COLETÂNEA DE ARTIGOS

EDIÇÃO III - 2021

SUMARIO

SUMARIO

SUMARIO

INTRODUÇÃO

As organizações estão inseridas em um ambiente altamente competitivo. Esta realidade obriga as empresas a serem eficazes eficientes e efetivas. Os lucros estão cada vez menores e o preço de seus produtos e/ou serviços são ditados pelo mercado. Para que as margens de lucro sejam compatíveis com as suas necessidades, as organizações precisam melhorar os seus processos e nesta busca o gerenciamento de risco é fundamental. Além desta vertente empresarial, outro ponto tem afetado o sucesso das organizações, o aumento da criminalidade. Aumento este, decorrente de uma série de fatores, dentre eles a falência do Sistema Público de Segurança. A soma de fatores empresariais e públicos tem potencializado a importância da Segurança Empresarial na obtenção do sucesso corporativo. Com esta potencialização, fez surgir a necessidade de departamentos de segurança com atuação científica, ou seja, não se admite mais o empirismo ou o "achismo" nas ações de segurança. Este contexto fez elevar o nível da prestação de serviços terceirizados de segurança ou de sistemas orgânicos de segurança. Para gerir o Sistema de Segurança é necessário um profissional altamente qualificado. Uma pessoa que gerencie de forma científica. Que saiba interagir a teoria com a prática. Alguém que tenha as competências (conhecimento, habilidade e comportamento) necessárias para ajudar a empresa a ser altamente competitiva. Esta necessidade criou a base para o surgimento dos cursos de graduação e pós-graduação na área de Segurança Empresarial. Cursos que são multidisciplinares e focados na prática. Mas para que os cursos cumpram com a sua missão é fundamental a existência de fontes de consulta. Não existe nenhuma dificuldade para a aquisição ou consulta de livros, dvds e periódicos nas áreas de

engenharia, administração, direito, psicologia, ética, comunicação, economia, dentre outras. O mesmo não acontece com a área de segurança. Não podemos negar que já temos alguns livros, dvds e períodos, mas não na quantidade e qualidade que a evolução do segmento necessita.

Baseado no exposto acima, é que estamos lançando mais uma edição da COLETÂNEA DE ARTIGOS. Uma coletânea de artigos que busca dotar os gestores dos conhecimentos necessários para serem capazes de fazer uma gestão científica e alinhada com a estratégia da empresa. Não queremos afirmar que os assuntos abordados nos diversos artigos estão esgotados, mas pontos importantes foram abordados. Além de abordarmos os pontos principais, temos o objetivo de despertar nos leitores a percepção da importância de aprofundamento dos diversos temas. São artigos produzidos por nossos sócios.

DESEJAMOS AOS LEITORES UMA ÓTIMA LEITURA E MUITO SUCESSO NA GESTÃO DOS SEUS DEPARTAMENTOS OU EMPRESAS.

ASCENSÃO NA CARREIRA DO PROFISSIONAL DE VIGILÂNCIA

Anderson Moura, MBS, CPSI, CIGR, CIEIE, EAR, MBA
Gestor de Segurança Empresarial

Por certo a ascensão profissional de vigilância no Brasil não é uma missão muito fácil de ser cumprida. Com frequência sou indagado sobre a “mágica” da evolução da minha carreira na segurança privada. Norteado por esta demanda resolvi escrever este artigo para contribuir com os colegas que visam crescimento na área.

Iniciei minha carreira na segurança patrimonial em 1999, aos 18 anos, como Porteiro na Empresa Servus Serviço de Mão de Obra (do grupo Vigor Vigilância que entrou em falência no mesmo ano). Como “agravante” em ato contínuo ao meu alistamento no Exército Brasileiro fui dispensado por excesso de contingente. Essa foi a maior barreira que tive que enfrentar por muitos anos na minha carreira profissional. Cabe-se aqui um agradecimento muito especial ao Amarildo Moraes, hoje Diretor de Negócios na Verzani & Sandrini que foi a pessoa que me concedeu a primeira oportunidade na área, a qual no ano passado (2020), após 21 anos, já como tomador do serviço de segurança patrimonial tive o prazer de encontrar e agradecê-lo pessoalmente.

No primeiro dia de trabalho, em 22 de fevereiro de 1999, realmente não possuía noção da minha tarefa e/ou objetivo naquele posto de serviço. Tratava-se de um condomínio comercial na região da Vila Olímpia (São Paulo – SP), onde diversas multinacionais possuíam sede. Ressalta-se que até então eu havia trabalhado apenas em metalúrgicas, pois minha formação profissional na época era de Ajustador e Torneiro Mecânico pelo SENAI, não tendo qualquer experiência em segurança patrimonial.

Por isso, com a doutrina aprendida no SENAI, observei a postura e a maneira de atuação dos profissionais mais experientes, o Supervisor (orgânico) e Vigilante Líder (terceirizado), percebendo como se davam às abordagens junto aos condomínios, prestadores de serviços, visitantes e subordinados. Não obstante, utilizei a mesma lógica com os colegas de trabalho e a partir deste momento percebi claramente o que eu deveria e não deveria fazer como profissional de portaria.

Neste sentido já temos o "Primeiro Capítulo da Mágica". Não importa qual a sua função saiba claramente qual o objetivo do seu posto de serviço.

Atuei nas folgas trabalhadas, conhecidas no meio como "FTs", em alguns Shoppings Centers de São Paulo. Foi uma grande experiência, já que a estrutura de segurança patrimonial de um Shopping Center é muito robusta, destacando-se o Plano de Segurança, a distribuição tática dos postos de serviço, suas áreas de coberturas, os protocolos junto aos condôminos (lojistas), os aparatos de segurança eletrônica e etc.

Além disso, ressalta-se a diversidade do público e os múltiplos serviços ofertados naquele espaço. Com isso aprendi o "Segundo Capítulo da Mágica" a importância da educação. Sem sombras de dúvidas, percebi, muito rapidamente, que as abordagens e interações com emprego da educação eram altamente eficazes. O emprego da educação no conflito evita o confronto.

Em 2001, já com 21 anos, após concluir o curso de formação obtive minha primeira promoção assumindo a função de vigilante na Estrela Azul Serviços de Vigilância, Segurança e Transporte de Valores. Logo no início, atuei em algumas instituições bancárias, sendo certo que em poucos dias aprendi, trabalhando armado na porta giratória o "Terceiro Capítulo da Mágica". Todo profissional de segurança deve ter inteligência emocional. Trata-se da capacidade de identificar e lidar com as emoções e sentimentos pessoais e de outros indivíduos.

Após dois anos, em 2003, ainda como empregado da Estrela Azul fui efetivado como vigilante na sede de uma empresa multinacional americana de geração e distribuição de energia elétrica. Passados dois anos, em 2005, a referida empresa mudou de endereço passando a ocupar por inteiro um edifício comercial na Vila Olímpia, mesma região onde iniciei minha jornada em 1999. Neste movimento, fui destacado para atuar no posto da Automação Predial, uma espécie de central de segurança local com encargo de controlar por meio de computadores os sistemas de: Controle de acesso, elevadores, iluminação, portões da garagem, ar-condicionado central, alarme de incêndio e os equipamentos de gravação do sistema de Videovigilância (CFTV). Ficava ali o "Quarto Capítulo da Mágica" para manutenção do meu novo posto e avanço na carreira tive que buscar conhecimento. Nesse caso específico em informática, uma área que até então desconhecia completamente. Ainda neste ano, ingressei na universidade cursando Gestão de Segurança Empresarial obstinado pela busca do conhecimento.

No ano de 2007, já empregado da Evik Segurança e Vigilância dada falência da Estrela Azul em 2006, mas ainda no mesmo cliente, fui convidado a participar do processo seletivo para Central de Segurança Corporativa. Uma nova área gerida diretamente pela Segurança Empresarial daquela multinacional com emprego de mão de obra terceira.

Após ser aprovado pelo cliente, fui promovido a vigilante líder e aprendi o “Quinto Capítulo da Mágica” a manutenção e evolução somente viriam se eu me tornasse uma pessoa organizada, ou seja, organização era fundamental para liderar uma Central de Segurança nível Brasil. Após 9 meses de serviço, já formado na universidade, fui promovido a supervisor de segurança patrimonial daquela Central.

A grande notícia chegou em outubro de 2008, quando fui contratado como Técnico de Segurança Empresarial Junior daquela multinacional. Em ato contínuo veio o “Sexto Capítulo da Mágica” a humildade. Tal virtude caracterizada pela consciência das próprias limitações, modéstia e simplicidade. Eu sabia claramente onde desejava chegar, porém, nunca esquecendo de onde eu havia vindo. Como no ciclo PDCA, a partir deste momento e, até hoje, percorro recorrentemente os “Capítulos da Mágica” planejando e definindo metas, colocando em prática, analisando os resultados e consertando o que deu errado baseado nas lições aprendidas coletadas durante o processo. Este conjunto de ações são sustentadas pela busca cíclica por conhecimento, trabalho em equipe, dedicação, disciplina, educação, Networking e muita humildade e humanidade.

O “Sétimo Capítulo da Mágica” a disciplina. Não importa se você atua na segurança orgânica ou terceirizada obedecer às regras, aos superiores, aos procedimentos é um valor essencial para o profissional de segurança patrimonial carregar durante a sua trajetória no “Oitavo e Último Capítulo da Mágica” a humanidade. Jamais perca a humanidade durante sua ascensão profissional. Deve-se lembrar diariamente que seus liderados possuem dificuldades, necessidades, anseios e objetivos. Além disso, treinamentos recorrentes nos temas: Direitos Humanos e Uso Progressivo da Força são extremamente necessários e nunca estiveram em alta como atualmente. É importante ressaltar que uma ação indevida da vigilância compromete o tomador de serviço, a empresa de vigilância e todos os profissionais operacionais envolvidos no incidente.

Para concluir, trago uma reflexão inserindo ao tema uma analogia ao filme “O Resgate do Soldado Ryan” (1998). Para quem não assistiu ou não se recorda, segue a sinopse:

No dia 6 de junho de 1944, dia “D” da segunda Guerra Mundial, o Capitão Miller recebe a missão de comandar um grupo do Segundo Batalhão para o resgate do soldado James Ryan, o caçula de quatro irmãos, dentre os quais três morreram em combate. Por ordens do chefe Marshall, eles precisam procurar o soldado e garantir o seu retorno, com vida, para casa.

Após toda jornada, com diversas baixas no grupo liderado pelo capitão Miller, o soldado Ryan é localizado e, como não poderia ser diferente, havia uma missão a ser cumprida antes do seu retorno. Já ferido, na última frase antes de morrer, o capitão John Miller (interpretado pelo ator Tom Hanks) disse ao James Ryan (interpretado pelo ator Matt Damon): “JAMES FAÇA POR MERECER”!

Depois de muitos anos, já bem idoso, acompanhado pela sua família em visita ao túmulo do capitão, o Ryan declara ali que pensou por toda vida na frase dita pelo capitão em seus minutos finais e afirma ter honrado o feito por ele. Na cena final, o Ryan pede a sua esposa para ratificar ali, no túmulo do capitão, que foi um bom homem.

Refletindo acerca do tema é possível inferir que a carreira de um profissional de segurança privada é extremamente difícil, densa e cheia de dessabores o que requer o emprego dos “Capítulos da Mágica”: Objetivo, educação, inteligência emocional, conhecimento, organização, humildade, disciplina e humanidade. Por isso “FAÇA POR MERECER” cada degrau sobrepujado na sua ascensão profissional.

O QUE TRAZ A SENSAÇÃO DE SEGURANÇA – CONDOMÍNIOS

Carlos Köhler
Graduado em Segurança Pública, pós-graduado em Segurança Privada, Sócio Honorário CEAS-INTERNACIONAL, CEO do Grupo CINDAPA.

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 da 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 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 uma 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 dissimilou a ação criminosa para esta pessoa, os vigilantes são quem fornecem essa sensação de segurança. Agora vejamos um outro exemplo em que uma pessoa que seria roubada e foi dissimulada por ter sido visualizada nas câmeras de videomonitoramento na tentativa de subir o muro para invadir a sua residência e cometer o roubo. Para esta pessoa é bem mais provável que para ela o que traz a sensação de segurança são as câmeras de videomonitoramento.

Ambas tiveram estímulos diferentes, proporcionando experiências diferentes e, por consequência, respostas diferentes. São apenas exemplos que servem como uma metáfora para compreendemos 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 teve qualquer tipo de experiência, quais são seus estímulos que dariam a sensação de segurança? Podem ser inúmeros, principalmente a pré-disposição genética, o meio e as escolhas, entre outras; assim sendo, as sensações de segurança são diferentes para cada pessoa ou grupo de pessoas pelos estímulos a que esteve exposta. Há outras que foram afetadas pelas experiências e traumas que outros tiveram, uns se sensibilizam mais que outros. 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 ser para outro e vice-versa, assim como o que resolveu algum problema de segurança numa situação não indica necessariamente que resolverá em todos os outros. Da mesma forma, o que deu certo para um contexto 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 e sem 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 a subjetividade do indivíduo, enquanto que 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. AUTOR Carlos Köhler, CPSI, CISI, MBS e CRA

PREVENÇÃO DE PERDAS EM EMPRESAS DE SEGURANÇA PRIVADA

Antônio Mota, CPSI, DIDS
Divisão de Consultoria e Treinamentos
Consultoria e Assessoria em Segurança Privada
Mota Associados Consultoria

Na gestão de empresas especializadas de segurança privada, é necessário que os sócios, investidores, gestores administrativos e operacionais tenham visão de negócio, pleno conhecimento da legislação especifica do seguimento de segurança privada, também é necessário um planejamento estratégico para a gestão do negócio e de custos para otimizar os resultados quanto a satisfação de seus clientes/contratantes e haja lucratividade. Segundo publicação no site da FENAVIST recentemente, somente no ano de 2020 as empresas de segurança privada foram multadas em mais de 1 (um) milhão de reais por irregularidades cometidas pelas gestões, onde geralmente um simples prazo perdido, uma falta de comunicação de ocorrência com produtos controlados (armas, munições e coletes) em até 24 horas do ocorrido e até 10 dias do ocorrido com apresentação de relatório de procedimento apuratório e BO Policial, um transporte de arma sem a devida autorização da DELESP/PF, etc. geram multas causando impactos financeiros que as vezes torna inviável a continuidade do negócio da empresa e seus sócios se obrigam a cancelar suas atividades ou então alguns casos excepcionais migram para a ilegalidade já que alguns contratantes desconhecem a legislação e não cobram a documentação mínima necessária e obrigatória para uma empresa está devidamente legalizada para funcionar. Outro problema é falta de pessoas qualificadas e comprometidas para a gestão dos dados da empresa pelo sistema GESP - Gestão Eletrônica de Segurança Privada controlado e fiscalizado pela PF – Polícia Federal. Fazer gestão da empresa de segurança privada pelo GESP não é tarefa simples tendo em vista que a operação já tem a missão e outras tarefas para atender os clientes/contratantes e

a operação propriamente dita. Outro aspecto é o custo para manter um funcionário com pagamento de salários, encargos e demais benefícios, além dos riscos com passivo trabalhista. A alternativa econômica e viável é a terceirização da gestão dos dados e processos da empresa de segurança privada. Assim a prestação de serviços de gestão pelo GESP torna-se mais viável, econômica e os gestores não precisam se preocupar com mais essa demanda. Pois, na gestão de dados e processos, os gestores são informados e atualizados mensalmente quanto a todas as alterações e demandas com relação a empresa no GESP. As CNVs são devidamente expedidas em até 30 dias da contratação de qualquer vigilante e/ou renovadas após o vencimento no período de 5 anos. Também é atualizado com exclusão e/ou cadastramentos de vigilantes demitidos e admitidos, vinculação e desvinculação de armas de fogo, controle de coletes balísticos e processos de destruição de coletes vencidos para descartes conforme a legislação, entre outras demandas tais como: Alterações de Atos Constitutivos, processos de compra de armas, munições e coletes, Autorizações para transporte de armas, revisões anuais de autorização de funcionamento, etc.
Por tanto, fazer uma boa gestão de GESP e de custos operacionais de uma empresa especializada de segurança privada, resulta em lucratividade e mantém uma imagem positiva da empresa para seus contratantes, empregados e principalmente do órgão regulador e fiscalizador (DELESP/CGCSP/PF).

QUAL A IMPORTÂNCIA DO SISTEMA DE SEGURANÇA DO HOTEL PARA O HÓSPEDE?

Dr. Renato Santos Figueiredo,CPSI,CIGR,CISI,CIPSI,CIEIE,CEGRC,DIDS
Presidente CEAS-BRASIL e Secretário Geral CEAS-INTERNACIONAL, capítulo Brasil

Por que é importante contar com um sistema de gestão integrada para prevenir os riscos e garantir a continuidade de negócio?

A melhoria da qualidade dos serviços de um hotel é algo a ser perseguido. Nesta busca, as questões de segurança não podem ser menosprezadas. Para se responder a pergunta tema que leve a uma efetiva tomada de decisão, é necessário concentrar a atenção no cliente, uma vez que, para melhorar a qualidade, deve-se saber o que ele precisa e exige.

Para alcançar a qualidade, deve haver gestão e, para isso, é preciso implantar uma cultura de segurança na empresa. Não se trata de tomar algumas medidas isoladas para fornecer segurança, mas implementar uma mudança na visão organizacional. Do ponto de vista da estratégia corporativa, é necessário trabalhar: visão, missão, valores e princípios. Já do ponto de vista da estratégia pessoal, deve-se trabalhar: conhecimento, habilidade e atitude. Com estas estratégias, tende-se a alcançar mais EFICIÊNCIA no serviço, maior EXCELÊNCIA e mais SEGURANÇA.

A empresa deverá optar entre a necessidade de mudança de paradigma ou pela imobilidade. No meio desta realidade de mudança que leva a novas exigências, por que resistir a mudanças? Ou, nesse caso, por que negar que, se permanecer imóvel diante da demanda por mudanças, pode-se tornar a empresa ineficaz?

A partir do confronto entre optar por uma mudança ou manter-se apegado a esquemas antigos, surgirá uma nova cultura na empresa. A mudança proposta de acordo com

uma visão sistêmica não deve ser gerada verticalmente (topo da pirâmide para a base operacional), mas sim, a mudança deve ser operada e assumida em todas as áreas da empresa e todos os seus membros devem cooperar. Exemplo: a recepção do hotel geralmente está mais em contato com o hospede do que o Gerente Geral, para quem o hóspede faz comentários, reclamações.

É necessário criar a consciência da empresa como um todo, vista como um sistema, onde todas as pessoas devem contribuir para eliminar as falhas que podem surgir. A pessoa que recebe a reclamação deve informar ao setor correspondente de tal forma que, no menor tempo possível, o problema seja resolvido. Esta concepção da empresa como sistema, onde todos seus setores estão vinculados e cada área está capacitada para cumprir sua função, com um satisfatório grau de comunicação entre eles, é o que forma as bases para materializar o objetivo proposto, isto é: CONHECER O HOSPEDE E FIDELIZÁ- LO.

É necessário criar a consciência do trabalho em equipe. Para isso (como dito anteriormente) devem-se ter pessoas treinadas para cada função e um alto grau de comunicação entre as áreas. Mencionamos como objetivo: conhecer e fidelizar ao cliente-hóspede. Para isto é necessário:

- Identificar motivações, motivos e gostos.
- Avaliar o que se deve melhorar.
- Decidir como fazê-lo.
- Implementar controles
- Supervisionar.

Se segurança é uma prioridade nos dias de hoje, deve-se investir em um sistema de segurança nas vertentes preventiva e contingencial. Se um hóspede sair do hotel porque lhe foi roubado um objeto valioso, então cabe perguntar: A empresa investiu o suficiente para fornecer segurança? Se a empresa não investiu o suficiente, o que ela esperava da segurança?

Se na área da segurança não forem implementadas medidas de controle para reduzir os riscos, quem corre o risco não será somente o hóspede, mas também o hotel, o risco pode ser alto. A avaliação de riscos profunda pode minimizar resultados negativos e pode potencializar a segurança de todos.

A avaliação de riscos em cada cadeia de valor é uma parte importante da indústria hoteleira e turismo e por isso é relevante para qualquer empresa que planeje uma existência contínua.

Para reforçar a segurança, alguém (ou todos), em algum momento deve ter que denunciar algo ou dizer não. Isso pode ser difícil, especialmente se for percebido

que o colega de trabalho poderá ficar ressentido. Agora, se as mudanças forem implementadas corretamente, o funcionário deve saber que se ele denunciar a reclamação, por exemplo, para a área de manutenção, isso não causará a demissão de um funcionário.

A equipe deve ter clareza sobre quem faz o que e quando. Um programa realista de gerenciamento de qualidade deve ser implementado, de acordo com as dimensões, expectativas e recursos da empresa. Para as pessoas deve estar claro QUEM faz O QUE e QUANDO. A segurança não pode ser deixada de lado, mas deve ser planejada, enfatizando a adesão aos padrões. Para isso, deve existir:

- Consciência sobre a situação.
- Comunicação entre os diferentes setores.
- Liderança e autoridade.
- Trabalho em equipe.
- Tomada de decisão.

Isso significa gerar uma cultura de segurança, para a qual, além do feedback correto entre as partes, deve-se ter a capacidade de ouvir a necessidade de uma mudança no momento certo. Isso não significa mudança constante, porque neste caso a mudança se torna anárquica, mas uma vontade de ouvir as necessidades do hóspede no momento certo.

Cada funcionário deve ter conhecimento claro de qual é o seu papel, seu espaço dentro da empresa e sua função. Afirmar que a opinião de todos é necessária para gerenciar uma mudança de paradigma não implica ignorar que as decisões são feitas apenas por alguns. A decisão nunca é da ordem da horizontalidade, alguém deve assumi-la e torná-la concreta.

Aquele que toma a decisão de uma mudança, orientada para implementar uma política de segurança, deve ter a capacidade de liderar o caminho, e isso não significa apenas comando. Toda empresa deve estar ciente de seus pontos fortes e fracos, reforçar o primeiro e eliminar ou reduzir o último.

Alguns requisitos dos diferentes grupos de interesse são: Hóspedes: Querem um alojamento seguro; Pessoal: Querem um lugar de trabalho seguro; Investidores: Querem que o hotel proteja os ativos e a propriedade para garantir sua continuidade e êxito; A corporação: Deve garantir a segurança e a saúde dos empregados que viajam ao estrangeiro; Autoridades: Esperar que o hotel cumpra com todos os procedimentos de segurança.

A avaliação de riscos de um hotel, como de qualquer organização é uma parte importante da segurança corporativa. Os eventos que se podem minimizar, como incêndios, acidentes e lesões podem ser minimizados, contribuindo assim à continuidade do negócio.

A SEGURANÇA em um hotel é uma mudança que deve ser implementada ou reforçada, este modelo de negócios, como um SISTEMA EFICAZ, é uma proposta de ação.

AS BASES DO PROGRAMA DE COMPLIANCE

Professor Dr. Nino Meireles,CPSI,CIGR,CIEIE
Diretor de Formação e Extensão Universitária CEAS-BRASIL

Um programa de compliance deve ser sustentado em nove pontos importantes: apoio da alta administração, riscos, código de conduta e política de compliance, controles internos, treinamento e comunicação, disque denúncia, investigação interna, due diligence e auditoria e monitoramento.

APOIO DA ALTA ADMINISTRAÇÃO

É essencial o apoio da alta administração. Este apoio é demonstrado mediante:

- Declarações escritas para os colaboradores com o objetivo de comunicar e documentar os padrões éticos da empresa.
- Estar presente nos treinamentos de compliance.
- Engajamento e envolvimento na prevenção.
- Deve aderir às regras e ser um exemplo de bom comportamento.

RISCOS

É importante que, antes de se falar em riscos, se conheça os objetivos da empresa e do programa de compliance, pois o código de conduta, as políticas e os esforços de monitoramento deverão ser construídos com base nos riscos que forem identificados.

CÓDIGO DE CONDUTA E POLÍTICA DE COMPLIANCE

Após a identificação, análise e avaliação de riscos e a identificação de leis, regulamentações, códigos aplicáveis as operações, inicia-se a elaboração da política de compliance.

Essa documentação serve como a formalização daquilo que é a postura da empresa em relação aos diversos assuntos relacionados às suas práticas de negócios, e servirá como um norte que guiará os colaboradores para o caminho das práticas éticas e legais na condução das suas atividades. Principais políticas de compliance: anticorrupção; interação com entidades e setor público; cortesias comerciais; viagens e entretenimento; gestão de propriedade intelectual; conflito de interesses.

Na construção do código de conduta os pontos a serem levados em conta são:

- Mensagem do presidente.
- Linguagem acessível.
- Objetivo.
- Perguntas e respostas.
- Introduzir cada um dos assuntos relevantes para o programa de compliance.

CONTROLES INTERNOS

São mecanismos que asseguram que os livros e registros contábeis e financeiros reflitam os negócios e operações da empresa, conforme requerido por diversos instrumentos, como a Lei Sarbannes-Oxley.

Os controles internos estabelecem as regras para revisão e aprovação de atividades, existência das atividades, documentação suporte, processamento e registro das transações. Os controles internos podem ser considerados eficientes e eficazes se:

- Os objetivos das operações estão sendo alcançados.
- As demonstrações financeiras publicadas são preparadas de maneira confiável.
- As leis e regulamentos aplicáveis estão sendo cumpridos.

TREINAMENTO E COMUNICAÇÃO

Cada colaborador do topo da pirâmide à base operacional deverá entender os objetivos do programa de compliance, as regras e o seu papel para garantir o sucesso do programa.

DISQUE DENÚNCIA

Fornecem aos colaboradores e parceiros comerciais uma forma de alertar a empresa para potenciais violações ao código de conduta, a outras políticas ou mesmo a respeito de condutas inadequadas de colaboradores ou terceiros.

INVESTIGAÇÃO INTERNA

A empresa deve possuir processos internos que permitam investigações para atender às denúncias. Esses processos devem garantir que os fatos sejam verificados, responsabilidades identificadas e, em sendo necessário, definir as sanções e ações corretivas mais apropriadas a serem aplicadas.

DUE DILIGENCE

Empresas que realizam negócios por meio de parceiros, representantes ou revendedores devem adotar um processo de avaliação prévia à contratação (Due Diligence) para entender a estrutura societária e situação financeira do terceiro, bem como levantar se existe histórico de práticas comerciais antiéticas ou que, poderá expor a empresa a um negócio inaceitável ou que envolva riscos legais.

AUDITORIA E MONITORAMENTO

Processo constante para identificar se as bases do programa estão funcionando.

COMPLIANCE NAS ORGANIZAÇÕES

Professor Dr. Nino Meireles,CPSI,CIGR,CIEIE
Diretor de Formação e Extensão Universitária CEAS-BRASIL

A origem da palavra compliance verbo em inglês to comply que significa: cumprir, obedecer ou atender. A expressão é usada com o significado de estar em conformidade com regras, legislação e normas.

Risco de compliance é definido como risco legal, ou de sanções regulatórias, de perda financeira ou de reputação que uma empresa pode sofrer como resultado de falhas no cumprimento de leis, regulamentações, códigos de conduta e das boas práticas entre organizações. Para entender perda de reputação deve-se partir do pressuposto que essa se baseia na síntese de como os clientes, funcionários e acionistas vêem a organização. As principais subáreas são: risco de legislação, risco de contrato e risco tributário.

Compliance é uma questão de ética. O programa de compliance deve auxiliar funcionários na resolução de situações não cobertas pela legislação e tem dois objetivos: prevenir a ocorrência de infrações e demonstrar a eficácia dos controles. É importante saber quais normativas e leis são aplicáveis à empresa e qual a melhor maneira de se ajustar a elas e cumpri-las.

Programas voltados à boa conduta e programas de compliance devem estar integrados, pois se baseiam em valores e responsabilidade morais, bem como no cumprimento e conformidade das leis e políticas internas. Em uma economia em que 70% a 80% do valor do mercado vêm de ativos intangíveis de difícil avaliação (valor da marca, capital intelectual), a empresa torna-se vulnerável a tudo que possa prejudicar sua reputação.

SISTEMA DE COMPLIANCE

PREVENIR

- Gestão de riscos de compliance - Análise das operações da empresa com o objetivo de detectar os riscos de compliance e introdução de medidas para minimizar os riscos são os elementos chaves.
- Políticas e procedimentos - O código de conduta é o elemento chave do sistema de compliance. Nele se definem as normas de conduta essenciais.
- Formação e comunicação - As normativas são ineficazes se os colaboradores não as conhecem e não sabem como pôr em prática. Um dos elementos chaves para a implantação do sistema de compliance é a formação.
- Conselho e apoio - Dar conselho e apoiar as unidades de negócio é uma das funções principais do sistema de compliance.
- Coletividade - Uma empresa sozinha pode lograr resultados limitados na luta contra a corrupção. Para obter avanços substanciais é necessária uma atuação conjunta de todos ou ao menos, do maior número possível de participantes do mercado.

DETECTAR

- Canais de denúncia - Dispor de canais de denúncia e proteção ante possíveis sanções de colaboradores que informam sobre possíveis condutas indevidas.
- Controles - Com o objetivo de elevar a eficiência do sistema de compliance deve-se implantar um conjunto de controles que inclui tanto controles anticorrupção como controles antifraude.
- Revisão - O sistema deve ser avaliado permanentemente para poder localizar melhorias.
- Auditorias - Revisão periódica da implantação do Compliance Control Framework.
- Investigações - Processo de investigação dotado de recursos para analisar as possíveis infrações de compliance.

GESTOR DE COMPLIANCE

Responsável por saber que normativa(s) e lei(s) são aplicáveis à empresa e qual é a melhor maneira de ajustar-se a elas e as cumprir. Deve ter conhecimento amplo de leis e normas. Recomendável que conte com ampla experiência em assessorias jurídicas e/ou fiscais.

Deve ter expertise na definição e implementação de planos de compliance e no uso de metodologias e ferramentas que facilitam e agilizam seu trabalho.

MÉTODO

Definir objetivos

> A Norma ISO 19600:2015 é uma referência aplicável a qualquer empresa e oferece as diretrizes para implementar, avaliar, manter e melhorar um sistema de compliance.

Acompanhar mediante indicadores

> Verificar se os objetivos de compliance estão sendo alcançados. Permite ao gestor de compliance saber qual é o nível de risco atual, comunicá-lo à direção e desenvolver um plano de melhorias.

Utilizar métodos de análise de riscos

> Com o objetivo de detectar os riscos de compliance e introduzir medidas apropriadas para a minimização de riscos. Analisar e avaliar os riscos segundo seu impacto e sua probabilidade mediante alguma metodologia.

Monitorar

> Toda a informação gerada deve ser rastreada.

Gerar evidências

> No caso de se cometer alguma infração, um bom programa de compliance deve estar desenvolvido de maneira que possa demonstrar que existiam controles para evitá-lo e que estes eram eficazes.

Segregar funções

> Para evitar que uma única pessoa ou um único departamento leve a cabo tarefas incompatíveis que possam dar lugar a fraude, é recomendável segregar funções.

Elaborar um código de ética

É recomendável criar um Código de Ética e distribuí-lo para todos os departamentos.

Canal de denúncia

Para investigar casos de fraude, é importante existir um canal de denúncia (interno e externo), de forma que tanto colaboradores como clientes, fornecedores ou outros grupos de interesse possam denunciar condutas contrárias ao Código de Ética por parte de um colaborador ou um departamento.

A GESTÃO DE PESSOAS COMO FATOR DE SUCESSO

Dr. André Vicente dos Anjos, CPSI, CIGR, CIEIE, DIDS

Coordenador de Segurança Sênior do segmento varejo. Ph.D. pela Cambridge University. Doctor en Ciencias de la Seguridad pela Corporación Euro-Americana de Seguridad (Espanha). Graduado em Segurança Pública e Privada com Pós Graduação em Criminologia, Segurança Contra Incêndio e Pânico, Segurança e Ordem Públicas. Atua como docente da UNICEAS BRASIL e CEAS-BRASIL.

É muito comum nos congressos e encontros, interagindo com colegas do segmento, ouvir relatos de insatisfação com baixa performance e do desejo de substituir a empresa prestadora de serviços por dificuldades ou falhas observadas no cumprimento de suas atividades.

O detalhe curioso deste cenário é perceber que a maioria dos tomadores de serviço, mesmo tecendo ácidas críticas, exige da nova contratada o aproveitamento dos colaboradores da empresa anterior, respaldando-se nos argumentos de conhecimento da planta, critério de confiança, familiaridade com a equipe ou até pelo carisma, observado em determinado membro ou membros do time.

Não obstante, esse fato pode ser visto por diferentes prismas, significando, inclusive que a insatisfação se foca na organização (prestadora de serviços) e não na equipe e, por esta razão, é muito comum observar profissionais atuando no mesmo posto por mais de 20 anos, ratificando a teoria predominante de que o ser humano é o maior ativo de qualquer organização e grande diferencial competitivo do ponto de vista de cumprimento dos objetivos das corporações pelo mundo.

Vejamos. Não se objetiva aqui, nestas poucas linhas, avaliar quais os impactos deste contexto, mas observar a situação sob a ótica do cliente, que figura como parte mais interessada na excelência dos serviços entregues. Contudo, como não ponderar o fato de que a entrega de resultados é inerente ao capital intelectual e que, se os objetivos

contratuais não foram alcançados, qual a razão provável para a manutenção da mesma equipe em outra empresa?

Face a complexidade do assunto e da subjetividade que o reveste, consideramos inserir no conteúdo os resultados de uma pesquisa feita pela American Society for Quality (ASQ), uma das maiores associações do mundo, dedicada aos estudos, práticas e ferramentas destinadas a qualidade. A pesquisa feita pela ASQ apontou as principais causas que tem levado a perda de clientes e o resultado aponta que 79% das empresas abrangidas pela pesquisa deixou de ser cliente pelo modo como se sentiram tratados, seja por indiferença ou por reclamações não atendidas, ou seja, a falta do feedback nas demandas levadas pelos clientes figura em destaque na lista dos cinco maiores fatores.

	CAUSA	%
1º	Indiferença dos atendentes	65
2º	Reclamações não atendidas	14
3º	Vantagens oferecidas pela concorrência	10
4º	Mudança de endereço ou perda de referências	5
5º	Relações comerciais	5

FONTE: The American Society for Quality

A análise põe em destaque a área de suporte (atendimento ao cliente), haja vista ser o departamento responsável por acolher as demandas e identifica ainda a empatia como uma das competências mais relevantes no momento do atendimento aos clientes, não por acaso, esta importante competência está diretamente ligada aos fatores de insatisfação mais bem ranqueados.

Contudo, existem ferramentas que possibilitam a mitigação de um cenário de desgaste, como o marketing de relacionamento, por exemplo, que visa estreitar as relações, criando sinergia entre o cliente e o prestador de serviços, pautando seu foco em ações e atitudes que visam a antecipação dos desejos e necessidades, antes mesmo de serem expressadas.

Sim. O cliente é a razão da existência de qualquer negócio e a forma como as empresas se relacionam com eles é tão salutar que já existem departamentos exclusivos com este foco, atuando na captação, retenção (fidelização) e recuperação de clientes perdidos. Cliente é ouro!

Vale ressaltar que, nem o CNPJ, que é apenas um cadastro na junta comercial e nem o nome de uma empresa, mesmo que seja o mais emblemático e impactante, entregam resultados. A entrega dos serviços propostos por qualquer organização, ainda que esta possua o mais alto nível de avanço tecnológico, será sempre dos

recursos humanos e este é um fato inconteste. Não por acaso, Stephen Richards Covey, escritor e autor do best-seller administrativo Os Sete Hábitos das Pessoas Altamente Eficazes, apregoava: “Trate sempre os seus funcionários exatamente como quer que eles tratem os seus melhores clientes”.

Empresas comprometidas com o bem estar do seu maior ativo, se submetem anualmente ao crivo avaliativo do time, através de uma rigorosa pesquisa de clima organizacional chancelada pela empresa de consultoria global Great Place to Work, pois se interessam, de fato, em conhecer e entender as opiniões de seus colaboradores, considerados fundamentais para o cumprimento dos objetivos estratégicos.

Já passou da hora dos empresários perceberem que a relação com seu maior ativo vai além do compromisso de efetuar o pagamento na data acordada, proporcionar infraestrutura e uniformes adequados, fornecer EPIs e EPCs em conformidade com as normas vigentes. Estes são quesitos básicos e obrigatórios. A gestão de pessoas deve ser pensada como um subsistema do macro sistema organizacional, de modo que haja a sinergia entre o desempenho do capital humano e o objetivo da organização.

Valorize o seu maior ativo. Ouvir o time já é um bom começo.

INTELIGÊNCIA NA SEGURANÇA: O APRENDIZADO EM ESCALA

Eder Menezes, EAS, CPSI, CIGR, CIEIE

Fundador e Presidente da Security Project & Consult; Especialista em Segurança Empresarial; Graduado em Gestão de Segurança Privada pelo Centro Universitário Internacional Uninter; Graduado em Gestão em Segurança e Defesa Cibernética pelo Centro Universitário Internacional Uninter; Instrutor de Segurança Patrimonial credenciado pela Policia Federal; Especialização em Comportamento de Excelência pela Strong Esags Escola Superior de administração e Gestão e pela Faculdade de Engenharia de São Paulo no curso Avançado em Segurança Empresarial - MBS Master Business Security - BRASILIANO INTERISK Gestão de Riscos Corporativo

A Inteligência compreende ações de obtenção de dados associadas à análise para sua compreensão. A análise transforma os dados em cenário compreensível para o entendimento do passado, do presente e para a perspectiva de como tende a se configurar o futuro (ABIN Agencia Brasileira de Inteligência) A inteligência integrada à segurança é uma ferramenta de alto valor e intrínseca na gestão moderna na segurança corporativa. Em um mundo que se transforma rapidamente, com novas dinâmicas de negócios e demandas dos clientes, os métodos tradicionais não são mais uma garantia de sucesso. As organizações precisam redefinir suas estratégias de crescimento, seus modelos de negócios e até mesmo a própria noção de trabalho para acompanhar as mudanças e prosperar.

A velocidade das transformações no mundo globalizado e as constantes alterações nas condições ambientais das empresas, bem como a redução das distâncias e a veemência da troca de informações, enfatizam a necessidade da manutenção de um sistema de inteligência. O ambiente corporativo está vivenciando o chamado Mundo VUCA, uma sigla representada para definir a volatilidade (volatility), a incerteza (uncertainty), a complexidade (complexity) e a ambiguidade (ambiguity) nos ambientes e nas situações de negócio (BRASILIANO 2016).

A Inteligência faz uso de análise e de dados disponíveis nas diversas áreas do pensamento. A longe disso, efetua realizações em busca de dados com uso de técnicas periciais, desenvolvidas por meio de capacitação específica.

A técnica oferece ao qualificado de Inteligência acesso a dados que não estão disponíveis ao pesquisador ou ao público em geral e a dados que são protegidos impropriamente por aqueles que os possuem.

A Inteligência tem ainda a instigação de tratar os dados alcançados, atribuir fidúcia e obter um significado de agregação, treinamento e utilização das técnicas requer conhecimento do processo de diversas áreas.

Os dados têm sua credibilidade avaliada no processo de análise e são apreciados a partir de metodologia específica de criação do entendimento da Inteligência. Outras metodologias de análise que possam apoiar a produção do entendimento são também empregadas. A análise permite a compreensão dos fenômenos e a elaboração de cenários prospectivos que orientam a tomada de decisões. (ABIN Agencia Brasileira de Inteligência)

A INTELIGÊNCIA A PARTIR DAS "BORDAS".

A inteligência como parte de inovação e transformação vêm das bordas. O exemplo do que ocorre com os órgãos de segurança pública, a segurança privada deve programar uma atividade de inteligência com a finalidade de dar suporte ao planejamento e execução de suas atividades, de forma a agir preventivamente e preferencialmente antes da ocorrência de um fato previsível e evitável. Inteligência é Inovar, que significa criar um produto ou serviço diferente para expandir ou conquistar novos mercados. Nesse contexto, a melhor maneira de impulsionar a atividade de inteligência nas organizações é pelas bordas. Isso significa identificar as áreas problemáticas e desenvolver ações para obter, analisar e disseminar informações que interfiram de forma positiva ou negativa na segurança da organização e que permitam ações preventivas, a contar de que seja possível entender as forças exponenciais que estão por trás da organização.

Neste contexto, o controle da Inteligência para o secretariado em níveis mais elevados de decisão e caracterização de políticas na planície da segurança privada deve ser analisado pela alta gestão, no nível de direção das organizações, sendo responsável pelas ações em longo prazo e que prepara para os acontecimentos futuros, sempre com base nos propósitos traçados em planos estratégicos.

INTELLIGENCE OUT / INTELLIGENCE IN UMA VISÃO DE LONGO PRAZO.

Esta é a principal diversidade desse entendimento. Desenvolvi uma abordagem chamada “intelligence out / intelligence in”. O “Intelligence out” consiste em olhar para frente, projetar como será o plano de inteligência estratégica daqui a 5 a 6 anos e monitorar quais os tipos de empresas ou de negócios que terão sucesso nesse período. A “Intelligence in”. Trata-se de um movimento contínuo, de entrada – olhar para um futuro, mas detectar as oportunidades do hoje, do agora, programar as transformações necessárias para chegar lá, sem perder o foco no futuro.

OS PRINCIPAIS PONTOS DE ATENÇÃO PARA ESSE MODELO?

Uma das sugestões é que as organizações encontrem uma borda que seja complementar ao negócio existente. Uma equipe de inteligência bem composta proporciona ao gestor uma maior tranquilidade e aumenta a capacidade de concretização de planos e certamente maior poder de resposta diante de situações difíceis. Tal equipe tem plena convicção da importância de suas atribuições, sendo assim esse é um tipo de recurso indispensável para um gestor moderno. Para alcançar esse objetivo devemos nos cercar de pessoas competentes e que realmente tenham conhecimento na área, geralmente essas pessoas são apaixonadas pela sua área de atuação trabalham pelo prazer de produzir conhecimento, transformam informações insuficientes e imprecisas em dados razoáveis e utilizáveis para que a alta gestão tomem as melhores decisões e na hora certa.

COMO OS LÍDERES ESTÃO LIDANDO COM ESSAS MUDANÇAS?

Acredito que há uma percepção crescente de profissionais de inteligência ao redor das empresas de segurança corporativa e que o mundo está mudando de uma forma que eles não entendem completamente. Parte da necessidade envolve aumentar a conscientização sobre os impactos dessas mudanças. O medo de assumir os riscos e errar os diagnósticos é imenso. Inovar com inteligência implica tomar caminhos desconhecidos e há sempre riscos associados à inovação. As grandes empresas têm a cultura de minimizar riscos. As organizações têm de capturar as novas oportunidades que surgem dessas mudanças. Elas precisam utilizar de um time de inteligência inovador, precisam laborar como nunca fizeram antes e encontrar novas maneiras de criar valor – e isso requer inteligência para inovar.

A tática lida com a forma de batalha individual e a estratégia com o seu uso. Pensar com inteligência e estrategicamente não é uma ciência exata, pensar significa meditar, construir ideias relacionadas, refletir sobre algo. Embora instituído em um ramo do entendimento humano, não há como ensinar um administrador ou toda uma organização a utilizar um plano de inteligência. A consequência da desinformação,

do desinteresse por parte da alta gestão, reflete-se, consequentemente, em toda a organização e pode ser perigoso, sobretudo em virtude do não entendimento por parte do gestor do valor estratégico que as suas decisões podem causar na organização. Desde as eras mais primitivas, o homem se utilizava de processos que continuam em franca evolução. A cada dia, surgem novas teorias e modelos que orientam as corporações nessa fascinante missão de superar os desafios impostos pelo mercado e pelas demandas sociais. A cada dia, o mercado limita os espaços para profissionais com atuações amadoras. É imprescindível que o profissional de Segurança Privada ou Pública se mantenha em processo de evolução acadêmica e qualificação intelectual contínua, pois o mercado exige e os desafios demandam conhecimentos.

DESAFIOS E OPORTUNIDADES PARA UMA NOVA LIDERANÇA EM SEGURANÇA PRIVADA NA ERA PÓS-COVID-19

Manuel Sánchez Gómez - Merelo
Consultor Internacional de Seguridad Pública y Privada
Presidente · Director General de GET (Grupo Estudios Técnicos)
Director de Programas de Seguridad del Instituto Universitario General Gutiérrez Mellado IUGM-UNED

Como resultado da análise VUCA e DAFO, a atual situação apresenta uma visão de grande incerteza: um presente sombrio e um futuro imprevisível. Por isso, temos que nos reinventar para passar de um terreno baldio para um próspero, detectando novas oportunidades.

É preciso uma nova leitura da globalização tal e como a conhecemos até agora, contemplando os novos e grandes desafios, exigências e oportunidades.

Tanto as organizações como os gestores estão vivenciando uma autêntica revolução condenada a diferentes abordagens e mudanças de paradigma, que nos permitem atuar por meio de novas estratégias baseadas no conhecimento e na inteligência.

Neste novo mundo global, é necessário que os líderes e membros de equipes tenham capacidade para gerir com uma visão holística, para compreender e fazer frente a entornos multidisciplinares e complexos.

Terá que trocar atitudes e paradigmas na liderança de equipes, uma mudança radical na cultura corporativa. Temos que potencializar a inteligência emocional e a estratégia em toda a organização, começando pelo comitê de gestão.

CINCO NOVAS ESTRATÉGIAS PARA O ATUAL ENTORNO VUCA:

Cada dia que passa, o mundo VUCA (Volátil, Incerto, Complexo e Ambíguo) se torna

mais presente e isso impacta diretamente na maneira que pensamos e atuamos estrategicamente.

- Potencializar os pontos fortes. comprovar a eficiência de seus pontos fortes e identificar áreas de melhoria, já que a atualidade exige novas habilidades diretivas para realizar mudanças.

- Reorganizar os recursos. Otimizar e reduzir custos de maneira efetiva e rápida para a adaptação à nova situação.

- Aceitar que não existe solução fácil. Estabelecer programas de inteligência emocional aplicados à organização para desenvolver a capacidade adaptativa das equipes.

- Estabeleça estruturas neurais. Aumente a colaboração, promova um bom ambiente de trabalho e desenvolva relacionamentos de valor compartilhado.

- Emerja e aprimora os valores da organização. Avalie e vislumbre novas oportunidades e valorize de forma proativa os pontos fortes da organização com base no conhecimento, experiência e inteligência.

Na era pós-COVID-19. Neste novo e desconhecido cenário, os diretores não só devem reformular suas estratégias de continuidade de negócio ou funcionamento, mas sim devem encontrar a maneira de liderar o futuro, influir em sua configuração e preparar-se para administrar as provocações e dificuldades que nos afetarão nos próximos anos.

MISSÃO E VISÃO INTERDISCIPLINAR

O novo presente e futuro dependem de colocar em prática o que aprendemos, sabendo que temos que navegar entre a incerteza e as maiores complexidades que se esperam daqui para a frente nas atividades industriais, comerciais e sociais.

Temos que consolidar uma sólida base humanística, analítica e ética baseada na inteligência emocional e motivar e buscar um maior envolvimento em equipes e ambientes de oportunidade.

A missão e a visão devem ser interdisciplinares, de longo prazo e com uma perspectiva que leve em consideração elementos de cultura, responsabilidade social e ética.

GESTÃO DO RISCO E A SEGURANÇA

Era pós-COVID-19. Novas seguranças, novos líderes e diretores (3ª parte), de Manuel Sánchez Gómez-Merelo. A gestão de riscos no ambiente organizacional é um tema

complexo de sistematizar. Depende de um grande número de variáveis internas e externas, que se inter-relacionam e se influenciam de uma forma muito ágil e dinâmica.

Atualmente, é importante e imprescindível a exaustiva identificação, análise e avaliação do risco como base para o estabelecimento de um Plano de Segurança Integral para a contingência e continuidade de funcionamento da organização.

A GESTÃO INTEGRAL DO RISCO TEM QUE TER UMA VISÃO TRANSVERSAL E MULTIDISCIPLINAR.

Além disso, uma gestão abrangente de segurança, baseada em recursos estabelecidos, integração de sinergias e soluções para minimizar riscos, deve estar alinhada com os objetivos da organização. Essa abordagem deve abranger, fundamentalmente, tanto a segurança física quanto a lógica ou a segurança da informação e da comunicação.

CAPACIDADE DE ADAPTAÇÃO E INOVAÇÃO

A análise de tendências para a nova normalidade põe de especial manifesto a necessidade de impulsionar a transformação digital das organizações que devem contemplar em seus planos estratégicos mais imediatos.

No ambiente atual da VUCA, as pessoas que lideram organizações ou projetos devem fazê-lo com grande capacidade de adaptação e inovação.

A análise das tendências para a nova normalidade põe de especial manifesto a necessidade de promover a transformação digital das organizações que deve ser considerada nos seus planos estratégicos mais imediatos.

Era pós-COVID-19. Novas seguranças, novos líderes e gestores (3ª parte), de Manuel Sánchez Gómez-Merelo. Assim, a digitalização, tomada como um exemplo transversal, não só proporciona inteligência artificial e novas possibilidades de informação e comunicação, mas também possibilita o trabalho em novos ambientes e traz agilidade e flexibilidade para qualquer aspecto do modelo de atividade como: orientação ao cliente, estrutura organizativa, gestão da mudança, liderança organizacional, segurança e privacidade do dado, desenvolvimento dos produtos, serviços e processos, personalização, decisões tecnológicas, integração dos sistemas de informação, etc.

Outros fatores que, não só não trocam, mas sim além disso saem fortalecidos desta crise, são a colaboração e o trabalho conjunto entre diferentes disciplinas, que vão terminar convergindo tecnologicamente e gerando espaços de inovação mais dinâmicos.

PLANEJAMENTO INTEGRAL

Nossas atividades produtivas, econômicas e sociais têm sofrido um forte contingenciamento devido à crise social e sanitária provocada pela COVID-19, o que nos obriga a rever e alterar todos os nossos Planos de Contingência e Continuidade desde que uma nova realidade foi implantada que, como já estamos comprovando, pode ter vindo para ficar.

A necessidade de novos planos de contingência é motivada pela emergência causada por risco à comunidade. A incerteza e o pessimismo gerados devem ser apenas aquele pano de fundo de percepção de insegurança que temos e devemos seguir trabalhando neste novo ambiente que nos obriga a mudanças perceptíveis nos processos, usos e costumes nos quais temos que tentar minimizar a materialização de riscos, estudando e implementando toda a segurança a nosso alcance, físicas e lógicas, públicas e privadas.

Os novos desafios e exigências devem ser articuladas na mesma direção que os objetivos de qualquer tipo de Plano Integral de Segurança, sendo o Diretor responsável por:

- A organização, direção, fiscalização e administração dos serviços e recursos de segurança (prevenção + proteção) disponíveis.
- A identificação, análise e avaliação de situações de risco, ameaças e vulnerabilidades que possam afetar à integridade das pessoas e ao patrimônio.
- O planejamento, organização e controle das atuações precisas para a implantação das medidas condizentes a acautelar, proteger e reduzir a manifestação de riscos de qualquer natureza com meios e medidas precisas, mediante a elaboração e desenvolvimento dos planos de segurança aplicáveis.
- O controle do funcionamento e manutenção dos sistemas de segurança.

CAPACIDADE DE RESILIÊNCIA E COLABORAÇÃO

De acordo com um estudo recente da revista Science, os profissionais subestimam sua própria resiliência - eles não percebem como será fácil mudar sua visão de mundo se algo ruim acontecer.

Era pós-COVID-19. Novas seguranças, novos líderes e diretores (3ª parte), pelo Manuel Sánchez Gómez-Merelo. Os diretores resilientes são capazes de enfrentar o fracasso, recuperar-se, adaptar-se rapidamente à mudança e à incerteza, para sair fortalecidos de tudo isso.

Portanto, temos que potencializar esta habilidade e:

Aceitar a realidade, veja-a como ela é e em toda a sua crueza. Quanto à liderança, implica comunicar-se com transparência e relatar a situação real.

Encontrar o sentido e saber aproveitar as lições aprendidas das situações mais comprometidas para interpretar e direcionar os acontecimentos.

Adaptar-se às novas situações, já sejam do ambiente ou trabalhistas. As mudanças são sempre oportunidades.

Procurar a orientação para as soluções e não ficar paralisados pelos problemas. Terá que estabelecer novos objetivos e transmiti-los à equipe.

Reconhecer as habilidades, confiar nelas e as utilizar para adaptar-se aos novos desafios e mudanças.

Mova-se em um ambiente otimista e positivo e lidere com convenção os novos planos, mudanças e objetivos.

Manter um posicionamento objetivo analisando e avaliando as vantagens e os inconvenientes de cada situação e ambiente.

Avalie o positivo de cada situação e de cada mudança e relativizar as incertezas e problemas.

A resiliência deixou de ser o grande esquecido e passou a ser um recurso de primeiro nível. Os gerentes das organizações mais resilientes são aqueles com os sistemas de valores mais estáveis e compartilhados.

É, portanto, um elemento chave em um entorno incerto no que as organizações deverão fazer da resiliência uma prioridade.

FORMAÇÃO MULTIDISCIPLINAR

A importância da formação sempre esteve muito presente no ambiente empresarial e nas organizações públicas, mas agora é mais necessária que nunca.

Conceitos como reinvenção e especialização são a prioridade atual de todos os componentes das equipes de trabalho e, mais ainda, dos líderes e diretores com maior exigência de conhecimento transversal e integração global.

Para estar ao dia das últimas tendências, a formação contínua é uma das principais ferramentas ante situações irreversíveis de mudança.

Temos que aprender a enfrentar esse ambiente de incertezas, esse panorama complexo, com uma visão correta do futuro. Se há alguns anos a formação contínua

era uma mais-valia, agora é absolutamente necessária, sobretudo nas equipes de gestores em competências identificadas como críticas no ambiente pós-COVID-19, como inovação, liderança, trabalho colaborativo e resiliência.

Precisamos formar gestores capazes de administrar empresas, instituições e projetos com um renovado enfoque: liderar organizações ou projetos com uma grande capacidade de adaptação e inovação e com visão interdisciplinar. Líderes e diretores que tenham grande capacidade de entendimento e resiliência, capazes de administrar a informação, trabalhar em estruturas neuronal, aprender continuamente e viver na mudança e adaptação, com autonomia e capacidade de liderança pessoal.

A TÍTULO DE CONCLUSÕES

A repentina crise sócio sanitária da COVID-19 inundou-nos completamente no ambiente VUCA, obrigando-nos a resolver problemas rapidamente, a aprender e a adaptar-nos, a responder a novos desafios e a tomar decisões em tempo real para alcançar os nossos novos objetivos.

Estamos perante uma nova "vucalidade", um ambiente de volatilidade, incerteza, complexidade e ambiguidade onde a nossa atual provocação deve ser assumida e estamos neste ambiente a desenvolver novas competências de gestão, atitudes e soluções de "gamificação" com instrumentos para consegui-lo com êxito e naturalidade, abordando totalmente a pura essência organizacional com inteligência emocional.

Foi pós-COVID-19. Nova segurança, novos líderes e diretores (3ª parte), de Manuel Sánchez Gómez-Merelo. Vendo como a crise da COVID-19 está se desenvolvendo, é mais uma estratégia do que um plano para um ambiente VUCA, está mudando e apenas previsível, suponha uma Mudança de paradigma muito relevante face a processos suportados em ambientes previsíveis e pouco dinâmicos.

Esta transformação necessária passa por realizar novos esforços para conseguir ser um líder ou diretor mais flexível, desenvolvendo: a aprendizagem constante e ágil, o enfoque neuronal e colaborativo do trabalho, a velocidade para administrar a adaptação e a mudança, a confiança nas pessoas e seu desenvolvimento, tira-a de decisões intuitiva sobre a base da gestão do risco e a comunicação constante e transparente.

Nestes momentos que estamos vivendo, com tantas mudanças, tão imprevisíveis, e com tanto impacto na vida em todos os âmbitos, falar de estratégia pode parecer algo complexo, mas é necessário ter aprendizagens e experiências para aplicação no meio e comprido agrado.

Assim, queria resumir, com meu particular acrónimo de “PODEREMOS”, que temos que atuar com a Proatividade, Oportunidade, Desafios, Relações, Experiência, Motivação, Observação e Soluções.

Uma página de segurança torna-se um dia em um assunto essencial e irredutível para as organizações e para a sociedade em geral, razão pela qual, em meio a essa crise socio sanitária, os diretores de segurança vão adquirir maior importância e destaque, não só em relação a Gestão usual de riscos e segurança, não para ser ornamentada com a sua formação e capacidade, tanto para adaptação rápida ao novo ambiente, como para a utilização de novas ferramentas tecnológicas, de forma a convergir e otimizar recursos.

A segurança se converteu hoje em dia em um tema essencial e irredutível para as organizações e para a sociedade em geral, razão pela qual, em meio desta crise socio sanitária, os diretores de segurança adquiriram maior importância e protagonismo, não só em relação com a habitual gestão do risco e as seguranças, a não ser fazendo ornamento de sua formação e capacidade, tanto para a rápida adaptação ao novo entorno, como para o uso de novas ferramentas tecnológicas, de cara à convergência e à otimização de recursos.

> “Acusar a outros das adversidades é ignorância.
> Acusar-se a gente mesmo demonstra um pouco de entendimento.
> Não acusar a ninguém é sabedoria”.
> Epícteto (filósofo grego)

ATAQUES CIBERNÉTICOS, 11 FORMAS DE VENCER AS DEFESAS DE SUA EMPRESA!

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.

CONTEXTO DOS ATAQUES CIBERNÉTICOS

Os cibercriminosos estão utilizando outras técnicas para vencer as defesas das empresas e com isso estão tirando o sono dos executivos C-level. Os hackers estão usando voz e currículos para tentar penetrar nos sistemas corporativos e roubar informações, além dos já conhecidos phishing e ransomware.

Um levantamento da empresa de segurança da informação e cibernética Kaspersky, divulgado em junho de 2020, retrata que houve um crescimento de 330% de ciberataques, no Brasil, utilizando o acesso remoto. Esta estratégia é extremamente eficaz e tira o sono dos executivos de qualquer segmento empresarial.

O Brasil é o líder de ciberataques ransomware, reportado em outro relatório da Kapersky, também em junho referente as empresas durante a pandemia.

Esse aumento de ataques teve como causa o despreparo das empresas, de todos os segmentos, quando houve a determinação do “Home Office” pelos governos estaduais e municipais, em função do COVID–19. Na realidade as empresas não tinham opção, pois suas operações não poderiam parar. Então houve o disparo do Plano de Continuidade de Negócios – PCN, mesmo sem estarem estruturados.

Para que tenhamos uma ideia deste despreparo, em pesquisa feita aos domicílios, revelou que mais de 75% dos empregados em “Home Office” utilizavam seus próprios equipamentos. Ou seja, internet desprotegida, computadores sendo utilizados não só pelos empregados, mas também para seus familiares. Imaginem a insegurança com que as empresas estiveram e ainda estão sendo expostas.

Vale ressaltar que, embora algumas empresas tenham oferecido o computador oficial, a grande maioria utilizava seu telefone celular pessoal para acessar arquivos da empresa, respondiam e-mails e pior, interagiam pelos aplicativos, muito comuns durante a pandemia de COVID–19.

Brecha aberta, os hackers aproveitaram estas fragilidades, entre elas o grande despreparo dos empregados das empresas, em termos de sensibilização às melhores práticas sobre questões de CyberSecurity Risks - ataques cibernéticos - através do conhecidíssimo phishing.

Diante desta vulnerabilidade, os hackers acessavam os sistemas das empresas e a partir daí roubavam, sequestravam e/ou adulteravam os dados e/ou informações, para pedirem resgate.

Um ponto positivo para os cibercriminosos, foi a mudança do seu modus operandi, quebrando padrões, adaptaram-se para o momento vivido durante a pandemia do COVID–19. Realizaram uma Ruptura de Tendência.

TÉCNICAS E TÁTICAS DE ATAQUES CIBERNÉTICOS EM ASCENSÃO – UTILIZADAS PELOS HACKERS

As técnicas e táticas de ataques cibernéticos, foram retiradas do site da Information Week, em julho de 2020.

1. Golpes de Doação

Desde que o isolamento social começou, houve muitas campanhas de fraude disparadas por e-mails. Todas elas pediam praticamente a mesma coisa: Doações para organizações de saúde e outras entidades na linha de frente no combate ao COVID–19.

2. Aplicativos Móveis

O problema é que essas organizações e entidades, quando não existiam, tinham suas marcas falsificadas pelos golpistas. Um exemplo foi o disparo de campanhas em nome da Organização Mundial da Saúde (OMS), que também sofreu uma tentativa de invasão nos sistemas.

Ainda em meio à pandemia, o movimento Black Lives Matter também se tornou alvo de golpistas, que passaram a disparar vários conteúdos SPAM para diferentes públicos em nome da iniciativa.

Aqui temos duas situações:

- 1ª Situação:

  A primeira é em relação a empresas como Google e Apple que desenvolveram aplicativos de rastreamento para identificar pessoas que estiveram próximas a outra infectada pelo COVID–19. Os hackers, com grande flexibilidade, não perderam tempo e 12 aplicativos maliciosos foram disponibilizados na Play Store (Google) e App Store (Apple), de acordo com o site www.informationweek.com. Todos eles serviam apenas para baixar um malware nos dispositivos dos usuários.

- 2ª Situação:

  Já a segunda situação é bem específica do Brasil. Com o anúncio do auxílio emergencial, diversos aplicativos em nome da Caixa Econômica Federal surgiram. Foram mais de 60 sites e aplicações falsas desenvolvidas em um mês e, recentemente, um app malicioso foi disponibilizado para furtar o benefício cedido pelo governo por causa do COVID-19.

3. DDoS

Esse tipo de ataque é bem conhecido, desde o início da pandemia até maio, ataques DDoS aumentaram 67%.

Os ataques DDoS, Ataques de Negação de Serviço distribuído em rede. Esse tipo de ataque aproveita os limites de capacidade específicos que se aplicam a todos os recursos de rede, como a infraestrutura que viabiliza o site de uma empresa. O ataque DDoS envia múltiplas solicitações para o recurso Web invadido com o objetivo de exceder a capacidade que o site tem de lidar com diversas solicitações, impedindo seu funcionamento correto.

Entre os alvos comuns de ataques DDoS estão:

- Sites de compras virtuais;
- Cassinos on-line;
- Qualquer empresa ou organização que dependa do fornecimento de serviços on-line.

Como funciona um ataque DDoS?

Os recursos de rede, como servidores Web, conseguem atender a um limite finito de solicitações simultaneamente. Além do limite de capacidade do servidor, o canal que conecta o servidor à Internet também tem largura de banda/capacidade finita. Sempre que o número de solicitações excede os limites de capacidade de qualquer componente da infraestrutura, o nível do serviço tende a sofrer de uma das deficiências:

- A resposta às solicitações é muito mais lenta do que o normal.
- Algumas ou todas as solicitações dos usuários podem ser totalmente ignoradas.

Em geral, o objetivo final do invasor é impedir totalmente o funcionamento do recurso da Web, ou seja, uma "negação de serviço" total. O invasor também pode solicitar um pagamento para interromper o ataque. Em certos casos, um ataque DDoS pode até ser uma tentativa de desacreditar ou prejudicar os negócios de um concorrente.

Para enviar uma grande quantidade de solicitações ao recurso da vítima, o hacker em geralmente estabelece uma "rede zumbi" de computadores infectados.

Como o criminoso controla as ações de cada computador infectado da rede zumbi, a simples escala do ataque pode sobrecarregar os recursos da Web da vítima.

4. Phishing

O phishing é uma ameaça cibernética bastante aliada da dependência digital. Com o Home Office, muitos colaboradores trocam e-mails para resolverem algumas demandas e negócios do dia a dia.

Durante a pandemia, alguns desses e-mails maliciosos são disparados com mapas de contaminação e até mesmo outros conteúdos relacionados ao COVID-19, como se fossem legítimos. Porém, é nos pequenos detalhes (uma letra trocada, por exemplo) que mora o perigo.

Quando um colaborador clica inadvertidamente em algum link dentro desses e-mails, as chances de ele ter informações sensíveis (CPF, RG, número de cartão de crédito, login e senhas) roubadas são grandes.

5. Spear-Phishing

Se no phishing temos o disparo em massa de e-mails de uma forma genérica, o spear-phishing traz uma maior complexidade, porque é um tipo de ataque direcionado – seja a uma pessoa, uma instituição ou até mesmo a um estado ou país.

Esse tipo de ameaça cibernética vai reunir a maior quantidade de informações possíveis do alvo para, depois, disparar e-mails que vão parecer legítimos na tentativa de enganá-lo. A OMS – Organização Mundial da Saúde, também sofreu essas tentativas de ataque.

6. Vishing

Mesmo que muitas pessoas estejam mais conectadas, elas não são vítimas somente de ataques “digitais”. Por exemplo, antes mesmo do e-mail, o uso de voz era bem comum na tentativa de roubar as informações de alguém.

Essa prática é chamada de vishing — combinação das palavras voice (voz) e phishing — e ela recebeu uma atualização desde que o trabalho remoto ganhou força nas empresas. Os hackers fingem ser do suporte técnico da empresa para convencer os funcionários a divulgar login e senha ou inseri-los em um site falso. Para que tenham sucesso, costumam utilizar técnicas de indução nas conversações, visando retirar as informações em que a vítima perceba.

7. Smishing

O termo smishing é uma combinação de «SMS» (short message services, ou mensagens de texto) e “phishing”. No phishing, o criminoso virtual envia e-mails fraudulentos que buscam induzir o destinatário a abrir um anexo com malware ou clicar em um link malicioso. O smishing basicamente usa mensagens de texto no lugar de e-mails.

Uma mensagem de texto perversa pode estar a caminho de um smartphone perto de você. Muitas vezes, essa mensagem diz ser de seu banco e solicita suas informações pessoais ou financeiras, como o número da conta ou a senha do cartão. Fornecer essas informações é como dar aos cibercriminosos a chave de seu cofre.

As mensagens de textos são o recurso mais usado dos smartphones. A Experian descobriu que usuários adultos de dispositivos móveis, com idades entre 18 a 24 anos, enviam mais de 2.022 mensagens de texto por mês, em média, 67 por dia, e recebem 1.831.

Dois outros fatores tornam essa ameaça cibernética especialmente traiçoeira.
A maioria das pessoas conhecem um pouco os riscos das fraudes por e-mail. Provavelmente pode até desconfiar de e-mails que dizem “Olá! Dê uma olhada neste link interessante”, sem uma mensagem pessoal do suposto remetente.

No telefone, as pessoas são menos cautelosas. Muitas acreditam que seus smartphones são mais seguros do que os computadores. Mas a segurança dos smartphones é limitada e não oferece proteção direta contra smishing.

Conforme observado pela WillisWire, o crime virtual direcionado a dispositivos móveis está aumentando muito, junto com o uso desses dispositivos.

Entretanto, embora os dispositivos Android sejam o principal alvo de malware, simplesmente pela quantidade existente e pela flexibilidade que a plataforma oferece aos clientes (e aos cibercriminosos), o smishing, como o próprio SMS, atinge as várias plataformas. Os usuários de iPhones e iPads correm risco especificamente por acharem que estão imunes a ataques. Embora a tecnologia iOS da Apple para dispositivos móveis seja reconhecida pela segurança, nenhum sistema operacional é capaz de se proteger sozinho contra ataques como phishing. Outro fator de risco é que as pessoas utilizam o smartphone em qualquer lugar, geralmente quando está distraído ou com pressa. Isso significa que você está mais propenso a ser pego desprevenido e a responder sem pensar quando recebe uma mensagem que solicita informações bancárias ou o resgate de um cupom.

Resumindo, assim como a maioria dos cibercriminosos, o objetivo deles é roubar dados pessoais, que serão usados depois para roubar dinheiro, ou, às vezes, da empresa. Os cibercriminosos usam os métodos para roubar dados.

Eles podem fazê-lo baixar um malware que se instala no telefone. Esse tipo de malware pode se passar por um aplicativo legítimo, induzindo-o a digitar informações confidenciais e enviá-las aos criminosos virtuais. Por outro lado, o link na mensagem de smishing pode te levar para um site falso, que solicita a inserção de informações pessoais e sigilosas que os criminosos virtuais usarão para roubar sua identidade on-line.

Quanto mais pessoas usam seus smartphones pessoais no trabalho (uma tendência chamada de BYOD, ou “traga seu próprio dispositivo”), mais o smishing se torna uma ameaça para a empresa e para o cliente.

Por esta razão não é de se surpreender que o smishing se tornou a principal forma de mensagens de texto maliciosas.

8. Ransomware

Com as organizações cada vez mais dependentes do mundo digital para manter as suas operações, não é surpresa que os ataques ransomware tenham aumentado durante a pandemia do COVID–19.

Com uma maior vulnerabilidade da segurança das empresas — fruto da rápida e necessária migração para um “Home Office” —, os cibercriminosos passaram a olhar para as empresas que possuem uma infraestrutura crítica com o objetivo de travar os sistemas digitais até que um resgate seja pago.

Como isso é feito? Com a mesma tática que já falamos em outros tópicos: e-mails e sites falsos relacionados à COVID-19 são direcionados aos funcionários que agora

trabalham de casa. Basta um download de um conteúdo malicioso para que os invasores consigam sequestrar o sistema de toda a empresa. Fácil não? Por isso que a sensibilização dos empregados é uma arma estratégica na prevenção.

9. Currículos Maliciosos

Talvez essa seja uma das ameaças cibernéticas mais "peculiares" no momento. A alta do desemprego fez com que muitas empresas passassem a receber currículos de possíveis candidatos.

Segundo uma publicação da Check Point, empresa de solução de segurança cibernética, o número de currículos e formulários de licenças médicas com algum malware escondido dobrou desde o início da pandemia – geralmente em formato Word ou em planilha de Excel.

10. Sites Maliciosos de COVID-19

Muitas pessoas buscam na internet informações sobre o COVID-19. Isso se tornou uma oportunidade para cibercriminosos: 86 mil domínios com palavras-chave relacionadas à pandemia são de "alto risco" ou "maliciosos", apontou a Palo Alto Networks.

Segundo a publicação da empresa de segurança cibernética, "1.767 nomes de domínio de 'alto risco' e 'maliciosos' (C2, malware ou phishing) sobre o COVID-19 são criados diariamente".

Nunca é demais lembrar: para se informar sobre o COVID–19 deve-se acessar sites oficiais, tanto de órgãos federais, estaduais e municipais, veículos de imprensa tradicionais e de Universidades.

11. Ciberespionagem

Nem todo ataque cibernético tem um hacker independente por trás. Segundo uma reportagem do Jornal americano The Washington Post existem suspeitas de países que ordenaram invasões a hospitais e entidades de saúde presentes em outras nações.

Geralmente essas investidas buscavam informações sobre pesquisas relacionadas a cura do COVID-19. No entanto, são ataques cibernéticos mais sofisticados e difíceis de prevenir e mitigar.

CONCLUSÃO

As empresas de todos os tipos e tamanhos são suscetíveis aos ciberataques. A joia da coroa, os ativos considerados críticos devem estar mapeados, quais são os processos e/ou atividades críticas da empresa? Quais são as informações e dados críticos dos

processos críticos? Quais são os sistemas críticos que suportam as informações críticas dos processos críticos?

Mapeando esta tríade, a empresa estará segura, pois os cibercriminosos não irão atacar algo que não tenham retorno, seja financeiro, político ou simplesmente por ego e/ou emocional. Todos os esforços devem estar concentrados nestes três quesitos para que a empresa esteja preparada para enfrentar um ataque cibernético.

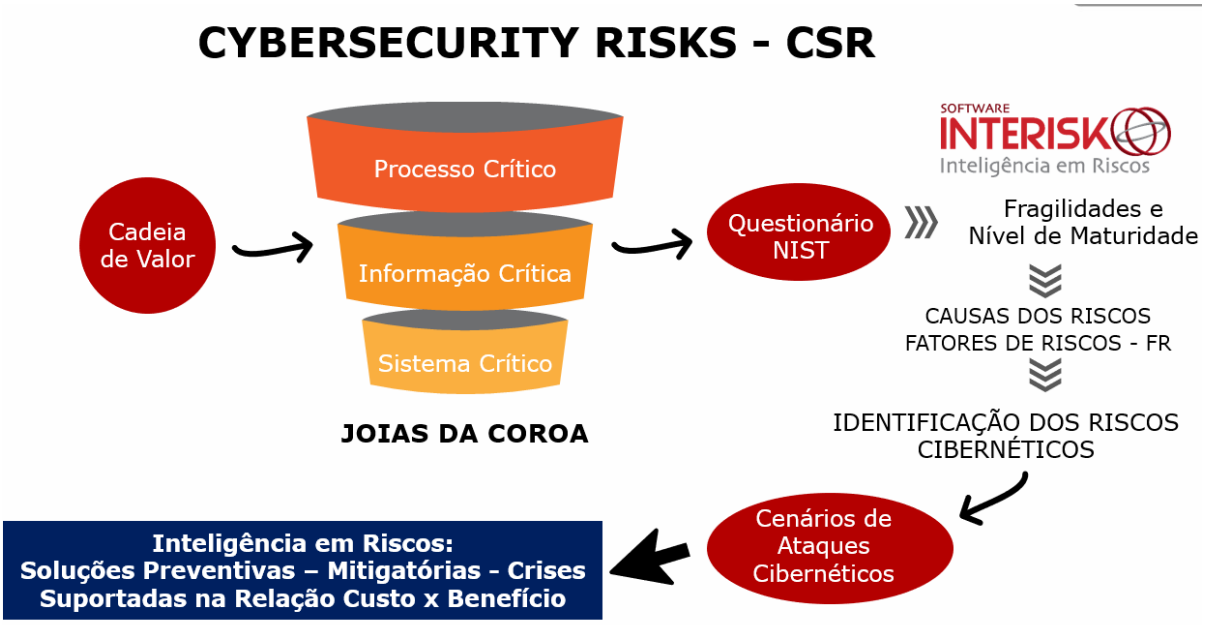


Figura 1: Joias da Coroa: Processo da Brasiliano INTERISK para avaliar e analisar riscos e ataques cibernéticos. Fonte: Brasiliano INTERISK.

Enquanto os ciber incidentes continuarem a ter um impacto negativo na reputação e no bem-estar financeiro das empresas, as ciber invasões continuarão a ser eventos de alta probabilidade de aumentar a pressão negativa sobre a vida empresarial.

SUPERVISOR DE SEGURANÇA EM SHOPPING CENTER

Manoel Ricardo Silva dos Santos

Supervisor de Segurança em Shopping Center, 14 anos atuando no varejo, Bacharel em Administração de Empresas, Pós Graduado Gestão em Segurança Institucional e Corporativa, MBA Executivo em Segurança Privada - SAFETY & SECURITY, Instrutor credenciado junto a Polícia Federal em 12 disciplinas, MBS em Segurança Empresarial, Certificado Internacional en Gestion de Riesgos, afiliado a CEAS Brasil (Corporación Euro-Americana de Seguridad) e ABSEG (Associação Brasileira dos Profissionais de Segurança).

A Escola de Sargento das Armas, uma das principais Organizações Militares do Exército Brasileiro, localizada na cidade de Três Corações, MG, estampa na fachada do Pavilhão de Comando a frase: “Sargento, elo fundamental entre o comando e a tropa.”

Figura 1: Pavilhão de Comando da EsSA. Fonte: Exército Brasileiro (2014), Twitter. Modificado pelo autor (2021)

Pois bem, assim é um Supervisor de Segurança em Shopping Center, um líder fazendo o elo entre o mall (clientes, lojistas, prestadores de serviço, entre outros) e Administração.

Qual a importância de um líder? Chiavenato responde que:

> A liderança é necessária em todos os tipos de organização humana, principalmente nas empresas e em cada um de seus departamentos. Ela é igualmente essencial em todas as demais funções da Administração: o administrador precisa conhecer a motivação humana e saber conduzir as pessoas, isto é, liderar. (1993, p. 172):

A ABRASCE (Associação Brasileira de Shoppings Centers), em seu site (2021) considera Shopping Center como um empreendimento com Área Bruta Locável (ABL), normalmente, superior a 5 mil m², formados por diversas unidades comerciais, com administração única e centralizada, que pratica aluguel fixo e percentual. Na maioria das vezes, dispõe de lojas âncoras e vagas de estacionamento compatível com a legislação da região onde está instalado. Funciona como um condomínio comercial, um empreendimento privado com acesso ao público.

Os shopping centers de média e grande dimensão funcionam como pequenas cidades, templo de culto à mercadoria. O modelo do shopping center, como o conhecemos hoje, nasceu nos Estados Unidos na década de 1950, com espaços privados objetivamente planejados para a supremacia da ação de comprar. O que se compra nesses centros, contudo, é muito mais do que mercadorias, serviços, alimentação e lazer.

Ao contrário de outros espaços com grande circulação de pessoas, como os bancos, por exemplo, os shopping centers possuem acesso liberado para todos. A organização de um shopping center é uma atividade muito complexa, porque requer uma clara visão do empresário na escolha e seleção de unidades, no equilíbrio da competição, no esmero, na decoração e no estilo. O estabelecimento comercial, que nele se instala, já deve estar em harmonia e correspondência com a clientela que frequentará o local.

É um espaço planejado sob uma administração centralizada, composto de lojas destinadas à exploração comercial e à prestação de serviços, com normas contratuais padronizadas, para manter o equilíbrio da oferta e da funcionalidade, procurando assegurar convivência integrada.

Os Shoppings não são apenas centros comerciais comuns, recebem exposições, desfiles, campanhas solidárias. Hoje são verdadeiros ponto de encontro entre lojas, marcas e pessoas. Por trás de tudo isso está a administradora que atua de acordo com sua missão, visão e valores.

Nos últimos anos, nenhum componente do ambiente de shopping center recebeu mais atenção que o setor de segurança. A sociedade se tornou mais consciente sobre a necessidade de segurança e espera níveis mais altos e mais visíveis.

Observando as funções da segurança pública e da segurança privada, podemos notar que existem algumas atividades em comum. Ambas têm como objetivo promover a proteção do patrimônio e pessoas, assim como manter a ordem e fazer cumprir determinadas regras. No caso da segurança do shopping, fazer cumprir o código de conduta e o regimento interno do empreendimento entre outras.

É muito importante observar que a segurança de um shopping center não possui "poder de polícia" e por isso não tem autoridade para deter suspeitos, fazendo isto apenas em caso de flagrante delito ou dentro dos procedimentos de abordagem em vigor nos empreendimentos.

A segurança neste segmento tem vários aspectos particulares. Um shopping center, ao invés de restringir o acesso, deve ser convidativo e estar sempre com as portas abertas. Isso permite que pessoas com as mais diversas intenções estejam neste local ao mesmo tempo. Os profissionais de segurança de um shopping center devem estar muito bem preparados para agir em caso de necessidade.

Estou falando do Supervisor de Segurança e seu time, pois como equipe de campo, serão as pessoas em primeiro contato com a necessidade.

Figura 2: Pirâmide organizacional Fonte: Gilles B. de Paula (2015), modificado pelo autor (2021)

No Planejamento Organizacional de um Shopping Center, o Supervisor de Segurança está no nível operacional. Todos os níveis são necessários: o estratégico para o orientar a visão, o tático para desdobrar essa visão em planos de ação menores, e o operacional para levar os planos a execução.

Supervisão compreende vários fatores, incluindo recrutamento, treinamento, disciplina, motivação, promoção e comunicação. Cada um destes fatores constitui uma habilidade específica.

Uma definição popular de Supervisão é a tarefa de fazer com que outros (liderados) realizem o trabalho, da forma que a liderança quer, quando ela quer que seja feita, e de boa vontade. Disposição, é claro, é o aspecto chave desta definição.

Desempenho é a responsabilidade final e a meta da Supervisão. Tudo gira em torno do desempenho do trabalho – execução na linha de frente. O desempenho do Supervisor, suas habilidades, é refletido no desempenho daqueles que trabalham com ele.

Cada colaborador é diferente do outro, o Supervisor deve lidar individualmente com cada liderado. Cada ser humano na face da terra é diferente. As diferenças são manifestadas não somente através de características físicas e impressões digitais, mas em como cada indivíduo reage a estímulos externos, como ele percebe as coisas, suas crenças, medos, aspirações e necessidades. Tais diferenças humanas significam que diferentes pessoas requerem diferentes tratamentos. Algumas podem requerer mais supervisão que outras.

Imergindo no mundo do Supervisor de Segurança, faço uma breve descrição sumária do cargo:

- Coordenar, distribuir e acompanhar os trabalhos de segurança empresarial em todas as dependências internas / externas do empreendimento, orientando seus liderados/contratados nos programas preestabelecidos pelos seus superiores hierárquicos e o constante em Manuais e Normas de Procedimentos; e

- Zelar pelos equipamentos de segurança utilizados para as tarefas do cargo, bem como, pelo patrimônio dos clientes, dos lojistas e do empreendimento em geral.

Esse líder tem em seu escopo as seguintes missões:

- Coordenar os trabalhos realizados pela vigilância própria e contratada, orientando-os quanto aos procedimentos adequados de cobertura dos postos de trabalho de acordo com os programas e escalas de serviço pré-determinadas, bem como, determinar prioridades e operações a serem realizadas nos casos de emergência.

- Orientar seus liderados quanto a procedimentos a serem tomados em situações de furtos, incêndios, socorro de emergência ou agressões entre os clientes, de maneira a preservar a imagem do empreendimento.

- Elaborar relatórios das atividades da área, de acordo com o processo de registro eletrônico de gestão de ocorrências, de modo a informar ao superior imediato as irregularidades encontradas, bem como, sugerir mudanças ou adaptações dos esquemas de segurança existentes, de acordo com os problemas mais constantes.

- Participar em conjunto com o seu líder da elaboração de escala de pessoal e remanejamentos, visando a otimização dos recursos humanos disponíveis e de acordo com a necessidade de delegação de funções, utilizando iniciativa própria para resolução dos problemas apresentados.

- Distribuir os trabalhos de vigilância de acordo com a escala elaborada orientando seus liderados quanto aos esquemas de segurança adotados, bem como, verificar se os postos estão corretamente ocupados e fiscalizar as vistorias diárias nas portas, escadas, carga e descarga, etc., antes, durante e após o expediente.

- Verificar diariamente o efetivo da vigilância própria e contratada, através de apresentação pessoal, instruindo-os nos programas e medidas de proteção física nas instalações externas e internas do empreendimento, bem como, testar os equipamentos de segurança utilizados pelos seus liderados.

- Ministrar treinamentos teóricos e práticas em segurança, orientando os seus liderados as normas adotadas e praticadas pelos órgãos oficiais e de competência.

- Executar outras tarefas correlatas a critério de seu superior imediato.

Para o sucesso na execução de suas rotinas e no desempenho de sua função, o Supervisor deve atentar para as competências, que nada mais são que conhecimentos, habilidades e atitudes, independentes ou não, o famoso CHA.

Não basta que o Supervisor tenha um determinado conjunto de competências, para que ele agregue valor aos trabalhos no empreendimento, é preciso também que ele as coloque em prática, ou seja, que ele as desempenhe.

As competências sugeridas são:

- Preparo e qualificação: conhecimento técnico, capacidade analítica, organização, comunicação, capacidade de negociação, introdução de novas práticas, geração de conhecimento e autodesenvolvimento;

- Capacidade de trabalho em equipe: interação, interlocução, cooperação e motivação;
- Compromisso com resultados: orientação para eficiência e eficácia, busca de orientação e foco em superação;
- Visão institucional: interesse pela instituição, compromisso com valores e articulação, e
- Características comportamentais: equilíbrio, relacionamento interpessoal, iniciativa, automotivação, empatia, discrição, disciplina e capacidade de concentração.

Como vimos, o Supervisor de Segurança possui um leque de atribuições e necessita de um vasto conhecimento para exercer sua função, o que demanda muita dedicação, tempo para aprendizado e qualificação. Este profissional deve ter em mente que seu papel é manter o nível de excelência e, para isso não deve ser um chefe, e sim um líder. Deve ainda ser capaz de discernir entre o certo, e errado e o aplicável a cada situação.

A utilização em conjunto das ferramentas de segurança de maneira eficiente, garantem o sucesso do trabalho. Resultados significativos começam a aparecer quando há o treinamento e aplicação correta do aprendizado.

Esse profissional, considerado os olhos da administração, deve sempre buscar a melhoria contínua em segurança, é preciso vencer as barreiras e os obstáculos de maneira estratégica, utilizando os conhecimentos para manter ou melhorar o padrão de segurança ofertado aos frequentadores, e assim, com certeza será o elo fundamental entre o comando (administração) e a tropa (time em campo).

REFERÊNCIAS

ABRAPP. Biblioteca digital. Disponível <https://www.abrapp.org.br/>. Acesso em 20jun2020.

ABRASCE. Definições e convenções. Disponível em <http://abrasce.com.br>. Acesso em 25jun2021.

Exército Brasileiro. “Em breve será divulgado edital para o concurso da EsSA. http://esa.ensino.eb.br #EsSAEB”, 20/06/2021, 23:35. Tweet.

PAULA, GILLES. Planejamento Estratégico, Tático e Operacional – O Guia completo para sua empresa garantir os melhores resultados! 2015. Disponível em <https://www.treasy.com.br/blog/planejamento-estrategico-tatico-e-operacional/>. Acesso em 25jun2021.

TAMMENHAIM, A. Gestão de operações de segurança: estratégia e tática. Paraná. Ed. Intersaberes. 2019.

TREIS, MANOELLA. As Diferenças entre Líderes X Chefes e os Reflexos dessas Posições. 2018. Disponível em <https://www.nucleodoconhecimento.com.br/psicologia/lideres-x-chefes>. Acesso em 25jun2021.

EMPRESAS BRASILEIRAS SÃO ALVOS FÁCEIS DE HACKERS POR FALHAS DE SEGURANÇA CIBERNÉTICA

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.

O vazamento de dados praticamente virou febre no mundo, crescendo ainda mais na pandemia. Por falha de segurança, o Brasil virou alvo muito fácil para que os criminosos abusem de suas ousadias estratégicas, fazendo vazar dados pessoais e sensíveis das empresas.

Os seguidos vazamentos de dados de brasileiros têm mostrado ao mundo e, principalmente aos hackers, que o Brasil é um campo muito fértil para que os criminosos cibernéticos possam agir de forma mais ampla e com certa tranquilidade. Nas últimas semanas, não tem sido raro nos depararmos com notícias sobre mega vazamentos de dados nas empresas brasileiras. O perímetro de segurança sofreu alterações, principalmente na pandemia, ampliando em muito a dificuldade dos responsáveis em cibernética das organizações a darem a respectiva tranquilidade aos gestores da alta gestão. Hoje os perímetros, em função da pandemia chegou no home office, com o Novo Normal. À medida que a força de trabalho se espalhou, a criatividade dos criminosos cibernéticos também teve que ter criatividade, elaborando novas formas de ataques e aproveitando a maior fragilidade do ecossistema: o recurso humano. Só que aí o Brasil tem um outro grande problema: sua alta gestão, diretoria, presidência e conselhos de administração, como conhecem pouco sobre segurança cibernética, os investimentos não ocorrem, fragilizando ainda mais todo o ecossistema.

Apesar de toda propaganda realizada por parte dos fabricantes e consultores por meio de seminários, webinar, lives, a realidade é que muitos gestores, continuam alienados a realizar investimentos segurança na segurança cibernética.

O estudo "Percepção do Risco Cibernético na América Latina em tempos de Covid-19", encomendado pela Microsoft e desenvolvido pela consultoria de risco e de seguros Marsh, aponta que devido ao baixo investimento, 30% das companhias observaram aumento nos ataques de phishing, malware e aplicativos web.

Ainda assim, mais da metade das companhias nacionais (56%) afirmam à pesquisa que investem 10% ou menos do budget de TI na área de segurança cibernética. Isso significa que o mercado nacional ainda não está maduro como se esperava após tantos eventos de 2020. Ou seja, somos a "bola" da vez em ataques cibernéticos por pura falta de maturidade!

Mas como investir em segurança? Deve haver critérios e um modelo estruturado para evitar o desperdício nos pontos denominados de ruptura. No passado, a era dourada de antivírus e firewalls, o custo das soluções de segurança representava uma mínima fração. Hoje, a realidade é muito diferente. As consequências sempre são severas ou massivas.

Antigamente um vírus levava até 3 meses para infectar o mundo. Hoje em dia isso acontece em alguns cliques. A dinâmica do mercado mudou radicalmente, saímos do mundo VUCA (volátil, incerto, complexo e ambíguo) e entramos abruptamente no mundo BANI (frágil, ansioso, não linear e incompreensível).

"BANI é uma estrutura para articular as situações cada vez mais comuns nas quais a simples volatilidade ou complexidade são lentes insuficientes para entender o que está acontecendo", diz o criador da terminologia em seu artigo oficial. "Situações em que as condições não são simplesmente instáveis, são caóticas; nos quais os resultados não são simplesmente difíceis de prever, e sim completamente imprevisíveis. Ou, para usar a linguagem particular desses frameworks, situações em que o que acontece não é simplesmente ambíguo, é incompreensível." Interessante é que o criador do anacrônico BANI, o antropólogo Jamais Cascio apresentou esse novo conceito, no evento do Institute for The Future (IFTF) em 2018, dois anos atrás da pandemia começar, porém já com sinais de novos comportamentos. Argumentou que agora nós não vivemos mais no mundo VUCA, mas sim no mundo BANI. A ampliação do perímetro aumentou a exposição e as oportunidades de lucros dos criminosos.

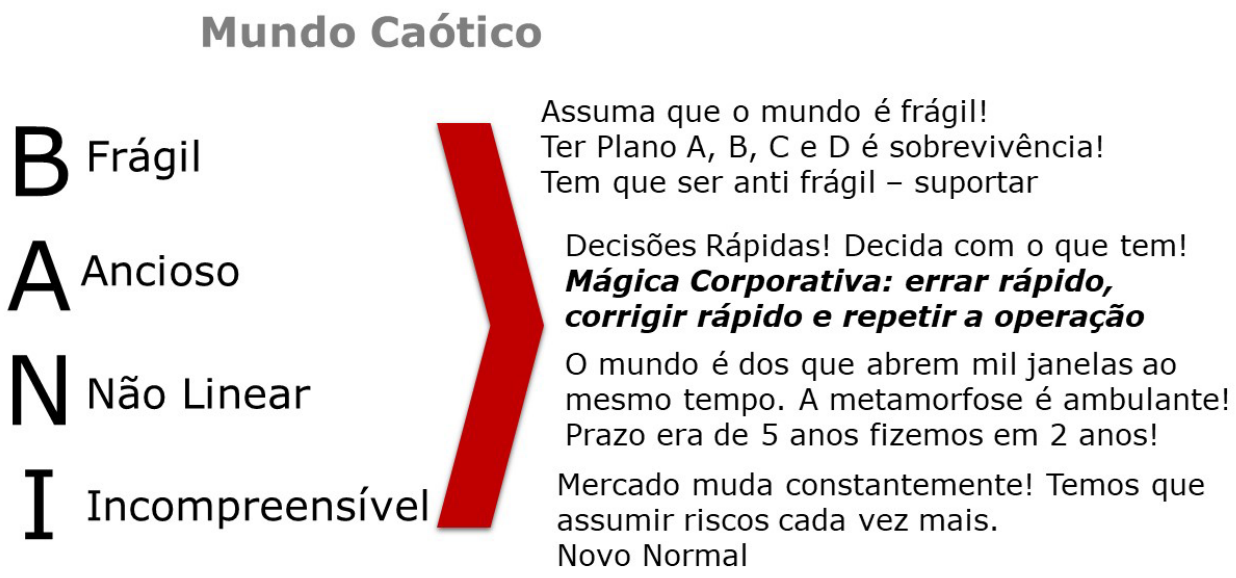


Figura 1: Mundo BANI – Situações Caóticas – Reações Extremas.
Fonte: Brasiliano, Antonio Celso Ribeiro. Apostilas de Aula de Gestão de Riscos

Para termos uma ideia mais clara, em fevereiro deste ano, vazaram em nível mundial, 3,2 bilhões de senhas de e-mail. O Brasil ficou atrás somente dos Estados Unidos, Inglaterra e Austrália, em uma lista de 50 países. Com este ranking, segundo a empresa de segurança cibernética Syhunt, o Brasil possui a quarta posição na sua administração pública. Embora tenhamos leis adequadas e que tratam do tema cibernéticos, para variar, não conseguimos colocar em prática. Com a criação da ANPD – Agência Nacional de Proteção de Dados, essa ainda necessita especificar e estabelecer de forma clara e transparente como as fiscalizações ocorrerão.

Dois pontos são atrativos para os criminosos cibernéticos no Brasil:

1. Baixíssimo investimento em segurança cibernética pela falta de sensibilização e conhecimento da alta gestão das empresas, tendo deixado inúmeras avenidas virtuais de acesso aos hackers;

2. A aproximação da vigência da LGPD, com as respectivas multas. O fato abriu espaço para crimes de extorsão e sequestro de dados pessoais e sensíveis das empresas.

Isso significa que a proteção das empresas deve ser cada vez mais robusta, estruturada e pensada. Os gestores devem estar sempre atentos e alinhados aos modelos de arquitetura como SASE (Secure Access Service Edge) e Zero Trust. Estes modelos, somados, permitem análise de comportamento de usuários, para evitar exposição de informações sensíveis e gerenciamento de soluções na nuvem para que todos os colaboradores estejam conectados a redes seguras.

Além disso, é importante destacar a necessidade de conscientização dos colaboradores e evitar o uso de dispositivos pessoais para fins profissionais. A pesquisa encomendada pela Microsoft destacou que apenas 23% das empresas afirmaram que seus funcionários estão usando exclusivamente equipamentos da empresa. Uma crua e nua realidade nas corporações. A Shadow IT representa um enorme risco às empresas e só pode ser evitada com investimento e educação de usuários.

Podemos enumerar sete principais causas do aumento exponencial dos vazamentos de dados:

1. Pouco e mal aplicado os investimentos em Segurança Cibernética;

2. Pandemia ajudou na formação de hackers em função da crise econômica brasileira. Os crimes cibernéticos fornecem uma visão de ganho sem riscos;

3. Falta de sensibilidade em relação aos phishing de e-mails, principalmente nas contas de e-mails pessoais;

4. Grande quantidade de mensagens, via apps. Neste turbilhão de informações, o número de mensagens falsas é muito grande. Tem que haver autenticação de mensagens;

5. Os apps dos bancos sempre serão alvos dos criminosos cibernéticos em função da existência das informações bancárias, que são uma mina de ouro para os golpistas;

6. Redes Sociais. Neste quesito, a sensibilidade dos usuários é chave. A publicação de fotos e comentários pode dar mais informações para os criminosos cibernéticos do que o roubo de dados;

7. Compras online, são extremamente cômodas, principalmente na pandemia. Mas se não tiver cuidado, trará riscos massivos para os usuários. Como já tem acontecido.

Como evitar então o vazamento de dados? Na nossa experiência e vivência nas consultorias, ao longo dos últimos 22 anos, é por meio de um Framework Preventivo Contra Vazamento de Dados Robusto, com processos e ferramentas consistentes. É difícil? Não. É trabalhoso? É, porque há necessidade de aculturar o mercado. Este é o grande desafio e a maior dificuldade, pois exige muita resiliência e uma cadência constante.

Nós, da Brasiliano INTERISK, definimos a prevenção contra vazamento de dados como sendo um conjunto importante de políticas, métodos e tecnologias, utilizadas para tentar evitar que dados estratégicos ou sensíveis – quesitos legais – sejam compartilhados indevidamente, subtraídos da empresa ou enviados para ambientes inseguros ou manipulados por usuários não autorizados.

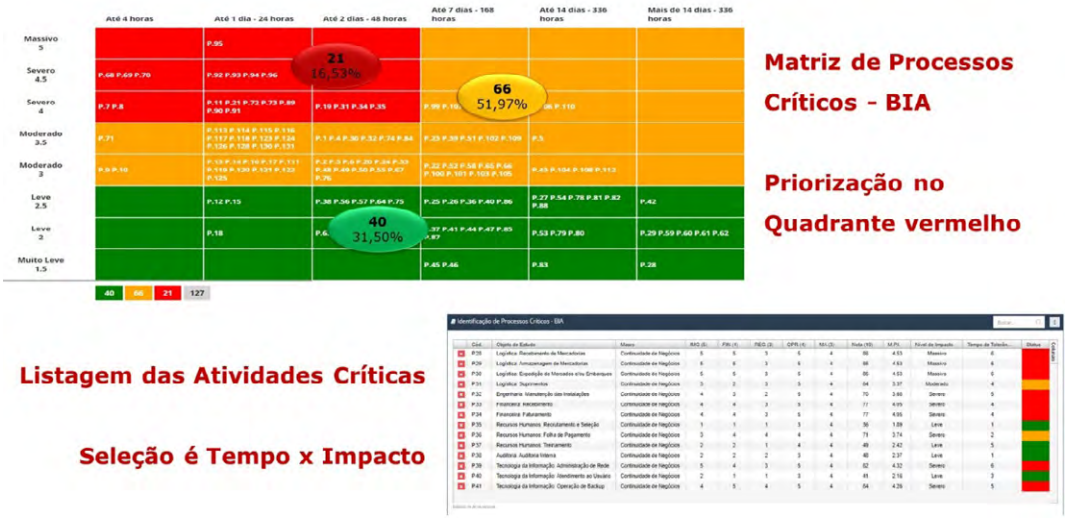
Qualquer empresa deve entender que para evitar o vazamento, tem que aceitar o fato de que as informações e dados estratégicos e críticos podem ser conseguidos de forma voluntária ou involuntária. Isso mesmo. Se um funcionário de médio escalão possui uma informação estratégica e não sabe o valor disso para a empresa, ele pode facilitar um grande vazamento por meio de conversas informais com grupos de amigos ou até mesmo virar vítima de engenharia social e/ou técnica de indução.

Para isso, as organizações devem apostar num Processo Estruturado Contra Vazamento de Dados, com metodologia e critérios parametrizados. A Brasiliano INTERISK acredita em metodologias, por isso estruturou um processo simples e prático por meio da nossa ferramenta INTERISK, que dispõe os seguintes passos:

PRIMEIRO PASSO

A empresa precisa identificar na sua cadeia de valor quais são os processos críticos que suportam o “core” do negócio. Esses processos devem merecer toda atenção do pessoal de segurança da informação, cibernética e segurança corporativa.

Pode-se utilizar como critério e parâmetro o BIA – Business Impact Analysis no qual medimos as consequências em termos de vazamento e sua falta nas tomadas de decisões e ou em processos de negócio.



Fonte: Software INTERISK

Acima, temos um exemplo no qual os processos localizados no quadrante vermelho são estratégicos e ou sensíveis.

SEGUNDO PASSO

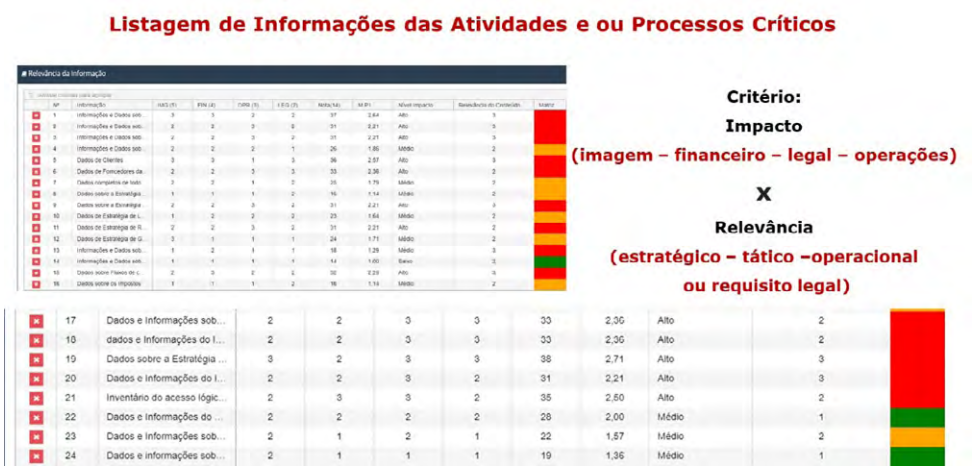
O segundo passo é o mais estratégico e importante, pois a empresa deve classificar

as informações pelo seu conteúdo estratégico e também pelos requisitos legais. Ressalto que grande parte das empresas mundiais, cerca de mais de 85%, não praticam essa etapa. A classificação das informações deve constar na Política de Segurança das Informações e Cibernética. É lá que precisa estar claro a classificação e o que ela irá demandar proteção diferenciada.

A classificação das informações não tem um critério definido, mas em termos de avaliação comparativa (benchmarking), pode-se classificá-las em quatro níveis:

1. Informações confidenciais – o mais alto nível;
2. Informações ou dados restritos – médio nível de confidencialidade;
3. Uso interno – o mais baixo nível de confidencialidade – público interno da empresa sabe da informação;
4. Informações e dados são públicos – todos podem ter a informação.

Com as informações já classificadas, elas devem ser rotuladas e tratadas, conforme sua política, podendo até integrar o IP da máquina e o e-mail do usuário a fim de saber se ele pode mandar essa informação para fora da empresa. Desta forma, o sistema de proteção de dados funciona. Percebem que se a empresa não classificar as informações, os sistemas serão inócuos.



Fonte: Software INTERISK

Acima, um critério que utilizamos para identificar informações ou dados estratégicos.

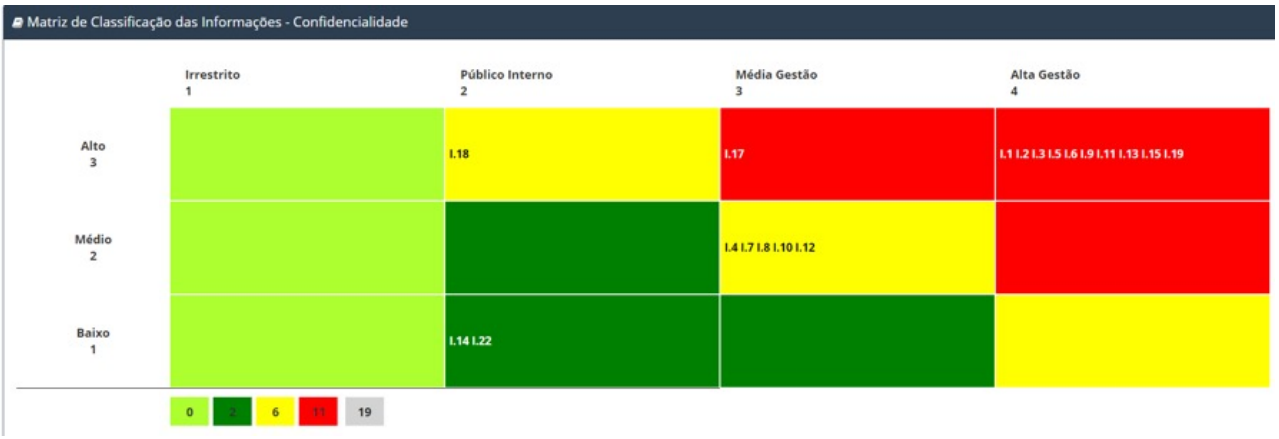
Estas informações, para melhor visualização, vamos para uma Matriz de Relevância:

Matriz de Relevância das Informações das Atividades Críticas da Empresa

Priorização das Informações das Atividades e ou Processos Críticos
Quadrante Vermelho

Fonte: Software INTERISK

Com as informações estratégicas e sensíveis identificadas, podemos classificar utilizando sua relevância versus sua confidencialidade, tal cruzamento vai para outra matriz denominada de Classificação de Informações e Dados. Trata-se de uma matriz que de forma direta, ao cruzar os dois parâmetros, automaticamente já disponibiliza o nível de tratamento desejado pela sua importância.



Fonte: Software INTERISK

Nesta fase, é fundamental saber também qual é a característica das informações e dados em relação a movimentação, ou seja, saber se elas estão:

- Em uso nas máquinas dos usuários;
- Em movimento na rede corporativa ou fora dela;
- Se estão armazenadas, como por exemplo em servidores.

A característica da movimentação irá direcionar a demanda da segurança necessária dessas informações.

TERCEIRO PASSO

Com base nos processos críticos para o “core” da empresa, as informações e dados classificados quanto sua confidencialidade necessitam de uma identificação. Em geral, questionamos: quais são os Sistemas de Tecnologia da Informação que sustentam os dois pilares? Usamos essa informação também para selecionar o inventário de sistemas, o BIA – Business Impact Analysis.

Exemplo de utilização do BIA para sistemas, com sua criticidade no quadrante vermelho.

Lista dos sistemas relacionados na matriz

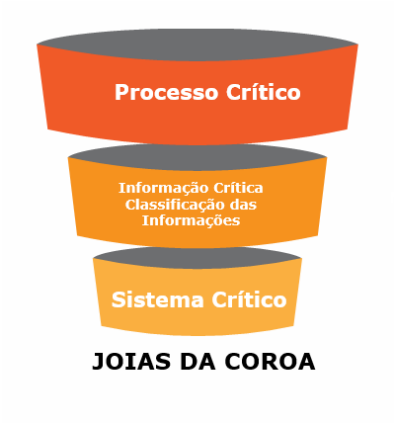
Cód.	Sistema	Impacto	Tolerância em Horas	Matriz
S.1	Sale Force	Severo	Até 1 dia - 24 horas	
S.2	WAMAS	Severo	Até 2 dias - 48 horas	
S.3	GERA	Severo	Até 2 dias - 48 horas	
S.4	Knapp - Transelevador	Severo	Até 2 dias - 48 horas	
S.5	Pratico Live	Severo	Até 2 dias - 48 horas	
S.7	Senior	Severo	Até 2 dias - 48 horas	
S.8	Linx	Severo	Até 2 dias - 48 horas	
S.60	Schaefer - Transelevador	Severo	Até 2 dias - 48 horas	
S.63	MES Apriso	Severo	Até 1 dia - 24 horas	
S.64	Sprinkler	Severo	Até 2 dias - 48 horas	
S.68	UC 4	Severo	Até 2 dias - 48 horas	
S.69	Avaya	Severo	Até 2 dias - 48 horas	
S.71	SAP R3	Severo	Até 2 dias - 48 horas	
S.72	SAP Retail	Severo	Até 2 dias - 48 horas	
S.73	SAP APO	Severo	Até 2 dias - 48 horas	
S.74	SAP BW	Severo	Até 2 dias - 48 horas	
S.75	SAP HANA	Severo	Até 2 dias - 48 horas	
S.76	SAP CRM	Severo	Até 2 dias - 48 horas	
S.77	SAP MII	Severo	Até 2 dias - 48 horas	
S.78	SAP PI	Severo	Até 2 dias - 48 horas	
S.79	SAP NFE	Severo	Até 2 dias - 48 horas	

Listagem dos Sistemas Que apoiam as Atividades Críticas

Critério de Seleção:

Tempo x Impacto

Fonte: Software INTERISK



Teoricamente, estou com minhas joias da coroa protegidas, certo?

Errado!

Ainda falta o elo mais crítico deste sistema: o fator humano!

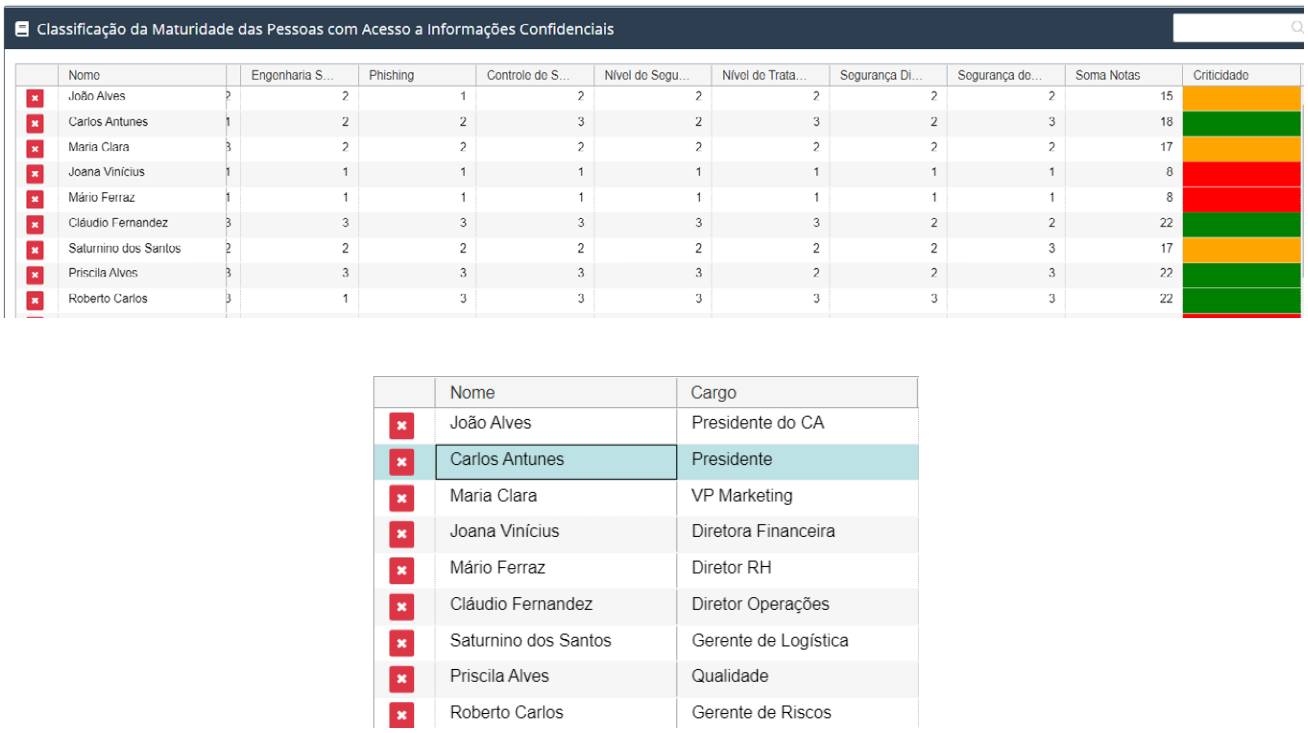
QUARTO PASSO

O quarto passo significa identificar quais são as pessoas, e não o cargo, que manipulam ou têm acesso às informações. Temos que saber o nível de maturidade destas pessoas. Isso mesmo! Temos que fazer uma avaliação e identificar seus pontos fracos nos quesitos:

- Engenharia social;
- Técnicas de indução;
- Phishing;
- Controle de senhas – de que forma controla e nível de complexidade;
- Nível de segurança de seu computador ou aparelho mobile: criptografado, utilização de senhas, entre outros;
- Nível de tratamento com segurança de documentos físicos: leitura em locais públicos, deixar o documento em cima de mesas, poltronas, salas de reunião, etc.;
- Segurança digital - trabalha em locais públicos com computador e aparelhos mobile;
- Segurança de redes: utiliza redes abertas públicas, tais como hotéis e aeroportos.

Qual a importância de sabermos a maturidade sobre confidencialidade das informações dessas pessoas sensíveis e estratégicas para as empresas?

A importância é identificar as fraquezas e tratá-las. Assim, é possível evitar que as organizações sejam alvos de possíveis agressores. Podemos montar uma régua, com base nos oito quesitos e termos um range de maturidade:



	Nome	Cargo
✖	João Alves	Presidente do CA
✖	Carlos Antunes	Presidente
✖	Maria Clara	VP Marketing
✖	Joana Vinícius	Diretora Financeira
✖	Mário Ferraz	Diretor RH
✖	Cláudio Fernandez	Diretor Operações
✖	Saturnino dos Santos	Gerente de Logística
✖	Priscila Alves	Qualidade
✖	Roberto Carlos	Gerente de Riscos

Fonte: Software INTERISK

Vejam que temos que avaliar a pessoa e não o cargo, pois cada um possui características e atitudes diferentes. Por esta razão, é primordial sabermos as pessoas na organização que manipulam as informações e dados sensíveis e estratégicos.

Fonte: Software INTERISK

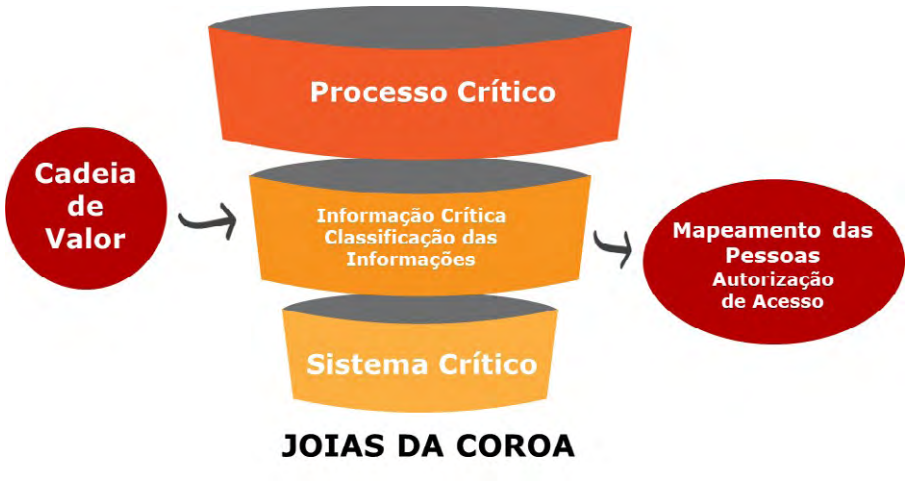
Em seguida, temos que saber quais informações essas pessoas manipulam e a criticidade apurada. No exemplo abaixo, Carlos Antunes – que é presidente da empresa possui um nível de maturidade boa. Classificado como verde, ele manipula algumas informações sensíveis.

Com esses quatro passos estabelecidos, poderemos identificar os riscos possíveis e a gestão dos ativos primordiais para a empresa. Vejam que as empresas ficam míopes em relação aos quesitos citados. Se preocupam em colocar muita tecnologia e esquecem o processo estruturado de Data Loss Prevention – DLP.

O que as organizações devem entender é o que define uma Maturidade em Segurança Cibernética é o foco nos objetivos e a interconectividade com a estratégia de negócios.

Caso não ocorra essa conexão, as empresas literalmente enxugarão gelo. Não é nada produtivo implantar uma série de sistemas sem que elas conheçam suas reais fragilidades.

Na Brasiliano INTERISK, elaboramos projetos de Data Loss Prevention - DLP no nosso sistema INTERISK, de forma que o dono do processo possa aplicar esta avaliação. Portanto, a eficácia será muito maior. A grande parte das empresas esquecem a primeira e quarta fase. Daí, vemos essa grande vulnerabilidade que as corporações possuem.



Fonte: Brasiliano INTERISK

Um processo estruturado de DLP coloca a empresa em grande vantagem competitiva, especialmente neste mundo BANI – Frágil – Ansioso – Não Linear – Incompreensível.

A IMPORTÂNCIA DA SEGURANÇA PATRIMONIAL NA ESCOLHA DO OPERADOR LOGÍSTICO

Alexandre Sabariz
Publicado no LinkedIn em 08/02/2018

A Segurança Patrimonial é considerada estratégica tendo em vista que as perdas patrimoniais podem causar sérios danos aos negócios, inclusive ao ponto de cessar as atividades da empresa. O valor da Segurança Patrimonial está diretamente relacionado a cadeia estratégica e aumenta de acordo com o valor agregado do produto final comercializado pela empresa.

A estrutura de Segurança Patrimonial alocada em cada instalação está diretamente relacionada aos riscos identificados.

Dessa forma, cabe destacar que mediante a escolha de um operador logístico que atenda diversas empresas numa mesma instalação que, claramente, o seu risco pode ser aumentado na mesma proporção do segmento de outras organizações que compartilhem o mesmo espaço.

A estrutura de Segurança Patrimonial deve, impreterivelmente, possuir procedimentos documentados que façam frente aos riscos identificados e requisitos legais de segurança.

Quando se armazena materiais e produtos de alto risco de furto, estes devem ser mantidos em locais fechados e com acesso restrito aos funcionários responsáveis por essa operação.

Um dos principais aspectos para monitorar a segurança patrimonial é no que tange ao controle de acesso de pessoas autorizadas a entrar nas instalações do

operador logístico (funcionários, prestadores de serviço e visitantes), que devem seguir procedimentos preestabelecidos e ter acesso restrito em conformidade com a necessidade de acesso funcional as diversas áreas da instalação.

Dispositivos de segurança devem ser utilizados com o objetivo de inibir, dificultar a invasão, ou subtração de bens e ainda, facilitar a identificação dos responsáveis por qualquer dano ao patrimônio.

O projeto de segurança patrimonial deve ser dimensionado de acordo com o risco afeto a cada instalação e em linhas gerais, deve prever a utilização de alguns recursos, entre eles: catracas, circuitos fechados de televisão, concertina, sensores de movimento, sistemas de alarme nos armazéns, guaritas blindadas, cercas elétricas e etc.

Os funcionários do depósito devem ser submetidos a treinamentos regulares de segurança patrimonial com o objetivo de elevar o nível de consciência em segurança e por consequência, reduzir a exposição de risco da empresa.

Abaixo requisitos mínimos de segurança a serem considerados na escolha de um operador logístico.

BARREIRAS PERIMETRAIS E ILUMINAÇÃO

1.1. Todo o perímetro da instalação deve ser protegido com muros e concertina.

1.2. Os portões de acesso para veículos e pessoas devem ser automatizados.

1.3. O acesso principal a instalação deve possuir um interfone para contato entre os fornecedores/visitantes e a portaria.

1.4. Todo o perímetro interno da instalação deve possuir uma iluminação compatível com a operação.

Nota importante: De acordo com o risco afeto a operação é importante avaliar a necessidade de portaria blindada e sistema de eclusa.

EQUIPE DE VIGILÂNCIA/PORTARIA & PROCEDIMENTOS

1.5. O efetivo de serviço deve ser adequado a demanda da instalação no tocante as atividades inerentes a vigilância/portaria.

1.6. A portaria deve possuir um meio de comunicação para contato com as pessoas chaves da instalação (responsável pela instalação, responsável pela segurança, responsável pelo depósito, etc.).

1.7. A portaria deve possuir um meio de comunicação para contato com serviços de emergência (Polícia, Socorro Médico, etc.).

1.8. A portaria deve possuir uma relação de telefones úteis para situações de emergência (contatos chaves, serviços de emergência e etc.).

1.9. A instalação deve possuir um procedimento formal para controle de acesso de pessoas e veículos. Este procedimento deve abranger, no mínimo, os seguintes tópicos:

- Tipos de crachás utilizados na instalação;
- Controle de acesso para funcionários, estagiários, contratados e visitantes;
- Acesso Proibido (arma de fogo e etc.);
- Verificação de volumes de funcionários, estagiários, contratados e visitantes;
- Verificação de veículos particulares com acesso ao interior da instalação;
- Áreas de acesso restrito (depósito e etc.).

1.10. A instalação deve possuir um procedimento formal para entrada e saída de materiais. Este procedimento deve descrever a forma de acesso e saída de materiais/ equipamentos de propriedades da CONTRATANTE, terceiros e da instalação (Operador Logístico).

1.11. A instalação deve possuir um procedimento formal sobre o controle de chaves (local de guarda, mecanismo de controle e etc.).

1.12. A equipe de vigilância/portaria deve possuir um procedimento formal sobre as rotinas afetas a vigilância/portaria.

1.13. A instalação deve informar de imediato ao CONTRATANTE qualquer irregularidade identificada no transcurso da operação, sob a ótica de Segurança Patrimonial, tais como: tentativa de invasão, diferença de estoque, furto interno, roubo, sabotagem e etc.

SISTEMA DE ALARME & CFTV

1.14. A equipe de vigilância/portaria deve possuir, no mínimo, um dispositivo de pânico silencioso ligado a uma empresa externa com monitoramento ininterrupto.

1.15. As portas de acesso ao depósito devem ser equipadas com dispositivo de alarme (detector de presença, sensor magnético ou dispositivo equivalente) ligado a uma empresa externa com monitoramento ininterrupto.

1.16. O sistema de alarme do depósito deve ser mantido ligado nos dias/horários sem atividade.

1.17. As gravações de imagens devem ser de boa qualidade nos períodos diurno e noturno.

1.18. O local destinado a gravação de imagens deve ser seguro e de acesso restrito.

1.19. Todos os pontos de acesso a instalação (acesso de pessoas e veículos) devem ser protegidos com câmeras.

1.20. Todos os pontos de acesso ao depósito (com produtos da CONTRATANTE) devem ser protegidos por câmeras.

1.21. As áreas de carga e descarga devem ser protegidas por câmeras.

1.22. O local destinado a gravação de imagens deve ser protegido por uma câmera.

1.23. O sistema de gravação digital de imagens deve comportar um arquivo de, no mínimo, 30 dias para cada câmera.

Por último, cabe o destaque aos aspectos inerentes ao Gerenciamento de Risco e Segurança Patrimonial em face da violência crescente que atinge o nosso país. Nesse tópico é de fundamental relevância uma análise criteriosa para determinar o grau de risco e atratividade dos produtos comercializados, assim como uma criteriosa escolha do operador logístico lembrando que no caso de espaços compartilhados existe a possibilidade de transferência de risco, entre produtos de maior atratividade para aqueles de menor atratividade.

Dessa forma, é de fundamental importância que a estrutura de Segurança Patrimonial esteja adequada para fazer frente às ameaças afetas a cada operação.

ENTREVISTA DE SEGURANÇA PATRIMONIAL COM OPERADOR LOGÍSTICO

Alexandre Sabariz
Publicado no LinkedIn em 14/02/2018.

Em continuidade ao artigo publicado anteriormente, segue abaixo modelo de entrevista a ser conduzida durante o processo de seleção de um operador logístico sob a ótica de segurança patrimonial. A partir das respostas obtidas nessa entrevista, o especialista deverá realizar uma análise frente aos riscos identificados na instalação e requisitos mínimos de segurança. Entende-se como aceitável a elaboração de um Plano de Ação para o atendimento dos requisitos não atendidos pelo operador, mas com a recomendação que a ocupação da instalação somente ocorra após o fiel cumprimento dos pontos sinalizados e que tal acordo, faça parte do contrato entre as partes - dispondo ainda de autonomia para a Área de Segurança auditar a instalação a qualquer momento mediante notificação prévia a contratada.

Nota 1: É de fundamental importância que a Área de Segurança Patrimonial participe ativamente desse processo de seleção juntamente com outras áreas chaves (Logística, Compras, Segurança do Trabalho e etc.) da companhia.

Nota 2: As questões formuladas nesse relatório devem ser avaliadas de acordo com o contrato que será desenvolvido com o operador logístico e grau de risco dos produtos da contratante, ou seja, o mesmo pode ser reduzido ou ampliado em conformidade com as necessidades do contratante.

i) Data:

ii) Nome do operador e endereço:

iii) Executada por:

1. Gerência da Unidade

1.1. Responsável pela Instalação:

1.2. Responsável pela Segurança Patrimonial:

2. Descrição da Unidade

2.1. Área Total:

2.2. Número de empregados diretos:

2.3. Número de empregados indiretos:

2.4. Padrão normal de Trabalho (horário de funcionamento):

2.5. Em algum momento, a unidade fica sem operação logística:

2.6. Como é o estacionamento (funcionários, prestadores de serviço, visitantes, interno/externo e etc.):

2.7. A portaria da empresa é construída em alvenaria, blindada, outras informações relevantes:

3. Missão da Unidade & Área de Responsabilidade

3.1. Quais a missão e visão da unidade sob a ótica do operador:

3.2. Quais os clientes atendidos na unidade:

3.3. Como esta unidade se encaixará na rede de distribuição da Contratante:

3.4. Qualquer plano futuro (expansão, redução, mudança de função e etc.):

4. Normas de Segurança & Armazenamento

4.1. Houve alguma mudança estrutural ou de desenho nas instalações desde a última inspeção (se for o caso):

4.2. Existe uma cerca de perímetro: Se afirmativo, de que tipo: correntes, rede soldada, tela laminada e etc.

4.3. Quantas entradas para a unidade existem e como o acesso é controlado:

4.4. Existe um procedimento formal (escrito) para controle de acesso de pessoas e veículos:

4.5. A unidade realiza verificação de veículos e pessoas: caso sim, como é o processo:

4.6. Qual é a estrutura e condição dos prédios:

4.7. Existe alguma iluminação externa e esta está em operação durante as horas noturnas:

4.8. Existe um sistema de circuito interno de TV (total de câmeras):

4.9. Ele cobre os prédios da unidade interna e externamente (depósito, áreas de acesso a unidade):

4.10. Todos os itens consignados da Contratante são monitorados por câmeras específicas:

4.11. Onde é mantido o sistema de gravação do circuito interno de TV e como este é protegido:

4.12. Qual o regime existente para o armazenamento das gravações:

4.13. Existe algum monitoramento do sistema fora da unidade:

4.14. Tem manutenção: Por quem:

4.15. Existe um Sistema de Detecção de Intrusos (Sistema de Alarme):

4.16. Quais áreas das instalações são cobertas por ele: Existe botão de pânico silencioso:

4.17. As portas de incêndio são conectadas a ele e estão ativas todo o tempo:

4.18. Quem monitora o alarme durante o expediente normal de trabalho e fora dele:

4.19. Quais os procedimentos para reagir a um alarme ativado:

4.20. Tem manutenção: Por quem:

4.21. Existe um Sistema de Controle de Acesso Eletrônico:

4.22. De tipo e quais áreas das instalações são cobertas: o acesso é seletivo:

4.23. Quem controla e programa o sistema:

4.24. Que procedimentos está em uso para controlar os crachás/cartões emitidos:

4.25. Tem manutenção: Por quem:

4.26. O Sistema de Controle de Acesso de visitantes emite crachás com fotos, nominais e sem fotos, não emite crachás nominais:

4.27. A portaria de entrada de caminhões é independente ou é a mesma utilizada para os demais veículos:

4.28. Existem vigilantes nas instalações (quantos / esquema de trabalho):

4.29. Qual empresa (empresa legalizada junto a DPF): há quanto tempo:

4.30. Como é realizada a comunicação entre os vigilantes (rádio, telefone, botão de alarme, etc.):

4.31. Eles possuem instruções específicas para cobrir tarefas de rotina e procedimentos de emergência:

4.32. É mantido um diário de ocorrências: Quem o verifica:

4.33. Como os visitantes são controlados:

4.34. Todas as datas e horas dos manifestos de consignação são carimbados antes da saída ou no momento da entrega:

4.35. É permitido aos motoristas supervisionar o embarque e desembarque da carga:

4.36. Existe uma área de espera para os caminhões no interior do operador:

4.37. Existe uma área de espera para os motoristas e acompanhantes no interior do operador (sala de TV, banheiro, etc.):

4.38. É executado um processo de checagem cadastral durante a admissão dos funcionários que trabalham na instalação: após a admissão, existe alguma outra rotina:

5. Relatório de Ocorrência

5.1. Que procedimentos existem para notificar a Contratante de:

5.1.1. Falha(s) no procedimento da contratante:

5.1.2. Ocorrências incomuns ou suspeitas:

5.1.3. Perda, furto ou roubo de qualquer produto da contratante:

5.2. Nos últimos 5 anos a unidade passou por alguma das seguintes situações (mesmo que tentativa frustrada):

( ) Roubo com utilização de arma de fogo

( ) Furtos de produtos fabricados ou comercializados pela empresa

( ) Roubo de carga

( ) Invasão de pessoal não autorizado

( ) Extorsão (da empresa ou de funcionários)

( ) Seqüestro de cargos chaves

( ) Ameaças de bombas

( ) Ameaças de invasão

( ) Ameaças relativas ao tráfico de drogas

( ) Tráfico interno de drogas

( ) Sabotagem

( ) Outras ameaças (favor descrever)

6. Outras informações

Nota: Espaço aberto para outras informações relevantes a segurança do depósito/ instalação.

REPORTAR A QUEM ...

Alexandre Sabariz
Publicado no LinkedIn em 16/10/2016.

Uma das discussões recorrentes em nosso segmento é sobre a qual área o Departamento de Segurança Patrimonial deva ser subordinado. Nas empresas globais não tenho nenhuma dúvida em apontar que a melhor alternativa é o reporte direto a Área Global de Segurança visando principalmente o alinhamento das premissas técnicas e corporativas associado à total independência nas ações locais. Ressalto principalmente a importância da independência para as ações locais no que tange aos processos de sindicância interna nos quais o Departamento de Segurança é um dos principais responsáveis pela apuração de possíveis desvios internos. Nas empresas locais ou globais (... que entendam que essa não é a alternativa), a busca da melhor solução em termos de subordinação não é um assunto pacificado. Reporte direto a Presidência (CEO), Departamento de Recursos Humanos, Departamento de Segurança do Trabalho (HES - Environment, Health and Safety) e Departamento Jurídico são alguns exemplos de subordinação identificados no Brasil para o Departamento de Segurança Patrimonial. Entendo que essa decisão deva levar em consideração principalmente o organograma funcional da companhia e as atribuições funcionais que serão delegadas ao Departamento de Segurança Patrimonial. Dentro dessa análise em busca da melhor alternativa, faço uma ressalva no sentido que o Departamento de Segurança Patrimonial não seja subordinado aos segmentos internos mais expostos a fraudes. Esse tipo de situação pode causar constrangimento e ineficiência em possíveis processos internos de apuração. Observamos dessa forma que tão importante quando determinar a melhor subordinação é identificar as áreas que devem ser evitadas para esse fim. Lembrando ainda que quando mencionamos

os organogramas usam-se as linhas cheias e pontilhadas para indicar as relações hierárquicas (solid-line) e as linhas pontilhadas para relações de intercâmbio de informações, mas sem relação de subordinação (dotted-line).

A IMPORTÂNCIA DOS INDICADORES DE PERFORMANCE NA SEGURANÇA EMPRESARIAL

Alexandre Sabariz
Publicado no LinkedIn em 30/08/2015

O indicador de performance (em inglês, Key Performance Indicator - KPI) são ferramentas de gestão a fim de realizar a medição e por consequência, o nível de desempenho de uma empresa, departamento ou de um processo, com foco no como e sinalizando quão bem os itens mensurados estão alinhados com os objetivos a serem alcançados. Na Segurança Corporativa assim como em qualquer outra área é de fundamental importância que existam indicadores de performance pois como mencionava o guru da Administração Moderna, Peter Drucker, «o que não é medido não pode ser gerenciado».

Os Indicadores de performance, por conceito, devem ser mensuráveis. Avaliando a particularidade mensurável de um indicador, podemos afirmar que o mesmo deve ser relevante e obedecer a lógica “SMART”. Em inglês, significa “específico” (sua medição deve obedecer a uma lógica clara e objetiva), “mensurável” (pode ser medido), «alcançável» (pode ser atingido), “relevante” (relevante para o responsável pelo processo e para a estratégia da organização) e, por último, deve ser medido em um “tempo” que será determinado previamente.

Nessa busca pelos indicadores chegamos até os Leading (lead) Indicators e Lagging (lag) Indicators. É difícil buscar uma tradução para o Português, mas após alguma pesquisa, entendo que a melhor forma de mensurá-los é que os Indicadores Lead apontam para o desempenho futuro e os Indicadores Lag para o desempenho passado. Todas as pesquisas, em empresas de referência, na busca pelos fatores determinantes para o sucesso do modelo de gestão, indicam que a

utilização balanceada de Indicadores Lead e Lag é um ponto comum. Dessa forma, é possível deduzir que a sua utilização combinada contribui para o processo de melhoria contínua das corporações.

Na condição de advisor de um Processo de Excelência Operacional estabelecido há oito anos e focado em Segurança Corporativa entendo que temos, no mínimo, quatro grupos de assuntos que obrigatoriamente devem ser mensurados:

- Os incidentes de segurança (lag indicator): incidentes na instalação, incidentes com ativos da companhia, incidentes com funcionários locais, incidentes com funcionários expatriados, incidentes com visitantes (business travelers) e etc.
- Resposta a incidentes de segurança (lag indicator): tempo para detecção e alerta, efetividade da resposta e etc.
- Programa de Conscientização em Segurança (lead indicator): alertas de segurança, relatórios mensais, treinamentos online, reuniões, palestras, campanhas, table top, drills e etc.
- Plano de Melhoria Contínua - Continuous Improvement Plan, CIP (lead indicator): revisão de processos, revisão dos planos de segurança, atualização do Risk/Threat Assessment, instalação de novos recursos de segurança eletrônica, upgrade em segurança eletrônica e etc. Em linhas gerais, uma aferição das melhorias programadas frente à efetividade das melhorias realizadas.

Outro ponto importante é o método para definição das métricas anuais. Recomendo a realização de, no mínimo, uma reunião de diagnóstico com a participação das pessoas chaves no processo tendo como parâmetro os resultados do ano anterior frente à expectativa para o novo ano e recursos disponíveis.

Nas empresas globais é de suma importância que existam indicadores de perfomance padronizados visando mensurar as regiões com maior criticidade para as operações e assim definir claramente quais os requisitos mínimos de segurança a serem desenvolvidos em cada local com o objetivo de reduzir e mitigar o risco de incidentes de segurança.

“Nós somos aquilo que fazemos repetidamente. Excelência, então, não é um modo de agir, mas um hábito. Will Durant”

OS PROFISSIONAIS MADUROS NO MUNDO VUCA

Alexandre Sabariz
Publicado no LinkedIn em 17/07/2019

No mundo VUCA os profissionais mais maduros precisam tomar muito cuidado para não cair na vala comum de expor o seu background com base, somente, no quantitativo de anos trabalhados. Tenho observado com certa frequência a máxima de falar em experiência com base na tese do acumulo de anos trabalhados e não, de conhecimentos adquiridos na mesma proporção.

Dentro dessa ótica, a oportunidade de conhecer diferentes realidades corporativas, normalmente, é um aspecto de grande valia nessa "jornada". Quando faço uma viagem ao passado é nítida a diferença para a geração dos meus pais sob diversas óticas e sob o prisma profissional não é diferente. Naquele tempo o nível de especialização e competitividade eram completamente diferentes e hoje, afirmo para os meus filhos que precisam trabalhar muito duro para alcançar o novo patamar que garanta um nível razoável de empregabilidade e trabalhabilidade. Apesar de ter somente 51 anos de idade, tenho amigos na mesma faixa etária já aposentados via serviço público e outros que por medo optaram por requerer a aposentadoria ainda dentro da atual regulamentação.

Para continuarem competitivos os profissionais maduros além da experiência adquirida pelos anos de serviço precisam agregar novos conhecimentos visando ampliar o escopo generalista e ainda, o conceito de "mente aberta" no sentido de aprender a desaprender para aprender novamente. Um outro aspecto que move a dinâmica da vida contemporânea é a resiliência. Quando penso em resiliência associo a capacidade de "navegar" em diversas atmosferas organizacionais, em qualquer nível

de pressão e exigências mantendo o nível de entrega e principalmente, preservando a saúde física e mental.

Em suma, como aprendemos na Matriz SWOT, precisamos trabalhar e aprender a lidar com as nossas forças e fraquezas visando fazer frente as novas oportunidades e ameaças do Mundo VUCA.

CONHECE O MUNDO BANI? NÃO? SERÁ QUE NÃO HÁ RISCO DE NÃO ACOMPANHAR O NOVO NORMAL?

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.

O mundo nunca foi tão digital como agora, tudo gera dados e muitos! A era dos dados gerou um ambiente de informação – e a Internet das Coisas – IOT – tem um papel extremamente motriz neste contexto.

Esse ecossistema é responsável pela aceleração do ritmo da evolução tecnológica, amplificando o acesso à tecnologia, encurtando de forma drástica o ciclo das transformações.

Com estas disrupções constantes e a chegada da pandemia COVID-19, o conceito de mundo VUCA - mundo Volátil, Incerto, Complexo e Ambíguo, conforme se refere o acrônimo em inglês, voltou com força total, com muitos gestores e empresários rápidos ao lembrarem dessa denominação, que por muito tempo foi utilizada para aconselhar empresas a se desenvolverem e navegarem em um cenário de completa névoa.

Quando falamos sobre o mundo VUCA, estamos nos referindo a um termo criado no final dos anos 80. A pandemia mostrou que a estratégia VUCA foi insuficiente perante as contingências que se apresentaram, uma vez que poucas empresas estavam verdadeiramente prontas para o que aconteceu —mostrando que o VUCA poderia ser uma ideia datada. Será?

HISTÓRICO DO TERMO VUCA

Dr. T. Owen Jacobs, psicólogo, que pesquisou e ensinou de 1974 a 2005, quando atuou no Instituto de Pesquisa do Exército Americano e ministrou cursos no War College sobre as questões ligadas ao comportamento da liderança estratégica, pensamento criativo e crítico, foi quem cunhou pela primeira vez o termo VUCA – Volatidade, Incerteza, Complexidade e Ambiguidade. Suas pesquisas focaram sobre os requisitos do desempenho estratégico dos líderes em situações incertas e voláteis, com o objetivo de identificar e desenvolver habilidades necessárias para a liderança estratégica do Exército Americano. O Dr. Jacobs pesquisou e coletou dados sobre as conexões entre personalidade, habilidades interpessoais e habilidades que levavam a um grau de eficácia do líder nos ambientes, que poderiam reproduzir as incertezas do campo de batalha e dos contextos que os generais teriam que enfrentar como comandantes de tropas de ocupação em territórios, áreas e ou países hostis. O Dr. Jacobs montou um processo de avaliação para identificar especificamente os principais atributos de liderança que prevêem o sucesso do líder. Os atributos avaliados são projetados para permitir a descoberta de necessidades específicas de desenvolvimento no nível médio, superior e executivo, e, são considerados altamente preditivos (que se pode predizer, prever por antecipação, com antecedência) para o futuro sucesso da liderança estratégica.

Dr. Jacobs publicou no War College, como professor de Liderança Estratégica, o livro intitulado The Competitive Edge. Neste livro o professor descreve o ambiente externo como preenchido de “volatility”, “uncertainty”, “complexity” e “ambiguity”, tendo o acrônico de VUCA. Enfatiza que o ambiente da era da informação, com um volume muito grande, está repleto de VUCA, fazendo com que a liderança que se descuidar e/ou não tenha rigor para entender o ambiente, possivelmente não conseguirá antecipar as mudanças e nem gerenciar riscos emergentes. Este é o desafio da liderança estratégica.

Escreve ainda que os líderes do século XXI devem se aproximar desse conceito com inteligência, energia e senso de urgência, confiante de que essas realidades e as complexidades podem ser facilmente transformadas em uma vantagem competitiva quando viradas contra os inimigos da nação. Dada a extensão de suas responsabilidades e os efeitos da expansão de suas decisões, os líderes estratégicos devem considerar uma grande variedade de fatos, influências e atores. Dizer que a eles que devem considerar que tudo pode ser apenas um ligeiro exagero, seria uma falta de visão holística. Aqui reside o ponto principal. Já comentava o Dr. Jacobs, que com grande volume de informações, fluxo em alta velocidade, tempo limitado e conhecimento finito, líderes efetivos devem, literalmente, decidir nos pontos focais, nos pontos que realmente darão retorno e eficácia na ação. Ou seja, a liderança estratégica deve determinar quais elementos do seu ambiente são mais importantes para uma situação particular ou decisão e, em seguida, concentrar sua atenção e esforços neste ponto.

Líderes estratégicos e estrategistas devem entender, interpretar e dominar o denominado ambiente VUCA!

Jacobs sugere que os líderes não podem alcançar um conhecimento completo sobre todo o contexto que incidem nas decisões estratégicas. O verdadeiro líder estratégico irá tomar decisões na maioria das vezes sem ter a imagem do quadro todo, pisando na incerteza. Isto não é novo, Clausewitz, o General Prussiano, que escreveu o Tratado chamado “Da Guerra” e que foi prisioneiro de Napoleão, já insistia que o Comandante Estrategista teria que ter sempre como amante a incerteza.

Por que isso? Porque o líder estratégico, tendo em vista sua posição, terá que tomar decisões rápidas e precisas, mesmo no ambiente VUCA, sem enxergar com clareza todas as variáveis. Para responder ao desafio do Mundo VUCA, primeiro devemos entender as implicações básicas dos seus termos:

- Volatilidade: a taxa de mudança do meio ambiente. Volatilidade na era da informação significa que mesmo os dados mais atualizados podem não fornecer um contexto adequado para a tomada de decisões. Além da capacidade de avaliar com precisão o ambiente atual, os líderes devem antecipar, mudar e fazer o seu melhor para prever o que pode acontecer dentro do escopo de tempo de um projeto, programa ou operação. Na verdade, este conceito está nos dizendo de forma clara, visando não perder a janela de oportunidade, que o ótimo é inimigo do bom. Ou seja, não adianta elaborar um ótimo projeto de lançamento de um produto, se a concorrência lançou na frente. Perdeu-se a oportunidade de ser o primeiro ou pioneiro. Volatilidade no meio ambiente inserido no contexto da era da quarta revolução industrial, cria um desafio especial para líderes estratégicos e toda sua equipe de suporte.

- Incerteza: a incapacidade de conhecer tudo sobre uma situação e a dificuldade de prever a natureza e efeito da mudança (o nexo de incerteza e volatilidade). Incerteza, na maioria das vezes, atrasa os processos de tomada de decisão e aumenta a probabilidade de divergir muito de opiniões sobre o futuro. Isso impulsiona a necessidade de o líder estratégico possuir uma gestão inteligente de riscos, abrangendo tanto as estratégias como as operações.

- Complexidade: a dificuldade de compreender as interações de múltiplas partes ou fatores e de prever os efeitos primários e subsequentes de mudar um ou mais fatores em um sistema altamente interdependente, interconectado. A complexidade difere de incerteza, pois a interconectividade entre as inúmeras variáveis torna o contexto muito mais complexo. Embora possa ser possível prever resultados imediatos de interações únicas e ou lineares. O desafio é que hoje as variáveis não fazem mais interações únicas, mas sim múltiplas, não lineares

que se multiplicam tão rapidamente que acabam tendo um resultado exponencial. Complexidade poderia ser resumido em criar incerteza devido ao grande volume de possíveis interações e seus resultados.

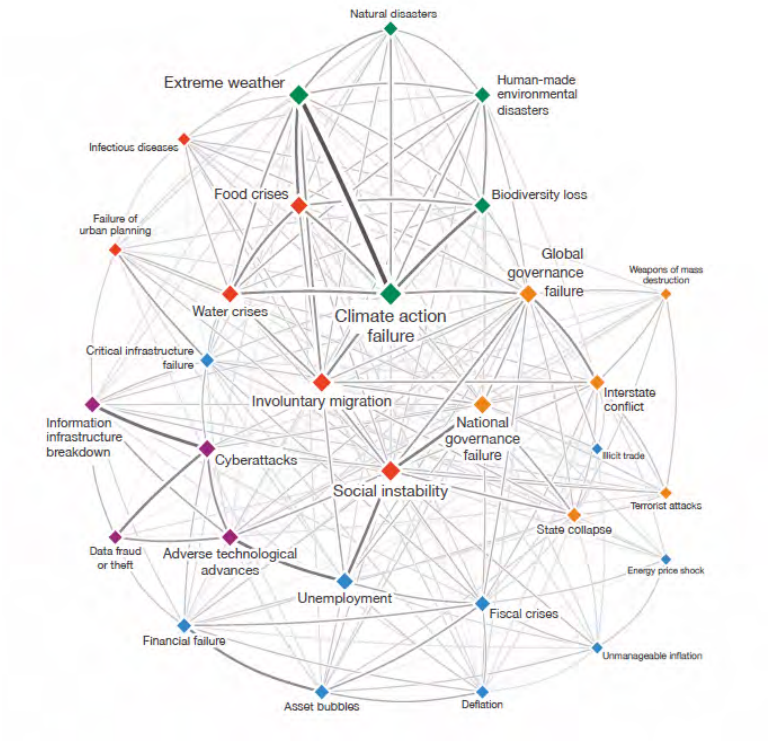


Figura 1: Matriz de Interconectividade entre os riscos globais.
Fonte: 15ª Relatório de Riscos Globais do Fórum Mundial 2020

A figura acima, representa o Mapa de Interconectividade entre os Riscos Globais. A complexidade da verificação e medição das consequências só é possível pelo mapa da interconetividade entre os riscos. A fotografia da motricidade dos riscos faz com que as lideranças empresariais enxerguem quais são os riscos sistêmicos, ou seja aqueles que influenciam um grande número de riscos, tornando-os estratégicos seu tratamento ou monitoramento.

A pandemia COVID-19, está prevista, como doença infecciosa, e no relatório disserta que se houvesse uma pandemia, grande parte dos Sistema de Saúde dos países, incluindo os do primeiro mundo, não iriam suportar a demanda. Ou seja, iriam a falência. Além do que a doença infecciosa, era considerada um risco motriz, com grande força de influência em todos os contextos dos países.

Este relatório foi publicado em 08 de janeiro de 2020, o que evidencia o negacionismo dos governantes e orgãos de inteligência de quase todo o globo.

- Ambigüidade: descreve um tipo específico de incerteza, que resulta de diferenças na interpretação de cada líder estratégico, quando pistas contextuais são insuficientes para esclarecer o significado. Ironicamente, "Ambíguo" é um termo ambíguo, cuja definição muda sutilmente dependendo da contexto de seu uso. Para os nossos propósitos aqui, refere-se à dificuldade de interpretar o significado quando o contexto é míope, borrado por fatores como cegueira cultural, viés cognitivo ou limitação perspectiva. No nível estratégico, os líderes geralmente podem interpretar legitimamente eventos em mais de uma ótica , elevando para o nível alto a probabilidade de uma má interpretação. Por esta razão é que os líderes devem sempre identificar quais são as incertezas críticas que colocam em exposição os propósitos de suas organizações. Sugerimos que utilize dois critérios, um é o impacto potencial no propósito e o outro é a probabilidade desta incerteza não acontecer. O foco será nas maiores incertezas, ou seja maiores probabilidades de não acontecerem e de maior impacto. A Matriz abaixo ilustra o quadrante estratégico que as incertezas deverão ser estudas e monitoradas.

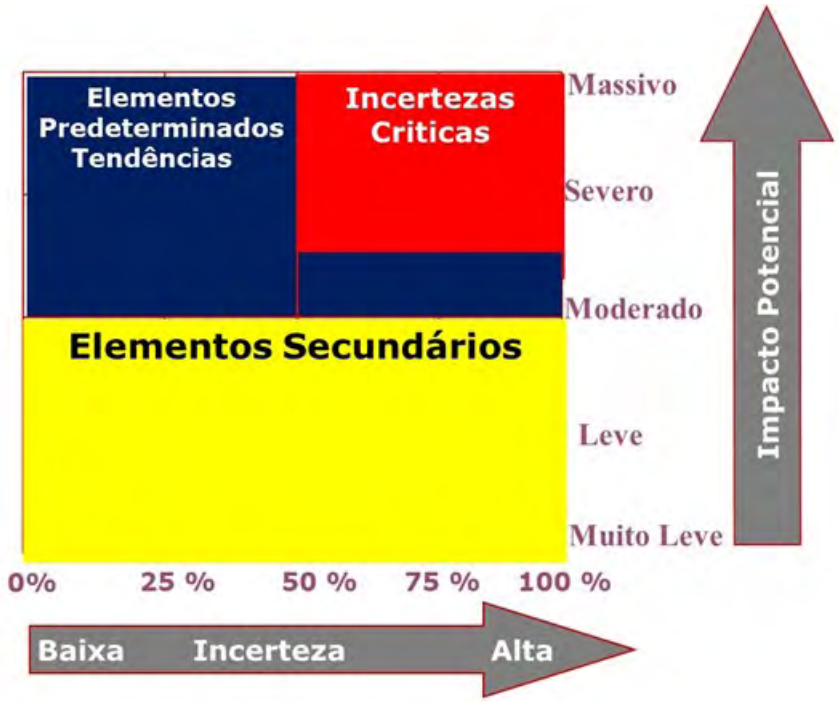


Figura 2: Matriz de Incertezas Críticas Visando Diminuir o Nível de Ambiguidade.
Fonte: Brasiliano, Antonio Celso Ribeiro. Apostilas de Aula de Cenários Prospectivos

Organizações grandes e complexas consistem em intrincadas redes de pessoal, componentes funcionais e operacionais. Alcançar Objetivos organizacionais, exige que esses componentes devam funcionar juntos e interagir com entidades igualmente complexas.

Um líder estratégico não só lidera a empresa, mas também deve representar sua empresa durante as interações necessárias com um labirinto de outras instituições que constituem o ambiente externo. Os Líderes Estratégicos devem moldar a forma e direção de suas empresas e influenciar os atores para que se esforcem na conquista dos objetivos. Devem colocar "coração e mentes". Dentro do ambiente VUCA, as tarefas devem ser realizadas de forma colaborativa e não através do esforço individual. Portanto a colaboração e a criação em conjunto, são insumos essenciais para o sucesso das empresas.

A figura abaixo resume o posicionamento do Mundo VUCA:

Figura 3: Mundo VUCA – Reações dos Líderes.
Fonte: Brasiliano, Antonio Celso Ribeiro. Apostilas de Aula de Gestão de Riscos

O que o mundo VUCA nos diz é que estamos saindo de um mundo de problemas que são resolvidos de modo cartesiano, linear, onde tudo é uma questão de análise e eliminação da incerteza para um mundo de dilemas. Mundo esse em que se exige paciência e engajamento com a incerteza, bem como orientação, processo de decisão e uma visão de perspectiva do futuro.

O COVID-19 MUDOU ESTÁ ÓTICA

A pandemia mostrou que a estratégia VUCA foi insuficiente perante as contingências que se apresentaram, uma vez que poucas empresas estavam verdadeiramente prontas para o que aconteceu mostrando que o VUCA já era uma ideia datada. Assim surgiu uma nova denominação que fala do cenário atual, levando em conta as mudanças da pandemia e outras que poderão surgir: o mundo BANI.

O conceito BANI foi desenvolvido pelo antropólogo, escritor e futurista norte-americano Jamais Cascio, que observou que o VUCA estava obsoleto e não mais funcionava em um mundo tomado pela pandemia.

BANI significa “Brittle, Anxious, Nonlinear, Incomprehensible”, ou Frágil, Ansioso, Não-linear e Incompreensível, em tradução livre.

O acrônimo carregaria a chave para que empresas possam prosperar e trazer disrupções sob a nova ótica que surgiu em 2020.

> “Um paralelo intencional com VUCA, BANI é uma estrutura para articular as situações cada vez mais comuns nas quais a simples volatilidade ou complexidade são lentes insuficientes para entender o que está acontecendo”, diz o criador da terminologia em seu artigo oficial. “Situações em que as condições não são simplesmente instáveis, são caóticas; nos quais os resultados não são simplesmente difíceis de prever, e sim completamente imprevisíveis. Ou, para usar a linguagem particular desses frameworks, situações em que o que acontece não é simplesmente ambíguo, é incompreensível.”

Interessante é que o antropólogo Jamais Cascio apresentou este novo conceito, BANI, no evento do Institute for The Future (IFTF) em 2018, três anos atrás, muito antes da pandemia começar, porém já com sinais de novos comportamentos. Argumentou que agora nós não vivemos mais no mundo VUCA, mas sim no mundo BANI.

A pandemia acelerou estes comportamentos.

ENTENDER OS CONCEITO BANI

Os quatro elementos do BANI são interconectados. Sistemas complexos e fortemente unidos tendem a ser frágeis e não lineares, o que por sua vez é incompreensível e, como resultado, gera ansiedade. É interessante notar que o contrário também acontece - a ansiedade nos leva a implementar uma infinidade de sistemas de segurança, mas em sistemas complexos, são os sistemas de segurança que geralmente contribuem ou causam as falhas. Vejamos suas definições:

Brittle - Frágil

> Sistemas frágeis são suscetíveis a falhas repentinas e catastróficas. Ao contrário de resilientes, eles são quebradiços. Estes sistemas são como o vidro de um smartphone, podem ser extremamente resistentes, mas quando quebram, eles não falham gradualmente ou graciosamente, simplesmente quebram de maneira incontrolável.

Anxious - Ansioso

Hoje, a ansiedade está no nível mais alto de todos os tempos, e isso também não é uma novidade, assim como a depressão. Em um mundo ansioso estamos constantemente no limite, esperando as próximas notícias ruins nos atingirem, ou a próxima distopia fictícia sendo apresentado como um caminho, não apenas possível, mas provável, e com muita credibilidade. Todos os elementos do termo do Mundo VUCA também geram ansiedade.

Non Linear - Não-Linear

Estudiosos e tecnólogos gostam de falar sobre crescimento ou mudança exponencial, mas em um sistema não-linear normal, a causa e o efeito estão aparentemente desconectados, e por isso não há uma melhora exponencial também. Às vezes, os dois (causa e efeito) apresentam um longo atraso entre eles - e pequenas ações tomadas, ou não, podem levar a impactos descontroladamente desproporcionais. Os seres humanos hoje, em termos técnicos, são péssimos em qualquer planejamento de longo prazo, e é por isso que agora, e pelas próximas gerações, temos que lidar com as mudanças climáticas para pior.

As mudanças climáticas, a pandemia e quaisquer outros ciclos de associação entre "causa e consequência" são um exemplo perfeito de como funciona um mundo não-linear.

Incomprehensible - Incompreensível

Arthur Clarke, autor de 2001: Uma Odisséia no Espaço, uma vez disse "qualquer tecnologia suficientemente avançada é como se fosse magia, e as coisas cotidianas agora são incompreensíveis". Estar vivo no século XXI é confiar em inúmeros sistemas complexos e incompreensíveis que afetam profundamente as nossas vidas. Ou você sabe me explicar como funciona o algoritmo do Facebook? E como a jornalista Quinn Norton apontou "até mesmo um desktop do Windows é tão complexo que ninguém no mundo sabe realmente o que está acontecendo ali ou como", e muito menos uma vasta rede desses computadores ou sistemas mais complicados.

COMO LIDAR COM ISSO

Para o antropólogo Jamais Cascio, a estrutura BANI oferece uma lente para ver e estruturar o que está acontecendo no mundo, e a sigla criada sugere oportunidades de resposta úteis para o mundo.

A fragilidade, de acordo com o antropólogo, pode ser enfrentada através de resiliência e liberdade; a ansiedade pode ser aliviada por empatia e atenção plena; a não-linearidade necessitaria do entendimento amplo do contexto e muita flexibilidade; e a incompreensibilidade pede transparência e intuição.

> "Essas podem muito bem ser mais reações do que soluções, mas sugerem a possibilidade de que respostas possam ser encontradas", comenta Jamais.

Nicholas Nassim Taleb, no seu livro Antifrágil: Coisas que se Beneficiam com o Caos, argumentou que deveríamos desenvolver sistemas antifrágeis sempre que possível. Quando não for possível, então a melhor opção seriam sistemas resilientes que falham normalmente. Porém, ao invés disso, em nossa incessante busca por eficiência, também estamos desenvolvendo e impulsionando sistemas frágeis. Com tecnologias como IoT (Internet das Coisas), estamos criando mais sistemas acoplados às nossas vidas, estes são inerentemente perigosos e complexos. E se falham, tende a ser muito mais problemático, beirando o caos.

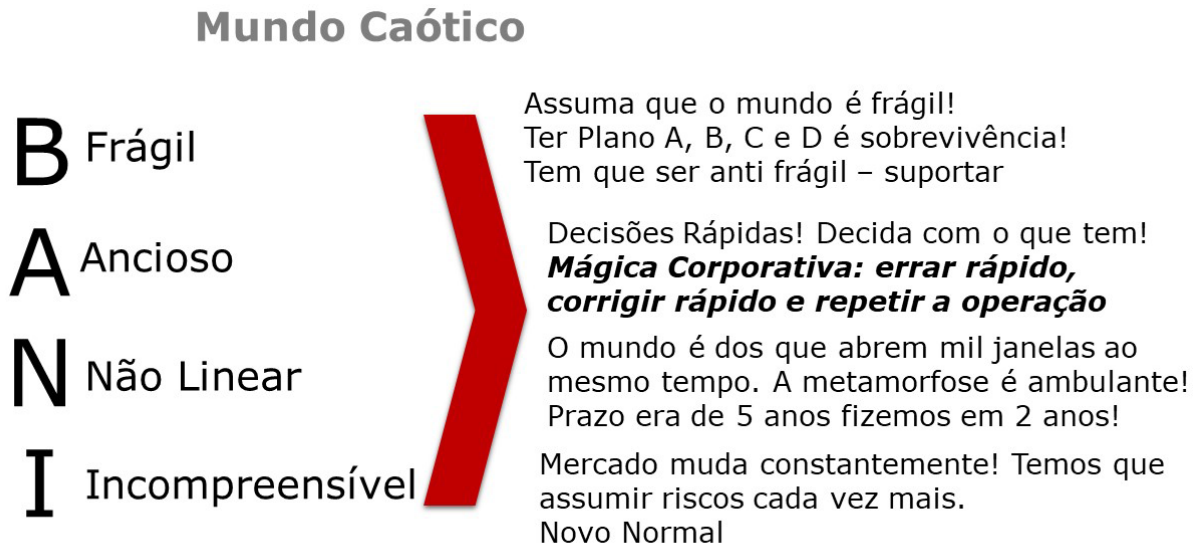


Figura 4: Mundo BANI – Situações Caóticas – Reações Extremas.
Fonte: Brasiliano, Antonio Celso Ribeiro. Apostilas de Aula de Gestão de Riscos

CONCLUSÃO

A conectividade já existia, apenas de forma diferente. Isto é irônico, pois o esforço para conectar tudo com tudo é brutal. Não existem respostas rápidas e fáceis, mas sim respostas construtivas e estas demandam estudo e tempo.

Por mais que utilizar o modelo do Mundo VUCA nos permita navegar com sucesso no ambiente atual, identificar alguns desses direcionadores do Mundo BANI nos permite dar os primeiros passos para mudar o ambiente. Aliás, o BANI pode até parecer mais assustador que o VUCA, em primeira vista, mas ele pode ser responsável por impulsionar a ação.

Está aí mais um conceito. Minha pergunta para você leitor:

É VUCA ou BANI?

O risco da escolha é nosso. Ou podemos fazer uma simbiose? Nossa ação é optar ou integrar. O tempo dirá!!!

COVID-19 AQUECE MERCADO CIBERNÉTICO NO BRASIL: NÚMERO DE ATAQUES TIVERAM CONSEQUÊNCIAS MASSIVAS EM INÚMEROS SEGMENTOS

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.

A falta de um Risk Assessment Cybersecurity nas empresas e instituições brasileiras, mostrando sua maturidade, potencializou de forma exponencial os ataques, com impactos massivos em vários segmentos, entre eles o hospitalar. A pandemia do Covid-19 elevou as ameaças cibernéticas, o Brasil foi um dos principais países alvos desses ataques. Falta sensibilização dos executivos C–level?

A resposta infelizmente é sim. Tanto a nível de Conselho de Administração como de presidência e diretoria. No artigo publicado em Harvard Business Review, em junho de 2020, os autores e especialistas de segurança cibernética, Thomas J. Parenty e Jack J. Doment, ambos fundadores da empresa de cibersegurança Archefact Group, identificaram que o primeiro foco de atuação para avaliar os riscos cibernéticos deve ser identificar as fragilidades das principais atividades da empresa, aquelas que são o "core business", e não as tecnologias em si.

Apesar dos bilhões gastos com segurança cibernética, os danos causados pelas violações continuam crescendo a cada ano, isto tem uma explicação lógica: as empresas não entendem e não conhecem seus riscos cibernéticos críticos.

Esta foi a principal razão que o Brasil, nos seis primeiros meses de 2020, foi o oitavo em número de recebimento de e-mails com temas ligados ao COVID-19.

No total foram 132 mil mensagens eletrônicas contendo algum tipo de arquivo malicioso. No mundo, os países que mais receberam ameaças desse tipo foram Estados Unidos, Alemanha e França. Estes e-mails maliciosos, detectados pela

empresa Trend Micro, o Brasil computou mais de 447 mil phishing no período, sendo o sétimo principal alvo dos atacantes no mundo.

A pandemia do COVID-19 fez com que os hackers encontrassem a vulnerabilidade do fator humano: curiosidade em clicar nas mensagens com temas relevantes do coronavírus. Por esta razão que é muito importante a sensibilização, evitando de ser alvo desta natureza. Manter os sistemas críticos, que suportam as informações críticas das atividades estratégicas é crucial para ter eficácia na segurança cibernética, além do usuário ter cautela ao abrir conteúdos de e-mails, é primordial nesse momento atípico em que estamos vivendo.

Abaixo temos a Matriz do COVID-19 Cruzando a Taxa de Reprodução x o Nível de Criticidade dos Estados do Brasil, dia 10 de setembro de 2020.

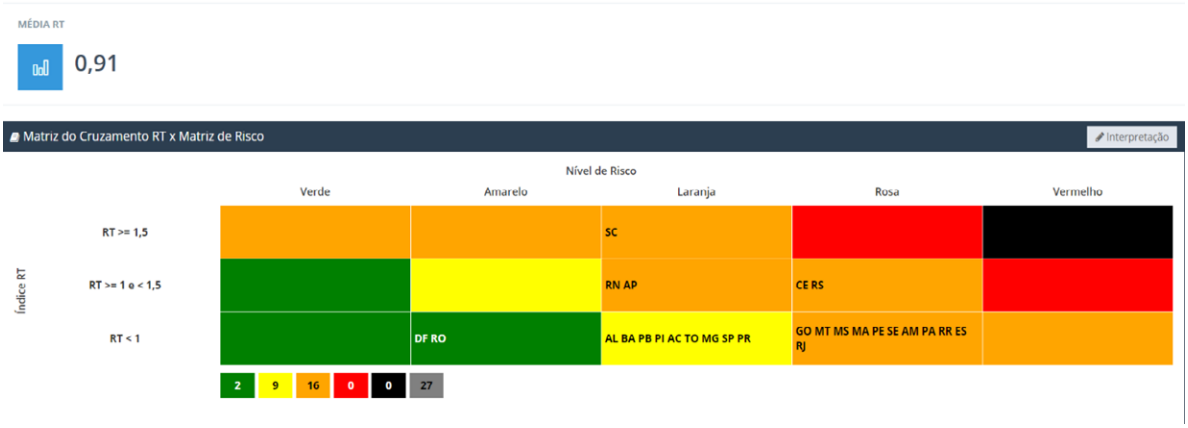


Figura 1: Metodologia CSR: Cybersecurity Risks – Matriz de Cruzamento RT x Matriz de Riscos Pandêmico - Fonte: Brasiliano INTERISK, 2020

A pandemia no Brasil está com um quadro, hoje, considerado gerenciado. Se olharmos a Matriz acima, podemos ver que a média nacional da taxa de reprodução do COVID-19, está abaixo de 1 – 0,91 - o que é um índice que considera a Pandemia controlada.

Temos apenas um Estado com índice da Rt acima de 1,5 – 1,66, Santa Catarina. O índice de 1,66 significa que a pandemia, no Estado de SC, está com uma velocidade muito alta – 100 brasileiros passam para 166. Ou seja, é considerado fora de controle.

Temos 04 Estados com o índice Rt entre 1,5 e 1,0. Velocidade mediana. O restante do Brasil está abaixo de 1,0. Cruzando com o número de infectados x leitos de UTI ocupados, chegamos no resultado da Matriz de Cruzamento, que na nossa visão já é gerenciado. As empresas, comércios e indústrias começam a retomar as suas atividades, e, com isso abre-se outra brecha em termos de segurança cibernética.

Em todo o mundo, nos seis primeiros meses do ano, a empresa de segurança cibernética Trend Micro bloqueou 8,8 milhões de ameaças desse tipo, das quais

quase 92% baseadas em e-mails. Entre janeiro e junho, os cibercriminosos mudaram seu foco para se aproveitar do interesse global na pandemia. O risco para as empresas foi agravado por falhas de segurança criadas por uma força de trabalho completamente remota.

As detecções de comprometimento de e-mail corporativo (BEC, na sigla em inglês) aumentaram 19% em todo o mundo em relação ao apurado no segundo semestre de 2019. Isso decorre em parte da maior exposição de pessoas, durante trabalho em Home Office e às técnicas de engenharia social.

Dentro deste contexto é que o processo de Risk Assessment em CyberSecurity Risks é essencial para a prevenção. A empresa irá enxergar seu real grau de maturidade frente as nomeadas "Joias da Coroa", ou seja, frente aos processos críticos de negócio, suas informações estratégicas e críticas dos processos críticos e os sistemas que suportam as informações e processos.

O processo CyberSecurity Risks, metodologia da Brasiliano INTERISK para a Gestão de Riscos Cibernéticos, o Risk Assesment compõe a elaboração da primeira e segunda etapas do processo para identificar os pontos deficientes e o nível de maturidade da empresa em termos de Cybersecurity. Na figura abaixo podemos ter a noção do processo como um todo e as fases do Risk Assessment.

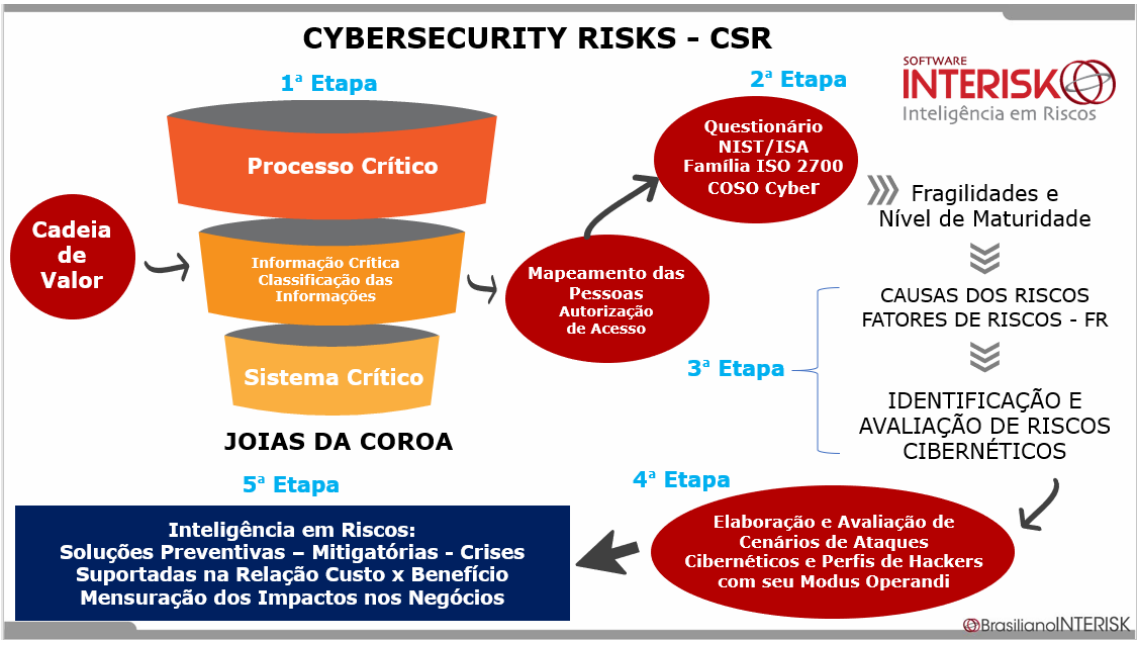


Figura 2: Metodologia CSR: Cybersecurity Risks – Fases.
Fonte: Brasiliano INTERISK, 2020

Frente a "Joias da Coroa" da empresa – processos críticos – informações estratégicas e críticas – sistemas críticos e saber mapear a maturidade das pessoas que lidam com as informações confidenciais e críticas, a empresa deve fazer um Risk Assessment, através do questionário NIST com as inclusões ainda das melhores

práticas do COSO Cyber e da ISO 27032 – Segurança Cibernética e ISO 27701 – Segurança da Privacidade.

O questionário NIST possui cinco funções da segurança cibernética, Identificar, Proteger, Detectar, Responder e Recuperar. Cada uma destas funções são parte do Sistema Integrado de Segurança Cibernética – SISC. A empresa com base nas respostas, passa a entender suas fragilidades e com isso pode ter seu nível de maturidade em segurança cibernética.

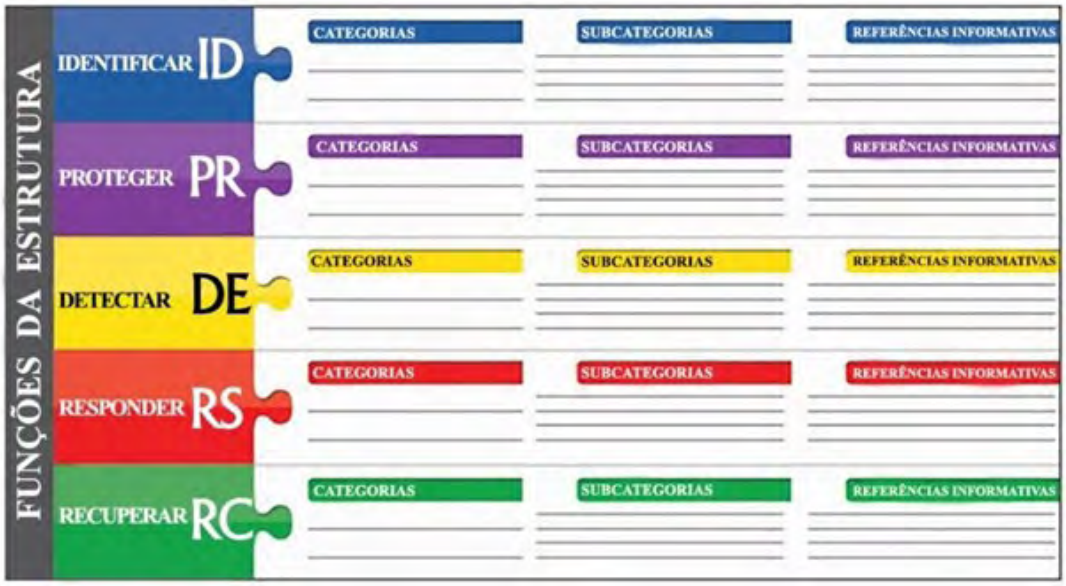


Figura 3: Estrutura do NIST- Fonte NIST 2018

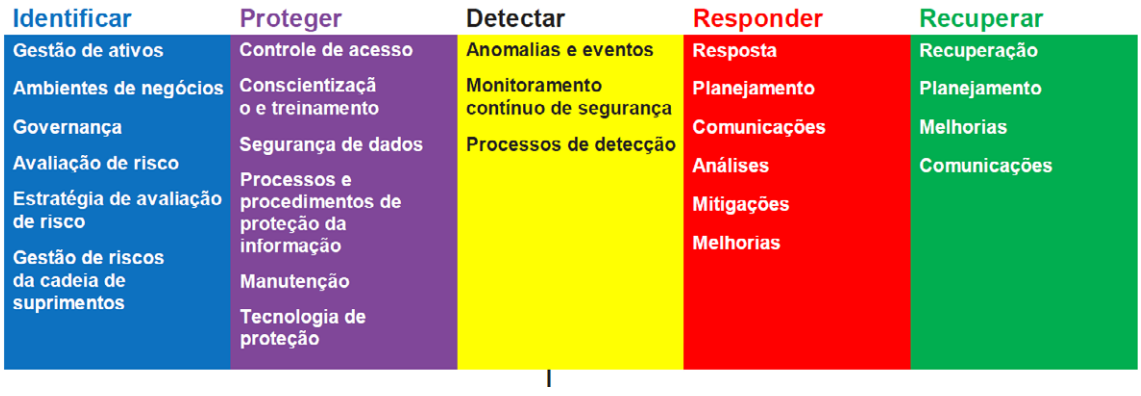


Figura 4: Funções da Estrutura CSF - NIST- Fonte NIST 2018

No sistema INTERISK temos o questionário automatizado, sendo necessário somente identificar as não conformidades e conformidades, para ranquear a Maturidade de Segurança Cibernética.

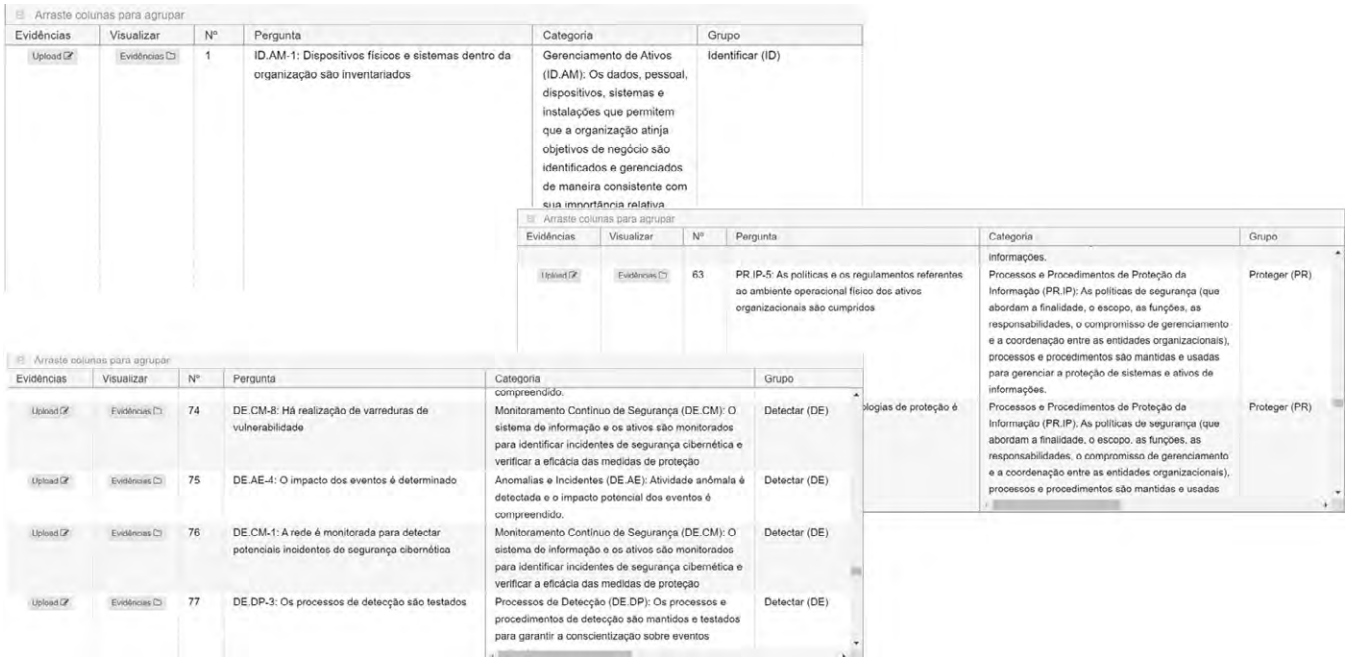


Figura 5: Questionário da Estrutura CSF – NIST 2018. Fonte Brasiliano INTERISK

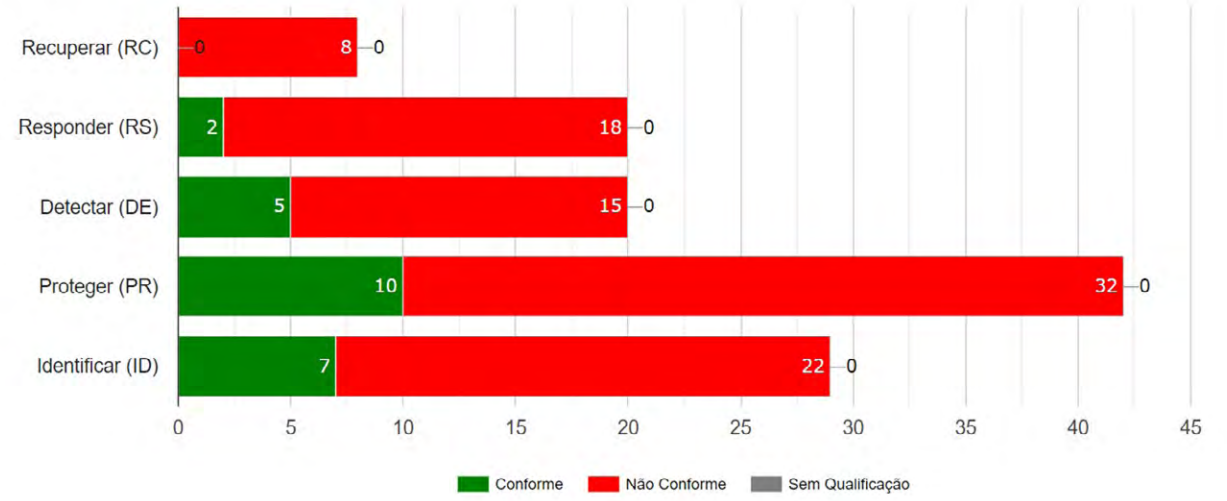


Figura 6: Indicador das Funções da Estrutura CSF – NIST 2018. Fonte Brasiliano INTERISK

A Maturidade da Segurança Cibernética, é elaborada automaticamente, com base em cinco níveis de criticidade:

Maturidade	De	Até	Recomendação
Insuficiente	0.00	3.00	Tratar
Regular	3.01	5.00	Desenvolver
Bom	5.01	7.50	Melhorar
Muito Bom	7.51	9.00	Aprimorar
Excelente	9.01	10.00	Manter

Figura 7: Níveis de Maturidade – Fonte: Brasiliano INTERISK

Nível 1: Ações vinculadas à Cibersegurança quase ou totalmente inexistentes. – VERMELHO

Nível 2: Há algumas iniciativas sobre Cibersegurança. Abordagens ad-hoc. alta dependência do pessoal. Atitude reativa diante de incidentes de segurança. –LARANJA

Nível 3: Há certas diretrizes para a execução das tarefas. Existe dependência do pessoal. Tem avançado no desenvolvimento dos processos e documentação das tarefas. – AMARELO

Nível 4: É caracterizado pela formalização e documentação de políticas e procedimentos. Governança da Cibersegurança. Métricas de acompanhamento. – VERDE CLARO

Nível 5: O Responsável pela Cibersegurança tem uma função chave no controle e melhora do SGSI. Realiza-se o controle interno. Trabalha-se na melhora continuada. A cibersegurança está alinhada com os objetivos e estratégias da organização. – VERDE ESCURO

O resultado automatizado pelo INTERISK é o Gráfico denominado Radar, onde é colocado o Nível Desejado e o Nível Atual. Com esta visão a empresa possui seu nível de fragilidade cibernética.

Descrição	Nível Desejado	Nível Atual
Identificar (ID)	10.00	2.41
Proteger (PR)	10.00	2.38
Detectar (DE)	10.00	2.50
Responder (RS)	10.00	1.00
Recuperar (RC)	10.00	0.00
SOMA	50.00	8.29
MÉDIA GERAL	10.00	1.66

Figura 08: Nível de Maturidade de Segurança Cibernética – Gráfico Radar.
Fonte: Brasiliano INTERISK

Neste caso a empresa em estudo possui um nível de maturidade muito baixo, o que a deixa fragilizada para ciberataques.

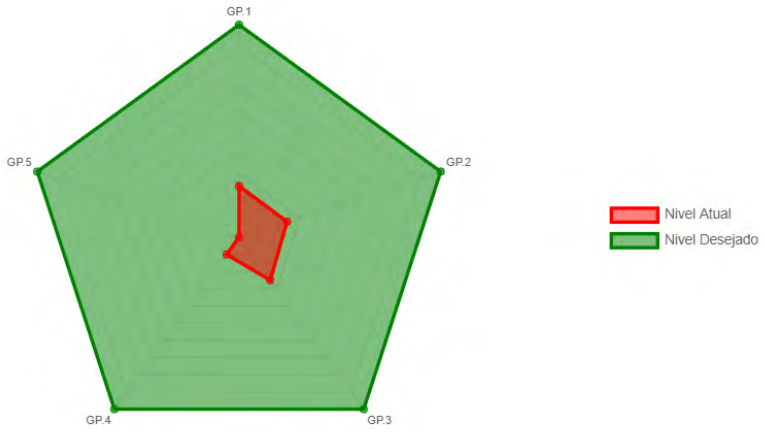


Figura 09: Nível de Maturidade de Segurança Cibernética – Gráfico Radar.
Fonte: Brasiliano INTERISK

O gráfico Radar é mais lúdico, e faz com que a alta gestão fique mais consciente da necessidade de investimento e onde, e o que investir.

O Risk Assessment é parte da Metodologia Cybersecurity Risks, que ao ser completada, passa a ser uma ferramenta de extrema utilidade, pois faz com que a empresa enxergue quais são seus cenários de ataques cibernéticos, com a descrição de como pode ser agredida, com qual perfil de hackers, tendo em vista seu negócio e o modus operandi.

Com estas informações, temos condições de realizar investimentos pontuais, otimizando recursos e tendo uma relação custo benefício muito mais equilibrada.

Por exemplo, o ransomware foi um fator constante de ameaça. As organizações globais também foram sobrecarregadas por um aumento significativo nas vulnerabilidades recém-divulgadas.

Com a pandemia, ainda em estado de alerta e as empresas mantendo o Home Office e empresas retornando a CyberSecurity Risks passa a ser uma ferramenta de análise estratégica para focar e otimizar os investimentos, fechando as vulnerabilidades existentes no seu sistema de proteção.

POLÍTICA DE SEGURANÇA

Professor Dr. Nino Meireles,CPSI,CIGR,CIEIE
Diretor de Formação e Extensão Universitária CEAS-BRASIL

A política é composta por um conjunto de regras e padrões sobre o que deve ser feito para assegurar que os ativos e os serviços importantes para a empresa recebam a proteção conveniente, potencializando o alcance das metas. Além disso, define o conjunto de normas, procedimentos e métodos utilizados para a manutenção da segurança, devendo ser formalizada e divulgada a todos os colaboradores; deve levar em conta o perfil da empresa e os negócios.

A construção apresenta quatro etapas. A primeira etapa é o levantamento, sendo composto por: obtenção dos padrões, normas e procedimentos de segurança já existentes; entendimento das necessidades e uso de recursos nos processos de negócio; obtenção de informações sobre o ambiente interno e externo. A segunda etapa é o desenvolvimento do conteúdo e normas. É composta por: gerenciamento da política (definição da segurança da empresa, objetivo do gerenciamento, fatores críticos de sucesso, gerenciamento da versão e manutenção da política e referência para outras políticas, padrões e procedimentos); atribuição de regras e responsabilidades e procedimentos de segurança. A penúltima etapa é o procedimento e revisão, nesta etapa deve-se fazer pesquisas sobre as melhores práticas em segurança utilizadas no mercado; desenvolvimento de procedimentos e formalização dos procedimentos para integrá-los às políticas da empresa. A última etapa é a aprovação e implantação, composta de: revisão e aprovação da política, normas e procedimentos; implantação com a utilização do endomarketing.

COMPONENTES

Especificação - Deve ser breve, utilizar palavras simples e formalizar o que é esperado dos colaboradores. Deve fornecer aos leitores informações suficientes para saber se os procedimentos descritos são aplicáveis a eles ou não. Deve descrever sua finalidade específica, por exemplo, se é orientada a pessoas, setores, áreas etc.

Declaração da alta administração - É muito importante, pois atesta a divulgação e exige sua utilização. Logo, demonstra aos colaboradores que a alta administração está de acordo com a política.

Autores - Os nomes dos profissionais que desenvolveram a política devem estar especificados para que qualquer dúvida de interpretação ou sugestões de mudanças possam ser enviadas.

Referências – É comum que as políticas façam referências a outros documentos existentes ou em desenvolvimento.

Procedimento para requisição de exceções - É importante não descrever sob quais condições as exceções serão concedidas, mas apenas definir os procedimentos de solicitação.

Procedimentos para mudanças - Definir os responsáveis para o controle e atualização da política, pois ela não é estática.

Datas - A política deve possuir a assinatura da alta administração aprovando-a, a data da última atualização e do inicio de sua vigência

PONTOS CRÍTICOS

Formalização dos processos e instruções de trabalho. Utilização de tecnologias capazes de prover segurança. Atribuição de responsabilidades e das respectivas punições. Treinamento e conscientização constantes.

CARACTERÍSTICAS

Verdadeira - Exprimir o pensamento da empresa e ser coerente com as ações da organização. Ela deve ser possível de ser cumprida.

Disponibilidade de recursos - Liberação de recursos financeiros e de pessoas para que as diretrizes descritas possam ser implementadas.

Válida para todos - A política deve ser cumprida por todos na empresa, desde o presidente até os colaboradores do nível operacional.

Simples - Ser de fácil leitura e compreensão, logo a linguagem deve ser simples e direta, evitando-se termos técnicos de difícil compreensão.

Comprometimento da alta administração - Deve ser assinada pela alta administração, pois desta forma fica claro o apoio à política.

BENEFÍCIOS

Curto prazo: formalizar e documentar os procedimentos de segurança; implementar novos procedimentos e controles; prevenir acesso não autorizado, danos ou interferência no andamento da atividade fim e maior segurança nos processos.

Médio prazo: padronizar os procedimentos de segurança incorporados à rotina da empresa; adaptar de forma segura novos processos; qualificar e quantificar os sistemas de resposta e ter conformidade com padrões de segurança.

Longo prazo: retorno do investimento realizado, por meio da minimização da incidência de problemas relacionados à segurança e consolidar a imagem associada à segurança.

PUBLICAÇÃO, DIVULGAÇÃO E TREINAMENTO

Para que a cultura da empresa seja mudada em relação ao tema segurança é essencial que os colaboradores estejam preparados através de ações de endomarketing. Quando a organização investe na conscientização, ela aumenta a probabilidade de sucesso do processo de implementação da política. Todos os colaboradores, terceiros e prestadores de serviço devem ser treinados e sofrer atualização regular sobre a política de segurança. Para que o programa de conscientização seja eficaz é necessário: planejar, implementar, manter e avaliar periodicamente.

O programa apresenta três fases.

- Primeira fase - Identificação do escopo. O escopo deve contemplar o treinamento de todos colaboradores.
- Segunda fase - Identificação dos instrutores.
- Terceira fase - Identificação do público-alvo, pois nem todos os colaboradores necessitam do mesmo tipo de treinamento.

MANUTENÇÃO

O intervalo médio para a revisão da política é de seis meses a um ano, mas deve ser realizada uma revisão sempre que forem identificados fatos novos, não previstos na versão atual que possam ter impacto no sistema de segurança da empresa. O processo de revisão deve abranger:

- Eventuais riscos identificados.
- Alterações na legislação do negócio.
- Incidentes de segurança.
- Vulnerabilidades encontradas.
- Alterações na estrutura organizacional e mercado.

OS DESAFIOS DA PRESTAÇÃO DO SERVIÇO DE SEGURANÇA

Professor Dr. Nino Meireles,CPSI,CIGR,CIEIE
Diretor de Formação e Extensão Universitária CEAS-BRASIL

Vários são os desafios a serem enfrentados pelas empresas prestadoras de serviço de segurança no nosso País. Desafios estes, que estão nos ambientes interno e externo. Para analisarmos o ambiente externo iremos utilizar como referência as cinco forças de Michael Porter (ameaça de novos entrantes, poder de barganha dos fornecedores, poder de barganha dos clientes, produtos substitutos e concorrência).

A empresa que presta serviço de segurança faz parte de um setor de negócio, no qual surgem constantemente novas organizações (novos entrantes). Estas novas empresas trazem ameaças às empresas existentes, por trazerem capacidade de produção adicional.

Em relação aos fornecedores não podemos esquecer que para o desenvolvimento da atividade de segurança privada é necessário, muitas vezes, a aquisição de produtos controlados (armamento letal e não letal, munição e colete balístico). Esses fornecedores passam a ser poderosos, pois não existem produtos substitutos e constituem um pequeno número de grandes empresas fornecedoras altamente concentradas.

Os clientes também têm poder, pois a prestação de serviço não apresenta muita diferenciação, aja vista ser uma atividade bastante regulamentada. Além

deste aspecto, temos o problema das prestações de serviço ilegais (empresas clandestinas) e a falta de cultura de segurança na maioria das organizações. Esta falta de cultura faz com que o preço seja o principal ponto a ser levado em consideração pela empresa cliente.

Ainda em relação aos clientes outro ponto importante é a relação expectativa e percepção. Existem três situações possíveis: percepção menor que a expectativa; percepção igual a expectativa; percepção maior que a expectativa. Na primeira relação teremos um cliente insatisfeito, pois ele esperava mais do que recebeu na prestação do serviço. Na relação de igualdade, o cliente recebe do prestador o que ele esperava, temos uma situação de normalidade. Na terceira relação teremos a condição de cliente encantado, pois o cliente recebeu mais do que ele esperava da prestação de serviço. Esta é a condição que deve ser buscada por toda empresa prestadora de serviço, pois o cliente encantado não tem o interesse de trocar o parceiro.

Para enfrentar o desafio da relação expectativa e percepção as empresas prestadoras de serviço deveriam utilizar o Modelo dos Cinco Gaps (Parasuraman), pois torna mais fácil a compreensão das causas geradoras da distância entre a expectativa e a percepção do cliente.

Produtos substitutos (serviços substitutos) são os diferentes bens ou serviços que vêm de fora do setor e que desempenham as mesmas funções de um produto do setor, ou seja, estamos falando da atividade clandestina e da vertente dos agentes de portaria. Eles representam uma ameaça em virtude dos preços competirem entre si. A disponibilidade de novos serviços leva os consumidores a fazerem comparações de qualidade, performance e preço.

A concorrência é sem dúvida alguma a mais poderosa das cinco forças. Esta força é influenciada por concorrentes numerosos. As principais armas são: preço, qualidade, performance dos itens oferecidos, serviço ao consumidor, garantias, propaganda e promoções especiais e inovação de produtos.

Além das forças de Porter é importante a compreensão, por parte das empresas prestadoras de serviço de segurança, das características da prestação de serviço: intangibilidade, inseparabilidade, variabilidade, perecibilidade e heterogeneidade. Características importantes, mas muitas vezes negligenciadas e quando negligenciadas, interferem negativamente na prestação de serviço. Além destas características outro ponto importante do ambiente externo é a análise criteriosa do mercado de recursos humanos (vigilante, gestor operacional, gestor tático).

Em relação ao ambiente interno os principais desafios são: visão sistêmica, visão de negócio, gestão com base em diretrizes. A não percepção de empresa como um sistema aberto leva à concepção equivocada de que o sucesso de um setor leva necessariamente ao sucesso empresarial. A sinergia entre os departamentos é muito importante.

Outro desafio é a definição de qual é o negócio da empresa que presta serviço de segurança. Deveria ser desenvolver soluções de segurança e não vender homens e ou equipamentos. A visão restrita de negócio interfere no resultado empresarial. O último desafio é o modelo de gestão. A falta de se fazer gestão com base em metas, sem indicadores, interfere negativamente no sucesso empresarial.

Podemos afirmar que os desafios estão nos ambientes interno e externo. A compreensão deles é essencial para que as empresas tenham sucesso e enfrentem o processo de entropia.

Sucesso!!!!!

INTELIGÊNCIA EM RISCOS: INTERCONECTIVIDADE VERSUS MOTRICIDADE EM RISCOS

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.

Um dos maiores problemas identificados na área de Gestão de Riscos Corporativos é a não identificação do Risco Sistêmico. Você sabe o que é?

Pois bem, O risco sistêmico é o risco responsável por "colapsar um sistema inteiro, oposto de colapso de partes e componentes individuais". Os riscos sistêmicos são caracterizados por:

- Pontos de ruptura modestos, combinando indiretamente para produzir grandes falhas;
- Contágio ou compartilhamento de risco, como uma perda que desencadeia uma reação de outras;
- Sistemas sendo incapazes de recuperar o equilíbrio depois de um choque.

Isto quer dizer que são riscos que na grande maioria, não possuem criticidade alta (resultado da probabilidade x impacto – posição na Matriz de Criticidade), mas possuem grande influência sobre os outros riscos considerados críticos.

Na realidade o gestor não enxerga o risco sistêmico porque só elabora a Matriz de Criticidade dos Riscos e com somente esta Matriz fica com uma visão míope no tratamento e na priorização.

Na área de gestão de riscos não é comum a prática de utilizar ferramentas para que os gestores possam enxergar de maneira prática e fácil os riscos sistêmicos. Por esta razão falta a visão de antecipação.

No ano de 2020 ficou evidenciado a falta de percepção dos governantes e das áreas de inteligência, a antecipação da pandemia do COVID-19. A maior evidência é o Relatório de Riscos Globais, publicado pelo Fórum Mundial, na sua 15a edição, onde na sua prospectiva conseguiram identificar a possibilidade de materialização de Doenças Infecciosas. Vejam as tabelas abaixo:

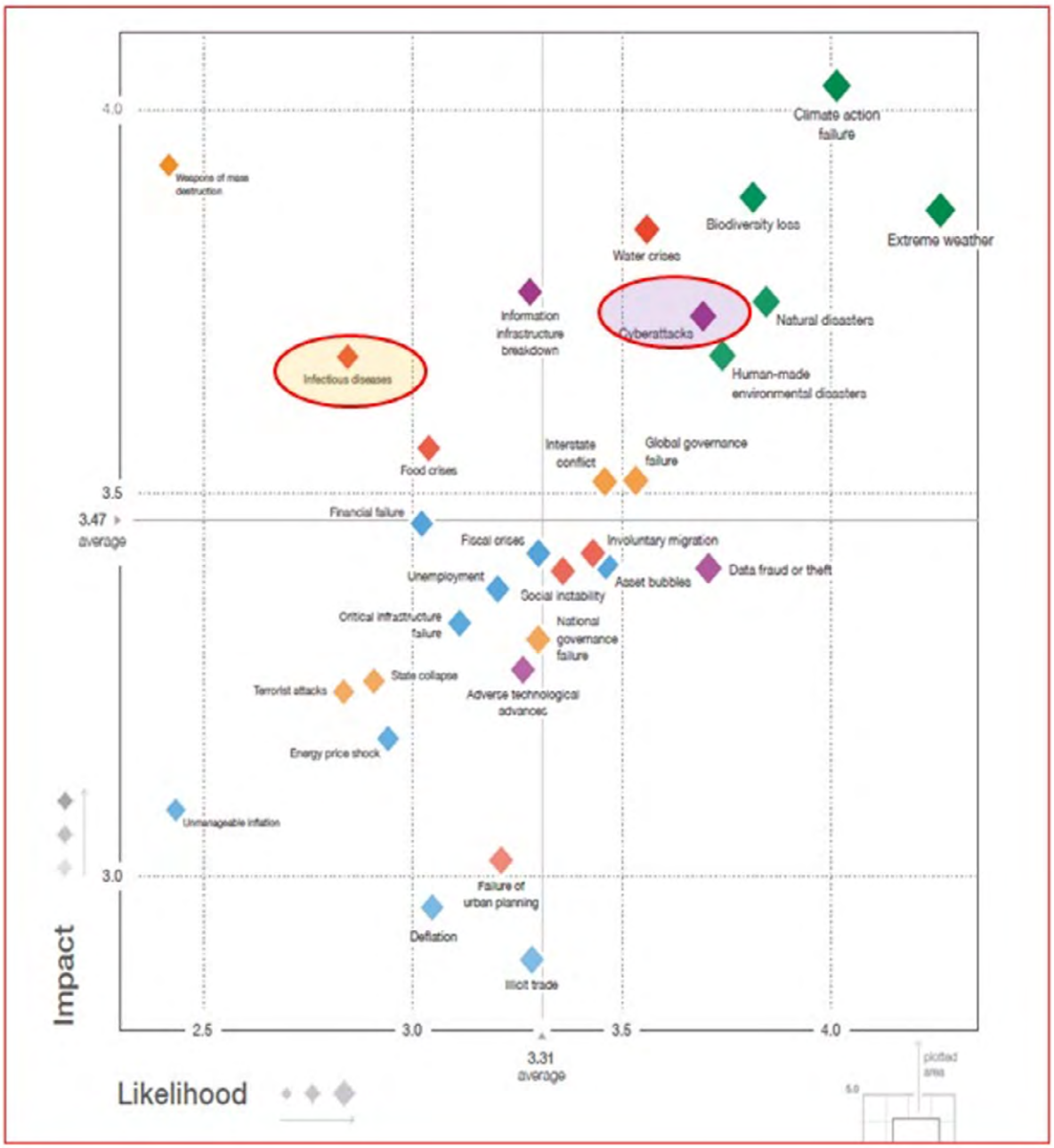


Figura 1: Matriz de Criticidade dos riscos globais.
Fonte: 15ª Relatório de Riscos Globais do Fórum Mundial 2020

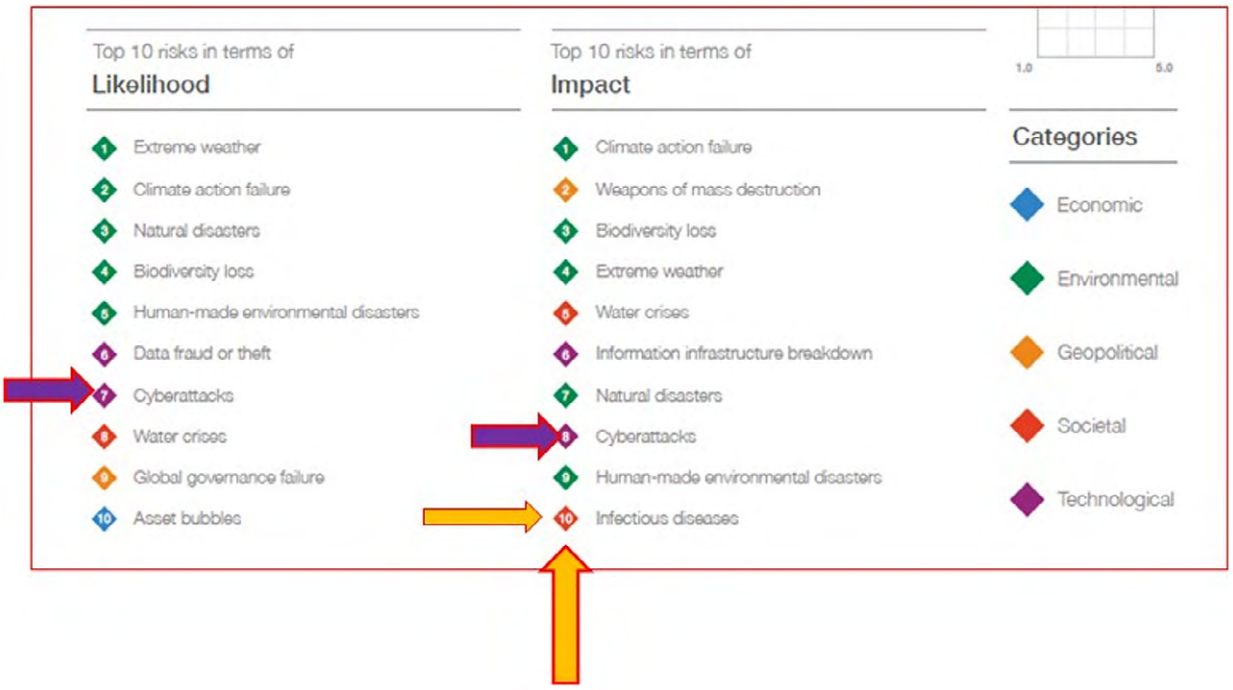


Figura 2: Criticidade dos riscos globais.
Fonte: 15ª Relatório de Riscos Globais do Fórum Mundial 2020

Vejam que em termos de criticidade de riscos, probabilidade versus impacto, o fórum mundial conseguiu acertar no alvo em termos de pandemia e de aumento exponencial de ataques cibernéticos.

Agora vendo o gráfico abaixo, identificamos claramente, pelo tamanho das setas a motricidade dos riscos, onde a pandemia é muito forte, pois gera impactos de todas as naturezas. O que isto significa? Que se não for tratada prioritariamente, continuará causando impactos cada vez maiores.

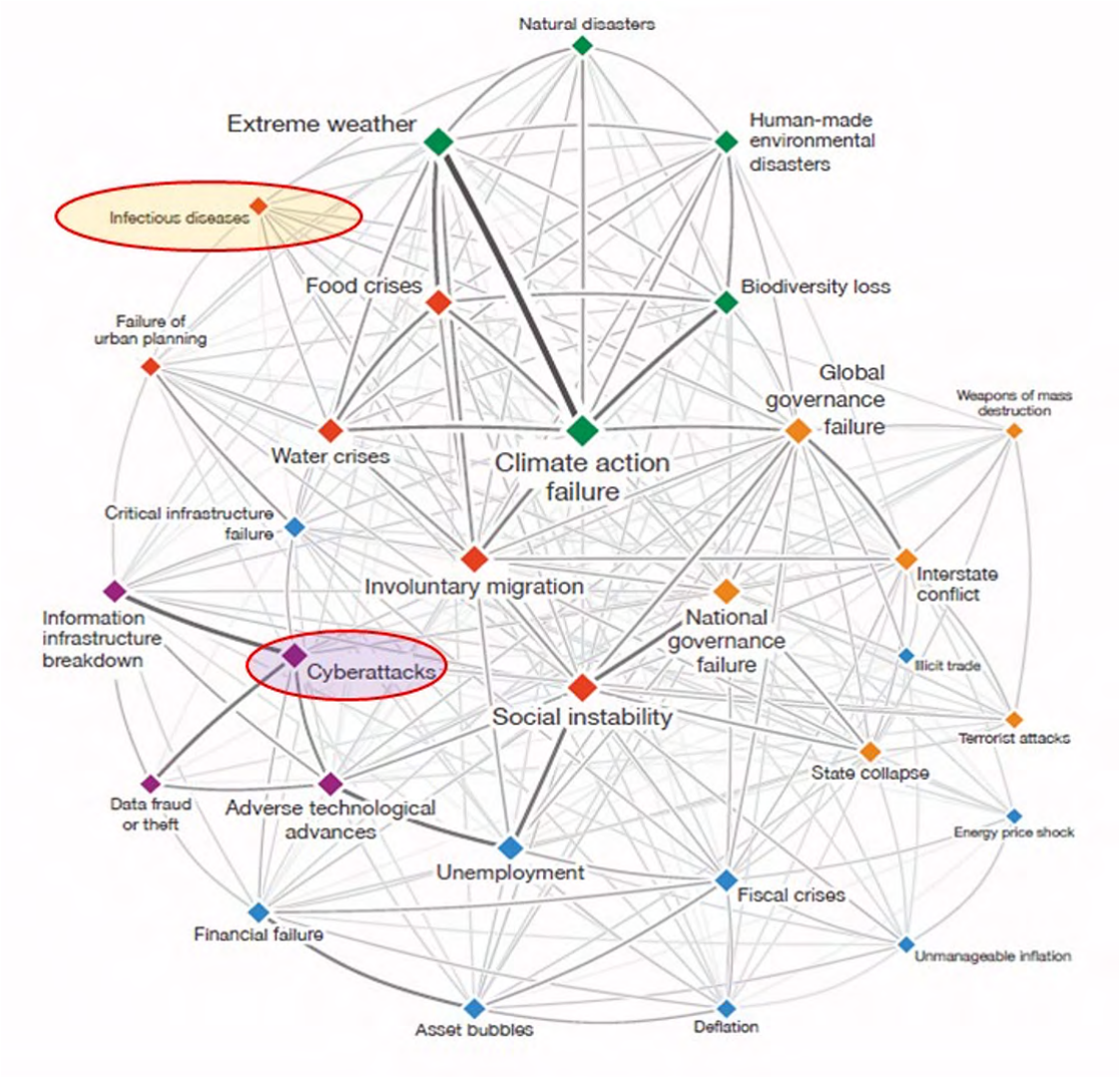


Figura 3: Interconectividade entre os riscos globais
Fonte: 15ª Relatório de Riscos Globais do Fórum Mundial 2020

O fórum mundial utiliza um método subjetivo para elaborar a interconectividade, baseada nas opiniões de especialistas. Tipo método de Delphi.

Nós da Brasiliano INTERISK utilizamos no nosso sistema a aplicação do Teorema de Bayes, probabilidades condicionantes. Pegamos esta técnica, desenvolvida pelo cenarista francês Michael Godet, onde utiliza a Matriz de Impactos Cruzados como base para elaborar a Matriz de Interconectividade e daí ter a característica do risco. Se ele é Motriz, Ligação, Dependente ou Independente.

A Brasiliano INTERISK ainda inovou, cruzando as Matrizes de Criticidade (probabilidade x impacto) e a de Interconectividade, gerando automaticamente no nosso sistema INTERISK uma Matriz de Priorização.

O INTERISK é o único software de gestão de riscos que possui esta técnica. Portanto de modo prático e automático o gestor passa a enxergar quais são suas reais prioridades.

Abaixo vou escrever um caso prático para que o leitor tenha uma clara noção da aplicação da Interconectividade.

Olhando a Matriz de Criticidade abaixo, vemos o Risco 91 plotado no quadrante amarelo, portanto é um risco que está em uma área de monitoramento, não exigindo plano de ação. Correto? Não! Vejamos.

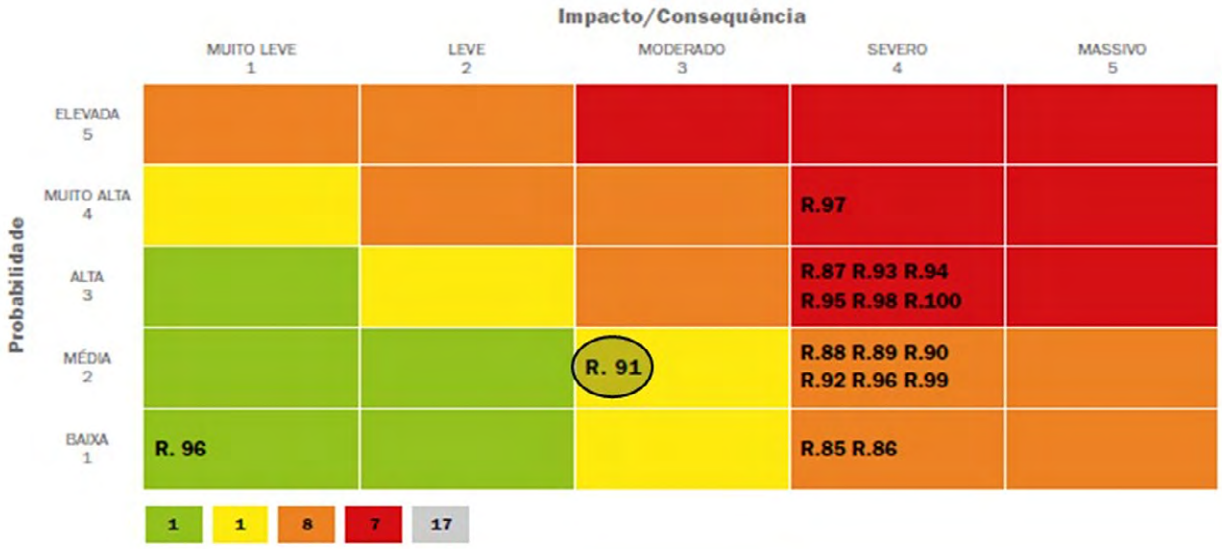


Figura 4: Matriz de Criticidade – Probabilidade x Impacto.
Fonte: Software INTERISK – Estudo de Caso

Este risco pode ser motriz, ou seja, tem características de influenciar outros riscos a se materializarem. Como podemos saber disso?

Temos que aplicar a técnica dos Impactos Cruzados, com base no Teorema de Bayes – Probabilidades Condicionantes, para identificar os motrizes e os dependentes. Os Impactos Cruzados identificam os riscos que possuem forte conectividade com os outros, podendo ser motrizes ou dependentes.

Quem pede para utilizar esta técnica junto com a Matriz de Criticidade? O fórum mundial, em Davos, que publica o Global Risk Report, sugere a aplicação das duas matrizes pela área de riscos, visando obter a visão do risco sistêmico. O antigo COSO ERM de 2004, já descrevia a necessidade de realizar a interdependência entre riscos e fatores de riscos. Portanto diante da dinamicidade do Mundo VUCA – Volátil, Incerto, Complexo e Ambíguo, e agora também o mundo BANI (ver artigo nesta edição), o gestor de riscos das empresas podem utilizar esta técnica para obter a visão de antecipação.

Começamos em montar a Matriz de Impactos Cruzados - MIC ente riscos, conforme modelo abaixo:

Fatores	X1	X4	X5	X6	X7	X8	X10	X11	X13	X14	X15	X16	X17	X20	D
X1	Xx	2	3	3	0	0	0	3	1	1	0	0	1	0	14
X4	0	Xx	0	0	0	0	0	3	0	0	0	0	0	0	3
X5	3	2	Xx	3	2	1	0	3	3	3	2	2	3	2	29
X6	3	2	3	Xx	2	2	0	3	1	3	0	0	3	0	22
X7	0	1	2	2	Xx	3	3	3	3	3	3	3	3	3	32
X8	0	1	2	2	3	Xx	3	3	3	3	3	3	3	3	32
X10	0	1	1	1	3	3	Xx	3	2	3	3	3	0	3	26
X11	2	1	1	1	3	3	2	Xx	3	2	3	3	3	3	30
X13	2	1	2	2	3	3	3	3	Xx	2	3	3	0	3	30
X14	3	2	3	3	3	3	3	3	3	Xx	3	3	0	3	35
X15	2	2	3	3	3	3	3	3	3	3	Xx	3	2	3	36
X16	3	2	3	3	3	3	3	3	3	3	3	Xx	2	3	37
X17	0	3	2	2	2	3	1	3	1	2	3	3	Xx	3	28
X20	2	2	3	3	3	3	3	3	3	3	3	3	2	Xx	36
M	20	22	28	28	30	30	24	39	29	31	29	29	22	29	Xx

Legenda:
1. Baixo Nível de Escolaridade
4. Elevada carga tributária
5. Desigualdade social
6. Exclusão social
7. Corrupção policial
8. Corrupção no Judiciário
10. Inteligência Policial
11. Legislação Brasileira
13. Sistema Carcerário
14. Violência Urbana
15. Facções Criminosas estruturação do crime como empresa
16. Facções Criminosas: assistencialismo
17. Valores éticos e morais nas empresas
20. Estruturação das milícias em função da inoperância do Estado.

Figura 5: Matriz de Impactos Cruzados. Fonte: Software INTERISK – Estudo de Caso

A MIC, construída através de eixos na horizontal e vertical, com os riscos que serão estudados. A entrada das informações sempre é pelo eixo vertical e perguntamos qual o nível de influência (métrica 0, 1, 2 e 3) em os outros riscos se materializarem ou não materializarem. Ou seja, queremos saber o nível de influência que cada risco possui, tanto faz para os outros riscos materializarem ou não materializarem. Queremos identificar a Motricidade do Risco. E fazemos isso com todos os riscos ente eles.

O resultado na vertical é a Motricidade e na Horizontal é a dependência.

Para montar a Matriz de Motricidade dos Riscos, que possui quatro quadrantes, utilizamos no eixo da Motricidade o mais alto e o mais baixo, divide por dois temos o eixo central da Motricidade. No eixo da Dependência aplicamos a mesma técnica.

$$PM = \frac{VM + vM}{2}$$

PM = Ponto Médio da Motricidade
VM = Valor mais alto de motricidade
vM = Valor mais baixo da motricidade

$$PD = \frac{VD + vD}{2}$$

PD = Ponto Médio da Dependência
VD = Valor mais alto da dependência
vD = Valor mais baixo da dependência

Figura 6: Pontos Médios dos eixos de Motricidade e Dependência.
Fonte: Software INTERISK – Estudo de Caso

Com isso Montamos a Matriz de Motricidade com quatro quadrantes, conforme abaixo:

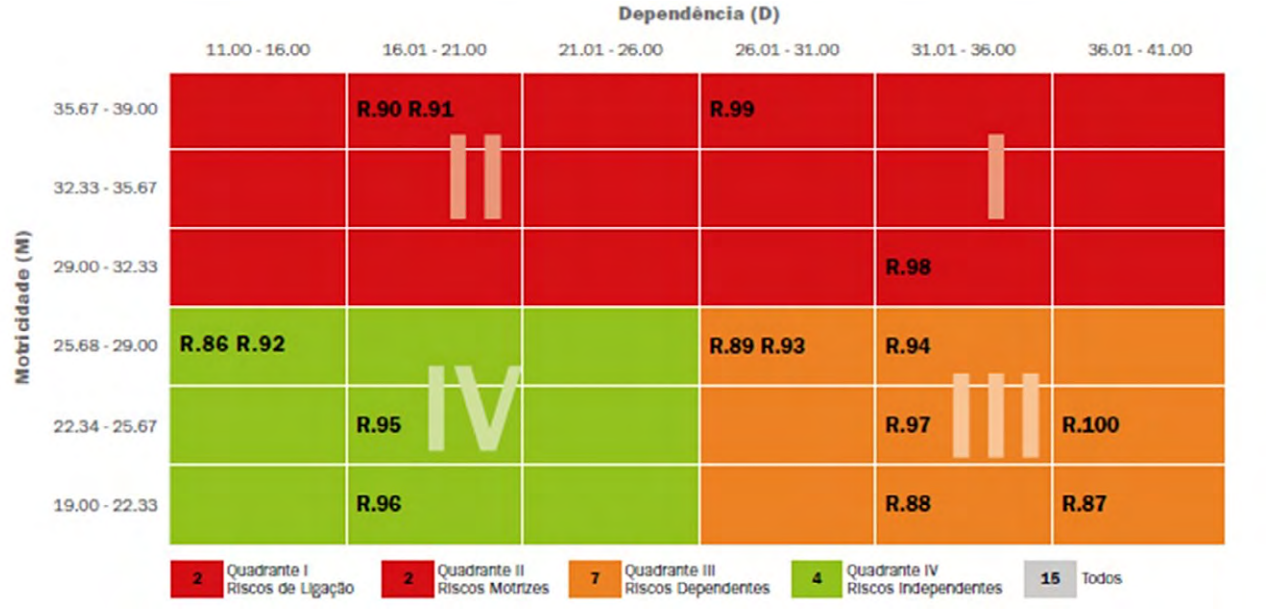


Figura 7: Matriz de Motricidade com 4 quadrantes. Fonte: Software INTERISK – Estudo de Caso

A interpretação dos Quadrantes são:

> I – Ligação – Significa que os riscos são dependentes e motrizes ao mesmo tempo, influenciam e são influenciados entre si. O contexto destes riscos é de instabilidade, mas influenciam o quadrante III, onde estão os riscos dependentes;
>
> II – Motriz – Significa que os riscos são motrizes, ou seja, aqueles que influenciam nos riscos localizados no quadrante I e III. Estes são os riscos sistêmicos. Podem até não serem críticos, mas são estratégicos;
>
> III- Dependentes – Significa que estes riscos para serem materializados ou não, dependem dos riscos plotados nos quadrantes I e II. Não adianta tratar estes riscos como prioridade, mesmo que sejam críticos. Pois a fonte geradora destes riscos se não for tratada continuará influenciando-os. Portanto os riscos nos quadrantes I e II são prioritários;
>
> IV – Independentes – Significa que estes riscos não possuem conectividade com nenhum risco. Posso denominá-los de “zangados”, pois não querem comunicação com nenhum risco. Não quer dizer que não são críticos, mas o tratamento, se for um risco críticos, será estanque.

Vendo a Matriz de Motricidade acima, vemos que o Risco 91, que possui uma criticidade média, quadrante amarelo, mas está plotado no quadrante II, então é um risco com alta motricidade. Este risco, embora sem criticidade, é um influenciador entre os riscos. Vejam que interessante, pois se só praticamos a Matriz de

Criticidade, teríamos outra visão, outra decisão tomada, em quais riscos investir e com quais recursos.

O Software INTERISK, único do mercado que possui a Matriz de Priorização, fruto do cruzamento das Matrizes de Criticidade x Motricidade, fornece aos gestores, de forma automatizada, a priorização para tratamento dos riscos. Esta Matriz leva em consideração tanto a motricidade como a criticidade.

O fruto é a Matriz de priorização, 4 x 4. No eixo horizontal inserimos os quadrantes da Matriz de Motricidade e no eixo vertical os quadrantes da Matriz de Criticidade.

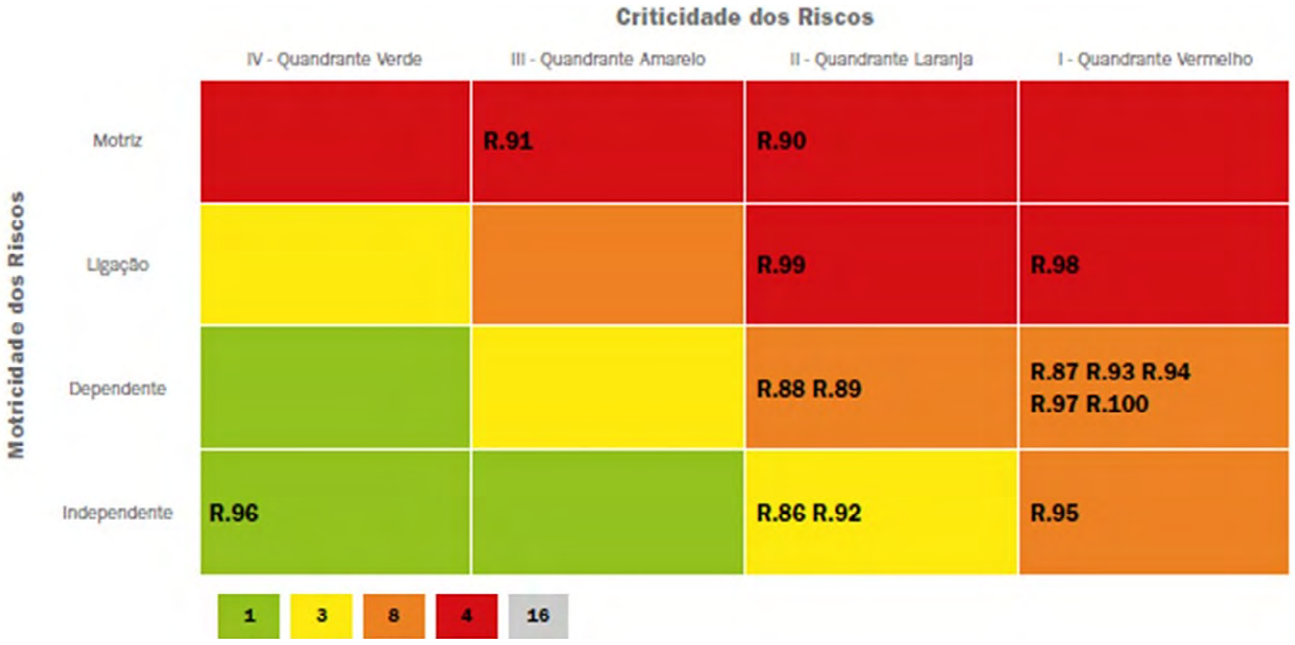


Figura 8: Matriz de Priorização. Fonte: Software INTERISK – Estudo de Caso

A “pintura” da Matriz de priorização deve seguir uma lógica integrando a motricidade e criticidade. Todos os riscos motrizes são prioritários independente de sua criticidade. Já os de ligação, devemos focar nos críticos do quadrante laranja e vermelho. Os riscos dependentes e os de ligação de criticidade média, possuem uma priorização secundária. Todos os riscos dependentes com criticidade muito alta e alta, quadrante vermelho e laranja da criticidade, possuem uma priorização secundária. Os riscos independentes com criticidade muito alta (quadrante vermelho) possuem uma priorização secundária. Priorização terciária serão os independentes com criticidade laranja, os dependentes com criticidade amarela e os de ligação com criticidade verde. Os riscos que se encontram nos quadrantes verdes da priorização é puro monitoramento.

A Matriz de Priorização é estratégica, fornece aos gestores uma outra visão, sabendo onde alocar melhor os recursos. A matriz de Priorização ressalta os riscos sistêmicos, como o Risco 91, que está no quadrante vermelho para ser tratado. Outra vantagem é que otimiza recursos, pois neste caso o gestor de riscos só terá que elaborar planos

de ações para quatro riscos. Se o gestor de riscos fosse tratar um risco que esteja no quadrante laranja antes do vermelho, irá “enxugar gelo”, pois não conseguirá anular a causa raiz. A fonte geradora.

Por esta razão a importância do emprego da técnica da Interconectividade, fato que no Brasil é muito pouco utilizada.

O Software INTERISK, com a ferramenta da Motricidade x Criticidade fornece Inteligência em Riscos, o que agrega valor para os negócios da empresa, favorecendo sua competitividade. Com a Inteligência em Riscos os gestores, juntos com a alta gestão, terão a visão da antecipação, o que por si só diferencia em termos de ser resiliente e se for o caso antifrágil.

GLOBAL RISK REPORT 2021 RESSALTA RISCOS CIBERNÉTICOS E SOCIAIS COMO CRÍTICOS PARA HORIZONTE DE DOIS ANOS. A SUA EMPRESA ESTÁ PREPARADA?

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.

O custo humano e econômico imediato do Covid-19 é severo. Ele ameaça reduzir anos de progresso ao reduzir a pobreza e a desigualdade e ao enfraquecer ainda mais a coesão social e a cooperação global. As perdas de emprego, uma crescente divisão digital, as interações sociais rompidas e as mudanças abruptas nos mercados podem levar a consequências massivas e a oportunidades perdidas para grandes partes da população global. As ramificações – na forma da agitação social, fragmentação política e das tensões geopolíticas – moldarão a efetividade das respostas dos países a outras ameaças vitais da próxima década: os ciberataques, as armas de destruição em massa e, mais notavelmente, a mudança climática.

Estas são algumas conclusões que o Global Risk Report - GRR, 6a edição, publicado em janeiro de 2021, pelo Fórum Mundial, que fez sua pesquisa anual. Este ano, o GRR inovou ao inserir horizontes temporais para os riscos identificados, que fornece com isso a oportunidade de saber o nível de rapidez que as empresas e países devem reagir, tomando medidas preventivas e mitigatórias.

PERCEPÇÕES DOS RISCOS GLOBAIS

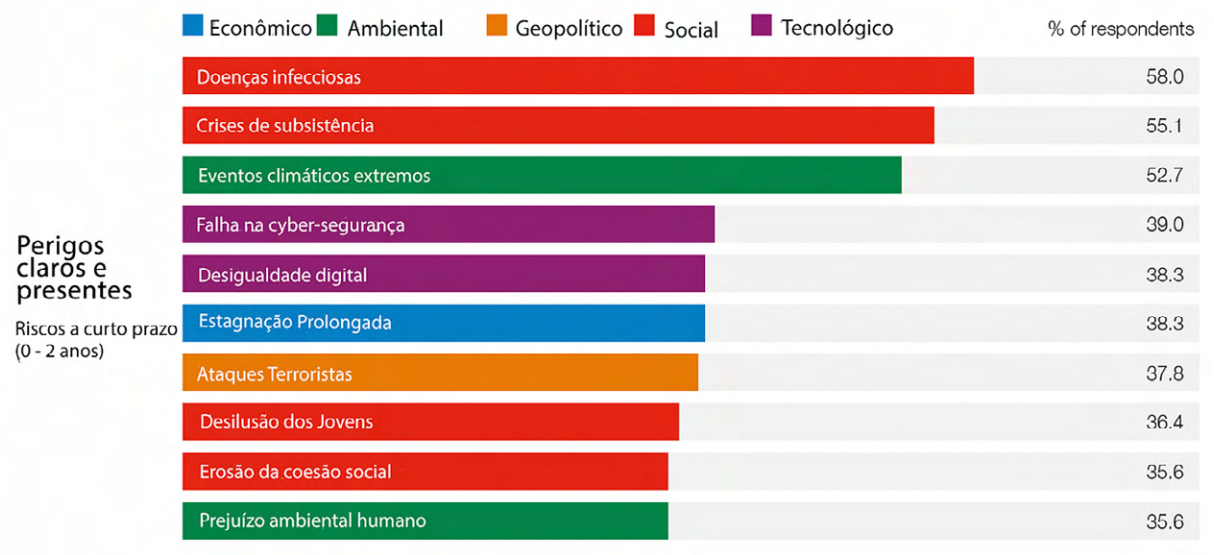
Entre os riscos de maior probabilidade dos próximos anos, estão o clima extremo, a falha na ação climática e o prejuízo ambiental movido pelo homem, assim como a concentração do poder digital, a desigualdade digital e a falha na cibersegurança.

Entre os riscos de maior impacto da próxima década, as doenças infecciosas estão em

primeiro lugar, seguidas pela falha na ação climática e outros riscos ambientais. Junto com eles estão as armas de destruição em massa, crises de subsistência e de dívida, além da quebra de infraestrutura na área de Tecnologia de Informação (TI).

Notamos que os riscos ligados à tecnologia estão em alta juntamente com os ambientais, sociais e econômicos. Eles reunidos fazem um ótimo caldeirão prestes a explodir, se as nações não fizeram suas lições de casa. Parece que negamos materialização desses riscos, o que é muito ruim para os países em desenvolvimento.

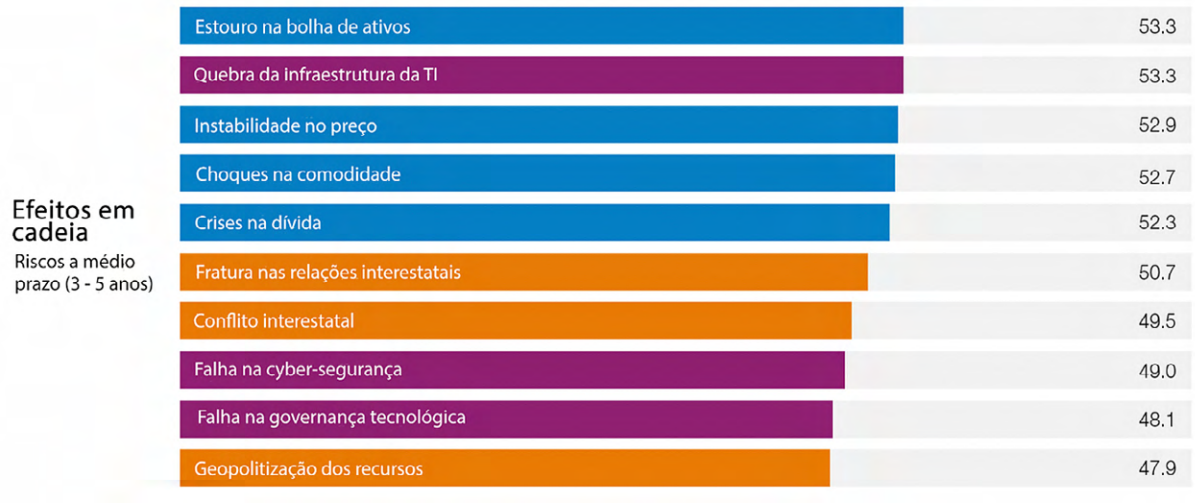
Quando analisamos o tempo dentro do qual esses riscos se tornarão uma ameaça crítica ao mundo, os sinais ficam ainda mais iminentes. Aqueles mais prováveis nos próximos dois anos incluem: crises de emprego e do meio de vida, desilusão generalizada dos jovens, desigualdade digital, estagnação econômica, prejuízo ambiental provocado pelo homem, erosão da coesão social e ataques terroristas.



Quadro 1: Global Risk Report, 16ª edição, 2021

Observamos acima que temos quatro riscos sociais, dois de tecnologia, um de geopolítica, um econômico e um de meio ambiente. Todos os nove possuem um impacto massivo no mundo dentro de curto prazo. Isso quer dizer que se os países não realizarem uma cooperação, teremos graves problemas a enfrentar. Cenários prospectivos devem ser elaborados para identificar seus fatores de riscos e saber quais são motrizes para poder operacionalizar medidas de prevenção e contenção.

Os riscos econômicos caracterizam proeminentemente no prazo de três a cinco anos, incluindo as bolhas de ativos, instabilidade do preço, choques na comodidade e crises da dívida. Tudo isso seguido por riscos geopolíticos, incluindo as relações e os conflitos interestatais e a geopolitização dos recursos.



Quadro 2: Global Risk Report, 16ª edição, 2021

A preocupação a médio prazo é o contexto econômico, integrado com o tecnológico que tem como consequência os geopolíticos. Como o próprio quadro descreve, é um efeito em cadeia.

No horizonte de cinco a dez anos, os riscos ambientais, como a perda de biodiversidade, as crises dos recursos naturais e a falha da ação climática, dominam junto com as armas de destruição em massa, efeitos adversos da tecnologia e o colapso dos estados ou as instituições multilaterais.

Quadro 3: fonte Global Risk Report, 16ª edição, 2021

Ameaças existenciais são aquelas denominadas de «transgeracionais» (afetando todas as gerações futuras) em escopo e «terminais» em intensidade são classificados como riscos existenciais. Embora um risco catastrófico global possa matar a grande maioria da vida na Terra, a humanidade ainda pode se recuperar potencialmente. Portanto, nossa situação pode ser considerada como grave. Temos três riscos

geopolíticos, dois de meio ambiente, dois sociais e um tecnológico. Os geopolíticos no meu ponto de vista são os motrizes para influenciar os demais.

FRAGILIDADE ECONÔMICA E DIVISÕES SOCIAIS ESTÃO CONFIGURADOS PARA AUMENTAR

As disparidades constituintes na saúde, educação, estabilidade financeira e tecnologia levou a crise a impactar desproporcionalmente certos grupos e países. Não apenas a Covid-19 provocou mais de 2.403.462 de óbitos, dia 14 de fevereiro, mas os impactos econômicos e de longo prazo continuarão a ter consequências devastadoras. O choque econômico da pandemia – horas de trabalho equivalentes a 495 milhões de empregos foram perdidos apenas no segundo trimestre de 2020. Tais fatos aumentam imediatamente a desigualdade, mas também geram uma recuperação desigual. Apenas 28 economias esperam ter crescido em 2020. A pesquisa do GRR 2021, com percentual de 60% dos entrevistados identificaram as “doenças infecciosas” e as “crises de subsistência” como as principais ameaças de curto prazo ao mundo. A perda de vidas e da subsistência aumentarão o risco da “erosão da coesão social”, também uma ameaça crítica de curto prazo.

AS CRESCENTES DIVISÕES DIGITAIS E A ADOÇÃO DA TECNOLOGIA REPRESENTAM PREOCUPAÇÕES

A Covid-19 acelerou a Quarta Revolução Industrial, expandindo a digitalização da interação humana com o e-commerce, educação online e trabalho remoto. Essas mudanças transformarão a sociedade bem depois da pandemia e prometem enormes benefícios. A habilidade para o teletrabalho e o rápido desenvolvimento das vacinas são dois exemplos, mas as alterações também arriscam exacerbar e criar desigualdades. As pesquisas do GRR 2021 classificaram a “desigualdade digital” como uma ameaça crítica de curto prazo.

Uma lacuna digital cada vez maior pode piorar as fraturas sociais e minar inclusive os prospectos de uma recuperação. O progresso na direção da inclusão digital é ameaçado pela crescente dependência digital, a automação rapidamente acelerada, manipulação, as lacunas no regulamento da tecnologia e as lacunas nas perícias e capacidades de tecnologia.

UMA GERAÇÃO DUPLAMENTE PERTURBADA DE JOVENS ESTÁ EMERGINDO NUMA ERA DE OPORTUNIDADES PERDIDAS

Embora o salto digital para adiante tenha desbloqueado oportunidades para alguns jovens, muitos agora estão entrando na força de trabalho sob uma era de gelo do

emprego. Jovens adultos ao redor do mundo estão vivenciando a segunda maior crise global em uma década. Já expostos à degradação ambiental, consequências da crise financeira, desigualdade crescente e da ruptura da transformação industrial, essa geração enfrenta sérios desafios relacionados à educação, o que impacta nos prospectos econômicos e na saúde mental.

De acordo com as pesquisas do GRR, 2021, o risco da "desilusão dos jovens" está sendo amplamente negligenciado pela comunidade global, mas ele se tornará uma ameaça crítica ao mundo a curto prazo. Os ganhos sociais a duras penas podem ser anulados se a geração atual perder oportunidades futuras e a fé nas instituições políticas e econômicas de hoje.

Movimentos de manifestações podem explodir pelos países. Se houver a comunicação devida e envolvimento da sociedade, muitos países poderão gerenciar esse tipo de crise.

O CLIMA CONTINUA A SER UM RISCO CRESCENTE À MEDIDA QUE A COOPERAÇÃO GLOBAL ENFRAQUECE

A mudança climática – contra a qual ninguém é imune – continua a ser um risco catastrófico. Embora as quarentenas por todo o mundo tenham feito com que as emissões globais caíssem na primeira metade de 2020, a evidência da crise financeira de 2008 e de 2009 alerta que as emissões podem voltar. Uma mudança na direção de economias mais verdes não pode ser atrasada até que os choques da pandemia diminuam. A "falha na ação climática" é o risco mais impactante e o segundo mais provável a longo prazo identificado pelo GRR, 2021.

As respostas à pandemia provocaram novas tensões domésticas e geopolíticas que ameaçam a estabilidade. A divisão digital e uma futura "geração perdida" provavelmente testarão a coesão social de dentro das fronteiras, exacerbando a fragmentação geopolítica e a fragilidade econômica global. Com impasses e pontos de inflamação aumentando em frequência, as pesquisas do GRR 2021 classificaram o "colapso estatal" e o "colapso do multilateralismo" como ameaças críticas de longo prazo.

As potências médias - os estados influentes que, juntas, representam uma parcela maior da economia global do que os EUA e a China juntos – geralmente são campeões na cooperação multilateral do comércio, diplomacia, clima, segurança e, mais recentemente, da saúde global. Entretanto, se as tensões geopolíticas persistirem, as potências médias lutarão para facilitar uma recuperação global numa época, cuja coordenação internacional é essencial já que reforça a resiliência contra crises futuras. O GRG 2021 assinala um desafiador panorama geopolítico marcado pela "fratura das relações interestatais", "conflito interestatal" e "geopolitização dos recursos". Ou seja, todos previstos como ameaças críticas ao mundo de três a cinco anos.

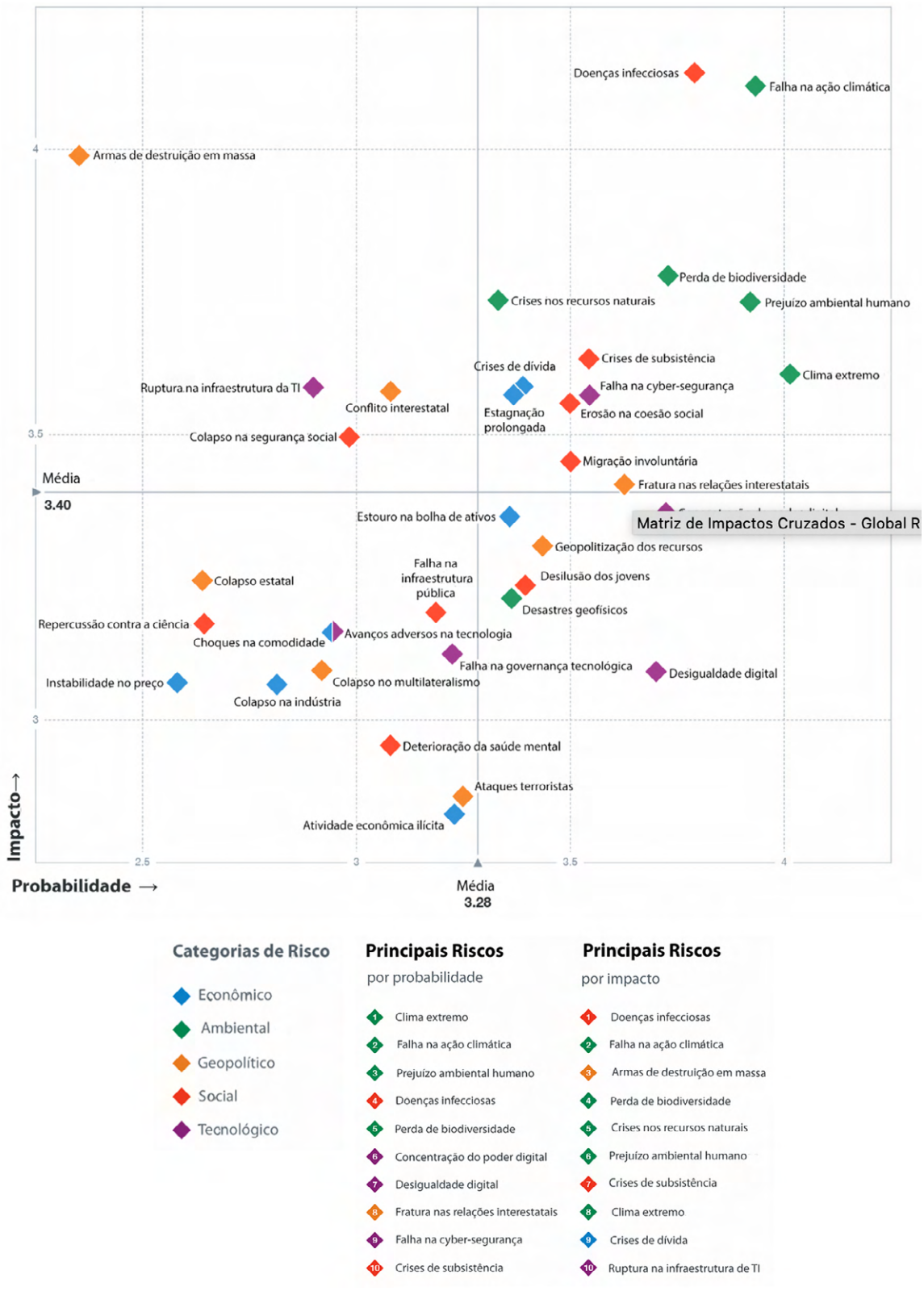


Figura 1: Matriz de Criticidade dos Riscos Globais. Fonte: Global Risk Report, 16ª edição, 2021

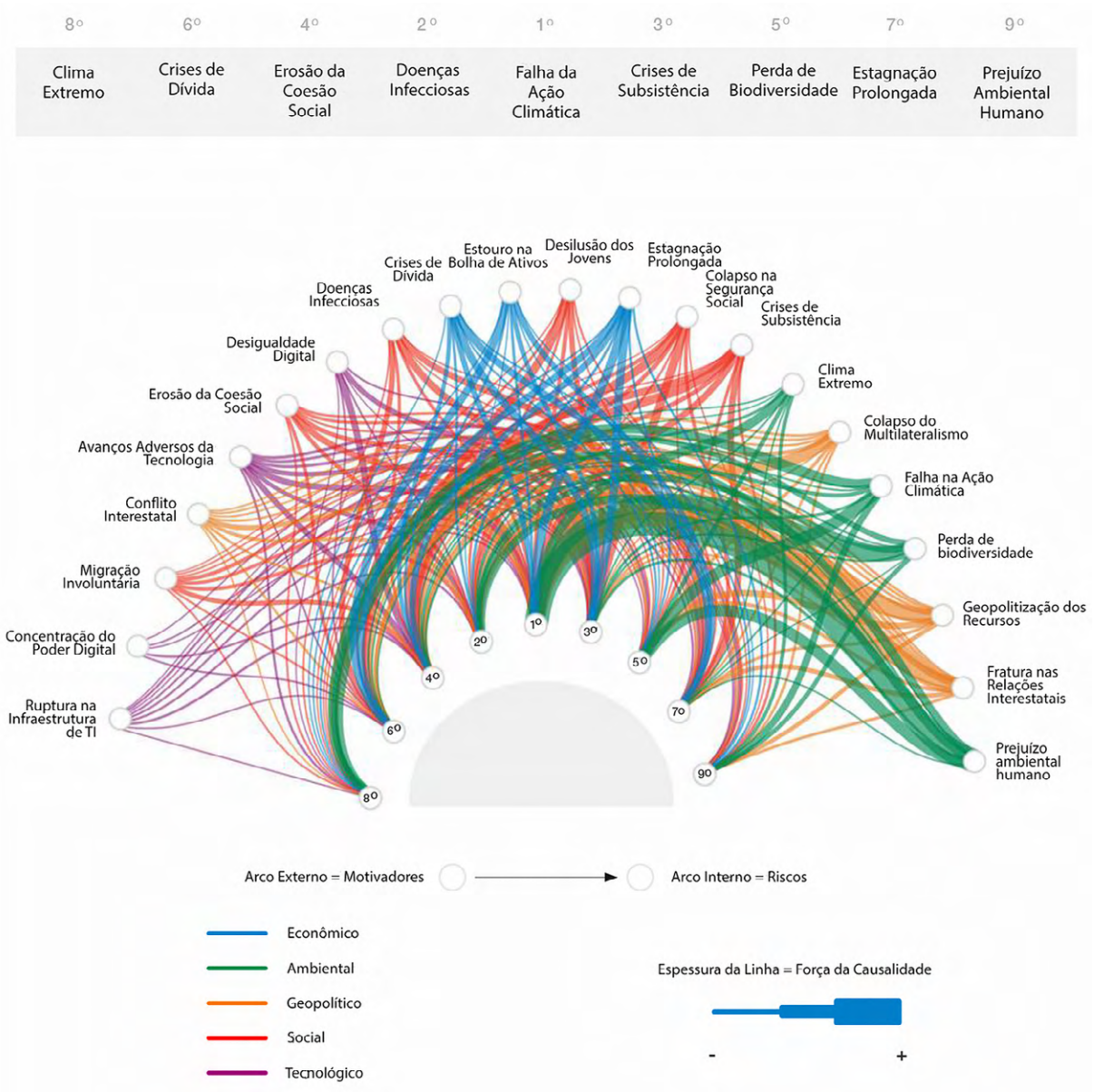


Figura 2: Interconectividade - Riscos Motrizes. Fonte: Global Risk Report, 16ª edição, 2021

Podemos observar que os nove riscos globais motrizes são:

MOTRICIDADE DOS RISCOS GLOBAIS	CLASSIFICAÇÃO
FALHA DA AÇÃO CLIMÁTICA	1º
DOENÇAS INFECCIOSAS	2º
CRISE DE SUBEXISTÊNCIA	3º
EROSÃO DA COESÃO SOCIAL	4º
PERDA DA BIODIVERSIDADE	5º
CRISE DE DÍVIDA	6º
ESTAGNAÇÃO PROLONGADA	7º
CLIMA EXTREMO	8º
PREJUÍZO AMBIENTAL HUMANO	9º

Tabela 1: Motricidade dos Riscos Globais. Fonte: Global Risk Report, 16ª edição, 2021

Reparem que os riscos tecnológicos não são motrizes, mas sim consequentes do contexto que o mundo poderá viver, se nada for feito a curto prazo. Os riscos tecnológicos já estão em andamento, pois vários dos motrizes já estão se manifestando, ocasionando consequências severas aos países.

Figura 3: Modelagem dos Riscos Globais – Prospectiva. Fonte: Global Risk Report, 16ª edição, 2021

Notem que todos os riscos sociais e de meio ambiente sem exceção possuem uma prospectiva subida em termos de probabilidade e impacto. Isto significa que se nada for feito, a chance de materialização é muito alta. Os riscos econômicos temos a subida mais da probabilidade e um dos riscos, choque nos comodities, com redução

de impacto. Os riscos geopolíticos todos sobem a probabilidade e o risco de aramas de destruição em massa aumenta muito a probabilidade já com impacto massivo. Os riscos tecnológicos todos sobem a probabilidade, ficando o colapso na Intraestrutura de TI estacionado.

PANORAMA INDUSTRIAL POLARIZADO PODE EMERGIR NA ECONOMIA PÓS-PANDEMIA

Conforme as economias emergem do estímulo da Covid-19, os negócios enfrentam uma agitação. As tendências existentes receberam um novo impulso pela crise: agendas nacionalmente focadas para conter perdas econômicas, transformação tecnológica e mudanças na estrutura social, incluindo comportamentos do consumidor, natureza do trabalho e função da tecnologia tanto no trabalho, como em casa. Os riscos comerciais emanando essas tendências foram ampliados pela crise e incluem a estagnação nas economias avançadas e o potencial perdido nos mercados emergentes e em desenvolvimento, o colapso dos pequenos negócios, a ampliação das lacunas entre as grandes e as pequenas empresas, e a redução do dinamismo do mercado sem contar a exacerbação da desigualdade, o que torna mais difícil conseguir um desenvolvimento sustentável de longo prazo.

Com os governos ainda deliberando como se afastar da emergência para a recuperação e as empresas antecipando um panorama comercial modificado, existem oportunidades para investir no crescimento inteligente, limpo e inclusive que melhorará a produtividade e a entrega das agendas sustentáveis.

MELHORES ATALHOS ESTÃO DISPONÍVEIS PARA GERENCIAR RISCOS E MELHORAR A RESILIÊNCIA

Apesar de alguns exemplos marcantes de determinação, cooperação e inovação, a maioria dos países lutou com aspectos da gestão de crise durante a pandemia global.

Embora seja cedo para esboçar lições definitivas, o GRR 2021 identificou como estratégicas para a preparação global quatro áreas vitais da resposta dada a Covid-19:

- A autoridade institucional;
- O financiamento do risco;
- A coleção da informação;
- O compartilhamento de informações;
- O compartilhamento de equipamentos vacinas.

O GRR 2021 identificou cinco domínios para uma resposta eficaz no futuro próximo:

- Tomada de decisões governamentais: os governos serem mais rápidos com informações compartilhadas e lições aprendidas de outros países;
- Comunicação pública: manter transparência por meio de relatórios públicos tipificados, gerando confiança;
- Capacidades do sistema de saúde: muitos países fizeram esforços extraordinários para expandir a capacidade do sistema de saúde na primeira onda da pandemia, por exemplo, atrasando o atendimento eletivo, realocando profissionais médicos e construindo novos hospitais temporários. No entanto, além das deficiências de epi, os sistemas de saúde também muitas vezes ignoraram o desafio de controlar infecções em instalações de alto impacto, como casas de acolhimento, onde idade e saúde precária deram origem a elevados números de óbitos. Em muitos casos, também não houve premeditação suficiente ao esgotamento crônico entre os funcionários do sistema de saúde, pois as ondas subsequentes da pandemia coincidiram com a necessidade de atender a outras condições que haviam piorado durante os bloqueios;
- Gestão do confinamento: após a abertura gradual das economias, muitos governos estavam relutantes em reverter bloqueios prolongados em todo o país. Ao invés disso, tentar curtos (duas a quatro semanas) restrições locais mais matizadas (como toques de recolher, fechamentos de hospitalidade, proibições de mistura entre famílias e proibição de viagens). O tempo e condições para a implantação dessas medidas, além de suas perspectivas de sucesso no controle da disseminação do vírus, geraram discussões políticas e resultados mistos resultaram em alguns governos retornando as abordagens nacionais mais restritas;
- Assistência financeira aos vulneráveis: as medidas de bloqueio causaram uma forte desaceleração na produção econômica, colocando em risco empregos e empresas. Os países mais ricos procuraram definir e entregar pacotes de ajuda para os grupos mais afetados e apoiaram os empregadores em seus esforços para reter funcionários. No entanto, a eliminação do apoio deixará muitas empresas com decisões difíceis de emprego. O rápido aumento do desemprego no segundo semestre de 2020 começou a pressionar ainda mais outras disposições do sistema de bem-estar social e os desafios exacerbados de saúde mental. Economias em desenvolvimento com finanças públicas limitadas muitas vezes enfrentavam a difícil escolha entre bloqueios ou pouca assistência financeira para aqueles que perderam

seus meios de subsistência e manter suas economias abertas, correndo o risco de rápida disseminação do vírus e sistemas de saúde sobrecarregados. Em muitas economias, os mercados informais também complicaram a distribuição da assistência financeira.

CONCLUSÃO

Entretanto, se as lições desta crise informarem apenas os tomadores de decisão sobre como melhor se preparar para a próxima pandemia – ao invés de melhorar os processos, as capacidades e a cultura de risco – o mundo estará novamente planejando para a última crise ao invés de antecipar a próxima.

A resposta à Covid-19 fornece quatro oportunidades de governança para fortalecer a resiliência dos países, negócios e comunidade internacional. São elas:

(1) formular os frameworks analíticos que assumem uma visão baseada na holística e nos sistemas dos impactos de risco;

(2) investir nos "campeões de risco" de alto perfil para encorajar a liderança nacional e a cooperação internacional;

(3) melhorar as comunicações de risco e combater a desinformação;

(4) explorar novas formas de parcerias público-privadas na preparação do risco.

Vejam que dos quatro pontos que o GRR 2021 chegou a conclusão de melhoria em respostas e de antecipação, três são da nossa área: gestão de riscos. Portanto, cabe aos gestores de riscos ficarem atentos com essa enorme oportunidade, pois as empresas e governos estarão a partir de agora tentando identificar os "Campeões de Riscos".

O GRR 2021 ressalta que faltou visão de antecipação. Fica claro para mim que houve uma grande falha nos serviços de inteligência, que negaram os sinais de algo estava por vir. O GRR 2021 descreve as "red flags" que lançou nas suas últimas edições:

O Relatório Global de Riscos tem discutido frequentemente o risco de pandemias para a saúde e os meios de subsistência. A edição de 2020 flagra como os sistemas de saúde em geral estavam despreparados, sem condições de atender alta demanda.

As edições de 2018 e 2019 destacaram ameaças biológicas e resistência antimicrobiana; enquanto a de 2016 ressaltou que a crise do Ebola “não seria a última epidemia grave”. Além disso, alertou que “os surtos de saúde pública provavelmente se tornarão cada vez mais complexos e desafiadores”.

O relatório também explorou aspectos da gestão do risco e da resiliência às crises: as edições de 2018 e 2019, por exemplo, analisaram os impactos da complexidade e do viés cognitivo na avaliação e resposta de riscos. A experiência da Covid-19 oferece uma oportunidade para que a área de gestão de riscos e de inteligência atualize seus processos e métodos de avaliar e monitorar riscos, visando a visão de antecipação e adaptação.

VIOLAÇÃO DE DADOS CUSTA, NA MÉDIA GLOBAL, US$ 3,8 MILHÕES PARA AS EMPRESAS. ENTENDA COMO OCORRE!

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.

A falta de um programa de prevenção de Vazamento de Dados, mais conhecido como Data Loss Prevention – DLP, segundo a IBM Security que anunciou os resultados de um estudo global que examina o impacto financeiro das violações de dados, revelando que, em média global, uma violação custa US$ 3,8 milhões para as empresas, e contas comprometidas de funcionários foram a causa mais cara.

No Brasil, o custo médio da violação de dados é de R$ 5,88 milhões de reais (cerca de US$1,12 milhão), um aumento de 10,5% em relação ao ano anterior comparando o valor em reais (R$ 5,32 milhões de reais em 2019).

CAUSAS MAIS COMUNS

Ao analisar as violações de dados sofridas por mais de 500 organizações pelo mundo, 80% dos incidentes estudados resultaram na exposição das informações de identificação pessoal de clientes. Entre todos os tipos de dados expostos nessas violações, as informações pessoais de clientes também foram as mais caras para as empresas.

O relatório aponta as perdas financeiras que as organizações podem sofrer caso dados sejam comprometidos, à medida que empresas acessam cada vez mais dados sensíveis por meio do trabalho remoto e operações de negócios na nuvem.

Um outro estudo da IBM descobriu que mais da metade dos funcionários que começaram a trabalhar em casa devido à pandemia não recebeu novas orientações sobre como lidar com as informações pessoais de clientes.

Patrocinado por IBM Security e conduzido pelo Instituto Ponemon, o Relatório de Custo da Violação de Dados 2020 (Cost of Data Breach 2020) é baseado em entrevistas realizadas com mais de 3.200 profissionais de segurança em organizações que sofreram alguma violação de dados durantes o último ano.

Algumas das principais descobertas do relatório incluem:

1. Tecnologia inteligente reduz custo de violações pela metade;

   Empresas que implementaram tecnologias de automação de segurança (que utilizam IA, análise de dados e orquestração automatizada para identificar e responder aos eventos de segurança) tiveram menos da metade dos custos de violação de dados quando comparadas às que não implementaram essas ferramentas – US$2,45 milhões vs US$6,03 milhões, em média.

2. Pagamento pelas credenciais comprometidas;

   Em incidentes nos quais atacantes acessam a rede das corporações usando credenciais comprometidas ou roubadas, as empresas viram o custo de violação de dados ser quase US$1 milhão mais alto em comparação à média global, chegando a US$4,77 milhões por violação. Ataques maliciosos, que exploram a vulnerabilidade de terceiros, foi a segunda origem com maior custo (US$4,5 milhões) para esse grupo.

3. Custo de mega violações aumenta aos milhões;

   Os custos das chamadas mega violações, nas quais mais de 50 milhões de registros são comprometidos, subiram de US$388 milhões para US$392 milhões. Violações nas quais 40 – 50 milhões de registros foram expostos custaram para as empresas US$364 milhões em média, um aumento de US$19 milhões comparado ao relatório de 2019.

4. Ataques de estado-nação (nation-state) – a violação mais prejudicial.

   As violações de dados que possam ter sido originadas dos ataques de estado-nação foram as mais caras em comparação com outros atores de ameaças examinados no relatório. Conhecidos como “state-sponsored attacks”, esses ataques tiveram uma média de U$4,43 milhões em custo de violação de dados, superando os cibercriminosos motivados financeiramente e os hackativistas.

A conclusão do Relatório da IBM Security é a de que quando se trata da capacidade de mitigar o impacto de uma violação de dados, enxerga-se uma clara vantagem de empresas que investiram em tecnologias automatizadas.

Em um momento em que as empresas estão expandindo sua presença digital a um ritmo acelerado e a falta de skills no setor de segurança da informação e cibernética persiste, as equipes podem ficar sobrecarregadas ao proteger mais dispositivos, sistemas e dados. A automação da segurança cibernética pode ajudar a resolver essa carga, permitindo uma resposta mais rápida à violação e significativamente mais econômica, em relação custo x benefício.

VULNERABILIDADE PREFERIDA DOS HACKERS

Credenciais de funcionários e nuvens configuradas incorretamente, ponto de entrada preferido dos atacantes.

Credenciais roubadas ou comprometidas e nuvens com configurações incorretas foram as causas mais comuns de violações maliciosas para as empresas que participaram do estudo, representando aproximadamente 40% dos incidentes. Com mais de 8,5 bilhões de registros expostos em 2019 e atacantes usando e-mails e senhas previamente expostos em uma a cada cinco violações estudadas, as empresas estão repensando sua estratégia de segurança pela adoção da abordagem de confiança-zero (zero trust) – reexaminado como eles autenticam os usuários e como a extensão de acesso aos usuários são concedidos.

Similarmente, a luta das empresas com a complexidade da segurança – o principal fator de custo de violações – está contribuindo para que as configurações incorretas de nuvem se tornem um desafio de segurança crescente. O relatório de 2020 revelou que os atacantes usaram as configurações incorretas de nuvem para violar as redes em 20% do tempo, aumentando o custo de violações para US$4,41 milhão em média.

TECNOLOGIAS AVANÇADAS FAZEM A DIFERENÇA NA PREVENÇÃO

Tecnologias avançadas de segurança ajudam os negócios.

O relatório destaca a crescente divisão no custo de violações entre empresas que implementaram tecnologias avançadas de segurança e aquelas que estão atrasadas, revelando uma diferença de economia de US$3,58 milhões para companhias com automação de segurança totalmente implementada versus aquelas que ainda não implementaram este tipo de solução.

As empresas participantes do estudo que contavam com automação de segurança totalmente implementada também relataram um tempo de resposta significativamente mais curto às violações, outro fator-chave mostrado para reduzir os custos de violação

na análise. O relatório constatou que inteligência artificial, machine learning, análise de dados e outras formas de automação de segurança permitiram às empresas responder a violações até 27% mais rápido do que as empresas que ainda não implantaram a automação de segurança.

FALTA DE PLANOS DE RESPOSTAS A INCIDENTES ESTRUTURADOS – FATOR CHAVE.

A preparação para resposta a incidentes também continua influenciando fortemente as consequências financeiras de uma violação. Empresas que não possuem uma equipe designada ou testes de planos de resposta a incidentes, sofrem em média com um custo de US$5,29 milhões em violação, enquanto as empresas que possuem equipes dedicados, testes e simulações sofrem menos de US$2 milhões em custo de violações. Isso reafirma que a preparação e a prontidão geram um ROI significativo em segurança cibernética.

ALGUNS OUTROS ITENS DE INSEGURANÇA IDENTIFICADOS:

1. Riscos do trabalho remoto têm um preço – Com modelos de trabalho híbrido criando ambientes menos controlados, o relatório descobriu que 70% das empresas que adotaram o teletrabalho em meio à pandemia esperam que os custos de violações de dados se agravem.

2. CISOs culpados pelas falhas por violações, apesar do poder limitado de tomada de decisão: 46% dos entrevistados disseram que o CISO/CSO é responsabilizado pelas violações. Detalhe importante é que apenas 27% afirmaram a tomada de decisão sobre política de segurança e tecnologia vem do CISO/CSO. O relatório concluiu que a nomeação de um CISO foi associada com uma economia de US$145.000 versus a média de custo por violação.

TENDÊNCIAS REGIONAIS E POR INDÚSTRIA

- O estudo analisou o custo de violações de dados em diferentes indústrias e regiões, descobrindo que as violações de dados nos Estados Unidos são muito mais caras, custando US$8,64 milhões em média.

- No Brasil, o estudo também observou um aumento no número de dias para identificar a violação de dados, que subiu de 250 para 265 dias, e para conter a violação, que cresceu de 111 para 115 dias, em comparação a 2019. Vejam que é uma grande deficiência não identificar rapidamente.

- Globalmente, a indústria de saúde continua apresentando os

mais altos custos médios de violação, com US$ 7,13 milhões – um aumento de mais de 10% em comparação com o estudo de 2019.

CONCLUSÃO

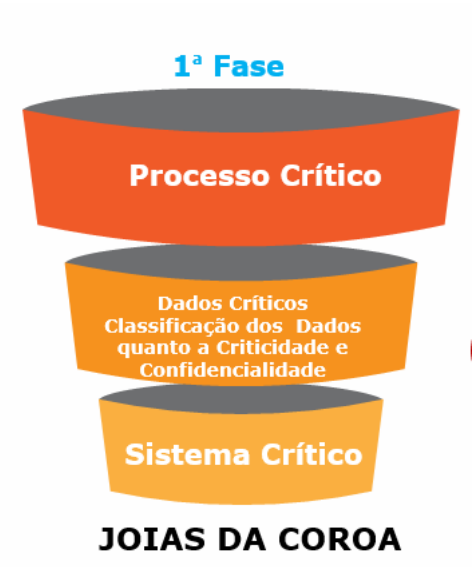
Nossa conclusão, pelo que podemos ler do Relatório da IBM Security, que ainda falta, principalmente no Brasil um Programa Formalizado de DLP.

A empresa deve entender que para evitar a violação de dados tem que aceitar o fato de que as informações e dados estratégicos e críticos podem ser conseguidos de forma Voluntária ou involuntária. Isso mesmo. Se um funcionário de médio escalão possui uma informação estratégica e não sabe o valor dela para a empresa, há grande possibilidade de vazar através de conversas informais com grupos de amigos, ou mesmo, ser vítima de engenharia social e ou técnica de indução. Vimos no Relatório da IBM Security que a utilização de credenciais de funcionários ou ex-funcionários foi uma das brechas mais utilizadas. Outro tópico foi a falta de uma estrutura de respostas a incidentes, causando retardo e custos maiores.

Para isso a empresa deve ter um Processo Estruturado contra Vazamento e Violações de Dados, com metodologia e critérios parametrizados.

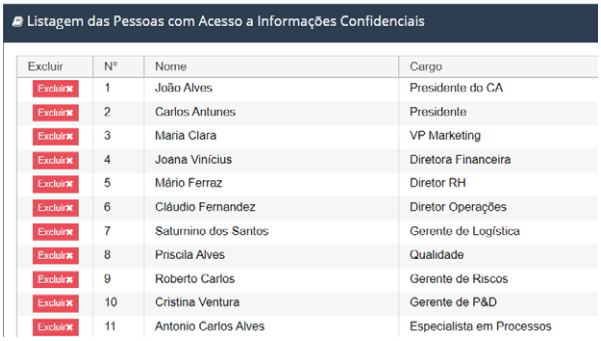
A Brasiliano INTERISK possui um processo estruturado, simples e prático, em três fases, em que percorremos nas empresas:

1. Identificação das denominadas Joias da Coroa:



2. Identificação da Maturidade das Pessoas com acesso a estes dados:

Lista de Pessoas com acesso aos Dados.



Listagem das Pessoas com Acesso a Informações Confidenciais

Excluir	Nº	Nome	Cargo
Excluir	1	João Alves	Presidente do CA
Excluir	2	Carlos Antunes	Presidente
Excluir	3	Maria Clara	VP Marketing
Excluir	4	Joana Vinícius	Diretora Financeira
Excluir	5	Mário Ferraz	Diretor RH
Excluir	6	Cláudio Fernandez	Diretor Operações
Excluir	7	Saturnino dos Santos	Gerente de Logística
Excluir	8	Priscila Alves	Qualidade
Excluir	9	Roberto Carlos	Gerente de Riscos
Excluir	10	Cristina Ventura	Gerente de P&D
Excluir	11	Antonio Carlos Alves	Especialista em Processos

Lista de Pessoas com acesso aos Dados.

Identificar a Maturidade das Pessoas em Segurança Cibernética

Pontuação dos Quesitos	Nível de Maturidade
8	Baixa
9 - 17	Média
> 17	Alta

1 - Baixa maturidade
2 - Média maturidade
3 - Alta maturidade

Classificação da Maturidade das Pessoas com Acesso a Informações Confidenciais

Nome	I...	Phishing	Controle de S...	Nível de Segu...	Nível de Trata...	Segurança Di...	Segurança de...	Soma Notas	Criticidade
João Alves	2	1	2	2	2	2	2	15	
Carlos Antunes	2	2	3	2	3	2	3	19	
Maria Clara	2	2	2	2	3	3	2	17	
Joana Vinícius	1	1	1	1	1	1	1	8	
Mário Ferraz	1	1	1	1	1	1	1	8	
Cláudio Fernandez	3	3	3	3	3	2	2	22	
Saturnino dos Santos	2	2	2	2	2	2	3	17	
Priscila Alves	3	3	3	3	2	2	3	22	
Roberto Carlos	1	2	3	3	3	3	3	21	

Quesitos: Engenharia Social; Técnicas de Indução; Phishing; Controle de senhas; Nível de Segurança de seu computador ou aparelho mobile; Nível de tratamento de documentos físicos; Segurança digital – Trabalhar em locais públicos; Segurança de Redes.

Tríade para saber quem lida com o que e por onde passam os dados – Ciclo.

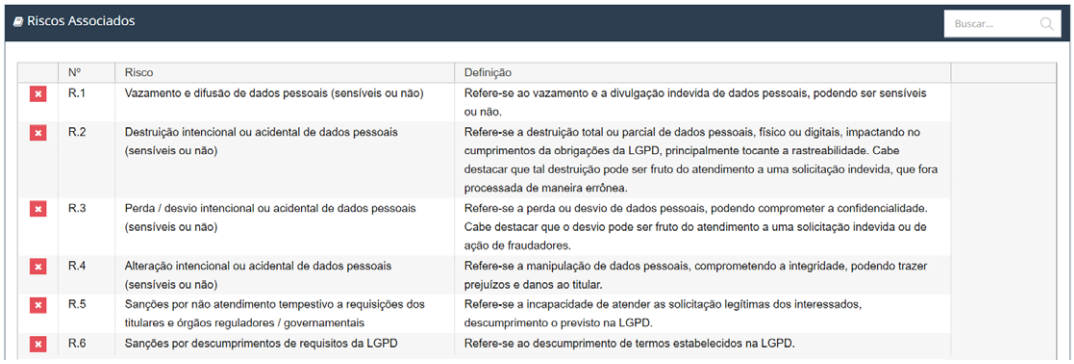
Associar as Pessoas Críticas X Dados Críticos e Pessoais X Sistemas dos Dados Críticos e Pessoais

3. Análise Situacional para Identificar as Vulnerabilidades e Ameaças:

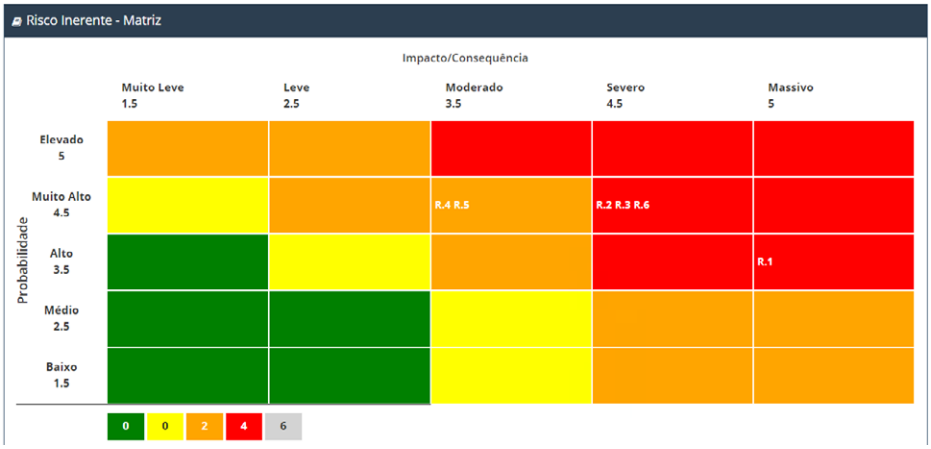
Este diagnóstico é elaborado através de um Check List das Melhores Práticas.

Com isso saberemos quais são as Vulnerabilidades e Ameaças existentes.

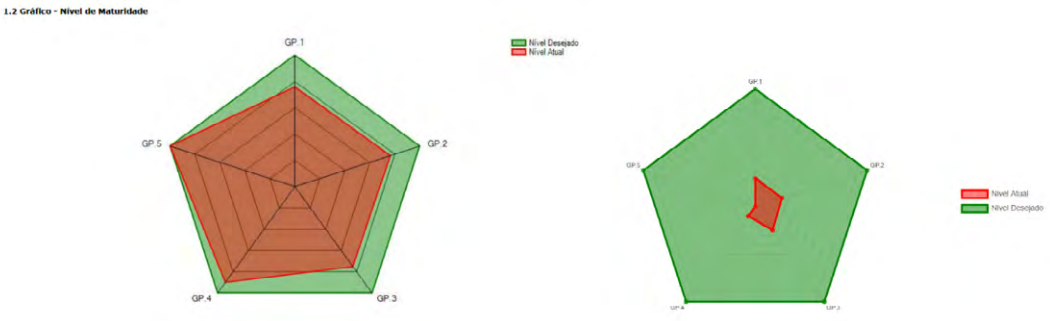
Ameaças



Grau de Criticidade



Como resultado desta Terceira fase temos o Nível de Maturidade:



1.1 Resultado - Nível de Maturidade

QUESITOS DE MATURIDADE	NÍVEL DESEJADO	NÍVEL ATUAL
GP.1 - Identificar (ID)	10,00	7,59
GP.2 - Proteger (PR)	10,00	7,62
GP.3 - Detectar (DE)	10,00	7,50
GP.4 - Responder (RS)	10,00	9,00
GP.5 - Recuperar (RC)	10,00	10,00
SOMA	**50,00**	**41,71**
MÉDIA GERAL	**10,00**	**8,34**

MATURIDADE	DE	ATÉ	RECOMENDAÇÃO
Insuficiente	0,00	3,00	Tratar
Regular	3,01	5,00	Desenvolver
Bom	5,01	7,50	Melhorar
Muito Bom	7,51	9,00	Aprimorar
Excelente	9,01	10,00	Manter

4. Sugestões Estruturantes:

Soluções Preventivas e Mitigatórias.

4ª fase

Sugestões Estruturantes
Tecnológicas
Organizacionais: Planos de Respostas a Incidentes
Pessoal: Sensibilização

Com isso a empresa estará preparada para conter vazamentos e violações, além de reagir com maior rapidez e flexibilidade.

RELAÇÕES DE GÊNERO NA SEGURANÇA PRIVADA: ESTUDO COM GUARDIÃS EM UMA ORGANIZAÇÃO DO SUDESTE BRASILEIRO

Carlos Alberto Zanandreis da Silveira
Luciano Zille Pereira
Artigo originalmente publicado nos anais do XXIII SEMEAD – novembro 2020

1. INTRODUÇÃO

As mulheres brasileiras vêm alcançando desde os anos 70 e 80, ganhos sociais, políticos e econômicos, principalmente, em função das lutas feministas amparadas pela Constituição Federal de 1988, que preconiza a igualdade de direitos entre homens e mulheres, reforçado pela Lei Maria da Penha, de agosto de 2006 (Andrade, Macedo & Oliveira, 2014).

Dados da Pesquisa Nacional por Amostra de Domicílio (PNAD) de 2019 apontam que as mulheres são a maioria na população brasileira (51,1%), porém quando se observa a representação gerencial (39,1%) e política (10,5%) a situação se inverte em relação aos homens. Tal situação vem sendo resultado de uma cultura imposta pela sociedade com a definição de papéis de mulheres e homens (Louro, 1997; Beauvoir, 2008; Bourdieu, 2011; Herrera, 2014; Matos, 2018).

No entanto, os movimentos feministas vêm proporcionando ganhos sociais levando as mulheres a terem maior condição de atuarem em mercados de trabalho até então considerados masculinos como a construção civil, motoristas profissionais, meios militares e a segurança pública e privada. A segurança privada é um desses setores que tem tido o aumento da participação feminina apesar de sua origem remontar à segurança pública, de origem militarizada e masculinizada (Daniel, 2011; Reis, 2013; Herrera, 2014; Stachowitsch, 2015, Leite, 2016; Silva & Ferreira, 2016; Matos, 2018).

Em relação à segurança privada, 553.905 trabalhadores, 500.176, equivalente a 90,3% representavam o gênero masculino. No entanto, o aumento da participação feminina neste setor vem se dando, principalmente, em função da mudança de perfil de atendimento dos clientes contratantes do serviço de segurança privada como as instituições financeiras, casas comerciais, shopping centers, entre outros (Federação Nacional das Empresas de Segurança e Transporte de Valores [Fenavist], 2019).

No curso de formação de vigilantes não há diferença de conteúdos aplicados para homens e mulheres e estas perfazem aproximadamente 20% das turmas, com resultados tão bons quanto aos participantes homens. Porém, ao se comparar com a participação no mercado de trabalho, esse percentual passa a ser de apenas 9,7%, o que pode ocorrer em função da institucionalização do security man, que preconiza uma visão de que as mulheres não impõem respeito, além de que a força física tem grande importância no trabalho que envolve a segurança (Diogo & Coutinho, 2013; Stachowitsch, 2015).

Considerando o contexto apresentado até então, este estudo objetivou descrever e analisar as relações de gênero na segurança privada, na percepção das vigilantes (guardiãs), que atuam em uma empresa do setor de segurança privada localizada em um estado do sudeste brasileiro.

2. REFERENCIAL TEÓRICO

O estudo de gênero envolve relações sociais e históricas ligadas a aspectos políticos, da economia e da psicologia. Portanto, contribuem para analisar ações de diversos atores sociais envolvidos em relação à temática da segurança (Eichler, 2015; Cardeal & Ribeiro, 2017).

Silva et al. (2014) salientam que as estatísticas têm mostrado o aumento da participação feminina no mercado de trabalho, inclusive com atuação em setores que antes eram destinados somente aos homens.

Campos, Silva, Miranda e Cappelle (2017), apontam que a literatura tem ampliado os estudos sobre as relações de gênero e a participação da mulher. Explicam que apesar do desenvolvimento econômico do Brasil, a inserção feminina ainda não ocorreu em plenitude, em função da visão patriarcal que prevalece gerando preconceitos e segregações.

Drydakis, Sidiropoulou, Bozani, Selmanovic e Patnaik (2017), apontam que as principais argumentações para confirmar tais pensamentos referem-se às menores oportunidades de acesso ao mercado de trabalho, diferenças salariais a favor dos homens em funções semelhantes, maior carga de trabalho, isso sob a égide de um sistema social que determina uma hierarquia simbólica.

Cappelle, Miranda e Mafra (2012) apontam que a entrada da mulher no mercado de trabalho tem promovido mudanças nas organizações, principalmente em funções antes ocupadas por homens. Porém, essa maior participação está atrelada à busca de condições para que possam conciliar as atividades domésticas e familiares com a profissão, visto que isto pode torna-se um dos limitadores para a participação feminina no mercado de trabalho (Sousa & Guedes, 2016).

Lima, Voig, Feijó, Camargo e Cardoso (2017), revelam que um dos fatores que dificultam às mulheres serem contratadas e ascenderem a cargos mais elevados na hierarquia das organizações prende-se ao fato de os gestores, normalmente, preferirem contratar funcionários que se assemelham ao seu próprio perfil. Como a maioria das empresas a gestão está sob a responsabilidade de homens, estes criam restrições para a contratação de perfis femininos. Nessa direção, a dificuldade de ascensão das mulheres a cargos de uma hierarquia superior nas organizações ocorre, portanto, não fica claramente explícito, lembrando o termo denominado de 'teto de vidro', fruto de uma construção social que descrimina e coloca empecilhos às mulheres para o ingresso e ascensão nas organizações (Gontijo & Melo, 2017; Bertrand, 2018).

Santos, Tanure e Carvalho (2014) explicam que o 'teto de vidro' é uma representação simbólica das dificuldades impostas em uma organização para a ascensão feminina, porém não é facilmente percebida e identificada. No "teto de vidro" ocorre a discriminação por preferência, em que a organização prefere conceder oportunidade a cargos mais elevados na hierarquia ao homem, mesmo que sua condição de produzir seja semelhante à da mulher. A base dessa preferência está ligada a conceitos culturais e valor de quem escolhe. Outro aspecto abordado é que o fenômeno do "teto de vidro", de certa forma, ocorre quando as mulheres buscam ascender a funções estratégicas na hierarquia organizacional (Santos et al., 2014; Oliveira & Woida, 2018).

Em relação ao gênero, alguns estudos têm mostrado a presença feminina em setores de trabalho antes considerados masculinos, como o de segurança, em que as mulheres têm ascendido à segurança pública como polícias civis, militares, guardas municipais e a segurança privada. Porém, ao analisar tais estudos, percebe-se que a ascensão vem ocorrendo com a presença de preconceitos, desafios e conflitos (Calazans, 2004; Cappelle & Melo, 2010; Ribeiro, 2018).

Ribeiro (2018) salienta que atividades ligadas à aplicação da lei e à vigilância, normalmente, são atribuídas aos homens, pois requerem a aplicação de repressão e força física que não são características encontradas nas mulheres. A inserção das mulheres na área da segurança visa, entre outros aspectos, menor truculência nos atendimentos. Para Diogo e Coutinho (2013) as mulheres vêm buscando o trabalho no setor de segurança privada com intuito de obter melhorias nas condições de vida. Entre os desafios desse setor estão a maior exigência dos clientes com aspectos relacionados à fragilidade da mulher para o serviço de segurança, aliado às restrições da atuação da mulher em postos noturnos, como também aqueles considerados mais perigosos. Para a contratação da vigilante feminina, algumas exigências adicionais

existem como não terem filhos nem a intenção momentânea de ter, boa apresentação pessoal, comportamento e desempenho compatível com a função.

3. MÉTODOLOGIA

A pesquisa foi descritiva, e neste estudo descreveu-se a percepção das vigilantes femininas (guardiãs) sobre as relações de gênero em relação às atividades de segurança privada na organização pesquisada. A abordagem foi qualitativa, por meio de estudo de caso, onde o caso estudado foi à relação de gênero na percepção das vigilantes que atuam em uma empresa privada em um estado do sudeste brasileiro.

A unidade de análise consistiu nas relações de gênero e a unidade de observação foi à empresa de segurança privada pesquisada, onde os sujeitos foram às próprias vigilantes pesquisadas, identificadas aleatoriamente, de acordo com interesse e disponibilidade para participar da pesquisa.

A coleta de dados foi realizada por meio de entrevista semiestruturada, com a participação de onze vigilantes femininas que atuam no setor operacional da empresa e um gestor que tem como atribuição a coordenação geral do serviço de vigilância. As entrevistas foram previamente consentidas e agendadas, realizadas nas próprias dependências da empresa e foram submetidas ao critério de saturação, que segundo Fontanella, Ricas e Turato (2008), que consiste em um processo contínuo de obtenção de dados, desde as primeiras entrevistas, observado o momento em que estas passam a não mais contribuírem para acrescentar dados para análise.

Os dados foram analisados com base na técnica de análise de conteúdo categorial (BARDIN, 2016), onde as categorias de análise foram previamente definidas com base nos objetivos do estudo, sendo elas: perfil profissional, desenvolvimento funcional, condições de trabalho, processos de trabalho e relações de gênero e estratégias de defesa.

4. ANÁLISE E DISCUSSÃO DOS RESULTADOS

Para fins da análise dos dados as vigilantes foram identificadas com a sigla GUA (guardiãs), seguida do número de ordem em que as entrevistas foram realizadas, sendo de 1 a 11. O gestor de segurança foi identificado como GES.

Em relação à atuação na atividade de vigilância, dez vigilantes, ou 90,9%, têm mais de um ano de atuação no posto de trabalho na empresa pesquisada. Considerando o tempo total na área da vigilância, 63,5% das entrevistadas têm oito anos ou mais em relação ao tempo de atuação na segurança privada.

Quanto ao estado civil, sete ou 72,7% são solteiras, o que pode indicar uma tendência do perfil para atuação neste segmento profissional. Quanto à idade, as 11 entrevistadas possuem entre 25 a 46 anos, sendo que a maioria está acima de 35 anos.

Em relação à escolaridade, seis possuem ensino médio completo, cinco possuem curso superior, sendo quatro de graduação tecnológica em gestão de segurança.

Os dados mostraram que os postos de serviço em que as vigilantes atuam são diversificados: cinco atuam em condomínios empresariais, duas no setor industrial, duas em shopping center, uma no varejo e uma em condomínio residencial. Em todos os postos de serviço as vigilantes atuam como prestadoras de serviço terceirizado tendo como chefias locais o cliente contratante dos serviços, em sua maioria, supervisores homens.

No que se refere à jornada de trabalho nove vigilantes, ou 81,8%, atuam na escala de serviço 12 x 36, ou seja, trabalham 12 horas no posto de serviço e descansam 36 horas. Trata-se de uma escala predominante na área de segurança, o que foi apontado pelas pesquisadas como uma das condições que as motivam atuar nesta área, pois conseguem certo equilíbrio entre a vida profissional e a pessoal.

4.1 Categorias e subcategorias de análise

As categorias de análise foram definidas a priori, tendo como base os objetivos da pesquisa e as subcategorias emergiram como resultado das entrevistas realizadas, utilizando-se o critério da frequência com que foram obtidas, com um percentual de pelo menos 40,0% das ocorrências, conforme constam na Figura 1, a seguir.

Categorias de análise	Subcategorias
Perfil profissional	- Critérios para contratação; - Processo seletivo.
Desenvolvimento funcional	- Carreira funcional; - Qualificação profissional.
Condições de trabalho	- Ambiente físico; - Equipamentos; - Apoio institucional.
Processos de trabalho e relações de gênero	- Processos de trabalho; - Relações de gênero.
Estratégias de defesa	- Normas institucionais; - Estratégias de enfrentamento.

Figura 1 – Matriz de relação: categorias versus subcategorias.
Fonte: Elaborado pelo autor (2019).

4.1.1 Perfil profissional

Esta categoria surgiu da necessidade de se identificar na pesquisa as características exigidas pela organização para contratação das vigilantes. Os profissionais autorizados a realizar a atividade de segurança privada são os vigilantes capacitados em cursos de formação de vigilantes. Tais profissionais devem possuir, segundo a Portaria 3233/2012 da Polícia Federal, os seguintes requisitos: ser brasileiro, ter idade mínima de 21 anos, possuir instrução mínima de 4ª série do ensino fundamental, ser aprovado em curso de formação de vigilante em escola autorizada pela Polícia Federal, apresentar avaliação médica e psicológica, estar em dia com obrigações eleitorais e militares e possuir idoneidade (atestados) e registro no cadastro de pessoas físicas (Zanetic, 2009; Fenavist, 2019).

Quanto às exigências requeridas para a função, não se veem diferenciações para vigilantes masculinos e femininos. Ou seja, as exigências legais não determinam especificidades relativas ao gênero (Brasil, 2019).

4.1.1.1 Critérios para a contratação

Esta subcategoria emergiu das respostas das entrevistadas, que apontaram dois aspectos: a não definição clara dos requisitos exigidos pela organização, exceto a exigência do curso de vigilância e documentos que comprovam idoneidade, habilidades para lidar com público, porte físico e postura. Portanto, não ficou claro os critérios específicos para o processo de contratação.

4.1.1.2 Processo seletivo

O processo seletivo consiste basicamente em entrevista de triagem realizada com a psicóloga da empresa e, algumas vezes, com o gestor de segurança, após as vigilantes serem indicadas pelos clientes e entregarem o currículo vitae. Após a entrevista, as candidatas que preencherem os requisitos do cargo, seguem no processo, realizando testes psicológicos e exame médico de acordo com o posto de trabalho a ser ocupado. O relato a seguir retrata as etapas do processo seletivo:

> Meu processo seletivo foi em função de um setor de trabalho que a empresa tinha ganhado. O supervisor lá deste novo setor fez a minha indicação. Fiz a entrevista e consegui ser contratada (GUA 11).

Ficou evidenciado nas entrevistas que o processo seletivo tem um padrão definido, passando por indicação do cliente e entrega de currículo vitae, entrevista, testes psicológicos e exame médico. Essa rotina é apontada por Diogo e Coutinho (2013), onde salientam que o processo seletivo nas empresas de segurança visa atender as demandas dos clientes e dos postos de serviço.

4.1.2 Desenvolvimento funcional

Esta categoria de análise objetivou identificar e descrever os requisitos necessários para que as vigilantes possam ascender a níveis mais elevados na hierarquia da organização onde atuam. Um primeiro aspecto que a categoria mostra é que, de maneira geral, as empresas de segurança não têm um plano de carreira para os vigilantes. A situação fica mais crítica quando se trata das guardiãs, pois há muito menos opções de postos de serviços, além de não serem a primeira opção de escolha dos clientes e da empresa para as funções de líder e supervisão.

4.1.2.1 Carreira funcional

Esta subcategoria emergiu da categoria desenvolvimento funcional, principalmente, sob a ótica negativa por parte das vigilantes entrevistadas, que, em sua maioria, não veem oportunidades de ascensão profissional, notadamente, se comparadas aos vigilantes masculinos, o que pode ser verificado no estudo de Diogo (2012) quando aponta que a ascensão feminina neste setor é para poucas. O relato a seguir ilustra essa situação:

> No cargo de guardiã é muito difícil a possibilidade de a ascensão. Não vejo muito espaço, não. A guardiã pode ir lá, faz o curso, pode fazer o curso de extensão e não faz diferença para o seu desenvolvimento na carreira (GUA 2).

Evidenciou-se entre as respostas das vigilantes que as raras perspectivas de crescimento inerentes à carreira, em geral, são de ser um líder no setor onde atuam a de ser um supervisor interno ou externo e, mais raramente, a de ser coordenador e gerente, que é o nível mais elevado nesta categoria funcional.

As entrevistas também apontaram que as vigilantes estão preocupadas com suas carreiras, visto que a maioria delas vislumbrou a necessidade de terem mais oportunidades, embora estas praticamente não ocorrem. Constatou-se, portanto, que as ações da organização vão de encontro ao que se preconiza como ideal na gestão de carreiras, contrariando o que apontam Trambaioli e Joviliano (2015), salientando que as organizações estão trabalhando pelo desenvolvimento de carreiras cada vez mais e, com isso, motivando e obtendo melhores resultados.

4.1.2.2 Qualificação profissional

Esta subcategoria, que também emergiu da categoria desenvolvimento funcional, teve como referência os relatos das entrevistadas ao vislumbrarem as remotas possibilidades de crescimento na organização a partir da qualificação. Apesar de considerarem que as oportunidades são poucas e a organização não possuir um plano de carreira, ficou evidenciado nas entrevistas que a qualificação profissional é importante para desenvolver um bom trabalho e ter a oportunidade de evoluir na carreira, mesmo que de forma restrita. Para as funções de líder de setor e de

supervisor interno, a influência do cliente é considerável, sendo a indicação um fator determinante para ascensão na carreira. O relato a seguir aponta nessa direção:

> Na verdade, tudo tem que partir da pessoa, né, ela buscar o crescimento, buscar aprimorar as coisas, e creio eu que outras pessoas da empresa, sabendo que você tá buscando aprimorar o seu currículo, pode ser que futuramente, né, te dê oportunidade, faça alguma entrevista com você, algum processo seletivo, para ver se encaixaria na vaga, no entanto isto não vem ocorrendo (GUA 11).

Zanetic (2009) e Diogo e Coutinho (2013) apontam que o nível de exigência do setor de segurança é cada vez maior e isso exige qualificação, porém a situação relatada enfatiza de maneira importante que mesmo buscando se qualificar as oportunidades de ascensão na carreira para as mulheres na área de segurança se torna difícil, conforme argumenta Santos et al. (2014).

4.1.3 Condições de trabalho

Esta categoria está relacionada às condições de trabalho no que tange a recursos materiais, ambiente físico e apoio institucional inerente ao trabalho das vigilantes. Vieira, Lima e Lima (2010) e Ribeiro et al. (2011), apontam que as condições de trabalho dos vigilantes, de maneira geral, estão ligadas às características do posto de trabalho em que atuam, ou seja, cada cliente com suas regras, níveis de exigência e às condições físicas dos postos, que são diferentes, configura assim, o ambiente em que os vigilantes atuam.

Em relação aos equipamentos utilizados pelas empresas de segurança, estes são padronizados e controlados pelas normas da Polícia Federal. De forma geral, o que se apurou com base nas entrevistas é que não há muitas diferenciações do que é oferecido em termos de condições de trabalho entre vigilantes homens e mulheres, ou seja, as condições são, na maioria das vezes, inadequadas para o trabalho.

4.1.3.1 Ambiente físico

Esta subcategoria emergiu em relação à categoria condições de trabalho, tendo por base os relatos das vigilantes, quando apontaram que, em termos de ambiente, não há diferenças entre homens e mulheres e que, de forma geral, ficou dividido entre aquelas que acreditam que têm uma boa condição e aquelas que acreditam que existem problemas para a realização das atividades.

Ficou evidente que o cliente (tomador do serviço) é que, normalmente, se responsabiliza pelas condições de trabalho, que de forma geral, não são as melhores. Uma explicação apontada por Brasil (2019) é em virtude da Portaria 3233/2012 da Polícia Federal que define critérios obrigatórios em relação às condições de atuação do vigilante. Tal situação é confirmada pelos estudos de Vieira et al. (2010) e Ribeiro et

al. (2011) que apontam que as condições de trabalho dos vigilantes, de maneira geral, estão ligadas às características do posto de trabalho em que atuam.

4.1.3.2 Equipamentos

A subcategoria 'equipamentos' também não mostrou diferenças em relação ao gênero. Os equipamentos são fornecidos pela empresa ou cliente e são obrigatórios, com padrão definido e controlados pela Polícia Federal. Sobre os materiais fornecidos, as guardiãs reclamaram do uniforme, que as tornam masculinizadas, por ser padrão, ou mesmo, por sua qualidade e tamanho. No relato a seguir, argumentações são apresentadas neste sentido:

> O uniforme já é padrão. A mulher já vai ficar com uma característica bem masculina, embora tenha a diferença que o homem usa gravata e a mulher usa lencinho (GUA 3).

A Portaria 3.233/2012 da Polícia Federal trata do uniforme como uso obrigatório, visando demonstrar ostensividade. Essa portaria ainda menciona os itens que devem constar junto ao uniforme e equipamentos de proteção obrigatórios (Brasil, 2019).

Os relatos trazem ainda que apesar de não haver restrições legais para uso de armamento em relação aos vigilantes homens e mulheres, há postos (clientes) que definem que as mulheres não utilizem armamento, não ficando claro o motivo desta discriminação para as entrevistadas, o que sugere preconceito e desvalorização em relação ao trabalho feminino.

4.1.3.3 Apoio institucional

Esta subcategoria surgiu em decorrência de as vigilantes terem apontado em suas falas dois aspectos: um ligado ao apoio da empresa para a realização de suas atividades e outro, à resolução de problemas no ambiente de trabalho. Destacaram que há diferenças de apoio quando se considera o gênero dos profissionais de segurança. Um aspecto relevante que se evidenciou foi a importância da relação das vigilantes com os supervisores, que, no caso da empresa estudada, são somente homens. Ou seja, todas as mulheres na empresa são subordinadas a chefia de homens, o que faz com que possam surgir situações conflitantes e diferenciações de tratamento em virtude do gênero. O relato a seguir aponta nessa direção:

> Sempre tem uma diferença de apoio entre os vigilantes masculinos e as guardiãs. Para falar a verdade (risos), mas eu falo assim: é, aquela questão deles lá, dos mais chegados deles, entendeu. Geralmente os homens são os mais chegados porque homem tem mais afinidade, são mais conversados, né (GUA 3).

Um dos aspectos apontados no estudo de Vieira et al. (2010) que comprometem a relação da empresa de segurança com os funcionários é a terceirização, provocando

na equipe de vigilância a sensação de abandono. Segundo os autores, a empresa contratante somente aparece nos setores de trabalho quando ocorrem problemas para punir ou ficar do lado do cliente e, até mesmo, dar ordens que divergem do que os vigilantes receberam do contratante no posto onde atuam, o que os pressiona ainda mais e isso mostra uma visão de que estão 'largados' e que não têm apoio da empresa da qual são funcionários. Karacan (2011) enfatiza que para o bom desempenho nas tarefas de segurança, é preciso de apoio e isso deve ter a atenção das gerências.

4.1.4 Processos de trabalho e relações de gênero

Esta categoria de análise visa identificar e descrever os processos de trabalho e as relações de gênero percebidas pelas vigilantes no contexto do trabalho. O serviço de vigilância é utilizado para prevenir ou reduzir a ocorrência de atos delituosos nas organizações, podendo ser realizados por meios eletrônicos e/ou humanos (Kusther, Binotto, Siqueira, Nogueira & Casarotto, 2010). Baseado na Lei Federal 7.102/1983 e na Portaria 3233/2012 da Policia Federal, a atuação na atividade de segurança visa vigiar, proteger e guardar os bens e imóveis, evitando a ocorrência de riscos diversos. Infere-se que os processos de trabalho da segurança são estabelecidos, principalmente, pelas empresas de vigilância e, de outro lado, pelas empresas contratantes do serviço que acabam por escolher com quem trabalham, além de definirem as atividades a serem executadas.

Vieira et al. (2010) mencionam que há setores que colocam as vigilantes somente em postos que têm a presença de outros vigilantes masculinos, visto que, se atuarem sozinhas, pode fragilizaria a segurança. No entanto, os vigilantes masculinos atuam sozinhos nos postos de trabalho.

4.1.4.1 Processos de trabalho

Esta subcategoria surgiu em função das operações realizadas no dia a dia de trabalho das vigilantes, que consiste em proteger o patrimônio e as pessoas, realizar rondas no setor de trabalho, implementar e fiscalizar as normas estabelecidas, controlar o acesso de pessoas, mercadorias, documentos, veículos e agir em situações que possam gerar danos ao patrimônio, tais como, incêndios, invasões, furtos, roubos e depredações.

A Portaria 3233/2012, que regula as atividades de responsabilidade dos vigilantes, não distingue as atividades para vigilantes masculinos e femininos. As atribuições variam pelas características dos locais onde os vigilantes atuam e, normalmente, são postos de serviço como hospitais, shoppings centers, condomínios, bancos, indústrias, eventos, entre outros. O relato a seguir possibilita uma visão das atividades realizadas pelas vigilantes:

> Faço tudo que o vigilante masculino faz, sem receio. As mulheres hoje lá no meu setor dirigem viatura e se precisar, faz a ronda. Ficam no meio da pista fechando o trânsito e direcionando as locomotivas (GUA 5).

Os dados obtidos mostram que em cada posto de trabalho os processos são diferenciados conforme referenda o estudo de Troit (2015) e que tanto os homens quanto as mulheres os realizam. Outra característica percebida foi que os processos de trabalho são de natureza mais rotineira, não havendo grandes alterações no dia a dia de trabalho. Diogo e Coutinho (2013) apontam que há certa padronização dos serviços a cargo das mulheres em atividades mais rotineiras e para os homens as atividades apresentam potencial de maior risco. Praticamente, inexiste um posto de atuação feminina mais crítico em que a guardiã atua sozinha, sempre em dupla com um vigilante homem.

4.1.4.2 Relações de gênero

Esta subcategoria emergiu das falas das vigilantes quanto à preferência dos clientes pela contratação dos serviços masculinos. Os dados mostraram visões estereotipadas em relação às diferenças de tratamento por parte das chefias em relação às mulheres vigilantes e à visão das vigilantes sobre as relações de gênero em suas atividades.

As relações de gênero perpassam por uma discussão que transcende a divisão sexual do trabalho meramente biológica, envolvendo discussão sobre uma visão de subalternidade dos papéis atribuídos às mulheres em um contexto histórico e cultural (Silva, et al., 2014; Mattos, Cordeiro, Araújo & Almeida, 2015).

As entrevistas apontaram que a maioria das vigilantes acredita ser mais fácil a condição de promoção funcional para o vigilante masculino do que para as guardiãs. Também foi salientado pela maioria das entrevistadas que a influência do cliente nesse aspecto é preponderante. Por não haver diferenças na formação e na legislação que regula a profissão, a discriminação ocorre simplesmente pela escolha das chefias e contratantes, que consideram a segurança uma atividade de risco, portanto, opta-se pelos vigilantes homens em detrimento das vigilantes mulheres. Outro aspecto que foi evidenciado é que as guardiãs, em sua maioria, acreditam que têm condições de realizar as mesmas atividades dos vigilantes masculinos. A visão do gestor da empresa de segurança também corrobora com essa percepção, ilustrada pelo relato a seguir:

> Eu acredito que para muitos tomadores de serviço ainda tem aquela história antiga de que o vigilante tem que ser um 'brutamonte', um guarda-roupa né (risos), como diz no ditado popular aí. Mas hoje sabemos que não é bem assim. Acho que a força está na mente, né, no diálogo. Então, acredito que isso (essa visão) vem diminuindo ao longo do tempo, mas, infelizmente, ainda temos muitos que pensam assim (GES).

O próprio fato de haver setores que não permitem que as guardiãs assumam postos por serem armados demonstra uma diferenciação de gênero em relação às atividades executadas. Percebe-se ainda, que tal resistência ocorre a partir dos gestores, que, normalmente, são homens e não querem contratar mulheres para essas atividades,

acreditando que são atividades que necessitam do uso da força e que, portanto, são mais aptos os perfis masculinos (Oliveira, Brangion & Magalhães, 2011).

Quase a unanimidade das vigilantes entrevistadas afirmou que não se sente inferiorizada em relação aos homens para a realização das atividades, sentindo-se em condições de executarem todas aquelas relativas à função e muitas vezes até com vantagens sobre os vigilantes homens como o relato a seguir aponta:

> Hoje em dia, a segurança não exige só força. Na maioria das vezes, nem exige força. A segurança hoje em dia exige é inteligência, comprometimento, atenção. São coisas que não só homens têm. Qualquer pessoa que se dispor ao trabalho e a adquirir conhecimento é capaz de fazer, principalmente, as mulheres, que, muitas vezes, em algumas situações, tem uma percepção melhor, uma dedicação maior se comparadas aos homens (GUA 4).

Percebe-se por meio dos relatos que as vigilantes acreditam que, para mostrar seu valor, consideram que o trato com as pessoas, a gentileza e a atenção são diferenciais e que tais aspectos são inerentes às guardiãs, porém não sabem dizer o motivo das diferenças nas definições para os postos de trabalho. Arostegui (2015) enfatiza que a presença feminina nas forças de segurança tende a oferecer uma melhoria na eficácia operacional e que estas têm melhores condições de reduzir as tensões, além de menor possibilidade do uso de força excessiva.

Apesar de algumas pesquisadas afirmarem que não percebem falas ou ações que desvalorizem as vigilantes, a maioria citou algum caso que demonstra esta visão preconceituosa, que pode ser explicada pela divisão sexual do trabalho, sendo relegadas a trabalharem em algumas posições de menor risco, se comparadas aos homens.

Para Baylão e Schettino (2014), a discriminação aparece quando o tratamento não é igualitário diante das condições de trabalho que são iguais. Salienta-se que o quantitativo de vigilantes masculinos e femininos nos postos de serviço não pode ser atribuído exclusivamente à empresa de segurança. Ocorre também por definição do cliente tomador de serviço, em função de preconceito, conforme já salientado na fala do gestor da empresa de segurança pesquisado. O relato a seguir confirma essa situação:

> A diferença na contratação eu acho que é mais em função da exigência do lugar. Acho que eles (contratantes) dão mais ênfase para o masculino, porque eu acho que eles imaginam que o homem intimida mais (GUA 8).

Outro aspecto marcante nas respostas das vigilantes prende-se àquilo que Daniel (2011) afirma serem estratégias dos homens, que por meio de ‘brincadeiras’ e ‘piadinhas’, relacionadas à sexualidade no local de trabalho, são marcadas por ‘cantadas’ e ‘convites para sair’. O relato a seguir retrata essa situação:

> Nos postos de trabalho, inclusive chefias, as brincadeiras, piadinhas e até 'cantadas' é o que mais acontece: as pessoas confundem as coisas, acham que a gente é objeto sexual. Hoje em dia você contratar uma guardiã, se ela não for linda, não tiver todo esse perfil, não serve (GUA 9).

Nas entrevistas realizadas, nove das onze vigilantes entrevistadas disseram que já se sentiram assediadas por colegas, supervisores e, principalmente, clientes e visitantes nos postos em que atuam. As estratégias são elogios fora de hora, convites para sair, olhares e atitudes de intimidade. Tal situação confirma a visão de Cruz (2018) de que a opressão de gênero não é um simples aspecto individual, mas tem o caráter coletivo e social.

4.1.5 Mecanismos de defesa

Esta categoria emergiu a partir do objetivo de se analisar e descrever as estratégias de defesa utilizadas pelas vigilantes diante das circunstâncias narradas de desvalorização e discriminação. Desta categoria emergiram duas subcategorias: normas institucionais e mecanismos de enfrentamento.

Para Campos (2019), os mecanismos de defesa são formas inconscientes de proteção do ego em relação a sentimentos difíceis de lidar e que podem gerar algum tipo de conflito, porém, ajudam a enfrentar os desafios. A seguir, apresenta-se relato que mostra a adoção de mecanismo de defesa utilizado pelas vigilantes:

> A gente tem que saber lidar com certos tipos de situação, né. Tem que ter a cabeça fria, concentração, não absorver certos tipos de coisa, para não ficar chateada. Acho que é isso, a própria negação (GUA 10).

Observou-se com base nos dados obtidos que as vigilantes adotam estratégias para lidar com situações de conflito e assédio no ambiente de trabalho. A maioria delas se posicionam com postura da passividade, evitando os conflitos e acreditando que a situação é assim mesmo, naturalizando aparentemente os problemas vivenciados.

4.1.5.1 Normas institucionais

Esta subcategoria evidenciou-se com base nos dados obtidos por meio das entrevistas, em que a maioria das vigilantes alegou a necessidade de se apoiarem nas normas institucionais como forma de justificar suas ações e, assim, buscar evitar os conflitos e tensões inerentes ao contexto do trabalho. Santiago (2013) aponta que uma das formas de defesa utilizadas pelos trabalhadores consiste em às vezes deixar de manifestar o senso crítico para não correr o risco de perder o emprego. Com isso, comportam-se de maneira dependente das normas, protegendo-se no papel e muitas vezes, deixando de ser um sujeito ativo, o que pode ser observado por meio do relato a seguir:

> Eu me senti constrangida e diante do constrangimento, me vi na necessidade dar a resposta para ele que não cabia a mim, ou seja, era norma da empresa (GUA 2).

Percebe-se que o uso das normas da empresa funciona como forma de proteção na realização do trabalho.

4.1.5.2 Mecanismos de enfrentamento

Esta subcategoria emergiu das respostas das vigilantes diante de alguns desafios enfrentados, como o desrespeito, a dupla jornada e situações de assédio que ocorreram em determinadas circunstâncias. A maioria das respondentes apontou para a necessidade de terem que provar sua competência de uma maneira mais intensa que a dos vigilantes masculinos. Yadav e Kiran (2015) salientam a maior probabilidade de estresse das guardas de segurança femininas ocorre em virtude das dificuldades que têm que enfrentar no trabalho. O relato a seguir sintetiza uma das maneiras de enfrentamento utilizadas pelas guardiãs:

> Eu acho que a vigilante feminina tem que se dedicar mais que o vigilante masculino para se destacar, por causa da falta de credibilidade que as pessoas não dão para as guardiãs (GUA 10).

Dois aspectos se destacaram nas respostas das vigilantes: primeiro o de valorizarem os aspectos positivos da mulher em relação aos homens, por exemplo, a atenção e a percepção de detalhes e, segundo a percepção de que precisam se destacar e produzirem no trabalho tão bem ou mais, se comparadas aos homens. Esses comportamentos levam ao respeito e manutenção dos empregos, demonstrando compromisso e profissionalismo que exercem as atividades, além de ressaltarem aspectos que acreditam ser do feminino como diferenciais na atividade de vigilância. O relato do gestor da segurança reforça essa situação:

> A vantagem de ter a mão de obra feminina é a dedicação e a concentração. A mulher consegue, como eu já disse, fazer duas ou três coisas ao mesmo tempo. Isso eu acho que é vantagem. A desvantagem é só mesmo a questão da gravidez. Olhando pelo lado do empresário, eu acho que aí tem uma pequena desvantagem. No mais, é só ganho (GES).

Sobre os comportamentos de assédio, a ação das guardiãs consiste em buscar evitar o assediador, muitas vezes, levando a situação na 'brincadeira'. O fato de estar presente nas organizações, onde a maioria é do gênero masculino, nenhuma das vigilantes alegou como defesa o fato de levar o caso a alguma chefia ou, mesmo, de denunciar o assédio. Isso pode ocorrer por necessidade de manter o emprego.

Em relação ao trabalho doméstico, também considerado como 'dupla jornada', Mattos et al. (2015) reiteram que as questões do lar ainda permanecem, prioritariamente, sob

a responsabilidade das mulheres, o que faz com que elas busquem um equilíbrio entre as atividades na empresa e no lar. O relato a seguir ilustra essa situação:

> Administro a dupla jornada com muita luta, porque não é fácil. É muito desgaste. Eu, por exemplo, tento sempre separar o trabalho da família. Na hora que eu estou no serviço, é meu trabalho. Ali não é família. Não tem que levar eles para lá, meus problemas, nada. É muito cansativo, mas trabalhar 12 x 36 horas, é o que nos dá oportunidade de administrar isso. No dia de folga, dá para você fazer as coisas de casa e ter o seu descanso (GUA 3).

Apesar da maioria das vigilantes serem solteiras, algumas são mães de um filho, o que leva a uma maior dedicação no ambiente do lar. Somente uma das onze entrevistadas salientou não ter obrigações desta natureza. A escala 12 x 36 horas comum na segurança, parece ser também um dos motivos que as levam à fixação e certo crescimento do número de mulheres no setor da segurança, uma vez que permite conciliar a atividade profissional com a do lar.

5. CONSIDERAÇÕES FINAIS

Esta pesquisa atingiu o seu objetivo que consistiu em descrever e analisar as relações de gênero na segurança privada, na percepção das vigilantes (guardiãs), em uma empresa do setor de segurança privada localizada em um estado do sudeste brasileiro.

Em relação à categoria ‘perfil profissional’, a pesquisa revelou que não ficou claro para as vigilantes, além dos critérios estabelecidos pela portaria 3233/12, o perfil definido para a contração destas profissionais, visto que os critérios adicionais em relação a portaria mencionada, são estabelecidos pelos clientes tomadores dos serviços e que existe uma variação de requisitos de cliente para cliente. Em relação ao processo seletivo, este se dá por meio da indicação de funcionários das empresas de vigilância e dos próprios clientes, como também da escola de formação de vigilantes. Posteriormente, os currículos são analisados, seguindo-se a entrevista com o setor de psicologia, gestor operacional e exames médicos, procedimentos que se aplicam tanto para os vigilantes homens quanto para as vigilantes mulheres (guardiãs).

Na categoria ‘desenvolvimento funcional’, identificaram-se diferenças de oportunidades em relação à questão de gênero, evidenciando a dificuldade das guardiãs para ascenderem a funções mais elevadas na hierarquia organizacional (teto de vidro), assim como a ausência de um plano de carreira, o que agrava esta situação.

Há um reconhecimento por parte das vigilantes de que a área de segurança está ficando cada vez mais exigente e de que fatores como o bom atendimento e o trato mais qualificado para com as pessoas são características cada vez mais exigidas. Isso vem dando às mulheres uma maior oportunidade de serem valorizadas, por

acreditarem que apresentam tais habilidades com mais qualidade que os vigilantes homens.

Na categoria ‘condições de trabalho’, observou-se diferenças de tratamento em função do gênero, principalmente, advindas dos supervisores que interagem melhor com os vigilantes homens, constituindo-se motivo de maiores oportunidades de crescimento para estes, em detrimento das vigilantes mulheres, caracterizando-se, portanto, um comportamento discriminatório.

Em relação aos ‘processos de trabalho e relações de gênero’ percebeu-se que não há um padrão definido para a atuação dos vigilantes. Ou seja, os processos ocorrem em cada posto de trabalho e há uma percepção das vigilantes de que na distribuição de tarefas as mulheres são alocadas para a realização de atividades que acreditam não haver maiores riscos físicos. Destaca-se, portanto, que o curso de formação de vigilantes é único em termos de conteúdo para vigilantes homens e vigilantes mulheres. Essa situação faz com que as vigilantes percebam que existe um tratamento discriminatório no trabalho em relação a elas.

Tratando das relações de gênero, os relatos das vigilantes evidenciaram que é uma opção dos clientes a pouca utilização das guardiãs nos postos de trabalho. Portanto, existe uma visão estereotipada em relação ao serviço de segurança, em que a força é um fator preponderante. As vigilantes destacaram que realizam atividades mais ligadas ao receptivo e abordagens em mulheres e crianças. Verificou-se, também, que as promoções para supervisores ou mesmo, cursos de qualificação para outras atividades na empresa são mais direcionadas para os vigilantes homens, havendo, portanto, discriminação. Identificou-se também, a ocorrência de assédio sexual, aspecto marcante nas respostas das vigilantes, principalmente, por parte dos supervisores e contratantes do serviço.

Foi unânime a visão das guardiãs de que acreditam que têm condição para realizar todas as atividades que os vigilantes masculinos realizam e que têm habilidades que as diferenciam positivamente em relação aos vigilantes homens, como percepção apurada, atenção e dedicação. Na estrutura organizacional da empresa pesquisada, nos cargos de liderança, principalmente na área operacional, praticamente inexistem mulheres, o que pode ser explicado pela discriminação.

Na categoria ‘mecanismos de defesa’ os resultados demonstraram que diante dos desafios de preconceitos, brincadeiras, assédio, tensões e conflitos, as vigilantes adotam algumas posturas de defesa ou enfrentamento de situações adversas, tais como a negação e o equilíbrio pessoal, que se apresentaram como alternativas para evitarem uma maior tensão no dia a dia do trabalho. Fazem isso levando as falas e comportamentos como brincadeiras, ou mesmo, desconsiderando tais situações como ofensivas, como estratégia para manutenção do emprego.

Esta pesquisa contribuiu por trazer à discussão a perspectiva do gênero em um campo ainda pouco explorado, que é a segurança privada, contribuindo também ao apontar para as tensões e possíveis adoecimentos que podem advir a partir da vivência em situações adversas experimentadas pelas profissionais femininas com atuação na área da vigilância. No âmbito organizacional, esta pesquisa contribuirá com a empresa pesquisada à medida que possibilitará compreender de forma mais profunda a utilização do trabalho feminino, o que servirá para reflexão em relação a uma melhor utilização e valorização desta mão-de-obra. Assim, poderá reverter em melhores resultados com a aplicação de novas políticas e práticas na área de gestão de pessoas. Em relação ao contexto social, este estudo pode contribuir para reflexões relativas às discriminações que vem ocorrendo em relação à mulher como profissional, a partir do momento em que o conceito da divisão sexual do trabalho passa a ser mais bem reconhecido e enfrentado.

Como limitação e sugestão para a realização de estudos futuros, sugere-se o desenvolvimento de novas pesquisas envolvendo os clientes, tomadores do serviço, levando em consideração que estes, na maioria das situações, são os efetivos gestores do serviço de vigilância e os eu mais propiciam as discriminações identificadas por este estudo.

REFERÊNCIAS

Andrade, L. F. S.; Macedo, A. S., & Oliveira, M. L. S. (2014). A produção científica em gênero no Brasil: um panorama dos grupos de pesquisa de administração. RAM Revista Administração Mackenzie, edição especial, 48-75.

Arostegui, J. L. (2015). Gender and the Security Sector: Towards a More Secure Future. Partnership for Peace Consortium of Defense Academies and Security Studies Institutes. Source: Connections, 14(3), 7-30.

Bardin, L (2016). Análise de conteúdo. Lisboa: Edições 70.

Baylão, A. L. S., & Schettino, L. S. O. (2014). A inserção da mulher no mercado de trabalho brasileiro. Anais do Simpósio de Excelência em Gestão e Tecnologia – SEGET, Rio de Janeiro, RJ, Brasil.

Beauvoir, S. (2008). O segundo sexo. Rio de Janeiro: Nova Fronteira.

Bertrand, M. (2018). The Glass Ceiling. Working paper. The University of Chicago Booth School of Business, 38(1). 1-17.

Bourdieu, P. (2011). Economia das trocas simbólicas (5a ed.). São Paulo: Perspectiva.

Brasil, Ministério da Segurança Pública. (2019). Segurança privada, legislação, normas e orientações. Recuperado de: http://www.pf.gov.br/servicos-pf/seguranca-privada/legislacao-normas-e-orientacoes/leis.pdf.

Calazans, M. E. (2004). Mulheres no policiamento ostensivo e a perspectiva de uma segurança cidadã. São Paulo em Perspectiva, 18(1), 142-150.

Campos, R. C. (2019). O conceito de mecanismos de defesa e a sua avaliação: alguns contributos. Revista Iberoamericana de Diagnóstico y Evaluación e Avaliação Psicológica, 50(1), 149-161.

Campos, R. C., Silva, K. A. T., Miranda, A. R. A., & Cappelle, M. C. A. (2017). Gênero e empoderamento: um estudo sobre mulheres gerentes nas universidades. Revista Latino Americana de Geografia e Gênero, 8(2), 97-115.

Cappelle, M. C. A., Miranda, A. R. A., & Mafra, F. L. N. (2012). Relações de gênero e poder: um estudo com professoras-gerentes em uma universidade pública. Revista Administração em Diálogo, 14(3), 110-136.

Cappelle, M. C. A., & Melo, M. C. O. L. (2010). Mulheres policiais, relações de poder e de gênero na Polícia Militar de Minas Gerais. Revista de Administração Mackenzie, 11(3), 71-99.

Cardeal, C. C., & Ribeiro, L. M. L. (2017). Relações de gênero nas guardas municipais. Revista Brasileira de Segurança Pública, 11(1), 50-72.

Cruz, M. H. S. (2018). Empoderamento das mulheres. Inc. Soc., 11(2), 101-114.

Daniel, C. O (2011). Trabalho e a questão de gênero: a participação de mulheres na dinâmica do trabalho. O Social em Questão, 25(1), 37-55.

Diogo, M. F. (2012). Só tem homem, pera né, eu também quero entrar nesse lugar: reflexões sobre a inserção de mulheres no segmento de vigilância patrimonial privada. (Tese de Doutorado). Programa de Pós-Graduação em Psicologia, Centro de Filosofia e Ciências Humanas, Florianópolis, SC, Brasil.

Diogo, M. F., & Coutinho, M. C. (2013). A inserção de mulheres no segmento de vigilância patrimonial privada: entre conquistas e manutenções. Revista PSICO, 44(3), 421-431.

Drydakis, N., Sidiropoulou, K., Bozani, V., Selmanovic,S., & Patnaik, S. (2017). Masculine vs feminine personality traits and women's employment outcomes in Britain. Bonn/Alemanha: Institute of Labor Economics.

Eichler, M. (2015). Gender and private security in global publics. Oxford University Press, 10(1), 95-117.

Federação Nacional das Empresas de Segurança e Transporte de Valores (2019). VI Estudo do Setor da Segurança Privada. Anais do ESSEG, São Paulo, SP, Brasil. Recuperado de: http://www.fenavist.org.br/essegs.pdf.

Fontanella, B. J. B., Ricas, J., & Turato, E. R. (2008). Amostragem por saturação em pesquisas qualitativas em saúde: contribuições teóricas. Caderno de Saúde Pública, 24(1), 108-131.

Gontijo, M. R., & Melo, M. C. O. L. (2017). Da inserção ao empoderamento: análise da trajetória de diretoras de instituições privadas de ensino superior de Belo Horizonte. REAd, 23(1), 126-157.

Herrera, D. P. (2014). Patriarcado y Feminismo: relaciones de poder y perspectiva de genero. Desestructurando los mandatos de genero de la masculinidad. Revista del CEHIM, 10(1), 179-193.

Karacan, E. (2011). Job satisfaction of private security guards. Kocaeli Üniversitesi Sosyal Bilimler Enstitüsü Dergisi, 22(2). 203-239.

Kusther, E. A., Binotto, E., Siqueira, E. S., Nogueira, M. A. F. S., & Casarotto, E. L. (2010). Inovação tecnológica e suas influências no processo de gestão: uma análise no setor de segurança privada patrimonial. RGO - Revista Gestão Organizacional, 3(1), 103-123.

Leite, T. A. S. (2016). Gestão de riscos na segurança patrimonial: um guia para empresários e consultores. Rio de Janeiro: Qualitymark.

Lima, F. I. A., Voig, A. E. G. T., Feijó, M. R., Camargo, M. L., & Cardoso, H. F. (2017). A influência da construção de papeis sociais de gênero na escolha profissional. Revista Brasileira de Psicologia Educacional, 19(1), 33-50.

Louro, G. L. (1997). Mulheres na sala de aula. In: Del Priori, M. (Org.), História das mulheres no Brasil. São Paulo: Contexto UNESP.

Matos, G. I. (2018). Estudos de gênero e feminismos: uma análise bibliométrica da revista estudos feministas. (Dissertação de Mestrado). Universidade Estadual Paulista, UNESP - Faculdade de Filosofia e Ciências, São Paulo, SP, Brasil.

Mattos, A. I. S.; Cordeiro, T. M. S. C.; Araújo, T. M., & Almeida, M. M. G. (2015). Desigualdades de gênero: uma revisão narrativa. Bahia: Universidade Estadual de Feira de Santana.

Oliveira, D. A., Brangion, A. R., & Magalhães, Y. T. (2011). Representações sociais de gênero no setor de manutenção de uma empresa mineradora. Anais do Encontro Anual da Associação Nacional de Pós-Graduação e Pesquisa em Administração – ENANPAD, Rio de Janeiro, RJ, Brasil. Recuperado de:

Oliveira, B. B., & Woida, L. M. (2018). O Fenômeno glass ceiling e o acesso à informação: estudo sobre barreiras invisíveis impostas às mulheres no trabalho. Complexitas - Rev. Fil. Tem., 3(1), 61-75.

Reis, A. C. P. R. (2013). A influência do feminismo na escolha das mulheres por carreiras tradicionalmente masculinas. Anais do Simpósio de Excelência em Gestão e Tecnologia - SEGET, Resende, RJ, Brasil. Recuperado de:

Ribeiro, A. P. G.; Hirsch, C., Barreto, C.; Fontes, F. L. C.; Freitas, L. R. S., & Zatti, P. C. (2011). Relatório Final Estágio Supervisionado em Saúde Mental e Trabalho. Belo Horizonte: Faculdade de Filosofia e Ciências Humanas do Departamento de Psicologia – UFMG.

Ribeiro, L. (2018). Polícia Militar é lugar de mulher? Revista Estudos Feministas, 11(1), 37-54.

Santiago, E. B. O (2013). Ambiente de trabalho, estratégias de defesas e suas implicações na construção da identidade do trabalhador. Encontro Revista de Psicologia, 16(25), 35-51.

Santos, C. M. M., Tanure, B., & Carvalho, A. M. Neto. (2014). Mulheres executivas brasileiras: o teto de vidro em questão. Revista Administração em Diálogo, 16(3), 56-75.

Silva, J. S. F., Gomes, A. F., Santos, A. A., Santana, W. G. P., Chaves, A. M., & Piau, D. D. N. (2014). Relações de gênero no mundo do trabalho: um estudo com mulheres feirantes no interior da Bahia. Anais do Encontro Anual da Associação Nacional de Pós-Graduação e Pesquisa em Administração – ENANPAD, Rio de Janeiro, RJ, Brasil.

Silva, K. S., & Ferreira, M. L. A. (2016). Trabalho feminino ou trabalho masculino? Uma análise da inserção de mulheres em ocupações consideradas masculinas na cidade de Montes Claros/MG. Revista Alteridade UNIMONTES, 2(1), 96-108.

Sousa, L. P., & Guedes, D. R. (2016). A desigual divisão sexual do trabalho: um olhar sobre a última década. Estudos avançados, 30(87), 108-123.

Stachowitsch, S. (2015). The Reconstruction of Masculinities in Global Politics: Gendering Strategies in the Field of Private Security. Men and Masculinities, 18(3), 363-386.

Trambaioli, F. A. F., & Joviliano, R. D. (2015). A gestão de carreira como ferramenta para o desenvolvimento organizacional. Revista Fafibe On-Line, 8(1), 451- 462.

Troit, D. du. (2015). Working as a security guard on potchefstroom campus: issues, challenges and coping strategies. South African Review of Sociology, 46(2), 97-114.

Vieira, C. E. C.; Lima, F. P. A., & Lima, M. E. A. (2010). O cotidiano dos vigilantes: trabalho, saúde e adoecimento. Belo Horizonte: Fumarc.

Yadav, N., & Kiran, U. V. (2015). Occupational Stress Among Security Guards. Journal for Studies in Management and Planning, 1(7), 113-128.

Zanetic, A. (2009). Segurança privada: características do setor e impactos sobre o policiamento. Revista Brasileira de Segurança Pública, 3(4), 358-389.

NÃO SE FAZ SEGURANÇA COM ATOS E SISTEMAS ISOLADOS: EM DEFESA DE PROFISSIONAIS QUALIFICADOS E DE UMA SEGURANÇA INTEGRADA.

Carlos Alberto Zanandreis da Silveira

Gestor de Segurança, 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 CEAS (Corporacion Euro Americana de Seguridad) em MG.

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 forma que são geridos no dia a dia das empresas. É aí que já começam grandes problemas do processo de gestão de segurança. Muitos tomadores de decisão nas organizações, sejam de que porte forem, é comum ver a segurança não encarada e gerida com uma perspectiva técnica, mas, como algo que qualquer pessoa que não seja especialista possa fazer, partindo dos 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 ainda 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, onde 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 se ter em mente que qualquer decisão em relação a aspectos de segurança deve ter por base um olhar mais amplo, que avalia em primeiro lugar se tais ações são adequadas àquele tipo de organização e seu contexto interno e externo, bem como, também se a empresa tem condições de fazer tal investimento, levando em consideração tudo que ele implica relativo a investimento, profissionais envolvidos, infraestrutura necessária. E um terceiro ponto, não menos importante, ou talvez mais importante, é se tal ação realmente atende à necessidade de mitigação de riscos daquela empresa.

Pode-se inclusive fazer uma analogia de que um remédio pode ser indicado por um médico e ser útil a uma pessoa e não necessariamente ser adequado a outra, ou mesmo a dosagem que precisa ser ajustada a realidade desta. Nesta 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 daquele paciente e assim, possa diagnosticar e indicar o remédio mais adequado, e na medida mais coerente ao tamanho do problema detectado.

Quando se fala em segurança, 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 que há uma série de medidas que necessitam estarem integradas e adequadas. Imagine uma sinfonia onde possa até haver vários instrumentos, mas, cada um toca uma música diferente, ou num tom diferente. Não cumprirá seu papel e será visto 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 que realmente possam atuar no sentido de reduzir os riscos possíveis que precisam de antemão, serem 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 observa 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 que o local tinha um sistema de segurança, muitas vezes considerando como se 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 e inclusive em projetos de lei e ajustes nas legislações vigentes 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 com imagens de baixa qualidade e iluminações inadequadas. Quando das entrevistas e manifestações dos responsáveis destas empresas alegam terem investido em segurança, porém, neste caso especificamente, somente câmeras não impediriam que os crimes se perpetrassem. Se vê 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 e os sistemas de segurança física como portas, janelas, paredes, sejam 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 iniba a atuação da criminalidade. Isso hoje tem se mostrado um ledo engano visto que o cometimento de crimes tem ocorrido a luz do dia e a frente das imagens sem qualquer timidez.

Rodrigues (2009) disserta em seu artigo sobre segurança para escolas, que ao desenvolverem um projeto para cerca de 2000 escolas um problema percebido foi o de instalarem equipamentos de qualidade ruim, não ter havido monitoramento e nem gravação das imagens, além destas (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. Isto 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 darão condições do profissional da segurança apontar os principais riscos e ranquear as prioridades de tratamento daquela empresa. Tudo isso, acompanhando, 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 a 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 ter 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 fazendo 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 juntos atuarem para o resultado esperado. O que adiantaria ter um alarme (segurança eletrônica), se não há ninguém para dar uma resposta efetiva a 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 e não funcionando como um processo preventivo. E a premissa de um sistema de segurança é prevenir para que a ocorrência criminosa, de perda ocorra, e se 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 em 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 e as pessoas que atuam no local deixam portas abertas, ou agem de forma a fragilizar acessos ou acidentes? O que adianta ter os sistemas e eles não “conversarem” e se complementarem entre si? Se vê 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 pensando somente no custo e querem “baratear” os serviços, colocando vigias ou porteiros para fazerem 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 referente a forma que 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 protegendo.

Há ainda a ilusão que somente uma arma irá resolver o problema e temos visto nos noticiários que muitas vezes, a presença de um 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 na 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 a percepção de riscos e com conhecimento amplo sobre negócios e segurança.

As próprias empresas que comercializam produtos e serviços de segurança muitas vezes se 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 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 a 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 da 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 a 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 a organização.

Isso é um alerta, portanto para que as organizações busquem profissionais da 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 as 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.