REVISTA
GESTÃO DE RISCOS
EDIÇÃO 157 | JUNHO 2021

Brasiliano INTERISK
Inteligência em Riscos

RISCOS POLÍTICO E ECONÔMICO CAUSAM INSTABILIDADE

REVISTA
GESTÃO DE RISCOS
EDIÇÃO 157 | JUNHO 2021

Brasiliano INTERISK
Inteligência em Riscos

pg 4

Riscos político e econômico Brasil causam instabilidade: vamos superar?

A Revista GR é um PDF interativo, aqui além do texto, você vai encontrar links e botões clicáveis.

editorial

Marcos Alves Junior
Assistente de Comunicação e Marketing da Brasiliano INTERISK

Em sua edição 157, a revista Gestão de Riscos traz um conteúdo enriquecedor aos leitores que estão desenvolvendo conceitos e se atualizando diante aquilo que acontece no Brasil e no mundo relacionado aos cenários de Governança, Riscos e Compliance. É importante ressaltar que as nossas publicações são comprometidas com a responsabilidade social e científica.

Na seção "Ponto de Vista", expusemos o artigo "Riscos Político e Econômico Brasil causam Instabilidade: vamos superar?", escrito pelo professor, doutor e presidente da Brasiliano INTERISK, Antonio Celso Ribeiro Brasiliano, em que o autor discorre sobre os impactos econômicos gerados pelas decisões dos nossos governantes.

Já na seção "Cibernético", também redigido pelo Prof. Brasiliano, o texto trata sobre como as organizações podem adquirir uma visão de antecipação e adaptação diante do aumento expressivo do número de ataques cibernéticos no Brasil e no mundo.

No texto "ESG E O MEIO AMBIENTE: Precaução e Prevenção de Riscos", a doutora em direito ambiental, advogada, Consultora Sênior Associada da Brasiliano INTERISK, Silmara Veiga de Souza Calestini Montemor discorre sobre a agenda ESG, uma iniciativa que tem como objetivo fazer com que as organizações tratem as questões ambientais, sociais e de governança com maior responsabilidade.

O artigo intitulado "NÃO SE FAZ SEGURANÇA COM ATOS E SISTEMAS ISOLADOS: em defesa de profissionais qualificados e de uma segurança integrada", o autor, Carlos Alberto Zanandreis da Silveira, gestor de segurança e especialista em gestão de crises e emergências na Fundação Renova, aborda os desafios enfrentados no gerenciamento da segurança no âmbito das organizações.

Na seção "Gestão, Carlos Köhler, graduado em segurança pública, pós-graduado em segurança privada e CEO do Grupo CINDAPA, no texto "O que traz a sensação de segurança - Condomínios", faz uma breve reflexão em relação aos recursos que trazem a sensação de segurança às pessoas.

A leitura da análise de autoria de Gustavo Vedove, especialista em riscos, GCN e proteção de dados, permitirá compreender como funciona o método para mensuração do NRGCN - Nível de Resiliência em Gestão de Continuidade de Negócios, criado pelo próprio autor, com o objetivo de mensurar o nível de resiliência em Gestão de Continuidade de Negócios das empresas.

No artigo "Mundo Líquido - A Era da Informação, Fake News e Desinformação", escrito por Cláudio dos Santos Moretti, CES, ASE – Diretor da CSM – Consultoria e Treinamento em Segurança Empresarial, o autor relata que, em paralelo com o surto do COVID-19, o mundo sofre com uma epidemia de desinformação e fake news.

Por fim, na seção "Acontece", é possível acompanhar a cobertura de dois eventos. Um deles foi o webinar organizado pela Brasiliano INTERISK. Já o outro foi uma aula ministrada pelo professor Antonio Celso Ribeiro Brasiliano na 9ª melhor escola de negócios do mundo, de acordo com o ranking de educação executiva do jornal Financial Times.

Riscos político e econômico Brasil causam instabilidade: vamos superar?

Segundo especialistas, incluindo o ex-Presidente do Banco Central Affonso Celso Pastore, há grandes chances de desaceleração do PIB brasileiro em 2022, ano eleitoral, em função das medidas tomadas pelo Banco Central para barrar o descontrole da inflação. É assim que o populismo de Bolsonaro gera seus principais efeitos na piora dos preços e dos indicadores, alavancando o desânimo do Centro Financeiro de São Paulo e o desalento dos empresários em geral. Segundo Affonso Celso Pastore, em entrevista ao jornal O Estado de São Paulo, dia 19 de agosto de 2021, uma piora da economia, que tira popularidade e voto, pode levar o presidente Bolsonaro a forçar uma ruptura institucional. Será? Vamos analisar os sintomas!

Antonio Celso Ribeiro Brasiliano,
CEGRC, CIEAC, CIEIE, CPSI, CIGR, CRMA, CES, DEA, DSE, MBS

Bolsonaro fez acordo com o diabo, quero dizer, com o Centrão, para tentar manter-se no poder e articular sua reeleição seja a que preço for. Os integrantes do referido Centrão, que nunca deixaram de mamar nas tetas do governo, jamais tiveram tanto poder. Já tinham a chave do cofre desde as emendas do relator. Agora possuem a chave do Palácio da Alvorada.

Bolsonaro, ao que tudo indica, vai continuar gritando e fazendo suas micaretas e bravatas para manter engajado seu núcleo duro de apoio que, convenhamos, teve o efetivo consideravelmente reduzido nestes dois últimos anos. Percebendo a formação de um cenário claramente desfavorável, com o afunilamento dramático de suas opções políticas, ele parte para uma de suas cartadas prediletas, que é colocar gente na rua. Como não é bobo, sabedor dos riscos que corre e vestindo claramente o figurino do chantagista, manda recados a várias instituições em Brasília, dizendo que não sabe se terá controle do que possa acontecer no dia 7 de setembro, mencionando protestos e até, pasmem, insurreição.

Bolsonaro transformou-se, desse modo, num presidente que não pode mais ser levado a sério, pelo uso de um estoque de blefes e bravatas que parece inesgotável. Tornou-se "intutelável", fato revelado pelas evidências de que nem os integrantes da equipe de governo que lhe são mais chegados (Paulo Guedes, militares da reserva e representantes do Centrão) conseguem conter suas atitudes indecorosas e ações desvairadas. A consequência disso é seus ditos aliados, como Arthur Lira e Ciro Nogueira, e chefes dos demais poderes, Rodrigo Pacheco e Luis Fux, terem transitado daquilo que em política externa se chama de ações de "appeasement" para uma política de "containment".

Eu explico: "appeasement", é palavra que pode ser traduzida livremente pela expressão "bater palmas para o louco dançar" e que foi bem ilustrada pela cara de cinismo de Arthur Lima ao ser perguntado se Bolsonaro tinha palavra. Já "containment" (contenção, cerco ou isolamento) é simplesmente uma utopia, tendo em vista o cenário de profunda crise institucional que atravessamos, crise esta provocada pelas atitudes destrambelhadas do presidente. Falta estratégia, falta rumo, falta até propósito que não seja ligado, de maneira simplista, à nua e crua ambição de Bolsonaro se reeleger.

O caos em que vivemos é consequência direta dessa falta de rumo, da inexistência de um sentido político e capacidade de coordenação das necessárias reformas estruturantes (administrativa, tributária e eleitoral), sem falar da falta de liderança no tratamento da pandemia (já escrevi sobre este tema na última Revista Gestão de Riscos),

ensejando atitudes irresponsáveis e até, possivelmente, criminosas, segundo a CPI em curso.

Com esta condição embaralhada não há relevância nas pautas legislativas, como prova o descaminho da reforma tributária. Esquece Bolsonaro que sua função principal é ditar o sentido da agenda política. Na cabeça dele, só existe mesmo o que ele pensa e enxerga à sua maneira míope. Bolsonaro tem certeza de que o golpe já aconteceu, através do STF, que considera um bando de esquerdistas, corruptos e outros adjetivos...Vale então o contragolpe, que, na visão míope e acanhada de Bolsonaro, se julga apoiado pelo povo, e amparado legalmente pelo artigo 142 da constituição, que colocaria, segundo essa perspectiva esdrúxula, as Forças Armadas na função de "Poder Moderador", encarregadas de intervir e colocar ordem no caos – desde que essa intervenção seja executada segundo os parâmetros da mentalidade bolsonarista.

Bolsonaro age por impulso, por arroubos, de supetão. É ao mesmo tempo hesitante e confuso. Encurralado, vê o derretimento de seu potencial eleitoral aproximar-se rapidamente do ponto em que se tornará irreversível. Nada mais natural, nessa situação, que bata o desespero, gerando balbúrdia e confusão. Bolsonaro se encontra hoje em areia movediça: quanto mais se desespera e se debate, mais afunda.

O Governo age como aprendiz de feiticeiro, com um Congresso dominado pelo Centrão. Dois projetos, segundo especialistas, são essenciais: a reforma do imposto de renda e o calote dos precatórios. Esses projetos introduziram divisões no Congresso e entre empresários, tributaristas e outras categorias profissionais. Arthur Lira, Presidente da Câmara, frisou que não há consenso nas matérias. O governo jogou a toalha na sessão desta última quarta-feira, dia 18 de agosto e aceitou adiar a discussão da reforma do IR para uma data indeterminada. Portanto, o leão continua com fome. Na questão da PEC dos precatórios, há chances de derrota.

O projeto do IR é mais uma promessa de campanha que possivelmente não será cumprida. Nele estaria contemplado o aumento da faixa de isenção para os cidadãos de menor renda. Também conteria mecanismos para, mediante a previsão de alguns recursos extras, robustecer o Programa Bolsa Família, que seria transformada em Auxílio Emergencial com renda maior e novas atribuições.

A PEC dos precatórios foi a única forma que o Governo encontrou para empurrar as dívidas para as calendas – dívidas essas que já tiveram o trânsito em julgado, ou seja, não há mais a quem recorrer. É calote mesmo, da ordem de R$ 30 bilhões em recursos que seriam destinados ao Auxílio Emergencial, calote com fins puramente eleitoreiros.

Não se pode esquecer também que, se o governo decidisse pagar todos os precatórios, não possuiria caixa para isso e teria que atrasar a folha de pagamento do funcionalismo público e paralisar determinadas atividades públicas. Isso é de fato uma vergonha para os cidadãos, pois como o governo pede que paguemos os impostos se ele, governo, não cumpre com suas atribuições básicas? Onde está o exemplo propalado aos quatro ventos, a promessa de uma administração transparente, liberal, dotada de uma máquina estatal enxuta? A conclusão, com base nos fatos, é que todas as promessas foram puro embuste.

O risco econômico, com o risco fiscal embutido recrudesceu, com saltos do dólar, queda da bolsa e aumento da pressão inflacionária. O câmbio, que tinha chegado a R$5,00, está agora em R$5,30. A taxa de juros de 10 anos, que andava em torno de 8%, hoje está acima de 10%. A euforia foi embora. O risco já aparece na Bolsa, que devolveu tudo o que tinha ganhado em 2021. Esse é o clima com o qual Bolsonaro irá entrar na campanha eleitoral em 2022. As consequências para um desgoverno como o que estamos vivenciando são os projetos saírem irreconhecíveis, e as despesas penduradas nos cofres públicos.

Nosso risco político, hoje impulsionado pelos vetores das ações de Bolsonaro nos campos econômico e social, chegou nas alturas, segundo nossa metodologia. Estamos com uma métrica de 4,56, que nos coloca com uma classificação elevada – a mais alta que já tivemos desde a posse de Bolsonaro. Por esta razão o Risco Brasil explodiu, deixando um rastro de muita instabilidade.

Brasiliano INTERISK
Inteligência em Riscos

- Escala do Nível de Risco Político

ESCALA	NÍVEL DE RISCO POLÍTICO
4,51 - 5,00	Elevada
3,01 - 4,50	Muito Alto
2,01 - 3,00	Alta
1,51 - 2,00	Média
1,00 - 1,50	Baixa

Figura 1: Escala Métrica de Risco Político
Fonte: Software INTERISK

Nº	Macrofator	Nº	Fator de Risco	Peso	Nota	Total(Peso x Nota)	Pontuação Possível
1	Estabilidade do Governo	1	Governabilidade - Coalizão	5	5	25	25
1	Estabilidade do Governo	2	Governança	5	5	25	25
1	Estabilidade do Governo	3	Apoio Popular	5	5	25	25
2	Condições Socioeconômicas	4	Desemprego	5	5	25	25
2	Condições Socioeconômicas	5	Confiança do Consumidor	5	5	25	25
2	Condições Socioeconômicas	6	Pobreza / Desigualdade Social	5	5	25	25
3	Investimentos	7	Facilidade para Negócios	5	5	25	25
3	Investimentos	8	Acesso ao Crédito	5	5	25	25
3	Investimentos	9	Onerosidade dos Processos	4	5	20	20
4	Segurança Jurídica	10	Mudança nas Legislações com Critérios Políticos	5	5	25	25
5	Desordem Civil	11	Golpe de Estado	5	5	25	25
5	Desordem Civil	12	Violência Política	5	5	25	25
5	Desordem Civil	13	Conflitos Políticos	5	5	25	25
6	Geopolítica	14	Guerra / Conflitos Fronteira	5	1	5	25
7	Corrupção	15	Nível de Corrupção nas Instituições Estatais	5	5	25	25
8	Militares na Política	16	Possibilidade de Intervenção	5	5	25	25
9	Conflitos Religiosos	17	Atritos e Violência entre as Crenças	4	3	12	20
10	Conflitos Étnicos	18	Atritos e Violência entre os Grupos Étnicos	4	3	12	20
11	Accountability Democrático	19	Participação Ativa da Sociedade	5	5	25	25
12	Lei e Ordem	20	Desordens, Manifestações, Protestos e Vandalismos	4	4	16	20
13	Qualidade da Burocracia	21	Qualidade na Abertura de Empresas, Nível de Serviços de Cartórios, Mentalidade de Cartorial	4	4	16	20
Total (Soma das Colunas)				**100**	**95**	**456**	**500**
Nível Risco Político						**4,56**	**5**
Classificação do Risco Político							**Elevada**

Figura 2: Fatores de Riscos Políticos Mensurados
Fonte: Software INTERISK - Pesquisa sobre o Governo Bolsonaro

Bolsonaro tem feito um governo desastroso, para não dizer horroroso, em termos de gestão e estratégia. A estratégia escolhida por ele tem sido a do confronto e da agressividade. Só que o tiro está saindo pela culatra. A interpretação do mercado, não apenas minha, é de que quanto mais isolado e fraco ele está, mais agressivo fica, conforme já escrevi em parágrafos acima. É simplesmente por isso que ele não abandona sua cruzada contra integrantes do Judiciário, visando manter ativa e engajada sua base mais radical.

Ocorre assim um esvaziamento, um verdadeiro vácuo entre as intenções declaradas e as ações do presidente e seus acólitos. O contrário acontece no legislativo e no judiciário que, com ações bem direcionadas, esvaziam de sentido as palavras do presidente. O resultado inexorável é o descrédito que já se faz notar nas pesquisas de opinião. Enquanto Bolsonaro e seus vassalos gritam como moleques de rua pedindo briga, tribunais superiores, Câmara e Senado enquadram essas ações à luz da legislação e levam o time de Bolsonaro a fazer gol contra.

O que estamos vendo é, de um lado, a intenção de provocar e, do outro, o gesto de enquadrar os provocadores segundo os dizeres da constituição. De um lado, gritaria; do outro, mão firme. Até o momento, a mão firme está dominando o jogo.

Outro ponto importantíssimo, captado nas pesquisas dos institutos, é o crescimento da rejeição a Bolsonaro. Ele está, ao que tudo indica, entregando de bandeja o jogo a seu oponente. Será tão difícil enxergar isso?

Reproduzimos, nos prints a seguir, alguns resultados relevantes da pesquisa XP/Ipespe mais recente, de agosto de 2021.

Destaques

A rodada de agosto da pesquisa XP/Ipespe mostra continuidade na tendência de crescimento das avaliações negativas do governo Jair Bolsonaro.

No levantamento atual são 54% os que dizem considerar o governo ruim ou péssimo contra 52% no mês passado. O crescimento na rejeição é constante desde outubro de 2020, quando 31% diziam considerar a gestão ruim ou péssima.

Na outra ponta, os que veem o governo como bom ou ótimo somam 23%, 2 pontos a menos que na pesquisa de julho. Os dois números são os piores para o governo desde o início da série.

A insatisfação vem acompanhada de uma piora na percepção da direção da economia. O grupo dos que a veem no caminho errado, que vinha diminuindo a partir de abril, cresceu 4 pontos percentuais e chegou a 63%, mesmo patamar registrado em maio.

A visão contrasta com outros indicadores sobre a situação econômica: a percepção sobre as chances de manutenção de emprego, por exemplo, segue em tendência de alta desde maio. O grupo que vê possibilidade grande ou muito grande de continuar empregado chega a 56%.

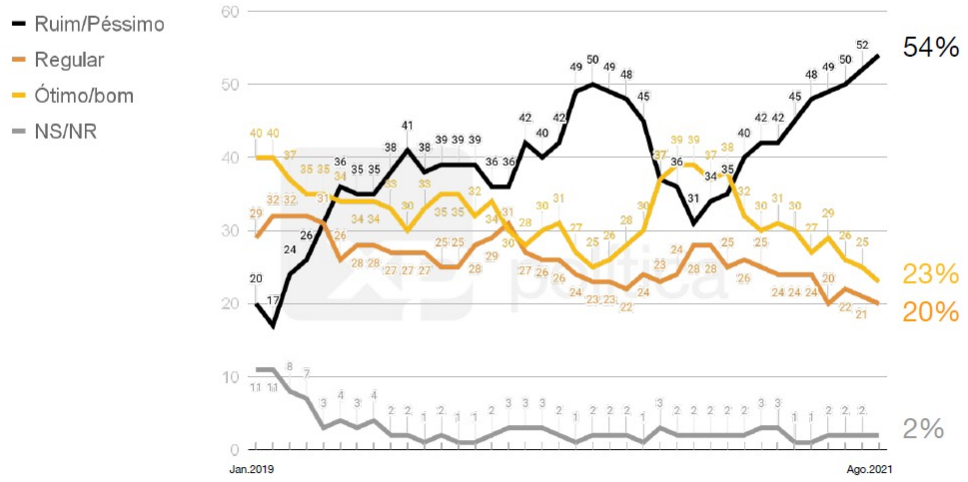
Print da Tela do Relatório da pesquisa XP/Ipespe, avaliação presidencial eleitoral 2022 - agosto 2021.

Creio que não precisamos falar mais nada. O derretimento está óbvio. Precisaria mudar radicalmente esta estratégia de confronto e radicalização, mas não acredito que isso aconteça, haja vista a teimosia e a inépcia de Bolsonaro e seus vassalos.

Reproduzimos a seguir mais telas da pesquisa XP/Ipespe, com os gráficos correspondentes.

Tendência permanece, e avaliação negativa da gestão Bolsonaro cresce a 54%

Como o sr. ou a sra. avalia o governo Jair Bolsonaro até o momento? Diria que está sendo:

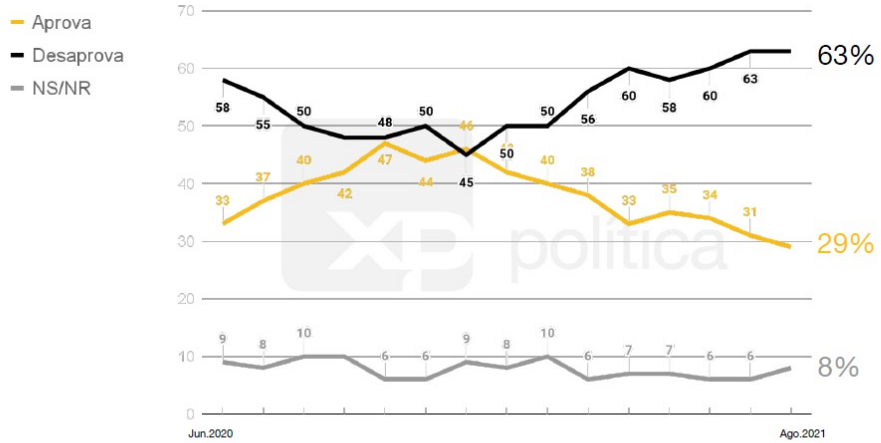


Fonte: pesquisa XP Ipespe Margem de erro de 3,2 p.p.

xp política 5

Desaprovação à administração Bolsonaro se mantém estável em 63%

O(a) sr.(a.) aprova ou desaprova a maneira como o presidente Jair Bolsonaro vem administrando o país?



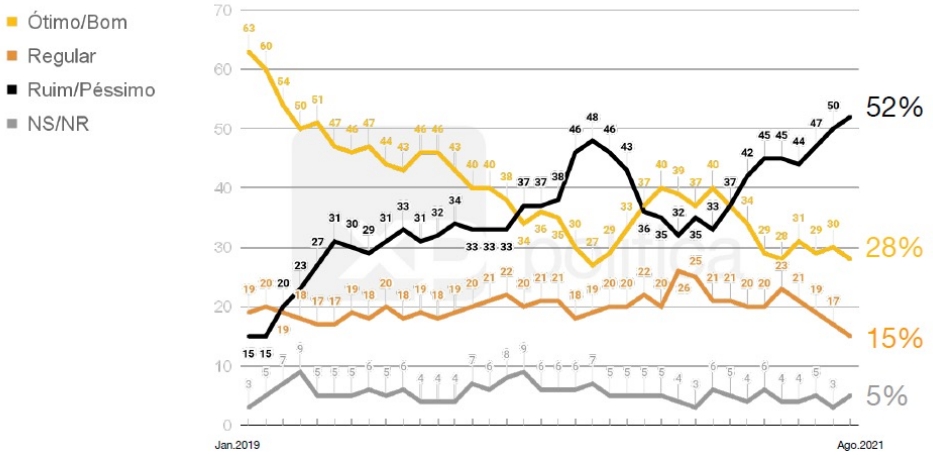
Fonte: pesquisa XP Ipespe Margem de erro de 3,2 p.p.

xp política 6

Print da Tela do Relatório da pesquisa XP/Ipespe, avaliação presidencial eleitoral 2022 - agosto 2021.

Expectativa negativa para restante do mandato de Bolsonaro cresce e vai a 52%

Pensando no restante do mandato, o(a) sr(a) acha que o presidente Jair Bolsonaro fará um governo:



Fonte: pesquisa XP Ipespe Margem de erro de 3,2 p.p.

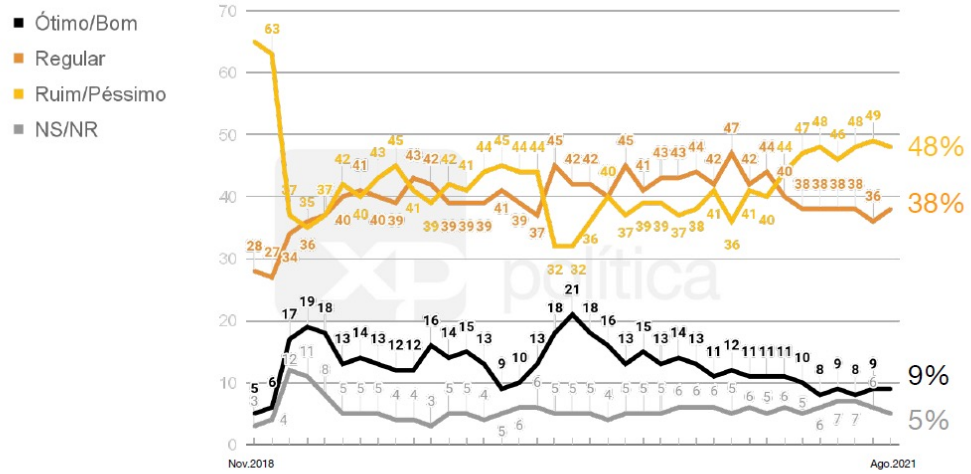
xp política 7

Print da Tela do Relatório da pesquisa XP/Ipespe, avaliação presidencial eleitoral 2022 - agosto 2021.

Os números acima demonstram que a população está insatisfeita com os rumos que o governo está dando para o Brasil.

Avaliação do Congresso segue estável; 48% veem atuação ruim ou péssima

Como o(a) sr(a) avalia o desempenho do atual Congresso Nacional?



Fonte: pesquisa XP Ipespe Margem de erro de 3,2 p.p.

xp política 10

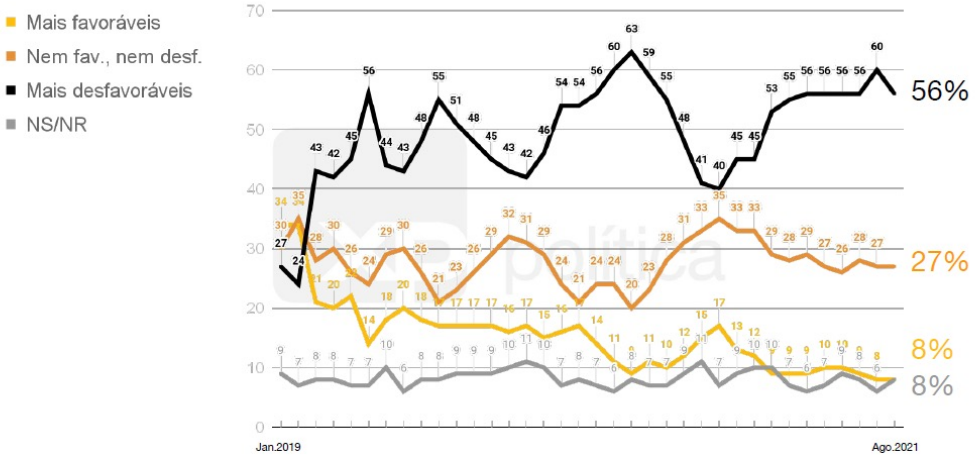
Print da Tela do Relatório da pesquisa XP/Ipespe, avaliação presidencial eleitoral 2022 - agosto 2021.

O slide acima demonstra que a população também está insatisfeita com a atuação do Congresso. Mesmo com a renovação, o presidencialismo de coalizão continua o mesmo, ou seja, as tão esperadas e prometidas mudanças simplesmente não aconteceram.

Outro ponto interessante é sobre as notícias veiculadas pela mídia. A população considera que o noticiário da mídia em geral não é favorável ao governo. Ou seja, a população considera que as notícias são mais negativas que os fatos em si, na minha interpretação.

Percepção de que noticiário é negativo para o governo recua 4 pontos e volta a 56%

Pelo que o(a) sr(a) sabe ou ouviu falar, as notícias que saíram recentemente sobre o governo federal e o presidente Jair Bolsonaro, na televisão, nos jornais, nas rádios e na internet foram:



Fonte: pesquisa XP Ipespe Margem de erro de 3,2 p.p.

xp política 12

Print da Tela do Relatório da pesquisa XP/Ipespe, avaliação presidencial eleitoral 2022 - agosto 2021.

Há na pesquisa ainda as simulações de 2º turno das eleições de Bolsonaro contra Lula e Bolsonaro contra outros candidatos. Bolsonaro perde para todos, sem exceção. É incrível essa percepção da sociedade brasileira. Há muitos votos brancos e nulos, mas o presidente perde em todas as simulações. É um grave sintoma de que algo não está bem. A equipe e o próprio Bolsonaro não enxergam isso. Será que não estão vendo que irão bater na muralha à frente? Será que não conseguem ajustar a rota que traçaram?

As eleições 2022 trarão a resposta, com certeza.

Para sintetizar o cenário que estamos vivenciando, cito 15 eventos futuros que, dependendo do desenrolar dos acontecimentos, poderão mudar os rumos das eleições de 2022. São eles:

1. *Alcance da Vacinação no Brasil contra o COVID 19;*
2. *Combate da variante Delta do COVID 19;*
3. *Crescimento do PIB – Crescimento econômico;*
4. *Inflação Alta;*
5. *PEC dos Precatórios;*
6. *Taxa de desemprego – Social;*
7. *Implantação do Programa Bolsa Família;*
8. *Efeitos Políticos da Crise Hídrica;*
9. *Desdobramentos das Investigações de Bolsonaro no TSE;*
10. *Desdobramentos do Resultado da CPI COVID 19;*
11. *Força do Movimento Pró-Impeachment;*
12. *Força do Movimento Pró-Bolsonaro;*
13. *Posicionamento das Forças Armadas diante do Cenário Político atual;*
14. *Viabilidade da Candidatura Terceira Via.*
15. *Aumento e Estabilidade de Rejeição do Governo Bolsonaro.*

Quando construímos a Matriz de Interdependência entre os eventos futuros, utilizando o Teorema de Bayes, Probabilidades Condicionais, podemos visualizar, na minha interpretação, o seguinte quadro:

Figura 3: Matriz de Interdependência – Eventos Futuros. Fonte: Software INTERISK

Temos 5 eventos considerados como Motrizes (influenciam todos os demais eventos futuros), 5 eventos considerados de ligação (influenciam os dependentes, são influenciados pelos motrizes e se influenciam reciprocamente, gerando grande instabilidade) e 5 eventos dependentes (influenciados tanto pelos Motrizes pelos de Ligação).

Neste quadrante de motricidade, temos 2 eventos relativos a quesitos da pandemia, que são primordiais para a retomada da economia, 2 eventos ligados à economia (que no cenário que se desenha deverá influenciar fortemente o aspecto econômico) e 1 evento relativo à rejeição de Bolsonaro, que poderá influenciar as questões políticas e o posicionamento das Forças Armadas.

Os 5 eventos Motrizes:

Cód.	Risco
R.96	Alcance da Vacinação no Brasil COVID 19
R.97	Combate a Variante Delta COVID 19
R.98	Crescimento do PIB - Econômico
R.99	Inflação Alta
R.110	Aumento e Estabilidade de rejeição do Governo Bolsonaro

Os eventos de ligação sofrem influência dos Motrizes e há forte conectividade entre eles. A PEC dos Precatórios tem viés político e é vital para a geração de caixa do Governo Federal. Os eventos políticos influenciam o posicionamento das Forças Armadas. Caso o resultado de alguma das diversas investigações em curso seja desfavorável a Bolsonaro, mesmo não ocorrendo qualquer tipo de punição, não haverá condições morais para que as Forças Armadas tomem um posicionamento a favor do presidente. E se a economia não caminhar, esta fator será decisivo para o aumento de rejeição de Bolsonaro e para o reforço do posicionamento das Forças Armadas.

Os 5 eventos de Ligação:

Cód.	Risco
R.100	PEC Precatórias
R.103	Efeitos Políticos da Crise Hídrica
R.104	Investigações Bolsonaro TSE
R.105	Resultado CPI COVID 19
R.108	Posicionamento das Forças Armadas - Cenário Atual

Os 5 eventos Dependentes:

Cód.	Risco
R.101	Taxa de Desemprego - Social
R.102	Implantação da Bolsa Família
R.106	Força Movimento Pró Impeachment
R.107	Força Movimento Pró Bolsonaro
R.109	Viabilidade da Terceira Via Presidencial

Os eventos dependentes são consequências dos resultados dos eventos localizados nos quadrantes de ligação e motriz. Por exemplo, a Viabilidade da Terceira Via Presidencial pode até surgir com outro viés, à semelhança do que ocorreu nas eleições passadas, quando Bolsonaro foi votado para que o PT não vencesse a eleição. Já está sendo ventilada a possibilidade de Lula não se candidatar e de o PT aliar-se à Terceira Via, visando aglutinar todos aqueles que estão contra Bolsonaro. Neste caso o Brasil poderia ter um clima

de união, não mais de polarização. Isso faria com que Bolsonaro perdesse já no primeiro turno. As manifestações pró e contra Bolsonaro dependem muito dos fatos que terão lugar nos próximos dias. Bolsa Família e outras pendências de natureza social dependem diretamente dos quesitos econômicos.

A Matriz de Interdependência nos orienta sobre onde temos que colocar a lupa para poder acompanhar os acontecimentos que estão por vir.

Na minha ótica, acredito que a cada dia que passa Bolsonaro fica mais isolado politicamente, perdendo aliados do próprio centrão, o que o deixa encurralado, com pouquíssimos caminhos a serem seguidos. Sua opção de tentar realizar uma ruptura institucional com suporte das Forças Armadas perde velocidade, o que pode gerar cada vez mais atitudes completamente desvairadas da parte dele.

Seu séquito de vassalos parece não enxergar esse isolamento, fruto de uma miopia ensejada pelo apego ao poder. Fazem tudo que o "chefe" manda, independentemente das incoerências e desvaneios dele. Não possuem coragem moral para saírem desse casulo.

Concluindo, podemos dizer que o Brasil é hoje detentor de um Risco Político e Econômico extremamente elevado, com recomendações exaradas por consultorias internacionais para que seus clientes investidores fiquem afastados do país, por uma questão de instabilidade social. A causa raiz dessa instabilidade social é o apego míope ao poder, que motiva o presidente a realizar ações puramente populistas.

Infelizmente, o Brasil perdeu mais uma oportunidade. Mais uma porta se fechou para o povo brasileiro em sua caminhada em direção a melhores condições de vida.

Concluo este artigo citando Rui Barbosa, autor de conferências notáveis sobre a fiscalização do poder. No livro "A Imprensa e o Dever da Verdade", em que reúne uma série de conferências descrevendo o que cabe à imprensa no que toca à fiscalização do poder, ele descreve como os homens públicos, justamente por serem públicos, estão submetidos

ao escrutínio da imprensa e dos cidadãos. Escreveu Rui Barbosa:

> *"O poder não é um antro, é um tablado. A autoridade não é uma capa, mas um farol. A política não é maçonaria, e sim uma liça. Queiram ou não queiram, os que se consagram à vida pública, até à sua vida particular deram paredes de vidro...Para a nação não há segredos; na sua administração não se toleram escaninhos; no procedimento dos seus servidores não cabe mistério; e toda encoberta, sonegação ou reserva em matéria de seus interesses importa, nos homens públicos, traição ou deslealdade aos mais altos deveres do funcionário para com o cargo, do cidadão para com o país."*

Incrível que as palavras acima, escritas há mais de 100 anos, ainda precisem ser lidas em voz alta para toda a nação brasileira, como nos dias que correm. Bolsonaro, na minha visão, ultrapassou todos os limites da ética e da responsabilidade em relação aos brasileiros que nele votaram, a todos desprezando na sua caminhada em prol de um projeto de poder pessoal e familiar.

Espero que ele naufrague no seu intento, torço para que isso aconteça, pelo bem dos brasileiros, em particular pelo bem dos meus filhos e netos.

Boa Leitura!

Antonio Celso Ribeiro Brasiliano

Publisher da Revista Gestão de Riscos e presidente da Brasiliano INTERISK - abrasiliano@brasiliano.com.br

Conheça já a solução INTERISK!

Com ela você faz análise de riscos de diferentes áreas da empresa, e conta com um sistema totalmente automatizado e parametrizável.

Como diferenciais temos:

- **Integra as inúmeras disciplinas de riscos corporativos, de forma automatizada - única no mercado;**
- **Realiza a interconectividade entre riscos - única no mercado;**
- **Identifica o apetite ao risco ajudando a determinar quais riscos a sua organização está disposta a assumir - diferencial único no mercado;**
- **Filtra um volume muito grande de informações;**
- **Automatiza ferramentas e métricas de Gestão de Riscos Corporativos; e**
- **Licença ilimitada.**

Saiba mais!

SOFTWARE INTERISK
Inteligência em Riscos

Cláudio dos Santos Moretti, CES, ASE
Diretor da CSM – Consultoria e Treinamento em Segurança Empresarial | claudio_moretti@uol.com.br

Mundo líquido - a era da informação, fake news e desinformação

O mundo mudou, ou melhor, o mundo vem mudando a cada dia.

Alvin Toffler, em seu livro A Terceira Onda (1980), descreve a evolução social como três ondas, sendo a primeira a da agricultura, onde o que tinha valor era a terra e o homem, sua força muscular. Na segunda onda o que prevalecia eram as máquinas e o homem, a era industrial. Na terceira onda, o que prevalece é a informação, o conhecimento, a imagem, enfim aquilo que é intangível, onde uma imagem, uma ideia uma criação ou inovação tem muito mais valor do que os produtos tangíveis, as fábricas, as máquinas etc.

A premissa é que o homem, ou melhor seu cérebro, suas ideias, sua imaginação, seus insights têm muito mais valor que a sua força, que as terras ou que as máquinas.

Um breve exemplo: No dia 14/06/21, o jogador de futebol Cristiano Ronaldo, CR7, numa entrevista, afastou as garrafas da Coca-Cola que estavam sobre a mesa. Esse gesto, pensado ou não, acabou por trazer uma perda de US$ 4 bilhões no valor de mercado da Coca-Cola, ou pelo menos ajudou nessa queda. Observem que a Coca-Cola não deixou de produzir nenhuma garrafa do produto e não fechou nenhuma fábrica, mas trinta minutos depois dessa atitude do jogador ela perdeu 1,6% no valor de suas ações. Apenas uma imagem, uma ideia, uma atitude. Coca-Cola

Toffer, em 1980, já antevia diversas mudanças sociais e tecnológicas.

Sua visão demonstrava, entre outras coisas, o uso extremado da tecnologia, não apenas na indústria, mas também na vida social, como é hoje. Os novos estilos de família, de trabalho, de economia, de conflitos políticos e comportamentos, além de escolas e empresas seriam radicalmente modificados.

Ele tinha esta visão em 1980 e hoje vemos os reflexos disso principalmente nas redes sociais e na importância que elas ganharam com aquilo que Zygmunt Bauman chamou de Mundo Líquido, onde as formas não existem ou pelo menos não são duradouras, nem produtos, nem relacionamentos, nem parcerias.

A conexão mundial trouxe para mais perto de todos nós e de todos os negócios aquilo que é conhecido como efeito borboleta, onde o bater das asas de uma borboleta pode resultar num tsunami do outro lado do mundo.

Hoje a informação é disponível em todo o mundo e ao mesmo tempo por conta da rede mundial de computadores, a internet.

Hoje, por conta da internet, a informação está disponível para todos em tempo real.

Internet

É certo que a internet trouxe enormes benefícios para toda a sociedade, ou pelo menos para a grande maioria que tem acesso a ela.

Mas apesar de a internet estar disponível desde a década de 1970, com maior uso doméstico no Brasil a partir da década de 1990, com a abertura do mercado, acredito ser uma tendência cada vez maior do seu emprego tanto nos negócios como na vida pessoal de cada um. Uma amostra disso é a IOT - Internet of Things ou Internet das Coisas.

Cada vez estamos mais dependentes da internet, em todos os aspectos.

Com o uso maciço e o advento das redes sociais como o Facebook, Instagram, twitter etc. a conexão entre usuários domésticos cresceu exponencialmente e demonstra sua força nas marcas, reputações, imagem, ideologias, etc.

Muitas pessoas ainda não perceberam a forma de atuação das redes sociais, nas quais, basicamente, temos três funções distintas:

- A primeira delas é como clientes, pagando pelas informações ou acessos a determinados conteúdos que achamos relevantes.
- A segunda é como funcionários das redes sociais, onde você posta conteúdos que irão gerar "likes", também quando curtimos algum conteúdo postado por outro "funcionário", quando compartilhamos conteúdos gratuitamente, as vezes a serviço de outros usuários, às vezes para serviços de IA - Inteligência Artificial, que alguém recebe por isso, etc. Ou seja, estamos trabalhando, produzindo, curtindo ou transferindo, compartilhando.
- A terceira função é como produto. Nós somos produtos para sermos utilizados por programas da IA, nossos dados são comercializados e podem ter propósitos de negócios, publicidade paga dos anunciantes, de políticos ou criminosos.

Como foi citado no documentário da Netflix, Privacidade Hackeada, 2019, "se você não está pagando, você é o produto".

As três funções citadas são utilizadas para ganhos, para os usuários, sim, o mesmo nome utilizado para quem é viciado em drogas, os dependentes químicos.

Nesse caso, pessoas fazem uso de forma viciante e não conseguem diminuir ou se livrar dessas drogas (as redes sociais).

Isso não quer dizer que elas sejam ruins ou que todos deveriam abandoná-las. Eu mesmo utilizo as redes sociais com frequência.

Os problemas em relação ao uso das redes é não entender o seu funcionamento, as regras do jogo, e eu vou apresentar algumas.

Inteligência Artificial

No livro Os Algoritmos Satânicos - O lado sombrio das redes sociais de Jair Lorenzetti Filho, 2021, o autor divide a rede em três áreas, que ele chama de "pessoas", sendo que a primeira se chama big data (nuvem de dados), que nada mais é que a nuvem onde eles guardam e organizam nossos dados, para as outras áreas usarem.

Ele exemplifica como se a big data fosse o arquivista de biblioteca da Inteligência Artificial.

A segunda área é o deep learning (aprendizado profundo), basicamente é como um vendedor comum, que passa o tempo todo monitorando todas as nossas "curtidas", buscas, preferências, enfim, analisando nosso comportamento.

E a última é a mais experta, o machine learning (aprendizado de máquina). "Este é um daqueles vendedores muito ligeiros, que usam aqueles recursos de vendas dos "universitários", conduzin-

do você até comprar o que eles querem. Por exemplo, a técnica do sim, onde eles vão lhe falando coisas que você vai sempre dizer sim, até a última que é para você comprar o que eles estão lhe vendendo. Se você não comprar ele começa sempre tudo novamente do zero, até você comprar. Sendo esperto e repetitivo ele lhe convence de qualquer coisa".

É por isso que quando você se interessa por um determinado produto, um tênis, por exemplo, ele passa a aparecer em todos os sites que você visita, sugerindo preços ou apresentando novos modelos.

Nós somos categorizados de acordo com nossas preferências, buscas e likes.

O que ocorre é que por nossos interesses, outros interessados "semelhantes" nos são "apresentados". Quer dizer que se você gosta de cães, por exemplo, os perfis com o mesmo interesse acabam aparecendo para você, em seu perfil e tudo o que for favorável a ele também. Dessa forma você fica numa "bolha", onde todas as postagens e notícias sobre o tema lhe serão apresentados sem que você perceba. O pessoal da área de marketing chama isso de bolha de filtragem.

A forma de fugir dessa bolha é observar perfis opostos, sejam produtos, ideologias, políticas etc. Do contrário, depois de algum tempo, você não conseguirá "enxergar" fora da bolha.

Desinformação

A desinformação sempre existiu, mas nem sempre foi percebida pela sociedade e a desinformação NÃO é uma informação acidentalmente enganosa, ela é feita de maneira proposital, com a finalidade de enganar.

Em muitos casos a desinformação vem inserida no contexto de uma informação verdadeira, que serve para lhe dar credibilidade. Então uma notícia real servirá como cavalo de Tróia para levar a informação falsa, a desinformação.

Desinformação tem diversos conceitos, como por exemplo, no livro Pequena história da desinformação de Vladimir Volkoff, 2004: "O termo surge no inglês (disinformation) em 1972 no Chambers Twentieth Century Dictionary em Londres com a seguinte definição "vazamento proposital de informações enganosas".

Operações Psicológicas

É o termo utilizado nos serviços de Inteligência para as técnicas que envolvem desinformação e propagandas enganosas. Essas técnicas foram muito utilizadas durante a segunda a Guerra Mundial (1939 – 1945) e durante o período da Guerra Fria (1947 – 1991). Os fundamentos das Operações Psicológicas são a indução de comportamentos e a influência nas ideias e conceitos que as pessoas receberão através da disseminação dessas cam-

panhas de propaganda que são manipuladas para persuadir a população.

Isso foi feito antes do advento da internet e, assim como ocorreu com a Atividade de Inteligência Competitiva, desenvolvida após o fim da Guerra Fria, as Operações Psicológicas também se adaptaram, principalmente com o uso das redes sociais.

Basta lembrar que a maior fonte de recrutamento do terrorismo são as redes sociais.

Boatos e Fake News

Os boatos e fake News podem ser entendidos como a desinformação em forma de notícias.

São disseminadas como memes, notícias fabricadas para uso de grupos extremistas.

Elas sempre foram utilizadas em campanhas políticas ou disputas, mas foi a partir de 2016, na eleição dos EUA, que elas ganharam força.

As redes sociais são campos férteis para a disseminação de boatos, fake news e as mentiras do dia a dia, principalmente depois que começou a ser utilizada de forma intensiva por políticos.

Um exemplo foi publicado pelo jornal The Washington Post, do dia 23 de janeiro de 2021. Donald Trump fez 30.573 afirmações falsas ou enganosas como presidente. Quase metade veio em seu último ano.

Deepfake

A tecnologia não para. Dia a dia vemos o seu desenvolvimento para o bem e para o mal. Nesse caso, essa ferramenta cumpre dois propósitos: o Deepfake é uma técnica que altera o visual, ou seja, altera o rosto de uma pessoa, por exemplo e faz uma montagem perfeita como se outra pessoas estivesse naquele vídeo.

De acordo com o livro Fake News: A Liberdade de Expressão nas Redes Sociais na Sociedade da Informação de André Faustino, 2019, a DeepFake apareceu pela primeira vez no outono de 2017, como um roteiro usado para gerar conteúdos adultos com troca de rosto. Depois, essa técnica foi aprimorada por uma pequena comunidade para criar um aplicativo amigável chamado FakeApp.

Com esse software a identificação das Fake News fica muito mais difícil, primeiro porque agora não são apenas fotomontagens que podiam ser facilmente identificadas, mas contam também com os vídeos e, principalmente porque muitos entendem que elas são “apenas uma forma de expressão” e, desse modo, continuam a se propagar nas redes.

Pós-verdade

Pós-verdade pode ser conceituada como afirmações, senten-

ças, ideologias sem qualquer lógica ou até mesmo conexão com a realidade.

Os fatos objetivos têm menor influência que os aspectos emocionais e as crenças pessoais.

As pessoas adotam essa ideologia e a repetem como um mantra sem prestarem atenção nos argumentos contrários, por mais válidos, lógicos e fundamentados que sejam, simplesmente ignoram.

Ou seja, a narrativa vale mais do que a verdade dos fatos.

Não foi à toa que a palavra pós-verdade (post-truth) foi considerada a palavra do ano (2016) na Universidade de Oxford, onde anualmente o Oxford Dictionaries, departamento da universidade responsável pela elaboração de dicionários elege uma palavra de maior destaque da língua inglesa.

Infodemia

A palavra refere-se a uma junção das palavras informação com epidemia.

A palavra infodemia se refere a um grande aumento no volume de informações associadas a um assunto específico, que podem se multiplicar exponencialmente em pouco tempo devido a um evento específico, como a pandemia atua, principalmente pelo uso das redes sociais.

Nas redes os rumores e desinformação, medos e supersti-

ções se espalham, se multiplicam por pessoas que não fazem nenhum tipo de checagem das informações.

Neste caso, pode induzir pessoas a cometerem erros que podem trazer problemas de saúde ou ampliar uma epidemia.

Conforme declarado pela OMS – Organização Mundial da Saúde, “o surto de COVID-19 e a resposta a ele têm sido acompanhados por uma enorme infodemia: um excesso de informações, algumas precisas e outras não, que tornam difícil encontrar fontes idôneas e orientações confiáveis quando se precisa”.

Alguns critérios para Identificar Mentiras

O professor Mike Caulfield, da Universidade do Estado de Washington orienta que se faça uma leitura lateral, que é a busca de outras fontes. Ele diz que normalmente se faz uma leitura vertical, em que lemos todo o texto e ficamos com apenas um lado da história. O ideal é pesquisar outras fontes, fazer novas leituras e tirar suas próprias conclusões.

Marianna Zattar apresenta algumas possibilidades de identificação de mentiras a partir das perguntas: Quem? Qual? Onde? Quando? Por quê? Como?

Quem publicou? Quem se beneficia ou pode ser prejudicado(a) com essa informação? Quem toma decisões sobre esse assunto? Quem são as pessoas chaves nesse assunto?

Qual o objetivo dessa informação? Qual é a outra perspectiva ou alternativa? Qual seria um contra-argumento? Qual é o cenário dessa informação?

Onde foi publicado? Onde estão as definições e situações similares? Onde isso foi compartilhado ou disseminado? Onde achamos mais informações? Onde essa ideia vai nos levar?

Quando isso foi publicado? Quando isso foi novo? Quando isso foi atualizado? Quando isso foi compartilhado/disseminado?

Por que essa informação foi criada? Por que isso é relevante? Por que as pessoas devem saber isso? Como sabemos que isso é verdade? Como sabemos que isso é falso? Como essa informação beneficia ou prejudica alguém?

Além disso, ainda existem os sites de checagem de notícias, como por exemplo:

www.boatos.org, www.aosfatos.org e o www.e-farsas.com e www.lupa.com, www.fatooufake.com e outros.

Conclusão

A sociedade está muito mais interligada com o mundo tanto entre as pessoas como entre os negócios e além dessa interrelação ainda temos a polarização política que tem seu viés positivo. Hoje as pessoas sabem mais os nomes dos onze ministros do STF – Supremo Tribunal Federal do que dos onze jogadores titulares da seleção brasileira.

Em qualquer formato, as mentiras com nomes diferentes continuarão até porque sempre existiram, fazem parte do comportamento humano e da convivência em sociedade, querendo ou não.

Mas o melhor é tentar identificar e sair da bolha ou sair da caverna, conforme lembraria Platão.

De qualquer modo, é sempre bom lembrar que aquilo que você posta nas redes sociais pode ser “guardado” por interessados e usado no futuro contra você.

Além disso, quando você dissemina mentiras nas redes sociais você perde credibilidade e a verdade sempre aparece.

Novidade no ar!!

Agora, a Brasiliano INTERISK também está presente no Instagram. Vamos levar até você sempre conteúdos exclusivos para deixá-lo por dentro de todas as novidades nas áreas de Compliance, Gestão de Riscos e Controles Internos.

Acesse o link abaixo, conheça o nosso perfil e nos siga nessa jornada de conhecimento!

Acesse agora!!

Brasiliano INTERISK
Inteligência em Riscos

Carlos Köhler
Graduado em Segurança Pública, pós-graduado em Segurança Privada, CEO do Grupo CINDAPA, CPSI, CISI, MBS e CRA.

O que traz a sensação de segurança em condomínios

Com frequência ouvimos a pergunta de síndicos, comitês de segurança e condôminos, sobre o que traz a sensação de segurança, se são os alarmes, câmeras, reconhecimento facial, vigilantes armados, ou fortes controles, entre tantos outros.

A segurança e sensação de segurança têm sido tema de estudos, tanto de profissionais de segurança privada quanto pública, e cabe nossa consideração sobre o assunto.

Este artigo se limita a uma breve reflexão sobre o que traz a sensação de segurança privada e não os condicionantes da segurança pública e privada. Assim sendo, discorreremos sobre a diferença entre estes termos no viés da segurança dos moradores em condomínios.

A resposta a esta pergunta merece muita consideração, pois o bem-estar e a vida das pessoas estão sendo afetadas. Mesmo que uma pessoa nunca tenha sido vítima, por exemplo, de roubo, poderá ter receio de que isso venha a ocorrer com ela um dia, causando medo e ansiedade, afetando a felicidade, a saúde, enfim, a vida das pessoas.

Segundo o dicionário Aurélio, sensação é uma "impressão causada num órgão receptor por um estímulo e que, por via aferente, é levada ao sistema nervoso central". Então, a sensação é causada por um estímulo sensorial, que pode ter diferentes reações para cada pessoa, pois há quase 8 bilhões de pessoas no mundo e cada uma diferente da outra, passando por experiências únicas.

Vejamos o exemplo de uma pessoa que reside em condomínio privado e seria vítima de roubo e que, pela ação de um vigilante que dissuadiu a ação criminosa, os vigilantes são aqueles que proporcionam essa sensação de segurança. Agora vejamos um outro exemplo em que uma pessoa que seria roubada e o criminoso foi dissuadido por ter sido visualizado pelas câmeras de videomonitoramento na tentativa de subir o muro para invadir a residência e cometer o roubo. Para esta pessoa é bem mais provável que a sensação de segurança seja proporcionada pelas câmeras de videomonitoramento.

Ambas tiveram estímulos diferentes, proporcionando experiências diferentes e, por consequência, respostas diferentes. São apenas exemplos que servem como uma metáfora para compreendermos como o indivíduo percebe a segurança a seu redor, é lógico que a ciência tem muito mais para explicar cada estímulo, mas, para entender esse contexto, é o suficiente.

E se nenhuma delas tiver passado por qualquer tipo de experiência, que estímulos lhe dariam a sensação de segurança? Podem ser inúmeros, principalmente a pré-disposição genética, o meio e as escolhas, entre outros; assim sendo, as sensações de segurança são diferentes para cada pessoa ou grupo de pessoas pelos estímulos a que esteve exposta. Há pessoas que foram afetadas pelas experiências e traumas que outras tiveram, umas se sensibilizam mais que outras. Assim, pela diversidade de pessoas e situações, nossos estímulos são mais ou menos afetados por determinada situação.

O que dá a sensação de segurança para um pode não proporcionar a mesma sensação para outro e vice-versa, assim como o que resolveu algum problema de segurança numa determinada situação não necessariamente resolverá o mesmo problema em outras situações. Da mesma forma, o que deu certo para um contexto não necessariamente vai dar certo para outro.

Outra analogia que podemos fazer é em relação a uma pessoa que se sente muito bem, muito disposta e ativa, crendo que sua saúde está excelente. Essa sensação de saúde não quer dizer que ela não esteja na iminência de um infarto causado por colesterol altíssimo. Assim sendo, a "sensação de saúde" pode nos enganar, é preciso conhecimento que só um especialista, como um médico, tem para poder diagnosticar e tratar.

Assim também acontece na área da segurança. Essa "sensação" pode não condizer com a realidade quando falta conhecimento, podendo levar a decisões erradas que comprometem a sua vida e a dos outros.

Por outro lado, a "sensação de segurança" de um profissional de segurança será baseada no conhecimento e experiências adquiridos ao longo dos anos, diferente de uma pessoa leiga com pouca ou nenhuma experiência que não dispõe das condições adequadas para oportunizar segurança.

Segurança é diferente de "sensação de segurança", enquanto segurança é a condição para que não haja perigo para pessoas ou bens, a "sensação de segurança" depende de cada pessoa e está associada aos estímulos que ela recebeu no decorrer de sua vida, ou seja, a "sensação de segurança" está relacionada à subjetividade do indivíduo, enquanto a segurança é científica.

REFERÊNCIAS

Ferreira, A. B. (2010). DICIONÁRIO DA LÍNGUA PORTUGUESA (5° ed.). Curitiba, PR: Editora Positivo.

Köhler, C. A. (2017). GESTÃO DA SEGURANÇA PATRIMONIAL: aplicação do método PDCA. São Paulo, SP, Brasil: Sicurezza.

Sua empresa conta com um plano dos possíveis Cenários Prospectivos que possam impactar no futuro dela?

No módulo de Cenários Prospectivos – CP do Software INTERISK, sua organização conta com uma ferramenta que auxilia no levantamento dos possíveis cenários dando uma visão ampla na avaliação das incertezas críticas que podem impactar nos objetivos da sua empresa.

Veja alguns diferenciais do Módulo CP:

- **Definição dos Eventos Futuros e Atores;**
- **Classificação dos Eventos - Método Delphi;**
- **Elaboração da Matriz de Impactos Cruzados;**
- **Elaboração da Matriz de Classificação dos Eventos;**
- **Entre outras vantagens.**

Conheça a metodologia!!

SOFTWARE INTERISK
Inteligência em Riscos

Gustavo Vedove
Especialista de Riscos, GCN e Proteção de Dados

Método para mensuração do NRGCN - Nível de Resiliência em Gestão de Continuidade de Negócios

Muito se aprendeu sobre GCN – Gestão de Continuidade de Negócios com a Pandemia da COVID-19 e o termo resiliência, apesar de ser antigo no linguajar dos negócios e da gestão de riscos, passou a ser muito citado. Nessa esteira, tivemos em 2020a atualização da ISO 22301:2013 (Segurança da sociedade — Sistema de gestão de continuidade de negócios) para ISO 22301:2020 (Segurança e resiliência — Sistema de gestão de continuidade de negócios). Por isso, resolvi criar um método para mensurar o nível de resiliência em Gestão de Continuidade de Negócios das empresas.

O método consiste em mensurar o nível de preparação da empresa para responder aos cenários de interrupção com potencial de crise, aos quais o negócio está exposto. Logo, uma boa análise de riscos para identificação destes cenários, é chave para o sucesso da correta mensuração.

VAMOS AO PROCESSO E METODOLOGIA!!!

DESCRIÇÃO DO PROCESSO

O nível de resiliência consiste de um indicador que consolida o resultado de todo programa de gestão de continuidade de negócios, levando em conta a estrutura existente, para responder aos cenários de interrupção.

O método é dividido em duas partes:

Parte 1	Parte 2
Requisitos do Programa de GCN (Gestão de Continuidade de Negócios) • Documentação; • Preparação das Pessoas; • Follow-up para Melhoria Continua.	**Capacidade de Pronta Resposta e Continuidade frente aos cenários de interrupção** • Estrutura Física; • Estrutura Tecnológica; • Estrutura de Supply Chain; • Pessoas; • Cenários de Negócio; • Disponibilidade de Recursos.

A parte 1 já é muito praticada no mercado, pois foca em avaliar a aderência da empresa às boas práticas de continuidade de negócios, tomando como base o atendimento aos requisitos das principais normas, ou seja, é uma avaliação do Programa de GCN. Os três temas que avaliamos na parte 1 são documentação, preparação das pessoas e ciclo de revisões.

Já na parte 2, são avaliadas as questões relacionadas à capacidade da empresa para responder aos cenários de interrupção e ameaça. Esta é a parte inovadora do método. São dadas notas por cenário, considerando a avaliação dos recursos e os planos existentes para atuar em contingências e gestão de crises.

Cada item de avaliação tem um peso proporcional à sua importância, peso este que a empresa deve estabelecer de acordo com seu entendimento.

Abaixo os critérios de avaliação:

Legenda dos Critérios de Avaliação		
Nota	**Classificação**	**Definição**
4		Muito satisfatório
3		Satisfatório
2		Parcialmente satisfatório
1		Estrutura apresenta gaps importantes
0		Insatisfatório

Cada item será avaliado na escala de 0 a 4. O método é subjetivo, cabendo ao avaliador estabelecer o critério de classificação conforme suas verificações, no âmbito do que a empresa possui formalizado e implementado. O método prescreve, até mesmo por uma questão de registro da condição avaliada, a necessidade de preencher as justificativas relativas a cada item.

Abaixo temos a demonstração do quadro de avaliação, com exemplos de itens a serem avaliados, cada um com seu peso, organizados por tema e divididos segundo as óticas de atendimento ao programa GCN e à preparação da empresa para responder aos cenários de interrupção (Parte 1 e 2). Pontos importantes:

a) As perguntas são apenas exemplos. O número de questões não está limitado à quantidade e a empresa pode "customizar" o assessment, incluindo suas questões, desde que alinhadas aos requisitos das normas e coerentes com os cenários aos quais está exposta.

b) O preenchimento das justificativas é somente para exemplificar, cabe ao especialista de GCN/Riscos detalhar os aspectos avaliados.

c) A premissa é colocar somente as principais questões a serem avaliadas, partindo do pressuposto de que, para chegar ao resultado, outras fases das normas de GCN já foram realizadas na organização. O objetivo do método é avaliar as questões mais relevantes.

d) Os cenários colocados são apenas exemplos. O número de cenários não está limitado a essa quantidade. A orientação é no sentido de que os cenários empregados sejam fruto da análise de riscos e envolvimento com a alta gestão, para que a avaliação seja específica da empresa. Somente assim será possível obter do estudo uma avaliação precisa do quanto a empresa está preparada para responder aos cenários que possam impactar a continuidade de seus negócios.

e) Conforme os itens C e D, o objetivo é ter uma avaliação focada, objetiva e customizada à realidade de riscos de continuidade aos quais a empresa está exposta, sem estender muito o check list de assessment, mantendo perguntas bem direcionadas e que realmente têm peso e relevância, para saber se a empresa tem seu Plano de Continuidade bem estruturado, oriundo de um bom diagnóstico realizado mediante a aplicação de técnicas reconhecidas.

Quadro de avaliação do nível de resiliência da empresa contra eventos que possam gerar interrupção dos negócios:

Parte 1 - Avaliação relacionadas aos requisitos do programa de GCN

	Requisitos avaliados	Peso	Nota	Total	Justificativas	Classificação
	Documentação					
1	Existe política e processo de GCN, atendendo às normas e boas práticas, com critérios definidos, para avaliação dos processos e sistemas críticos da empresa?	2	3	6	Nível satisfatório, tendo em vista que a empresa possui política e processo de GCN formalizados, atualizados e seguindo as boas práticas, com critérios estabelecidos para avaliação dos processos e sistemas críticos de negócio.	Satisfatório
2	Existe um estudo formalizado de análise de riscos por *site*, seguindo boas práticas, com critérios definidos?	3	3	9		Satisfatório
3	O BIA (*Business Impact Analysis*) é atualizado anualmente? A criticidade dos processos é avaliada sob a ótica de impacto no negócio e tempo máximo de indisponibilidade seguindo boas práticas?	3	4	12		Muito Satisfatório
4	Os cenários que podem causar interrupção nas atividades da empresa estão avaliados de forma atualizada, conforme a realidade das operações?	2	4	8		Muito Satisfatório
				35		
	Como está a preparação dos funcionários para lidar com os cenários de interrupção identificados?	Peso	Nota	Total	Justificativas	Classificação
5	Os funcionários foram treinados / sabem como agir em caso de concretização dos cenários?	3	3	9		Satisfatório
6	São ministradas palestras de GCN para todas as áreas da empresa?	2	3	6		Satisfatório
7	As áreas críticas participaram de testes de GCN no último ano?	3	2	6	Não foi possível testar todas as áreas críticas no ano. Não é garantido que as áreas críticas estejam aptas em relação aos procedimentos e estrutura de continuidade. Além disso, não foram feitos testes de mesa com a alta gestão.	Parcialmente Satisfatório
				21		
	Melhoria Contínua	Peso	Nota	Total	Justificativas	Classificação
8	Existe um processo de implementação de medidas mitigatórias para reduzir os riscos críticos conforme resultado da análise de riscos?	3	3	9		Satisfatório
9	Há investimento em recursos para sanar *gaps* que possam impossibilitar a execução dos planos de resposta a emergências / contingência por site?	3	2	6		Parcialmente Satisfatório
10	Os procedimentos são revisados conforme resultado dos testes e/ou mudança na empresa/contexto, visando deixá-los mais completos e seguros?	3	2	6		Parcialmente Satisfatório
11	São feitos investimentos em infraestrutura e tecnologia visando melhorar o nível de segurança e redundância da empresa, conforme novas ameaças e resultado dos testes de PCN?	4	1	4		Regular
				25		

Parte 2 - Capacidade de pronta resposta aos cenários de interrupção						
	Existe estrutura física de redundância / contingência para continuidade dos negócios de acordo com os cenários identificados?	Peso	Nota	Total	Justificativas	Classificação
	12 Indisponibilidade do site A	4	3	12		Satisfatório
	13 Indisponibilidade do site B	4	2	8		Parcialmente Satisfatório
				20		
	Existe estrutura tecnológica de redundância / contingência para continuidade de negócios de acordo com os cenários identificados?	Peso	Nota	Total	Justificativas	Classificação
	14 Indisponibilidade do sistema X	5	3	15		Satisfatório
	15 Indisponibilidade do sistema Y	6	2	12		Parcialmente Satisfatório
	16 Indisponibilidade do sistema Z	5	1	5		Regular
				32		
	Disponibilidade de recursos	Peso	Nota	Total	Justificativas	Classificação
	17 Todos os funcionários chaves, dedicados ao PCN, possuem notebook habilitado para trabalho remoto?	2	2	4		Parcialmente Satisfatório
	Requisitos avaliados	Peso	Nota	Total	Justificativas	Classificação
	18 A empresa dispõe de notebooks reservas habilitados e atualizados em local alternativo ao local de trabalho para suprir a necessidade dos funcionários chaves, dedicados ao PCN?	2	0	0	A empresa não tem equipamentos reservas, portanto, em um cenário de impossibilidade de acesso ao site X, cuja causa seja um incêndio que comprometa toda a edificação, a continuidade de negócios ficará comprometida.	Insatisfatório
	19 Os funcionários chaves, dedicados ao PCN, aderem ao procedimento de levar diariamente o notebook para casa, visando ter a ferramenta disponível em caso de impossibilidade de acesso ao site original?	3	1	3		Regular
				7		
	TOTAL			140		

Conforme avaliação de cada item através das notas, é feito o cálculo que resulta em uma escala de 1 a 5 níveis para chegar ao indicador de resiliência.

A nota é multiplicada pelo peso e cada item é somado, podendo gerar as informações em duas categorias:

- Indicador por categoria; e
- Indicador geral (Nível de Resiliência da Empresa).

Neste processo, como o objetivo principal é fazer uma avaliação customizada da empresa, haverá variação na quantidade de itens a serem avaliados (Perguntas). Desta forma, as escalas de classificação dos indicadores por categoria e geral irão apresentar discrepâncias e devem ser adaptados.

Segue abaixo a metodologia:

- Verificar o resultado máximo possível e traçar um range de 5 intervalos, mantendo coerência na divisão das pontuações mínimas e máximas. Os intervalos entre as pontuações irão determinar os níveis de classificação. Abaixo o exemplo, considerando o quadro supracitado.
- Nota máxima (248) dividida por 5 (quantidade de níveis de classificação) = 49,6
- Intervalo entre os níveis: manter o mais próximo da pontuação que representa 1/5.

Visão Indicador da Empresa

Legenda do Nível de Resiliência					
Nota	Classificação	Escala		Resultado da Avaliação	
		Mínimo	Máximo	Indicador	Nota
4	Muito satisfatório	198,8	248	Parcialmente satisfatório	140
3	Satisfatório	149,1	198,7		
2	Parcialmente satisfatório	99,4	149		
1	Regular	49,7	99,3		
0	Insatisfatório	0	49,6		

Visão Indicador por Categoria

Documentação					
Nota	Classificação	Escala		Resultado da Avaliação	
		Mínimo	Máximo	Indicador	Nota
0	Insatisfatório	0	8	Muito Satisfatório	35
1	Regular	8,1	16		
2	Parcialmente satisfatório	16,1	24		
3	Satisfatório	24,1	32		
4	Muito satisfatório	32,1	40		

Cada nível de classificação deve ter uma definição, esclarecendo os aspectos que as justifiquem, por tema, assim, para fins de auxílio, elaborei alguns direcionadores para enquadramento. Ver quadro abaixo “Critérios de avaliação por nível de classificação”.

O objetivo é definir por nível de classificação o grau qualitativo dos itens atendidos, conforme o grau de avaliação das partes 1 e 2 (requisitos das normas e capacidade de pronta reposta, respectivamente) do assessment do nível de resiliência.

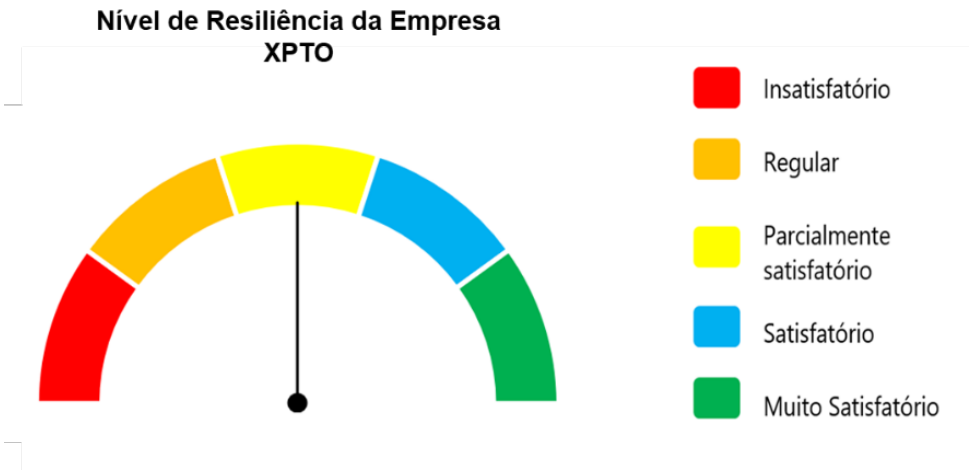
Critérios de avaliação por nível de classificação

	4	3	2	1	0
Avaliações	**Muito satisfatório**	**Satisfatório**	**Parcialmente satisfatório**	**Regular**	**Insatisfatório**
a) Atendimento aos requisitos das normas e as documentações estão atualizadas (Política GCN, BIA, PCN)	Atende todos os requisitos	Atende aos principais requisitos das normas e as documentações estão atualizadas.	Atende parcialmente aos requisitos das normas e as documentações estão atualizadas ou parte desatualizada.	Não atende ao mínimo necessário do que regem as normas de GCN.	Nenhum requisito é atendido satisfatoriamente
b) A empresa tem atualizados os diagnósticos de risco dos sites, sistemas e de criticidade dos processos seguindo os frameworks referência.	Possui análise de riscos, BIA atualizado, conhece todos os processos e sistemas críticos	A empresa conhece os riscos dos sites, sistemas e de criticidade de processos, mas existem oportunidade de melhoria nos processos.	A empresa não faz análise de risco de suas filiais, atende ao BIA e conhece a criticidade de sistemas e processos. Existem oportunidades de melhoria.	Não faz análise de riscos, o BIA precisa de melhorias e atualização, os cenários identificados não estão aderentes a realidade da empresa.	Não faz análise de riscos, o BIA não é aplicado, não possui política de GCN e para os documentos existentes é preciso revisão para melhorias.
c) Possui capacidade física, tecnológica, de recursos humanos e planos para responder aos cenários de descontinuidade	Possui local alternativo funcional de trabalho com ótima capacidade, possui infraestrutura para trabalho remoto com alta capacidade, possui distribuição de pessoas em diferentes sites, possui definição de áreas alternativas que possam exercer processos de áreas similares	Possui local alternativo funcional de trabalho com boa capacidade, possui infraestrutura para trabalho remoto para atender o mínimo necessário das equipes e possui distribuição de pessoas em diferentes sites para algumas áreas.	Possui local alternativo de trabalho, infraestrutura para trabalho remoto para atender o mínimo necessário das equipes, existem ajustes a serem feitos e pode não estar preparada para alguns cenários.	Os sites de contingência não atendem as necessidades, apesar de existirem alternativas ainda não formalizadas no plano.	Os sites de contingência não atendem as necessidades para cobrir cenários de descontinuidade.
d) Oferece alta segurança na disponibilidade dos dados e aplicações altamente críticas e críticas, através de sites redundantes, backups e DRP.	Possui todos os sistemas críticos espelhados e DRP atendendo todas as necessidades apontadas no BIA das áreas de negócio em termos de contingência	Possui os principais sistemas críticos espelhados e DRP atendendo as principais necessidades apontadas no BIA das áreas de negócio em termos de contingência	Possui os principais sistemas críticos com contingência, mas nem todos Ativo - Ativo e o DRP atendendo as principais necessidades, mas não está alinhado ao resultado do BIA.	O ambiente de contingencia de T.I não atende as necessidades em termos de continuidade de negócios seguindo as boas práticas. Sistemas críticos podem estar descobertos.	Não existem contingencias ou as existências são insuficientes.
e) A empresa possui cultura estabelecida de melhorias no programa de gestão de continuidade de negócios (Investe em melhorias).	Atua plenamente na melhoria das falhas apontadas em testes, análise de riscos, novos cenários, entre outros visando investir para sanar gaps e manter alta resiliência para responder aos cenários de descontinuidade	Possui processo de melhoria das falhas apontadas em testes, análise de riscos, novos cenários, entre outros visando investir para sanar gaps e manter alta resiliência para responder aos cenários de descontinuidade, no entanto, podem existir casos que o ciclo de melhoria não é aplicado	Não possui processo de melhoria das falhas apontadas em testes, novos cenários, entre outros ou o processo é informal, sem interface com as necessidades da gestão de continuidade de negócios.	O processo de cultura em GCN é insatisfatório, pode ser feita anualmente, mas sem abrangência adequada, além de não existir processo de investimento buscando melhorias.	Não existem ações de cultura em GCN.

Avaliações	4 Muito satisfatório	3 Satisfatório	2 Parcialmente satisfatório	1 Regular	0 Insatisfatório
f) Definição dos funcionários chaves está atualizada, as pessoas tem conhecimento e estão treinadas no plano de continuidade de negócios, bem como há substitutos definidos que também estão cientes dos procedimentos.	Atualizações anuais e conforme a mudança do quadro funcional das áreas, treinamentos aplicados a todos os funcionários, incluindo funcionários definidos como substitutos das pessoas chave do PCN	Atualizações anuais, mas não é garantido que há atualizações conforme mudança do quadro funcional das áreas, treinamentos aplicados a todos os funcionários, incluindo funcionários definidos como substitutos das pessoas chave do PCN	Definição dos funcionários chaves não está atualizada devido a dinâmica da empresa, as pessoas tem parcial conhecimento e estão treinadas no plano de continuidade de negócios.	Base de funcionários chaves está desatualizada ou mal avaliada devido a aplicação sem periodicidade do BIA, bem como os funcionários e substitutos não estão treinados.	Não existe definição de funcionários chaves, o tema PCN não é abordado com as áreas.
g) Estão estruturadas as contingências através de fornecedores alternativos.	Existem fornecedores alternativos operando e/ou homologados, prontos para atuação, com capacidade avaliada de atendimento, para todos os processos críticos da empresa dependentes de fornecedores críticos.	Existem fornecedores alternativos operando e/ou homologados, prontos para atuação, considerando os principais processos críticos, mas não necessariamente com capacidade avaliada de atendimento	Estão estruturadas algumas contingências através de fornecedores alternativos, mas existem cenários descobertos por dependência de fornecedor único.	Os processos críticos que dependem de fornecedores críticos não estão totalmente cobertos com estratégias de continuidade de negócios. Alguns processos estão menos expostos a fornecedor único, mas não existe um plano de contingencia entre os fornecedores e a contratante.	Os processos críticos que dependem de fornecedores críticos estão totalmente expostos a cenários de descontinuidade de negócios.
h) São feitos testes de PCN em DRP, Operacionais e testes de mesa.	São feitos periodicamente de acordo com a política de GCN testes operacionais de PCN, testes de mesa e testes DRP, envolvendo todas as áreas e sistemas críticos, bem como a alta gestão	São feitos periodicamente de acordo com a política de GCN testes operacionais de PCN, testes de mesa e testes DRP, envolvendo as principais áreas e sistemas críticos, bem como a alta gestão	São feitos periodicamente de acordo com a política de GCN testes operacionais de PCN, testes de mesa e testes DRP, envolvendo as principais áreas e sistemas críticos, bem como a alta gestão	O programa de testes é feito, mas não atende as necessidades.	O programa de testes não é aplicado.
i) A estrutura organizacional de crise está bem estabelecida, atualizada e formalizada nos níveis estratégico, gerencial e operacional.	Estrutura atualizada anualmente e conforme mudanças no quadro da alta gestão, com funções definidas e atualizadas conforme novos cenários, além da realização de treinamentos com este time	Estrutura atualizada anualmente, mas sem garantia de atualização conforme mudanças no quadro da alta gestão, com funções definidas e atualizadas conforme novos cenários, além da realização de treinamentos com este time	A estrutura organizacional de crise está criada, mas precisa ser atualizada e a cultura de gestão de crise precisa de mais atenção na empresa.	Existe a estrutura organizacional de gerenciamento de crise, mas está desatualizada e o tema GCN não tem a devido atenção junto a alta gestão.	A estrutura organizacional de gerenciamento de crise não está definida.

O resultado é o indicador da empresa, podendo ser visualizado também por categoria. Convém que o processo seja revisado anualmente, pelos seguintes motivos:

- Mudança nas condições de risco e ambiente de controles;
- Mudanças externas – fatores incontroláveis;
- Mudanças internas (estruturas, produtos e serviços, tecnologias, pessoas, sistemas, entre outros).



Os benefícios do indicador do nível de resiliência são:

- Visão do nível de preparação da companhia contra cenários adversos;
- Aumenta a transparência da gestão de continuidade, permitindo à empresa questionar periodicamente a quais cenários de interrupção / ameaças ela está exposta e se há meios de resposta em níveis satisfatórios;
- Oportunidade de melhoria no ambiente de controle - etapa de prevenção dos riscos (quando identificado e aplicável);
- Oportunidades de melhoria das contingências, planos de crise e protocolos de resposta;
- Governança;
- Documentação que auxilia no atendimento a auditorias.

Por fim, ressalto que o assessment deve ser adaptado à realidade de cada empresa, bem como os pesos dados a cada pergunta. É conveniente validar os cenários com a alta gestão, mas sem “enxugar muito”. Faz-se necessário também avaliar a preparação da empresa quando confrontada com todos os cenários aos quais ela está exposta, por mais remota que seja a probabilidade de ocorrência, pois em GCN não devemos nos apegar a isso, pelo menos a meu ver. Assim, espero ter contribuído com a comunidade de Gestão de Riscos e Continuidade de Negócios com este artigo.

WEBINAR

Plano de Resposta a Emergência e Crise - PRE

Prof. Dr. Antonio Brasiliano

CEGRC, CIEAE, CIEIE, CPSI, CIGR, CRMA, CES, DEA, DSE, MBS

Doutor em Ciência e Engenharia da Informação e Inteligência Estratégica pela Université Paris – Est (Marne La Vallée, Paris, França); **Presidente da Brasiliano INTERISK.**

INSCRIÇÕES GRATUITAS

31 de agosto | 11h00

https://www.brasiliano.com.br/eventos

Brasiliano INTERISK
Inteligência em Riscos

Brasiliano ministra aulas sobre gestão de riscos na Fundação Dom Cabral

Marcos Alves Junior
Assistente de Comunicação e Marketing da Brasiliano INTERISK

No dia 02 de junho, Antonio Brasiliano, professor, doutor e presidente da Brasiliano INTERISK, ministrou aula em uma das melhores escolas de negócios da américa latina. Considerada a 9ª melhor escola de negócios do mundo, de acordo com o ranking de educação executiva do jornal Financial Times, a FDC – Fundação Dom Cabral – é uma instituição especializada no desenvolvimento e capacitação de executivos, empresários e gestores públicos.

O professor abordou, inicialmente, o contexto atual do mercado de Governança, Gestão de Riscos e Compliance. Após introduzir o assunto para os alunos, ele discorreu sobre as quatro miopias inseridas na área de gerenciamento de riscos.

Brasiliano também abordou, de maneira específica, as melhores práticas de mercado no gerenciamento de riscos, com destaque para a aplicação da ISO 31000:2018 na Gestão de Riscos e para os modelos de controles internos COSO I – Revisão 2013 e COSO II ERM – Integrando Estratégia e Desempenho – 2017.

Antes de concluir a aula, o professor discorreu sobre aspectos relevantes e práticas obrigatórias no âmbito da área de gerenciamento de riscos corporativos das organizações. A área de gestão de riscos da empresa precisa trabalhar alinhada e em sincronia com os demais setores, mormente com a alta gestão, para obter os melhores resultados em termos de eficiência, eficácia e efetividade.

Marcos Alves Junior
Assistente de Comunicação e Marketing da Brasiliano INTERISK

Brasiliano apresenta webinar sobre prevenção contra ataques cibernéticos

No dia 23 de junho, Antonio Brasiliano, professor, doutor e presidente da Brasiliano INTERISK, apresentou um webinar sobre segurança cibernética denominado “Ataques Cibernéticos, como se prevenir”. O evento teve o objetivo de sensibilizar os gestores sobre a necessidade premente de as empresas investirem de forma consistente na estruturação do processo de segurança cibernética.

O evento tratou de um assunto que está em alta atualmente, em razão da proliferação dos ataques cibernéticos, com grande repercussão nos veículos de comunicação. De forma geral, esses ataques põem a descoberto as fragilidades das empresas no seu enfrentamento. Os danos resultantes são potencializados pela crescente dependência, da sociedade em geral e das empresas e organizações em particular, em relação às ferramentas de TI, no âmbito de uma sociedade cada vez mais conectada.

No webinar o professor citou exemplos de empresas de grande porte que sofreram ataques de cibercriminosos, gerando a paralização dos negócios e prejuízos milionários. Por tudo isso, o Professor assevera que, nesta era digital, a empresa que não tenha um processo estruturado de segurança cibernética pode estar em pleno voo cego, com todas as consequências decorrentes.

Segundo o Professor Brasiliano, para combater os ataques cibernéticos de maneira eficaz o mercado exige que um novo mindset, ou seja, uma nova mentalidade, seja incorporada por gestores e executivos.

Não conseguiu assistir ao evento online? Não tem problema, todos os eventos são gravados e estão disponíveis no canal oficial da Brasiliano INTERISK no Youtube. Caso também queira ter acesso à apresentação projetada no Webinar, é só **acessar aqui** ou nosso site, onde encontrará todas as apresentações disponíveis para download.

Silmara Veiga de Souza Calestini Montemor
Doutora em Direito Ambiental, Advogada, Consultora Sênior Associada da Brasiliano INTERISK

ESG e o meio ambiente: precaução e prevenção de riscos

Num mundo cada vez mais globalizado em que as relações estão cada vez mais intensas entre os países e entre os diversos atores, muito do que impacta uma localidade por mais distante em que esteja, acaba ressoando em diversos outros locais.

Como exemplo, temos o caso da recente tomada do Afeganistão pelos talibãs. Foi algo sentido e lamentado por todo o mundo, que compartilhou uma sensação de frustração diante dos acontecimentos.

Ocorre que, também nas relações comerciais, o mundo está cada vez mais conectado. Consequentemente, modificações nos costumes, por menores que sejam, como o fato de as pessoas deixarem de usar canudos plásticos em resposta ao lixo plástico existente nos mares, fatalmente impactam as empresas que vendem produtos com canudos, as quais precisam perceber esse movimento e se adequar. Paulatinamente as pessoas têm uma tomada de sentimento e de consciência de que suas ações impactam o meio ambiente.

Isso gera um encadeamento que precisa ser encarado. No ano de 2020 a BlackRock firmou entendimento no sentido de direcionar seus investimentos observando o cumprimento de uma agenda ESG.

ESG significa Environmental, Social e Governance, ou seja, atribui uma vertente ambiental, uma social e uma de governança aos negócios, iniciativa esta que extrapola em muito as práticas atualmente implantadas como GRI. Significa que uma empresa precisa ser plena nas suas relações.

O que é ser pleno?

Significa deslocar o fator ambiental da posição de escanteio e trazê-lo para o coração da empresa, de onde ele passa a bombear seus princípios para as demais áreas.

E quais são esses princípios?

De uma maneira básica, eles são Precaução e Prevenção, que têm a finalidade precípua de redução de riscos, que podem ser elencados, entre outros, como riscos financeiros, de danos à imagem, riscos de processos que podem levar em último grau à paralisação das atividades da empresa.

E o meio ambiente vai muito além da proteção das florestas, como se pensava há algum tempo. Podemos falar não somente em meio ambiente natural, como também em meio ambiente cultural, meio ambiente artificial, meio ambiente do trabalho, e há os que já falam em meio ambiente digital, e sobre isso se tratará a seguir.

O meio ambiente e as novas perspectivas da agenda ESG

Da maneira clássica, conhecemos por meio ambiente o natural, que é aquele propriamente dito no sentido ecológico, e que abarca as florestas, o ar, os mares e oceanos.

E quando se fala em questões do meio ambiente natural nas atividades empresariais tem-se em mente o impacto gerado sobre os recursos tais como a água, contaminações, e, sobretudo, os riscos pela responsabilidade ambiental que é

tríplice, podendo dar-se nas esferas administrativa, penal e civil (nesta esfera se responde de forma objetiva pelo que se sabe e pelo que deveria saber acerca dos eventuais danos). Além disso, já dentro de uma agenda ESG, trata-se da adoção de metas e métricas pelas empresas para mitigação, por exemplo, das emissões de gases do efeito estufa e redução da dependência de energia, mudando o modal para energias sustentáveis como a energia solar, colocando parâmetros e formas de verificação externa de atendimento a tais metas, de uma forma bastante conectada, por exemplo, com a Agenda 2030 da ONU.

Mesmo quando se fala das cidades, têm ganhado força práticas de permacultura, com telhados verdes, hortas coletivas, até porque o princípio dessa prática de agricultura afirma que o homem desconectado do meio ambiente se desconecta de si mesmo, ou seja, é trazido o meio ambiente natural para onde seria um local árido do meio ambiente artificial do qual falaremos adiante. Ou seja, quando falamos de meio ambiente natural na visão ESG é um horizonte bastante amplo que engloba o meio ambiente natural em suas diversas facetas, que compreende riscos, impactos e sua mitigação, novas formas de agir e de utilizar os recursos naturais, tudo isso sob o guarda-chuva dos princípios de Prevenção e Precaução.

Já o meio ambiente cultural, é aquele que engloba as práticas, os modos de fazer, agir, falar, as culturas e tradições na sua diversidade. Pode ser citado nas empresas a aquisição de força de trabalho de pessoas com perfil diverso, seja em função de raça, religião, idade, necessidades especiais, opção sexual, gênero e até mesmo de pessoas que atualmente não se identificam com nenhum gênero. E isso parece extremamente assustador, porque talvez as empresas ainda não estejam preparadas, mas talvez deva se pensar no quanto a diversidade pode somar no sentido de criatividade, como resultante do somatório de opiniões distintas que podem enxergar as coisas sob novas perspectivas.

E isso não somente por um dever de consciência, mas também como forma de evitar prejuízos financeiros, pois recentemente houve uma ação envolvendo uma das mais bem conceituadas empresas do país, a XP Investimentos. A ação cobra uma indenização de 10 milhões de reais por conta de uma foto da Ável Investimentos em Porto Alegre, empresa ligada à XP Investimentos, em que de cento e onze funcionários apareciam nove mulheres, ao menos aparentemente não se viam negros na foto, traçando um perfil de pessoas jovens, brancas e do sexo masculino. Na visão dos que ingressaram com o processo, não se está refletindo o ordenamento social, composto também de negros, por exemplo.

Continuando, há também o meio ambiente artificial, constituído pelas ações e intervenções do homem, como as cidades, prédios. E talvez essa possa ser apontada como a primeira

vertente da aplicação dos conceitos ambientais nas empresas com implantação de princípios da agenda de ODM's (Objetivos do Desenvolvimento do Milênio), especialmente visando à garantia da qualidade de vida e do respeito ao meio ambiente (Objetivo n. 7).

Essa mudança estrutural no meio ambiente artificial é relativamente fácil de demonstrar: na década de 1980 era comum passar-se por ruas e avenidas de prédios de escritórios e ver luzes acesas durante toda a noite. Hoje tem-se em mente que o último a sair apaga as luzes; antigamente os relatórios eram todos impressos, e atualmente até os CEO's evitam imprimir documentos em grande número; começaram a ser pensados edifícios com maior iluminação e ventilação natural; e estratégias como reaproveitamento de água das chuvas, colocação de painéis solares e utilização de energias renováveis. Tudo isso são fatores que ao longo do tempo geram uma significativa economia de recursos e também uma melhor qualidade de vida para os que trabalham em tais ambientes.

Além de tudo o que já foi colocado, temos o meio ambiente do trabalho que precisa ser salubre em todas as suas vertentes, um local de convívio saudável, onde as pessoas vão passar boa parte de suas vidas, e deve estar distante de práticas abusivas em face de funcionários. Isso engloba o cumprimento de leis trabalhistas da maneira tradicional, mas também vem tomando vertentes como práticas de incentivo aos colaboradores para que se sintam realmente parte, para que evoluam profissionalmente oferecendo perspectivas, tornando-se protagonistas no seu espaço de ação por menor que este seja, valorizando a pessoa daquele colaborador, porque uma das formas de desumanizar alguém é tirar o valor de seu trabalho, transformando-a num mero instrumento.

Pelas novas práticas, na visão correta dentro da agenda ESG, o colaborador merece ser visto como um indivíduo, recebendo um treinamento adequado para aquela função para agir e reagir de forma ordenada e correta dentro das situações e problemas do cotidiano. E isso também evita danos, como o emblemático caso do Carrefour em Porto Alegre em que houve a morte de um consumidor, o que gerou um prejuízo mais do que financeiro (foi realizado acordo para pagamento de 115 milhões de reais), isso refletiu na imagem da empresa e possivelmente respingará ainda ao longo de alguns anos, e se deverá gastar muito mais em ações sociais e de marketing para reverter essa situação.

A empresa precisa prover treinamento, e pagar adequadamente os seus terceirizados para que estes também forneçam um treinamento adequado, porque lidar com o público, necessariamente envolve fatores adversos, pessoas sob estado alterado, por exemplo. Então, é necessário haver um protocolo para isso, porque é uma situação cotidiana; e protocolos para o caso contrário também, formas de proteção no caso de funcionários

serem agredidos pelos consumidores, porque o funcionário não é obrigado a se submeter a humilhação para se manter num emprego.

Engloba ainda o meio ambiente digital, aquele composto pelos recursos de tecnologia. E desse é fácil citar exemplos de abusos, tal como cobranças sucessivas e incansáveis, com mais de vinte telefonemas a consumidor em um único dia; práticas agressivas de marketing por meio de algoritmos que praticamente perseguem o potencial consumidor nas suas redes; ligações e reuniões seguidas mesmo em horários fora do expediente pelas empresas em tempos de home office. Tudo isso precisa ser visto dentro do princípio da Dignidade Humana, por muitas vezes irem além da mera perturbação do sossego, que, inclusive, constitui por si só um crime.

Pensamos numa mudança estrutural de comportamento empresarial, e se até então a perspectiva empresarial baseava-se no lucro, modernas teorias já vinham realçando o sentido da função social da empresa. A própria Constituição Federal de 1988 no art. 5°, XXIII, afirma que a propriedade atenderá a sua função social, incluindo-se, portanto, as empresas, o que vem repetido no art. 170, III, capítulo destinado a tratar da ordem econômica.

E mais uma vez se vai além, não se trata apenas de cumprimento da função social da empresa através da série de deveres e obrigações legais, como o pagamento de impostos e obrigações trabalhistas, que por si só muitas vezes já aparentam ser um fardo demasiadamente intenso. Mas sim da mudança no paradigma ético propriamente dito.

Modernamente pelos conceitos de ESG entende-se que a empresa de forma objetiva é responsável pela sua pegada no mundo, seja no sentido de pegada ambiental enquanto impactos pela sua existência, seja de pegada social, constituída pelas suas relações e como influencia a sociedade, e seja também pela sua governança de como ela se estrutura, relaciona-se em sua estrutura interna e também em relação aos stakeholders em termos de ética e de transparência. É algo difícil, sem dúvidas.

Em suma, o que precisa ser visto é que além de a agenda ESG estar se tornando uma imposição do mercado, o não cumprimento voluntário representa alto risco financeiro, e a exposição de falhas em tempos de internet pode representar uma verdadeira catástrofe em termos de imagem a acompanhar a empresa por anos, podendo se sobrepor e apagar o brilho de muitos esforços e trabalhos positivos realizados.

De qualquer forma, é preciso ter em mente que, não obstante a relevância das políticas aplicadas ao mercado pelos agentes globais, o certo é que, no final das contas, quem direciona o mercado e impulsiona todas essas práticas e mudanças de conduta é a própria sociedade em si, esse universo

pulverizado de milhões de seres, que devem agir conscientemente, no sentido de livremente optarem por soluções e direcionamentos que efetivamente se adéquem ao bem-estar coletivo.

REFERÊNCIAS

BLACKROCK. Uma mudança estrutural nas finanças. Disponível em: https://www.blackrock.com/br/larry-fink-ceo-letter. Acesso em 19 ago. 2021.

BRASIL. Constituição da República Federativa do Brasil de 1988. Brasília, 05 de outubro de 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm#adct. Acesso em 28 mar. 2020.

CANOFRE, F.; NOGUEIRA, I.. Com acordo de 115 milhões, Carrefour evita processo pelo caso Beto Freitas. Jornal Folha de São Paulo. Disponível em: https://www1.folha.uol.com.br/mercado/2021/06/com-acordo-de-r-115-milhoes-carrefour-evita-processos-pelo-caso-beto-freitas.shtml. Acesso em 19 ago. 2021.

OBJETIVOS DO DESENVOLVIMENTO DO MILÊNIO. Agenda 2030. Disponível em: http://www.odmbrasil.gov.br/os-objetivos-de-desenvolvimento-do-milenio. Acesso em 19 ago. 2021.

OLIVEIRA, I. Após foto com homens brancos, ação pede indenização de 10 milhões à XP e a Ável. Portal UOL. Disponível em: https://economia.uol.com.br/noticias/redacao/2021/08/18/ongs-pedem-indenizacao-xp-avel-por-falta-diversidade-entre-colaboradores.htm. Acesso em 19 ago. 2021.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. Objetivos do Desenvolvimento Sustentável. Disponível em: https://brasil.un.org/pt-br/sdgs. Acesso em 19 ago. 2021.

SANTOS, R. Racismo Estrutural, Entidades ajuízam ação contra Ável e XP por processos seletivos discriminatórios. Revista Consultor Jurídico, 18 de agosto de 2021. Disponível em: https://www.conjur.com.br/2021-ago-18/entidades-ajuizam-acao-avel-xp-condutas-discriminatorias. Acesso em 19 ago. 2021.

Sua organização está preparada paras os desafios impostos pelo avanço da tecnologia?

Com o Software INTERISK a sua organização conta com um processo estruturado para prevenção do vazamento de informações e dados. Venha conhecer a nossa ferramenta, ela dispõe de um método assertivo de DPL (Data Loss Prevention) no qual prepara a sua organização para variados cenários de vazamento de dados confidenciais garantindo responsabilidades na classificação das informações.

Alguns passos do processo:

1. **Identificação dos processos críticos;**
2. **Identificação e classificação das informações críticas;**
3. **Identificação e classificação dos sistemas que suportam os processos;**
4. **Mapeamento e listagem de pessoas;**
5. **Plano de ação com soluções preventivas e mitigatórias.**

SOFTWARE INTERISK
Inteligência em Riscos

Fale com um de nossos especialistas!

Prof. Dr. Antonio Celso Ribeiro Brasiliano,
CEGRC, CIEAC, CIEIE, CPSI, CIGR, CRMA, CES, DEA, DSE, MBS
Doutor em Ciência e Engenharia da Informação e Inteligência Estratégica pela Université Paris – Est (Marne La Vallée, Paris, França); presidente da Brasiliano INTERISK.

Como as empresas podem obter uma visão antecipada e de adaptação aos ataques cibernéticos

A detecção de sintomas de ataques cibernéticos a sistemas empresariais, abrangendo tanto TI (Tecnologia da Informação – Nível Corporativo) quanto TO (Tecnologia Operacional – Nível Industrial e Operações de Negócio) a tempo de as empresas acionarem suas defesas e em paralelo realizarem a análise de como o ataque poderá ser materializado, aí incluída uma projeção dos prováveis impactos, de modo a reduzi-los mediante um eficaz gerenciamento dos incidentes, passou a ser um desafio estratégico para os gestores da segurança cibernética, informação e privacidade - CIP.

As empresas necessitam ser resilientes às ameaças cibernéticas e para isso necessitam estruturar respostas adequadas ao perfil de ataques que poderão sofrer. Isso significa que a percepção de sintomas de que há algo anormal nas redes e sistemas é um fator crítico de sucesso. Mediante uma antecipação bem-sucedida, as empresas podem estruturar muito mais assertivamente suas defesas cibernéticas e também gerenciar as respostas adequadas aos incidentes. Um Plano de Resposta a Incidentes bem estruturado, com o emprego de cenários prospectivos de ataques cibernéticos é o grande diferencial para mitigar consequências.

Hoje, as empresas encontram-se submetidas a pressões intensas, tanto oriundas da área externa quanto da área interna: da área externa, as ameaças crescem de forma exponencial, incidindo sobre um perímetro estendido (sem fronteira definida, na verdade), perpetradas por hackers cada vez mais capacitados; já as pressões vindas da área interna devem-se principalmente à insuficiência orçamentária (resultado da não conscientização da alta gestão) e da carência de recursos humanos capacitados, o que redunda na falta de agilidade de antecipação e de resposta.

Na verdade, a segurança cibernética deve estar à frente dos hackers para poder prevenir e mitigar os ataques. Esse é o grande desafio. Na figura a seguir, demonstramos graficamente essas pressões.

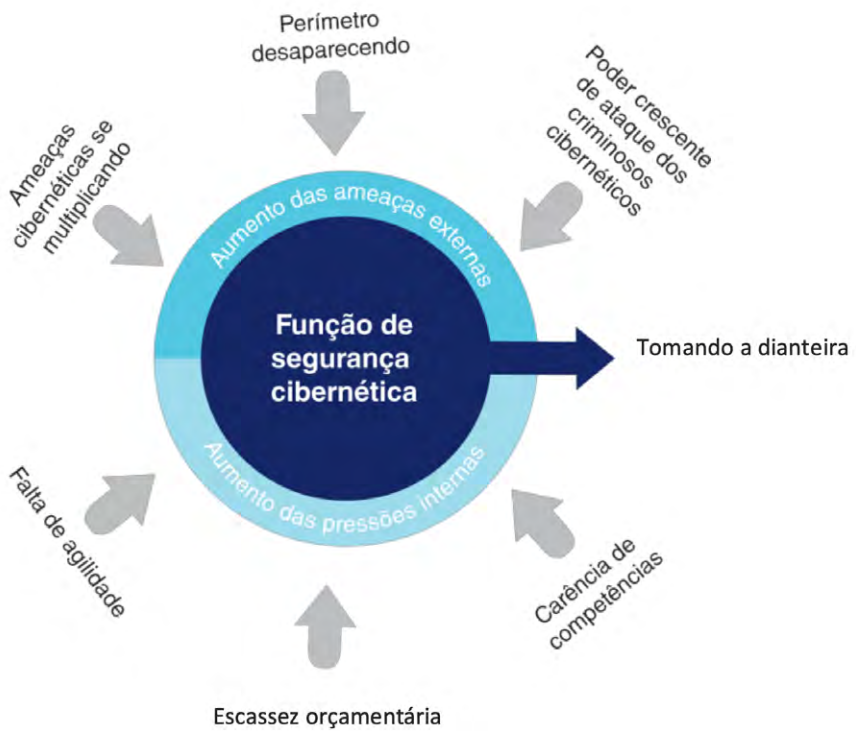


Figura 1: Pressões da Segurança Cibernética
Fonte: Metodologia da Brasiliano INTERISK – Construção de Cenários de Ataques Cibernéticos

Para fazer face a ameaças cada vez mais sofisticadas, a empresa deve dispor de uma capacidade muito forte de detecção, visando entender como os ataques cibernéticos podem ser materializados, bem como a estratégia empregada e o vetor de ataque utilizado. Para isso, deve entender muito bem suas próprias vulnerabilidades e saber qual o perfil de um possível agressor. Deve também identificar, sob a ótica do hacker, que tipo de vantagem sobre a empresa ele (hacker) poderá ter, caso o ataque obtenha sucesso. O diagrama de causa e efeito (figura 2) mostra as perguntas que devem ser respondidas pelos gestores da CIP (Cibernética, Informação e Privacidade), de modo a obter a visão antecipada do evento.

Portanto, antes de pensar em tecnologia as empresas devem pensar em antever os modi operandi do agressor, bem como o seu perfil.

Desta maneira, a empresa, para ter cyber resiliência com muita agilidade, deve percorrer três fases em seu processo de atuação preventiva e mitigatória. São elas:

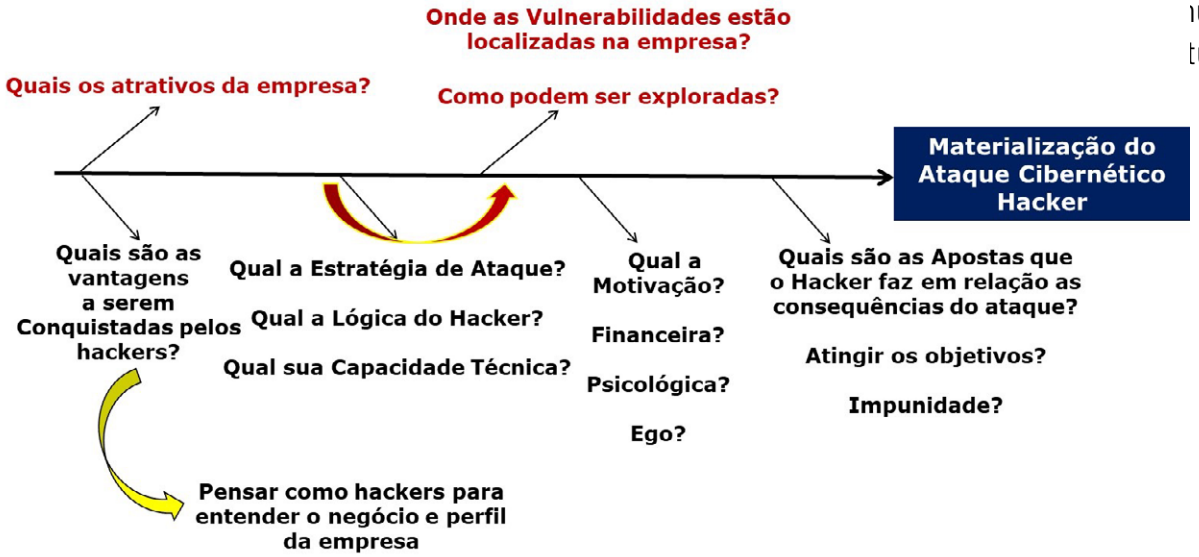


Figura 2: Diagrama de Causa e Efeito para ataques cibernéticos.
Fonte: Metodologia da Brasiliano INTERISK – Construção de Cenários de Ataques Cibernéticos

Figura 3: As fases dos ataques cibernéticos.
Fonte: Metodologia da Brasiliano INTERISK – Construção de Cenários de Ataques Cibernéticos

Detecção

É a capacidade das organizações de prever e detectar ameaças cibernéticas. As organizações precisam realizar um trabalho de inteligência com foco nas ameaças cibernéticas e nas medidas de defesa ativa para prever quais ataques estão sendo orientados em sua direção e detectá-los quando eles estiverem próximos, antes que sejam bem-sucedidos. A empresas precisam ter dados sobre o que vai acontecer e para isso devem contar com um trabalho de inteligência analítica sofisticada que lhes proporcione um alerta antecipado quando situações anômalas estiverem ocorrendo no tráfego da rede ou no sistema.

Defesas e segurança

Os mecanismos de defesa de segurança formam basicamente o escudo de defesa, a muralha que o hacker tentará vencer. Tudo começa com a determinação do grau de risco que a empresa está preparada para enfrentar, tendo em vista o levantamento e a avaliação de cenários de ataques cibernéticos de toda a sua superfície de ataque. Em seguida emprega as três linhas de defesa:

Primeira Linha: encarregada de executar medidas de controle nas operações do dia a dia;

Segunda Linha: responsável por implantar funções de monitoramento contínuo pelo SOC – Security Operation Center (Centro de Operações de Segurança), incluindo o SIEM – Security Information and Events Management (Gerenciamento de Segurança da Informação e Eventos), em toda a infraestrutura de TI da empresa, aí incluídos os sistemas de segurança, controles internos e Cyber Security Risks Assessment (Avaliação dos Riscos e Cenários Cibernéticos);

Terceira Linha: Responsável por exercer uma forte e independente auditoria interna.

Reação

Caso a Detecção não funcione (a organização não percebeu a chegada da ameaça) e haja uma falha na Defesa de Segurança (as medidas de controle não eram fortes o suficiente), as empresas precisam estar preparadas para lidar com a provável interrupção das operações e para gerenciar a crise, ter devendo dispor de uma pronta capacidade de resposta a incidentes.

Elas também precisam estar preparadas para preservar provas de maneira segura, do ponto de vista forense, e, em seguida, investigar a violação, a fim de satisfazer partes interessadas cruciais, como clientes, reguladores, investidores, autoridades policiais e o público em geral, qualquer uma das quais poderia mover ações por perdas e danos ou por descumprimento de obrigações. Caso as partes responsáveis pelo incidente sejam identificadas, a empresa poderá mover processos contra elas.

Finalmente, elas também precisam estar preparadas para retornar à rotina de negócios o mais rapidamente possível, ou seja, recuperar o quanto antes o costumeiro ritmo das operações. Aprender com o incidente é crucial para que a empresa não volte a cometer as mesmas falhas, daí a necessidade de registrar todas as ações realizadas e o grau de eficácia nelas obtido no sentido de conter, erradicar e recuperar.

Em função disso, é cada vez mais importante correlacionar as informações e, assim, garantir a segurança dos negócios, através da inteligência analítica.

De acordo com o Daniel Lima, em seu artigo “Como tratar milhares de informações e garantir a segurança do seu negócio?”:

Mas como fazer isso na mesma velocidade em que aparecem novas ameaças e um turbilhão de informações para serem gerenciadas? A resposta é adotar plataformas de segurança inteligente. Elas se tornaram um elemento fundamental na estratégia de segurança das áreas da Cibernética, Informação e Privacidade – CIP para gerenciar estes desafios, possibilitando detecção e respostas automáticas e emitindo dashboards e

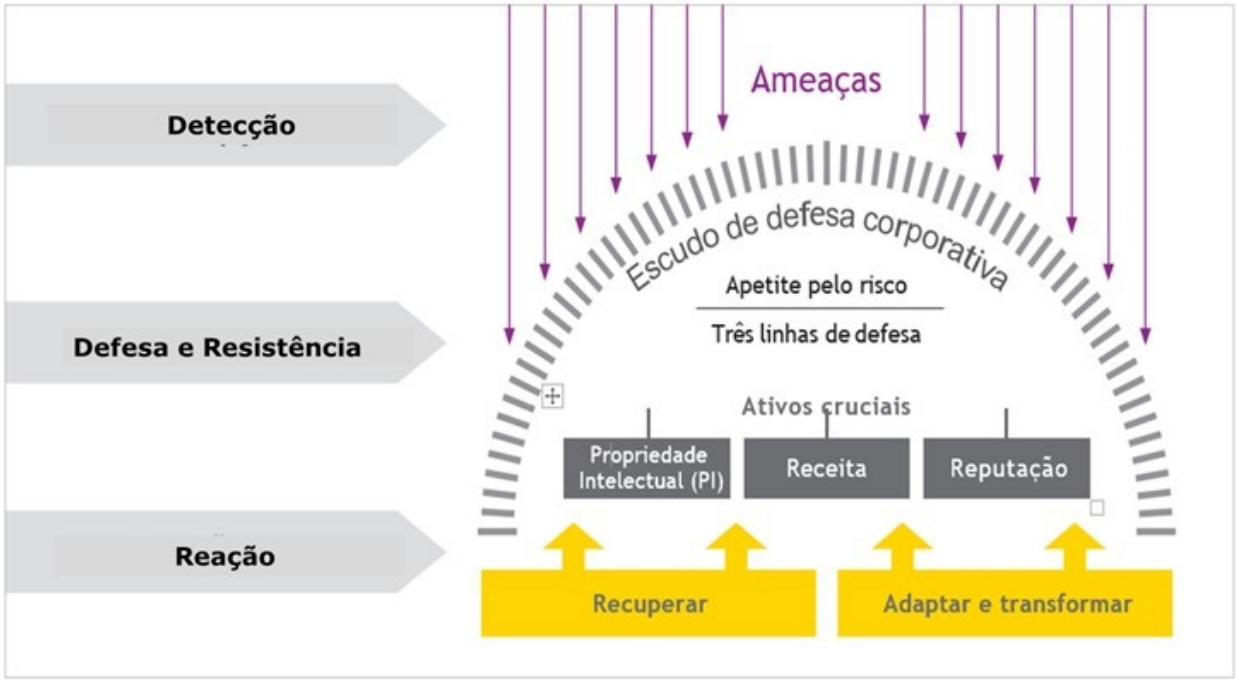


Figura 4: Fases dos ataques cibernéticos – Visão Esquemática.
Fonte: Metodologia da Brasiliano INTERISK – Construção de Cenários de Ataques Cibernéticos

relatórios que permitirão às empresas identificar, realizar a triagem e atuar de forma mais eficaz durante os incidentes.

Porém, adotar uma nova ferramenta e ter uma abordagem prospectiva impõe desafios aos líderes das empresas. Para enfrentar esses desafios, ou pelo menos os mais importantes dentre eles, cumpre à Alta Administração responder às seguintes perguntas:

- Como manter os especialistas da empresa atualizados e motivados?
- Como garantir a nova plataforma rodando de forma plena?
- A empresa faz uso de todo o potencial da nova plataforma? Ou usa apenas parte do seu potencial?
- Adianta a empresa ter visibilidade das ameaças e não ter um time 24×7 atuando nos incidentes?
- A empresa acompanha de forma direta os novos modi operandi dos hackers em outros países?
- A empresa está adicionando inteligência ao seu sistema de segurança CIP e aos seus processos?

Todas essas dúvidas nos mostram que essas plataformas, por si sós, não atingem os resultados necessários para garantir a proteção dos dados. É preciso contar com um parceiro especializado em segurança CIP que forneça serviços do tipo SOC, agregando processos e conhecimentos maduros, além de um time de especialistas nessa tecnologia, com analistas de segurança que atuem 24 horas por dia, 7 dias por semana, assegurando que nenhum incidente de segurança identificado pela solução passe despercebido ou deixe de ser triado e tratado.

A detecção de ameaças e de violações de conformidade em tempo aceitável e a capacidade de gerenciar incidentes com o mínimo de impacto certamente farão diferença no desempenho do negócio.

Por isso garantir segurança para o negócio não pode ser um mero exercício de especulações. Se não tiver consciência plena de quais são as Joias da Coroa (aquilo que é crítico, relevante e essencial) do negócio e não concentrar o foco na proteção ao redor delas, a empresa poderá pagar o preço por cenários de ataques cibernéticos que não estão no radar. A consequência será massiva, prejudicando os setores operacional, legal e financeiro, além da imagem da empresa.

Possuir a visão de antecipação e adaptação é o grande desafio para os líderes empresariais neste século XXI.

Corporación Euro-Americana de Seguridad
CEAS INTERNACIONAL

C.E.G.R.C

CERTIFICADO DE ESPECIALISTA EM GESTÃO DE RISCOS CIBERNÉTICOS

A Certificação de "Especialista em Gestão de Riscos Cibernéticos" CEGRC, surge como um projeto de colaboração entre CEAS-INTERNACIONAL (Espanha) e a Brasiliano INTERISK (Brasil), para assegurar a solvência e sustentabilidade dentro das organizações.

O propósito de obter uma certificação em Gestão de Riscos Cibernéticos é aprender a considerar e preparar-se para os riscos a que estão expostos uma organização em suas operações.

INFORMAÇÕES:
www.ceasbrasil.com.br
www.ceasinternacional.org
contato@ceasbrasil.com.br

Brasiliano INTERISK
Inteligência em Riscos

Carlos Alberto Zanandreis da Silveira
Especialista em Gestão de crises e emergências na Fundação Renova. Professor do curso de Gestão da Segurança Privada e do MBA em Gestão Estratégica e Inteligência na segurança privada do Centro Universitário Unihorizontes. Mestre em Administração e delegado da CEAS (Corporación Euro Americana de Seguridad) em MG.

Não se faz segurança com atos e sistemas isolados: em defesa de profissionais qualificados e de uma segurança integrada.

Um papel importante dos profissionais e empresas de segurança deve ser o de esclarecer e orientar a todos os usuários e ou contratantes do serviço de segurança sobre aspectos relevantes de seus respectivos planejamentos. Há um senso comum em relação a aspectos da segurança que perpassam muitas decisões a respeito dos sistemas utilizados e da forma como são geridos no dia a dia das empresas. É aí que começam grandes problemas do processo de gestão de segurança.

É comum ver muitos tomadores de decisão nas organizações, sejam de que porte forem, encararem a segurança encarada e gerida, não sob uma perspectiva técnica, mas como algo que qualquer pessoa que não seja especialista possa fazer, partindo de conhecimentos (se existem) esparsos sobre o assunto. É relevante considerar sempre que segurança é um serviço técnico e deve ser estruturado por profissionais tecnicamente habilitados para tal.

Há organizações que colocam sua segurança sob a responsabilidade de profissionais de outras áreas, ou ainda de alguém que seja antigo na empresa e que para não ser desligado, por gratidão ou amizade, é colocado como responsável da área de segurança. Nessa posição, além de não buscar capacitação adequada, faz o serviço sem tanta motivação, pois considera que está sendo deixado de lado ao ser designado a esta função. Há ainda a visão de que o custo com segurança é alto e assim, para "economizar", o próprio administrador tenta realizar as ações seguindo manuais padronizados e conselhos esparsos de alguém que já atuou na segurança pública ou queira vender algum produto.

Nesse ínterim, é comum ouvir frases do tipo: Ouvi dizer que... Um amigo meu disse que... Eu li numa revista... Na empresa tal fizeram assim... Não há problema que qualquer profissional possa fazer um benchmarking, é aliás essencial ter este olhar, porém, é preciso ter-se em mente que qualquer decisão em relação a aspectos de segurança deve ter por base um olhar mais amplo, que avalie, em primeiro lugar, se tais ações são adequadas àquele tipo de organização e seu contexto interno e externo, e em segundo lugar se a empresa tem condições de fazer tal investimento, levando em consideração tudo que ele implica no que diz respeito a investimento, profissionais envolvidos e infraestrutura necessária. Um terceiro ponto, tão ou mais importante, é verificar se tal ação realmente atende à necessidade de mitigação de riscos daquela empresa.

Pode-se inclusive fazer uma analogia com um remédio que, receitado por um médico, pode ser útil a uma pessoa e não necessariamente ser adequado a outra, até mesmo pela dosagem que precisa ser ajustada à realidade de cada paciente. Desta analogia, o que se conclui é que, para se indicar um remédio de maneira responsável e adequada, é preciso que um profissional médico habilitado e gabaritado possa avaliar as condições de cada paciente e assim diagnosticar e indicar o remédio mais adequado e na medida mais coerente com o tamanho do problema detectado.

Quando se fala desse tema, Lima (2014) contribui afirmando que segurança empresarial é o "conjunto de medidas de prevenção que visa assegurar a integridade física e moral das pessoas e a proteção do patrimônio e imagem da empresa eliminando e reduzindo os riscos potenciais". Ao apresentar a ideia de conjunto, o autor apresenta uma série de medidas que necessitam estar integradas e adequadas. Imagine uma orquestra dotada de vários instrumentos, mas na qual cada musicista toca uma música diferente, ou num tom diferente. Claro que essa orquestra não cumprirá seu papel e será vista como algo ruim. Neste

mesmo conceito, pode-se perceber que as medidas de segurança precisam estar adequadas à imagem e cultura organizacional, e por consequência ao negócio, e que devem ser ações com potencial de atuar no sentido de reduzir os riscos possíveis que precisam, de antemão, ser conhecidos. Ainda, ao abordar o termo “conjunto de medidas”, já se entende que um processo adequado de segurança não está baseado em uma só ação isolada e desconectada da realidade da empresa e de um efetivo resultado esperado.

Quando se observam as organizações, na perspectiva de segurança, tem-se percebido, nos noticiários atuais, ocorrências de crimes, em empresas de diversos portes, passando por sérios problemas de segurança, mesmo após terem investido em algum sistema, imaginando que estariam protegidas. Nestes noticiários, inclusive, há alusão ao fato de que o local tinha um sistema de segurança, muitas vezes considerando que esse sistema é que não foi eficaz e não atendeu ao objetivo, sendo que na realidade a possível ineficácia está atrelada ao seu uso inadequado. Sabará e Alves (2015) afirmam que, desde 1996, houve um aumento considerável e grande difusão dos serviços de vigilância eletrônica, que é o investimento mais comum, constando inclusive em projetos de lei e ajustes na legislação vigente, permitindo e limitando tais serviços.

Um exemplo, é o caso de locais que têm um sistema de câmeras, que fazem gravações, porém esse sistema somente serviu para gravar a ocorrência. Muitas destas cenas são gravadas com imagens de baixa qualidade e iluminação inadequada. Em suas entrevistas e manifestações, os responsáveis destas empresas alegam ter investido em segurança, porém, neste caso especificamente, somente câmeras não impediriam que os crimes fossem perpetrados. Vê-se aí que não basta ter um sistema de câmeras se estas não são monitoradas para uma ação de resposta imediata quando da detecção de alguma invasão. Ou ainda, que não adianta ter uma câmera se os sistemas de segurança física, como portas, janelas, paredes, são frágeis e fáceis de transpor. Há uma crença de que ter um sistema de segurança, mesmo que ele não esteja adequadamente alinhado com as melhores práticas, seja o suficiente para que haja a inibição da atuação da criminalidade. Isso hoje tem se mostrado um ledo engano, visto que o cometimento de crimes tem ocorrido à luz do dia e à frente das câmeras, sem qualquer timidez.

Rodrigues (2009) disserta em seu artigo sobre segurança para escolas, que no desenvolvimento de um projeto para cerca de 2000 escolas, um problema percebido foi a instalação de equipamentos de má qualidade, não ter havido monitoramento e nem gravação das imagens, além de estas (imagens) serem de baixa qualidade de visualização e identificação. Ou seja, não basta somente colocar um sistema de qualquer jeito. A própria definição do tipo de equipamento, dos posicionamentos, do tempo de gravação, da visualização, da manutenção e integração com outros sistemas (alarmes e vigilância) deve ser algo pensado nos projetos. Isso falando somente de um sistema de câmeras.

Um problema sério que se vê, é que estes decisores das organizações querem começar pelo que deve ser a etapa final do processo de gerenciamento de riscos. Querem começar pela medida a ser tomada. A ISO 31000, que apresenta as melhores práticas de gerenciamento de riscos no mundo, aponta exatamente um caminho necessário para que se chegue ao final com decisões de tratamento dos riscos de uma maneira concreta e metodológica. O caminho apresentado pela ISO 31000 é o de inicialmente se estabelecer o contexto organizacional em relação a gestão de riscos (Cultura, política, interesses, visão a respeito do processo de gerenciar riscos naquela organização, interesses dos patrocinadores, suportabilidade de perdas da organização, entre outros), acompanhado de um levantamento de informações internas e externas àquela empresa, e a partir disso, identificando bens, riscos, vulnerabilidades, fatores causais, capazes de mostrar o retrato atual daquela empresa, a que chamamos de diagnóstico.

Em seguida, é necessária uma análise dos riscos (medição da probabilidade x impacto) que dará condições ao profissional da segurança de apontar os principais riscos e ranquear as prioridades de tratamento daquela empresa. Tudo isso, acompanhado, o tempo todo, de um processo de comunicação com as áreas e pessoas-chaves da empresa, e de uma análise de todo o processo de gerenciamento de riscos e construção deste, visando à melhoria contínua. Só aí então é que será possível apontar quais as melhores ações de tratamento para estes riscos organizacionais, onde se poderá definir que riscos podem ser assumidos, que riscos devem contar com ações para detectar antecipadamente os perigos, que ações são definidas a partir de tal detecção (respostas) e que riscos devem ter tratamento para redução das vulnerabilidades, mitigando a possibilidade da sua ocorrência, ou até, assumir os riscos não adotando nenhuma prática de redução das probabilidades.

Meirelles (2011) salienta que a segurança é um subsistema de uma organização, tal como, o departamento comercial, administrativo, gestão de pessoas etc., que juntos vão oferecer seus serviços e conhecimentos em prol do objetivo maior, do sistema (Organização). Mas, é também, um sistema em si que é estruturado em subsistemas para chegar ao seu objetivo, ou seja, a área de segurança para gerar os resultados que se espera dela, é suportada por subáreas, que são divididas nos diversos sistemas de segurança. Desta forma, quando se fala em segurança física, segurança eletrônica, inteligência e contrainteligência, segurança das informações, entre outras, falamos de sistemas que devem atuar em conjunto para obter o resultado esperado. O que adiantaria ter um alarme (segurança eletrônica), se não há ninguém para dar uma resposta efetiva à situação (vigilância)? O que adianta uma câmera, se não há uma visualização ativa e preventiva? Como dito anteriormente, ela servirá somente para rever como os criminosos agiram, não funcionando como um processo preventivo. E a premissa de um sistema de segurança é prevenir, para que a ocorrência criminosa não ocorra e, se isso não for possível, que se tenha uma resposta rápida e adequada.

Outro aspecto que precisa ser avaliado é que, atualmente, alguns sistemas isolados de segurança não dissuadem mais os

criminosos. Estes esperam a oportunidade, observam e avaliam suas vulnerabilidades. O que adiantaria você ter um sistema que as pessoas não conhecem, não sabem operar? O que adianta ter equipamentos que as pessoas não têm treinamento e orientação de quando e como utilizar? O que adianta ter até vários sistemas de segurança, se as pessoas que atuam no local deixam portas abertas, ou agem de forma a fragilizar acessos ou acidentes? O que adianta ter os sistemas se eles não "conversarem" e não se complementarem entre si? Vê-se aí que não basta só ter isoladamente um sistema de segurança pensado. É preciso, com o diagnóstico organizacional em mãos, definir-se a proteção, tendo por base a interligação de pessoas, sistemas e procedimentos. E tudo isso deve estar alinhado com os valores e objetivos estratégicos da organização.

Em segurança, tudo deve ser bem pensado e planejado. Ao implantar uma vigilância, por exemplo, muitas organizações pensam somente no custo e querem "baratear" os serviços, colocando vigias ou porteiros como encarregados de atividades que por lei só podem ser realizadas por vigilantes, ou ainda, querem um vigilante, mas, não se pensa no perfil deste profissional de acordo com aquilo que a organização espera para sua atividade, ou ainda, contratam empresas que não tenham a devida autorização para o fornecimento dos serviços. Os exemplos recentes de uma rede de supermercados, referentes à forma como sua equipe de segurança respondeu ao problema, mostram que uma ação de segurança mal planejada ou executada pode ser mais cara para a organização de que o prejuízo que esteja procurando evitar.

Há ainda a ilusão de que somente uma arma irá resolver o problema e temos visto nos noticiários que muitas vezes, a presença de armamento no posto de trabalho serve mais para atrair os bandidos, interessados na arma, do que qualquer outro bem da organização. Assim, da mesma maneira que citamos o exemplo do médico, sistemas de segurança precisam ser pensados de acordo com a realidade de cada organização e focados em atuar nas reais e principais necessidades da empresa, o que equivale dizer que antes de se implantar qualquer mecanismo de segurança será necessário um diagnóstico adequado, conforme apontado anteriormente. E isso não pode, e não deve ser realizado por qualquer pessoa. É preciso ter profissionais qualificados, habituados à percepção de riscos e com conhecimento amplo sobre negócios e segurança.

As próprias empresas que comercializam produtos e serviços de segurança muitas vezes focam somente em "vender", o que é plenamente compreensível, porém, precisam também, estas organizações, não se municiarem somente de vendedores, mas, de consultores de segurança experientes que possam inclusive agregar valor aos serviços que prestam e produtos que vendem. Que possam compreender o real problema de segurança de seu cliente para oferecer uma solução possível numa relação interessante de custo x benefício.

Na pesquisa de Souza et al. (2017), os principais motivos que têm levado as empresas ou mesmo pessoas particulares a contratarem serviços na área da segurança é em primeiro lugar a insegurança com a criminalidade vigente nas cidades, visando

prevenir a perda de seus bens. Outro motivo é tentar estabelecer um controle social (práticas mais adequadas de comportamento) nas pessoas que veem e sabem que existem sistemas de segurança no local e ainda em virtude de exigências legais e de seguradoras. Porém, é preciso refletir que somente sistemas adequados à realidade da empresa, integrados e bem instalados oferecerão a estas empresas aquilo que buscam quando desejam adquirir os produtos ou serviços. E mais, é preciso haver a perspectiva de manutenção preventiva e corretiva, e mesmo, revisão dos planos de segurança, visto que os riscos migram e modificam-se com o tempo e circunstâncias de um negócio ou localidade.

O fato de a segurança ser algo inerente ao viver das pessoas, e uma necessidade básica, como afirma Maslow, não significa que estruturar um plano de segurança ou uma ação de segurança seja algo simples e separado da realidade das organizações em que se quer implantar. É ainda Meirelles (2011) que afirma a necessidade de 3 perguntas estratégicas serem respondidas: O que se quer do sistema de segurança? O que é permitido fazer? O que o sistema de segurança sabe fazer? Perguntas essenciais juntamente com os recursos disponíveis e o alinhamento estratégico para a definição do sistema mais adequado à organização.

Isso é um alerta, portanto para que as organizações busquem profissionais da área de segurança que tenham experiência e qualificação para tal, que as escolas de formação destes profissionais se adequem as novas realidades do mercado e principalmente que os próprios profissionais invistam na sua qualificação, não só com cursos e diplomas, mas, no desenvolvimento de habilidades essenciais a qualquer negócio na atualidade e ofereçam às empresas muito mais do que uma câmera, um alarme ou qualquer sistema isoladamente.

REFERÊNCIAS

MEIRELES, N. R. Gestão Estratégica do sistema de segurança: conceitos, teorias, processos e prática. Sicurezza. Coleção gestão de riscos. São Paulo. 2011.

LIMA, S. A. Manual de Consultoria em segurança empresarial. Editora Gregory. São Paulo. 2014.

RODRIGUES, S. A. Plano de segurança para as escolas do Estado de São Paulo: o controle eletrônico através das câmeras. 2009.

SABARA, M. T. Ribas; ALVES, Daniela Alves de. Disciplina e Controle: análise de uma rede de monitoramento visual.2015.

SOUZA; et al. Câmeras de segurança e seus sistemas tecnológicos: percepções sobre os motivos da utilização. Anais do XIV SEGET. Rezende. 2017.

Quer ficar por dentro de todas as novidades relacionadas a Governança, Riscos e Compliance?

Se inscreva nas nossas plataformas digitais e assine a nossa Newsletter para receber conteúdos gratuitos mensalmente.

Acesse aqui!

Além disso em nosso canal do Youtube você tem acesso a playlists exclusivas e gravações de eventos já realizados.

Patrocinadora oficial da

Revista

MÁS SEGURIDAD

Servicios informativos de y para la industria

REVISTA
GESTÃO DE RISCOS

Brasiliano INTERISK
Inteligência em Riscos

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

www.brasiliano.com.br

Publisher: Antonio Celso Ribeiro Brasiliano

Edição: Enza Cirelli

Edição de arte: Marina Brasiliano

Edição de texto com supervisão: Marcos Junior

Foto da capa: Antonio Brasiliano

Edição 157 - Abril/Maio 2021 | ISSN 1678-2496N

Data de publicação: 26 de agosto de 2021

A revista Gestão de Riscos é uma **publicação gratuita** eletrônica e online da Brasiliano INTERISK

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