêmico que contemple, desde o diagnóstico situacional da planta a ser protegida, passando pela análise dos riscos até o Plano de continuidade do negócio, por exemplo.

Um dos objetivos da implementação de um plano de continuidade do negócio é entender, de maneira profunda, os processos da organização de modo a possibilitar que esta se recupere de forma estruturada de impactos leves, médios ou massivos, pois mesmo com um modelo de gerenciamento de riscos bem estruturado e implantado, é possível que um ou mais riscos se materializem, inclusive de forma recorrente.

Segundo Adriana Beal (2005), embora o processo de gestão da continuidade do negócio possa resultar na identificação de oportunidades, redução de ameaças e vulnerabilidades, gerando recomendações para a melhoria dos controles, o seu principal foco é a recuperação de eventos. As etapas são: entender a empresa, determinar a estratégia de GCN, desenvolver e implementar a resposta de GCN e testar, manter e revisar.

Uma das formas mais eficazes de diminuir a possibilidade de falhas ou ainda de corrigi-las em tempo é a implementação de um CICLO PDCA. Sendo uma das mais relevantes metodologias quando se trata em melhoria contínua de processos, é indispensável sua aplicação, pois pode ser usado como método de implantação de novas ideias quanto na solução de diferentes problemas, podendo ser implementado em todos os níveis da organização, no âmbito estratégico, tático e operacional.

Lembrando que, os processos, junto com outros importantes componentes do sistema, estão entre os pilares de qualquer organização e uma das pedras

basilares na integração de todas as áreas da empresa, desde a direção até o chão de fábrica.

A gestão sistêmica assegura o cumprimento de metas e prazos, a qualidade das ações de maneira a proporcionar diferencial competitivo em um mercado saturado de iguais.

Prof. Dr. André Vicente dos Anjos, CIGR, CPSI, CISI

Coordenador de Segurança Sênior.

Especialista em Riscos Corporativos.

Consultor de Segurança Segmento Varejo.

CONTRATAÇÃO DE SERVIÇOS DE SEGURANÇA PRIVADA DE FORMA CORRETA PARA EVITAR RISCOS DESNECESSÁRIOS POR DESCUMPRIMENTO DE REGULATÓRIOS OU CRISES NO SEU NEGÓCIO?

Prof. Dr. Antônio A. Mota, CPSI

Primeiro vamos esclarecer o obvio, a Segurança Privada é regulamentada, controlada e fiscalizada pela Polícia Federal (PF) através das Delegacias de Controle de Segurança Privada (DELESP) e Coordenação-Geral de Controle de Serviços e Produtos (CGCSP), com base ainda na lei 7.102/83 de 20 de junho de 1983 e da atual Portaria 3.233/2012 – PF e 10 de dezembro de 2012.

Uma empresa especializada em segurança privada somente poderá funcionar se autorizada pela PF podendo ser comprovado através de publicação no Diário Oficial da União (DOU) com o Alvará de Autorização de Funcionamento ou com o Alvará da Renovação da Revisão de Autorização de Funcionamento que é obrigatório a renovação a cada ano.

Salientamos ainda, que uma empresa de segurança privada somente poderá prestar os seus serviços especializados nas seguintes condições:

• Com atividades que esteja autorizado pela PF (Vigilância Patrimonial; Escolta Armada; Segurança Pessoal Privada e Transporte de Valores).

• Somente prestar serviço nos estados que possua Matriz e/ou Filiais devidamente autorizadas pela PF.

• Não poderá prestar serviços com profissionais que não estejam devidamente contratados com Carteira de Trabalho assinada e todos assegurados em contrato com seguradora por conta do empregador.

• Não poderá prestar serviços com profissionais que não possuam seus cursos de formação de vigilantes ou de extensão em dia dentro da validade de 02 anos sendo obrigatório os cursos de reciclagens conforme as atividades que os vigilantes estejam atuando.

• Todos os vigilantes contratados pelas empresas na sua prestação de serviços deverão estarem relacionados e segurados com Seguro de Vida em Grupo constando em contrato assinado com uma seguradora.

• Nos contratos de vigilância patrimonial, escolta armada e segurança pessoal, a empresa poderá adicionar postos de supervisão, desde que os supervisores apenas supervisionem ou coordenem as atividades dos vigilantes pertencentes a própria empresa.

• Todos os vigilantes deverão portar suas Carteiras Nacional de Vigilantes (CNV) que a empresa tem a obrigação de providenciar em até 30 dias da contratação dos vigilantes que ainda não possuam CNV.

• Nos postos com arma de fogo, todos os vigilantes deverão obrigatoriamente usar Coletes a Prova de Balas. Tomando os devidos cuidados seguindo o que está descrito acima, elaborando um Procedimento Operacional Padrão (POP) por posto de serviço, promover os treinamentos adequados conforme cada cliente, e supervisão com

acompanhamento constante de seus efetivos, certamente a empresa evitará transtornos e crises, inclusive perdas de contratos e financeiras.

• Riscos que deverão ser prevenidos e evitados: Multas aplicadas pela PF, passivos trabalhistas, indenizações para cobertura de seguro obrigatório do risco de vida em grupo, rescisões de contratos, glosa de faturamento etc.

“Crise é um fenômeno complexo, com finalidades e origens diversas, que se caracteriza por uma mudança de estado às vezes subitamente gerando dúvidas e elevados transtornos, e com grandes chances de agravamento principalmente se não for dada atenção imediata podendo gerar consequências com perdas irreversíveis”.

Destacamos que as responsabilidades por contratar bem a prestação de serviços de segurança privada com excelência, eficácia e efetividade, deve ser compartilhada pelos gestores representantes do contratante e contratado. Inclusive devendo envolver as áreas jurídicas e compliance.

Antônio A. Mota, Doutor em Filosofia em Ciências de Segurança Internacional, Ph.D. Membro do Grupo de Excelência em Defesa e Segurança – CRA – CE. Sócio honorário da CEAS Internacional – Capítulo Brasil nº 12. Sócio na ABSEG nº 570

Contatos: Cel. 85 99145-7777 | e-mail: aa.mota@motaassociados.com.br

Novos Desafios e exigências de Segurança Global em Instalações Portuárias

Manuel Sánchez Gómez-Merelo

Consultor Internacional de Segurança

A segurança nas instalações portuárias, como princípio geral, deve basear-se no livre acesso à prestação de serviços, ressalvadas as limitações de espaço, capacidade das instalações, normas de segurança ou ambientais.

São áreas de atuação muito sensíveis a mudanças e modificações nas normas ou protocolos operacionais, pois são instalações complexas e vulneráveis, permanentemente em operação, cenários múltiplos, atividades diversas, dimensões especiais, e tudo isso operando sob uma gama muito ampla de riscos e ameaças.

Por isso, a segurança é a base e a referência de toda a atividade e deve ser considerada como uma otimização da gestão portuária para garantir eficiência, rapidez e flexibilidade.

Têm as mesmas bases de segurança, prevenção e proteção do interesse industrial, económico e social. Os principais objetivos são identificar as condições de insegurança, deficiências, vulnerabilidades e deficiências em questões de segurança para estudar soluções específicas.

As instalações portuárias são, em geral, infraestruturas estratégicas sobre as quais assenta a operação de serviços essenciais e, em grande medida, são classificadas como infraestruturas críticas quando a sua operação é essencial e não permite soluções alternativas.

Os Setores Estratégicos e Infraestruturas Críticas são uma das áreas de estudo do Curso de Diretor de Segurança em Infraestruturas Críticas e Estratégicas, aprovado pelo Ministério do Interior para a qualificação de Diretores de Segurança Privada.

Riscos, ameaças e vulnerabilidades

Risco, ameaça e vulnerabilidade são três conceitos que estão inter-relacionados, mas não se sobrepõem. O risco é o motor do progresso. A ameaça está em toda parte e a vulnerabilidade é inversamente proporcional às medidas tomadas antes que a ameaça se torne realidade.

Os novos desafios para uma eficaz Gestão de Riscos nas instalações portuárias devem ser contemplados: no Quadro Situacional, com uma análise rigorosa das vulnerabilidades e ameaças; o Quadro Estratégico, considerando as linhas de ação, alinhamento e estrutura de segurança; a Estrutura Operacional, para gerenciamento abrangente de riscos e ameaças.

Segurança Global, Integral e Integrada

Nas instalações portuárias, a segurança deve ser vista como uma segurança pública e privada única, abrangente e integrada.

Em geral, são instalações complexas com múltiplos cenários e áreas de atuação (acesso e atracação, produção, armazenamento, circulação, etc.); diversos locais e ambientes (localização urbana, situação de acesso, impacto social e econômico, etc.); demanda por capacidade de resposta (número especial de atendimentos, permanência, armazenamento, etc.); fornecimento de características especiais (tipologia, tecnologias, especializações, pesquisas, etc.); múltiplas atividades e serviços (restauração, venda comercial, terminal de passageiros, oficinas, armazéns, etc.); viajantes, trabalhadores e visitantes permanentes (transportes, diferentes níveis sociais e culturais, capacidade económica, emprego, etc.).

Meios e medidas de controle e segurança

A implementação da segurança desde o design são muito importantes e definitivas como novos desafios e requisitos e para isso são de especial relevância: a identificação, análise e avaliação de riscos, ameaças e vulnerabilidades; consideração da estrutura legal e regulamentos nacionais e internacionais, como os Códigos ISPS/ISPS; a implementação e gestão de meios e medidas de segurança para proteção perimetral e deteção de intrusão; o controle e gestão de acessos de pessoas e veículos; sistemas de inspeção e controle de acesso a objetos, mercadorias e contêineres; sistemas inteligentes de vigilância e controle por vídeo; sistemas de comunicação e proteção da informação; a organização dos serviços de vigilância e controle de patrulha; a centralização, integração e gestão de sistemas de segurança e cibersegurança, etc.

Gerenciamento abrangente de riscos e segurança

Todo o catálogo de riscos, ameaças e vulnerabilidades, e seus correspondentes meios e medidas de segurança para sua minimização, devem ser tratados sob plataformas de gestão abrangentes e integradas.

É assim que temos de integrar os diferentes tipos de segurança como: a segurança contra incêndios como protagonista potencial e real, a segurança industrial como base de garantia de funcionamento, a segurança eléctrica como base de energia contínua, a segurança em instalações especiais como áreas significativas, a segurança em emergências como proteção contra incidentes, segurança ambiental como controle de poluição, segurança contra intrusão como base contra atos ilegais ou antissociais, segurança arquitetônica e viária como parte da prevenção e proteção das atividades, segurança da informação como garantia exigida de confidencialidade.

Esta gestão de segurança integral e integrada deve estar imersa nas atividades produtivas com uma definição clara de objetivos com uma política de segurança e uma organização e procedimentos voltados para a prevenção.

Todas as atividades de segurança devem ser coordenadas sob uma direção e liderança global envolvendo todos os trabalhadores e mantendo um nível de treinamento e comunicação especializados, de acordo com esses novos desafios e demandas para obter um verdadeiro ecossistema de segurança global.

Planos de segurança, controle e contingência

A implementação de um ecossistema de segurança global exige também uma nova integração e unificação dos diferentes planos a estabelecer, tais como: o Plano Diretor de Segurança, os planos de Operador e os Planos Específicos como infra-estruturas críticas, os Planos de Autoprotecção e Emergência, os Planos de Contingência e Continuidade de Negócios.

Da mesma forma, devem ser estabelecidos e integrados nesta unificação os seguintes planos: proteção da informação, computação e redes; planos de segurança contra incêndio e explosão; planos de segurança contra atos antissociais ou ilícitos; e os correspondentes à segurança do transporte, meio ambiente e saúde ocupacional.

Direção de Segurança Global

Derivado de várias situações como: a recente pandemia, a aceleração da transformação digital, a globalização dos riscos e ameaças, a guerra na Ucrânia, as mudanças significativas na logística e transporte, etc., fizeram com que as instalações portuárias, tanto o CSO (Chief Security Officer) responsável pela segurança física da organização, bem como o CISO (Chief Information Security Officer) responsável pela segurança lógica ou cibersegurança e informação, estão motivados a desenvolver ainda mais suas carreiras porque precisam lidar com problemas transversais e globais com um horizonte mais amplo e uma visão holística.

São líderes que estão em um estágio em que seus programas estão maduros, ordenados e evoluindo, mas as Autoridades Portuárias e entidades públicas e privadas precisam de novas estratégias e liderança em questões de segurança global.

Nesse sentido, a indústria de valores mobiliários tem todas as medidas e meios para alcançá-lo sob este novo esquema de Segurança Global.

Manuel Sánchez Gómez-Merelo
Presidente · Director General de ET. Estudios Técnicos, s.a.
Director de Programas de Protección de Infraestructuras Críticas del
Instituto Universitario General Gutierrez Mellado IUGM-UNED
http://www.manuelsanchez.com

O PROFISSIONAL DE SEGURANÇA E OS DESAFIOS DOS AVANÇOS TECNOLÓGICOS

Edvaldo Almeida

O mercado da Segurança Privada traz muitos desafios para os profissionais e para as empresas desse segmento, tão castigado pelas mudanças tecnológicas, pelas legislações que não acompanham essa evolução e pela competitividade de preços, que colocam cada vez mais a qualidade em segundo plano, quando se trata de investimentos em segurança. Cada vez menos empresas investem realmente nos seus quadros de Segurança Corporativa, e incorporam o departamento nos processos decisórios.

Por outro lado, o número de profissionais capacitados para atuarem de forma estratégica dentro das organizações nesse segmento, também são em número reduzido, tornando nossa atividade mais desafiadora e carente na atuação mais incisiva dentro das empresas, sejam na área orgânica ou na prestação de serviços.

Dentre os muitos fatores que tornam o mercado mais competitivo e desafiador para o profissional de segurança, a tecnologia é um dos protagonistas nesse cenário, já que resultados na gestão dos riscos e dos planos de continuidade de negócios onde apostamos nossas fichas em nossos planos e segurança, dependem também da tecnologia, por ser essa um fator crítico de sucesso.

Nos anos noventa, com o conceito do uso de Sistemas Integrados de Segurança, onde o alicerce do nosso planejamento estava em três pilares básicos; o homem, a tecnologia e os procedimentos; iniciamos uma cultura de integração desses conceitos, utilizando de forma constante os sistemas de monitoramento e alarmes como aliados em nossos planos de segurança. No entanto, a rapidez com que as mudanças aconteciam nas tecnologias, fizeram com que equipamentos ficassem obsoletos em pouco tempo de uso. Nessa época, os desafios para a concepção dos sistemas de segurança, eram os elevados custos dos equipamentos, as mudanças e avanços desses sistemas e o uso de metodologias científicas para apresentar os fundamentos e resultados que as empresas teriam com a aceitação daquilo que estávamos propondo.

Muitas empresas, por não estarem alinhadas com essas idéias, conceberam sistemas que se transformaram em verdadeiros “Franksteins”, que é o que chamo quando não há integração entre os três pilares (Homem-Tecnologia-Procedimento), pois não adianta implantar um sistema eletrônico de segurança sem avaliar o cenário, integrar o homem a essa tecnologia e fazer com que os procedimentos contemplem de forma clara qual o papel de cada um nesse planejamento. O homem é a engrenagem mais importante desse ciclo, pois ele detém o discernimento para agir da forma mais apropriada diante dos alertas gerados pela tecnologia, cabe a ele a obrigação de saber como essas tecnologias funcionam, porque elas estão dispostas daquela forma e quais os procedimentos para utilizá-las. Inúmeros exemplos àquela época eram comuns e amplamente divulgados pela mídia. Por exemplo, reportagens demonstravam ocorrências onde os transgressores obtiveram sucesso no seu ato ilícito, porque os sistemas de CFTV estavam desativados, não estavam gravando

imagens ou até foram levados pelos meliantes, desconsiderando um planejamento de monitoramento, layout, redundância e auditoria dos sistemas.

No momento contemporâneo, vivemos uma realidade que nos permite pensar em soluções integradas de forma mais dinâmica e robusta, com resultados na prevenção, com custos-benefícios interessantes e com efetivo reduzido. Avançamos em dez anos mais do que nos cinquenta anos anteriores. Os conceitos de sistemas com analíticos, sistemas com deep learning, integração de softwares inteligentes às câmeras, combinação de tecnologias com uso de câmeras, alarmes e drones, são hoje, uma realidade presente em muitas empresas, e em crescente avanço com as Startups correndo em busca de inovações.

Hoje podemos planejar sistemas que suportem de forma otimizada o efetivo da segurança, através do uso de sistemas de monitoramento que integram os equipamentos em si, assim como, alertas inteligentes que possibilitam resultados valorosos na prevenção das ocorrências. Essas novas possibilidades que a tecnologia traz, embora necessárias, atingem os empregos na área de segurança, pois precisamos de efetivos menores, porém, mais qualificados. Portarias remotas, smart lockers, rondas com drones, cercas inteligentes e muitos outros aparatos influenciam no efetivo destinado a proteção local. Cabe ao profissional de segurança buscar cada vez mais a qualificação e interagir com essas tendências.

Com os avanços tecnológicos nos sistemas de monitoramento de imagens, um novo desafio surge concomitantemente para os profissionais de segurança, e exigem reflexão e conhecimento. O desafio do uso do reconhecimento facial por câmeras inteligentes, que geram alertas e disparam processos de acordo com a concepção do seu plano estratégico de segurança.

Hoje a China por exemplo, possui oito das dez cidades mais vigiadas do mundo, Londres vem em sexto lugar e Atlanta em décimo. Singapura vai instalar cem mil câmeras com essa tecnologia.

No Brasil, Rio de Janeiro, Bahia, São Paulo e Paraíba, tomaram a dianteira no uso dessas tecnologias. Após quatro meses de teste com algumas dezenas de câmeras instaladas em Copacabana e no Maracanã no ano de 2019, o Rio de Janeiro realizou a prisão de 63 pessoas. Dentre os presos havia gente procurada pelos mais diversos delitos, desde o não pagamento de pensão alimentícia até tráfico de drogas e homicídios.

Já na cidade de San Francisco, Estados Unidos, o uso de sistemas com reconhecimento facial foi proibido pelo governo local, a decisão afeta diretamente os órgãos públicos, que ainda poderão usar câmeras comuns e câmeras com reconhecimento de placas de veículos. As empresas privadas não foram afetadas pela decisão.

No Brasil também, o metrô de São Paulo sofreu uma ação impetrada em março de 2022, pelas Defensoria Pública do Estado de São Paulo, Defensoria Pública da União, Instituto Brasileiro de Defesa do Consumidor (Idec), Intervozes, Artigo 19 Brasil e América do Sul e do Coletivo de Advocacia em Direitos Humanos (CADHu).

Os proponentes da ação, que é a primeira do gênero no Brasil, requerem a proibição de coletar, mapear e registrar sem consentimento prévio informações sobre os rostos de seus cerca de quatro milhões de usuários diários, usando como justificativa a segurança pública. A ação defende que a proteção a dados pessoais é um direito reconhecido pela Constituição, através da recente emenda constitucional 115, e, também pela LGPD (Lei Geral de Proteção de Dados).

O Metrô de São Paulo afirmou que o seu Sistema de Monitoramento Eletrônico "não tem reconhecimento facial do cidadão ou qualquer personificação ou formação de banco de dados com informações pessoais". E que sua implantação atende aos requisitos da LGPD. De acordo com a empresa, o sistema é exclusivo para o apoio operacional e atendimento aos passageiros. "Com ele, é possível fazer a contagem de passageiros, identificação de objetos, monitoramento de crianças desacompanhadas, invasão de áreas como a via por onde passa o trem, animais perdidos, ou monitoramento de deficientes visuais pelo sistema, gerando alertas nessas situações para que os funcionários ajam rapidamente.

Já o Governo da Bahia publicou um decreto em março desse ano, que permite o uso de imagens cedidas pela sociedade, para investigar e prevenir crimes. Chamado de Projeto Câmera Interativa, a medida foi tomada para ampliar o sistema de monitoramento da Secretaria da Segurança Pública (SSP-BA). A Bahia conta com um Centro de Operações e Inteligência, desde o ano de 2016, onde as forças de segurança do estado como Polícias Militar, Civil e Técnica, Corpo de Bombeiros e efetivos federais e municipais atuam de forma integrada. Esse conceito colaborativo entre as forças pública e a sociedade privada fortalece as estratégias de segurança onde todos ganham.

Diante do cenário atual, caberá aos profissionais de segurança participar ativamente dessas discussões e atualizarem seus conhecimentos, tanto na parte de tecnologia, quanto na parte das legislações, que são essenciais para balizar nosso planejamento. Leis como a LGPD (Lei Geral de Proteção de Dados), que já é vigente no Brasil desde o ano de 2018 com efeitos legais desde agosto de 2021, são essenciais para o profissional de segurança, pois todos os dias tratamos de dados sensíveis que estão previsto nesta lei, na qual estão previstos sansões pesadas com multas que podem chegar a cinquenta milhões por evento.

Para o gestor de segurança, ao planejar os sistemas que envolvem tecnologia com o uso de imagens, biometria, armazenamento, tratamento e descarte de todas essas informações, é necessário estar atento e aliado ao Compliance da sua organização, elencar seus passos básicos para prover a conformidade do sistema. Tenha em mente os princípios básicos para se enquadrar na LGPD:

Finalidade: a realização do tratamento deve ocorrer para propósitos legítimos, específicos, explícitos e informados ao(à) titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;

Adequação: a compatibilidade do tratamento deve ocorrer conforme as finalidades informadas ao(à) titular, de acordo com o contexto do tratamento;

Necessidade: o tratamento deve se limitar à realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;

Livre acesso: é a garantia dada aos(às) titulares de consulta livre, de forma facilitada e gratuita, à forma e à duração do tratamento, bem como à integralidade de seus dados pessoais;

Qualidade dos dados: é a garantia dada aos(às) titulares de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;

Transparência: é a garantia dada aos(às) titulares de que terão informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;

Segurança: trata-se da utilização de medidas técnicas e administrativas qualificadas para proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;

Prevenção: compreende a adoção de medidas para prevenir a ocorrência de danos por causa do tratamento de dados pessoais;

Não discriminação: sustenta que o tratamento dos dados não pode ser realizado para fins discriminatórios, ilícitos ou abusivos;

Responsabilização e prestação de contas: demonstração, pelo Controlador ou pelo Operador, de todas as medidas eficazes e capazes de comprovar o cumprimento da lei e a eficácia das medidas aplicadas.

Para os profissionais do segmento da Segurança Privada no Brasil, afirmo que os conceitos básicos que trouxemos do passado, ainda são importantes. O CPTED (Crime prevention through environmental design) onde utilizamos design ambiental como aliado, o conceito do Neighborhood Watch onde buscamos a visibilidade, comunicação e interatividade, ainda são ferramentas que nos ajudam nas concepções, pois, às vezes a precipitação em investir em novidades faz com que erremos nas escolhas. Mas, no final, teremos que nos reinventar e unir todo esse “Ecosistema” que norteiam a segurança no mundo contemporâneo.

É importante saber que os temas tecnologia, legislações e estratégias são interdependentes, pois todos interagem e influenciam diretamente sobre o outro. Portanto, é interessante ao profissional de segurança mergulhar no conhecimento sobre os temas como a Lei Geral de Proteção de Dados Pessoais, Lei nº 13.709/2018, Sistema de Gestão de Compliance – ISO 19.600 de 2014 e ISO 37.301 de 2021 e Gestão de Risco ISO 31.000 de 2018.

Ed Almeida
Profissional de Segurança Privada
edvaldoalmeidar@gmail.com
Linkedin: Edvaldo Almeida
Youtube: Vamos Falar de Segurança

REFERÊNCIAS

Website Mobile Time - Polícia do Rio prende 63 pessoas com tecnologia de reconhecimento facial em quatro meses
https://www.mobiletime.com.br/noticias/06/11/2019/policia-do-rio-prende-63-pessoas-com-tecnologia-de-reconhecimento-facial-em-quatro-meses/

Globo.com – G1 San Francisco proíbe o uso do Reconhecimento Facial
https://g1.globo.com/pop-arte/noticia/2019/05/16/san-francisco-proibe-a-policia-de-usar-reconhecimento-facial.ghtml

Website Tecnoblog - São Francisco proíbe uso de reconhecimento facial pelo governo

https://tecnoblog.net/noticias/2019/05/15/sao-francisco-proibe-reconhecimento-facial/
Website UOL – Metrô de São Paulo é alvo de ação inédita que pede o fim do reconhecimento facial
https://noticias.uol.com.br/colunas/leonardo-sakamoto/2022/03/03/metro-de-sp-e-alvo-de-acao-inedita-que-pede-fim-do-reconhecimento-facial.htm
Governo Federal – Lei Geral de Proteção de Dados
https://www.gov.br/cidadania/pt-br/acesso-a-informacao/lgpd

ISO - International Organization for Standardization – Gestão de Riscos
https://www.iso.org/search.html?q=iso%2031000

ISO - International Organization for Standardization - Compliance
https://www.iso.org/search.html?q=iso%2037301&hPP=10&idx=all_en&p=0

ISO - International Organization for Standardization - Compliance
https://www.iso.org/search.html?q=iso%2019600&hPP=10&idx=all_en&p=0

FORMAÇÃO DO PROFISSIONAL VIGILANTE NA SEGURANÇA PRIVADA – DE QUEM É A RESPONSABILIDADE?

Prof. Dr. Antônio A. Mota, CPSI

Atuando como gestor na atividade de segurança privada e empresarial há 31 anos, e como instrutor credenciado na Polícia Federal (PF) para ministrar aulas nos cursos de segurança privada desde 1998, venho acompanhando a evolução do seguimento, sendo que esta atividade no Brasil surgiu para atender aos estabelecimentos financeiros (bancos) através dos Decretos Federais nº 1.034/69 e nº 1.103/70, e consequentemente atender a outras instituições e empresas públicas e privadas. Na sequência, a atividade de segurança privada foi regulamentada através da Lei 7.102/83 de 20 de junho de 1983. Com a evolução da atividade de segurança privada, uma das preocupações e atenções foi com a formação dos vigilantes, pois o mercado está cada vez mais exigente e os contratantes e usuários dos serviços de segurança privada necessitam que os vigilantes estejam com seus níveis de preparo em conformidade com as necessidades atuais.

No início, a formação dos vigilantes em segurança privada era muito escassa, não havia literatura abrangente e a formação era baseada na experiência empírica dos instrutores e em fundamentos militares. Lembro que a primeira carga horária para formar os vigilantes foi de 120 h/a, em 2006 tivemos uma alteração para 160 h/a, e em 2012 tivemos a última mudança para 200 h/a com um total de 15 disciplinas. O curso de formação de vigilantes e suas extensões têm validade de 02 (dois) anos, após homologação na Delegacia de Controle de Segurança Privada (DELESP), sendo necessário os vigilantes retornarem às salas de aulas a cada 02 (dois) anos, o que requer que os instrutores também se atualizem, renovem seus conhecimentos e aperfeiçoem suas metodologias de ensino.

Sendo imprescindível a melhoria contínua na formação dos vigilantes na segurança privada, faço a seguinte pergunta: de quem é a responsabilidade pela formação do profissional vigilante? Visando uma formação eficiente, eficaz, qualificada e com um preparo de alto nível, além de habilitados pelo órgão regulador, respondo que a responsabilidade é compartilhada entre a PF, as Escolas de Formação e os Instrutores.

- **Polícia Federal através da Coordenação-Geral de Controle de Serviços e Produtos (CGCSP) –** compete a CGCSP elaborar, revisar e atualizar as disciplinas, os conteúdos programáticos das aulas, a regulamentação e a fiscalização.
- **Escolas de Formação de Vigilantes –** cabe aos administradores e os coordenadores de Cursos de Formação de Vigilantes (CFV), cumprir os regulatórios, selecionar bem seus instrutores com base em critérios específicos, com os perfis e habilitações para cada disciplina.
- **Instrutores Credenciados –** já aos instrutores, precisa se capacitarem e se manterem atualizados visando preparar melhor os vigilantes nos cursos de formação, extensões e reciclagens. Vejo que cada instrutor deve ter 03 (três) objetivos básicos como formador - Ensinar, Orientar e Motivar, enquanto docentes.

- A Associação Brasileira de Cursos de Formação e Aperfeiçoamento de Vigilantes (ABCFAV), vem contribuindo para melhorar a capacitação dos instrutores e a formação dos vigilantes, tendo como foco preparar e capacitar os profissionais para atender o mercado de trabalho.

- Procurando entender como se encontra a formação e capacitação dos instrutores, bem como de que forma as escolas estão contratando seus instrutores, vejo que existe um grande efetivo de instrutores credenciados nas mais diversas disciplinas. Identifiquei ainda que pessoas foram credenciados e nunca ministraram uma aula, seja por falta de oportunidade ou pelas escolas já terem instrutores suficientes para atenderem às suas demandas. Existem ainda funcionários de escolas de CFV e consultores cobrando para realizarem o credenciamento de instrutores, mesmo não havendo vagas disponibilizadas nas escolas de CFV. Na minha análise, entendo que os credenciamentos de instrutores deveriam ser apenas realizados pelas escolas de formação de vigilantes após serem aprovados em processo seletivo, comprovarem suas qualificações e atenderem aos requisitos exigidos pela legislação.

- Apresento a seguir, um levantamento geral por estado sobre as quantidades de escolas de formação de vigilantes e as quantidades de instrutores credenciados:

ESTADO	ESCOLAS - CFV AUTORIZADAS			INSTRUTORES CREDENCIADOS POR ESTADO
	MATRIZ	FILIAL	TOTAL	
AC	3	0	3	60
AL	4	0	4	74
AP	3	0	3	104
AM	3	1	4	175
BA	18	2	20	464
CE	9	0	9	260
DF	8	0	8	462
ES	3	0	3	174
GO	8	1	9	304
MA	6	2	8	182
MT	4	0	4	81
MS	3	1	4	105
MG	13	14	27	1.003
PA	10	5	15	346
PB	4	3	7	157
PR	12	1	13	488
PE	9	1	10	211
PI	4	0	4	125
RJ	22	13	35	532
RN	2	1	3	142
RS	21	2	23	690
RO	2	1	3	96
RR	1	0	1	35
SC	7	6	13	402
SP	48	11	59	1.883
SE	3	0	3	92
TO	1	0	1	28
TOTAL GERAL	**231**	**65**	**296**	**8.675**

Fonte: Polícia Federal

Analisando o quadro acima, observa-se que existe uma quantidade expressiva de instrutores credenciados na PF para ministrar aulas nos cursos de formação de vigilantes, porém, observando as quantidades de escolas devidamente autorizadas a funcionar por estado, são muitos os instrutores credenciados, mas que não existe demanda para todos. Observa-se ainda que pela grande quantidade de instrutores credenciados, as escolas de formação de vigilantes têm a seu favor várias opções para selecionar melhor seu corpo de instrutores.

A origem dos instrutores nos cursos de segurança privada, são militares das forças armadas na reserva, policiais militares, civis e penais, bombeiros militares e civis, guardas municipais, profissionais com cursos superiores para atender as disciplinas especificas que são obrigatórias pela legislação para o credenciamento, gestores e consultores de segurança com experiência comprovada, e profissionais que atuam na atividade de segurança privada. Um dos fatores que contribuiu para o aumento do credenciamento de Instrutores na PF, foram os cursos de graduação tecnóloga, pós-graduação e especializações nos cursos de segurança promovidos por faculdades e universidades. Quanto a contratação de instrutores nas Escolas de Formação, a maioria são autônomos, exercem suas atividades nas suas organizações e empresas, e ministram aulas conforme suas disponibilidades de horários.

A CGCSP e a ABCFAV estão com uma excelente parceria e alinhadas na promoção de eventos e cursos para aprimorar a formação e capacitação dos instrutores e consequentemente dos vigilantes. Destaco como ações positivas a ABCFAV, que promoveu o curso – Gestão da Diversidade em parceria com a Universidade Zumbi dos Palmares, e a PF, que lançou recentemente, através da plataforma ANP Cidadã, o Curso de Didática para Instrutores de Formação de Vigilantes - 2022.x1. visando a elevar o nível da qualidade do ensino oferecido pelas Escolas de Formação e Vigilantes.

Diante das ações promovidas pelas entidades supracitadas, cabe aos instrutores buscarem as suas atualizações de conhecimentos, pois, como formadores, todos têm a missão de repassarem aos alunos e vigilantes seus conhecimentos e suas experiências adquiridas, visando à formação de profissionais qualificados e aptos a exercerem a profissão com eficiência e eficácia, o que é fundamental para elevar o nível da segurança privada.

Na qualidade de instrutores credenciados na PF, que cada um possa cumprir o seu papel de ensinar, orientar e motivar. Dessa forma, os alunos e os profissionais de segurança privada poderão se qualificar melhor e se motivarem para elevar a qualidade de suas atividades.

Antônio A. Mota, CPSI
Doutor em Filosofia em Ciências de Segurança Internacional, Ph.D. Membro do Grupo de Excelência em Defesa e Segurança – CRA – CE
Sócio honorário da CEAS Internacional nº 12/Sócio na ABSEG nº 570
Contatos: Cel. 85 99145-7777 | e-mail: aa.mota@motaassociados.com.br

RELAÇÕES HUMANAS EM SEGURANÇA

Dr. Renato Figueiredo, CPSI,CIGR,CISI,CIEIE,CEGRC,CIEAC,MBS,DIDS

As Relações Humanas constituem o pilar fundamental sobre o qual se deve basear a gestão profissional da segurança. A prática correta das relações interpessoais é fator gerador de paz, bem-estar e tranquilidade. Bom tratamento, respeito, consideração e valorização das pessoas são as melhores referências para um atendimento eficaz e de qualidade. A Segurança Privada não pode ser abstraída dos princípios que regulam a convivência harmoniosa e equilibrada, pois seu fundamento de existência é o serviço, a assistência e a ajuda ao próximo. Consequentemente, o exercício de boas Relações Humanas é uma estratégia preponderante nas operações rotineiras de segurança.

Generalidades

O desempenho trabalhista do profissional de segurança, demanda de um alto sentido de responsabilidade e critério de atuação. Em grande parte de seu esquema operativo, os serviços de segurança baseiam-se nas relações entre o pessoal de agentes, supervisores, protetores, chefes e gerentes de segurança e os usuários do sistema, denominados: clientes, visitantes, vendedores, fornecedores, funcionários, motoristas, colegas de trabalho, etc., todos esses atores demandam de um trato respeitoso, prudente e agradável.

Nessa nova forma de convivência humana, pesa muito a capacidade que o profissional de segurança tem de interagir com as pessoas, pois dependerá de sua conduta, comportamento e tratamento que prestarem, do nível de tranquilidade e confiança que geram no ambiente em que o momento de prestar o serviço de proteção. Lembremos que as Relações Humanas em segurança devem ser pautadas no RESPEITO; O tratamento respeitoso gera CONFIANÇA; E a confiança leva à LEALDADE.

O sucesso profissional e pessoal dependerá em grande parte das excelentes e cordiais relações que o profissional de segurança estabelece com as pessoas com quem interage no dia a dia do seu local de trabalho. Por isso, é importante que todo profissional de segurança esteja preparado para gerenciar as relações humanas com inteligência, responsabilidade e sabedoria.

Relações Humanas em Segurança

A principal virtude de um Profissional de Segurança em seu relacionamento com os outros é o equilíbrio emocional; sua tranquilidade gera segurança quando tem o dom de transmiti-la. A grandeza reside na ousadia de interagir e caracterizar a relação, graças à sua atitude mental e processo de amadurecimento interno, bem como à sua capacidade de conhecer e conviver com os outros.

Um profissional de segurança não pode reagir sem refletir, ele precisa rever, em cada ação, as estratégias disponíveis e caminhos de saída, e tomar decisões

ponderadas e analisadas, sempre considerando as consequências que podem derivar de decisões precipitadas ou erradas.

Fatores que favorecem as Relações Humanas em Segurança

O respeito

O respeito é a essência das Relações Humanas na vida comunitária, no trabalho em equipe e em qualquer tipo de relacionamento interpessoal. É aceitar e compreender os outros como eles são, tratando-os com bondade e cortesia. O respeito deve ser a REGRA DE CONDUTA para todos os profissionais de segurança.

O respeito cria um ambiente de cordialidade e segurança; permite a aceitação das limitações dos outros e o reconhecimento das virtudes dos demais. Evita ofensas e ironias; não permite que a violência se torne o meio para impor critérios. O respeito conhece a individualidade de cada ser humano e aceita, satisfeito, o direito de ser diferente. Todo relacionamento humano está enraizado no respeito.

A Cortesia

A cortesia como importante ferramenta nas Relações Humanas auxilia na eficácia da comunicação e consequentemente no relacionamento dos indivíduos, melhorando assim sua qualidade de vida. A atitude cortês é um testemunho de consideração, respeito e apreço pelo outro, isso não significa estar em situação de inferioridade. Ser cortês cria um ambiente mais amigável e calmo no qual as pessoas podem realizar suas atividades com segurança e confiança.

O Profissional de Segurança deve ser uma pessoa cortês e respeitosa, buscar tratamento amável e gentil com as pessoas que dirige, com seus amigos, clientes, colegas de trabalho, etc. Um relacionamento cortês gera um ambiente saudável, agradável, calmo e seguro, onde as pessoas podem realizar suas atividades de vida com muita confiança.

O comportamento

Para ter sucesso no trabalho e ter um bom prestígio e imagem como Profissional de Segurança, é vital controlar nossas emoções, a gestão inteligente da IRA e nosso autocontrole. Embora existam muitas razões pelas quais as pessoas ficam com raiva e chateadas, devemos ter em mente que a raiva é o resultado de nossa percepção de uma situação que nos causa perturbação.

Diante de uma circunstância ou evento infeliz, o profissional de segurança deve decidir como reagir; agir impulsivamente e gritar não é um comportamento profissional. O que se deve fazer é esforçar-se de maneira consciente para controlar-se a si mesmo e permanecer tranquilo. Lembremos que em nossas tarefas diárias de proteção e controle, muitas vezes somos submetidos a pressões, situações de risco, violência e crise, portanto, como Profissionais de

Segurança, devemos nos comportar de acordo com nossas funções, prestígio e altura.

Problemas Humanos em Segurança

A profissão de segurança é uma das mais complexas que existem, pois na maioria das vezes, os recursos humanos são o mecanismo fundamental de sua existência e funcionamento. O principal recurso que todo, coordenador, diretor ou gerente de segurança deve gerenciar é o humano. Trabalhar com seres humanos, por natureza, gera conflitos, interesses particulares e necessidades individuais e coletivas. Ainda mais na área de segurança onde a eficiência, operacionalidade e qualidade do serviço dependem do fator humano.

Os sistemas e estruturas de segurança modernos exigem profissionais comprometidos fielmente com os objetivos organizacionais; indivíduos proativos e dinâmicos, altamente motivados no seu desempenho profissional. Pois a essência do serviço que está na base da operação de segurança requer a cooperação de colaboradores com atitude positiva, comportamento adequado, vontade inflexível e a predisposição necessária para desempenhar com eficiência suas tarefas de proteção e vigilância.

As Relações Humanas se constituem no pilar fundamental sobre o qual deve sustentar-se a gestão profissional de segurança. Uma correta prática das relações interpessoais é um fator gerador de paz, bem estar e tranquilidade. O bom trato, o respeito, a consideração e a valorização às pessoas são as melhores referencias de um serviço efetivo e de qualidade. A segurança privada não pode abstraísse dos princípios que normalizam a convivência harmônica e equilibrada, pois seu fundamento de existência é o serviço, a assistência e a ajuda ao próximo. Em consequência, o exercício das boas relações humanas resulta uma estratégica preponderante nas operações de rotina de segurança.

Renato Figueiredo, CPSI,CIGR,CISI,CIEIE,CEGRC,CIEAC,CIPSI,MBS,DIDS

Presidente CEAS-BRASIL e Secretário Geral CEAS-INTERNACIONAL

Bibliografia:

- Manual de Estudos “Desenvolvimento Humano do Profissional de Segurança. Ing. Seg. Marco Heredia R.

- Manual de Estudos “Gestão do Desenvolvimento Humano do Profissional de Segurança”. Prof. Dr. Nino Meireles

Rumo a uma nova percepção de segurança e proteção. Desafios e oportunidades

Manuel Sánchez Gómez-Merelo

Consultor de Segurança Internacional

A percepção de insegurança é o alarme que é causado em nosso cérebro e nos mantém vivos, mas a diferença entre se sentir seguro e estar realmente seguro tem a ver com saber quais são as novas ameaças que enfrentamos agora e quais possibilidades realmente temos que evitar para não viver permanentemente com medo.

Sentir-se seguro refere-se a uma percepção, a uma experiência, que pode ou não ser ajustada à realidade e o sentimento de segurança depende sobretudo de termos uma percepção de controle do momento.

Para isso, entender o que está acontecendo é especialmente importante, pois as notícias sensacionalistas, informações tendenciosas e até mesmo contraditórias geram alarmes sociais e causam tantos danos à população, pois aumentam seu sentimento de insegurança e descontrole.

Por outro lado, o modo como cada um enfrenta as adversidades diz muito sobre nós mesmos e, mais do que as circunstâncias, é o que faz a diferença em ver a tragédia ou a oportunidade.

A segurança é uma experiência subjetiva e intrínseca de cada pessoa e, levando em consideração essa definição, é razoável pensar que o sentimento ou a real segurança muda dependendo das circunstâncias.

Devemos prevenir, tomar as medidas necessárias e controlar, dentro de nossas possibilidades, o meio ambiente para nos protegermos.

Agora, os riscos colocados pela pandemia são reais, COVID-19, apesar de sua baixa taxa de mortalidade, é uma ameaça à saúde pública devido ao seu alto índice de mutação e contágio, então vamos lembrar que o medo bem educado é que ele chama de prudência e é uma excelente virtude.

Passado ... análise e realidade

No passado recente, mais do que o conceito de segurança, o que mudou foram as circunstâncias e, de fato, nos deparamos com uma situação em que teremos que analisar e reavaliar continuamente o que é seguro e o que não deve ser protegido como prioridade, nossa saúde em sentido amplo para entender que devemos não apenas nos proteger da infecção, mas também da ansiedade, da depressão que pode ser produzida por um excesso de proteção em nosso dia a dia.

A recente pandemia é uma oportunidade para examinar o estilo de vida que levamos em nossos negócios, trabalho e atividades sociais.

Assim, simplesmente aplicando o bom senso e tendo em conta que vivemos períodos muito incertos em que não devemos deixar de analisar o passado, não devemos assumir o que é seguro e o que não é, devemos analisar cada situação de acordo com as circunstâncias, o momento e o contexto.

Vamos tentar construir um senso de segurança sentindo que temos um certo grau de influência, controle e poder sobre o que pode nos afetar.

Apresentar… imagem complicada

COVID-19 virou nossa sociedade global de cabeça para baixo e mudou nossa percepção de segurança. Coisas que antes eram tão normais e tão "seguras", como participar de reuniões, eventos sociais ou mesmo reuniões familiares, tornaram-se difíceis para nós.

Mas, uma qualidade maravilhosa do ser humano é a nossa capacidade de adaptação e agora, devemos aprender a mudar muitas coisas e nos adaptar a novas circunstâncias, sejam temporárias ou vieram para ficar.

Temos que assumir que, embora haja coisas que não devemos ou podemos fazer, existem outras que seguem perfeitamente as medidas de prevenção ou proteção, principalmente as indicadas pelas autoridades sanitárias.

Os confinamentos tiveram um efeito aparentemente negativo na saúde das pessoas, mas fizeram com que muitas pessoas parassem e se conscientizassem de muitas coisas e de que a saúde está em primeiro lugar: a saúde.

Existem muitas medidas de prevenção e proteção que dependem fortemente de nós, embora as vulnerabilidades sejam um problema muito sério.

No entanto, o nível de demanda e segurança das organizações clientes públicas e privadas estão aumentando. A pandemia impulsionou a digitalização, mas também transformou a maneira como nos comunicamos e interagimos.

Portanto, agora é imprescindível antecipar-se às demandas e novas necessidades dos cidadãos, entidades públicas e privadas para analisar os novos desafios e requisitos que levam a cabo uma nova estratégia de segurança.

Não vale mais ser reativo, esperar que chegue à demanda por novos títulos, é preciso monitorar e analisar para avançar, propor atualizações e recomendações, até mesmo mudanças de paradigma.

Para isso, devemos promover e acelerar o processo da necessária colaboração público-privada, que tantos benefícios pode trazer aos cidadãos e à sua segurança.

Futuro… desafios e oportunidades

Proporcionar ao cidadão novas soluções é um verdadeiro desafio. O bom é que temos ferramentas ao alcance para conseguir isso, além de novas tecnologias como Internet das Coisas, Inteligência Artificial, Plataformas de Treinamento Online, Sistemas de Acompanhamento, Monitoramento e Controle, etc.

Proatividade e customização são as chaves da nova estratégia de segurança e seus principais desafios se concentram em: Capacidade de integração e implantação de soluções operacionais especializadas; Projetos de segurança abrangentes para minimizar vulnerabilidades físicas e lógicas; gestão de risco abrangente; Exploração e gestão de dados para otimizar processos críticos; Implantação de redes de comunicação robustas, inteligentes e seguras; Melhorar a resiliência, especialmente em segurança cibernética; Integrar informações para garantir eficiência operacional; Construir melhores serviços aprimorando a inteligência por meio da informação; Personalização do gerenciamento de vídeo inteligente.

Temos que desenvolver projetos de integração que vão desde a análise atual das diferentes atividades, até a nova abordagem da infraestrutura tecnológica e as soluções operacionais que permitem a gestão e exploração adequada de ações futuras devido à evolução estratégica, tecnológica, operacional, etc.

Esta nova proposta será a segurança global, física e lógica e cibersegurança para cada infraestrutura ou organização, dos seus processos para garantir a continuidade da atividade ou negócio.

Igualmente importante é a convergência de regulamentos e novas abordagens para a segurança desde o projeto.

Uma nova proposta de convergência e análise de ideias em colaboração para: Encontrar o ponto de equilíbrio das ações; o complexo desafio da transformação digital; treinamento especializado para novos profissionais; prioridades de segurança no teletrabalho; a revisão dos planos de segurança e emergência, etc.

Em suma, a análise e abordagem para a convergência dos valores mobiliários e suas entidades, para um novo Plano Integrado e Integrado de Segurança.

Com tudo isso, aprenderemos a confiar, a nos sentir seguros e protegidos, mesmo que haja circunstâncias que estejam além do nosso controle. Vamos aprender a gerenciar a incerteza.

Manuel Sánchez Gómez-Merelo
Presidente · Director General de ET. Estudios Técnicos, s.a.
Director de Programas de Protección de Infraestructuras Críticas del
Instituto Universitario General Gutierrez Mellado IUGM-UNED
http://www.manuelsanchez.com

Artigo Plano de Resposta Emergências - PRE: O que é e como fazer

Sandra Alves Bispo, CPSI, CISI

O Plano de Resposta a Emergências - PRE visa estabelecer procedimentos para fornecer resposta imediata e efetiva a um incidente.

O PRE contém um conjunto de procedimentos, orientações e informações para direcionar respostas imediatas e efetivas às emergências com o propósito de minimizar danos ou prejuízos aos funcionários, contratados, ao público, à propriedade e seus equipamentos, e ao meio ambiente.

Segundo a ISO 22301, o incidente está definido como “situação que pode representar ou levar à interrupção de negócios, perdas, emergências ou crises”.

Dentro dessa premissa, a ISO 22301 apresenta o conceito do Sistema de Gestão de Continuidade de Negócios - SGCN, o qual abrange o Plano de Resposta a Emergências - PRE, o Plano de Gerenciamento de Crises - PGC, o Plano de Continuidade de Negócios - PCN e o Plano de Recuperação de Desastre - PRD. Esses planos mitigam uma interrupção gradual ou súbita e por esse motivo precisam estar integrados.

Abaixo, apresentamos uma imagem ilustrativa com uma visão holística da necessidade da integração dos planos.

Visão holística - Integração dos planos

Neste artigo, vamos abordar especificamente o Plano de Resposta a Emergências - PRE.

O objetivo e escopo de cada PRE deve ser definido, acordado com a alta direção e entendido pelas pessoas que irão realizar o plano. Qualquer relação com outros planos ou documentos relevantes que existam na organização deve ser

claramente especificada e o método de obtenção desses documentos deve ser descrito.

Devem ser identificados e providenciados todos os recursos de resposta, incluindo os sistemas e equipamentos de emergência, empresas contratadas prestadoras de serviços de apoio na resposta a emergência. O dimensionamento dos recursos de resposta deve ser adequado aos cenários de riscos identificados a partir do estudo de Análise e Avaliação de Riscos.

O processo de elaboração do Plano de Resposta a Emergências - PRE contém seis fases. Abaixo, framework com os principais elementos.

Framework para elaboração do PRE

1. Comunicação e Consulta

A comunicação e consulta é a forma de estabelecer o processo e a estratégia de comunicação com as partes interessadas. Esta fase permeia todo o processo de elaboração do Plano de Resposta a Emergências - PRE, considerando por exemplo, a elaboração do PRE, campanhas de sensibilização e treinamentos.

2. Contexto Estratégico

Ao estabelecer o contexto, a empresa articula seus objetivos e define os parâmetros externos e internos a serem levados em consideração na confecção do Plano de Resposta a Emergências - PRE e estabelece o escopo e os critérios para o restante do processo.

Nessa etapa é importante:

- Entender os Objetivos Estratégicos e as Estratégias
  - Qual a missão, visão e valores da empresa?
  - Quais são os serviços e/ ou atividades essenciais da empresa?

- Qual é o público-alvo (foco)?
- Quais são as oportunidades e ameaças que existem no ambiente da empresa?
- Quais as forças e fraquezas da empresa?
- Quais são os objetivos estratégicos da empresa?
- Quais são as iniciativas estratégicas necessárias para atingir os objetivos?

- Entender a Análise e Avaliação de Riscos
  - Entendimento e análise do mapa de riscos, os quais serão utilizados como base para a construção dos cenários de riscos.

Exemplo - Matriz de riscos - Software INTERISK

3. Construir Cenários de Riscos

Para a elaboração do Plano de Resposta a Emergência - PRE, é necessário que se construam Cenários de Riscos.

A construção dos Cenários de Riscos deve ter como referência a Matriz de Riscos da empresa e o *brainstorming* com uma equipe multidisciplinar das áreas que influenciam o contexto do objeto de estudo.

Na construção dos Cenários de Riscos, avalia-se o contexto interno e externo no qual a empresa está inserida. Os cenários serão mensurados considerando-se impactos moderados, severos e massivos. O objetivo da mensuração é permitir que as estratégias estabelecidas nos protocolos considerem esses impactos para que a empresa possa preparar-se.

Cenário	Modelo
Nº 3 - Manifestação com Potencial de Violência contra Propriedade e Funcionários	Canvas

Criticidade Cenário	
Moderado	Manifestação da comunidade local ou ONGs, na porta da empresa, com faixas e cartazes, sem impedir ou restringir o acesso de pessoas e veículos. Os manifestantes fazem alerta sobre condições ambientais e sociais consideradas inadequadas, querendo que a empresa tome conhecimento e providências
Severo	Manifestação da comunidade local, ONGs ou grupos organizados na porta da empresa, com faixas e cartazes, com impedimento e restrição de acesso à empresa de pessoas e veículos. A empresa não sofre descontinuidade das operações e tarefas críticas em função equipes operacionais terem que dobrar seu turno de trabalho. Os manifestantes querem que a empresa resolva os problemas ambientais e sociais consideradas inadequadas
Massivo	Manifestação da comunidade local, ONGs ou grupos organizados na porta da empresa com faixas e cartazes, com impedimento e restrição de acesso à empresa e de pessoas e veículos. A empresa sofre descontinuidade das operações e tarefas críticas, ocorrendo inclusive a expulsão da equipe que lá se encontrava. Os manifestantes só aceitam sair da empresa quando resolver os problemas das reinvindicações

Conceito

Conceito:

- Caracterizada como Manifestação com Violência, com agressão direta a empresa e pessoas, com o uso de inflamáveis, armas de fogo, armas brancas e vandalismo.
- Caracterizada como Manifestação Pacífica, com uso de cartazes, placas, bloqueios parciais ou totais de acesso e palavras contra a empresa.

Política Diretriz

De forma a mitigar o impacto do risco, as diretrizes são:

- Monitorar mobilizações ou movimentos através de redes sociais, portais de notícias, blogs, entre outros, permitindo uma visão antecipatória e prospectiva dos fatos, favorecendo a rápida tomada de decisão e efetividade das ações.
- A empresa não reage durante manifestações, deixando que a Segurança Pública controle a situação.
- Em caso de manifestação confirmada, enviar ofício solicitando auxílio da Segurança Pública, para que esteja presente no início da ocorrência. Alertar a equipe interna e colaboradores (conforme protocolo) sobre o evento.
- Permitir a manifestação pacífica - livre circulação externa, desde que não comprometa o acesso e ocorra invasão.

Probabilidade	Impacto	Evento Crítico (Cenário)
Alta	Severo	

Exemplo - Cenário de risco - Software INTERISK

4. Construir uma Estrutura Corporativa de Emergência e Crise

Estabelece a estrutura organizacional e o fluxo de ativação do Plano de Resposta a Emergência - PRE para assegurar resposta rápida e sistemática a situações de cenário de risco.

O acionamento de cada equipe depende do nível de criticidade do incidente.

A estrutura de gestão de crises pode ser composta, por exemplo, por três níveis de gerenciamento.

- Comitê Corporativo de Gestão de Crise: Atua em nome do e se reporta ao Presidente (ou pessoa designada por ele). É responsável por gerenciar todos os eventos de crise corporativa, os quais afetam ou têm o potencial de afetar a empresa em sua totalidade.

- Comitê Local de Gestão de Crise: O CLGC administra crises locais e supervisiona a resposta a emergências.

- Equipe de Resposta a Emergência: A ERE oferece recursos de resposta imediata e local a qualquer emergência que possa ocorrer no nível local, como princípios de incêndios, inundações e acidentes de trabalho.

Exemplo - Abrangência da estrutura de gestão de crise

5. Elaborar Protocolo de Resposta a Emergência - Base em Cenários de Riscos

Estabelece os Protocolos de Resposta a Emergência para tratamento da ocorrência do incidente, ou seja, para o cenário de risco em estudo. Cabe destacar que para cada Cenário de Risco deve ser elaborado um Protocolo de Resposta a Emergência.

No exemplo abaixo, temos um Protocolo de Resposta a Emergência escrito no Modelo Canvas, o qual tem como objetivo estruturar resposta efetivas, trazendo praticidade e dinamicidade à análise das ações.

Cenário			
Nº 3 - Manifestação com Potencial de Violência contra Propriedade e Funcionários			
Consequências			
Imagem	**Financeiro**	**Legal / Regulatório / Social / Ambiental**	**Operacional**
Projeção negativa na imprensa e redes sociais	Prejuízos decorrentes de paralização parcial ou total da empresa	Fiscalização de órgãos reguladores, principalmente ligada à sustentabilidade	Paralização da produção parcial ou total
Reflexo nos produtos da marca, com postagens contrárias aos produtos da empresa.	Custos de estrutura, operação, pessoas, jurídico, por exemplo	Possíveis perdas de licenças junto à órgãos ambientais	Danos a equipamentos e materiais utilizados na produção
		Possíveis ações judiciais reparatórias do meio ambiente	Possível impacto psicológico de colaboradores e até mesmo perda de colaboradores

Ações Operacionais

Equipe de Resposta a Emergência - ERE

Supervisor de Segurança

- Monitorar a mídia local sobre o ato de manifestação;
- Alertar o Líder de Segurança/equipe, caso os manifestantes ameacem a segurança do empreendimento;
- Orientar o Líder de Segurança acerca de medidas adicionais necessárias;
- Acionar a central de monitoramento;
- Acionar a Equipe de Manutenção – se necessário;
- Acionar bombeiro civil/brigada combate a incêndio interna, em caso de manifestação com uso de inflamáveis;
- Reportar informações sobre a ocorrência para o Gerente de Segurança;
- Após o término da ocorrência, acionar Equipe de Serviços Gerais (limpeza nos locais afetados).

Líder de Segurança

- Avaliar a necessidade de reforço da equipe de segurança e reportar a situação para o Supervisor de Segurança;
- Providenciar aumento do efetivo e posicionar a equipe de segurança em locais críticos (entrada e saída de veículos, catracas / controle de acesso, perímetro, doca e áreas. Inflamáveis);
- Bloquear os acessos, impedindo a entrada e saída de quaisquer pessoas – escadas, elevadores, acesso ao lobby e estacionamento, visando garantir segurança pessoal e informa o supervisor.

Central de Monitoramento

- Acionar órgãos de Segurança Pública (Polícia Militar e Polícia Civil), mediante a determinação do gerente de segurança;
- Monitorar através do sistema de registro de imagens (CFTV) a evolução da manifestação;
- Manter informada a equipe em campo, principalmente o Supervisor/ Líder de Segurança atualizado sobre a situação, dados do monitoramento e qualquer mudança do cenário, destacando os locais de maior concentração de pessoas, número de manifestantes, características físicas dos mais exaltados, etc.;
- Resgatar imagens (gravação) para análise da ocorrência pelo gerente de segurança.

Vigilantes

- Posicionar-se em locais críticos conforme orientação do Líder de Segurança;

Recursos Operacionais

- Estrutura de segurança (mão de obra e sistemas de segurança).
- Sala de crise interna.
- Sala de crise externa.
- Assessoria ambiental.

Parcerias

- Empresa de Segurança.
- Hospitais.
- Ambulância.
- Corpo de Bombeiro.
- Polícia Militar.
- Polícia Civil.
- Seguro.
- Sindicato dos Trabalhadores.
- Imprensa.

Recursos Financeiros

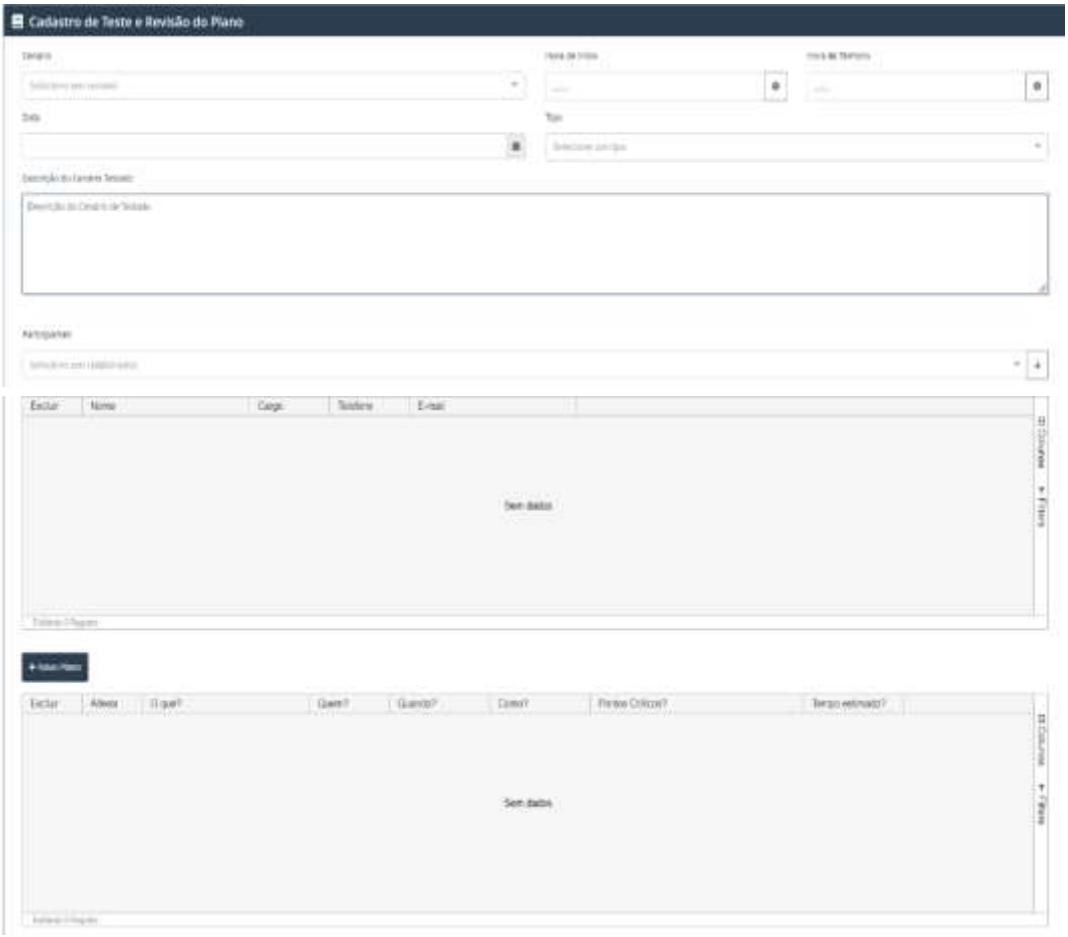
- Custos devido aos danos causados pela manifestação, por exemplo, estrutura, operação, pessoas, jurídico.

Probabilidade	Impacto	Evento Crítico (Cenário)
Alta	Severo	

Exemplo - Protocolo de Resposta a Emergência - Modelo Canvas - Software INTERISK

6. Realizar Testes e Revisão do PRE - Monitoramento e Análise Crítica

O simulado - teste de mesa tem como objetivo validar o nível de aderência das medidas, através de cenários progressivos, de tal forma que a Estrutura Corporativa de Emergência e Crise responda, de forma integrada, ao Protocolo de Resposta a Emergência



Exemplo - Formulário Teste de Mesa - Software INTERISK

Cabe ressaltar que todo e qualquer tipo de empresa deve dispor de um Plano de Resposta Emergências - PRE, inclusive integrado ao Sistema de Gestão de Continuidade de Negócios.

Não ter este plano estruturado significa que a empresa não tem planejamento, não tem pessoas treinadas para emergências e não tem estrutura pronta para esse tipo de atendimento.

Vale destacar que a elaboração de um Plano de Resposta a Emergências requer o envolvimento de uma equipe multidisciplinar, conhecimento dos processos existentes e a aplicação de ferramentas para a correta construção de cenários, para que a organização tenha protocolos efetivos de resposta a emergência.

Solicite uma demonstração do Software INTERISK - Módulo GCN para visualizar na prática a elaboração do Plano de Resposta a Emergências.

Sandra Alves Bispo, CPSI, CPSI
Diretora de Relacionamento da Brasiliano INTERISK

COMPLIANCE TRIBUTÁRIO

Flavio Fleury de Souza Lima, CIEAC, CISI, CIGR

A adequação da gestão das empresas às regras de *compliance* talvez seja um dos temas mais importantes para o setor corporativo atualmente, tanto em relação às questões regulatórias, financeiras e penais, como no âmbito fiscal e tributário.

Vindo do verbo em inglês *to comply*, o termo *compliance* deve ser traduzido como “agir de acordo com as regras”. O *compliance* tributário está ligado ao cumprimento e à conformidade com os regulamentos, normas e diretrizes que se referem à tributação incidente sobre o seu negócio. Portanto, podemos definir o *compliance* tributário como os serviços de regulamentação e conformidade das empresas com o Fisco.

Trata-se, então, do conjunto de medidas adotadas para garantir a conformidade dos procedimentos fiscais, não só com o pagamento de tributos, mas, também, com a apuração e a disponibilização de forma correta da documentação que deve ser entregue ao Fisco.

Dessa forma, para atender ao dever de estar em concordância com as regras tributárias, o *compliance* tributário atua como uma vistoria cuidadosa das informações fiscais que a própria empresa realiza para detectar erros ou incoerências, além de evitar multas que poderiam ser geradas por esses problemas.

Com o advento da Lei nº 12.846/13, chamada Lei Anticorrupção, foi trazida para o nosso ordenamento jurídico a possibilidade de responsabilização civil e administrativa da pessoa jurídica envolvida em atos contra a administração pública. A referida lei atribuiu, ainda, uma expressiva relevância à adoção dos programas de *compliance* empresarial.

Frente a esta nova realidade, então, o *compliance* tributário assumiu grande importância tanto na relação entre contribuinte e Estado, como sob o aspecto da necessidade de conformidade tributária.

A realidade tributária de uma empresa não se limita ao departamento fiscal, como poderíamos imaginar. Na verdade, praticamente todas as áreas de uma empresa se envolvem nesta questão.

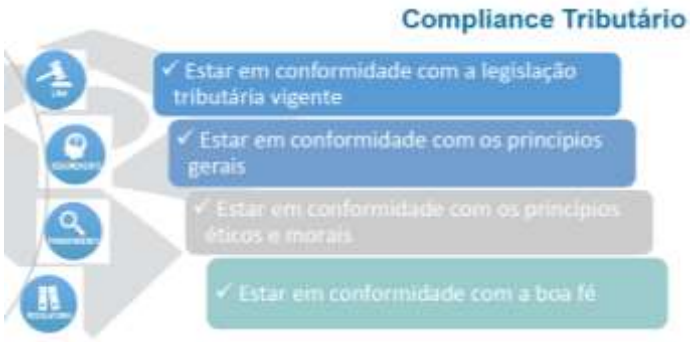
O setor de faturamento, por exemplo, comete um erro na emissão de uma nota fiscal. Ou o setor de recebimento ao dar entrada em uma nota fiscal não verifica a correta classificação fiscal da mercadoria. Ou, ainda, o setor de vendas não tem o correto entendimento da carga tributária que incide na operação e concede um desconto maior do que a operação poderia suportar.

O que pode acontecer nos casos em que erros semelhantes não forem percebidos? Como saber se não ocorreram outras vezes? E se a Receita Federal identificar inconsistências nas notas fiscais de um negócio e, antes que ele possa corrigi-las, o autua por isso? Como evitar que outros erros dessa ordem voltem a acontecer?

Havendo uma política de *compliance* tributário, tais erros seriam identificados e corrigidos a tempo, não gerando nenhuma complicação extra ou prejuízo para a empresa.

Os exemplos apresentados são mais corriqueiros do que se pode imaginar e podem ajudar a entender por que a prática de *compliance* tributário é tão importante.

No setor fiscal basta trocar a nota fiscal por uma guia de pagamento de tributos ou por uma declaração de obrigação acessória entregue com alguma não conformidade, por exemplo. Se esses documentos forem preenchidos e enviados com erros ao Fisco, a menor das complicações para o empresário será o custo extra com impostos. Ele poderá cair na malha fina da Receita, ser auditado e multado.



E é justamente para evitar esse tipo de situação que serve o *compliance* tributário.

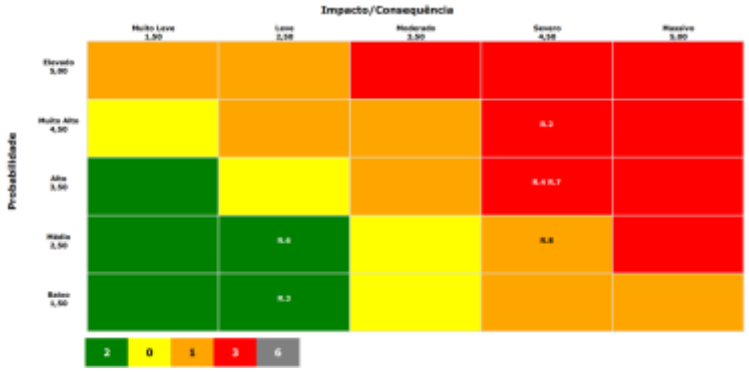
Sem contar com ferramentas e sistemas que proporcionem uma melhor administração das atividades tributárias, um negócio se encontrará exposto à ocorrência de falhas que poderão afetar seu faturamento e toda a sua estrutura.

Com uma boa política de *compliance* tributário é possível, ainda, reduzir custos. Isso porque, tendo um melhor acompanhamento das mudanças que ocorrem

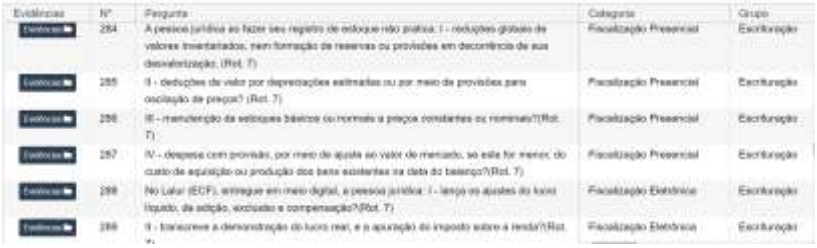
diariamente na legislação fiscal brasileira e exercendo um melhor controle sobre os registros fiscais, torna-se muito mais fácil evitar a perda de recursos resultante de pagamentos tributários maiores que o devido.

Pensando em seu negócio, a Brasiliano INTERISK, que possui grande experiência, nacional e internacional, em desenhar e implantar soluções em Riscos Corporativos, criou a Divisão de Risco Tributário, cujo objetivo foi desenvolver e implementar a disciplina de gerenciamento de riscos tributários.

Apresentada ao mercado em dezembro de 2021, de forma inédita, esta ferramenta permite que as empresas quantifiquem os riscos tributários a que estão expostas e, também, o quanto tais riscos representam financeiramente em seu patrimônio, possibilitando uma melhor compreensão deles e, também, o correto desenvolvimento de um plano de mitigação.



Temos acompanhado o enorme avanço tecnológico da Receita Federal do Brasil e consequentemente da inteligência fiscal aplicada, fator que elevou exponencialmente os riscos de detecção de erros e inconsistências pelo fisco, e concluímos ser inevitável que as empresas invistam em novos mecanismos de inteligência em sua gestão tributária para evitar impactos, como as perdas financeiras, multas, autuações, responsabilização criminal, alta exposição da empresa junto ao fisco e, principalmente, perdas de créditos tributários e de oportunidades para reduzir os custos fiscais do negócio.



Nº	Pergunta	Categoria	Grupo
166	A pessoa jurídica, na determinação do lucro real, exclui do lucro líquido do período de apuração as receitas financeiras decorrentes de ajuste a valor presente de elementos do ativo de que trata o art. 4º da Lei nº 12.973, de 2014, nos períodos de apuração em que forem apropriadas? (Rot. 6)	Fiscalização Eletrônica	Apuração da Base de Cálculo
167	A pessoa jurídica, na determinação do lucro real, exclui do lucro líquido do período de apuração os valores decorrentes do ajuste a valor presente de elementos do passivo de que trata o art. 5º da Lei nº 12.973, de 2014, nos períodos de apuração em que ocorrerem as hipóteses relacionadas nos incisos I a V do caput, observadas as demais condições estabelecidas no artigo? (Rot. 6)	Fiscalização Eletrônica	Apuração da Base de Cálculo
168	A pessoa jurídica, na determinação do lucro real, exclui do lucro líquido do período de apuração o valor do aporte de recursos efetivado pelo Poder Público em função de contrato de parceria público-privada nos termos do § 2º do art. 6º da Lei nº 11.079, de 2004? (Rot. 6)	Fiscalização Eletrônica	Apuração da Base de Cálculo

Através da adoção de uma política de *compliance* tributário e a consequente implementação da uma ferramenta de gerenciamento de riscos da Brasiliano INTERISK, sua empresa a crescerá independentemente do nível em que ela se encontra, uma vez que o Escopo e o Framework utilizados sempre estarão em conformidade com as necessidades e grau adequado para a maturidade existente na sua empresa.

Nossas soluções de gestão de riscos tributários e *compliance* tributário visam garantir que a área tributária de sua empresa esteja em conformidade com as normas fiscais vigentes no País para que ela possa operar e crescer com segurança.

Flavio Fleury de Souza Lima, CIEAC, CISI, CIGR
Especialista nas áreas de imposto sobre a renda,
contribuição social sobre o lucro líquido, PIS e Cofins. Formado pelo CPOR/SP, é graduado em administração de empresas pelo Mackenzie e cursou direito na UNIP. Atualmente trabalha como Diretor Associado da Divisão
de Risco Tributário na Brasiliano INTERISK.

GOVERNANÇA CORPORATIVA EM SÍNTESE

Edvaldo Almeida

Vivemos em mundo globalizado onde a competitividade e a abertura dos mercados, obrigaram as empresas a adotarem posturas mais agressivas com o objetivo de conquistar espaço e expandir seus negócios. Dentro desse espectro, as organizações se viram diante de agentes externos e internos que influenciaram diretamente no rumo dos seus negócios. Acontecimentos no mercado financeiro, nas mudanças geopolíticas, nos mecanismos de controle provenientes das legislações de cada país que interrelacionam mercados e muitos outros fatores mudaram as exigências para a manutenção e até sobrevivência das empresas, sejam no âmbito público ou privado.

Nos anos noventa, essa mobilização do mercado de capitais, o crescimento dos negócios corporativos e o desenvolvimento econômico das nações, foram os grandes propulsores da necessidade do estabelecimento de diretrizes que comprovem que as organizações possuem solidez, mecanismos de controle e responsabilidade contábil, ambiental e social. Surgiu assim o modelo de Governança Corporativa, onde quatro pilares foram definidos como alicerce para demonstrar que uma organização possui credibilidade e está apta a realizar negócios com riscos reduzidos para seus investidores. Os quatro pilares; segundo a IBGC (Instituto Brasileiro de Governança Corporativa); são:

- 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 conduzem à preservação e à otimização do valor da organização;
- 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;
- Prestação de contas (accountability): Os agentes de governança devem prestar contas de sua atuação de modo claro, conciso, compreensível e tempestivo, assumindo integralmente as consequências de seus atos e omissões e atuando com diligência e responsabilidade no âmbito dos seus papéis.
- 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.

O conceito de Governança Corporativa teve sua origem em três marcos históricos:

1. O **ativismo de Robert Monks**, que a partir da segunda metade dos anos 80, mudou o curso de governança dos Estados Unidos;

2. **O Relatório Cadbury**: Menos personalista que o ativismo de Monks, produzido de comitê constituído no Reino Unido em 1992, para definir responsabilidades de conselheiros e executivos, visando à prestação responsável de contas e transparência, em atenção aos interesses legítimos dos acionistas;

3. **Os Princípios da OCDE:** definidos em 1998, voltados para o bom funcionamento das corporações e dos mercados de capitais e, por esta via, para o desenvolvimento das nações;

Todo esse arcabouço que o mercado vem estruturando foi fortalecido após escândalos corporativos envolvendo empresas norte-americanas como a Enron, a WorldCom e a Tyco, desencadeando discussões sobre a divulgação de demonstrações financeiras e o papel das empresas de auditoria. No ano de 2002, o congresso norte-americano, em resposta às fraudes ocorridas, aprovou a Lei Sarbanes-Oxley, com importantes definições sobre práticas de Governança Corporativa. Também conhecida como **Sox**, a **Lei Sarbanes-Oxley**, foi sancionada para proteger investidores e demais stakeholders dos erros das escriturações contábeis e práticas fraudulentas.

As principais ferramentas utilizadas na Governança Corporativa, que asseguram o controle da propriedade sobre a gestão, foram concebidas para garantir que os interesses dos sócios estejam alinhados com os interesses dos stakeholders. São elas: o conselho de administração, a auditoria independente e o conselho fiscal.

O conselho de administração tendo principal responsabilidade agir no interesse dos proprietários monitorando e controlando formalmente os executivos. Cabe ao conselho estabelecer estratégias para a empresa, elegendo e destituindo o principal executivo, fiscalizando e avaliando o desempenho da gestão e escolhendo a auditoria independente. Importante ressaltar o controle sobre os **insiders** (Executivos de alto nível, ativos na empresa, eleitos para o quadro de diretoria por constituírem uma fonte de informação sobre as operações diárias da empresa), **outsiders** (Pessoas eleitas para o conselho de administração para prover consultoria independente) e **outsiders relacionados** (Pessoas que têm alguma relação (contratual ou não) com a empresa e que não estão envolvidas nas suas atividades diárias.), pois são os grupos que formam o conselho e possuem uma interdependência no resultados, embora cada grupo tenha sua autonomia assegurada, cabe a alta gestão do conselho estabelecer qualquer intervenção para garantir a continuidade do negócio.

A auditoria independente garantindo imparcialidade e apontando os pontos críticos observados, que possam divergir dos controles e objetivos estratégicos da empresa.

O conselho fiscal com o objetivo de contribuir para salvaguardar os interesses da própria companhia, ao exercer o papel de fiscalizar os atos dos

administradores, opinar sobre diversas matérias, denunciar desvios e irregularidades e prestar contas diretamente aos acionistas por meio de pareceres.

No mundo contemporâneo, após o amadurecimento diante de casos corrupção, desvios de interesses, uso de informações não fidedignas e outros fatores, evoluímos no campo da Governança Corporativa, ganhando importantes aliados, que nasceram da evolução nas legislações e integração das informações. Hoje temos ferramentas importantes, com diretrizes e normatizações que servem de norte para a gestão das organizações, ferramentas de gestão importantes como as normatizações ISO 19600 Gestão de Compliance, ISO 37.000 Governanças nas Organizações, ISO 37.301 Gestão de Compliance, ISO 31.000 Gestão de Riscos Corporativos e ISO 22.301 Gestão da Continuidade de Negócios, são determinantes para a estruturação da Governança Corporativa.

Em abril de 2010 o Reino Unido promulgou a Lei **The Bribery Act**. O ato abrange o direito penal relacionado ao suborno e combate à corrupção. A legislação abrangente anticorrupção e suborno do Reino Unido entrou em vigor em 1º de julho de 2011.

Inspirado nessa lei, o Brasil estabeleceu a Lei Anti-corrupção, **Lei** nº 12.846, de 1º de agosto de 2013, trata da responsabilização administrativa e civil de pessoas jurídicas (empresas) pela prática de atos de corrupção contra a administração pública, nacional ou estrangeira, e atende ao pacto internacional firmado pelo Brasil para fortalecer a Governança Corporativa.

No ano de 2016, com o objetivo de proteger os dados dos usuários europeus, a União Européia estabelece a **GDPR**, **General Data Protection Regulation** (Regulamento Geral de Proteção de Dados), trata-se do conjunto de regulações a respeito de proteção de dados na União Europeia. Seguindo a mesma linha da GDPR, o Brasil promulga em 2018 a Lei 13.709 - LGPD, Lei Geral de Proteção de Dados, que tem como objetivo proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Todas as normatizações e legislações surgidas, influenciam diretamente no planejamento estratégico da Governança Corporativa nas empresas, e estabelecem uma integração como foco na gestão de riscos, análise constante dos sistemas de compliance e monitoramento ininterrupto dos fatos internos e externos, e, legislações.

A Governança Corporativa se tornou um grande “Ecosistema” onde o conhecimento dos fatores internos e externos, o estabelecimento de diretrizes estratégicas com foco nos controles e a integração entre todos os setores, serão fatores determinantes para a sobrevivência das organizações.

Edvaldo Almeida
edvaldoalmeidar@gmail.com
(71) 99129-0801

Resiliência Diante de Riscos Geopolíticos

Prof. Dr. Antonio Celso Ribeiro Brasiliano,
CIEAI, CEGRC, CIEAC CIEIE, CPSI, CIGR, CRMA, CES, DEA, DSE, MBS

Um plano de crise e ou de continuidade de negócios é apenas um exercício de racionalização de uma realidade que, por essência, continua aleatória. Operacionalizar o Plano requer consciência situacional e flexibilidade mental para enfrentar o inesperado.

Nos últimos dois anos, parece que vivemos em um estado de crise contínua, pois eventos globais inesperados perturbaram organizações em todas as partes do mundo. De uma pandemia global e interrupções maciças da cadeia de suprimentos ao aumento da inflação/custo de vida e ataques cibernéticos em larga escala que pararam as empresas em seus rastros, organizações grandes e pequenas enfrentaram inúmeros desafios. Consequentemente, a resiliência operacional nunca foi tão vital.

Agora, uma crise geopolítica também demonstra a necessidade crítica de organizações resilientes e robustas que possam se adaptar e flexionar rapidamente para tomar decisões e ações. Mundo BANI!!

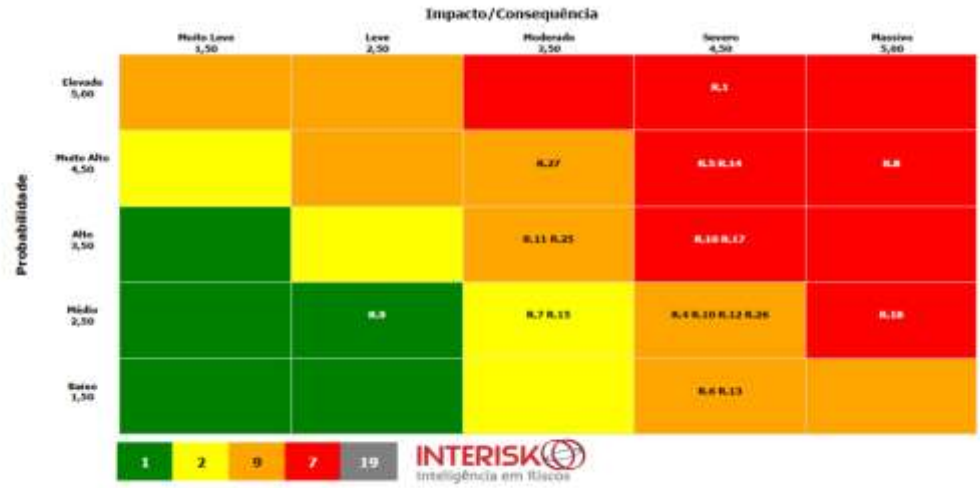
A crise na Ucrânia apresenta-se multifacetada, afetando a segurança do pessoal, as cadeias de suprimentos, os fornecedores e a economia. É fundamental que as organizações avaliem os efeitos futuros imediatos e potenciais e tomem medidas rápidas. Há necessidade de elaborar cenários prospectivos de curto prazo, de acordo com o andamento da guerra.

Avaliar o impacto

O primeiro passo para formular uma resposta é avaliar o impacto de qualquer ameaça ou interrupção e entender completamente quais operações de negócios, clientes, fornecedores e parceiros podem ser afetados.

Organizações com escritórios em áreas afetadas pela crise geopolítica devem considerar como as operações diárias serão afetadas. A segurança dos funcionários deve ser a prioridade máxima. As empresas também devem considerar que intervenções governamentais, como sanções, limitações financeiras ou restrições de toda ordem, podem dificultar a capacidade da organização de funcionar normalmente.

Mesmo que uma organização não tenha ligações diretas com as áreas afetadas, ela não existe no vácuo. As empresas devem identificar o impacto nos fornecedores críticos e como isso afeta diretamente os seus negócios. Exemplo no Brasil é o agronegócio, em função da descontinuidade dos fertilizantes! Elaborar uma Matriz de Riscos é essencial para entender seus contextos.



O efeito sobre os fornecedores e sua cadeia de suprimentos pode não ser imediatamente aparente, por isso as organizações devem entrar em contato proativamente com provedores de terceiros e perguntar sobre suas operações e planos de resiliência.

Crise pede ação

Crise requer uma resposta. Por isso é fundamental que cada empresa tenha um plano abrangente de crise e continuidade de negócios que foi desenvolvido com as principais partes interessadas e possa ser rapidamente ativado para garantir a continuidade das operações.

Haverá muitas partes móveis nesse processo. Ativar subgrupos e subtarefas para orquestrar a resposta completa do negócio é fundamental para permanecer organizado e eficiente. Os subgrupos devem assumir tarefas separadas da resposta geral dos negócios, como alternativas de fornecedores e logística geográfica de escritórios, e se envolver com os principais stakeholders das áreas críticas para decisões e aprovações de emergência. Manter o conjunto dos insumos críticos atualizado durante a ativação dos planos será fundamental para o sucesso.

Entender as dependências do fornecedor e da cadeia de suprimentos e projetar potenciais impactos durante eventos disruptivos requer o mapeamento dos processos de negócios em detalhes; de preferência que esta ação tenha acontecido antes da crise. As organizações devem se concentrar em processos de negócios críticos que suportam serviços e produtos críticos. Se uma organização não tiver um mapa completo de fornecedores/cadeia de suprimentos para seus produtos e serviços críticos, ela deve usar dados existentes sobre serviços e produtos comerciais críticos e se engajar a partir desse ponto.

Elaborar um BIA – Bussiness Impact Analysis de processos e sistemas é primordial para o entendimento do que é essencial para suas operações. Através de uma Matriz de priorização a organização é mais fácil perceber quais as ações que devem ser operacionalizadas, de forma rápida.

Engajar-se com fornecedores essenciais e entender plenamente sua posição e operações direcionará os próximos passos. Em alguns casos, os fornecedores podem continuar as operações como de costume, mas em outros, um fornecedor alternativo pode ter que ser encontrado – e rapidamente.

Prepare-se para o longo prazo – Cenário Mapa do Inferno

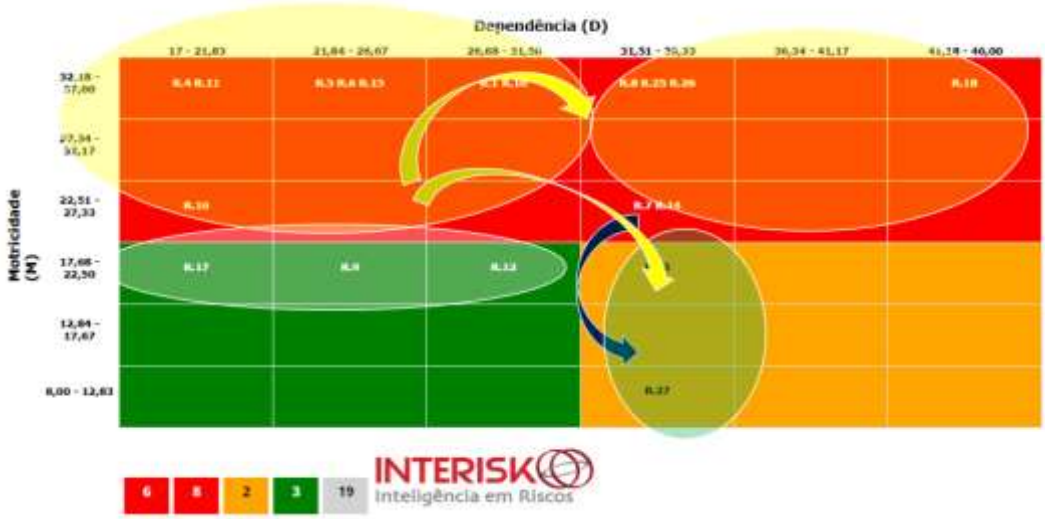
Os efeitos do COVID mostraram a importância de ter um plano de longo prazo e de alto nível para uma crise econômica, e para que os líderes estejam preparados para quando o fluxo de caixa e o mercado não estiverem agindo favoravelmente.

Planos não são o objetivo final. Eles são um bom exercício, mas é a resposta músculo-memória ao objetivo que causa um impacto em tempos de crise. As organizações devem ser capazes de olhar para um plano, entender como a situação atual se desvia do plano e agir rapidamente. Temos que entender que um plano é apenas um exercício de racionalização de uma realidade que, por essência, continua aleatória. A incerteza nunca irá desaparecer, tem que ser gerenciada, através da flexibilidade mental dos executores dos respectivos planos.

É fundamental ter dados sobre como as operações funcionam e entender todas as peças móveis que contribuem para o negócio como de costume. Mapear esses dados de forma organizada permitirá ação sem demora quando interrupções de longo prazo afetarem uma organização. Entender como uma organização funciona fornece o conhecimento para colocá-la de novo em funcionamento.

Entender os dados e informações críticas da empresa garante flexibilidade operacional.

O mapeamento de processos começa dentro de uma organização e se estende às dependências internas e externas, incluindo fornecedores, cadeia de suprimentos, aplicativos, pessoas e sites físicos que suportam funções comerciais diárias. Simplesmente saber quem supervisiona quais funções e tarefas não é suficiente. Um processo de negócios pode ter várias equipes em diferentes regiões/países e usar fornecedores diferentes para o mesmo produto/serviço simplesmente por causa da diferença geográfica. Temos que entender completamente as operações em todos os níveis de motricidade, temos que realizar impactos cruzados, e saber quem é motriz e quem é dependente passa a ser crucial para a sobrevivência.



Entender a conectividade de seus fornecedores com sua operação é crucial para sua sobrevivência. Saiba em quais fornecedores você confia, em quais operações é possível reconhecer o impacto em um negócio em tempos de crise e informar decisões pensadas.

Priorizar a Resiliência

A resiliência operacional fornece as ferramentas para entender os pontos de dados e locais da operação. Uma vez que uma organização entenda seus dados, ela pode ser efetivamente mapeada e analisada para múltiplas situações, independentemente da natureza da interrupção. Seja uma crise geopolítica, desastre natural ou escassez da cadeia de suprimentos, a resiliência fornece a capacidade de digerir dados e tomar medidas rápidas.

O planejamento proativo oferece a oportunidade de ter múltiplas opções discutidas e aprovadas anteriormente para o pior cenário. Daí a importância de construir e levar em consideração sempre o cenário denominado “mapa do inferno”.

As empresas não podem alcançar resiliência sem entender totalmente seus processos críticos. Depois de identificar processos críticos, deve ser discutido e planejado quando o negócio parar. As operações críticas geralmente incluem

pessoas, aplicativos, sites e fornecedores que permitem que uma organização cumpra sua promessa de marca aos clientes em condições normais. Ao priorizar a resiliência, as organizações podem garantir que não haja um único ponto de falha.

Pivotar e Adaptar

Nos últimos dois anos, grandes crises afetaram quase todas as organizações de alguma forma. Devemos reconhecer que as interrupções estão aqui para ficar; não é mais uma questão de se, mas quando outra crise ocorrerá. Nunca foi tão importante ser capaz de pivotar e se adaptar a qualquer interrupção.

É fundamental que as empresas hoje entendam o cenário global de riscos para que possam responder proativamente e se antecipar a possíveis interrupções.

Às vezes, a reação excessiva pode apresentar a melhor opção. Crises previsíveis dão às empresas o tempo e a capacidade de responder antes que a situação fique insuportável. Monitorar o cenário global continuamente oferece às organizações o tempo para agir diante do perigo iminente, especialmente quando a vida e a segurança estão em risco.

Segurança Humana em Primeiro Lugar

Ao se preparar para quaisquer interrupções, as organizações devem colocar as pessoas em primeiro lugar. Com os dados adequados, preparação e plano, as empresas podem adaptar perfeitamente novos modelos de operação e logística e se preocupar com o que realmente importa: as pessoas e sua segurança.

Nenhum negócio pode existir sem seus funcionários. Ao mostrar um cuidado genuíno com os funcionários e suas famílias que podem ser afetados por uma crise, as organizações podem aumentar o moral de seu pessoal. "Estamos todos juntos nisso" vai além de posts nas redes sociais ou outros conteúdos de

marketing. Ao mostrar um cuidado genuíno, a fidelização de funcionários e clientes aumentará muito além do período de interrupção.

As organizações também devem ser corajosas e defender o que acreditam ser moralmente certo. Não seja o único atrasado enquanto todos estão tomando uma posição particular por medo. Não se trata de política; trata-se de cuidar da vida humana e colocar as pessoas em primeiro lugar.

Olhando para o futuro

A guerra da Ucrânia evolui a cada minuto. A situação que um negócio enfrenta hoje pode ser diferente amanhã. As organizações devem priorizar a agilidade nessas situações para se flexibilizar e se adaptar à medida que novos eventos ocorram.

Com as medidas preventivas e proativas adequadamente planejadas e em vigor, as organizações podem priorizar o que realmente importa – a vida humana.

Prof. Dr. Antonio Celso Ribeiro Brasiliano, DICS, MCRC, CIEAI, CEGRC, CIEAC, CIEIE, CPSI, CIGR, CRMA, CES, DEA, DSE, MBS, Doctor en Ciencias de la Información e Ingeniería e Inteligencia Estratégica pela Universidad Paris-Est (Marne La Vallée, Paris, França); Doctor Internacional en Ciencias de la Seguridad, pela CEAS – Internacional – Madrid – Espanha, presidente da Brasiliano INTERISK. abrasiliano@brasiliano.com.br

ABNT NBR ISO 31022 – Diretrizes para a Gestão de Riscos Legais

Flavio Fleury de Souza Lima, CIEAC, CISI, CIGR

A grande variedade da regulamentação legal a que estão expostas as empresas que operam no ambiente global resultou na necessidade de aprimoramento da gestão de riscos legais.

Os riscos legais estão relacionados a danos ou a qualquer perda ocorrida em um negócio devido a negligência, em conformidade com as leis relacionadas ao negócio. Eles podem ser encontrados em qualquer fase do processo comercial. Pode haver erros em razão de falhas na interpretação das leis ou da não-apresentação de alguns documentos que precisam ser submetidos às autoridades que regulamentam um negócio específico.

A ABNT NBR ISO 31022 de 12/2020 - Gestão de Riscos Legais – é o conjunto de orientações para a gestão de riscos legais que estabelece diretrizes para a gestão específica desses riscos, constituindo-se em um documento complementar à NBR ISO 31000 que estabelece uma estrutura genérica para todos os tipos de riscos, conforme apresentado na figura abaixo:

Princípios

Os oito princípios encontram-se descritos no contexto da gestão de riscos legais. Adicionalmente, para a gestão desses riscos, é conveniente que o princípio da equidade também seja considerado.

A gestão de riscos legais integra a governança global da organização. As atividades do processo de gestão desses riscos devem ser incorporadas ao planejamento estratégico, às tomadas de decisões de negócios e aos processos de gestão da organização.

A integração da gestão de riscos legais nos processos e atividades organizacionais, papéis e responsabilidades apropriados deve ser estabelecida dentro da organização e deve ser integrada a outros sistemas de gestão, como *compliance*, segurança, qualidade e controles internos. Ao avaliar os riscos

legais e considerar as opções de tratamento, é conveniente que especialistas no assunto sejam consultados em conjunto com outros peritos ou especialistas.

No processo genérico de gestão de riscos, é importante avaliar os riscos legais da organização, dentro de um contexto apropriado, para que uma abordagem abrangente e pertinente à gestão desses riscos possa ser adotada.

A gestão de riscos legais em uma organização deve ser personalizada para refletir as diferenças do contexto externo, que inclui o contexto legal e regulatório e as características do setor, bem como o contexto interno da organização, incluindo a natureza da entidade legal, objetivos e valores da organização.

A organização deve ter um entendimento detalhado da **aplicabilidade, impacto e consequências da falha em cumprir leis pertinentes, e processos** para assegurar que leis novas ou atualizações aplicáveis sejam adequadamente identificadas, interpretadas e avaliadas em relação ao impacto. A organização deve minimizar a complexidade e o custo dos procedimentos legais e as consequências negativas dos riscos legais.

As organizações podem buscar ativamente oportunidades para evitar disputas ou litígios, tomando medidas para tratar riscos legais antes que um evento adverso possa ocorrer e buscando chegar a acordos que equilibrem custos, objetivos comerciais, reputação e tempo investido pela organização. Ao envolver todas as partes interessadas na gestão de riscos legais, uma organização pode mitigar eventos adversos, aí incluindo a aplicação regulatória.

A organização deve tomar cuidado para assegurar que privilégios legais (ou qualquer outra forma equivalente de proteção na jurisdição pertinente) sejam mantidos na medida do possível e que a confidencialidade seja mantida, mas, em todos os casos, essas proteções precisam ser avaliadas em relação aos benefícios da inclusão.

É importante, também, que a organização faça o monitoramento das mudanças nas leis e políticas públicas, no contexto em que opera, e que estabeleça indicadores apropriados de alerta precoce.

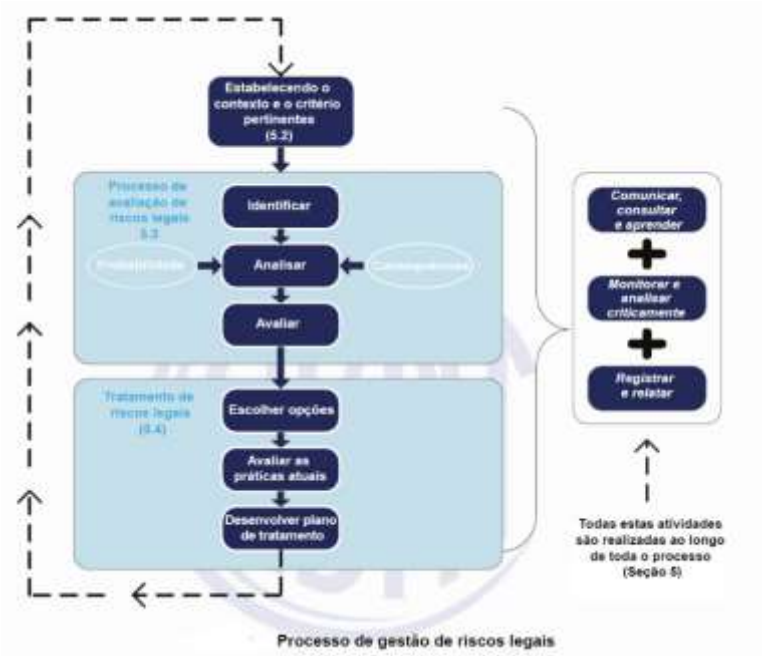
A gestão eficaz de riscos legais, além da experiência de consultores jurídicos internos, quando existentes, deve se utilizar da inteligência de negócios, análise de negócios, bancos de dados e sistemas jurídicos (incluindo gestão de casos), ferramentas e serviços de gestão de arquivos eletrônicos e know-how fornecido por leis externas às empresas, prestadores de serviços e consultores.

Se for tomado em consideração que as partes interessadas possam ter conhecimentos, expectativas e visões diferentes em relação aos riscos legais e que essas visões possam ser emocionalmente, socialmente, culturalmente e politicamente construídas e percebidas, convém que a organização desenvolva mecanismos formais e informais para ajudar a assegurar que fatores humanos e culturais não resultem inadvertidamente em riscos legais.

As organizações devem procurar incentivar a realização, os benefícios e as oportunidades da gestão dos riscos legais. Todo membro da organização deve estar ciente de como cada ação ou omissão afeta tais riscos. É conveniente que a organização considere e aja de acordo com as lições aprendidas, publique análises críticas de transações, melhores práticas, aconselhamento profissional de advogados internos e externos e alterações aplicáveis na lei.

Para os tomadores de decisão, o estabelecimento do princípio da equidade orienta a gestão de riscos legais, inclui a gestão de conflitos de interesses e fornece uma voz imparcial e independente na tomada de decisões, além de apoiar a *due diligence* e imparcialidade para os melhores interesses de uma organização.

A gestão de riscos legais é repetitiva e deve ser integrada em todas as atividades e operações da organização. Este diagrama foi desenvolvido para complementar a ABNT NBR ISO 31000:2018



Processo de gestão de riscos legais

A organização deve considerar os contextos externo e interno.

O contexto externo dos riscos legais se refere a fatores que estão fora da organização, mas relacionados à gestão de riscos legais.

Para se examinar e entender o contexto externo de riscos legais para organizações que operam em várias jurisdições, é preciso que as diferenças ambientais e culturais entre diferentes jurisdições sejam consideradas. Deve-se observar a aplicação extraterritorial das leis nacionais, qual lei da jurisdição se aplica a uma determinada situação e a identificação da jurisdição aplicável.

O contexto interno dos riscos legais concentra-se no controle ou se sujeita à autoridade de uma organização por meio de seus sistemas de governança e gestão. Isto inclui, dentre outros:

- a natureza da pessoa jurídica;
- a saúde financeira organizacional, seu modelo de negócios e a estrutura jurídica interna da organização, processos e funções;
- a governança da organização e suas estruturas de valor que promovem a integridade, como código de conduta e outras diretrizes de *compliance*;
- o atual estado das questões e assuntos legais e sua abordagem para a gestão de riscos legais;
- a experiência passada e histórico de disputas ou eventos legais desencadeados por risco legal na organização;
- os ativos que a organização possui, como propriedade intelectual e outros direitos legais para ativos tangíveis e intangíveis usados em processos e atividades;
- o efeito de direitos e deveres sob contrato; obrigações relacionadas ao dever de cuidar; a negligência e efeitos desencadeadores de indenizações, garantias e cláusulas de não confiança em contratos;
- os passivos decorrentes de questões trabalhistas, ambientais, tributárias e outras, decorrentes de fusões, aquisições e alienações; a política interna de gestão de riscos legais;
- outras informações e recursos relacionados aos riscos legais e sua gestão.

A norma ABNT NBR ISO 31022 define ainda que as organizações considerem critérios de riscos legais. O estabelecimento desses critérios é orientado por processos e requer que tais riscos sejam caracterizados e, posteriormente, medidos para que possam ser quantificados e o tratamento de risco apropriado aplicado.

A probabilidade de eventos relacionados a riscos legais pode envolver fatores como:

- a gama de leis, práticas e convenções de execução pelas autoridades reguladoras pertinentes;
- a melhoria e o *compliance* da estrutura existente para a gestão de riscos legais, incluindo estratégias, governança, regras internas e políticas; as demonstrações de *compliance* com as leis e as regras e políticas da organização por parte dos funcionários e contratados;
- a frequência e o número de atividades relacionadas aos riscos legais que ocorrem dentro de um determinado período;
- a falha em registrar, analisar e aprender com eventos anteriores; o *benchmarking* da frequência e o número de atividades relacionadas a riscos legais que ocorrem em um certo período em relação a outras organizações.

A gestão de risco legal requer, ainda, uma abordagem estruturada para avaliar riscos legais dentro do contexto de uma organização. Por meio da adaptação de técnicas adequadas de gestão de riscos, uma organização pode identificar proativamente os riscos legais e então reduzir, eliminar ou reconfigurar seus processos para minimizar a exposição a eles.

A matriz de identificação de riscos legais (MIRL) é uma abordagem para organizar os riscos legais identificados e coletados como eventos de diferentes tipos através de áreas/unidades/atividades de negócios. Ao considerar as várias áreas/ unidades /atividades de negócios envolvidas, a MIRL conecta os riscos legais de vários tipos às operações da organização. Em uma MIRL, todos os eventos de riscos legais identificados são categorizados em diferentes tipos.

Estes diferentes tipos de riscos legais podem ocorrer em diferentes de áreas de negócios e ter diferentes causas e características. A MIRL ajuda a compreender, sistematicamente, todos os riscos legais da organização.

A tabela abaixo (Anexo A da norma) fornece um exemplo de MIRL que categoriza os riscos legais dentro de seis diferentes tipos e inclui uma breve explanação das diferentes categorias.

Exemplo de uma MIRL

Parâmetro	Categoria 1	Categoria 2	Categoria 3	Categoria 4	Categoria 5	Categoria 6
Tipologias de risco legal	Imprevisibilidade	Não compliance com as leis aplicáveis	Quebra de contrato	Violação de direitos	Omissão no exercício de direitos	Escolha inadequada
Atividade de negócio 1						
Atividade de negócio 2						
Atividade de negócio 3 etc.						

Categorias

Categoria 1: A imprevisibilidade no contexto de riscos legais pode surgir quando uma organização enfrenta uma mudança significativa na lei em um ambiente, mercado ou território em que a organização possui operações ou se a organização decide entrar em um novo ambiente, mercado ou território em que as leis não são familiares à organização ou onde pode haver uma ausência da lei local em determinados aspectos.

Categoria 2: A não conformance ocorre quando uma organização viola uma lei aplicável. Por exemplo, uma organização falha em incluir uma informação apropriada em seus relatórios, de acordo com suas obrigações, junto aos reguladores.

Categoria 3: A quebra de contrato ocorre quando a organização ou a contraparte contratante quebra uma obrigação contratual em função do não desempenho ou desempenho inadequado, gerando consequências legais, como por exemplo, reclamações por danos ou direito da parte não inadimplente em rescindir o contrato. Por exemplo, a organização falha em entregar as mercadorias no prazo, de acordo com suas obrigações contratuais.

Categoria 4: A infração ocorre quando a organização invade ou viola os direitos legítimos ou expectativas de terceiros. Por exemplo, seria uma violação dos direitos de propriedade intelectual de terceiros usar sua marca comercial sem permissão. A infração pode surgir sob uma obrigação contratual de uma parte de um contrato ou pode surgir quando não há obrigação contratual.

Categoria 5: A omissão no exercício de direitos ocorre quando há uma conduta que fica abaixo dos padrões de comportamento estabelecidos por lei quanto à proteção de terceiros contra riscos de danos que não razoáveis. Uma organização pode agir negligentemente ou ser vítima de negligência de outros. Além disso, uma organização pode vir a ser negligente no exercício de seus próprios direitos, obrigações e responsabilidades, resultando em danos à organização. Por exemplo, se uma organização não notificar em tempo hábil suas seguradora em relação a um determinado sinistro, essa negligência no exercício de seus direitos pode resultar na perda do direito de cobertura relacionada à sua apólice de seguros.

Categoria 6: A escolha inadequada ocorre quando uma organização tem várias alternativas a serem consideradas em relação a uma questão que envolve riscos legais, os quais todos podem ser legais, mas cada um apresenta diferentes custos, implicações e consequências, ou seja, uma alternativa ou uma série de alternativas seriam abandonadas quando uma decisão é tomada. Por exemplo, uma empresa pode optar por resolver uma disputa com um parceiro comercial por meio de litígio ou arbitragem. Qualquer abordagem - litígio ou arbitragem - pode resolver a disputa, mas cada uma terá implicações diferentes em termos de preservação do relacionamento comercial entre as partes, aspectos relacionados a reputação na indústria e na comunidade, tempo envolvido necessário e custos incorridos.

Para que a categorização dos riscos legais seja útil, é importante reconhecer que as categorias podem não ser mutuamente exclusivas e que uma simples atividade de negócio pode gerar riscos legais que se enquadram em uma ou mais categorias.

O Anexo B nos fornece um exemplo de registro legal que é uma compilação de possíveis ocorrências de eventos de riscos legais com as leis correspondentes, possíveis resultados e consequências.

No Anexo C temos as orientações adicionais sobre como estimar a probabilidade de eventos relacionados a riscos legais.

O Anexo D demonstra a consequência financeira, regulatória, de reputação, geográfica e organizacional dos riscos legais.

E, por fim, o Anexo E fornece um breve resumo das principais cláusulas a serem consideradas ao analisar criticamente um contrato com a finalidade de minimizar os riscos legais.

Dentro de cada categoria de riscos legais pode haver bandeiras vermelhas - podem incluir jurisdições onde há falta de um estado de direito em pleno funcionamento ou instabilidade política; as condições que requerem que o fornecedor proveja uma indenização contratual devido ao extremo dever de cuidado requerido; e os produtos perigosos ou condições perigosas de desempenho - que devem ser identificadas e escaladas dentro da estrutura de governança organizacional a fim de que elas sejam tratadas adequadamente.

Flavio Fleury de Souza Lima, CIEAC, CISI, CIGR
Especialista nas áreas de IRPJ, CSLL, PIS e COFINS. Formado pelo CPOR/SP, é graduado em administração de empresas pelo Mackenzie e cursou direito na UNIP. Atualmente trabalha como Diretor Associado da Divisão de Risco Tributário na Brasiliano INTERISK.