Edição VIII – 2024

https://www.ceasbrasil.com.br / contato@ceasbrasil.com.br

CEAS - BRASIL

SUMÁRIO

Corporación Euro-Americana de Seguridad
CEAS INTERNACIONAL
CEAS BRASIL

INTRODUÇÃO

Marco Aurélio Alves Pereira, DICS, DIDS, MBA, MBCR, CIEAI, CEGRC, CIGR, CISI, CIAI, MBS, CES.

Preocupado em manter os Gestores de Segurança sempre atualizados com os temas referentes a gestão de riscos e segurança empresarial, a Corporação Euro Americana de Segurança (CEAS) no Brasil, traz a seus associados e parceiros o 8º volume de sua Coletânea de Artigos, repleto de temas de elevada importância ao mundo da Segurança.

O CEAS-Brasil não mede esforços no sentido de suprir as necessidades do mercado brasileiro nessas áreas, estimulando a produção de textos que são devidamente publicados e divulgados a todos os associados e colaboradores através das redes sociais da organização.

Todos sabemos que a segurança patrimonial é essencial para proteger bens, propriedades e recursos de uma organização ou pessoas. Com isso envolvendo a implementação de medidas preventivas, proativas e o uso de tecnologias avançadas para evitar roubos, danos, intrusões, mitigando riscos e além disto trazendo reduções de custos.

A Segurança mostra constantemente várias estratégias e práticas que podem ser adotadas para garantir a as diferentes organizações em seus diferentes segmentos, a segurança mostra-se muito resiliente e adaptável a qualquer cenário empresarial, e os gestores de segurança mostram-se mais audazes e com grande efetividade em suas ações, ganhando cada vez mais espaço frente a alta gestão.

Porém para isso não basta manter se atualizado, é preciso aperfeiçoar-se constantemente e fazer treinamentos segurança patrimonial em todas as áreas, eletrônica, pessoal, cyber crime, gestão empresarial, etc.

Portanto a segurança patrimonial deve ter a preocupação contínua de estar constantemente atualizada. E com isso é fundamental revisar e atualizar as medidas de segurança regularmente para se adaptar a novas ameaças e manter a proteção adequada.

O CEAS no Brasil, proporciona e estimula os profissionais de segurança, a alcançarem os seus resultados com mais embasamento e credibilidade, se observarmos o CEAS Brasil aplica o que o mundo empresarial utiliza em qualquer seguimento, o famoso PDCA (Plan, Do, Check, Act), ou seja melhorar processos e promover a melhoria contínua, sempre aplicando e oferecendo alto nível de capacitação, que reflete diretamente em diversos benefícios a seus colaboradores e associados.

Assim sendo, o nosso nobre Professor Dr. Renato Figueiredo, Presidente da CEAS-BRASIL, Secretário-Geral da CEAS-INTERNACIONAL e Coordenador da CEAS-INTERNACIONAL no âmbito do MERCOSUL, nos presenteia com mais uma coletânea de textos muito bem selecionados e que certamente, irão regularmente promover uma cultura de aprendizado e inovação no cenário da segurança, além de aumentar a nossa eficácia e eficiência, qualidade e competitividade.

Professor Dr. Renato Figueiredo, tenha certeza de que seu trabalho, reforça os valores e a formação dos gestores de segurança.

Aproveito também para cumprimentar a todos os autores que participaram com seus respectivos artigos em mais esta importante coletânea, que irá ser de grande valia ao nosso Grupo do CEAS, bem como à nossa sociedade brasileira de segurança.

Excelente e proveitosa leitura a todos!!!

Sucesso!!!

Marco Aurélio – Delegado CEAS Brasil SP, Sócio Honorário CEAS, Membro do Programa de Proteção das Indústrias do CIESP – Campinas-SP e Membro da ABFIP – Associação Brasileira das Forças de Paz.

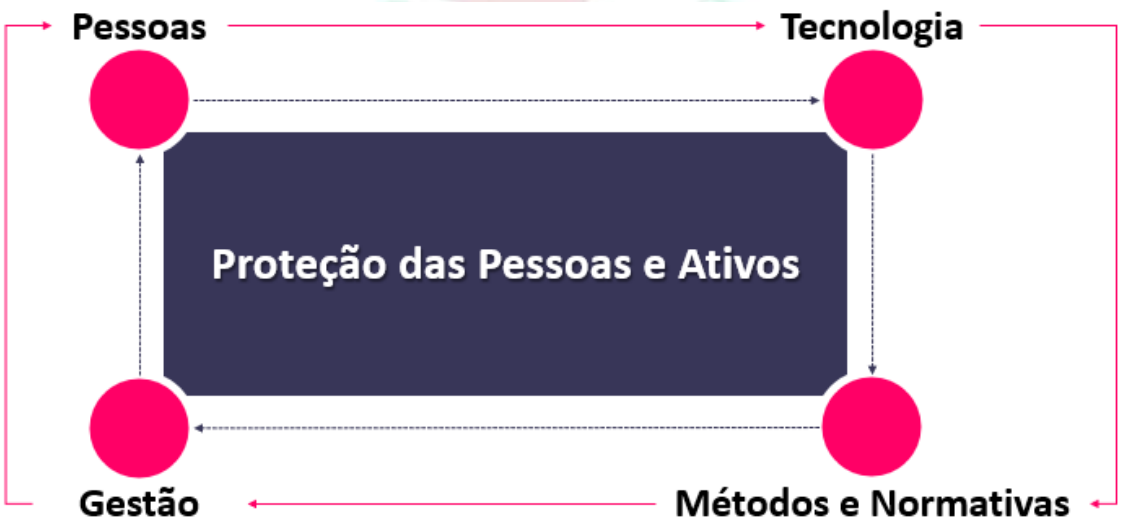
“A IMPORTÂNCIA DO ENDOMARKETING PARA SEGURANÇA EMPRESARIAL”

Anderson Moura, MBS, CPSI, CIGR, CIEIE, EAR, MBA

A Segurança Empresarial, por essência, exige ações burocráticas inerentes a sua atividade, onde por vezes causam ruídos e atritos. Neste contexto, um dos grandes desafios do Gestor de Segurança é o uso eficiente e correto da comunicação, pois quanto mais clara e direta for a mensagem, maior a sua credibilidade e entendimento junto à equipe e demais colaboradores da empresa.

Para adentrar no tema, se faz necessário acrescentar o conceito do Retângulo da Segurança Empresarial. Trata-se da representação visual do processo que visa proteger pessoas e ativos (tangíveis e intangíveis) da empresa.

Imagem - Retângulo da Segurança Empresarial



Percebe-se, nitidamente, a importância das Pessoas no processo de Segurança Empresarial. Sejam elas membros da equipe de segurança, bem como os demais colaboradores próprios e terceirizados da empresa.

Para conscientizar as pessoas é recomendável utilizar de uma ferramenta pouco explorada pelos gestores chamada Endomarketing. Esse recurso dará a correta forma e visibilidade às ações do departamento de Segurança Empresarial. Portanto, o presente artigo de opinião tem como objetivo aprofundar no conceito do Endomarketing apresentando seus benefícios se bem utilizado pelo Gestor de Segurança.

Realizando uma imersão no tema, o termo Endomarketing foi registrado no Brasil em 1996 pelo consultor de empresas o Saul Faingaus Bekin, como resultado da

sua jornada profissional, na época, na média gerência de uma empresa multinacional.

No entendimento de Bekin, o Endomarketing tem como objetivo realizar e facilitar trocas, construindo lealdade no relacionamento das pessoas com seu cliente interno, compartilhando seus objetivos, cativando e cultivando certa harmonia para fortalecer as relações interpessoais e, principalmente, a comunicação interna. O Endomarketing é, portanto, marketing interno ou marketing para dentro da empresa.

Assim, o objetivo do Endomarketing como ferramenta da Segurança Empresarial é criar consciência na organização acerca da visão, missão, procedimentos e métodos da área, transformando e recrutando os colaboradores em facilitadores, reforçando e consolidando a imagem do departamento e, criando valor para área.

Para Albrecht (2004), se os empregados não estão convencidos da qualidade dos serviços prestados por sua empresa e da importância de seus papéis nesta prestação, não há nada na terra que os torne dispostos a vendê-los para seus clientes. Portanto, nenhum colaborador da organização fará uma análise positiva do departamento de Segurança Empresarial e atuará como multiplicador, se não souber o “Porquê” da área (conceitos, objetivos e entregas).

Por vezes, o gestor de segurança não consegue transmitir com clareza o por que faz o que faz. Com o porquê, fica evidente o propósito, causa e crença da área. Por que controla irrestritamente todos os acessos? Por que realiza sistematicamente auditorias de segurança?

É sabido por todos do segmento que a missão de “fazer segurança” não é responsabilidade exclusiva do departamento de Segurança Empresarial e sim de todas as áreas e colaboradores da organização. O uso do Endomarketing é ferramenta fundamental para disseminar, alinhar e atribuir responsabilidade aos colaboradores quando o assunto é segurança. Aqui estamos falando de colaboração direta para o desenvolvimento de uma Cultura de Segurança.

Neste diapasão, a Segurança Empresarial tem oportunidade de seguir os mesmos passos da Segurança do Trabalho, pois é notório que nas últimas décadas houve relevante diminuição nos índices de acidentes de trabalho no Brasil. Deve-se parte desta redução, a disseminação interna de conceitos e técnicas de segurança pelas empresas, utilizando para isso canais, campanhas e instrumentos de comunicação contínuos e marketing interno, ou seja, o Endomarketing.

Especialistas em comunicação recomendam que tanto os colaboradores próprios ou terceirizados sejam atingidos por esforços idênticos de Endomarketing, já que “orbitam” o mesmo ecossistema e devem estar alinhados às políticas, estratégias e diretrizes da empresa. E, ainda, consideram que a informação flui internamente pelos caminhos, à saber: 1. Por meio das Lideranças; e 2. Por meio de canais, instrumentos e ações.

Mais do que simplesmente informar, o Endomarketing serve para disciplinar à direção e as lideranças da empresa para determinadas atitudes de aproximação que possam provocar maiores níveis de participação, incentivo e engajamento nos seus colaboradores.

Não é um processo horizontal, pois não trata do simples repasse da informação entre as pessoas e, sim, entre a empresa e seus colaboradores (próprios e terceirizados).

Por fim, a unificação do comportamento de todos os colaboradores da empresa, o engajamento no cumprimento das diretrizes e a credibilidade do departamento serão os pontos máximos a serem perseguidos pela Segurança Empresarial através de um processo de Endomarketing.

Anderson Moura, MBS, CPSI, CIGR, CIEIE, EAR, MBA

Gestor de Segurança Empresarial

“A IMPORTÂNCIA DAS MEDIDAS DE SEGURANÇA NO AMBIENTE ESCOLAR”

Walter Oliveira, CPSI

Estamos acompanhando nas mídias nos últimos meses diversas notícias sobre ataques a escolas. Conforme estudo feito pela UNICAMP de 2002 até 2023 foi contabilizado aproximadamente 22 atentados a escolas. Em São Paulo uma semana após o atentando a escola Thomazia Montoro, a polícia descobriu através de um trabalho de inteligências 279 ameaças de novos ataques.

Após o atentado que chocou o estado, ficou circulando diversas informações falsas, com o comunicado de possíveis novos ataques, essa corrente tem como objetivo causar pânico na população. Que por sua vez está em estado de choque e se sentindo insegura devido os últimos ocorridos.

É preciso ter cautela na divulgação de informações, temos que checar se ela vem de uma fonte confiável, pois podemos de forma involuntária estar compartilhando informações Fakes, e contribuindo de forma negativa para o estado de pânico da população.

Essa sensação de insegurança fez com que os movimentos políticos se manifestassem com projetos de leis que propõe segurança armada nas escolas, psicólogos, e o videomonitoramento. Esses projetos emergem da necessidade do sentimento de segurança.

Para entender os riscos e perigos de uma unidade escolar temos que saber a diferença entre Risco e Perigo;

Perigo: É um atributo de um objeto ou atividade que tem o potencial para causar danos ou perdas.

Risco: Está relacionado a probabilidade ou chances de um dano ou uma perda ocorrer.

Vamos supor que em uma unidade escolar tenha alguns casos de Covid 19, e por conta disso a escola recomenda que todos os alunos utilizem máscara. Neste caso a Covid 19 é o perigo. Ir sem máscara para escola é o risco. Pois as chances de se contaminar indo sem máscara é maior do ele indo de máscara. A ação da escola de orientar os alunos a usarem máscara é a prevenção para minimizar ou evitar o risco de contaminação.

As possibilidades de perigo e riscos em um ambiente escolar são diversas e se analisarmos os impactos que ele pode trazer, são sempre catastróficas.

Uma invasão, Assalto, Sequestro ou ataques, em uma escola é um evento trágico. Ele pode trazer danos a integridade dos alunos, professores e funcionários. Afetar a imagem da instituição e causa pânicos nos pais e responsáveis.

Os riscos expostos acima podem ser minimizados ou evitados seguindo um padrão de medidas, soluções, procedimentos e regras de comportamentos.

MEDIDAS DE SEGURANÇA

O investimento em segurança pode ser um fator importante para ajudar a minimizar os riscos em uma unidade escolar;

Segurança Perimetral: A unidade escolar deve conter em seu perímetro, muros altos com alguma barreira que impeça a invasão de pessoas indesejadas.

Segurança Eletrônica: Recomendamos que a unidade tenha câmeras de segurança em locais estratégicos e com monitoramento efetivo, com objetivo de garantir a visualização em tempo real de tudo que ocorre na parte interna e externa da escola. Assim como em seu perímetro, sensores, botão de pânico são equipamentos indispensáveis.

Segurança Física: Sou a favor da presença do vigilante de forma desarmada nas unidades escolares, com objetivo de realizar a vigilância da unidade, assim como o seu senso de segurança pode colaborar para identificar ações incomuns de alunos ou funcionários do colégio. A implantação de Catracas é fundamental para o controle de acesso.

MEDIDAS PEDAGÓGICAS

Pauta Pedagógica: Inserir nas pautas pedagógicas o assunto segurança.

Comitê de Segurança: Criar um comitê de segurança, justamente para falar sobre a segurança nas escolas. Importante que tenha um especialista em segurança que possa liderar e conduzir as ações de segurança.

Plano de emergência: Por mais que esteja tudo sobe controle é fundamental estar preparados para emergências. Com isso é necessário ter um plano de contingência, para os mais diversos problemas. Treine as equipes, faça simulados, crie rotas de fuga entre outras ações que sem dúvidas vão fazer toda diferença para segurança escolar.

REGRAS DE COMPORTAMENTOS

Conscientização dos Pais: Importante que as escolas através dos professores, monitores e psicólogos, conscientizem os pais ou responsável a monitorar o celular de seus filhos as redes sociais e as companhias, amizades e colegas. Importante deixar claro para os pais e responsáveis que a escola e responsável por alfabetizar, mas quem tem o trabalho de educar são os pais ou responsáveis.

Psicólogos nas Escolas: A implantação de psicólogos nas escolas pode contribuir para uma análise mais detalhada do perfil de cada aluno e integrante das unidades escolares. Estamos em uma época diferente, aonde as crianças e os adolescentes passam boa parte do tempo em celulares e computadores, em

uma era aonde o bullying está cada vez mais presente na vida dos jovens, com isso cuidar da saudade mental deles é fundamental.

CONSIDERAÇÕES FINAIS

Todo local aonde possui um grande fluxo de movimentação está exposto a uma série de vulnerabilidades. As escolas são locais vulneráveis pois lá estão diversas crianças e adolescentes, que são os bens mais preciosas para suas famílias.

Garantir o bem estar e a segurança dos alunos e funcionários é o grande desafio das unidades de ensino. Investir em medidas de segurança é fundamental. Prevenção e segurança devem ser vistos como uma ação de acolhimento, e de liberdade no ambiente escolar, com objetivo de permitir um desenvolvimento saudável a todos os alunos e tranquilidade aos pais e responsáveis.

Referencias:

https://www.educacao.sp.gov.br/governo-de-sp-anuncia-pacote-com-politicas-publicas-para-ampliar-seguranca-nas-escolas-em-todo-estado/

https://www.bbc.com/portuguese/articles/ckryl4epnpeo

https://www.ibragesp.com.br/

Walter Oliveira, CPSI| Gestor de Operações

Formado em Gestão de Segurança Privada pela Cruzeiro do Sul Com MBA em Gestão Empresarial Pela Unip. Possui a Certificação CPSI (CERTIFICADO PROFESIONAL DE SEGURIDAD INTERNACIONAL) Instrutor de treinamento Credenciado pela Polícia federal, Grande experiência em prestação de serviços, atuando em grandes empresas, com expertise em diversos seguimentos.

“O ALINHAMENTO ESTRATÉGICO NA OPERACIONALIZAÇÃO DO SERVIÇO DE SEGURANÇA PATRIMONIAL”

Ronilson Silva

RESUMO

O presente artigo retrata algo de suma importância para obter a eficácia na operacionalização dos serviços de segurança patrimonial prestado nas organizações, o alinhamento estratégico que vem como forma de uniformizar as ações seja de contratante ou contratada todos tendo uma visão uniforme do processo, a implantação e operacionalização desta ferramenta no âmbito de prestação de serviços de segurança patrimonial contribui para que a empresa contratante alcance seu objetivos e anseios operacionais e institucionais no quesito segurança, quando a empresa contratada ou terceirizada tem o conhecimento dos anseios estratégicos da empresa contratante torna-se mais fácil de elaborar uma estratégia de recrutamento e ir ao mercado já com um perfil de profissional definido e com a ciência de que o serviço de segurança patrimonial será prestado de maneira eficiente e tal serviço de maneira indireta irá assegurar não só a continuidade do negócio como também o alcance dos objetivos traçados, a operacionalização do serviço de segurança patrimonial sem que as estratégias e objetivos de ambas as partes estejam alinhadas, tende ao fracasso,

1. PALAVRAS CHAVE: alinhamento, contratante, informação, segurança.

INTRODUÇÃO

O que a segurança deve proteger? Essa reflexão é o ponto inicial para qualquer plano de proteção, segundo Tinoco (2020). Saber o que proteger em cada negócio é a primeira pergunta, pois há diferença na proteção de uma mina de ouro, de um grande evento ou de uma loja de varejo. Apesar de tudo ser segurança, cada negócio tem sua característica própria que exigirá um sistema de segurança aderente às suas necessidades

De acordo com Barros (2017), o alinhamento estratégico consiste num ajuste entre diversos aspectos organizacionais que contribuem para a implantação efetiva da estratégia. Uma calibragem entre elementos variáveis específicos da organização, de forma que eles viabilizem (ou não inibam) a implementação da estratégia, e potencializem os resultados esperados.

Para Aladim (2017), a maioria das prestações de serviço exige que tenha interação entre o cliente e o prestador de serviços, e essa interação deve ser realizada de forma única, já que cada demanda é singular.

Ou seja, um alinhamento ou um único objetivo sendo levado ao conhecimento de todos os níveis setoriais de uma organização a fim de que todos os

colaboradores sejam parte desta engrenagem criada para mover a máquina empresarial ao alcance de seus objetivos.
É aí que entra a segurança privada, pois tal atividade não se enquadra nem no início e nem no fim do negócio, e sim como atividade meio, isto é, dando o suporte para que todos os objetivos propostos sejam alcançados.

De acordo com Bassi e Monteiro (2017), os sistemas de segurança e seu planejamento são essenciais para as empresas. E, para que sejam funcionais, é necessário que haja uma sintonia entre eles e os propósitos organizacionais. Sem alinhamento, corre-se o risco de se construir uma ilha dentro da empresa, ou seja, de isolar o setor, o que seria ruim do ponto de vista estratégico, pois a empresa é um sistema e, como tal, se torna iminente a busca da inter-relação entre suas partes.

Por tudo isto torna-se necessário que o assunto alinhamento estratégico e a operacionalização dos serviços de segurança privada seja aprofundado e discutido nesse artigo que buscará responder à seguinte questão: qual a relação sobre o alinhamento entre a área estratégica da empresa contratante e a área estratégica da empresa prestadora de serviços de segurança patrimonial (contratada) para a tomada de decisão e alcance dos objetivos propostos em planejamento ou propostos também em contrato?

O objetivo geral desse estudo é verificar a participação ou não do setor de segurança nos momentos de tomada de decisão de uma organização.
Os objetivos específicos são: identificar os níveis setoriais de uma organização contratante, identificar como é a relação entre os setores estratégicos da empresa contratante e da empresa contratada, identificar a participação do setor de segurança na tomada de decisão...

Analisando este cenário de alinhamento de estratégias entre contratado (terceirizada) e tomadora de serviços, surgem vários *gaps*, resultantes do desencontro ou desconhecimento das informações voltadas para a estratégia de alcance de objetivos finais propostos pelo setor estratégico da empresa contratante, tomadora de serviços.

A metodologia utilizada para a construção desse estudo se deu através de pesquisas bibliográficas sobre o assunto e pesquisa qualitativa na qual foram realizadas entrevistas semiestruturadas, visitas técnicas com observação não participante e pesquisa documental sobre contratos de prestação de serviço de segurança terceirizados e sobre os objetivos contratuais dispostos nos mesmos. Para análise dos dados foi utilizada a análise temática.

A partir da observação de níveis táticos e operacional de uma empresa de segurança privada, percebeu-se a existência de alguns *gaps* que tem dificultado à efetividade e o alcance dos objetivos traçados pelo setor de prestação de serviços de segurança nas organizações. A experiência operacional aliada aos conhecimentos estratégicos e táticos sobre o cenário que envolve a prestação dos serviços de segurança trouxe uma visão macro de todo o processo, o que permitiu perceber a importância de se planejar ações que resultem em um alinhamento de estratégias que possa abranger todos os níveis da organização

contratante e também da contratada. Essa foi a motivação para o desenvolvimento desse estudo.
O estudo irá contribuir norteando o entendimento sobre a as consequências oriundas da falha de alinhamento nas informações entre a empresa contratada e a empresa contratante, pois tal falha prejudica os setores responsáveis a buscar meios de disseminação das informações de forma estratégica para todos os setores da organização e, por ouro lado, o alinhamento quando buscado permite que diferentes setores sejam terceirizados, orgânicos ou trabalhem em conjunto.

O presente trabalho está dividido em seções da seguinte maneira: primeiro serão apresentados os objetivos, justificativa, problema, metodologia e contribuição que será construída como resultado do estudo. Em segundo, será apresentada a fundamentação teórica aprofundando-se sobre alinhamento estratégico e as práticas de execução do serviço de segurança patrimonial. Posteriormente, será apresentada a metodologia com as ferramentas que foram utilizadas. Em seguida, serão apresentados e discutidos os resultados alcançados. E, por fim, apresentar-se-ão as considerações finais e referências.

2. FUNDAMENTAÇÃO TEÓRICA

Para Rodrigues (2015), a necessidade de as organizações promoverem o alinhamento de suas estratégias com os processos internos e os externos torna-se cada dia mais iminente configurando como uma necessidade crescente. Além disso, a informação deve ser integrada aos produtos, serviços e, principalmente, às decisões. Essa integração torna-se função vital da gestão de qualquer empresa. Não há gestão possível sem informação.

2.1 Planejamento Estratégico

Para Ribeiro (2021), o Planejamento Estratégico se trata do processo de gerenciamento usado para criar um plano de como atingir um objetivo ou metas. Com ele, pode-se criar na empresa uma visão de médio e longo prazo. Serve para identificar as etapas ou que serão usadas para a empresa atingir seus objetivos, podendo se em todo o negócio ou em áreas específicas (marketing, retenção de clientes, lançamento de produtor, e outros).

Já para Barreto (2015), entende-se que o Planejamento Estratégico é apontado como uma ferramenta de gestão, sendo um dos pontos essenciais para adequar problemas encontrados nas organizações. Ele aponta as medidas positivas que uma empresa deve tomar para enfrentar ameaças e aproveitar as oportunidades encontradas em seu ambiente. Neste sentido, justifica-se avaliar a maneira como ele é implementado dentro das empresas para atestar sua eficácia e salientar os aspectos que o recomendam, especificamente apontar tais resultados quando aplicados em empresas de pequeno porte, pois estas em especial, por não possuírem muitas vezes uma equipe de gestores com acesso a informações mais especializadas acabam por não ter uma boa continuidade no mercado.

Conforme Valentin (2019), o planejamento estratégico é divido em três níveis são eles estratégico, tático e operacional, o nível estratégico fixa a natureza de

uma organização definem missão, visão e valores da organização, compete aos cargos com alta responsabilidade e alta administração, o nível tático se refere aos cargos de executivos de diretoria e gerencia de media responsabilidade, que gerenciam os recursos disponibilizados visando atingir os planos, projetos e ações definidos pelo nível estratégico, e o nível operacional visa otimizar as operações elaborando procedimentos que irão contribuir para que os objetivos e planejamentos estratégicos e táticos sejam implantados e executados de maneira que os objetivos sejam alcançados.

Ainda de acordo com Souza (2007), em um cenário de maior notoriedade dos micros e pequenos empreendimentos, ou melhor, conforme a terminologia usual sugere “micro e pequenas empresas” o planejamento estratégico começa, ainda que timidamente, a ser realizado como processo contínuo de interação entre empresa e ambiente, fato justificado em parte pela complexidade, abrangência e qualificação exigidas dos empreendedores-gestores.

Para Chiavenato (2004), o planejamento estratégico se trata de um processo essencial dentro das organizações por que traça diretrizes para o estabelecimento dos planos de ação que resultarão em vantagem competitiva. Ele identifica os recursos potenciais, reconhece fraquezas e estabelece um conjunto de medidas integradas a serem implementadas assegurando o sucesso dos resultados planejados. Ele somente atinge sua eficácia máxima quando entendido e realizado por todas as pessoas da organização em um mutirão permanente organizado e orquestrado.

Nota-se a grande relação da implantação e execução do planejamento estratégico com o cuidado e qualidade das informações pois decisões de suma importância para o desempenho competitivo da organização serão elaboradas a partir de informações que deverão ser de extrema fidelidade ao cenário atual seja de natureza interna ou externa, seja na análise de mercado ou analisando as próprias forças e fraquezas de uma organização.

Nos dias atuais tem se tornado eminente a existência da necessidade de se alinhar operacionalização dos serviços de segurança a alguns pontos que são característicos de cada empresa e são ligados às evidências que comprovam, por exemplo, o motivo da existência da missão, visão e valores da empresa.

Conforme Carvalho e Santos (2016), os conceitos de planejamento estratégico enfatizam a elaboração das diretrizes organizacionais. A missão, como sendo a razão de ser da empresa; a visão, concretizada como o direcionamento e os valores, considerados como os padrões para o comportamento das pessoas na organização.

Nos tempos atuais, as empresas tem tido como ativo mais valioso a informação como engrenagem para impulsionar objetivos assim como um motor que, para seu perfeito funcionamento, tem uma central que emite informações que fazem com que cada compartimento se comunique com o outro e que ajam juntos para assim impulsionar o motor.

No mundo corporativo essa informação chega a cada componente, sistema ou setor de uma empresa como um norte ou um plano, ou ainda como estratégia para ser executada ou implementada operacionalização cotidiana. Mas, para que a execução seja eficiente e cumpra o seu proposto é necessário um pouco mais de aprofundamento sobre o assunto estratégia.

2.2 Gestão Estratégica e a Tomada de Decisões

Conforme Estevão (1998) o conceito de estratégia está ligado a qualquer processo de tomada de decisões que afete toda a organização por um prazo temporal dilatado; constitui, assim, um conjunto de decisões e de ações que têm por finalidade assegurar a coerência interna e externa da organização, mobilizando todos os seus recursos.

Já para Nicolau (2001), a concepção predominante na literatura entende que a estratégia é um processo que se desenvolve através de uma série de etapas sequenciais, racionais e analíticas e envolve um conjunto de critérios objetivos baseados na racionalidade econômica para auxiliar os gestores na análise das alternativas estratégicas e tomada de decisão.

Em outras palavras, a estratégia surge como demonstração de intenção e definição de meios que irão de acordo com esta, que tem como objeto final o alcance de objetivos traçados e propostos, que podem ser, em alguns casos, a execução do serviço de segurança privada; este objetivo proposto passa por um suporte para que não haja nenhuma objeção ou discordância que possa dificultar ou atrapalhar o alcance dos objetivos.

Ou seja, a estratégia estabelecida ou elaborada tendo esses três fatores preponderantes em sua elaboração permite que a organização dispute e se lance no mercado relacionado ao seu segmento se atualizando e se adaptando às inovações e a volatilidade do mundo atual, sempre mantendo sua essência ou originalidade o que certamente irá forjar sua identidade, em uma visão macro do mercado essa organização será conhecida pelo seu padrão que é visível e relacionado à sua marca.

Ainda de acordo com Cançado (2016), a gestão estratégica é característica de uma esfera privada, onde as relações de poder são institucionalizadas e é muito claro para os participantes seu papel no contexto organizacional. Pode-se argumentar que pode existir hierarquia na esfera pública, porém, quando isto acontece há a apropriação do público pelo privado e a esfera pública se torna uma esfera privada, pois para que a esfera seja realmente pública, ela deve ser o espaço para que as pessoas privadas se inter-relacionem em igualdade de condições. Não estamos considerando aqui representação como hierarquia, podem haver representantes na esfera pública, mas eles devem ser passíveis de serem substituídos pelo desejo do público, o que não acontece na esfera privada.

Conforme Aranha (2020), o gestor de segurança, seja contratante ou contratado, é o responsável em mitigar os riscos da empresa, protegendo pessoas e bens, tangíveis e intangíveis. O sucesso da gestão está relacionado ao engajamento

entre esses profissionais, que com análise conjunta, irão tomar as melhores decisões para a organização.
Contudo deve se levar em consideração também as peculiaridades existentes na execução do serviço de segurança privada principalmente a regulamentação do serviço tal como direitos, deveres e outros pontos que certamente ou na maioria das vezes vão na contramão dos anseios de muitos empresários que necessitam da prestação de tal serviço.

Ou seja, na visão de Moraes (2005), o domínio da informação sempre teve fundamental importância para as corporações do ponto de vista estratégico e empresarial. Dispor da informação correta, na hora adequada, significa tomar uma decisão de forma ágil e eficiente. Com a evolução dos sistemas de informação, ganhou-se mobilidade, inteligência e real capacidade de gestão. A informação é substrato da inteligência competitiva e deve ser administrada em seus particulares, diferenciada e salvaguardada. Ela funciona como um recurso essencial para a definição de estratégias alternativas e para a constituição de uma organização flexível, onde o aprendizado é constante.

Já o mercado de segurança privada tem se tornado cada dia mais exigente e taxativo quanto às atribuições do vigilante, pois cada vez mais as organizações definem sua necessidade em ter não só alguém para lhe fornecer segurança ou sensação de segurança, e sim uma pessoa que em casos de necessidade atuam também em outras pontas como, por exemplo, orientando, fiscalizando e executando normativos internos das organizações, normativos esses que às vezes foge do contexto segurança.

De acordo com o exposto em Portaria Nº 3.233/2012, no art.163 parágrafo 3°, cabe ao vigilante, no exercício de suas funções, o exato cumprimento de seus deveres traduzindo-se na fiel observância das normas estabelecidas pelo órgão fiscalizador (Polícia Federal), bem como também adotar conduta de retidão e lealdade profissional para com a empresa que o empregar e aquela que de seu serviço utilizar, informando prontamente seu superior imediato qualquer irregularidade que puder resultar em responsabilidade administrativa da empresa (BRASIL, 2012). É importante ressaltar o dever de disciplina consciente no tocante ao cumprimento de seus deveres e comprometimento profissional, independentemente de fiscalização.

Para Moretti (2020), os executivos das grandes organizações sabem que pessoas bem preparadas passam uma imagem de empresa séria, bem administrada e gera confiança aos clientes, além da diferenciação entre concorrentes, principalmente quando se trata da aplicação de tecnologia em segurança e qualificação de versatilidade.

Estes fatores também transmitem uma sensação de facilidade em assimilar os normativos e estratégias que constantemente passam por revisões.

De acordo com Minelli (2017), a disseminação dessas informações deve ser feita de acordo com as políticas internas da organização. Muitas vezes os problemas de pertencimento acontecem, pois os empregados não se identificam com essas políticas. Por isso, o ideal é que essas políticas já sejam reveladas ainda durante

os processos seletivos e de contratação. Mostrar sempre aos empregados suas responsabilidades e o papel deles dentro da empresa, o quão relevante eles são para o desenvolvimento e crescimento da companhia.

E quando entendemos a necessidade e os resultados benéficos que o alinhamento das informações de uma maneira macro, seja empresa terceira ou contratante, surge a necessidade de se evidenciar como de fato estes resultados tem sido construídos; e para que isso seja possível, deve-se acompanhar o processo de perto, utilizando várias metodologias, sendo uma delas bastante eficaz, o *Balanced Scorcard* (BSC).

Para Galas (2006), o BSC é uma ferramenta ou instrumento de gestão que possibilita o alinhamento da organização com a estratégia empresarial, a TI como um fator crítico de sucesso para o desempenho competitivo das organizações e o alinhamento da TI com o negócio da empresa como um importante fator de alavancagem do desempenho organizacional.

Contudo a eficácia na utilização desta ferramenta demanda de um conhecimento aprofundado dos processos da organização privada e (ou) terceirizada em todos os níveis, sendo estratégico, operacional e tático, é esse conhecimento que irá munir o gestor com informações que irão preencher cada etapa do BSC.

2.3 Alinhamento Estratégico e prestação de Serviços de Segurança Privada

De acordo com Torres (2010), a informação passou a ser o eixo central das empresas a partir das últimas décadas do século XX. Para alcançar o sucesso competitivo, as organizações precisam cumprir novas exigências no ambiente da informação. Investir, gerenciar e explorar o conhecimento passou a ser um fator crítico de desenvolvimento.

Para Barros (2017), o alinhamento estratégico se define como um ajuste entre diversos aspectos organizacionais que contribuem para a implantação efetiva da estratégia. Uma calibragem entre elementos variáveis específicos da organização, de forma que eles viabilizem (ou não inibam) a implementação da estratégia, e potencializem os resultados esperados.

Conforme Meira (2021), O alinhamento estratégico, possibilita que possamos utilizar tais informações para que seja possível a implementação do planejamento estratégico e que este planejamento atinja todo os níveis da organização. Assim, se o que for definido no planejamento estratégico for observado e cumprido por todos os estágios e níveis em uma organização, haverá o alinhamento.

Ainda conforme Meira (2021), garantir o alinhamento estratégico a partir do planejamento estratégico, consiste em um aspecto fundamental da gestão estratégica, com vista a alcançar os resultados pretendidos por uma organização.

Como dito em tópico anterior, a execução e implantação do planejamento estratégico segue diretamente ligada às estruturas e técnicas de

operacionalização do BSC, Balanced Scorecard, por tanto para que haja eficácia na implantação do planejamento estratégico é necessário que se conheça a fundo todo o aspecto de funcionalidade e montagem do BSC.

Para Cordeiro (2005), apesar do seu caráter prescritivo, o Balanced Scorecard pode ser utilizado para descrever as relações entre algumas variáveis chaves da gestão estratégica e consequentemente analisar a estratégia e o processo de gestão estratégica de uma organização. Neste caso, seu foco principal são os fatores que podem ser medidos por meio de indicadores, como o desempenho de processos, percentuais de satisfação de clientes e resultados de pesquisas de clima organizacional. Por outro lado, alguns fatores críticos para a gestão estratégica como estrutura e cultura organizacionais e alguns outros recursos, tangíveis e intangíveis, que não podem ser medidos numericamente, acabam não sendo contemplados diretamente por essa abordagem. Além disso, permanece uma tendência à implementação de uma estratégia previamente escolhida sob uma perspectiva “de fora para dentro”, apoiada na utilização de relações de causa e efeito lineares (não sistêmicas).

É importante ressaltar que o objeto de estudo desse artigo não se direciona somente à prestação de serviços de segurança terceirizado; o presente estudo visa abranger todo setor de segurança presente nas organizações sejam eles prestados por empresas terceiras ou também as organizações que possuem um serviço de segurança orgânico.

Para Oliveira (2004), os serviços de segurança privada configuram despesas diretas para os contratantes, ou seja, geralmente podem ser caracterizadas como um insumo que participa indiretamente do processo de produção de bens e serviços, sem deixar, no entanto, de ser crucial. Sua importância está em garantir o respeito aos direitos de propriedade privada adquiridos, sustentando as relações econômicas entre os agentes.

Conforme o site gestaodesegurançaprivada.com, o conceito de Segurança Orgânica se resume na pessoa jurídica de direito privado autorizada a constituir um setor próprio de vigilância patrimonial ou de transporte de valores, nos termos da Lei Nº 7.102, de 20 de junho de 1983. Refere-se ao conjunto de ações e medidas de segurança realizadas por recursos humanos da própria instituição, cuja finalidade é a proteção e salvaguarda das pessoas, bens, valores, áreas e instalações de uma empresa.

Nota-se então que a segurança independente se orgânica ou terceirizada tem um papel muito importante na continuidade do negócio, como citado anteriormente nesse artigo o setor serve de sustentação ou suporte para o perfeito funcionamento e concretização de objetivos de todos os setores de uma organização.

Essa afirmação salienta ainda mais a iminência da necessidade e importância do alinhamento estratégico para o sucesso de uma organização em todos os níveis setoriais inclusive na segurança e na operacionalização de seus serviços.

Os gestores de segurança das organizações sejam eles orgânicos ou dedicados pela empresa terceira para aquele posto, devem estar presentes e participar da elaboração das diretrizes da organização, também das tomadas de decisões da organização, a fim de se inteirar quantos aos objetivos traçados pela organização e assim se ajustar e instruir a sua equipe quanto à maneira de execução do serviço de segurança tendo como norte as diretrizes e objetivos propostos pelo tomador de serviço.

Conforme Barros (2017), outro fator importante na eficácia da implementação das estratégias, relacionado às pessoas nas organizações, além do acesso às informações, é a questão do poder. Os líderes encarregados de conduzir o processo dependem cada vez mais dos subordinados, e podem se utilizar do poder formal, concedido pela autoridade de seu cargo.

É de extrema importância que a execução de tal serviço não tenha nenhum tipo de interferência no andamento do negócio principal em execução na organização. Contudo, estas interferências ou *gaps* e falhas consequentemente surgem fruto do não conhecimento das diretrizes da organização a qual se presta o serviço de segurança patrimonial.

Segundo Kutsher (2009), os elementos denominados Tecnologia da Informação e Comunicação (TIC) são os recursos de informação que a organização possui para adquirir dados operacionais, internos e externos, dos quais, a organização utiliza na produção de conhecimento, de modo a facilitar a tomada de decisão. Estes dados, informação e conhecimento devem ser compartilhados dentro do sistema organizacional para que surtam os efeitos esperados. De modo geral, a tecnologia da informação e comunicação é aquela que os colaboradores de uma organização dispõem para adquirir, tratar, processar e comunicar informação.

3. METODOLOGIA

Para Oliveira (2011), metodologia literalmente diz respeito ao estudo sistemático e lógico dos métodos empregados nas ciências, seus fundamentos, sua validade e sua relação com as teorias científicas. Apesar de utilizar procedimentos que variem de uma área da ciência para outra, por exemplo, da área de exatas para a área de humanas - diferenciadas por seus distintos objetos de estudo, consegue-se determinar alguns elementos que diferenciam o método científico de outros métodos (filosófico e algoritmo, matemático etc.).

Como metodologia para estruturar esse estudo foi realizado um levantamento de dados, no qual utilizou-se de uma abordagem qualitativa, por meio de questionários aplicados aos profissionais ligados a gestão de empresas, do âmbito de tomadoras de serviço e também do âmbito de prestadora de serviços (terceirizadas),

Além disso, a fim de buscar de forma mais aprofundada o que fica exposto e acordado nos contratos de prestação de serviços de segurança privada patrimonial, foi realizado análise de documentos por meio da análise de conteúdo.

Análise de conteúdo, segundo Bardin (2016), é um método muito empírico dependente do tipo de fala a que se dedica e do tipo de interpretação que se pretende como objetivo. Não existe coisa pronta em análise de conteúdo, mais somente algumas regras de base por vezes dificilmente transponíveis. A técnica de análise de conteúdo adequada ao domínio e ao objetivo pretendido tem que ser reinventada a cada momento, exceto para usos simples e generalizados como é o caso de escrutínio próximos da decodificação e de respostas á perguntas abertas de questionários cujo conteúdo é avaliado rapidamente por temas.

Devido a pouca exposição de informações relacionadas às normas contratuais, o que é um conjunto de informações confidenciais, analisou-se um único contrato do qual se obteve um norte quanto ao modelo contratual de prestação de serviços de segurança patrimonial privada. Entretanto, o contrato analisado tem algumas peculiaridades por se tratar de um contrato de prestação de serviços de segurança patrimonial para uma instituição pública, que tornou ainda mais interessante o estudo.

Na próxima etapa teremos de fato a exposição de tais dados garimpados, e então teremos também o parecer de pessoas ligadas a todo o processo de alinhamento e estratégico.

4. APRESENTAÇÃO E DISCUSSÃO DOS RESULTADOS

Um dos objetivos deste estudo foi identificar os níveis setoriais de uma organização, realizou-se um levantamento de informações em livros e artigos voltados para o assunto cerne deste objeto de pesquisa.

Conforme Valentin (2019), o planejamento estratégico é divido em três níveis são eles estratégico, tático e operacional, o nível estratégico fixa a natureza de uma organização definem missão, visão e valores da organização, compete aos cargos com alta responsabilidade e alta administração, o nível tático se refere aos cargos de executivos de diretoria e gerencia de media responsabilidade, que gerenciam os recursos disponibilizados visando atingir os planos, projetos e ações definidos pelo nível estratégico, e o nível operacional visa otimizar as operações elaborando procedimentos que irão contribuir para que os objetivos e planejamentos estratégicos e táticos sejam implantados e executados de maneira que os objetivos sejam alcançados.

Cada setor de uma organização está enquadrado dentro de um desses níveis é esta identificação que possibilita as ações hierárquicas que permitem o planejamento, definição, responsabilização e operacionalização das ações.

Dentre os profissionais que responderam ao questionário, constatou-se que não existe este elo de ligação quando falamos de alinhar e disseminar as informações entre os níveis estratégicos de ambas as partes, cabe ressaltar que o profissional de segurança que atua na ponta da linha, dedicado ao setor contratante tem acesso a tais informações, porém de forma sucateada e restrita, ou seja, a informação e a estratégia traçadas pelo setor estratégico das empresas contratantes passam por um tratamento e, às vezes chega ao receptor

final sem riqueza de detalhes ou, em outras vezes, o profissional nem toma conhecimento dessas estratégias, o que tem gerado barreiras que tem resultado na ineficácia da operacionalização do serviço.

Devido á complexidade e dificuldade em obter informações tidas como confidenciais e imprescindíveis para a vantagem competitivas das organizações, foram aplicados somente dois questionários a profissionais ligados a gestão de empresas de segurança que prestam serviço, são eles o senhor Breno dos Santos Alves, atuante na área de coordenação de segurança patrimonial da empresa Engeseg Empresa de Vigilância Computadorizada do grupo GPS, e também o senhor Alan Otaviano Gestor de Segurança da empresa AGE group, profissionais que já atuam no mercado de segurança privada a mais de dez anos e possuem uma vasta experiência tanto pratica quanto teórica, o que enriquece ainda mais o conteúdo deste estudo.

Conforme o senhor Alan Otaviano, gestor de segurança da empresa prestadora de serviços de segurança patrimonial, grupo AGE Vigilância e Segurança Patrimonial, quando perguntado como é feita a divisão setorial dentro da empresa, o mesmo informou que é feita toda uma análise de aptidão e de competências buscando sempre um profissional que irá fazer com que a máquina empresarial continue em movimento tomadas as devidas proporções de necessidades de qualificação destinadas ao setor lotado.

4.1 Planejamento estratégico.

Para Chiavenato (2004), o planejamento estratégico se trata de um processo essencial dentro das organizações por que traça diretrizes para o estabelecimento dos planos de ação que resultarão em vantagem competitiva. Ele identifica os recursos potenciais, reconhece fraquezas e estabelece um conjunto de medidas integradas a serem implementadas assegurando o sucesso dos resultados planejados. Ele somente atinge sua eficácia máxima quando entendido e realizado por todas as pessoas da organização em um mutirão permanente organizado e orquestrado.

Tal afirmação do altor retrata tamanha a importância do processo de identificação das vulnerabilidades para que seja definido um plano de ações que irão de encontro a tais vulnerabilidades afim de saná-las, e também que este plano de ações chegue ao conhecimento em um nível macro da organização ou seja todos os setores pois o grande fator de sucesso na implantação de uma estratégia e quando todas as partes pertencentes desta estratégia participam de forma atuante desde a elaboração da mesma até sua implantação e operacionalização na forma de execução dos serviços pertinentes a cada setor inclusive o setor de segurança patrimonial.

O respondente senhor Breno Alves, entende que há uma grande semelhança entre os processos de planejamento estratégico e alinhamento estratégico, contudo o mesmo entende que o alinhamento estratégico se dá por meio de um entendimento de que todos caminhem na mesma direção, desenvolvendo uma cultura da qual todos os funcionários vão se identificar com a marca e proposito,

par seguirem em conjunto na busca de melhores resultado, tornando a gestão cada vez mais efetiva.
É importante ressaltar que o estudo nos trouxe uma visão quanto às definições dos setores de uma organização e o quanto estas definições setoriais estão linkadas às áreas de planejamento que são elas estratégica, tática e operacional, ou seja, o planejamento estratégico tem como objetivo abranger todos os níveis setoriais de uma organização.

4.2 Alinhamento estratégico.

Para Barros (2017), o alinhamento estratégico se define como um ajuste entre diversos aspectos organizacionais que contribuem para a implantação efetiva da estratégia. Uma calibragem entre elementos variáveis específicos da organização, de forma que eles viabilizem (ou não inibam) a implementação da estratégia, e potencializem os resultados esperados.

Em visita a uma empresa do ramo de logística ferroviária que por combinado com o representante da mesma o qual me conduziu durante a visita, não será identificada, foi possível identificar o quão importante é o alinhamento estratégico na execução dos serviços de segurança patrimonial, existe um grande desencontro de informações quanto aos normativos da área de segurança e a implantação, execução, e cumprimento de tais normativos.

Notou-se que a grande dificuldade na execução do serviço de segurança é o não conhecimento de todos os normativos, pela parte dos profissionais de segurança e também os colaboradores da empresa, o que implica na não cooperação dos colaboradores com o sistema que está sendo implantado.

Notou-se também que os setores estratégicos de segurança e os outros setores da empresa tem enfrentado um distanciamento muito grande, uma grande dificuldade de interação no quesito informações e procedimentos ligados a execução dos serviços de segurança patrimonial.

Contudo as repostas dos respectivos respondentes conclui-se que as empresas ainda não têm conhecimento do quão benéfico para a empresa é que as informações pertinentes ao alcance dos objetivos estratégicos sejam disseminadas de maneira macro em toda a empresa seja nos setores orgânicos seja nos setores terceiros.

O respondente senhor Alan Otaviano partilha deste pensamento pois segundo o mesmo como gestor de segurança, participa de algumas, mas poderia participar mais, pois, algumas diretrizes e decisões estratégicas, ainda não são compartilhadas em tempo com o departamento de segurança.

4.3 Tomada de decisões

O processo do planejamento estratégico como ponto inicial para que sejam elaboradas as estratégias a serem implementadas, podem ter variados objetivos porem se olharmos com um olhar macro do sistema empresarial entendemos

que somente com planejamento e o alinhamento entre ambos os níveis setoriais da empresa alcançamos a vantagem competitiva.
A segurança privada entra no processo como uma via de suporte para garantir que todos os processos sejam operacionalizados conforme o esperado, por isso e muito importante a participação do setor de segurança no ato das tomadas de decisão, no direcionamento das estratégias e também na implantação das mesmas.

Contudo o resultado dos questionários aplicados nos permite constatar que na maioria das vezes não acontece com a participação da segurança, conforme o senhor Breno Alves, na maioria das vezes o gestor da área de segurança já recebe as demandas de implantação das estratégias já definidas e quando é permitido pelo gestor da empresa contratante , o gestor da empresa contratada ainda que de forma limitado, expressa sua visão de melhorias retificando ou ratificando as diretrizes em sua implantação e execução e também dos processos que já estavam definidos.

Já conforme o senhor Alan Otaviano, o mesmo participa de algumas, contudo ressalta que poderia participar mais, pois, algumas diretrizes e decisões estratégicas, ainda não são compartilhadas em tempo em tempo hábil com o departamento de segurança, o que as vezes dificulta para o gestor de segurança buscar profissionais com uma qualificação especifica visando atender aos anseios e objetivos propostos na elaboração de tais diretrizes buscando este alcance com qualidade e eficácia.

Conforme Barros (2017), outro fator importante na eficácia da implementação das estratégias, relacionado às pessoas nas organizações, além do acesso às informações, é a questão do poder. Os líderes encarregados de conduzir o processo dependem cada vez mais dos subordinados, e podem se utilizar do poder formal, concedido pela autoridade de seu cargo.

É necessário que o gestor setorial utilize de suas ferramentas técnicas práticas e pessoais para fazer com que a informação relacionada às diretrizes elaboradas chegue ao conhecimento de todos os colaboradores da organização.

4.4 Contrato e o ato da contratação.

Pelo fato de informações contratuais estarem dentro de acordos sigilosos entre prestadora e tomadora de serviços foi possível analisar somente um contrato de licitação de prestação de serviços de segurança patrimonial de um órgão Público, para ser mais especifico foi analisado um contrato de licitação, que contém todo o normativo contratual relacionado a prestação de serviços de segurança patrimonial no banco do Brasil Edital de número 33/2021, aberto no dia 01/06/2021, pelo Banco Central do Brasil, sendo referente a prestação de serviços nas agências que compõem a Gerencia Administrativa de Belo Horizonte.

Nota-se claramente em contrato de edital que não existe nenhuma preocupação quanto a parte contratante com o perfil adequado de profissional para desempenhar tal serviço em suas agências bancárias, em todo momento se

explicita o objeto contratual que conforme o edital é, Prestação de serviços de vigilância ostensiva armada, por postos de serviço, objetivando a guarda do Meio Circulante, a condução de veículos em operações de transporte de valores e a proteção das instalações do Banco Central do Brasil em Belo Horizonte.

Como já sabemos toda instituição já tem sua cultura organizacional e operacional elaborada e implantada, falando sobre alinhamento estratégico e a disseminação de informações que iram munir aos tomadores de decisão ao elaborar a estratégia de operacionalização do serviço de segurança, nota-se já no tópico 4.2.2 do pregão a existência de um fator que provavelmente dificulta muito a participação da empresa terceira na construção ou elaboração de uma estratégia de execução do serviço de segurança patrimonial armada, pois no tópico veda a participação de toda e qualquer empresa que não se enquadrar nas cláusulas contratuais expostas no decorrer do Edital e em seus anexos.

Continuando a análise do contrato de edital em sua totalidade, notou-se que existe uma grande preocupação de se amarrar o contrato nos âmbitos jurídicos, não tendo nenhuma preocupação com os profissionais que irão desempenhar o trabalho nos setores quanto a perfil profissional, qualificação e também do perfil geral buscado pelo autor do edital no caso o Banco Central do Brasil.

Todos os fatores jurídicos referente a execução do serviço são citados no edital porem não se encontrou nenhum tópico referente a perfil adequado do profissional que irá assumir o posto, ou a garantia ou obrigatoriedade de reuniões periódicas de gestão do serviço.

Nota-se ainda que tal preocupação fica por conta mesmo da empresa que irá prestar o serviço isso fica claro pois os respondentes do questionário aplicado quando perguntados sobre a preocupação de se contratar um profissional com características adequadas ao setor onde será prestado o serviço, os mesmos confirmaram que encontram dificuldades devido a escassez de informações relacionadas a cultura e perfil de profissional desejado, conforme o senhor Breno Alves, Este e um gap que muitas terceirizadas ao implantar um serviço não se atentam, a maioria apenas se baseia no que o Edital solicita, temos dois porem no contrato público participamos de uma licitação, com no máximo uma visita técnica, ficando assim difícil de se traçar um perfil, mas no contrato privado temos a oportunidade reunirmos com o Gestor, Administrador ou até mesmo os proprietários, onde temo uma grande oportunidade de traçar o perfil deseja e principalmente necessário para aquele local, atividade e particularidades.

Ainda segundo o senhor Alan Otaviano, esta dificuldade existe também devido aos prazos para processos seletivos e contratações, que muitas vezes, são contratos fechados de última hora, não havendo tempo hábil para tal análise, incluindo que o tomador, na sua maioria, indica os profissionais ou já até possuem uma equipe prestando o serviço no local e exigem a continuidade do pessoal, onde, somente temos a oportunidade de conhecer o perfil de cada um no decorrer do trabalho.

4.5 Comunicação entre contratante e contratada.

Para Aladim (2017), a maioria das prestações de serviço exige que tenha interação entre o cliente e o prestador de serviços, e essa interação deve ser realizada de forma única, já que cada demanda é singular.
É de suma importância que o distanciamento de informações entre as partes tem que ser encurtado cada vez mais buscando a uniformidade das informações relacionadas a objetivos e normativos de execução dos trabalhos.

Conforme o senhor Breno Alves tal comunicação existe somente no ato da implantação dos profissionais nos postos ou por alguma necessidade de melhorias de processos e procedimento, será tratada de forma conjunta e formalizada em contrato.

Já segundo o senhor Alan Otaviano este contato existe e é feito por meio de comunicações formais, ofícios, e-mails, etc., onde, por esses meios, provoca-se encontros e reuniões entre tomador e contratada, no intuito de apresentar projetos e sugestões para aqueles que tomam decisões dentro das organizações.

No caso da empresa visitada durante pesquisa é um pouco diferente existe um estreitamento entre contratada e contratante, pois o seguinte contrato exige um supervisor de segurança dedicado somente para aquela empresa ou seja o supervisor da contratada atende somente este contrato dedicando do seu tempo integral de trabalho para a gestão e operacionalização do serviço, de maneira que o supervisor possa acompanhar de perto a operacionalização do trabalho, e que o supervisor esteja próximo do nível estratégico da tomadora de serviços acompanhando de perto e tendo acesso a todas as informações relacionadas as novas diretrizes que sempre são revisadas e reimplantadas buscando a homogeneidade na operacionalização dos serviços sejam orgânicos, sejam terceirizados.

Um exemplo que as grandes empresas poderiam seguir pelo fato de definir em contrato a presença de um supervisor ou coordenador que seja dedicado único e exclusivo para a empresa tomadora de serviços, fator que viabiliza a comunicação dos níveis estratégicos da contratante e da contratada tornando assim mais fácil de assimilar os anseios estratégicos e operacionais da contratante.

O turnover de empresas prestadoras de serviço de segurança tem sido grande pois temos visto que a preocupação maior é sempre os valores contratuais que consequentemente geram vantagem competitiva sendo a prestadora de serviços detentora de muitos contratos e muitos setores.

5. CONSIDERAÇÕES FINAIS

Em virtude dos fatos mencionados, foi possível detectar alguns gaps existentes na comunicação entre contratante e contratada, e conhecer também algumas dificuldades resultantes destes gaps, como por exemplo a dificuldade de se traçar um perfila de profissional de segurança patrimonial adequado para

atender os anseios operacionais e estratégicos de uma organização contratante devido ao distanciamento existente entre ambas.

Portanto o material elaborado nos trouxe o entendimento de que a preocupação com a existência de um alinhamento de informações, um canal direto de comunicação estratégica entre contratada e contratante parte na maioria das vezes da gestão da empresa contratada, constatou-se também que a necessidade de atender na integra os anseios operacionais, culturais e internos de uma organização tomadora de serviço é um dos grandes vilões das relações contratuais entre as empresas que prestam o serviço de segurança patrimonial.

Conseguimos analisar de uma maneira coorporativa o quão importante é o alinhamento estratégico para a eficácia na operacionalização da prestação de serviço de segurança patrimonial.

Entendemos que o alinhamento estratégico nos deu uma noção sobre as divisões dos níveis setoriais das organizações, haja vista que todas as áreas de uma organização certamente fazem parte de um desses níveis de planejamento, estratégico, tático e operacional, o acesso a estratégia elaborada em sua integra irá depender de qual nível estratégico você faz parte.

O estudo realizado nos permitiu concluir o pensamento de que o grande desafio que as organizações têm enfrentado é a questão de fazer com que as empresas terceiras e prestadoras de serviço consigam também prestar um serviço de qualidade que atenda aos anseios do contratante e que este serviço consiga ser eficiente e mantenha a essência e os princípios traçados e propostos pela contratante em sua cultura organizacional cotidiana.

Tal fato ocorre mediante a falta de uma descrição correta dos pontos a serem atendidos no ato de firmação de contrato ou seja, nem sempre existe a preocupação de ambas as partes, contratante e contratada, em buscar um perfil adequado e exclusivo para aquele setor toda empresa tem seu normativo interno, no nível estratégico então existem algumas normas de confidencialidade, que muitas vezes influenciam de forma direta ou indireta na execução do serviço de segurança privada, prestado nas organizações.

Os respondentes dos questionários aplicados ratificaram a ideia de que a comunicação entre contratante e contratada tem sido um grande problema também no quesito eficácia de operacionalização dos serviços de segurança, haja vista que conforme os respondentes várias vezes a comunicação é tardia e os processos engessados, a empresa contratada na maioria das vezes não tem se quer o direito de opinar quanto a estratégia e processos de operacionalização, além de ter que contratar pessoas que a empresa detectou que não correspondem aos anseios do contratante, contudo devido as normas contratuais, que hora tem condicionamento como manter a equipe de trabalho que já vem remanescente da empresa que prestava serviço anteriormente naquele setor.

Dito isto concluímos que todo o processo se encaixa desde o planejamento estratégico quando na elaboração das estratégias, as métricas de prospecção

de resultados, a estratégia pronta, a disseminação desta estratégia em todos os níveis setoriais de uma organização, inclusive os setores de prestação de serviços (terceirizados), em especial o setor de segurança, irão contribuir para que a organização obtenha vantagens competitivas, haja vista que a máquina empresarial e todos os elementos que compõem está maquina trabalharão de maneira uniforme, contribuem para o sucesso no alcance dos objetivos traçados pelo nível estratégico de uma organização, tendo a segurança patrimonial como parte atuante no suporte a todos os setores.

REFERENCIAS

Aladim, Carolina Trópia. **O DESAFIO PARA A EMPRESA PRESTADORA DE SERVIÇOS EM IDENTIFICAR AS EXPECTATIVAS E SATISFAZER AS NECESSIDADES DOS CLIENTES.** Belo Horizonte MG, Faculdade Ietec, 2017.

BARRETO, Carla Alessandra, **A IMPORTÂNCIA DO PLANEJAMENTO ESTRATÉGICO PARA AS PEQUENAS EMPRESAS.** Tatuí-SP, FAESB, 2015.

BARROS,Luiz Monteiro.**Alinhamento Estratégico.** São Paulo-SP, Edição do autor, 2017.

BASSI,Luiz Carlos, MONTEIRO, Carlos Gomes. **Planejamento estratégico em Segurança.** Londrina-PR, Editora Educacional, 2017.

BRASIL. **Portaria DPF 3233/2012**: Dispõe sobre as normas relacionadas às atividades de Segurança Privada. Disponível em: < >. Acesso em: 15 Mai. 2022.

CANÇADO, Airton Cardoso. **GESTÃO SOCIAL E GESTÃO ESTRATÉGICA: REFLEXÕES SOBRE AS DIFERENÇAS E APROXIMAÇÕES DE CONCEITOS.** São Paulo SP, RGSA, 2016.

CARVALHO, E. da N.; SANTOS, R. M. G. dos. As Diretrizes Organizacionais: uma análise prática da missão, visão e valores em uma pequena empresa em Mossoró-RN. **Revista Foco**, [S. l.], v. 9, n. 1, 2016. Disponível em: <https://revistafoco.emnuvens.com.br/foco/article/view/226>. Acesso em: 22 Maio. 2022.

CORDEIRO, José Vicente Bandeira Melo de. **ALINHAMENTO ESTRATÉGICO: ESTUDOS MULTICASOS EM EMPRESAS PARANAENSES DE MÉDIO PORTE.** Florianópolis-SC, UFSC, 2005.

CHIAVENATO, Idalberto. **PLANEJAMENTO ESTRATÉGICO, Fundamentos e Aplicações,** Editora Elsevier, Rio de Janeiro RJ, 2004.

ESTEVÃO, Carlos, **Gestão Estratégica nas Escolas,** São Paulo SP, C.O.V.C, 1998.

GALAS, Eduardo Santos. **O BALANCED SCORECARD E O ALINHAMENTO ESTRATÉGICO DA TECNOLOGIA DA INFORMAÇÃO: UM ESTUDO DE CASOS MÚLTIPLOS.** São Paulo SP, 2006, pg. 02.

KUTSHER, Eribelto Alves. **INOVAÇÃO TECNOLOGIA E SUAS INFLUENCIAS NO PROCESSO DE GESTÃO: Uma análise no setor de Segurança Patrimonial.** Santa Catarina-SC, RGO, 2009.

MEIRA, Josiane Santana. **ALINHAMENTO ESTRATÉGICO NA GESTÃO PÚBLICA DE UM MUNICIPIO DO OESTE PAULISTA.** Presidente Prudente SP, Y3, 2021.

MINELLI, Wallesca. **Particularidades da Comunicação com o funcionário terceirizado.** São Paulo-SP, FCL,2017.

MORAES, Paulo Eduardo Sobreira. **SEGURANÇA COMO ESTRATÉGIA DE GESTÃO DA INFORMAÇÃO.** RET, 2005.

MORETTI, Claudio dos Santos. **A SEGURANÇA PRIVADA NO BRASIL. Histórico e Evolução.** USA, Independently Publiched, 2020.

NICOLAU, Isabel. **O Conceito de Estratégia.** Campo Grande-MS, INDEG/ISCTE, 2001.

OLIVEIRA. Maxwell Ferreira de. **METODOLOGIA CIENTIFICA. Um manual para a realização de pesquisas em administração.** Catalão-GO,UFG, 2011.

OLIVEIRA, Aryeverton Fontes de. **EMPRESAS DE VIGILANCIA NO SISTEMA DE PRESTAÇÃO DE SERVIÇOS DE SEGURANÇA PATRIMONILA PRIVADA: UMA AVALIAÇÃO DA ESTRUTURA DE GOVERNANÇA.** Piracicaba-SP, DBD/USP, 2004.

RIBEIRO, Felipe Nunes. **PLANEJAMENTO ESTRATÉGICO: Aplicação de Ferramentas para Aumento da Competitividade da Empresa.** Serra, ES., R.E. DOCTUM, 2021.

RODRIGUES, Antonio de Andrade. **Alinhamento Estrarégico nas Organizações.** Rio de Janeiro-RJ,UNIRIO/UFRJ. 2015.

SOUZA, Wendel. **O PLANEJAMENTO ESTRATÉGICO NAS MICRO E PEQUENAS EMPRESAS.** São Paulo SP, Centro Universitário Senac, 2007.

TINOCO, Gabriel.**Segurança Empresárial da teoria á prática.** São Paulo_SP, GESEG, 2022.

TORRES, Marcelo Teixeira. **A GESTÃO DA SEGURANÇA DA INFORMAÇÃO E SEU ALINHAMENTO ESTRATÉGICO NA ORGANIZAÇÃO.** Revista Interface Tecnologia, 2010.

VALENTIN, Marta. **Tipos de Planejamento.** São Paulo SP, Universidade Estadual Paulista, UNESP, 2019.

“AVALIAÇÃO DE VULNERABIDADES EM INSTALAÇÕES: ESTRATÉGIAS ESSENCIAIS PARA UMA SEGURANÇA REFORÇADA”

Dr. Hebert Magno, CPSI, CIGR, CIEIE, CISI, DIDS

Introdução:

A segurança de instalações tornou-se uma prioridade crítica em um mundo dinâmico e cada vez mais interconectado. Para garantir a proteção eficaz de propriedades e ativos, a avaliação de vulnerabilidades emerge como uma ferramenta crucial. Este artigo explora estratégias essenciais para realizar uma avaliação abrangente de vulnerabilidades, destacando a importância dessa prática na mitigação de riscos e na promoção de ambientes mais seguros.

Segundo o Prof. Dr. Nino MEIRELES em seu Livro Gestão Estratégica do Sistema de Segurança SICUREZZA 2011, O autor destaca que falhas, sejam em componentes humanos ou equipamentos, são fatores de risco que muitas vezes levam a acidentes. A gestão de riscos envolve identificar possíveis falhas e adotar medidas para minimizá-las, reduzindo probabilidade e impactos. A análise de falhas inclui identificar modo e tipo de falha, agentes promotores e inibidores, fase do ciclo de vida do componente ou sistema, e quando os agentes promotores foram introduzidos.

Segundo Prof. Dr. Nino MEIRELES, existem cinco modos de falha: omissão, falha na missão, por ato estranho, sequencial e temporal. A falha humana é destacada, sendo classificada em técnica, descuido e consciente. A falha técnica ocorre pela falta de meios adequados, enquanto a falha por descuido é esporádica e relacionada à desatenção. A falha consciente envolve escolhas de comportamento inseguro por parte do humano.

Ainda segundo autor Prof. Dr. Nino MEIRELES, expõem que as falhas podem ser randômicas ou sistemáticas. A cultura da empresa influencia o comportamento humano. A falha composta é comum, e a decomposição de falhas é crucial para ações preventivas. No contexto de falhas de equipamento, destacam-se falhas do tipo T (incapacidade de exercer a missão), D (falhas esporádicas) e C (falhas sistemáticas por ajustes incorretos).

Agentes promotores de falhas incluem primário (ligado ao ambiente e carga qualificada), secundário (ligado a condições adversas), comando (quando o componente age sob comando do sistema) e intruso (quando atua fora do sistema normal). A falha de causa comum, resultante da ação simultânea de agentes promotores em elementos redundantes, é destacada como um fator limitante no aumento da confiabilidade do sistema.

Compreendendo a Avaliação de Vulnerabilidades: Antes de mergulharmos nas estratégias específicas, é vital entender o que envolve a avaliação de vulnerabilidades. Essa prática vai além de simples inspeções visuais, buscando identificar pontos fracos em sistemas de segurança, procedimentos operacionais e infraestrutura física.

Segundo Prof. ANTONIO CELSO RIBEIRO BRASILIANO, PhD, Livro Gestão e Análise de Riscos Corporativos 2010 2ª edição, Pag. 8, Premissas estratégicas**:** O gerenciamento de riscos corporativos é baseado na premissa de que as organizações existem para gerar valor às partes interessadas. Enfrentando incertezas, os administradores precisam decidir até que ponto aceitar essas incertezas e como elas podem afetar a geração de valor. Incertezas representam riscos e oportunidades, e o gerenciamento de riscos corporativos ajuda os administradores a lidar eficazmente com essas incertezas, riscos e oportunidades para melhorar a capacidade de gerar valor.

Segundo Prof. ANTONIO CELSO RIBEIRO BRASILIANO, PhD, 2010 Livro Gestão e Análise de Riscos Corporativos 2ª edição. O valor é maximizado quando a organização equilibra metas de crescimento e retorno de investimentos com os riscos associados. Os objetivos estratégicos do gerenciamento de riscos corporativos incluem alinhar o apetite a risco com a estratégia, fortalecer decisões em resposta aos riscos, reduzir surpresas operacionais, identificar e administrar riscos múltiplos, aproveitar oportunidades e otimizar o capital.

Essas qualidades ajudam os administradores a atingir metas de desempenho e lucratividade, evitando a perda de recursos. O gerenciamento de riscos corporativos também contribui para a comunicação eficaz, o cumprimento de leis e regulamentos, e a preservação da reputação da organização.

Além disso, a seção aborda a relação entre eventos, riscos e oportunidades, destacando a importância de identificar e administrar eventos que possam impactar negativa ou positivamente a organização.

Eventos – Riscos e Oportunidades: Eventos podem ter impactos negativos ou positivos. Impactos negativos representam riscos que podem prejudicar a criação de valor, enquanto os impactos positivos representam oportunidades que podem favorecer a realização de objetivos. O gerenciamento de riscos corporativos direciona oportunidades para os processos de elaboração de estratégias, planejando como aproveitá-las.

Definição De Gerenciamento De Riscos Corporativos: O gerenciamento de riscos corporativos é um processo conduzido por conselho de administração, diretoria e demais empregados. Ele visa estabelecer estratégias para identificar eventos potenciais em toda a organização, administrar os riscos de maneira compatível com o apetite a risco e garantir o cumprimento dos objetivos.

Essa definição destaca que o gerenciamento de riscos corporativos é contínuo, conduzido por profissionais em todos os níveis da organização, aplicado à definição de estratégias e abrangendo todos os níveis e unidades. Ele

proporciona garantia razoável para o conselho de administração, sendo orientado para a realização de objetivos em categorias distintas.

Realização De Objetivos: Com base na missão ou visão da organização, a administração estabelece planos e seleciona estratégias para alcançar objetivos em quatro categorias: estratégicos, operacionais, comunicação e conformidade. Esses objetivos são orientados para a criação e preservação de valor.

Componentes Do Gerenciamento De Riscos – Metodologia COSO – ERM:

A Metodologia COSO - ERM define oito componentes inter-relacionados do gerenciamento de riscos corporativos: Ambiente Interno, Fixação de Objetivos, Identificação de Eventos, Avaliação de Riscos, Resposta a Risco, Atividades de Controle, Informações e Comunicações, e Monitoramento. Esses componentes formam um processo multidirecional e interativo.

Relacionamento Entre Objetivos e os Componentes Da Metodologia COSO – ERM: Existe um relacionamento direto entre objetivos e os oito componentes do gerenciamento de riscos corporativos, ilustrado em uma matriz tridimensional. Isso permite manter o foco na totalidade do gerenciamento de riscos em uma organização.

Fases da Avaliação do Risco.

a. Planejamento: Definir objetivos claros e escopo da avaliação. Identificar ativos críticos e áreas prioritárias.

b. Coleta de Dados: Revisar planos arquitetônicos e de segurança existentes. Entrevistar pessoal-chave para entender procedimentos operacionais.

c. Análise de Riscos: Identificar ameaças potenciais e avaliar sua probabilidade de ocorrência. Classificar vulnerabilidades com base na criticidade e impacto.

d. Recomendações e Relatórios: Propor soluções para mitigar vulnerabilidades identificadas. Elaborar relatórios detalhados, oferecendo orientações claras para a implementação de melhorias.

Tecnologia e Inovação na Avaliação

A utilização de tecnologia desempenha um papel significativo na modernização das avaliações de vulnerabilidades. Sistemas avançados de vigilância, sensores inteligentes e análise de dados são ferramentas poderosas para identificar e monitorar potenciais riscos.

Tratamento de Riscos e Elaboração do Plano de Ação

Segundo Prof. ANTONIO CELSO RIBEIRO BRASILIANO, PhD, 2010 Livro Gestão e Análise de Riscos Corporativos 2ª edição. Pag. 103. Depois de identificados, avaliados e mensurados, deve-se definir qual o tratamento que será dado aos riscos. Na prática, a eliminação total dos riscos é impossível. Nesse contexto, a Matriz de Riscos e a Classificação do Nível de Riscos apoia a priorização e visa direcionar os esforços relativos a novos projetos e planos de ação elaborados, a fim de minimizar os eventos que possam afetar

adversamente e maximizar aqueles que possam trazer benefícios para a organização.

1. Identificação, Avaliação e Mensuração dos Riscos: Inicie identificando os riscos relevantes para a organização. Avalie e mensure esses riscos para entender sua gravidade e probabilidade de ocorrência.

2. Definição das Estratégias de Tratamento dos Riscos: Utilize a Matriz de Riscos e a Classificação do Nível de Riscos para priorização. Alinhe a estrutura de controles internos aos objetivos estratégicos da organização. A alta administração deve definir sua postura em relação aos riscos, considerando efeitos, aversão, resposta e análise de custo-benefício.

3. Aplicação das Estratégias de Tratamento: Considere opções como evitar o risco, aceitar (reter, reduzir, transferir, explorar), remover a fonte, alterar probabilidade ou consequências, compartilhar e reter conscientemente. Utilize o diagrama exemplificando as estratégias de tratamento dos riscos para orientação.

4. Elaboração do Plano de Ação: Utilize a técnica das perguntas 5W2H (What, Who, When, Where, Why, How, How Much) para detalhar o plano. Responda a perguntas como "O que fazer?", "Quem é responsável?", "Quando implantar?", "Onde será implementado?", "Por que é necessário?", "Como será implementado?" e "Quanto custa?". Estabeleça objetivos qualitativos para cada solução.

5. Recursos para Mitigação dos Riscos: Considere meios técnicos (ativos e passivos), humanos e organizacionais. Classifique os recursos em Meios Humanos, Meios Técnicos (ativos e passivos) e Meios Organizacionais (planos de prevenção, emergência, continuidade, manutenção e auditoria).

6. Ferramenta de Apoio à Decisão - Priorização das Ações: Utilize critérios como esforço de implementação e benefício estimado. Para o esforço de implementação, considere custo, tempo e autonomia. Para o benefício estimado, avalie o impacto no contexto, probabilidade de sucesso e eficácia operacional.

7. Matriz de Priorização de Ações: Cruze os critérios de esforço de implementação e benefício estimado em uma matriz. Categorize as ações nos quadrantes I (implementação imediata), II (reavaliação a médio prazo) e III (descarte).

8. Integração e Monitoramento: Garanta a integração efetiva com os diversos departamentos da empresa. Estabeleça um sistema de monitoramento contínuo para avaliar a eficácia das ações implementadas. Este passo a passo fornece uma visão abrangente do processo de tratamento de riscos, desde a identificação até a implementação de ações prioritárias, garantindo uma abordagem estruturada e eficaz.

Monitoramento e Análise Crítica dos Riscos

Para o autor Prof. ANTONIO CELSO RIBEIRO BRASILIANO, PhD, 2010, Livro Gestão e Análise de Riscos Corporativos 2ª edição. Pag. 117. O monitoramento e a análise crítica devem ser planejados como parte do processo de gestão de riscos e deve envolver a checagem ou vigilância regulares. Podem ser periódicos ou acontecer em resposta a um fato específico.

De maneira clara e objetiva, o monitoramento abrange dois processos essenciais. O primeiro consiste na verificação da execução do Plano de Ação proposto, utilizando indicadores como "Executado", "Em Execução" e "Não Executado". Além disso, é crucial acompanhar os resultados das ações propostas, avaliando se os objetivos foram alcançados e identificando eventuais dificuldades, o que demanda a implementação de ações corretivas. Esse processo é denominado monitoração.

Envolvimento da Equipe

A avaliação de vulnerabilidades não deve ser encarada como uma tarefa isolada. Envolva a equipe de segurança, colaboradores e, quando possível, especialistas externos. A diversidade de perspectivas fortalece a análise e as soluções propostas.

Adaptação às Mudanças.

Ambientes e ameaças evoluem. Uma avaliação de vulnerabilidades deve ser um processo contínuo, adaptando-se às mudanças na infraestrutura, tecnologia e nas próprias ameaças. Revisões regulares garantem a eficácia contínua das medidas de segurança implementadas.

Conclusão

Em um mundo onde a segurança é um fator essencial, a avaliação de vulnerabilidades em instalações emerge como uma ferramenta indispensável para a proteção eficaz de ativos. Ao adotar estratégias abrangentes, incorporando tecnologia, envolvendo a equipe e mantendo uma abordagem adaptativa, as organizações podem fortalecer significativamente sua postura de segurança, criando ambientes mais seguros e resilientes.

Dr. Hebert Magno, CPSI, CIGR, CIEIE, CISI, DIDS. Membro e Delegado CEAS Regional-MG, Doctor Internacional en Ciencias de la Seguridad, pela Corporación Euro-Americana de Seguridad – Madrid, Espanha. Membro do Comitê Público da Associação Nacional dos Profissionais de Privacidade de Dados. Membro do Comitê Público do Instituto de Defesa Cibernética.

“COMPETÊNCIA: O QUE É, TIPOS, ELEMENTOS ESSENCIAIS QUE A COMPÕEM E COMO ADQUIRIR”

José Sérgio Marcondes, CES, CPSI

Descubra a importância da competência para sua carreira profissional. Saiba como conhecimento, habilidades e atitudes se entrelaçam para impulsionar seu sucesso.

Competência pode ser definida como uma capacidade que engloba um conjunto de conhecimentos, habilidades e atitudes inter-relacionados, dos quais uma pessoa necessita para desempenhar uma determinada atividade ou função de forma eficaz e eficiente.

No cenário cada vez mais competitivo do mundo profissional, a palavra “competência” se destaca como um dos fatores mais críticos para o sucesso. Você já se perguntou o que exatamente essa palavra significa? E como a competência se traduz no desempenho excepcional no trabalho

Neste artigo, exploraremos em detalhes o significado e os componentes da competência, revelando como ela é fundamental para alcançar o sucesso em sua carreira. Prepare-se para uma jornada que irá transformar sua compreensão sobre o que é necessário para se destacar no mercado de trabalho e alcançar suas metas profissionais.

O que significa competência?

Competência é uma capacidade que engloba um conjunto de conhecimentos, habilidades e atitudes inter-relacionados, dos quais uma pessoa necessita para desempenhar uma determinada atividade ou função de forma eficaz e eficiente. Em outras palavras, competência é a capacidade de um indivíduo de realizar uma tarefa ou atividade, com base em seus conhecimentos, habilidades e atitudes.

Portanto, uma competência é uma combinação sinérgica de conhecimento, habilidades e atitudes que capacita um indivíduo a executar eficazmente suas funções profissionais. Ela é crucial para o desempenho bem-sucedido em uma variedade de ocupações e contextos organizacionais.

É importante notar que a competência só pode ser realmente avaliada quando se observa o comportamento da pessoa em seu ambiente de trabalho, já que a teoria e o conhecimento teórico devem ser colocados em prática para demonstrar verdadeira competência.

Quais são os elementos da competência?

Os elementos que compõem a competência no contexto organizacional são:

1- **Conhecimento:** O conhecimento é a base de uma competência. Refere-se ao conjunto de informações, teorias e conceitos que uma pessoa possui sobre um determinado assunto ou área de conhecimento. O conhecimento fornece a compreensão teórica necessária para desempenhar uma tarefa ou função de maneira eficaz.
2- **Habilidades:** As habilidades são a capacidade prática de aplicar o conhecimento adquirido. Elas representam o "saber fazer". As habilidades envolvem a execução de tarefas, a aplicação de técnicas específicas e a realização de ações práticas relacionadas a uma competência.
3- **Atitudes:** As atitudes referem-se a aspectos sociais e emocionais envolvidos no trabalho. Isso inclui o interesse, a motivação, a determinação e o comportamento de uma pessoa em relação ao trabalho, aos colegas e às situações. As atitudes desempenham um papel importante na forma como alguém aborda as tarefas e interage com os outros no ambiente de trabalho.

Em conjunto, esses elementos formam a competência de uma pessoa.

A competência é a capacidade de saber o que precisa ser feito (conhecimento), ser capaz de fazê-lo de maneira prática e eficaz (habilidades), ter a motivação e a atitude corretas para realizar a tarefa (atitudes) e demonstrar isso por meio do comportamento no ambiente de trabalho. Esses elementos são interligados e essenciais para um desempenho bem-sucedido em uma função ou ocupação profissional.

Qual é a diferença entre competência e habilidade?

A competência é um conceito mais amplo que abrange não apenas habilidades, mas também conhecimento e atitudes. É um conjunto de características inter-relacionadas que capacita uma pessoa a desempenhar eficazmente uma função ou tarefa específica em seu ambiente de trabalho

Já a habilidade é uma parte específica das competências e se refere à capacidade prática de realizar tarefas ou ações com destreza. Ela inclui a capacidade de aplicar o conhecimento para realizar ações específicas com eficiência. Ter habilidades é um dos componentes que contribuem para alguém ser considerado competente em seu campo de atuação.

Qual a importância da competência?

A competência desempenha um papel vital no desenvolvimento pessoal e no sucesso das organizações. Ela é um fator-chave para o desempenho superior, a inovação, a satisfação no trabalho e a capacidade de enfrentar desafios em um ambiente de trabalho em constante evolução.

A seguir alguns dos principais motivos pelos quais a competência é fundamental:

1- **Melhor Desempenho Individual:** Pessoas competentes têm a capacidade de desempenhar suas funções de maneira mais eficaz e eficiente, o que leva a um desempenho individual superior. Isso se traduz em maior produtividade, qualidade do trabalho e realização de objetivos pessoais e profissionais.

2- **Resolução Eficaz de Problemas:** Pessoas competentes são mais capazes de identificar e resolver problemas de maneira eficaz.
3- **Inovação e Crescimento:** Competências não se limitam a realizar tarefas existentes, mas também incluem a capacidade de inovar e se adaptar.
4- **Crescimento Profissional:** Competências sólidas proporcionam oportunidades de desenvolvimento profissional e avanço na carreira. Indivíduos competentes são mais propensos a assumir cargos de liderança e responsabilidades crescentes.
5- Satisfação no Trabalho: Pessoas competentes sentem-se mais confiantes em suas habilidades, o que pode levar a um maior nível de satisfação e engajamento no trabalho.
6- **Reputação e Credibilidade:** Indivíduos e organizações conhecidos por sua competência ganham reputação e credibilidade no mercado.
7- **Retenção de Talentos:** Organizações que reconhecem e recompensam a competência tendem a atrair e reter talentos de alta qualidade. Os funcionários competentes são valiosos e, quando se sentem valorizados, são mais propensos a permanecer na empresa.
8- **Melhor Desempenho Organizacional:** Uma força de trabalho competente é um dos principais impulsionadores do sucesso organizacional. As empresas que investem no desenvolvimento de competências de seus funcionários geralmente alcançam maior eficiência, inovação e satisfação do cliente.

Quais são os tipos de competências?

No contexto organizacional, as competências podem ser classificadas em diferentes tipos, dependendo de como são aplicadas e em que nível são relevantes. A seguir alguns dos tipos de competências comuns:

1- **Competência Organizacional:** As competências organizacionais se referem a capacidade de uma organização de integrar e coordenar seus recursos e processos, de forma estratégica, competitiva e única, de forma que agreguem valor à organização, formando sua identidade e gerando vantagem competitiva sustentável.
2- **Competência Individual:** As competências individuais se referem à capacidade de um indivíduo de realizar suas funções e tarefas de maneira eficaz.

3- **Competência Comportamental ou Soft Skills:** As competências comportamentais são relacionadas às atitudes e comportamentos de uma pessoa no ambiente de trabalho. Exemplos incluem a capacidade de comunicação eficaz, empatia, resolução de conflitos, trabalho em equipe e liderança.
4- **Competência Técnica ou Funcional:** As competências técnicas estão relacionadas às habilidades e conhecimentos específicos necessários para realizar as tarefas e funções dentro de uma determinada profissão ou área de atuação.
5- **Competência Gerencial:** As competências gerenciais se referem à capacidade de um indivíduo de desempenhar funções de liderança e gestão de equipes e recursos de maneira eficaz, contribuindo para o sucesso de uma organização.

O que é ter Competência?

Ter Competência significa ser capaz de realizar suas funções de maneira eficaz, eficiente e consistente, atendendo ou superando as expectativas e padrões de desempenho estabelecidos. Isso envolve a aplicação de conhecimento, habilidades, atitudes e comportamentos apropriados para a função ou cargo que a pessoa ocupa em uma organização.

Em termos mais específicos, ter competência no trabalho implica:

1- **Ter conhecimento adequado:** O que implica que a pessoa possui o conhecimento necessário para desempenhar sua função. Envolve estar atualizado com as melhores práticas, técnicas, teorias, regulamentações relevantes e desenvolvimentos recentes em sua área de atuação. É o “Saber Sobre” que capacita o indivíduo a manter-se informado e atualizado em sua profissão.
2- **Ter habilidade prática:** Isso abrange a capacidade de aplicar o conhecimento de maneira eficaz na execução de tarefas e na resolução de problemas. É o “Saber Fazer” que permite que a pessoa execute suas responsabilidades com destreza, eficiência e rapidez.
3- **Ter atitude positiva:** Isso engloba uma atitude proativa, engajada e positiva em relação ao trabalho. É o “Querer Fazer bem feito” que motiva a pessoa a realizar suas responsabilidades com entusiasmo, comprometimento e dedicação.

A sinergia desses três componentes é o que forma a competência de um profissional. A sinergia envolve a interação cooperativa dos três elementos, que quando trabalhados juntos, produzem resultados mais eficaz, eficiente e harmoniosos.

Ter conhecimento sem habilidade prática pode resultar em ineficácia, assim como ter habilidade prática sem conhecimento adequado pode levar a ações fora de padrões estabelecidos. Já a falta de atitude pode resultar em inércia e falta de progresso. Ter Competência, portanto, é ser capaz de gerar sinergia entre esses três elementos.

Exemplos de Competências

- Competências de Liderança: Envolve a aptidão para liderar e gerenciar equipes. Inclui de tomada de decisão, delegação, motivação e gerenciamento de conflitos.

- Competências de Comunicação: Envolve a capacidade de se expressar claramente, ouvir atentamente, fazer apresentações e escrever de forma convincente.

- Competências Interpessoais: Se relacionam com a capacidade de construir relacionamentos sólidos no local de trabalho, incluindo empatia, inteligência emocional e resolução de conflitos.

- Competências de Inovação e Criatividade: Com a crescente importância da inovação, know-hows relacionadas à geração de ideias criativas, resolução de problemas complexos e adaptação a mudanças estão se tornando cruciais.

- Competências de Gerenciamento de Tempo: São capacitações essenciais para otimizar a produtividade e gerenciar eficazmente o tempo, priorizar tarefas e manter-se organizado.

Como Adquirir e Desenvolver Competência?

Adquirir e desenvolver competência é um processo que envolve o desenvolvimento de conhecimento, habilidades, atitudes relevantes para sua área de atuação. A seguir alguns passos essenciais para você adquirir e desenvolver suas competências:

1- **Defina Seus Objetivos:** Comece definindo claramente seus objetivos de desenvolvimento de competência. O que você deseja alcançar? Quais competências são necessárias para atingir seus objetivos?
2- **Autoconhecimento:** Avalie suas habilidades, conhecimentos e atitudes atuais. Identifique suas forças e áreas que precisam de aprimoramento. O autoconhecimento é fundamental para direcionar seus esforços de desenvolvimento.
3- **Identifique Competências Requeridas:** Entenda as competências necessárias para a sua área de atuação. Isso pode envolver pesquisa, conversas com colegas e a análise de descrições de cargos e requisitos profissionais.
4- **Plano de Desenvolvimento:** Crie um plano de desenvolvimento pessoal que inclua objetivos claros, prazos e ações específicas para adquirir as competências desejadas. Seja realista em relação ao tempo e recursos necessários.
5- **Aprendizado Formal:** Busque oportunidades de aprendizado formal, como cursos, workshops, treinamentos ou programas educacionais. Essas fontes podem fornecer conhecimento teórico e prático essencial.
6- **Aprendizado Informal:** Busque informações em bons livros e em artigos confiáveis da internet. Aprenda com a experiência do dia a dia. A prática

contínua é fundamental para desenvolver habilidades. Aprenda com erros e sucessos.

7- **Feedback:** Esteja aberto ao feedback. Peça feedback de supervisores, colegas e subordinados para identificar áreas de melhoria e ajustar seu plano de desenvolvimento.

Adquirir competência é um processo contínuo. À medida que o ambiente de trabalho evolui e suas metas mudam, você pode precisar ajustar seu plano de desenvolvimento. O compromisso com o aprendizado contínuo é essencial para se manter competente em sua área de atuação.

Conclusão

A competência é a base do sucesso profissional. Compreender a relação entre conhecimento, habilidades e atitudes é fundamental para alcançar o desempenho excepcional no ambiente de trabalho. Espero que este artigo tenha fornecido insights valiosos sobre como desenvolver e aplicar competências em sua carreira.

Lembre-se de que a busca contínua por competência é uma jornada que vale a pena. À medida que você aprimora seu conhecimento, aprimora suas habilidades e cultiva atitudes positivas, você se torna um profissional mais eficaz e valioso.

Aproveite ao máximo essa compreensão e comece a aplicá-la em sua vida profissional. E se você está ansioso para explorar ainda mais o mundo das competências, convidamos você a ler nosso próximo artigo sobre ‘As Principais Competências que um Profissional Deve Possuir’

José Sergio Marcondes – CES – CPSI – Gestor, Consultor e Diretor do IBRASEP. Especialista em segurança com competências sólidas nas áreas de segurança privada e gestão empresarial. Conecte comigo nas redes sociais.

“CPSI – CERTIFICADO PROFESIONAL EN SEGURIDAD INTERNACIONAL: ALCANÇANDO A EXCELÊNCIA EM SEGURANÇA”

José Sergio Marcondes, CES, CPSI

Saiba como a CPSI, Certificado Profesional en Seguridad Internacional, valida as competências dos profissionais de segurança e como elevam o padrão profissional.

O CPSI, Certificado Profesional en Seguridad Internacional, é um reconhecimento e certificação concedidos pela CEAS Internacional a profissionais da área de segurança que demonstram amplo conhecimento e habilidades no gerenciamento de questões relacionadas à segurança em um contexto internacional.

Em um cenário globalizado, a segurança desempenha um papel crucial, e os profissionais dedicados a esse campo de atuação enfrentam o desafio de comprovar seus conhecimentos e habilidades adquiridos ao longo dos anos. Neste contexto, o Certificado Profesional en Seguridad Internacional (CPSI) surge como uma resposta a essa necessidade.

Em um ambiente profissional cada vez mais competitivo e exigente, esta certificação se destaca como um diferencial competitivo importante para os profissionais que buscam não apenas se destacar, mas também exercer posições de liderança em nível global.

Nosso artigo explora os elementos fundamentais dessa certificação, destacando por que ela se tornou essencial para aqueles que aspiram a uma carreira sólida e respeitada na segurança nacional e internacional. Descubra como o CPSI pode transformar sua jornada profissional.

Certificação do Profissional da Segurança Privada

A Certificação do Profissional da Segurança Privada é um processo pelo qual um profissional pode obter um reconhecimento oficial de suas competências (conhecimentos e habilidades) na área da segurança. Essas Certificações são concedidas por organizações especializadas e reconhecidas internacionalmente como a Corporación Euro-Americana de Seguridad (CEAS), representada no Brasil pela CEAS-BRASIL.

CEAS-BRASIL, é uma Instituição Certificadora Internacional com sede no Brasil que disponibiliza 9 tipos de certificações:

Certificado Profesional en Seguridad Internacional "CPSI"

Certificado Internacional en Gestión de Riesgos "CIGR"

Certificado Internacional de Especialista en Investigación Empresarial "CIEIE"

Certificado Internacional de Especialista Antifraude y Compliance "CIEAC"

Certificado Especialista en Gestión de Riesgos Cibernéticos "CEGRC"

Certificación Profesional Internacional en Seguridad Industrial "CPI-SI"

Certicación Internacional Especialista en Análisis de Inteligencia "CIEAI"

Certificado de Consultor Internacional en Seguridad Integral, Gestión de Riesgos y Preveción de Pérdidas "CISI"

Certificado Internacional de Protección Personal "CIPP"

Sobre a Corporación Euro Americana de Seguridad (CEAS)

A CEAS-INTERNACIONAL é uma Associação Internacional representada por Secretarias Gerais em 73 países, com profissionais afiliados em mais de 100 países. Composta por mais de 10.000 membros associados em todo o mundo, incluindo destacáveis especialistas reconhecidos na ampla gama dos Serviços de Segurança.

Com sede em Madrid, Espanha, a CEAS-INTERNACIONAL possui personalidade jurídica e está registrada fiscalmente no Censo de Entidades Jurídicas do Ministério da Fazenda da Espanha, além de contar com representação na ONU. A associação possui sedes em diversos países, incluindo o Brasil. A CEAS oferece várias certificações relevantes para a segurança privada, como o Certificado Profesional en Seguridad Internacional (CPSI).

O que é CPSI – "Certificado Profesional en Seguridad Internacional"?

O CPSI, Certificado Profesional en Seguridad Internacional, é um reconhecimento e certificação concedidos pela CEAS Internacional a profissionais da área de segurança que demonstram amplo conhecimento e habilidades no gerenciamento de questões relacionadas à segurança em um contexto internacional.

O CPSI atua como um selo de qualidade, atestando a competência do profissional para assumir responsabilidades de gestão e lidar com uma variedade de situações de risco de segurança em âmbito mundial. É uma certificação internacional de segurança reconhecida por empresas e organizações em todo o mundo.

O Certificado Profesional en Seguridad Internacional, concedido pela CEAS Internacional, destaca-se como o mais alto reconhecimento mundial para profissionais de segurança. Ele é concedido apenas a profissionais que demonstraram amplo conhecimento e habilidades para lidar com as responsabilidades da gestão de segurança em diversas situações de risco em qualquer parte do mundo.

A certificação serve como um reconhecimento visível do domínio profissional demonstrado nos conceitos, princípios e competências essenciais de segurança, fundamentais para as melhores práticas de gerenciamento de segurança.

Para que serve o CPSI?

O CPSI serve como um indicador de competência profissional no seguimento da segurança, proporcionando às empresas nacionais e internacionais um padrão que garante conformidade com as melhores práticas mundiais da indústria de segurança.

Diferenciando-se de outras Certificações, o CPSI é reconhecido e endossado por entidades governamentais, universidades, associações de segurança e forças de segurança em todo o mundo. Possuir o CPSI é um selo de credibilidade e prestígio profissional

Ao obter uma Certificação, o profissional de segurança demonstra seu compromisso com a excelência e a conformidade com os padrões e melhores práticas do mercado. Além disso, essas Certificações podem ajudar a aumentar a credibilidade e a empregabilidade do profissional, oferecendo uma vantagem competitiva no mercado de trabalho.

Qual a importância do CPSI?

O Certificado Profesional en Seguridad Internacional é uma certificação importante para os profissionais e setor da segurança privada por vários motivos.

1- **Para os profissionais:**

- **Reconhecimento e credibilidade profissional:** A CPSI é uma certificação reconhecida por empresas e organizações em todo o mundo. Ela demonstra que o profissional possui os conhecimentos e habilidades necessários para gerenciar as atividades da segurança.
- **Melhores oportunidades de emprego e carreira:** Pode ajudar os profissionais a obter promoções, aumentar seus salários e abrir novas oportunidades de emprego e carreira.
- **Acesso a treinamento e desenvolvimento profissional:** Da acesso a treinamentos e desenvolvimento profissional oferecidos pelos CEAS, o que pode ajudar os profissionais a se manterem atualizados com as últimas tendências e tecnologias em segurança.

2- Para o setor da privada:

- Melhor qualidade dos serviços: A CPSI ajuda a garantir que os profissionais de segurança sejam qualificados e experientes. Isso pode levar a uma melhor qualidade dos serviços de segurança oferecidos.
- Redução de riscos: Pode ajudar a reduzir os riscos para as empresas e organizações que contratam profissionais de segurança comprovadamente qualificados e competentes.
- Melhor imagem do setor: A CPSI ajuda a melhorar a imagem do setor de segurança privada ao incentivar e contribuir para a capacitação continua dos profissionais da segurança.

Como e Onde Obter o CPSI?

O processo de obtenção do CPSI exige que os candidatos atendam a requisitos específicos estipulados pela CEAS Internacional. É direcionado a profissionais com experiência comprovada na área de segurança, incluindo anos em um cargo de responsabilidade. O candidato interessado terá de submeter seu currículo à análise da Comissão de Certificação da CEAS, demonstrando sua qualificação.

Mai informações sobre o Certificado Profesional en Seguridad Internacional "CPSI" pode ser obtida no site do CEAS Brasil ou pelo e-mail contato@ceasbrasil.com.br.

Por Que Devo Ser um Profissional Certificado CPSI?

Ser um profissional certificado CPSI confere uma série de benefícios. Além do reconhecimento internacional, a certificação valida suas competências, abrindo portas para oportunidades de ascensão e aumentos salariais. Empresas multinacionais, cada vez mais, buscam profissionais certificados para garantir os mais altos padrões de segurança em suas operações.

O Certificado Profesional en Seguridad Internacional não apenas valida as competências dos profissionais de segurança, mas também eleva o padrão da indústria global, promovendo a segurança eficaz em um mundo cada vez mais interconectado. Investir na obtenção do CPSI é investir em um futuro profissional seguro, reconhecido e respeitado internacionalmente.

Principais Benéficos do Certificado Profesional en Seguridad Internacional "CPSI"

Reconhecimento profissional: A certificação valida as competências do profissional de segurança, proporcionando reconhecimento formal de sua capacitação na área. Isso pode aumentar a confiança e respeito dos empregadores, clientes e colegas de trabalho;

Credibilidade profissional: A certificação confere credibilidade ao profissional, demonstrando que ele atende a um conjunto de padrões estabelecidos por uma organização certificadora independente e respeitada no seguimento da

segurança. Isso pode ajudar a elevar a reputação do profissional e melhorar suas perspectivas de emprego e carreira.

Oportunidades de emprego: Muitas organizações valorizam profissionais certificados em processos de contratação. A certificação pode ser um fator diferencial na escolha de um candidato, oferecendo vantagens competitivas e ampliando as oportunidades de emprego.

Progressão na carreira: A certificação pode abrir portas para promoções e avanço na carreira. Ela pode ser um critério importante para o crescimento profissional, permitindo que os profissionais de segurança se destaquem e sejam considerados para cargos de maior responsabilidade e remuneração.

Atualização de conhecimentos: A obtenção e a manutenção da certificação CPSI exige a educação continuada e atualização de conhecimentos. Isso incentiva os profissionais a se manterem atualizados sobre as melhores práticas, novas tecnologias e tendências emergentes no campo da segurança.

Networking e pertencimento a comunidades: A certificação CPSI permite que os profissionais se conectem com outros membros da comunidade de segurança certificados, o que pode levar a oportunidades de networking, colaboração e compartilhamento de conhecimentos.

Padronização de conhecimentos e práticas: A certificação estabelece um conjunto comum de conhecimentos e competências para os profissionais de segurança. Isso contribui para a padronização das práticas da indústria, garantindo que os profissionais estejam alinhados com as melhores práticas e normas estabelecidas.

Conclusão

O Certificado Profesional en Seguridad Internacional (CPSI) não apenas representa um marco em sua carreira de segurança, mas também é a chave para abrir portas em um mundo profissional cada vez mais competitivo.

Neste artigo, exploramos os benefícios substanciais desta certificação, desde o reconhecimento profissional até as oportunidades de carreira ampliadas. Ao investir no CPSI, você não só investe em si mesmo, mas também contribui para elevar os padrões globais da indústria de segurança privada.

Para continuar sua jornada de aprimoramento profissional, convido você a explorar nosso próximo artigo sobre Certificação Profissional: o que significa, sua importância e como ela beneficia os profissionais. Este é o próximo passo na construção de uma carreira sólida e respeitada. Descubra como as certificações moldam o caminho para o sucesso.

José Sergio Marcondes – CES – CPSI – Gestor, Consultor e Diretor do IBRASEP. Especialista em segurança com competências sólidas nas áreas de segurança privada e gestão empresarial. Conecte comigo nas redes sociais.

Ajudar a divulgar nosso trabalho é fundamental! Curta e compartilhe nossas publicações com seus amigos nas redes sociais. Essa atitude não apenas incentiva o autor a publicar mais artigos relevantes, mas também possibilita que mais pessoas tenham acesso a esse conteúdo valioso.

“DESCUBRA OS SEGREDOS PARA O SUCESSO NA PROFISÃO DE VIGILANTE: 10 DICAS ESSENCIAIS”

José Sergio Marcondes, CES, CPSI

Conheça os Segredos do Sucesso na Profissão de Vigilante: Estratégias práticas para alcançar reconhecimento, satisfação pessoal e avanço na carreira.

O sucesso na profissão de vigilante é um conceito subjetivo e pessoal, variando de acordo com os objetivos, valores e aspirações de cada profissional. Não se restringe apenas a aspectos financeiros, abrangendo também elementos como satisfação pessoal, equilíbrio entre vida pessoal e profissional, desenvolvimento contínuo e reconhecimento por um trabalho significativo.

Neste contexto, já parou para pensar nos requisitos necessários para se destacar na desafiadora profissão de vigilante e alcançar o tão desejado sucesso? Essa carreira demanda competências técnicas, interpessoais e comportamentais específicas, além de exigir dedicação e uma postura exemplar em diversas situações.

Se você está em busca de orientações sólidas para prosperar e alcançar sucesso na desafiadora profissão de vigilante, está no lugar certo. Este é o artigo onde você absorverá dicas valiosos e inspiradores, essenciais para impulsionar sua carreira e atingir os objetivos almejados.

Neste artigo, exploraremos os conceitos fundamentais de carreira e sucesso profissional, desvendando os segredos para se destacar na profissão de vigilante. Você terá acesso a dicas práticas e comprovadas, essenciais para trilhar um caminho de destaque nesse campo desafiador.

O Caminho para o Sucesso na Profissão de Vigilante?

O sucesso profissional é um conceito subjetivo e pessoal que varia de acordo com os objetivos, valores e aspirações individuais de cada pessoa. Em termos gerais, pode-se dizer que o sucesso profissional envolve o alcance de objetivos e realizações significativas no contexto do trabalho e da carreira.

Assim como em qualquer outra profissão, a carreira de vigilante é uma jornada individual, permeada por desenvolvimento e progresso ao longo do tempo. Inicia-se com a escolha consciente da profissão, seguida por uma busca contínua por educação e treinamento específico, elementos essenciais para adentrar o campo da segurança privada.

A trajetória do vigilante se delineia conforme ele adquire conhecimentos e habilidades prática, avançando para posições mais estratégicas e assumindo responsabilidades adicionais. A progressão na carreira de um vigilante pode incluir especializações em áreas específicas, como segurança eletrônica, eventos, transporte de valores, escolta armada ou segurança pessoal. Essa

especialização não apenas aprofunda seus conhecimentos técnicos, mas também abre portas para oportunidades mais especializadas e financeiramente recompensadoras.

Indicadores de Sucesso na Profissão de Vigilante

O sucesso na carreira de vigilante vai além de aspectos financeiros ou status social; ele abrange satisfação pessoal, equilíbrio entre vida profissional e pessoal, desenvolvimento contínuo e contribuição significativa para a segurança do cliente e comunidade em geral. Reconhecimento, reputação, progressão na carreira e a realização de objetivos pessoais são indicadores-chave de uma carreira bem-sucedida.

O vigilante de sucesso é aquele que encontra significado e propósito no seu trabalho, mantendo um equilíbrio saudável entre as demandas profissionais e pessoais. Além disso, o reconhecimento pela competência, confiabilidade e respeito na comunidade profissional são marcadores cruciais de sucesso na profissão de vigilante.

Possibilidades de Crescimento na Profissão de Vigilante

A profissão de vigilante oferece diversas opções de crescimento e avanço na carreira. Estas incluem:

1. **Especialização em Áreas Específicas**: Aprofundar-se em setores específicos da segurança privada, como segurança eletrônica, eventos, segurança pessoal ou transporte de valores, proporciona conhecimentos técnicos mais especializados.
2. **Supervisão ou Coordenação:** Profissionais experientes e com habilidades de liderança podem avançar para cargos de inspeção e supervisão, orientando e supervisionando outros vigilantes.
3. **Gerenciamento de Segurança**: Com experiência consolidada e nível educacional aduado, é possível buscar posições de gerenciamento, onde se planeja, implementa e supervisiona estratégias de segurança em organizações.
4. **Consultoria em Segurança**: Tornar-se consultor de segurança, oferecendo serviços especializados a empresas que buscam aprimorar suas práticas de segurança, é uma opção valiosa para profissionais experientes e com boa formação.
5. **Empreendedorismo**: Abrir um negócio de segurança privada, oferecendo serviços especializados no seguimento, é uma possibilidade para vigilantes empreendedores, que tem uma visão maior e mais ambiciosa com relação a sua participação no setor da segurança privada.

A progressão na carreira depende de fatores como educação, treinamento, conhecimento, habilidade atitude, oportunidade e demanda do mercado. Buscar aprimoramento contínuo, participar de cursos e demonstrar comprometimento

com a excelência profissional são fundamentais para avançar na área da segurança privada.

Dicas Essenciais para o Vigilante de Sucesso

1.Educação e Treinamento: Investir em formação e qualificação adequada por meio de cursos é fundamental para desempenhar as funções de vigilante com eficácia e em conformidade com as regulamentações.

2.Conhecimento da Legislação: Estar familiarizado com as leis e regulamentos pertinentes à profissão é crucial para atuar dentro dos limites legais e garantir conduta profissional adequada.

3.Desenvolvimento de Habilidades de Comunicação: A comunicação eficaz, tanto verbal quanto escrita, é essencial para interações bem-sucedidas, exigindo habilidades de expressão clara e escuta ativa.

4.Manter-se Atualizado: O acompanhamento contínuo das mudanças na área de segurança privada, bem como a participação em cursos de atualização, é vital para se manter competitivo.

5.Cultivar Habilidades Interpessoais: Desenvolver empatia, respeito e diplomacia facilita a interação com pessoas de diversas origens, contribuindo para um ambiente seguro.

6.Manter a Calma Sob Pressão: Em situações de emergência, a capacidade de manter a calma e agir de acordo com protocolos estabelecidos é essencial.

7.Cultivar a Ética Profissional: Honestidade, integridade e profissionalismo são características cruciais para um vigilante bem-sucedido, garantindo conduta ética em todas as situações.

8.Buscar Oportunidades de Desenvolvimento: Estar aberto a novas oportunidades de aprendizado e crescimento é essencial para expandir conhecimentos e redes de contatos.

9.Cuidar de Si Mesmo: A saúde física e emocional é vital para o desempenho consistente, exigindo hábitos saudáveis, boa forma física e cuidados com o bem-estar.

10.Ser Resiliente: A resiliência, a capacidade de se adaptar e se recuperar diante de desafios, é fundamental para lidar com as demandas físicas, emocionais e mentais da profissão.

Essas dicas fundamentais contribuem para o sucesso de um vigilante, possibilitando uma carreira sólida e gratificante na área de segurança privada. O equilíbrio entre educação, habilidades interpessoais e resiliência é a chave para um desempenho excepcional nesse campo dinâmico e desafiador.

Conclusão

Neste artigo, exploramos os segredos para alcançar o sucesso na profissão de vigilante, desvendando estratégias e dicas práticas para se destacar nesse campo desafiador. Recapitulando os principais pontos abordados, enfatizamos a importância do desenvolvimento de competências técnicas, interpessoais e comportamentais.

A profissão de vigilante exige um compromisso contínuo com a excelência e a ética profissional. Além disso, é fundamental cultivar a resiliência para lidar com situações desafiadoras e manter a calma sob pressão. O sucesso na profissão não se limita à proteção física, mas envolve também o estabelecimento de relacionamentos positivos com colegas de trabalho, superiores, clientes e o público em geral.

Considerando esses aspectos, reforçamos a importância de continuar buscando o aprimoramento profissional e o desenvolvimento pessoal. Para isso, convidamos você a ler nosso próximo artigo, 'Descubra as Opções de Carreira na Segurança Privada'. Nesse conteúdo, você encontrará informações valiosas sobre as diversas possibilidades de carreira na segurança privada, bem como conselhos práticos para alcançar o sucesso em sua jornada profissional.

Se você gostou do artigo e achou útil, por favor, deixe um comentário logo abaixo para compartilhar sua opinião conosco. Ela é extremamente valiosa para mim!

Um forte abraço e votos de sucesso!

José Sergio Marcondes – CES – CPSI – Gestor, Consultor e Diretor do IBRASEP. Especialista em segurança com competências sólidas nas áreas de segurança privada e gestão empresarial. Conecte comigo nas redes sociais.

“Empresas brasileiras continuam com nível de segurança cibernética abaixo da média mundial”

Antonio Brasiliano, PhD, DICS, MCRC, CIEAI, CEGRC MBCR, CIEAC, CPSI, CIGR, CRMA, CES, DEA, MBS!

As empresas brasileiras continuam capengando em termos de segurança cibernética. O nível de segurança se encontra abaixo da média mundial, o que significa que, embora ainda haja preocupação por parte dos executivos C-Level e do Conselho de Administração, as ações ensaiadas até agora podem ser consideradas pífias. Não há planejamento e muito menos visão holística dos riscos interconectados que interferem na segurança cibernética.

Podemos citar a pesquisa internacional do MIT, com seu Índice de Defesa Cibernética, conforme descrito abaixo.

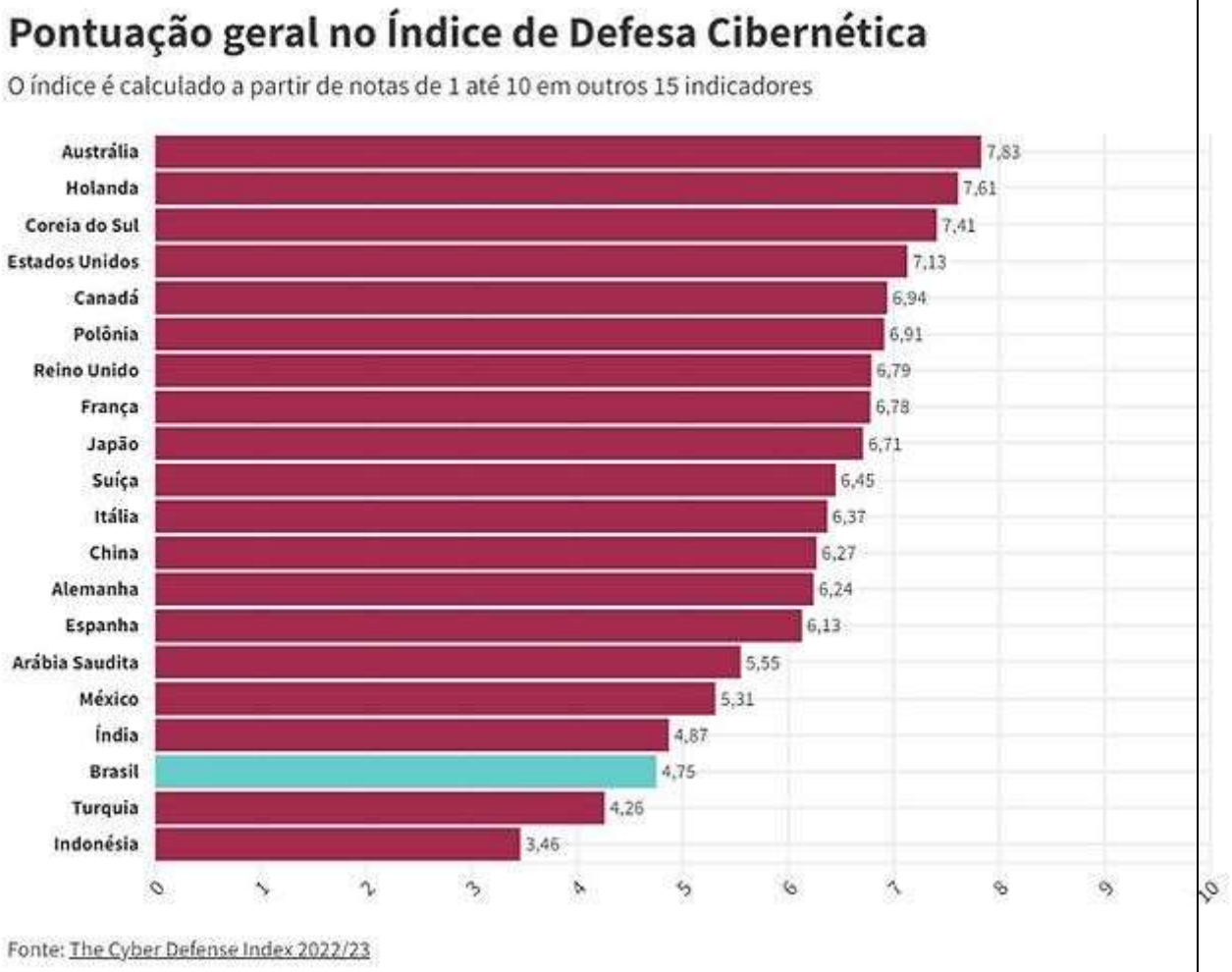
Pesquisa do Índice de Defesa Cibernética – MIT Technology Review – 2022/2023

Publicado pelo Insights, braço do MIT Technology Review, o Índice de Defesa Cibernética mede a capacidade das maiores economias digitais do mundo de se preparar, responder e se recuperar ante ameaças à cibersegurança. O indicador avalia a adoção, pelas instituições dos 20 países analisados, de tecnologias e práticas digitais para aumentar sua resiliência a ataques cibernéticos. Além disso, a pontuação traduz o nível de segurança das transações digitais promovidas pelos governos e estruturas políticas de cada país.

São 15 indicadores formulados para medir as pontuações, distribuídos em 4 grandes dimensões:

1. **infraestrutura crítica;**
2. **recursos de cibersegurança;**
3. **capacidade organizacional;**
4. **comprometimento com as políticas públicas.**

De acordo com o Índice de Defesa Cibernética do MIT Technology Review Insights realizado entre 2022 e 2023, o Brasil está em posição desfavorecida quando o assunto é cibersegurança. Após dois anos de uma pandemia que forçou e antecipou o processo de digitalização, o País ficou entre os três com progresso mais lento na criação das defesas cibernéticas, à frente apenas da Turquia e da Indonésia. Isso explica por que as empresas, tanto públicas quanto privadas, vêm apanhando constantemente dos hackers.

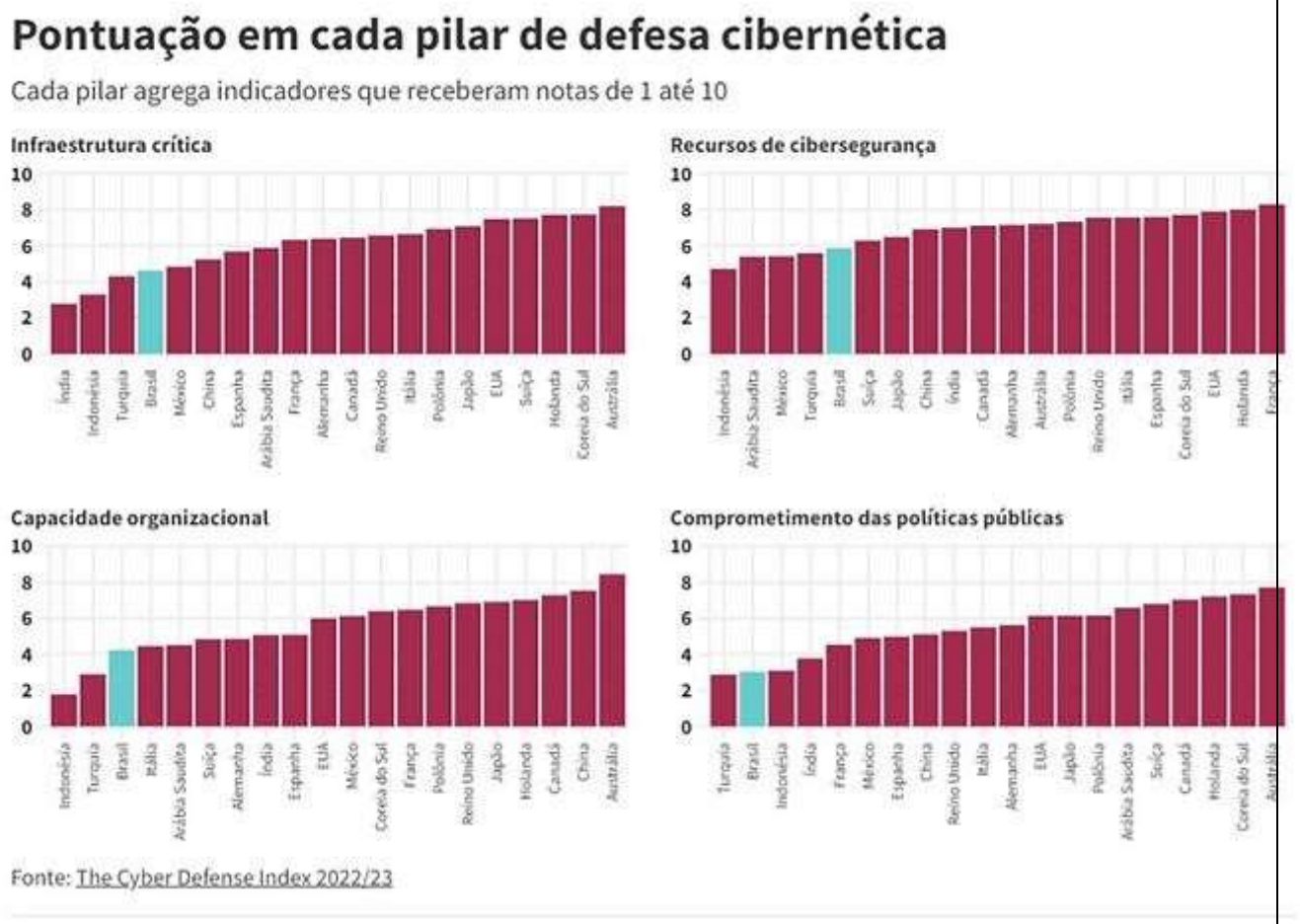


Fonte: The Cyber Defense Index 2022/23

O indicador de infraestrutura crítica avalia se o país dispõe de redes de telecomunicações digitais seguras e robustas e os recursos computacionais que sustentam as principais atividades econômicas. É também levado em consideração um indicador geral de capacidade de telecomunicação avaliado pelas Nações Unidas, além de métricas para incorporar o número de data centers e servidores seguros disponíveis no país. Também foram feitas entrevistas com especialistas globais sobre a robustez da infraestrutura de telecomunicações de cada economia. Coletivamente, os indicadores deste pilar equivalem a 30% da pontuação final do Índice de Defesa Cibernética e, nele, o Brasil marcou 4,63 de 10 pontos possíveis.

Já o pilar de recursos de segurança cibernética reúne avaliações de mecanismos tanto tecnológicos quanto jurídicos para prevenir o acesso e o uso inadequado de dados sensíveis. Ele inclui a avaliação holística da agência das Nações Unidas especializada em tecnologias da informação e da comunicação, além da classificação de proteções de privacidade digital desenvolvida pela própria equipe de Insights do MIT Technology Review e de opiniões de entrevistados sobre a qualidade do emprego das ferramentas e da infraestrutura de segurança cibernética em seus respectivos mercados.

É no pilar de recursos de segurança cibernética que o Brasil apresenta seu melhor desempenho, com nota 5,87.



Já a avaliação da capacidade organizacional mede a relativa maturidade em cibersegurança e a experiência digital das empresas e instituições de cada país.

Esse pilar inclui a medida da participação digital no governo, até que ponto as organizações estão familiarizadas com a inteligência artificial e as avaliações de entrevistados sobre o grau em que os recursos de segurança cibernética estão integrados em suas organizações. Neste quesito, o Brasil marcou 4,24 pontos.

O último grupo de indicadores diz respeito ao comprometimento das políticas públicas do país com a segurança cibernética. Ele mede a abrangência, a qualidade e a eficácia do ambiente regulatório no aprimoramento e promoção de práticas resilientes de cibersegurança. Os indicadores que fazem parte deste pilar incorporam a avaliação do Banco Mundial sobre a eficácia do governo e a qualidade de sua regulamentação de segurança cibernética, além de avaliações de entrevistados sobre a robustez e integridade dessa regulamentação. Esta é a nota mais baixa do Brasil: 3,04 pontos.

Conclusão

A média do Brasil é muito baixa: 4,75. Esta nota demonstra pouca sensibilidade dos Conselhos de Administração, aliada ao desinteresse dos altos executivos em operacionalizar determinadas estratégias cibernéticas e, o mais importante, empoderar a área de riscos corporativos. Portanto, isso se aplica não somente à área de segurança de TI/TO/Cibernética, como também à área de riscos corporativos, caracterizando a necessidade de que a empresa disponha de uma segunda linha ativa, que funcione de fato como a supervisora de todas as topologias de riscos da empresa.

O maior erro que as empresas cometem é o de não integrar a gestão de riscos. Existem ainda determinadas áreas completamente segregadas da área de riscos corporativos, e, com isto a sintonia fina acaba sendo diluída. As empresas, em vez de investirem no entendimento das Joias da Coroa para saber o que de fato precisa ser protegido, investem muito tentando fechar uma grande superfície de ataque. O hacker, como estrategista que é, realiza o reconhecimento das vulnerabilidades e age sobre elas, explorando-as com eficácia, de forma a atingir seus resultados.

Já nos perguntamos mais de uma vez por que os investimentos em cibernética crescem e os ataques continuam a ocorrer. Devemos estar fazendo alguma coisa errada!

Continuaremos a enxugar gelo? O tempo dirá! Espero que nossa mentalidade mude, de modo a que tenhamos processos estruturados, metodologias e tecnologias eficazes, além de muita capacitação!!

Conheça a metodologia de segurança cibernética "**CYBERSECURITY RISKS – CSR**", que aborda a identificação e proteção das "Joias da Coroa", expressão usada em segurança da informação para se referir aos ativos mais valiosos e críticos de uma organização, como informações confidenciais, propriedade intelectual, dados sensíveis dos clientes e sistemas essenciais para as operações da empresa. Proteger as "Joias da Coroa" é fundamental para a segurança cibernética de uma empresa, pois o comprometimento desses ativos pode ter um impacto significativo nos negócios e na reputação da organização.

Antonio Celso Ribeiro Brasiliano, PhD, Doctor of Philosophy in International Security Sciences, pela Cambridge International University, Inglaterra, Reino Unido. Presidente da Brasiliano INTERISK.

“Novo Paradigma de Segurança. Novas Tecnologias e Aplicações”

Manuel Sánchez Gómez-Merelo

Consultor de Segurança Internacional

É evidente que vivemos numa sociedade onde o espaço a percorrer é cada vez maior e o tempo necessário para respostas é cada vez mais curto, portanto, os melhores resultados de segurança que podemos oferecer residem na nossa capacidade de adaptação à globalização e às mudanças no mundo. face aos novos desafios e exigências. Os avanços tecnológicos e a sua constante evolução dão-nos a oportunidade de desenvolver novos métodos, ferramentas e competências para nos mantermos seguros.

A segurança já não se encontra na estabilidade, mas na nossa capacidade de adaptação às mudanças dos tempos e às exigências particulares de cada caso e momento.

Novos desafios e exigências de segurança

Um contexto de insegurança global, onde conceitos como o ciberterrorismo ou o cibercrime estão cada vez mais presentes nas nossas atividades, o que exige novos desenvolvimentos dos mecanismos de cibersegurança.

Um novo campo de batalha digital, o ciberespaço, onde aumentam as ameaças, os riscos e as vulnerabilidades cibernéticas, com uma atividade crescente, tanto por parte dos Estados (em plena expansão dos seus interesses geopolíticos através de ações cibernéticas de natureza exploratória ou ofensiva), como das organizações terroristas, grupos de criminalidade organizada e outros intervenientes individuais.

Assim, no âmbito da União Europeia, o ciberespaço é definido como “o espaço virtual através do qual circulam os dados eletrônicos dos computadores do mundo”. Para esta organização supranacional à qual pertencemos: “Manter um ciberespaço aberto, livre e seguro é um desafio global que a UE deve enfrentar em conjunto com parceiros e organizações internacionais relevantes, o setor privado e a sociedade civil” (Conselho da União Europeia 2013 (12.02) (OR. em) 6225/13).

Perante novos desafios e exigências, em termos de riscos e ameaças, devemos avançar num conceito de segurança global e conceptual, que, ao contrário de tempos anteriores, se renova constantemente, e dentro de um espaço definido por quatro referências: circulação, complexidade, contingência e resiliência.

Neste renovado contexto de segurança, é necessário prestar especial atenção aos problemas apresentados pelas interdependências da segurança interna e da segurança externa, procurando uma maior dedicação de recursos ao tratamento global dos riscos e ameaças.

Novo paradigma de segurança

Estamos perante a abordagem de um novo paradigma afetado por um conjunto de conceitos, tecnologias, métodos e planos com visão e aplicação globais face a novos desafios e exigências de segurança.

As ameaças cibernéticas devem ser enfrentadas a nível global porque no atual ambiente internacional, caracterizado por tensões de baixa intensidade, com áreas limitadas de conflitos violentos, a “circulação global” causa uma ampla gama de problemas, incluindo a segurança da informação e das comunicações, e as ameaças cibernéticas devem ser enfrentadas, prevenidas, analisadas e combatidas, fornecendo soluções e respostas rápidas para eliminá-las.

Novos sistemas e tecnologias

Atualmente, assistimos a uma progressiva convergência de sistemas de tecnologia da informação (TI) com sistemas de tecnologia operacional (TO) e gestão de segurança, utilizados para o controle e monitoramento de eventos, processos, dispositivos e incidentes, realizando ajustes nas operações comerciais e industriais, o que indica que a inovação tecnológica será decisiva na sua transformação.

Assim, a convergência dos serviços em nuvem é acelerada, promovendo o surgimento de serviços mais rápidos e eficientes. Isto está levando a soluções inteligentes em tempo real, como controle e gerenciamento mais eficientes de sistemas de segurança baseados em nuvem, permitindo-nos ter análises imediatas e tomar melhores decisões no gerenciamento de sistemas em tempo real.

Da mesma forma, na recente Sicur2024 (Exposição Internacional de Segurança), a inovação e o desenvolvimento tecnológico foram os principais protagonistas deste encontro profissional onde foi abordada a segurança integral a partir de cinco grandes áreas (segurança, cibersegurança, segurança contra incêndios e emergências, segurança no trabalho). Aí destacaram as soluções de segurança mais inovadoras do mercado, fruto dos últimos avanços em investigação, desenvolvimento e inovação realizados pelas empresas do sector.

Nesse sentido, vale destacar a apresentação das tecnologias de Inteligência Artificial Imagem Signal Processing (AI-ISP), que estão revolucionando as imagens de vídeo e proporcionando visuais de alta qualidade graças à redução inteligente de ruído, com imagens mais claras e nítidas em ambientes com pouca luz., resultando em respostas mais direcionadas e eficientes. Novas soluções de segurança para autenticação de identidade digital, salvaguardas de segurança cibernética e verificação e autorização de identidade são avanços fundamentais.

Da mesma forma, a IA está a acelerar a transformação do sector da segurança, aumentando as capacidades perceptivas dos sistemas. Isto é possível graças à integração com luz visível, áudio, raio X, luz infravermelha, radar e outras tecnologias.

Deve-se ter em conta que as aplicações baseadas em IA estão destinadas a revolucionar vários setores, e uma preparação que proporcione conhecimentos básicos suficientes destas novas tecnologias ajudará a reforçar a utilização adequada e a acelerar as aplicações no domínio da segurança.

No entanto, há que ter em conta que a IA proporciona vantagens indubitáveis na recolha de informação, no seu processamento, na tomada de decisões e na autonomia dos sistemas, mas coloca grandes desafios éticos, legais e estratégicos.

A IA tem registado avanços significativos nas últimas décadas e a sua aplicação no domínio da segurança e da defesa revolucionou a forma como os governos e as forças armadas enfrentam os desafios contemporâneos. Desde a recolha de informações até à tomada de decisões estratégicas, a IA provou o seu valor em diversas áreas cruciais para a segurança nacional.

Cultura e treinamento de segurança

Novos profissionais de segurança não nascem, eles são feitos. Assim, as competências e conhecimentos necessários para poder utilizar as novas tecnologias neste novo paradigma de segurança refletiram-se na resolução de problemas, na capacidade de adoptar soluções rápidas ou de criar serviços novos, eficientes e eficazes, suscitados sob o conceito de global, abrangente e segurança integrada.

Para tal é fundamental renovar-nos, sair da zona de conforto e apostar numa cultura de segurança e na consequente formação contínua especializada, desenvolvendo capacidades futuras e cultivando a mentalidade de crescimento e adaptação aos novos desafios e exigências que os importantes área de segurança exige.

Não tenhamos medo da mudança, porque só através da aceitação e da procura ativa de novas competências e soluções poderemos garantir a nossa segurança (prevenção + proteção) numa sociedade em constante transformação. A mudança não é mais uma ameaça, mas uma oportunidade para crescer e atingir o nosso potencial máximo de segurança. As novas necessidades e novas abordagens à transformação digital e digitalização trazem novas ferramentas de gestão operacional em Segurança Pública e Segurança Privada e desafiam-nos a enfrentar, com preparação e entusiasmo, a implementação de novas soluções em sistemas e serviços integrados.

Além disso, esta abordagem de segurança global proporciona uma visão mais completa ao minimizar as obrigações inerentes ao cumprimento regulamentar em Espanha, como é o caso da Lei de Segurança Privada (Ministério do Interior, 2014), da Lei Orgânica de Proteção de Dados Pessoais de Caráter Pessoal (Ministério da Justiça, 1999) ou a Lei de Proteção de Infraestruturas Críticas (Ministério do Interior, 2011).

No entanto, deve-se ter em mente que nenhuma das novas abordagens e soluções para todos estes novos desafios e exigências em termos de segurança será possível sem a revisão, adaptação e adaptação à mudança dos próprios regulamentos, que necessitam de adaptação e abrangem requisitos como: a aprovação de tipos de contratantes, certificações de sistemas de segurança, certificações no domínio da segurança da informação face a novas ameaças

(como ataques cibernéticos ou crimes cibernéticos), novas medidas de segurança e cibersegurança que devem ser normalizadas, bem como a adaptação e regulamentação da formação e da formação especializada.

Resumindo

Estamos totalmente imersos num novo paradigma de segurança, novos sistemas de investigação, prevenção, proteção e resposta inteligente aos novos riscos e ameaças a serem enfrentados.

A complexidade derivada da globalização e a elevada interligação (de seguranças e inseguranças) devem ser adaptadas e contrastadas com a situação de segurança básica enfrentada pelas infraestruturas estratégicas e críticas em geral, com especial incidência em alguns países.

Em termos de segurança, é importante não esquecer e aceitar permanentemente a realidade de que não temos e não podemos ter tudo sob controlo. Segurança total não existe. Portanto, em vez de nos limitarmos a resolver as consequências das nossas vulnerabilidades, promovamos a força que a inteligência e a coordenação dos meios e medidas de segurança nos podem proporcionar.

Manuel Sánchez Gómez-Merelo

Consultor Internacional de Seguridad Pública y Privada

Presidente e Diretor Geral de Grupo Estudios Técnicos (GET)

Diretor de Círculo de Seguridad

Sócio-Consultor de ComOutGlobal

“Novos riscos, ameaças e exigências de segurança e resiliência”

Manuel Sánchez Gómez-Merelo

Atualmente, vivemos tempos turbulentos nas cidades de todo o mundo derivados de uma certa globalização de crises políticas, económicas e sociais que, de uma forma ou de outra, acarretam também novos riscos e ameaças que exigem uma maior exigência de segurança e resiliência. o momento.

Estes novos requisitos, juntamente com a expansão exponencial da digitalização, os novos dispositivos da Internet das Coisas (IoT) e as aplicações de Inteligência Artificial (IA), estão a expandir os limites da rede, ao mesmo tempo que aumentam as vulnerabilidades e o risco de ataques cibernéticos.

Novos riscos e ameaças

Deparamo-nos com a necessidade de rever a realidade dos nossos valores mobiliários devido ao aumento de novas ameaças ao desenvolvimento da vida social e das suas infraestruturas estratégicas e críticas, principalmente devido ao aumento da criminalidade cibernética e de outras consequências derivadas de conflitos armados como os que existem na Ucrânia, na Faixa de Gaza e em Israel. A isto somam-se fenómenos meteorológicos severos e desastres naturais resultantes das alterações climáticas.

Neste sentido, os ataques cibernéticos contra instituições públicas aumentaram 95 por cento só no último semestre de 2022 e, até 2025, estima-se que 30 por cento das infraestruturas críticas sofrerão uma violação de segurança.

O aumento dos riscos e ameaças e a importância das vulnerabilidades mostram, mais uma vez, que os governos e as entidades públicas e privadas devem melhorar a sua capacidade de prevenir e proteger contra riscos e reagir às ameaças.

Não fazer nada não é mais uma opção. Continuar a depender de sistemas ultrapassados ou obsoletos e de redes e tecnologias de comunicação isoladas, enquanto os riscos continuam a multiplicar-se, não é uma abordagem viável, e já não se pode confiar em estratégias passadas para construir a segurança e a resiliência que o século XX XXI impõe.

Vale destacar algumas considerações e desafios especiais para as redes e tecnologias de proteção da informação e das comunicações, bem como aplicar novas formas de pensar as vulnerabilidades que, com o desenvolvimento da digitalização, estão mais expostas a riscos e ameaças que podem espalhar rapidamente.

A digitalização também estreita a ligação entre riscos físicos e cibernéticos. A convergência entre TI e tecnologias operacionais (TO) cria vulnerabilidades e oportunidades para ataques.

Novas demandas por segurança e resiliência

O desenvolvimento de iniciativas de digitalização aumenta a agilidade operacional, a eficiência e a produtividade, mas novas salvaguardas devem ser revistas e propostas para proteger os cidadãos e as operações públicas e privadas, e a sua resiliência deve ser reforçada para que possam garantir a continuidade da operação em qualquer circunstância.

As organizações são um alvo potencial de ataques e, portanto, é necessária uma atenção renovada ao risco, à resiliência e à segurança para:

- **Garantir a continuidade de serviços críticos e estratégicos e proteger dados e informações confidenciais.**
- **Minimizar os custos de segurança, implementando proteção adequada para cada tipo de risco cibernético ou físico que enfrentam.**
- **Reduzir as perdas económicas e de prestígio devido a ataques cibernéticos e físicos.**
- **Manter a reputação e a confiança dos cidadãos.**
- **Proteger os cidadãos, fornecendo-lhes informações importantes relacionadas com a saúde e a segurança (prevenção e proteção).**

Neste sentido, os sistemas de notificação em massa podem alertar rapidamente as pessoas sobre os processos a implementar em situações de emergência, para que possam tomar as medidas necessárias e realizar as ações adequadas com base na sua segurança e na dos seus entes queridos.

Uma rede institucional e empresarial segura e resiliente apoia comunicações e ações de missão crítica, bem como IoT e tecnologias de segurança física e cibernética, que são essenciais para operações confiáveis.

Para aumentar a segurança e proteção em edifícios e espaços públicos, é necessária uma rede multisserviços segura que suporte as aplicações e processos necessários para proteger contra riscos e ameaças e manter a disponibilidade e continuidade do serviço em todos os momentos, com maior fiabilidade.

Cada organização, pública ou privada, deve desenvolver, com uma abordagem holística, estratégica e tática, processos padronizados de segurança e resiliência adaptados ao seu perfil de risco personalizado, localização, objetivos, etc.

Para aumentar a segurança e a resiliência, tendo em conta a evolução das inseguranças, devem ser delineadas e escolhidas soluções adequadas, reavaliando os riscos cibernéticos e físicos, as áreas de exposição e possíveis consequências, bem como as diferentes opções para prevenir, proteger e reagir. contra-ataques em cada caso, começando com uma auditoria para avaliar os riscos e o potencial de perda para cada vulnerabilidade identificada.

Para combater o cenário de ameaças em rápida mudança, é importante reavaliar periodicamente os riscos e monitorizar continuamente os riscos cibernéticos e físicos com recursos também para novas vulnerabilidades.

Novas tecnologias e procedimentos

Como já comentamos, o rápido desenvolvimento da digitalização trará benefícios, bem como novos riscos e vulnerabilidades, num mundo e numa sociedade globalmente digitalizados, em que pessoas, objetos, sistemas e processos estão conectados.

Esta ligação especial facilita a utilização da tecnologia IoT e, a informação que ela fornece, automatiza os fluxos de trabalho para aumentar a eficiência e acelerar as respostas para que as organizações e os cidadãos utilizem dados precisos e em tempo real, tanto para aumentar a sua visibilidade, como para tomar decisões informadas.

No entanto, vale a pena repetir que as tecnologias também introduzem um novo conjunto de riscos físicos e cibernéticos que devem ser abordados, uma vez que podem ser utilizados a favor e contra as organizações.

Podemos tomar a inteligência artificial (IA) como exemplo. A IA ajuda a prevenir, proteger e acelerar respostas a ameaças cibernéticas e físicas, mas também revela vulnerabilidades para ações maliciosas, como a quebra de palavras-passe de sistemas ou a própria manipulação de dados.

Aproveitar a inovação e a integração de serviços e tecnologia para mitigar os riscos dos processos e das pessoas reduzirá os perigos rumo à melhoria contínua com as mesmas soluções avançadas que ajudam a proteger os cidadãos, as infraestruturas e os espaços públicos seguros, com base em soluções flexíveis e compatíveis desde as fases iniciais de conceção. .

O reforço da segurança e da resiliência é um objetivo prioritário das instituições e organizações públicas e privadas, seguindo a abordagem e o processo holístico recomendado, e novas oportunidades para tirar partido das soluções de redes e comunicações são essenciais para permitir uma maior eficiência, eficácia e colaboração, protegendo e garantindo aos cidadãos segurança.

Manuel Sánchez Gómez – Merelo
Consultor Internacional de Seguridad Pública y Privada
Presidente de Grupo Estudios Técnicos (GET)
Director de Círculo de Seguridad
Socio-Consultor de ComOutGlobal

“O papel reservado à Inteligência Artificial na implantação da Agenda ESG”

Décio Luís Schons, *CIEAI, CEGRC, CIGR, CISI*

Há pouco mais de um ano, a empresa OpenAI revelava ao mundo o ChatGPT, despertando enorme entusiasmo – e preocupação – sobre o progresso acelerado da inteligência artificial (IA).

Neste texto, falaremos, básica e resumidamente, sobre os impactos reais e presumidos da IA sobre a Agenda ESG.

Já são claramente perceptíveis os benefícios que esse novo ator tecnológico poderá trazer às atividades humanas em geral e à Agenda ESG em particular. Na verdade, trata-se de uma ferramenta poderosa que pode ser usada para melhorar as práticas ESG e até mesmo revolucionar a forma como encaramos esse tema. Ao automatizar tarefas, identificar padrões e fazer previsões, a IA pode ajudar as empresas a reduzir o seu impacto ambiental, a melhorar a sua responsabilidade social e a reforçar a sua governança.

Na dimensão Meio Ambiente, é sabido que a IA vem ajudando as empresas a prever condições meteorológicas extremas com mais precisão. Sabe-se também que o agronegócio tem sido beneficiado com o desenvolvimento de variedades mais resistentes à seca e a determinadas pragas agrícolas. Enquanto isso, uma área bastante sensível, que é a gestão de resíduos, é bastante beneficiada pelo emprego da IA para auxiliar na identificação precisa do lixo reciclável.

A IA é muito útil na coleta e análise de grandes quantidades de dados ESG, o que irá certamente ajudar as empresas a identificar tendências, a acompanhar o desempenho próprio e das demais empresas do seu setor e a tomar decisões mais informadas.

Na área de Gestão de Riscos, os métodos de IA podem ser usados para avaliar a exposição de uma empresa aos riscos ESG, tais como aqueles embutidos nas alterações climáticas, os inerentes às práticas laborais e à governança corporativa. Esses dados e informações são valiosos no desenvolvimento de estratégias para mitigar riscos e proteger a reputação das empresas.

A IA tem um papel importante na identificação de oportunidades de investimento sustentável e no desenvolvimento de estratégias de investimento que se alinhem com os objetivos ESG de uma empresa. Ela tem ainda o potencial de ser usada para envolver as partes interessadas e coletar feedback sobre iniciativas ESG. Essas informações auxiliam a melhorar o desempenho e a construir confiança entre as partes interessadas.

Por outro lado, como nem tudo são flores, já vêm sendo externadas preocupações quanto aos impactos que a inteligência artificial poderá exercer sobre as mais variadas atividades, com reflexos desta vez negativos sobre a Agenda ESG.

Uma consequência das mais funestas do uso da IA diz respeito à utilização de dados viciados. Obviamente, decisões tomadas a partir de dados obtidos com algum viés serão intrinsicamente tendenciosas, podendo mesmo vir a ser injustas ou discriminatórias. Por exemplo, um modelo de empréstimo alimentado por IA com dados tendenciosos do passado pode inclinar-se a negar empréstimos a pessoas de determinadas etnias, mesmo que estas sejam tão dignas de crédito quanto os mutuários pertencentes ao grupo predominante naquele ambiente.

Outro perigo digno de nota diz respeito a possíveis comprometimentos da privacidade. Por exemplo, um sistema de marketing alimentado por IA que rastreie a atividade online das pessoas poderia coletar dados sobre suas preferências pessoais, dados esses que seriam usados depois para influenciar suas decisões mediante o uso de publicidade – algo que seria eticamente inadmissível.

Não passa despercebido a qualquer observador o progressivo processo de automatização de muitas tarefas atualmente realizadas por seres humanos, o que pode levar à pura e simples eliminação de empregos. Como exemplos disso, podemos citar os chatbots com tecnologia de IA fazendo o trabalho dos representantes de atendimento ao cliente e os algoritmos de negociação com tecnologia de IA assumindo o lugar dos analistas financeiros.

A desumanização da força de trabalho pela IA ameaça a estrutura socioeconômica de qualquer sociedade, ao mesmo tempo em que introduz o potencial de discriminação nas decisões relativas a emprego. Nesse sentido, a greve de quatro meses de duração, desencadeada em julho deste ano pelo sindicato dos atores de Hollywood, é emblemática dos problemas que podem ser causados pelo uso irresponsável da IA.

Em recente aparição pública, o Sr Elon Musk, proprietário da Tesla e do X (antigo Twitter) classificou a IA como a força mais perturbadora da história, chegando mesmo a afirmar que “chegará um ponto em que nenhum trabalho será necessário”.

É de fato provável que a IA tire os empregos de milhões de trabalhadores ao redor do mundo. Para completar, ela irá certamente contribuir para agravar o quadro de desigualdade digital hoje existente, uma vez que não estará acessível a todas as partes interessadas. Esse aspecto é definitivamente conflitante com os ideais de inclusão social tão alardeados pelos entusiastas das práticas ESG. As grandes

empresas de tecnologia do Vale do Silício já começam a sentir a pressão dos acionistas focados em ESG, preocupados com a eliminação de empregos devido à IA.

Talvez o aspecto mais constrangedor de todo o processo seja a possibilidade de concretização de uma hipótese até agora estabelecida apenas nos enredos de filmes de ficção científica. Na medida em que os sistemas de IA se tornam mais sofisticados, eles podem se tornar mais difíceis de controlar, o que pode levar a IA a tomar decisões que não atendam aos melhores interesses de seus proprietários. Por exemplo, um sistema bélico controlado por IA poderia decidir pelo uso de armas nucleares, mesmo que tal hipótese contrariasse a vontade dos decisores humanos.

Como é fácil perceber, estamos tratando aqui de efeitos desencadeados a partir da utilização da IA e que afetam diretamente as dimensões mais sensíveis da Agenda ESG, quais sejam o Capital Humano e o Capital Social, com sérias possibilidades de interferência também na dimensão Ambiental. Sendo assim, é intuitiva a necessidade de implantação de diretrizes de governança de dados e sistemas de gestão de riscos corporativos nas organizações, de modo a fazer face a essas circunstâncias.

Não existem respostas prontas nem soluções fáceis para as grandes questões que envolvem o tema e que estarão cada vez mais presentes em nosso cotidiano. Como partes interessadas na questão, cabe-nos estudar o assunto, de modo a ter opinião bem-embasada a respeito.

Se sua empresa deseja se aprofundar em gerenciamento de riscos ou em outros temas relacionados, entre em contato conosco, na Brasiliano INTERISK. Oferecemos soluções de Inteligência e Gestão de Riscos com base na Interconectividade, garantindo transparência nos processos de Governança, Riscos e Compliance.

O **INTERISK** é uma plataforma tecnológica e automatizada que integra diversos módulos – entre eles, o **Software de ESG**, que aplica questionários personalizados, mede a maturidade dos padrões ESG e fornece uma visão integrada da cultura, maturidade e perfil de risco da empresa. Isso possibilita à empresa avaliar sua posição atual e estabelecer metas de maturidade.

Décio Luís Schons, CIEAI, CEGRC, CIGR, CISI - General-de Exército da Reserva, é Vice-Presidente de Operações de Consultoria da empresa Brasiliano INTERISK

“O Papel Vital da Segurança Ativa no Universo da Segurança Física: Como contribui para proteção”

José Sergio Marcondes – CES – CPSI

Saiba como as medidas de segurança ativa contribuem para o fortalecimento da segurança física. Conheça as principais medidas para prevenir e responder a ameaças

Segurança Ativa refere-se a medidas e tecnologias que exigem intervenção ou ação direta para prevenir ou responder a ameaças iminentes. Ao contrário da segurança passiva, que se baseia em barreiras físicas e estruturais, a Segurança Ativa envolve o uso de sistemas eletrônicos, dispositivos e procedimentos que demandam uma resposta ativa por parte de operadores humanos ou inteligência artificial.

Essas medidas desempenham um papel crucial na promoção da segurança física ao possibilitar detecção, alerta e resposta rápidos diante de ameaças e eventos adversos. Essa abordagem permite intervenções pontuais e eficazes, contribuindo para a proteção de vidas, propriedades e ativos.

Em um cenário onde ameaças iminentes exigem respostas rápidas e eficientes, a Segurança Ativa emerge como a resposta dinâmica que redefine a forma como enfrentamos desafios no campo da segurança.

Neste artigo, exploramos os principais conceitos, tipos e aplicações da Segurança Ativa. Prepare-se para descobrir como essa abordagem está moldando o futuro da proteção física, proporcionando não apenas detecção precoce, mas também uma resposta proativa a situações críticas.

No contexto da segurança física, o termo “segurança ativa” refere-se a medidas e tecnologias que demandam intervenção ou ação direta para prevenir ou responder a ameaças iminentes. Ao contrário da segurança passiva, que se baseia em medidas físicas e estruturais, a segurança ativa envolve o uso de sistemas eletrônicos, dispositivos, e procedimentos que necessitam de uma resposta ativa por parte de operadores humanos ou inteligência artificial. Essas medidas são projetadas para identificar, alertar e, em alguns casos, intervir diante de situações de risco ou ameaças.

Essas medidas ativas incluem, entre outras coisas, sistemas de vigilância, sistemas de alarme, controles de acesso eletrônicos, O objetivo primário da segurança ativa é proporcionar uma resposta rápida e eficiente diante de ameaças identificadas, contribuindo para a proteção de vidas, propriedades e ativos.

Em resumo, a segurança ativa é uma abordagem dinâmica que se concentra na detecção proativa e na resposta imediata a situações de risco, complementando as medidas de segurança passiva para criar um sistema global e robusto de proteção.

Objetivos da Segurança Ativa

Os objetivos da segurança ativa no contexto da segurança física são centrados em detecção, alerta e resposta rápidos diante de ameaças de segurança ou eventos adversos. A seguir alguns dos principais objetivos associados à implementação de medidas de segurança ativa:

- **Integração com Medidas Passivas:** Garantir uma integração eficiente com as medidas de segurança passiva para criar um sistema abrangente e equilibrado.
- **Prevenção e Dissuasão:** Desencorajar potenciais intrusões ou atividades criminosas por meio da presença visível de sistemas de segurança ativa, como câmeras e alarmes.
- **Monitoramento Contínuo:** Manter uma vigilância constante sobre áreas críticas ou sensíveis para identificar padrões incomuns ou atividades suspeitas.
- **Detecção Imediata de Ameaças:** Identificar e reconhecer prontamente qualquer atividade suspeita, intrusão ou evento que represente uma potencial ameaça à segurança.
- **Alerta Rápido:** Emitir alertas imediatos e eficazes para operadores de segurança e equipe de pronta respostas diante de situações de emergência ou atividades fora do padrão.
- **Coordenação Eficiente:** Facilitar alertas e comunicação e a coordenação eficazes entre as equipes de segurança, permitindo uma resposta rápida e coordenada.
- **Resposta Imediata a Intrusões:** Iniciar prontamente procedimentos de resposta, como a mobilização de equipes de segurança ou a ativação de barreiras, em caso de detecção de intrusões.
- **Minimização de Danos:** Reduzir o impacto potencial de eventos adversos, como incêndios, vazamentos de gases ou intrusões, por meio de respostas rápidas e eficientes.
- **Conformidade com Normas e Regulamentações:** Atender às normas e regulamentações relevantes, garantindo que as medidas de segurança ativa estejam em conformidade com padrões específicos do setor.
- **Fornecer Evidências para Investigações:** Coletar e armazenar dados, informações e evidências úteis em caso de incidentes para facilitar investigações posteriores.

A implementação eficaz de medidas de segurança ativa contribui para um ambiente mais seguro, proporcionando não apenas a detecção precoce de ameaças, mas também uma resposta rápida e coordenada para mitigar os riscos associados a eventos adversos.

Qual a importância das Medidas de Segurança Ativa?

As medidas de segurança ativa desempenham um papel crucial na promoção da segurança física ao oferecer detecção, alerta e resposta rápidos diante de ameaças e eventos adversos. A importância dessas medidas pode ser destacada por vários motivos:

- **Detecção Precoce de Ameaças:** As medidas de segurança ativa permitem a identificação imediata de atividades suspeitas ou ameaças potenciais, possibilitando a tomada de medidas preventivas antes que situações adversas se desenvolvam.
- **Alerta Imediato e Comunicação Eficiente:** A capacidade de emitir alertas rápidos proporciona uma comunicação eficiente entre os sistemas de segurança e as equipes responsáveis, permitindo uma resposta coordenada e rápida.
- **Prevenção de Incidentes Críticos:** Ao dissuadir potenciais intrusões ou atividades criminosas, as medidas de segurança ativa desempenham um papel fundamental na prevenção de incidentes críticos e na proteção de propriedades e pessoas.
- **Minimização de Perdas em Caso de Incidentes**: Em situações como incêndios ou vazamentos de substâncias perigosas, a detecção precoce possibilita a ativação rápida de sistemas de segurança para minimizar perdas materiais e proteger vidas.
- **Aumento da Consciência Situacional:** As medidas de segurança ativa proporcionam uma visão mais abrangente da situação, permitindo uma avaliação precisa do ambiente e a tomada de decisões informadas.
- **Integração com Medidas de Segurança Passiva:** Ao trabalhar em conjunto com medidas de segurança passiva, as medidas ativas oferecem uma abordagem holística para a segurança física, proporcionando camadas complementares de proteção.
- **Sensação de Segurança:** A presença de medidas de segurança ativa pode aumentar a sensação de segurança entre os ocupantes de um ambiente, promovendo um ambiente mais tranquilo e protegido.

Em resumo, as medidas de segurança ativa desempenham um papel essencial na criação de ambientes seguros, proporcionando uma resposta eficaz a eventos adversos e contribuindo para a proteção de vidas, propriedades e ativos críticos. A integração equilibrada de medidas ativas e passivas é fundamental para estabelecer uma abordagem completa e eficaz para a segurança física.

Principais Medidas de Segurança Ativa

As principais medidas de segurança ativa variam de acordo com o contexto e os requisitos específicos de cada ambiente. No entanto, algumas medidas são comumente utilizadas em diversos setores para promover a segurança. A seguir algumas das principais medidas de segurança ativa:

- **Sistemas de Vigilância por Vídeo:** Câmeras de vigilância monitoradas em tempo real ou gravadas para detecção e registro de atividades suspeitas.
- **Sistema de Alarmes de Segurança:** Dispositivos que identificam movimento ou intrusão em áreas específicas e emitem alertas quando detectam atividades não autorizadas.
- **Controle de Acesso Eletrônico:** Sistemas que regulam o acesso a áreas restritas por meio de cartões de proximidade, biometria ou outros métodos eletrônicos. Buscam garantir que apenas pessoas autorizadas tenham acesso a locais específicos.
- **Sistemas de Alarme de Incêndio:** Detectores de fumaça, calor ou chamas conectados a sistemas de alarme para alertar sobre potenciais incêndios.
- **Sistemas de Detecção de Gases:** Sensores que monitoram a presença de gases perigosos e emitem alertas em caso de vazamentos.
- **Sistemas de Controle de Iluminação**: Iluminação automatizada que responde a sensores de movimento ou horários específicos. Visam melhorar a visibilidade e dissuadir atividades suspeitas durante a noite.
- **Sistemas de Comunicação de Emergência:** Redes de comunicação dedicadas para coordenação eficiente durante situações de emergência. Visam a comunicação rápida e eficaz entre equipes de segurança.
- **Sistemas de Controle de Tráfego:** Barreiras automáticas, semáforos e sistemas de controle de tráfego para gerenciar o fluxo de veículos. Visam regulamentar o acesso a áreas específicas e garantir a segurança no trânsito.
- **Drones de Vigilância:** Utilização de drones equipados com câmeras para monitoramento aéreo, para ampliar a capacidade de vigilância em áreas extensas ou de difícil acesso.
- **Equipamentos de Detecção de Metal:** Detectores de metais para verificar a presença de objetos proibidos em locais específicos. Visam reforçar a segurança em áreas de acesso restrito.
- **Simulações de Crise e Treinamentos:** Exercícios regulares para simular situações de crise e testar a eficácia dos procedimentos de segurança. Visam preparar a equipe para responder eficazmente a situações adversas.

A implementação adequada dessas medidas de segurança ativa contribui para a criação de ambientes mais seguros, oferecendo uma resposta proativa a ameaças potencial.

Planejamento e Implementação da Segurança Ativa

O planejamento e implementação da segurança ativa envolvem uma abordagem estratégica e cuidadosa para garantir a eficácia dos sistemas e procedimentos. A seguir algumas das etapas do desenvolvimento e implementação de medidas de segurança ativa:

1. **Avaliação de Riscos:** Envolve a identificação e avaliação abrangente dos riscos específicos associados ao ambiente, identificando ameaças potenciais, vulnerabilidades e possíveis impactos.
2. **Objetivos e Metas de Segurança:** Refere-se ao estabelecimento de objetivos claros e metas mensuráveis para a segurança ativa, alinhados com os riscos identificados e as necessidades específicas do local.
3. **Arquitetura de Segurança:** Elaboração de um design abrangente dos sistemas de segurança ativa a serem implementados, considerando as tecnologias necessárias, layout físico, e integração com medidas passivas.
4. **Seleção de Tecnologias e Equipamentos:** Escolha cuidadosamente das tecnologias e equipamentos necessários para atender aos objetivos de segurança, considerando câmeras, sensores, sistemas de detecção, entre outros.
5. **Integração com Medidas Passivas:** Garantia de integração eficiente com as medidas de segurança passiva já implementadas, garantindo uma abordagem holística.
6. **Considerações Legais e Regulatórias:** Certifique-se de que todas as medidas de segurança ativa estejam em conformidade com as normas e regulamentações locais e setoriais.
7. **Treinamento e Conscientização:** Realização de treinamentos regulares para garantir que a equipe de segurança e outros usuários estejam familiarizados com os procedimentos e tecnologias implementadas.
8. **Simulações e Testes:** Conduza simulações de crises e testes regulares para garantir que os sistemas de segurança ativa funcionem corretamente e que a equipe esteja preparada para emergências.
9. **Avaliação e Atualização:** Realize avaliações periódicas dos sistemas de segurança ativa, identificando áreas de melhoria e realizando atualizações conforme necessário.
10. **Parcerias com Especialistas:** Considere a possibilidade de buscar orientação de especialistas em segurança eletrônica para garantir a eficácia e a atualização contínua dos sistemas. Lembre-se de que, a especialização pressupõe atuação na sua área de especialização e trabalho em conjunto com especialistas de outras áreas.

O planejamento e implementação eficazes da segurança ativa demandam uma abordagem holística, considerando aspectos técnicos, humanos e regulatórios para garantir uma proteção abrangente contra ameaças potenciais.

Conclusão

A Segurança Ativa revela-se como uma estratégia fundamental no contexto da segurança física. Desde a detecção proativa até a resposta eficaz, exploramos minuciosamente como essa abordagem dinâmica molda os padrões da segurança física.

Neste artigo, abordamos a definição, objetivos, principais tipos e a importância da segurança ativa, destacando seu papel crucial na promoção da segurança física ao oferecer detecção, alerta e resposta rápidos diante de ameaças e eventos adversos.

Ao encerrar, convido-o a ler o nosso próximo artigo sobre Segurança Passiva. Que não apenas revela os conceitos da Segurança Passiva, mas também oferece insights práticos sobre como criar ambientes verdadeiramente seguros desde a concepção.

Se você gostou do artigo e achou útil, por favor, deixe um comentário logo abaixo para compartilhar sua opinião conosco. Ela é extremamente valiosa para mim!

José Sergio Marcondes – CES – CPSI – Gestor, Consultor e Diretor do IBRASEP. Especialista em segurança com competências sólidas nas áreas de segurança privada e gestão empresarial.

“Paradigmas Ambientais e Agenda ESG”

Décio Luís Schons, CIEAI, CEGRC, CIGR, CISI

Ao longo da história da nossa civilização moderna, a paixão pelo lucro e pela posse de bens que destaquem o detentor entre seus pares tem sido uma constante. A mentalidade mercantilista estimula a busca da riqueza e da notoriedade social, muitas vezes a qualquer custo. A preocupação com os aspectos que dizem respeito ao indivíduo e sua família normalmente sobrepujam as considerações relativas à comunidade e à sociedade em geral. Num mundo em que os seres humanos se consideram em estado de permanente conflito com seus semelhantes, na competição por bens e proeminência social, as preocupações relacionadas ao bem-estar da coletividade não desfrutam de grande popularidade.

Um dos fatores contribuintes para essa forma egoísta de pensar foi sem dúvida a noção, amplamente disseminada, de que os recursos naturais do planeta seriam inesgotáveis, ou de que teriam uma duração tão extensa que não se justificariam ações mais custosas em benefício de sua preservação. Além disso, o bem-estar ou até mesmo a sobrevivência das futuras gerações não entrava nas cogitações da maioria das pessoas, em particular daquelas dotadas de poder de decisão. No mesmo passo, a influência da ação humana sobre o clima costumava ser considerada (e ainda é, por parte de muitos) mera fantasia sensacionalista com o objetivo de colher resultados a partir do amedrontamento de parcelas vulneráveis da população.

Nos últimos anos, vem tomando corpo a noção de que o desenvolvimento da sociedade deve ser pautada pelos parâmetros ESG (Ambiental, Social e de Governança). A consciência da finitude dos recursos naturais e da consequente necessidade de utilizá-los de forma racional vai assim, aos poucos, se agregando ao inconsciente coletivo. A favorecer essa percepção de que algo de anormal acontece com o clima da Terra temos a instabilidade e as alterações climáticas impulsionadas por fenômenos como o El Niño, sejam esses eventos decorrentes da ação humana, sejam decorrentes dos ciclos naturais característicos do planeta.

Em consequência dessa nova mentalidade, manifestações em diversas dimensões começaram a ocorrer ao redor do mundo, num processo favorecido em grande parte pela facilidade de acesso à informação e aos meios de comunicação. Assim é que diversos movimentos de conscientização e divulgação de conceitos e práticas alinhadas à preservação ambiental têm aflorado, indicando novas tendências que vão adquirindo características cada vez mais abrangentes.

A partir do momento em que um número ponderável de grandes empresas concluiu que esse processo era de fato inelutável, a prática dos princípios ESG passou a ser tomada a sério. A disposição, neste momento, é claramente a de assegurar que novos desastres ambientais, como aqueles ocorridos no Brasil há poucos anos, com o rompimento de barragens contendo resíduos de operações de mineração, nunca mais voltem a ocorrer.

Não há como negar que a complexidade das atividades econômicas aumentou sensivelmente a partir do momento em que os parâmetros ESG passaram a ser levados em consideração. Não se trata mais apenas de uma relação produtor-produto-consumidor, em que o lucro do produtor e a satisfação do cliente em relação ao produto fornecido eram os aspectos determinantes. O número de atores envolvidos aumentou muito, pois assumiram papel de destaque as partes interessadas (stakeholders), sejam elas representadas pelos acionistas, clientes, funcionários ou o público externo afetado de alguma forma pelas atividades da organização. Um olhar inquiridor também é dirigido aos integrantes da cadeia de valor, de modo a determinar se eles cumprem seus papéis no que se refere ao atendimento dos parâmetros ESG.

De forma até um pouco surpreendente, a Agenda ESG revelou-se, além de tudo, uma maneira eficaz de gerar valor em médio e longo prazos para os acionistas das empresas, permitindo conciliar o sucesso financeiro com o respeito aos padrões de responsabilidade socioambiental. Isso se deve em grande parte ao fato de a ampla difusão da temática ESG ter provocado, da parte de um stakeholder fundamental – o cliente – um olhar crítico sobre as práticas adotadas pelas empresas, condicionando sua boa vontade e disposição para o consumo do produto à satisfação dos parâmetros ESG por parte da empresa. Naturalmente, aquelas empresas que não atendem (ou que pelo menos não pareçam atender) a esses parâmetros deixarão de ter seus produtos acolhidos de forma positiva pelo público consumidor mais esclarecido.

Não há como negar que hoje o comprometimento com a preservação do ambiente natural e de biomas sensíveis encontra-se em nível sem precedentes, atitudes que não tendem a arrefecer no futuro previsível. Assim sendo, mesmo se levarmos em consideração a hipótese bastante improvável de que as mudanças climáticas não dependem, ou dependem muito pouco, da ação do ser humano sobre a natureza, é forçoso admitir que estamos tendo a oportunidade de assistir a uma quebra de paradigmas de grandes proporções e de abrangência incomum.

O **Software ESG** do **INTERISK** é uma ferramenta fundamental para as empresas que desejam alinhar suas práticas e estratégias aos parâmetros ESG (Ambiental, Social e de Governança). Com a crescente conscientização da finitude dos recursos naturais e a necessidade de utilizá-los de forma racional, as empresas estão cada vez mais voltadas para a preservação ambiental e o bem-estar social. Nesse contexto, o **INTERISK** oferece suporte na gestão e monitoramento dos aspectos da Agenda ESG, ajudando as organizações a atenderem aos requisitos, de maneira a gerar valor a médio e longo prazos. Além disso, a ferramenta auxilia na identificação de riscos ambientais e na

implementação de práticas sustentáveis, contribuindo para um desenvolvimento mais responsável e alinhado com as demandas atuais da sociedade.

Solicite uma demonstração!

Décio Luís Schons, CIEAI, CEGRC, CIGR, CISI - General-de-Exército da Reserva. Vice-Presidente de Operações de Consultoria da empresa Brasiliano INTERISK.

“Por que a Gestão de Demandas Regulatórias é essencial para o sucesso das empresas?”

Marcos Alves Junior, CIEIE, CIGR, CPSI

As demandas regulatórias referem-se às obrigações legais e regulamentares impostas às empresas por órgãos governamentais. Elas abrangem uma ampla gama de requisitos, como licenças, certificações, relatórios e conformidade com normas específicas.

A Gestão de Demandas Regulatórias é o processo pelo qual as empresas organizam, monitoram e cumprem essas demandas. Envolve o desenvolvimento de estratégias para lidar com as exigências regulatórias, a implementação de controles e processos internos para garantir a conformidade, além da avaliação contínua do cumprimento das regulamentações.

A importância da Gestão de Demandas Regulatórias para as empresas é múltipla. Em primeiro lugar, o cumprimento das exigências regulatórias é essencial para evitar multas e penalidades legais, que podem ter um impacto financeiro significativo. Além disso, o não cumprimento das regulamentações pode levar à perda de reputação e confiança dos clientes, afetando negativamente os negócios.

Uma gestão eficaz das demandas regulatórias também permite que as empresas identifiquem oportunidades de melhoria e inovação. Ao acompanhar as mudanças nas regulamentações, as empresas podem se antecipar às exigências futuras e se adaptar mais rapidamente, ganhando vantagem competitiva.

Por fim, a Gestão de Demandas Regulatórias promove a transparência e a responsabilidade corporativa. Ao demonstrar compromisso com a conformidade legal, as empresas fortalecem sua imagem perante os stakeholders e contribuem para um ambiente empresarial mais ético e sustentável.

Em resumo, as demandas regulatórias são obrigações legais impostas às empresas, e a Gestão de Demandas Regulatórias é o processo pelo qual essas demandas são gerenciadas. Sua importância reside na garantia da conformidade, na redução de riscos legais e financeiros, na promoção da inovação e na construção de uma reputação sólida.

Fazer a gestão de demandas regulatórias traz diversas vantagens para as empresas. Em primeiro lugar, ao cumprir as obrigações legais e regulamentares, as empresas evitam multas e penalidades que poderiam impactar negativamente suas finanças.

Além disso, a gestão adequada das demandas regulatórias contribui para a construção de uma boa reputação. Empresas que demonstram compromisso com a conformidade legal ganham a confiança dos clientes, fornecedores e investidores, o que pode resultar em parcerias sólidas e oportunidades de negócio.

A gestão de demandas regulatórias também promove a eficiência operacional. Ao implementar controles e processos internos para garantir o cumprimento das regulamentações, as empresas podem identificar áreas de melhoria e otimizar suas operações.

Por outro lado, as consequências da não implementação da gestão de demandas regulatórias podem ser graves. A não conformidade com as obrigações legais pode resultar em multas elevadas, com impacto financeiro significativo nas empresas. Além disso, a reputação da empresa corre o risco de ser prejudicada, levando à perda de clientes e oportunidades de negócio.

A falta de gestão adequada das demandas regulatórias também expõe as empresas a riscos legais. A ausência de controles internos e processos para garantir a conformidade pode levar a processos judiciais e litígios, com custos adicionais e danos à imagem da empresa.

Em resumo, as vantagens de fazer a gestão de demandas regulatórias incluem evitar multas, construir uma boa reputação, promover a eficiência operacional e fortalecer parcerias de negócios. Por outro lado, as consequências de não fazer essa gestão incluem multas, danos à reputação, riscos legais e perda de oportunidades de negócio. Portanto, é essencial que as empresas invistam na gestão adequada das demandas regulatórias para garantir sua conformidade e sucesso no mercado.

Nós da Brasiliano INTERISK, apresentamos uma solução prática e objetiva para automatizar o recebimento e controle de informações das Demandas Regulatórias. Com nosso Software de Gestão de Demandas Regulatórias - GDR, você pode cadastrar, classificar e anexar documentos para análise, além de contar com um workflow que envolve pareceres das áreas responsáveis.

Não importa o tamanho da sua organização, o workflow da Gestão das Demandas Regulatórias garantirá excelência no monitoramento dos requisitos, reduzindo riscos e aumentando a produtividade e eficiência das operações.

Nosso sistema unificado e centralizado permite a gestão eficiente dos requisitos legais. Cadastre, classifique e elabore pareceres das áreas responsáveis agora mesmo!

Quer saber mais sobre o Software de Gestão de Demandas Regulatórias? **Clique aqui e solicite uma demonstração da plataforma!**

Marcos Alves Junior, CIEIE, CIGR, CPSI, **Redator, Editor de texto, Criador de vídeos. Cursou Gestão Empresarial na Anhanguera. Formado pela Uninove – Universidade Nove de Julho em Comunicação Social – Jornalismo. Assistente de Comunicação e Marketing na Brasiliano INTERISK.**

“DESAFIOS PROFISSIONAIS PARA A GESTÃO DE SEGURANÇA EMPRESARIAL”

Dr. Sérgio Leônidas Dias Caldas, CRA, MBA, MBR, CPSI, CIEIE, CIEAC, CIGR, DIDS, MSDIS, DICS

Os desafios empresariais estão cada vez maiores, pois as exigências do mercado e o desempenho dos concorrentes estão crescendo rapidamente. Para fazer frente a esta realidade as empresas necessitam superar continuamente os seus patamares de atuação.

Esta superação não é conseguida com a rotina do dia a dia, é necessário alcançar níveis superiores. A gestão das perdas e o gerenciamento pelas diretrizes potencializam o alcance destes níveis.

O gerenciamento pelas diretrizes busca atingir as metas que não podem ser alcançadas com a rotina do dia a dia e está voltado para solucionar os problemas prioritários da empresa. Nesta busca, percebemos a importância do gerenciamento dos riscos e das perdas, pois o alcance das metas passa pela melhoria dos processos.

Este tipo de gerenciamento deve ser utilizado para conduzir as mudanças que são necessárias para que as empresas alcancem as metas. Mudanças necessárias em virtude do mercado impor metas desafiadoras. Neste processo, é necessária a atuação criativa e dedicada de todos os colaboradores.

Como a gestão da segurança tem que está alinhada com as metas estratégicas da empresa é lógico que o gestor da segurança empresarial terá que gerir com base em diretrizes. As diretrizes do gestor da segurança serão desdobramentos das diretrizes estratégicas.

O sistema preventivo e contingencial de segurança serão desenvolvidos para dar suporte ao alcance das metas desenvolvidas pela alta administração, ou seja, a gestão da segurança não é uma coisa a parte, mas sim integrada ao negócio da empresa.

Para que o gestor da segurança corporativa possa atuar na gestão de perdas é necessário que ele tenha conhecimentos específicos desta área da segurança empresarial.

Os desafios empresariais estão a aumentar, à medida que as exigências do mercado e o desempenho dos concorrentes crescem rapidamente. Para fazer face a esta realidade, as empresas necessitam de melhorar continuamente os seus níveis de desempenho. Essa melhora não se consegue com a rotina do dia a dia, é preciso atingir níveis mais elevados. A gestão de perdas e a gestão por diretrizes potencializam o alcance desses níveis.

A gestão por diretrizes busca atingir metas que não podem ser alcançadas com o dia a dia e visa solucionar os problemas prioritários da empresa. Nessa busca,

percebemos a importância do gerenciamento de riscos e perdas, pois o alcance das metas depende da melhoria dos processos.

Esse tipo de gestão deve ser utilizado para impulsionar as mudanças necessárias para que as empresas atinjam seus objetivos. Os movimentos necessários no mercado impõem metas desafiadoras. Neste processo é necessária a atuação criativa e dedicada de todos os colaboradores.

Como a gestão de segurança deve estar alinhada aos objetivos estratégicos da empresa, é lógico que o gestor de segurança empresarial deva administrar com base em diretrizes. As diretrizes do gestor de segurança serão desdobramentos das diretrizes estratégicas. O sistema de segurança preventiva e contingencial será desenvolvido para apoiar o alcance dos objetivos desenvolvidos pela alta administração, ou seja, a gestão da segurança não é apenas uma parte, mas sim integrada ao negócio da empresa.

Para que o gestor de segurança corporativa possa atuar na gestão de perdas é necessário que ele tenha conhecimento específico desta área de segurança empresarial.

Dr. Sérgio Leônidas Dias Caldas, CRA, MBA, MBR, CPSI, CIEIE, CIEAC,

CIGR, DIDS, MSDIS, DICS

Doctor en Ciencias de la Seguridad (Espanha) | Gestão Empresarial e Corporativa | Prevenção e Controle de Perdas | Riscos

“PORTARIAS VIRTUAIS”

“TRANSFORMANDO A SEGURANÇA RESIDENCIAL E CORPORATIVA”

Edvaldo Almeida

No mundo moderno, onde a tecnologia permeia cada aspecto de nossas vidas, é natural que setores como o de segurança também evoluam e se adaptem às novas demandas, tendências e possibilidades. Uma das inovações mais marcantes nesse sentido é o surgimento das portarias virtuais, um conceito que revoluciona a maneira como condomínios residenciais e corporativos lidam com o controle de acesso e segurança.

Globalmente, a adoção de portarias virtuais também está em ascensão, refletindo uma tendência em direção à automação e tecnologia nos setores de segurança residencial e corporativa. Embora não existam estatísticas precisas sobre o número exato de condomínios que utilizam portarias virtuais em outros países, há evidências que sugerem um aumento significativo na sua adoção em várias regiões do mundo.

Nos Estados Unidos, por exemplo, as portarias virtuais estão se tornando cada vez mais comuns em condomínios residenciais de alto padrão, bem como em edifícios comerciais e corporativos. Empresas especializadas em segurança eletrônica e serviços de portaria remota têm relatado um aumento na demanda por esses sistemas, impulsionado pela busca por soluções mais eficientes e tecnologicamente avançadas.

Da mesma forma, em países da Europa, como Reino Unido, Alemanha e França, a tecnologia de portarias virtuais está sendo adotada em uma variedade de ambientes, desde residências individuais até complexos de apartamentos e escritórios. A ênfase na segurança, combinada com avanços na tecnologia de vigilância e comunicação, tem impulsionado essa tendência em muitas partes do continente.

Embora não haja dados específicos sobre a adoção de portarias virtuais fora do Brasil, é evidente que essa tendência é global e está se expandindo em diferentes partes do mundo, à medida que as comunidades buscam soluções inovadoras para proteger suas propriedades e garantir a segurança de seus residentes e funcionários.

O QUE SÃO AS PORTARIAS VIRTUAIS?

As portarias virtuais, também conhecidas como portarias remotas ou portarias digitais, são sistemas de segurança que substituem a presença física de porteiros por uma estrutura baseada em tecnologia. Por meio de câmeras de vigilância, intercomunicadores e softwares específicos, as portarias virtuais permitem o controle de acesso a condomínios de forma remota, geralmente por uma central de monitoramento.

Em condomínios mais adeptos a essa tecnologia e com padrão de investimento mais elevado, temos observado inclusive a instalação de outras extensões que agregam outras funcionalidades ao sistema, como por exemplo, instalação de Smart Lockers ou Armários Inteligentes, que já possuem condições de recepcionar entregas e emitir recibos.

FUNCIONAMENTO E TECNOLOGIAS ENVOLVIDAS

O funcionamento das portarias virtuais é relativamente simples, porém altamente eficaz. Câmeras estrategicamente posicionadas capturam imagens dos visitantes que chegam ao local, que então são visualizadas e analisadas por operadores remotos em uma central de monitoramento. Os visitantes podem se comunicar com os operadores por meio de intercomunicadores instalados na entrada do condomínio. Com base nas orientações dos moradores ou protocolos pré-estabelecidos, os operadores podem liberar ou negar o acesso.

Além das câmeras e intercomunicadores, as portarias virtuais também podem integrar outras tecnologias, como sistemas de reconhecimento facial, leitores de biometria, leitores de cartão de acesso e até mesmo inteligência artificial para identificar comportamentos suspeitos.

ERROS PROVOCADOS POR FALTA DE ANÁLISE CRÍTICA

A febre do mercado diante do crescimento desse segmento, trouxeram muitas empresas a investirem nesse tipo de negócio. Porém, a falta de expertise e know-hall na área de Segurança por essas empresas, levaram muitos clientes finais a adotarem a contratação de sistemas que ao invés de trazer uma solução eficiente, trouxeram problemas e divergências entre os usuários e fragilizaram a corrente de segurança do estabelecimento.

O sucesso na implantação desse tipo de tecnologia depende de avaliações críticas. Em condomínios por exemplo, deve-se considerar a localização, fluxo de pessoal, layout, volume de serviços recepcionados no local, tipo de tecnologia a ser implementada e principalmente, a cultura de segurança dos condôminos.

Muitas vezes a adoção desse tipo de serviço é realizado sem as devidas prévias considerações. A empolgação pela tecnologia pode induzir o contratante a erros, e geralmente, para retificar o processo de aquisição e mudanças de equipamentos é muito dispendiosa. Por isso, antes de decidir pelo uso das novas tendências que a tecnologia traz, é necessária uma consultoria que tenha uma visão multidisciplinar e esteja ambientada com as soluções já testadas antes no mercado e adequação.

VANTANGENS DA PORTARIA VIRTUAL

A implementação de portarias virtuais traz uma série de vantagens tanto para os moradores quanto para os gestores de condomínios. Algumas vantagens consideráveis:

1- Redução de Custo: A redução na contratação de porteiros em tempo integral tem impacto positivo nos custos operacionais do condomínio.

2- Aumento da Eficiência: Com o monitoramento remoto 24 horas por dia, esse sistema permite que o serviço funcione sem interrupções.

3- Maior Segurança: A tecnologia empregada nas portarias virtuais proporciona um controle de acesso mais rigoroso e preciso, reduzindo os riscos de invasões ou incidentes de segurança. Evitam o confronto direto e rendição do porteiro, além da possibilidade de alertas para as autoridades policiais, já que o ambiente é monitorado de forma virtual através de CFTV e gerido por protocolos de segurança decididos previamente pelo condomínio.

4- Facilidade de Gerenciamento: Os sistemas de portaria virtual geralmente incluem ferramentas de gerenciamento intuitivas que permitem aos moradores controlar o acesso de visitantes de forma rápida e conveniente.

5- Integração com outros sistemas: As portarias virtuais podem ser integradas a outros sistemas de segurança, como alarmes, sensores de movimento e controle de acesso, criando uma solução abrangente e coesa.

DESAFIOS E CONSIDERAÇÕES

Apesar das vantagens claras, a implementação de portarias virtuais possuem aspectos importantes a serem considerados, que são muitos, porém, existem três que se destacam:

1- Dependência de Conexão de Internet: Como as portarias virtuais operam por meio de conexões de internet, a estabilidade e a velocidade da rede são cruciais para garantir o funcionamento adequado do sistema.

2- Proteção contra Hackers: Como qualquer sistema baseado em tecnologia, as portarias virtuais estão sujeitas a possíveis ataques cibernéticos. É fundamental implementar medidas de segurança robustas para proteger os dados e garantir a integridade do sistema. A empresa detentora do sistema deve ter uma política clara de cyber segurança e apoiar o contratado nessas questões.

3- **Aceitação dos moradores:** Nem todos os moradores são adeptos a ideia da portaria virtual e não se sentem confortáveis com a ideia de substituir porteiros por um sistema digital. É importante esclarecer e explorar os pontos de preocupação dos usuários do sistema para garantir uma aceitação considerável. Lembrando que a portaria virtual não elimina a necessidade da presença humana para outras demandas existentes e outras ocorrências que poderão demandar ações que somente o homem tem a capacidade de operacionalizar.

CONCLUSÃO

As portarias virtuais representam uma evolução significativa no campo da segurança residencial e corporativa, oferecendo uma alternativa moderna e eficaz ao modelo tradicional de portaria física. Ao combinar tecnologia avançada com processos eficientes, esses sistemas proporcionam maior controle, segurança e conveniência para moradores e gestores de condomínios. No

entanto, é importante abordar os desafios e considerações associados à implementação dessas soluções para garantir seu sucesso a longo prazo. Com a devida atenção aos detalhes e investimento em medidas de segurança, as portarias virtuais têm o potencial de se tornar uma parte indispensável do panorama da segurança moderna.

O homem de segurança sempre será essencial no processo, porém, a evolução das funções que envolve a tecnologia exige que ele se volte para o aprendizado e conhecimento das novas ferramentas que a sua atividade demanda. Apesar do homem ser o elo mais importante da corrente no sistema de segurança, as mudanças tecnológicas influenciarão a sua visão e prática dentro da operação, e inevitavelmente, os empregos sofrerão uma queda, mas ainda haverá espaço para aqueles que acompanharem essa evolução, pois toda tecnologia precisa de alguém para operá-la.

Edvaldo Almeida

Administrador, pós-graduado em Gestão Estratégica, especialista em Gestão de Segurança. Profissional de Segurança Privada com experiência de Gestão da Segurança, Análise de Risco, Planejamento da Segurança, Treinamento e Consultoria. Idealizador do Canal Vamos Falar de Segurança.

edvaldoalmeidar@gmail.com

“Riscos à Segurança de Shopping Centers: Descubra quais são e Estratégias para tratá-los”

José Sergio Marcondes – CES – CPSI

Descubra os segredos para um shopping mais seguro! Explore nosso guia abrangente sobre Riscos à Segurança de Shopping Centers e as estratégias de tratamento.

A segurança em shopping centers é uma prioridade essencial para garantir um ambiente seguro e agradável aos consumidores, condição fundamental para o sucesso do empreendimento. Contudo, manter essa condição é um desafio para os gestores de segurança, considerando que os Riscos à Segurança dos Shopping Centers têm se tornado cada vez mais significativos e desafiadores.

De maneira objetiva, os Riscos à Segurança de Shopping Centers envolvem a probabilidade de eventos negativos ou ameaças ocorrerem, resultando em danos e perdas para frequentadores, trabalhadores, lojistas ou proprietários do centro comercial. Nesse cenário, a experiência de compra se entrelaça com desafios inerentes à segurança.

Assegurar a segurança dos shopping centers está diretamente ligado à capacidade do gestor de segurança em identificar, avaliar e tratar os diversos tipos de riscos potenciais relacionados à segurança desses empreendimentos. Um desafio que demanda conhecimento e habilidades nos processos de gestão de riscos.

Em nosso artigo, exploraremos minuciosamente os “Riscos à Segurança de Shopping Centers”, revelando os diversos riscos que podem comprometer não apenas a integridade física dos frequentadores, mas também a estabilidade financeira e reputacional dos empreendimentos comerciais.

O que são Riscos à Segurança de Shopping Centers?

Riscos à Segurança de Shopping Centers podem ser expressos como a probabilidade de uma ameaça explorar uma vulnerabilidade específica, resultando em danos ou perdas para pessoas ou ativos do shopping.

Os Riscos à Segurança de Shopping Centers podem ser definidos como a probabilidade de um evento negativo ou ameaça ocorrer e gerar danos e perdas aos frequentadores, trabalhadores, lojistas ou proprietários do empreendimento comercial.

Em outras palavras, por “risco”, queremos dizer a viabilidade de uma ameaça se materializar em dano. Assim, existem riscos altos e baixos, e riscos estão associados ao trabalho, processos empresariais, segurança, economia, saúde, meio ambiente, etc.

A ABNT NBR ISO 31000:2018 define riscos como efeito da incerteza nos objetivos. Nesse sentido, o risco de segurança também pode ser uma circunstância, evento ou ação com potencial de causar perdas ou danos aos objetivos dos Shopping Centers.

A segurança em shopping centers é uma prioridade essencial para garantir um ambiente seguro e agradável para os visitantes. Para manter essa condição, é necessário identificar e tratar os diversos tipos de Riscos à Segurança dos Shopping Centers.

Principais Riscos à Segurança de Shopping Centers

1. **Furtos (a frequentadores e lojistas):** possibilidade de indivíduos agirem de maneira sorrateira para subtrair pertences de frequentadores ou mercadorias de lojas. Riscos Associados: Perda de propriedade, impacto na receita dos lojistas, redução da sensação de segurança dos clientes.

2. **Roubo (a frequentadores e lojistas):** envolvendo o uso de violência ou ameaça para roubar bens ou valores dos frequentadores ou legistas. Riscos Associados: Impactos físicos e psicológicos para as vítimas, riscos de danos permanentes, prejuízo financeiro.

3. **Furtos ou Danos de Veículos:** possibilidade de veículos serem alvo de furtos, arrombamentos ou vandalismo enquanto estacionados no interior do shopping. Riscos Associados: Prejuízo financeiro para os proprietários dos veículos, impacto na reputação do shopping.

4. **Acidentes com Veículos (colisões ou atropelamentos):** Risco de acidentes envolvendo veículos nas áreas de estacionamento ou acessos. Riscos Associados: Lesões pessoais, danos a propriedades, responsabilidade legal.

5. **Fraudes:** atividades fraudulentas, como falsificação de cartões de crédito ou manipulação de transações. Riscos Associados: Perda financeira para lojistas e frequentadores, impacto na confiança do público.

6. **Sabotagem:** atos intencionais para danificar propriedades, sistemas ou operações do shopping. Riscos Associados: Danos físicos, interrupção de serviços, impacto na segurança.

7. **Vandalismo:** possibilidades de destruição ou danificação intencional de propriedades, incluindo instalações e equipamentos. Riscos Associados: Danos materiais, custos de reparo, deterioração da aparência do shopping.

8. **Quedas:** Risco de acidentes devido a condições do piso, buracos ou falta de iluminação. Riscos Associados: Lesões pessoais, responsabilidade legal para o shopping.

9. **Incêndios:** probabilidade de ocorrência de incêndios que podem resultar em danos significativos. Riscos Associados: Perdas materiais, lesões pessoais, interrupção nas operações.

10. **Interrupções no Fornecimento de Água e Energia:** Possibilidade de falta de fornecimento de recursos essenciais. Riscos Associados: Impacto nas operações, desconforto para frequentadores, perda de receita.

11. **Falhas no Sistema de Comunicação:** possibilidade de interrupções nos sistemas de comunicação, afetando a coordenação e resposta a emergências. Riscos Associados: Dificuldade na gestão de crises, atrasos na resposta a incidentes.

12. **Contaminação por Doenças Infecciosas:** risco relacionado a surtos de doenças infecciosas, como pandemias. Riscos Associados: Risco à saúde pública, fechamento temporário, impacto nas operações.

13. **Alagamento/inundações:** ameaça de alagamentos causados por chuvas intensas. Riscos Associados: Danos a propriedades, interrupção de serviços, desconforto para frequentadores.

14. **Desmoronamentos:** risco de desabamentos devido a problemas estruturais ou condições climáticas extremas. Riscos Associados: Lesões graves, danos materiais significativos.

15. **Descarga Elétrica por Raios:** Risco de raios atingirem estruturas ou equipamentos elétricos. Riscos Associados: Danos a sistemas elétricos, risco de incêndio, lesões pessoais.

16. **Excessos/falhas Cometidos pelas Equipes de Segurança:** Falhas da equipe de segurança em identificar ou lidar com situações suspeitas e delicadas. Riscos Associados: danos morais, comoção pública, indenizações, prejuízo a imagem do empreendimento.

Cada um desses riscos requer uma abordagem específica de gestão e implementação de medidas preventivas para garantir a segurança e o bem-estar de todos os envolvidos no ambiente do shopping center.

Fatores que interferem no Nível de Riscos à Segurança de Shopping Centers

O nível de risco para a segurança de um shopping center é influenciado por uma combinação de fatores internos e externos. Dentre os principais fatores estão:

1. **Apoio da Alta Administração:** refere-se à postura e ao comprometimento dos líderes do shopping em relação às práticas de segurança. Isso inclui o investimento em recursos, a definição de políticas claras e a promoção de uma cultura organizacional que valorize a segurança.

2. **Sistemas de Segurança Implementados:** A presença e a eficiência de políticas e procedimentos de segurança, câmeras de vigilância, alarmes, controle de acesso e pessoal de segurança são determinantes na capacidade de proteger o shopping.

3. **Infraestrutura e Layout do Shopping:** A disposição física do shopping, a eficácia dos sistemas de vigilância e a acessibilidade das áreas desempenham um papel crucial na vulnerabilidade do local a diferentes ameaças.

4. **Localização Geográfica:** A localização do shopping em relação a áreas de alta criminalidade ou a presença de comunidades específicas pode influenciar significativamente o nível de risco.

5. **Contexto Socioeconômico:** O contexto socioeconômico da região desempenha um papel crucial no perfil de segurança.

6. **Tendências de Criminalidade na Região:** Monitorar e adaptar-se às tendências de criminalidade na área circundante é fundamental.

7. **Treinamento e Conscientização:** Funcionários bem treinados e conscientes das práticas de segurança são uma linha de defesa vital. Investir em programas educativos e de treinamento contínuo contribui significativamente para a prevenção e resposta eficaz a incidentes.

8. **Relações com Autoridades Locais:** A cooperação e comunicação eficazes com as autoridades locais, como polícia e serviços de emergência, são fatores internos que impactam a resposta a incidentes. A construção de parcerias sólidas fortalece a capacidade de enfrentar desafios de segurança.

Estratégias para Tratar os Riscos à Segurança de Shopping Centers

A gestão eficaz de riscos em um shopping center envolve a implementação de estratégias proativas para identificar, avaliar e tratar potenciais riscos. Abaixo estão algumas das principais estratégias para lidar com os riscos de segurança em um shopping center:

1. **Avaliação de Riscos:** Implementar um processo abrangente de avaliação de riscos visando identificar e avaliar vulnerabilidades e ameaças. Classificar os riscos de acordo com sua probabilidade e impacto é fundamental para priorizar as ações de mitigação.

2. **Tratamento de Riscos:** Adotar medidas preventivas, tais como reforço na segurança física, atualização de sistemas de vigilância e investimentos em tecnologias de detecção de ameaças. A prevenção é essencial para reduzir a probabilidade de ocorrência de incidentes.

3. **Colaboração com Autoridades Locais:** Estabelecer e manter uma cooperação eficaz com as autoridades locais, como polícia e bombeiros, é vital para aprimorar a resposta a incidentes. A comunicação e colaboração contínua fortalecem a capacidade de enfrentar desafios de segurança.

4. **Auditorias de Segurança:** Conduzir auditorias de segurança regulares para avaliar a conformidade com normas de segurança, identificar deficiências e implementar melhorias. A revisão sistemática é essencial para garantir a eficácia contínua das medidas de segurança.

5. **Gestão de Crises e Comunicação:** Desenvolver planos de gestão de crises que incluam estratégias de comunicação eficazes para garantir uma resposta coordenada e transparente em situações de emergência. A prontidão para lidar com crises é crucial para manter a confiança dos stakeholders.

A implementação dessas e outras estratégias de tratamento de riscos cria uma abordagem robusta para a segurança do shopping center, proporcionando um ambiente mais seguro para clientes, funcionários e visitantes.

Conclusão

Neste artigo, abordamos os complexos “Riscos à Segurança de Shopping Centers”, destacando riscos de furtos, incêndios, e até pandemias, oferecendo estratégias robustas para sua mitigação. Ressalto que cada um desses riscos requer uma abordagem específica de gestão e implementação de medidas preventivas para garantir a segurança e o bem-estar de todos os envolvidos.

Convido você a refletir sobre a importância de uma abordagem proativa na segurança desses ambientes dinâmicos. Afinal, a segurança de shopping centers vai além da proteção de propriedades – trata-se da preservação da experiência do cliente e da integridade dos negócios.

Para uma compreensão holística, sugiro a leitura do próximo artigo: “Vulnerabilidades de Segurança em Shopping Centers: Um Guia Completo

para a Proteção Efetiva“. Explore ainda mais estratégias essenciais para manter um ambiente seguro. A segurança é um compromisso contínuo, e nossa jornada de conhecimento apenas começou.

Um forte abraço e votos de sucesso!

José Sergio Marcondes – CES – CPSI – Gestor, Consultor e Diretor do IBRASEP. Especialista em segurança com competências sólidas nas áreas de segurança privada e gestão empresarial. Conecte comigo nas redes sociais.

“Riscos Emergentes: necessidade de rever a avaliação para antever e adaptar”

Antonio Celso Ribeiro Brasiliano, PhD, DICS, MCRC, CIEAI, CEGRC MBCR, CIEAC, CPSI, CIGR, CRMA, CES, DEA, MBS

O mundo está mais interconectado, volátil, incerto, complexo e acompanhado por uma crescente ambiguidade de informações. Isso dificulta a identificação de riscos emergentes e aumenta potencialmente a gravidade das consequências, com implicações massivas para as organizações.

Os riscos emergentes são caracterizados por serem novidade, possuírem dados e informações insuficientes e não terem referencial para a tomada de decisão.

Os riscos emergentes surgem de mudanças nos contextos organizacionais, das circunstâncias ou condições relacionadas a múltiplos aspectos do ambiente em que a organização opera. Podemos citar os seguintes exemplos:

- **riscos decorrentes de mudanças não reconhecidas nos contextos organizacionais;**
- **riscos criados pela inovação ou pelo desenvolvimento social e tecnológico;**
- **riscos relacionados a novas fontes ou a fontes de risco não reconhecidas anteriormente;**
- **riscos de processos, produtos ou serviços novos ou modificados;**
- **mudanças no modo como determinado risco impacta uma organização.**

As consequências podem incluir:

- **exposição a perigos imprevistos e ameaças com resultados incertos;**
- **maior exposição a perigos e ameaças oriundas de fontes de riscos conhecidas;**
- **oportunidades perdidas.**

Há necessidade de rever o Framework de Gestão de Riscos para aumentar a resiliência organizacional. O foco está nos riscos que têm potencial massivo de impacto sobre os objetivos empresariais.

A aplicação dos princípios e processos da ISO 31000 ao gerenciamento de riscos emergentes necessita de um aperfeiçoamento na capacidade de identificar os diferentes aspectos do ambiente do mundo de hoje. Mudanças são

indicadores ou sinais iniciais que identificam as vulnerabilidades e as fontes de riscos emergentes. Desta forma, a varredura contínua dos ambientes é crucial para que haja a identificação de sinais, mesmo que fracos, de condições em mudança que possam dar origem a riscos emergentes. A contínua varredura incentiva o desenvolvimento do conhecimento e fornece inteligência a ser aplicada à tomada de decisões, tanto no nível estratégico quanto no operacional.

Neste caso, o processo de gestão de riscos deve estar integrado à inteligência estratégica, visando aprimorar o conhecimento sobre os riscos emergentes. É importante ter em mente que a Inteligência é o resultado da coleta e análise de dados, que gera informações. O conhecimento, por sua vez, é constituído pelo processamento das informações úteis para a consecução dos objetivos da organização. Para riscos emergentes, a futura ISO 31050 integrou o Framework ISO 31000, com o ciclo de inteligência da ISO 56006 – Inovação:

Ciclo de inteligência para riscos emergentes aplicado ao processo ISO 31000

Fonte e Ponto de Atenção: Documento Draft de discussão e comentários ISO/CD 31050, não é norma oficial. Está sujeito a alterações sem aviso prévio e não pode ser referenciado como um padrão internacional.

É uma forma integrada de repassar todas as informações relevantes sobre os riscos emergentes, além de realizar as interconexões entre os diferentes riscos e identificar os riscos que influenciam alguns ou todos os demais riscos. Desta forma, os tomadores de decisão precisam reconhecer a importância da validação do processo de inteligência e do conhecimento acumulado. A incerteza inerente

aos julgamentos humanos e o potencial de viés cognitivo das percepções individuais devem ser considerados ao validar segundo o qual a informação foi convertida em conhecimento. Níveis significativos de incerteza sobre riscos emergentes podem dar origem a novas questões que irão requerer validação adicional.

O ciclo de inteligência irá cobrir essas etapas, se elas forem bem realizadas. Este é o desafio da integração de riscos e inteligência estratégica, framework este que a Brasiliano INTERISK já vem pregando no mercado, juntamente com os Impactos Cruzados, há mais de 15 anos! Minha expectativa é de que agora seja de fato efetivado!

O **Software INTERISK**, é uma ferramenta essencial para enfrentar os desafios na identificação e gerenciamento de riscos emergentes. Com a complexidade e volatilidade crescentes do ambiente empresarial, é crucial ter uma solução que integre informações relevantes e analise os impactos cruzados entre diferentes riscos. O **INTERISK** oferece recursos avançados para identificação e avaliação de riscos emergentes, alinhando-se à necessidade de aprimorar a capacidade das organizações de antecipar e responder a ameaças imprevistas. A integração do ciclo de inteligência da ISO 56006 ao processo de gestão de riscos, como proposto no documento Draft de discussão e comentários ISO/CD 31050, demonstra a relevância da abordagem do **INTERISK** para lidar com os desafios atuais. A utilização do **Software INTERISK** pode contribuir significativamente para a resiliência organizacional e o fortalecimento da capacidade de tomada de decisões estratégicas diante dos riscos emergentes.

Antonio Celso Ribeiro Brasiliano, PhD, DICS, MCRC, CIEAI, CEGRC MBCR, CIEAC, CPSI, CIGR, CRMA, CES, DEA, MBS, Doctor en Filosofía en Ciencias de la Seguridad Internacional, pela Cambridge International University, Inglaterra. Presidente da Brasiliano INTERISK.

“SEGURANÇA E GESTÃO DE EMERGÊNCIAS E CRISES COMO VALORIZAÇÃO DO PRODUTO EVENTO”

Carlos Alberto Zanandreis da Silveira

Introdução

Um dos negócios que no mundo atual mais tem números expressivos é o setor de eventos, tanto na perspectiva de geração de empregos, quanto na perspectiva de abertura de novos negócios e movimentação de outros setores de serviço como infraestrutura, segurança e limpeza, segundo a Associação Brasileira de Promotores de Eventos (ABRAPE). Este é um dos segmentos que mais sofreu no período da pandemia Covid-19. Nada difícil de compreender levando-se em consideração que um evento propõe a junção de pessoas, e isto acabou sendo uma das principais medidas a serem evitadas à época para conter o surto, onde segundo a associação, mais de 350 mil eventos foram cancelados no país.

Ainda segundo a ABRAPE, o setor de eventos é responsável por 4% (quatro por cento) do PIB e faturando em média R$230 bilhões entre 2020 e 2021. Por meio de eventos, as organizações projetam suas marcas, e claro há grandes patrocinadores. Também são os eventos grandes mobilizadores de lançamento de produtos de diversos setores de consumo. Ainda pode-se dizer que os eventos são oportunidades de atrair novos e aproximar o público para determinadas organizações. Sendo assim, o evento é um canal de lançamento e valorização de um produto e ao mesmo tempo, um produto em si.
Pensando nisso, será que as organizações querem que suas marcas e produtos estejam atrelados a escândalos, tragédias e mortes? Efetivamente, o bom senso afirma que não. Porém, as atitudes das próprias organizações e produtores de eventos podem contrariar esse objetivo quando não se atentam com atenção a um adequado planejamento de segurança e a preparação de respostas eficientes e eficazes aos riscos que não puderem ser evitados.

Qual o impacto da falta de cuidado com a segurança na perspectiva preventiva e reativa para as organizações promotoras e patrocinadoras? Secundariamente vale ainda perguntar: Investidores vão colocar seus recursos em produtos que podem comprometer suas marcas por causa de sérios problemas de segurança e de gestão de emergências e crises? Desta forma, o objetivo principal deste artigo é apresentar o impacto para o setor de eventos e as empresas promotoras da falta de atenção e displicência com os aspectos do planejamento de segurança, emergências e crises. Este estudo se pautará na apresentação de alguns aspectos pertinentes aos eventos avaliando um caso recente no Brasil, que foi o jogo das eliminatórias da Copa do Mundo
de 2026, entre Brasil x Argentina, no mês de novembro de 2023, no estádio Maracanã, no Rio de Janeiro.

Este estudo é relevante do ponto de vista de alertar as organizações do setor de eventos, ou que se utilizam de grandes eventos para promover seus produtos da importância que os cuidados com o planejamento de segurança e gestão de

emergências e crises tem no sucesso dos eventos e na valorização de seus produtos, ou mesmo, no risco existente as marcas, aos recursos que a falta de cuidado e displicência podem gerar a estas organizações. Como metodologia este artigo, pesquisas foram realizadas em mídias e jornais, bem como, em bibliografia sobre o assunto abordado.

O evento como produto e como ferramenta dos negócios e estratégias organizacionais

Simões (1995) salienta que um evento é um acontecimento que surge com o objetivo de alterar, alinhar a relação da organização com seu público, ou seja, se não houvesse o evento essa relação mais próxima não ocorreria e, consequentemente, o rumo dessa relação da organização promotora ou patrocinadora com seus públicos poderia ser diferente. Já Matias (2013) enfatiza que o evento deve ser planejado para alcançar rumos definidos. Esta afirmação pode nos levar a reflexão que se algo ocorre que inviabiliza parte ou totalmente este evento, ou ainda que gere um tipo de associação danosa, o resultado pode ser totalmente diverso do esperado.

A área de eventos sofreu um impacto muito grande no período da pandemia do Covid- 19, mas, dados recentes mostram que o setor de eventos vem retomando sua posição de destaque como apresenta a ABRAPE que nos seis primeiros meses de 2023 gerou um crescimento de mais de 42% com geração de mais de 12mil vagas de empregos. Números que ultrapassam o ano de 2022. O relatório de eventos no Brasil, promovido pela Opinion Box e a transformação digital.com, fizeram mais de 2000 entrevistas.

De acordo com Benitez e Nadruz (2019), os mais diversos tipos de eventos são oportunidades de negócio e precisam ter um padrão de qualidade para um público cada vez mais exigente nos aspectos de atendimento, organização, conforto e segurança. Aqui se vê que muitas vezes os organizadores buscam se ocupar de cuidar da beleza dos eventos e sua organização, porém, não é raro se ver uma despreocupação, ou a ausência de um mesmo nível de cuidado com aspectos de segurança e de atuação eficaz em situações de emergências e crises.

Os eventos se tornaram muito importantes e se uniram a outro tipo de negócio e mercado que é o turismo (MATIAS, 2013). O turismo de eventos e as redes sociais fizeram ainda que um evento seja em âmbito nacional ou internacional tenha a capacidade de atingir públicos a distâncias inimagináveis e, consequentemente, a repercussão do que ocorre em tal evento tem impactos positivos ou negativos em nível mundial. Esse potencial é que faz exatamente várias organizações utilizarem e colocarem suas marcas nos mais diversos tipos de eventos.

Conforme apontado pelo SEBRAE (2023), os eventos e o turismo de eventos trazem uma série de vantagens as organizações e as cidades produtoras, tais como maiores movimentações da economia local, bem como, arrecadação de impostos, combate a sazonalidade, atração de públicos diferentes, legado as cidades, entre outros. Desta forma, pode-se depreender que um evento pode ser

realizado por pequenas ou grandes organizações como oportunidade de se aproximar de seus públicos-alvo, sem falar naquelas organizações que seu negócio seja o próprio evento no que tange a organização e produção. Desta maneira, se vê que um evento é em si um produto, mas, também uma ferramenta que pode alavancar negócios, marcas e imagens organizacionais (reputação).

Segurança e Gestão de Emergências e Crises e sua relevância para eventos

Antes de mais nada é importante deixar claro o que este artigo entende como gestão de riscos e como gestão de emergências e crises. Segundo Leite (2016) é uma das funções da administração prover a segurança aos “stakholders” e assim a gestão de risco é um processo sistemático que visa maximizar oportunidades e minimizar perdas, melhorando os resultados. Já segundo Teixeira (2019) a gestão de riscos é um processo multidisciplinar de mapear, e identificar os riscos com posteriores decisões de como prevenir, mitigar e evitar que tais riscos ocorram. Como se vê, o processo de gestão de riscos está ligado a uma fase anterior que é preventiva. Já quando se fala na gestão de emergências e crises, segundo Costa (2008) a gestão de emergências e crises consiste no processo de enfrentar uma situação de emergência ou crise e trabalhar para preveni-la. Algo que significa antes de tudo entender e prevenir, e secundariamente atuar para administrar o que venha a ocorrer, sempre levando em consideração o interesse dos “stakeholders”. Daí podemos considerar que como a gestão de riscos é iminentemente preventiva, a gestão de emergências e crises se foca na administração do incidente que não pôde ser evitado para que os impactos sejam os menores possíveis.

O relatório de eventos no Brasil mostrou que 48% dos entrevistados sinalizaram que a infraestrutura (onde pode-se incluir a segurança) é um dos fatores que o fazem escolher o evento, e ainda 42% preocupam-se com a segurança Covid-19, que não deixa de ser uma preocupação com o fator segurança (OPINION BOX, 2022). Outro dado relevante da pesquisa é que em eventos esportivos, 69% do público prefere presencialmente, musicais, 78%, gastronômicos, 86%, e artísticos-culturais 81%. Se observa com isso, que determinados eventos terão maior sucesso com o público presente, e isso traz em si, o cuidado com a beleza, conforto, atendimento, mas, não menos importante dos aspectos de segurança. Vale lembrar o impacto negativo de tragédias ocorridas no Brasil como o da Boate Kiss, no Rio Grande do Sul, do Canecão Mineiro, em Belo Horizonte. Importante destacar ainda eventos com impactos negativos relativos ao futebol que vem sendo mostrado na mídia constantemente.

Em 1985, em Bruxelas, numa partida entre Liverpool (ING) x Juventus (ITA) houve 39 mortes e que geraram severas punições aos clubes ingleses. Mais recentemente, em 2022, no estádio Kanjuruhan, na cidade de Malang, na Indonésia um confronto generalizado gerou 125 mortes. No ano de 2023, no Brasil diversas partidas do campeonato nacional, na série A tiveram eventos de invasões, brigas, arremesso de objetos, entre outros. Por isso, o gestor de segurança Igor de Mesquita Pipolo alerta:

“a qualidade da segurança é fator crítico para o sucesso de um evento. De nada adianta planejar, mesmo que impecavelmente, uma recepção empresarial se o controle de acesso não for capaz de barrar “penetras” que tomam o lugar dos convidados. Pouco importa que um show tenha sofisticados recursos de som e imagem se um princípio de incêndio ocorrer, provocando um tumulto que deixe dezenas de pessoas feridas.” (PIPOLO, 2010, p.18)

O que se observa nestas ocorrências citadas e tantas outras que podem ser observadas não é somente o fato de não haver segurança, ou riscos de segurança não terem sido considerados, como rivalidade, lotação, uso de drogas lícitas e ilícitas, contexto social, etc. E ainda, o fato de não haver, ou não ter sido eficaz um plano de respostas as possíveis emergências. Importante sempre considerar que um problema de segurança age diretamente em vidas, e esta tem o poder de mobilizar grande repercussão na mídia e assim, um sério dano à reputação das organizações, fora outros impactos que se advém como processos judiciais, indenizações etc.

Vários equívocos conceituais se percebem comumente nos organizadores e decisores de eventos em relação aos aspectos de segurança e resposta a emergências, tais como: considerar a segurança somente como controle de acesso, considerar a segurança como algo não tão importante e relegar orçamentos parcos para seu planejamento e operacionalização, considerar segurança como despesa e não investimento na qualidade do evento, em função do desconhecimento ou orçamento contratar empresas e profissionais que não tenham liberação legal, formação, qualificação e experiência suficientes, “acreditar na sorte” de que nenhuma ocorrência de risco irá ocorrer, desconsiderar a atuação de fatores adversos externos, desconhecer o comportamento humano diante de situações de perigo (pânico), não identificar que algumas tomadas de decisão que aparentemente podem contribuir para a realização do evento, podem gerar severas vulnerabilidades de segurança ao mesmo evento.

Os idealizadores e produtores não podem deixar de reconhecer que não basta que o evento se realize, mas, é preciso, para se atingir o objetivo principal, que as pessoas, que são o foco do evento, possam chegar, entrar, vivenciar, sair e voltarem para suas casas com a melhor imagem e sensação possível daquele evento que participaram. Neste quesito a segurança é um dos aspectos essenciais para promover tal percepção.

Os impactos de uma má gestão de segurança e de emergências: Análise de um jogo pelas eliminatórias da Copa do Mundo de 2026

No dia 21/11/2023 estava prevista a realização de um evento de grandes proporções e de repercussão mundial no estádio do Maracanã, o jogo de futebol entre as seleções do Brasil e da Argentina, pelas eliminatórias da copa do mundo de 2026, na cidade do Rio de Janeiro, RJ. Analisando o produto evento, se tratava de um grande espetáculo com alto investimento de patrocinadores e cobertura de imprensa mundial, por se tratar de um dos maiores clássicos mundiais de futebol, além disso, seleções que juntas somam oito títulos

mundiais, mais ainda, por ter entre suas atrações a atual seleção campeã do mundo, jogadores renomados e, entre eles, Lionel Messi, um que hoje que atrai grande mídia com sua presença.

O evento teve atraso de 27 minutos em seu início, em função de brigas entre os torcedores dos dois países e, posteriormente, conflito do policiamento local que entrou para intervir no problema com a torcida da Argentina. Em pouco tempo, vários sites e jornais de todo o mundo mostravam as cenas de violência e cada um, a sua forma responsabilizava os órgãos envolvidos, fosse a FIFA, promotora, fosse a CBF, organizadora, fosse a segurança privada, fosse o policiamento. Não há dúvidas da má repercussão de imagem dos países e dos organizadores, e das marcas que estavam ali patrocinando tal evento. O objetivo de gerar aproximação com os públicos acabou sendo manchado e não atingido, visto as cenas de violência contra o próprio público presente.

Os autores Benites e Nadruz (2019) salientam que “em qualquer evento que se envolva um número considerável de pessoas é necessário que se faça um planejamento estratégico do próprio evento e dos níveis de segurança desejados” e foi exatamente o que não se viu ao analisar a situação. O problema de segurança gerado e a inabilidade de ter uma resposta a um risco de certa forma, até esperado, acabaram por fazer com que o evento perdesse valor, com o risco final de nem se realizar devido a ameaça da equipe Argentina de não jogar. Vê-se aqui que exatamente um aspecto que muitas vezes é pouco pensado e tem parcos investimentos, como o gerador do problema que poderia inviabilizar o evento, fora os impactos de imagem, prejuízos materiais que ocorreram. Isso, por si só, mostra que o mau planejamento ou a ausência de planejamento de segurança e de resposta a emergências em um evento podem acarretar o efeito contrário daquilo que se objetiva com a realização de um evento.

Um dos aspectos que se pode argumentar é que é corriqueiro haver eventos desse porte e todos já estão acostumados com sua realização, porém, aí se demonstra um erro grave na perspectiva de segurança e gestão de emergências, que é a não atenção a detalhes, a desconsideração de aspectos novos que estão inseridos no contexto do evento. Em relação a isso é Benites e Nadruz (2019) que reforçam:

Cada evento é único! Você pode ter a repetição do mesmo evento, no mesmo local com os mesmos participantes e ainda assim terá variáveis não computadas porque estaremos lidando com pessoas e seus sentimentos que por si só podem tender num dia para a mais pura diversão e em outro para uma propensão criminosa mesmo que seja induzida pelo calor do momento. (BENITES E NADRUZ, 2019. P.17)

Um primeiro aspecto é que o esquema de segurança não previu separação entre as torcidas por se tratar de um evento FIFA, e aí se vê, aspectos que foram relegados, tais como, recente final no mesmo estádio entre torcedores brasileiros e argentinos pela Copa Libertadores da América entre Fluminense x Boca Juniors que tiveram grandes conflitos fora e dentro do estádio, intensificação da rivalidade já histórica entre os dois países em função da última decisão de Copa

América, no mesmo local, ter sido vencida pela Argentina, e que esta seleção acabara de se tornar campeã mundial e liderar as eliminatórias, em que o Brasil vinha de resultados ruins e se projetava neste jogo uma grande oportunidade de recuperação. E também o fato de que o futebol em si é um jogo de paixões e ainda mais num local que havia o consumo de bebidas alcoólicas, num país em que ano a ano tem se demonstrado a incapacidade de lidar com torcidas organizadas e grupos que vão aos estádios para brigas. Culturas e momentos locais precisam ser considerados para as decisões de segurança. O que é ideal, pode não ocorrer a depender do contexto que há entorno.

Riscos precisam ser percebidos e analisados na avaliação da segurança para qualquer evento. As principais teorias de ciclo de vida das crises se baseiam que estas só ocorrem quando uma série de fatores pequenos são negligenciados (SALINAS, 2001). Não se pode desconsiderar qualquer fator e esperar que o público tenha a consciência. Segurança é antes de tudo antecipação tanto para prevenir, quanto para ter a resposta adequada pronta para entrar em funcionamento, sempre respeitando premissas, como a integridade física e emocional dos envolvidos. As próprias declarações posteriores ao evento demonstram que não ficou claro, ou não se esperava para um ou outro lado, os níveis de riscos envolvidos no evento.

Diante dos fatos expostos era de se esperar que havia a possibilidade da briga entre torcidas, porém a resposta à situação não se mostrou eficiente, e inclusive gerando interpretações diferenciadas quanto a truculência e desproporcionalidade da ação. Pode-se avaliar criticamente, o tempo demorado de acionamento e de resposta, a forma de abordagem entre outras coisas. As próprias pessoas que precisavam ser socorridas ou detidas não tinham um local adequado para deslocamento e retirada. Tão essencial quanto prevenir é ter uma resposta adequada e ágil a problemas que se esperam que possam ocorrer.

Tais fatores demonstram que havia um problema no planejamento e na operação de segurança do evento, e isso aponta para a necessidade de profissionais capacitados e experimentados na condução do planejamento de segurança. Não é uma alta formação acadêmica, ou uma alta patente que dá condições de se pensar e operacionalizar um evento da esfera privada. O planejamento estratégico de segurança precisa e deve estar alinhado com o planejamento estratégico do evento.

O que pode ser feito

Em qualquer evento é essencial que a gestão de segurança e de emergências e crises tenham a sua frente pessoas experientes e comprovadamente capacitadas, além disso, é preciso dar espaço para a atuação destes profissionais desde a concepção do evento para que haja, como dito, um alinhamento entre o planejamento estratégico do evento com o da segurança do evento.

Quando se fala na atuação de gerenciamento de riscos, a ISO 31000 sugere um caminho que não deveria ser desconsiderado: Estabelecer o contexto do evento num alinhamento claro entre as partes do que se deseja em relação ao plano de

segurança e as premissas que devem ser consideradas e a partir daí pode-se alinhar uma política ou diretrizes básicas ao trabalho da segurança, além claro da definição dos responsáveis e seus níveis de responsabilidade. Após isso, em conjunto com um bom e importante trabalho de inteligência, avaliar todos os contextos internos e externos e os riscos e vulnerabilidades existentes. Realizar uma criteriosa análise dos riscos estabelecendo na avaliação posterior aqueles que são prioritários seja por impacto ou por probabilidade de ocorrência.

Diante disso, ter ações integradas entre segurança privada, pública e tecnologias, bem como, definição dos processos preventivos e de resposta a cada situação. Neste ponto inclusive cabe dizer que é fundamental o alinhamento com todas as outras áreas envolvidas no evento, comunicação eficiente e treinamento dos envolvidos, principalmente daqueles que estarão formando um comitê de emergências e crises, que não pode faltar. Comitê este já com processos de resposta definidos e claros com todas as partes envolvidas. Vale a pena dizer que os produtores não deveriam assumir riscos que sejam iminentes, claros e impactantes sem a devida prevenção e resposta bem estruturada. Isso significa ouvir todos os envolvidos e dar o crédito devido as análises e cenários de riscos.

Aspectos importantes precisam fazer parte em todo o processo: Perfil qualificado das empresas e profissionais que forem atuar, capacidade de monitoramento e antecipação, comunicação rápida e eficiente, definição clara dos gatilhos para atuação das operações de resposta. A criação de uma sala de situação, uma espécie de central de inteligência que integre informações e possa avaliar cenários e dar o “start” nos gatilhos alinhados e treinados é uma medida que pode ser bastante eficaz.

Considerações finais

Ao se avaliar e relembrar do evento ocorrido no Rio de Janeiro em 21/11/23, a maior lembrança fica por conta dos problemas ocorridos e não do evento em si. Emocionalmente falando, para muitos a lembrança será de um momento danoso e perigoso e não de um evento prazeroso que valha a pena ir. Tudo que se refere a este evento, inclusive as marcas e organizações envolvidas será manchada pela ocorrência. Isso sem falar dos custos de reparação dos prejuízos, custas adicionais de processos, impacto nas imagens e novas produções destas organizações. O próprio fato deste evento estar hoje sendo utilizado como referência do presente artigo é uma demonstração que sua lembrança negativa se perpetuará por mais tempo.

O autor Pipolo (2010) enfatiza que não se pode esperar que profissionais que organizam saibam fazer segurança, mas, é importante que tenham noção da abrangência e suas responsabilidades com este tema e assim possam avaliar corretamente os planos de segurança que devem ser organizados por pessoas preparadas. O evento analisado demonstra claramente que problemas de segurança podem inviabilizar a ocorrência de um evento e gerar grandes impactos negativos aos envolvidos se esta temática não for tratada com a devida seriedade e por pessoas qualificadas para tal. Demonstra que as ações de segurança e de emergências e crises não são ações que devam ser relegadas

ao rol de custos, mas, que devem ser tratadas como investimento na qualidade do próprio evento.

A perspectiva de segurança deve ser avaliada em todas as etapas de um evento, o pré- evento, o evento em si, e o pós-evento. Todos os cenários precisam ser avaliados e aqueles que se mostram mais evidentes e impactantes precisam ter um planejamento de gestão das emergências com seus devidos gatilhos previamente definido, aprovado, treinado para a melhor execução possível.

REFERÊNCIAS

ABRAPE – **Associação Brasileira de Produtores de eventos**. Acesso em 30 de novembro de 2023. https://consumidormoderno.com.br/2023/08/11/setor-de-eventosmovimenta-mais-r-291-bilhoes-e-gera-66-dos-empregos-no-brasil/

BENITEZ, L; NADRUZ, M – **Grandes eventos: Planejamento e ação operacional** – Edição dos autores – Porto Alegre – 2019.

COSTA, R. Z – **Gerenciamento de crises em segurança empresarial e sequestros** – Editora Ciência Moderna – Rio de Janeiro – 2008.

LEITE, T. A. S. – **Gestão de riscos na segurança patrimonial:** um guia para empresários e consultores. – 1ª edição – Editora Qualytmark – Rio de Janeiro – 2016.

MATIAS, M. – **Organização de eventos, procedimentos e técnicas**. – Editora Manole - 6ª edição – São Paulo – 2013.

OPINION BOX E TRANSFORMAÇÃO DIGITAL - **Relatório Eventos no Brasil** – Outubro - 2022

PÍPOLO, I. M – **Segurança de eventos: novas perspectivas e desafios para produção**. - Núcleo – São Paulo – 2010.

SALINAS, A. V - **XXV ENANPAD** - Crises Organizacionais são uma questão de ciclos? Notas críticas e reflexões sobre o campo da gestão de crises. 2001. (Congresso).

SEBRAE -Turismo de eventos pode turbinar pequenos negócios - https://sebrae.com.br/sites/PortalSebrae/artigos/turismo-de-eventos-pode-turbinarpequenos-negocios,f00309f78a636810VgnVCM1000001b00320aRCRD – Acesso em 12/12/2023

SIMÕES, R. P. **Relações Públicas: função política**. - Summus – São Paulo – 1995.

TEIXEIRA, P. B. – **Caiu na rede. E agora? Gestão de crises nas redes sociais.** – Editora Évora – 2ª edição – São Paulo – 2019.

Carlos Zanandreis é professor universitário, com mais de 25 anos de experiência nas áreas de gestão de segurança e emergências/crises. Bacharel em Relações Públicas, Mestre em Administração e pós-graduado em Segurança Corporativa e Gestão de Riscos e Compliance. Atua como especialista em gestão de crises e emergências. É delegado CEAS (Corporacion Euro-Americana de Seguridad.

“Segurança Global Pública-Privada. Decálogo”

Manuel Sánchez Gómez-Merelo

Consultor de Segurança Internacional

Os grandes problemas globais envolvem atualmente o estabelecimento de uma nova ordem e de uma nova perspectiva que exige a abordagem de uma nova segurança abrangente, integrada e globalizada.

Devemos estar conscientes de que estão a ocorrer mudanças profundas, e não temporárias, no mundo de hoje, e que é necessário contribuir de uma forma mais eficaz e realista para melhorar a segurança global. Nesta perspectiva, devemos ajudar as instituições e organizações a redesenhar novas estratégias de segurança na nova ordem globalizada.

Um ambiente inseguro e instável num mundo que procura soluções para as alterações climáticas com consequências cada vez mais irreversíveis, enquanto a inteligência artificial (IA) entra nas nossas vidas antes da sua própria regulamentação, e a segurança e a informação tornam-se conceitos cada vez mais complexos e contraditórios.

Um mundo com novos desafios e exigências para o desenvolvimento de um novo conceito de Segurança Global, como a convergência de valores mobiliários, a transformação digital e a digitalização para a gestão operacional da segurança abrangente e integrada, pública e privada.

Vejamos com um pouco de detalhe a realidade do nosso novo projeto de estabelecimento de Decálogos de objetivos e ações a realizar em termos de segurança nos diferentes sectores ou áreas de atividade:

Segurança Pública-Privada. Modelo

O contexto em que estamos inseridos, e a importância que a Segurança Global está a assumir e irá assumir, exige novos tipos de análise e conhecimento multidisciplinar da situação e das medidas a adotar.

Perante os novos desafios e exigências de segurança, devemos estudar as grandes mudanças e tendências que vivemos, diferenciando os riscos económicos, políticos e de segurança que nos ameaçam, para desenhar um novo cenário futuro em que um modelo de governação de segurança global seja capaz de adaptar-se e responder aos novos desafios e exigências de prevenção e proteção.

Só uma segurança global, abrangente e integrada garante uma proteção eficiente contra ameaças globais e, para isso, devemos redefinir as políticas de segurança, criar uma nova cultura de segurança abrangente, estabelecer mecanismos de controlo e gestão da segurança física e de segurança, monitorizar o sistema de segurança, organizar a contingência e avaliar a resiliência.

Redefinindo a segurança

A transição da convergência para a Segurança Global é o avanço necessário para a redefinição e, sem dúvida, uma nova oportunidade para avançar num mundo de desafios coletivos e de futuro incerto, com a necessidade de compreender e enfrentar as novas mudanças sociais, económicas, energéticas e tecnológicas. , para promover o desenvolvimento deste conceito amplo da Nova Segurança que estamos desenhando e que estará presente a partir de agora.

Devemos também aproveitar a oportunidade para aplicar estes avanços da segurança global à segurança local, centrando-nos na prevenção + proteção eficiente dos cidadãos, dado que, neste

momento, as ameaças assumem muitas dimensões e formas, em áreas como a geopolítica, o crime, terrorismo, desastres naturais e, mais recentemente, pandemias globais. Devemos continuar a pensar globalmente, para agir melhor localmente.

Riscos e ameaças globais. Gerenciamento

Com os recentes aumentos das ameaças e da sua complexidade, a falta de um esquema de integração e unificação deixa de ser um simples inconveniente e passa a ser um problema grave, por aumentar riscos e vulnerabilidades, por impedir respostas coordenadas e abrangentes às contingências derivadas da materialização dos riscos e ameaças correspondentes.

É agora fundamental rever e conhecer os reais riscos a que estão sujeitos os sistemas operativos das organizações para os gerir. Neste sentido, estão a surgir uma infinidade de guias formais e informais, abordagens metodológicas e ferramentas ou plataformas de apoio, para tentar tornar objetiva a sua análise e avaliação, especialmente em tempo real.

Gestão abrangente de riscos

O objetivo é integrar todos os riscos dos departamentos da organização. Onde antes tínhamos um programa de gestão especializado para alguns deles, agora podemos garantir a existência de uma base de dados única e centralizada onde a informação sensível é gerida em tempo real e de forma eficiente.

Graças à nova Plataforma Abrangente de Gestão de Riscos e Segurança (GIRYS), podemos ter dados em tempo real; avaliar, melhorar e decidir ações preventivas e protetoras para controlar riscos e ameaças e minimizar erros ou consequências de incidentes.

Com isso, a maioria das organizações poderá observar um aumento na agilidade de controle e gestão, após aceitar que deve

ser: **Global:** como solução para gerenciar todas as áreas de risco da organização; **Escalável:** como uma plataforma que pode crescer em funcionalidades e gestão de segurança ao ritmo que a organização necessita; **Adaptável:** como sistema de gestão intuitivo, amigável e fácil de usar, capaz de se ajustar às necessidades da atividade **; Tenha informações em tempo real:** como um sistema de planejamento de recursos para saber instantaneamente o estado dos riscos da organização em todas as áreas.

O objetivo final do sistema é ajudar as organizações nas suas tarefas de administração e tomada de decisão, automatizando todos os seus processos.

Segurança Global. Esquema

Atualmente, os riscos e as ameaças globais têm muitas dimensões e formas, decorrentes de instabilidade geopolítica, crime, terrorismo, desastres naturais e, mais recentemente, pandemias globais, a guerra na Ucrânia e o conflito em Gaza, entre outros.

Neste sentido, a Segurança Global é um dos pilares fundamentais em que as organizações devem confiar, devendo ser entendida como um objetivo abrangente e integrado que visa proteger pessoas e bens ou ativos, além de servir para proteger interesses e operações estratégicas ou essenciais. Objetivos.

Novos desafios e exigências para a segurança global

Perante os novos desafios e exigências de segurança, devemos estudar as grandes mudanças e tendências que vivemos, diferenciando os riscos económicos, políticos e de segurança que nos ameaçam, para desenhar um novo cenário futuro em que um modelo de governação de segurança global seja capaz de adaptar-se e responder aos novos desafios e exigências de prevenção e proteção.

Os desafios importantes, no desenvolvimento de um novo conceito de Segurança Global, são a convergência de valores mobiliários, a transformação digital e a digitalização para a gestão operacional da segurança abrangente e integrada, pública e privada.

E há que ter em conta que o conceito de Segurança Global é especialmente importante no domínio da Proteção de Infraestruturas Críticas (PIC). Para isso, deve ser estabelecida uma Política Geral de Segurança Global onde devem ser considerados aspectos fundamentais, tais como: A proteção dos serviços essenciais; Gestão estratégica de segurança alinhada à política de riscos; A estrutura organizacional e as responsabilidades relativas à segurança abrangente; A responsabilidade, compromisso e participação de todos os colaboradores; Formação especializada e sensibilização dos recursos humanos afetos à prevenção e proteção; O desenvolvimento e gestão de capacidades de prevenção, detecção, proteção, resposta, resiliência e recuperação; Colaboração com as Forças e Órgãos de Segurança; Cumprimento regulamentar e aplicação de boas práticas; Melhoria contínua dos processos de segurança implementados.

Meios de segurança. Física e Lógica

Nos vários cenários de mudança que vivemos, na era da tecnologia e das incertezas de todos os tipos, é essencial dar uma resposta adequada e abrangente às exigências e necessidades da sociedade no atual sistema de convivência.

Como foi demonstrado, à medida que a adoção da tecnologia evolui, abrem-se oportunidades para toda a indústria. Novas abordagens de trabalho e conjuntos de recursos impulsionados por maior conectividade e disponibilidade de nuvem híbrida, bem como

a aplicação de IA, podem permitir maior escalabilidade, proteção e agilidade nas implementações de segurança nos próximos anos.

Neste sentido, a indústria da segurança está numa posição única para identificar os impulsionadores mais importantes, eventos disruptivos e desenvolvimentos derivados de novas tendências, exigências e desafios, que moldarão o novo cenário de Segurança Global.

No domínio da segurança física e lógica, o principal objetivo é o desenvolvimento de soluções integradas, escaláveis e multidimensionais através de um sistema integrado de comando, controlo e gestão com aplicação de novas técnicas de visualização de infraestruturas e sua envolvente.

Estas soluções combinam as mais avançadas características físicas de consciência situacional com as mais recentes técnicas de prevenção, deteção e mitigação de ameaças físicas ou cibernéticas, incluindo a compreensão do ciberespaço através da utilização de novas técnicas de visualização (interfaces cibernéticas, modelos 3D, cenários de realidade virtual/aumentada, etc.).

A transformação digital trouxe consigo uma mudança para implementações em nuvem e novos modelos de serviços que proporcionaram oportunidades para gerenciar o controle em aplicações de segurança, ativos físicos e dados, bem como o uso de novos formatos permitiu uma autenticação confiável e ágil.

O avanço nos últimos anos da Inteligência Artificial (IA) em aplicações sociais e de segurança infiltrou-se numa infinidade de dispositivos e continuará a disponibilizar uma verdadeira invasão desta ferramenta a todos os níveis, incluindo a segurança.

Tendências de segurança

Perante o aumento da desinformação e dos conflitos, as organizações têm de ser dinâmicas e criativas na forma como protegem os seus ativos, sejam eles tangíveis ou intangíveis, e para isso é necessário integrar uma série de medidas estratégicas

e controlos físicos e tecnológicos fundamentais. para a prevenção e proteção das próprias organizações ou infraestruturas.

Em qualquer caso, avançar para esta segurança global exige propostas viáveis e práticas e, sobretudo, muito empenho por parte dos especialistas das diferentes seguranças ou disciplinas das organizações, tendo sempre em conta os inúmeros riscos e ameaças que, como novos desafios, aguardam qualquer organização hoje.

Medidas de segurança. Planos e protocolos

A elaboração dos diferentes Planos de Segurança de edifícios e instalações, identificando vulnerabilidades e estabelecendo critérios para a aplicação de Medidas de Segurança, tanto técnicas como organizacionais, é essencial para a implementação da Segurança Global.

Igualmente importante é a elaboração dos Planos de Emergência necessários e dos procedimentos de atuação para o cumprimento nos estabelecimentos da Norma Básica de Autoproteção (bem como dos regulamentos locais e regionais que podem afetar cada estabelecimento).

Um capítulo à parte será a abordagem aos Planos de Segurança nas organizações designadas como operadores críticos, que têm a obrigação de apresentar um Plano de Segurança do Operador (PSO) e, após a sua aprovação pela Secretaria de Estado ou órgão delegado na sequência de um relatório do CNPIC, Plano Específico de Proteção (PPE).

Organização e gerenciamento de segurança

É um facto claro que, dada a gravidade dos novos riscos e ameaças que diariamente devemos enfrentar, a colaboração ao nível operacional da Segurança Privada com a Segurança Pública é uma obrigação.

Colaboração público-privada

A segurança é e será o novo desafio, principalmente nas esferas pública, cidadã e empresarial. Os responsáveis assumem cada vez mais importância em todas as entidades e organizações, com a missão de prevenir riscos e ameaças, controlar vulnerabilidades e garantir a gestão e intervenção, minimizar danos ou perdas e garantir a segurança.

O presente e o futuro da segurança cidadã oferecem uma série de vantagens muito positivas devido à existência de prestadores altamente especializados, profissionais responsáveis dos setores público e privado participantes e envolvidos nos projetos, numa clara aliança de colaboração operacional entre especialistas públicos e privados. privado. É através da colaboração operacional que são facilitadas as ações necessárias para otimizar a resposta aos novos desafios na Segurança Global e, especialmente, na Proteção de Infraestruturas Críticas.

A Espanha é uma potência em segurança pública e privada, mas precisa avançar nas suas questões pendentes. No entanto, a colaboração entre segurança pública e privada é um modelo de sucesso e motivo de orgulho.

Direção e gestão. Liderança

Até recentemente, integrar a segurança física e lógica sob um único responsável como o Diretor de Segurança era uma questão de vontade e otimização de recursos que algumas organizações vinham decidindo, mas especialmente pelo que aconteceu nos últimos anos, já não é uma questão de vontade. questão de otimização, mas irreversível, especialmente se envolver entidades ou infraestruturas críticas ou estratégicas.

Para a nova visão e missão de Segurança Global, abrangente e integrada, aliada à inteligência operacional e à gestão global, é necessário que os responsáveis pela segurança corporativa mudem a sua posição habitual de um esquema funcional, especializado e especialista, para um angular. com uma visão holística da organização e das suas atividades, que observa e analisa transversalmente a informação e, dentro dela, o que pode afetar o seu funcionamento e continuidade de forma global e sustentável.

A questão de determinar quem deve ser responsável pelo controlo da segurança das organizações é cada vez mais ampla e complexa, e é agora que devemos sublinhar a importância do novo perfil que temos vindo a propor para o Diretor Executivo de Segurança Global (CSO , CISO, CTI, etc.) que devem ter formação, conhecimentos, competências e habilidades adequadas para garantir a segurança global e proativa, abrangente e integrada (prevenção + proteção) de todos os ativos da organização, gerando as respostas corretas a incidentes e contingências críticas. .

Em suma, estamos a considerar um Diretor de Segurança Global, com uma visão holística, multidisciplinar e elevada capacidade de gestão, reportando diretamente à Direção Geral (CEO) e gerindo o risco global da organização.

Treinamento e treinamento especializado

Novos desafios e novas respostas globais exigem também uma visão partilhada, a par da preparação adequada de cada vez mais profissionais, executivos e operacionais, que devem ministrar formação e formação especializada e não linear, baseada em estratégias e pensamentos exponenciais, abertos e abertos. flexível, que os transforme nos líderes de segurança de que necessitamos.

Para tal, é necessária uma nova formação especializada, cujos principais objetivos são adquirir as competências essenciais ao desempenho de funções de segurança (prevenção e proteção), adquirindo as competências profissionais necessárias à concepção, planeamento, gestão e implementação dos correspondentes planos de segurança. e protocolos. Segurança.

Em suma, através da formação especializada, podemos contribuir para melhorar a prevenção e proteção em todas as suas áreas e garantir a modernização das condições de segurança nas nossas organizações e infraestruturas públicas e privadas.

Legislação e regulamentos

Nenhuma de todas as novas abordagens e soluções para os novos desafios e exigências de segurança será possível sem a revisão, adaptação e adaptação à alteração da regulamentação devido a outros requisitos ao nível dos requisitos como: tipo de empreiteiros aprovados, certificações no domínio da segurança da informação face a novas ameaças, como o ciberataque ou o cibercrime e as novas medidas de segurança e cibersegurança que deverão ser implementadas, bem como a adaptação da formação e educação especializadas.

A Lei 5/2014 de Segurança Privada, dependente do Ministério do Interior, é o nosso quadro regulamentar e, embora seja o mais extenso e robusto da Europa, demonstra relevância e garante a cooperação operacional público-privada para maximizar a eficiência do nosso serviço, encontra-se num momento urgente e importante de revisão e atualização para responder a estas novas demandas e desafios já mencionados.

Tem como objetivo prioritário e tema pendente, desde a Lei Orgânica 4/2015 de Segurança Cidadã, passando pela Lei 5/2014 de Segurança Privada e a sua falta de desenvolvimento regulatório, até à possível adaptação à nova ordem europeia de segurança da Lei 8/2011 sobre a proteção de infraestruturas críticas, a Lei 7/2021 sobre a proteção de dados e o desenvolvimento de legislação e regulamentos ou a lei da UE em matéria de cibersegurança.

Cultura de segurança e consciência cidadã

O objetivo é apresentar a cultura de segurança como um bem público, promovendo a evolução e o desenvolvimento de um paradigma de segurança partilhado, que se estende do global ao local.

As principais organizações focadas na análise do conceito de segurança deixaram claro o seu carácter evolutivo e a necessidade de o adaptar às transformações ocorridas com a crescente globalização da insegurança.

Plano Abrangente de Cultura de Segurança Nacional

Por Acordo do Conselho de Ministros, em maio de 2021, foi aprovado em Espanha o Plano Integral de Cultura de Segurança Nacional (Despacho PCM/575/2021, de 8 de junho), com o objetivo de servir de catalisador para a implementação progressiva de uma

política inclusiva, cultura de segurança participativa e colaborativa, tudo com o objetivo de fortalecer o Sistema de Segurança Nacional, melhorar a coordenação e eficácia da ação do Estado e a participação da sociedade.

Este Plano Integral de Cultura de Segurança Nacional foi elaborado com a participação dos vinte e dois Ministérios da XIV Legislatura de Espanha, da Secretaria de Estado das Comunicações e do Centro Nacional de Inteligência.

Manuel Sánchez Gómez-Merelo

Consultor Internacional de Seguridad Pública y Privada

Presidente e Diretor Geral de Grupo Estudios Técnicos (GET)

Diretor de Círculo de Seguridad

Sócio-Consultor de ComOutGlobal

“Sistema de Segurança para Condomínio: O que é, para que serve e qual a sua composição básica?”

José Sérgio Marcondes – CES – CPSI

Descubra como o Sistema de Segurança para Condomínio pode organizar e potencializar a proteção do seu condomínio. Saiba como manter seu imóvel protegido.

Definição de Segurança de Condomínio

A segurança de condomínio se refere a um conjunto de práticas, medidas e sistemas implementados para proteger as instalações, moradores, visitantes e propriedades dentro de um complexo residencial ou comercial compartilhado, conhecido como condomínio. O objetivo da segurança de condomínio é prevenir crimes, garantir a segurança das pessoas e promover um ambiente de convivência tranquilo.

Sistema de Segurança para Condomínio

Sistema de Segurança para Condomínio é um conjunto de medidas, dispositivos e procedimentos projetados para proteger a propriedade, moradores e visitantes em um complexo residencial ou comercial compartilhado. Esse sistema é implementado com o objetivo de prevenir crimes, garantir a segurança e promover um ambiente seguro e tranquilo. Ele pode variar em complexidade e escopo, dependendo das necessidades e do orçamento do condomínio.

Para que serve e qual o objetivo do Sistema de Segurança para Condomínio

O Sistema de Segurança para Condomínio tem vários propósitos e objetivos, todos centrados na segurança e bem-estar dos moradores e na proteção das instalações. A seguir os principais propósitos e objetivos de um Sistema de Segurança para Condomínio:

- **Prevenção de Crimes:** O objetivo principal é dissuadir a ocorrência de crimes, como invasões, roubos, vandalismos e outros incidentes. A presença visível de câmeras de segurança, sistemas de alarmes, agentes de segurança e outros dispositivos de vigilância pode desencorajar potenciais infratores.
- **Identificação de Suspeitos:** Caso ocorra algum incidente, as câmeras de segurança e outros dispositivos de vigilância são essenciais para identificar suspeitos e fornecer evidências às autoridades, o que pode facilitar a resolução de crimes.
- **Monitoramento em Tempo Real:** Um sistema de vigilância permite o monitoramento em tempo real das áreas comuns do condomínio. Isso pode ajudar a detectar atividades suspeitas ou comportamentos indesejados imediatamente.

- **Controle de Acesso:** O controle de acesso, realizado por porteiros e vigilantes, tem como objetivo garantir que apenas pessoas autorizadas entrem no condomínio. Isso ajuda a evitar visitantes indesejados ou não autorizados.
- **Resposta a Emergências:** Em situações de emergência o sistema de vigilância pode responder ou ajudar a coordenar a resposta eficaz das equipes de segurança e serviços de emergência.
- **Segurança dos Moradores:** Um sistema de vigilância aumenta a sensação de segurança dos moradores, permitindo-lhes viver com mais tranquilidade, sabendo que suas casas e famílias estão sendo protegidas.

Em resumo, o objetivo do Sistema de Segurança para Condomínio é criar um ambiente seguro, controlado e monitorado para os moradores, prevenir a ocorrência de incidentes indesejados e fornecer meios eficazes de resposta a situações de emergência ou violações da segurança. Esses sistemas desempenham um papel importante na proteção dos moradores e na preservação da tranquilidade no condomínio.

Qual a importância do Sistema de Segurança para Condomínio

O Sistema de Segurança para Condomínio é de extrema importância por várias razões, todas relacionadas à segurança, proteção e bem-estar dos moradores e das instalações do condomínio. Sua importância reside na criação de um ambiente mais seguro, protegendo os moradores e as instalações, prevenindo crimes e proporcionando tranquilidade para a comunidade. É uma ferramenta essencial para a gestão da segurança em condomínios residenciais e comerciais.

Sistema de Segurança para Condomínio

Principais recursos do Sistema de Segurança para Condomínio

Um Sistema de Segurança para Condomínio emprega uma variedade de recursos e meios para garantir a segurança dos moradores e das instalações. Esses recursos e meios são projetados para monitorar, controlar o acesso, prevenir incidentes e fornecer evidências em caso de problemas. A seguir os principais componentes típicos:

Programa de Segurança: Um programa de segurança é um conjunto de políticas, planos, projetos, procedimentos, atividades e recursos aplicados de forma coordenada para implementar e gerenciar o sistema de segurança do condômino. Envolve políticas, planos e procedimentos de segurança.

Câmeras de vigilância: As câmeras de vigilância são componentes fundamentais de um sistema de segurança em condomínios. Elas são estrategicamente instaladas em áreas comuns, entradas, saídas, garagens e outros locais críticos.

Sistemas de Controle de acesso: Sistema de controle de acesso: Inclui portões eletrônicos, sistemas de cartão de acesso ou biometria para garantir que apenas pessoas autorizadas entrem nas instalações.

Alarmes de Intrusão: Sistemas de alarme podem ser instalados para detectar intrusões ou atividades suspeitas. Eles são configurados para disparar um alarme audível e, em alguns casos, notificar uma central de monitoramento ou os próprios moradores.

Interfones e porteiros eletrônicos: Eles permitem a comunicação entre os moradores e visitantes antes de conceder acesso.

Iluminação de Segurança: A iluminação adequada em áreas comuns e externas é importante para evitar pontos cegos e fornecer segurança adicional durante a noite.

Central de Monitoramento: Muitos condomínios contam com uma central de monitoramento que opera 24 horas por dia, 7 dias por semana. Ela pode ser responsável por monitorar câmeras, alarmes e interações com porteiros ou moradores.

Recursos Humanos: Os recursos humanos desempenham um papel vital na implementação e manutenção do sistema de segurança em condomínios. Eles são responsáveis por garantir que as políticas de segurança sejam seguidas, monitorar e responder a incidentes.

Implementação do Sistema de Segurança para Condomínio

A implementação de um Sistema de Segurança para Condomínio envolve vários passos e considerações. É importante planejar cuidadosamente para garantir que o sistema atenda às necessidades de segurança do condomínio. A seguir as principais etapas para implementar um Sistema de Segurança para Condomínio:

Avaliação de Necessidades: Realize uma avaliação abrangente das necessidades de segurança do condomínio, que pode ser feito por meio de uma avaliação de riscos de segurança.

Desenvolvimento um programa de segurança: Desenvolva e implemente políticas, normas, planos, projetos e procedimentos de segurança.

Treinamento dos Moradores e Funcionários: Forneça treinamento aos moradores e funcionários do condomínio sobre como utilizar o sistema e as políticas de segurança em vigor.

Revisão e Atualização: Periodicamente, revise o sistema e suas políticas de segurança para garantir que eles ainda atendam às necessidades em constante evolução do condomínio. Atualize o sistema conforme necessário.

Conclusão

Em um mundo em constante mudança, a segurança do seu lar e da sua comunidade é mais importante do que nunca. Neste artigo, exploramos a aplicação e importância do ‘Sistema de Segurança para Condomínio’ e como ele desempenha um papel crucial na proteção de moradores, na prevenção de crimes e na promoção de um ambiente tranquilo.

À medida que encerramos esta discussão, fica claro que investir na segurança do seu condomínio é importante, porém esse investimento deve ser feito de forma ponderada e organizada, priorizando a necessidade e integração das soluções de segurança disponíveis no mercado. Visando sempre uma boa relação custo benefício.

José Sergio Marcondes – CES – CPSI – Gestor, Consultor e Diretor do IBRASEP. Especialista em segurança com competências sólidas nas áreas de segurança privada e gestão empresarial. Conecte comigo nas redes sociais.

“Tendências da Agenda ESG”

Décio Luís Schons, CIEAI, CEGRC, CIGR, CISI

Depois de um período de indisputada liderança entre as modernas tendências econômicas e comportamentais, a Agenda ESG parece ingressar em um ciclo de menor visibilidade.

Como marca característica deste início de ano, tiveram lugar nos EUA alguns eventos e tomadas de posição de atores políticos e econômicos que, em particular pela importância do cenário em que vêm ocorrendo, terão influência nas ações futuras ligadas a esse campo de atuação em todo o mundo. Repassemos alguns desses eventos.

A organização Climate Action 100+ se autodefine como “uma iniciativa liderada por investidores para garantir que as maiores empresas emissoras de gases de efeito de estufa do mundo tomem as medidas necessárias em relação às mudanças climáticas.” Segundo a página da organização na internet, mais de 700 empresas estão por ela congregadas na busca dos objetivos elencados.

Ultimamente, essa iniciativa vem sendo submetida a uma série de ações judiciais movidas particularmente por estados governados por políticos do Partido Republicano, que encaram a Agenda ESG como extremamente daninha à indústria de combustíveis fósseis. É o caso dos estados do Texas, Virgínia Ocidental e Oklahoma, onde grandes empresas de investimentos parceiras da Climate Action 100+ foram impedidas de manter negócios com entidades estatais. Além disso, 21 estados governados por republicanos estão investigando a citada iniciativa por possíveis práticas ilegais nas negociações com as diferentes empresas envolvidas no processo.

Como consequência, algumas das maiores empresas gestoras de fundos de investimentos, tais como a Black Rock, a JPMorgan e a State Street Global Advisors (SSGA), encerraram ou reduziram drasticamente sua participação na Climate Action 100+, atitudes que certamente terão repercussões significativas, não só nos EUA, mas em grande parte do mundo ocidental.

É fora de questão que a sigla ESG, que responde por Environment (Meio Ambiente), Social e Governança, está saindo de moda e poderá transformar-se em um termo bem menos frequente em um futuro próximo. Isso não significa, porém, que o ideário por ela abrangido perderá importância, até porque o agravamento da crise climática e os consequentes desastres meteorológicos em todo o planeta são eventos que já não podem ser negados.

É, portanto, de todo interesse acompanhar as principais tendências ligadas à sustentabilidade nos diversos campos da atividade humana. Percebe-se, de imediato, que essas tendências pertencem a um universo mais realista e menos ligado aos efeitos midiáticos, quando comparadas àquelas difundidas em anos anteriores.

Uma dessas tendências, ao que tudo indica, está no fortalecimento das empresas de capital misto, reunindo recursos públicos e privados em empreendimentos lucrativos que também contemplem o interesse público. Essa modalidade aparece neste momento como ferramenta fundamental para impulsionar as ações da Agenda ESG até 2030.

É também voz comum a ascensão do componente feminino na direção de negócios, contrariando as tendências históricas que nos mostram o ambiente empresarial dominado por indivíduos do sexo masculino. Em reforço a essa narrativa, existem diversos relatos dando conta de que empresas administradas por mulheres vêm apresentando resultados financeiros acima da média.

Para falar de outro tema bem ventilado, podemos ver como a IA vai assumindo um papel cada vez mais assertivo em nossa sociedade moderna. As expectativas geradas ocupam um amplo espectro, desde as mais otimistas até aquelas que veem na substituição dos seres humanos por robôs o ocaso da raça humana como agregado de seres pensantes e responsáveis.

Do outro lado estão aqueles empreendedores que veem na libertação dos seres humanos da execução de tarefas repetitivas e desgastantes um convite ao progresso, incentivados que somos agora a explorar áreas nobres da inovação e da expressão criativa. A partir daí, acredita-se num importante estímulo à empatia, à intuição, ao pensamento crítico e à criatividade nos mais diversos ambientes de trabalho.

Não devemos esquecer que a Agenda ESG é muito mais que um simples programa de sustentabilidade ambiental. Na verdade, em muitos casos, em particular naqueles negócios em que as possibilidades de danos ambientais são reduzidas, a Agenda ESG concentra-se em causar impactos sociais positivos, em particular no que diz respeito à governança ética. Desse modo, a visão de futuro dessas empresas passa a incorporar o preparo das novas gerações para lidar com esses desafios. Para isso, ganham espaço atividades como o reskilling (reciclagem profissional) e o upskilling (capacitação que visa ensinar aos trabalhadores novas competências, de modo a otimizar o seu desempenho) – tudo isso no contexto de uma cultura de aprendizado contínuo.

Vimos assim como, apesar de alguns tropeços, a Agenda ESG continua a avançar. É provável que a sigla ESG passe a ser menos empregada, o que não significa que ela irá cair no esquecimento. De qualquer modo, os princípios que a orientam serão preservados, pois dizem respeito ao bem-estar da humanidade.

Independentemente de paixões ideológicas, na maior parte das vezes ligadas a interesses corporativos, o universo empresarial já incorporou esses princípios às rotinas de planejamento e execução de grande parte das atividades das corporações. Seja com que nome for, a pauta da sustentabilidade continuará presente nas rotinas da vida de cada um de nós.

Acima de tudo, acreditamos ser de todo conveniente que temas de tal relevância não sejam considerados como armas em conflitos político-ideológicos, como temos presenciado ultimamente. A Agenda ESG, com este nome ou outro qualquer, deve situar-se acima dos interesses dessa pauta conflitiva, cujas consequências todos somos capazes de antever.

O **INTERISK** é uma plataforma tecnológica e automatizada que integra diversos módulos – entre eles, o **Software ESG** – compostos de diferentes disciplinas, o que garante a abrangência e a integração de todos os processos em um único framework. Solicite uma demonstração.

Décio Luís Schons, CIEAI, CEGRC, CIGR, CISI. General-de-Exército da Reserva. Vice-Presidente de Operações de Consultoria da empresa Brasiliano INTERISK

“Vulnerabilidades de Segurança em Shopping Center: Um Guia Completo para a Proteção Efetiva”

José Sergio Marcondes – CES - CPSI

Aprenda a lidar com as Vulnerabilidades de Segurança em Shopping Centers. Descubra quais são e as estratégias para criar um ambiente mais seguro e confiável.

Vulnerabilidades de Segurança em Shopping Center envolve falhas, fraquezas ou lacunas no Sistema de Segurança do Shopping Center que podem ser exploradas por indivíduos mal-intencionados ou eventos indesejados para causar prejuízos e danos. Assegurar a segurança de um shopping é uma tarefa complexa e crucial que demanda uma análise meticulosa das principais vulnerabilidades presentes nesses espaços.

Diversos tipos de vulnerabilidades podem comprometer a segurança em shopping centers. Identificar, compreender e desenvolver estratégias para lidar com essas diversas fraquezas é o primeiro passo para estabelecer medidas de segurança abrangentes e eficazes, proporcionando um ambiente mais seguro e confiável tanto para visitantes quanto para as operações do empreendimento.

Quando as vulnerabilidades não são tratadas de maneira adequada, elas se tornam pontos de entrada potenciais para ações prejudiciais por parte de indivíduos mal-intencionados ou eventos indesejados que podem acarretar perdas e danos. Em um cenário dinâmico de segurança empresarial, compreender as nuances intricadas das lacunas de segurança é fundamental para a proteção eficaz de empreendimentos.

Ao longo deste artigo, exploraremos não apenas os tipos específicos de vulnerabilidades que podem afetar a segurança de um shopping center, mas também estratégias abrangentes para as mitigar. Prepare-se para descobrir como uma gestão de vulnerabilidades é crucial para estabelecer medidas de segurança que garantam um ambiente acolhedor, protegido e operacional.

O que é uma Vulnerabilidade de Segurança em Shopping Center?

Uma Vulnerabilidade de Segurança em Shopping Center é uma falha, fraqueza ou lacuna no Sistema de Segurança em Shopping Center que podem ser exploradas por indivíduos mal-intencionados ou eventos indesejados para causar danos, roubo, vandalismo, ou outros incidentes prejudiciais.

As Vulnerabilidades de Segurança em Shopping Centers referem-se a pontos suscetíveis a ameaças e riscos que podem comprometer a integridade, a segurança e a operação eficiente do empreendimento comercial.

Essas vulnerabilidades de segurança podem abranger várias áreas do Shopping Center, desde aspectos físicos até questões operacionais, administrativas e tecnológicas, que, se não forem devidamente identificadas e mitigadas, podem

resultar em situações de risco para os empreendedores, clientes, funcionários, propriedades e informações sensíveis.

Em essência, as vulnerabilidades de segurança em shopping centers são fraquezas ou lacunas que podem ser exploradas, ameaçando a segurança global e a experiência do público em um shopping center. A gestão eficaz dessas vulnerabilidades é crucial para garantir um ambiente seguro, acolhedor e funcional.

Assegurar a segurança em Shopping Center é uma responsabilidade complexa, demandando uma integração de soluções de segurança que abrangem recursos humanos, físicos, tecnológicos e programas de segurança. É imperativo que os gestores de segurança adotem uma abordagem holística, visando proteger tanto os visitantes quanto as instalações e o negócio do empreendimento.

Quais são os Tipos de Vulnerabilidades de Segurança em Shopping Center?

Diversos tipos de vulnerabilidades podem comprometer a segurança em Shopping Center. De acordo com suas características, essas vulnerabilidades podem ser agrupadas em categorias distintas:

1. **Vulnerabilidades Administrativas:** Incluem falhas nos processos de gestão de segurança, como deficiências em investimentos, programas de segurança, tecnologias e treinamento de pessoal. Garantir uma administração eficaz é essencial para mitigar riscos nessa área.

2. **Vulnerabilidade de Infraestrutura:** Relacionadas à fragilidade de elementos físicos, como sistemas elétricos, sistema de comunicação, abastecimento de água, estruturas arquitetônicas/prediais e vias de acesso. A identificação e correção de vulnerabilidades nesse âmbito são cruciais para fortalecer a infraestrutura de segurança.

3. **Vulnerabilidade de Segurança Pessoal:** Envolvem atitudes e comportamento inadequados dos indivíduos que trabalham ou frequentam o local, como clientes, funcionários e prestadores de serviços. Estratégias de investigação social, treinamento e monitoramento são essenciais para enfrentar esse tipo de vulnerabilidade.

4. **Vulnerabilidades em Equipes de Segurança:** Referem-se a lacunas no desempenho das equipes de segurança, abrangendo aspectos como deficiência de recursos, treinamento inadequado, falta de coordenação e comunicação ineficiente. Investir na capacitação e coordenação das equipes é fundamental para reforçar a segurança.

5. **Vulnerabilidades de Segurança Física:** Englobam possíveis lacunas nos dispositivos destinados a garantir a integridade física do ambiente, como muros, cercas, portas, janelas, sistemas de iluminação,

manutenção de áreas verdes, controle de acesso, câmeras, sensores e deficiências no contingente de segurança. A manutenção periódica e a atualização desses dispositivos são medidas preventivas essenciais para fortalecer a segurança.

6. **Vulnerabilidades de Segurança Cibernética:** Estão ligadas a ameaças digitais que podem comprometer os sistemas e software integrados nos sistemas de segurança física, incluindo ataques de hackers e falhas abastecimento de energia. A implementação de medidas eficazes de segurança cibernética é crucial para proteger contra essas ameaças digitais.

Fatores que influenciam o nível de vulnerabilidades de segurança em shopping center

O nível de vulnerabilidade de segurança em shopping center pode variar por diversos motivos. Dentre eles estão:

1. **Alta Administração do Shopping Center:** A atitude e o comprometimento da alta administração desempenham um papel fundamental na segurança. Quando a administração valoriza a segurança e aloca recursos financeiros significativos para investimentos em medidas de segurança, isso demonstra um compromisso sério com a proteção do empreendimento.

2. **Proprietários e Gerentes de Lojas:** A segurança em um shopping center não se limita ao espaço geral, mas também se estende às lojas individuais. Proprietários e gerentes de lojas que valorizam a segurança demonstram responsabilidade tanto para com seus funcionários quanto para com os clientes. Ao disponibilizar recursos para a segurança em suas lojas, eles contribuem para um ambiente global mais seguro e protegido.

3. **Políticas e Estratégias de Segurança:** São cruciais para definir o padrão de práticas seguras. A criação de um plano de segurança abrangente, adaptado às necessidades específicas do shopping, ajuda a estabelecer diretrizes claras e promover um ambiente seguro e protegido.

4. **Equipe de Segurança:** Investir na capacitação regular da equipe, garantir condições de trabalho motivadoras, reconhecer o bom desempenho e cultivar um comprometimento com a segurança são essenciais.

5. **Frequentadores do Local:** A atitude preventiva e segura dos frequentadores do shopping center também é vital para a segurança geral. Isso envolve seguir as diretrizes de segurança, relatar comportamentos suspeitos, estar ciente do entorno e cuidar adequadamente de seus pertences.

6. **Índice de Criminalidade:** O índice de criminalidade na região onde o shopping está localizado pode influenciar a segurança do estabelecimento. Um entendimento profundo desse índice permite que o gestor de segurança adote estratégias de segurança específicas para mitigar riscos. Colaborações com as autoridades locais também é muito importante.

Principais Vulnerabilidades de Segurança em Shopping Center

A segurança de um shopping center pode apresentar diversos tipos de vulnerabilidades, dentre as principais destaco:

1. **Infraestrutura Física Inadequada:** Deficiência e falhas na infraestrutura de energia, comunicação, água, alimentação, entre outras.

2. **Facilidades de Acesso às Áreas do Shopping:** Considerando que se trata de um espaço privada de acesso público livre, qualquer pessoa pode ter acesso a este espaço. Esta condição deve ser cuidadosamente considerada no planejamento da segurança e monitorada para garantir a segurança do local.

3. **Proteção Física Insuficiente:** A ausência ou fragilidade em barreiras físicas, como cercas, muros, portas e portões, pode aumentar a vulnerabilidade do patrimônio.

4. **Facilidade de Acesso a Áreas Restritas:** Áreas restritas com pontos de entrada inadequadamente protegidos podem facilitar o acesso não autorizado de pessoas.

5. **Deficiência nos sistemas de prevenção, detecção e combate a incêndio:** Representa uma séria ameaça à segurança a integridade das pessoas e bens.

6. **Falhas em Sistemas de Vigilância:** Sistemas de vigilância eletrônica podem apresentar vulnerabilidades se não forem instalados corretamente e mantidos regularmente.

7. **Deficiências em Iluminação:** Áreas mal iluminadas podem criar ambientes propícios para atividades criminosas.

8. **Dependência de Segurança Eletrônica:** A dependência de sistemas eletrônicos de segurança pode resultar em vulnerabilidades se esses sistemas não forem mantidos em perfeito estado de funcionamento. Eles estão sujeitos a manipulações ou falhas de funcionamento. Para mitigar esses riscos, é fundamental manter um contingente de agentes de segurança que atenda às necessidades específicas do shopping. Isso é

particularmente crucial, levando em consideração as possíveis falhas nos sistemas eletrônicos e a necessidade de uma intervenção efetiva em situações de segurança.

9. **Manutenção Inadequada:** A falta de manutenção regular em sistemas de segurança pode resultar em mau funcionamento e, consequentemente, em vulnerabilidades.

10. **Contratação de Empresa de Segurança de Baixa Qualidade:** A seleção de uma empresa de segurança inadequada pode comprometer a eficácia das medidas de segurança, sendo essencial buscar parcerias credenciadas pela Polícia Federal, confiáveis e qualificadas.

Estratégias para Tratamento das Vulnerabilidades de Segurança em Shopping Center

Tratar as vulnerabilidades de segurança em shopping centers demanda uma abordagem abrangente, envolvendo diversas estratégias. A seguir algumas das principais medidas:

1. **Avaliação de Riscos:** É crucial conduzir avaliações regulares de riscos para identificar e compreender as ameaças específicas que o shopping pode enfrentar. A priorização das vulnerabilidades deve ser realizada com base na probabilidade de ocorrência e no impacto potencial.

2. **Implementação de Estratégias de Segurança:** Investir em sistemas de segurança adequados que atendam às necessidades identificadas no processo de avaliação de riscos é fundamental. A conciliação entre o uso racional de recursos eletrônicos e humanos é essencial para uma abordagem eficaz.

3. **Treinamento e Conscientização:** Realizar treinamentos regulares de segurança para os funcionários é crucial. Fornecer orientações sobre procedimentos de emergência e práticas seguras contribui para um ambiente mais preparado. Além disso, educar os legistas e funcionários do shopping por meio de campanhas de conscientização reforça as práticas de segurança.

4. **Presença de Segurança Humana:** Manter uma presença visível de agentes de segurança em áreas estratégicas do shopping é uma medida preventiva importante, que gera dissuasão e sensação de segurança. Estabelecer equipes de pronta resposta para lidar prontamente com situações de segurança é essencial para a eficácia do sistema.

5. **Parcerias com Órgãos de Segurança Pública:** Colaborar com as autoridades locais e órgãos de segurança pública é essencial. O

compartilhamento de informações e a coordenação de esforços em situações de emergência fortalecem a resposta conjunta.

6. **Inteligência de Segurança:** Utilizar Inteligência de Segurança para antecipar ameaças potenciais, analisando padrões e tendências, é crucial. A segurança deve atuar na antecipação e neutralização de vulnerabilidades e ameaças potenciais.

7. **Auditorias e Melhorias Contínuas:** Realizar auditorias de segurança periódicas para avaliar a eficácia das medidas de segurança é uma prática essencial. Implementar melhorias contínuas, baseadas em aprendizados de incidentes passados e evoluções nas ameaças, é uma abordagem proativa.

Conclusão

Encerrando nosso artigo, reforçando a importância crucial de adotar uma abordagem abrangente no tratamento das Vulnerabilidades de Segurança em Shopping Centers, visando garantir um nível adequado de proteção para o empreendimento. Destacamos a necessidade crítica de implementar medidas preventivas, fundamentais para estabelecer um ambiente seguro e funcional.

Destacamos que abordar as vulnerabilidades de segurança em shopping centers demanda uma visão completa, envolvendo estratégias que englobam desde a avaliação de riscos até a implementação de medidas concretas de segurança. Isso inclui o treinamento e conscientização da equipe, a presença estratégica de segurança humana, parcerias colaborativas com órgãos de segurança pública, inteligência de segurança, auditorias regulares e um compromisso contínuo com melhorias.

Para aprofundar sua compreensão sobre o tema, convidamos você a explorar o nosso artigo sobre as Ameaças à Segurança em Shopping Centers. Descubra as principais ameaças que esses espaços enfrentam e, mais importante, como enfrentá-las de maneira proativa.

José Sergio Marcondes – CES – CPSI – Gestor, Consultor e Diretor do IBRASEP. Especialista em segurança com competências sólidas nas áreas de segurança privada e gestão empresarial. Conecte comigo nas redes sociais

“Gestão Integral de Risco e Segurança nos Portos”

Para estabelecer uma gestão integral de riscos e segurança nas instalações portuárias, devemos começar por propor uma rigorosa auditoria de segurança onde a descrição das atividades gerais e particulares do porto e suas operações sejam a base do trabalho (tipos de embarcações que recebe e carga que recebe). alças, volume de tráfego e capacidade de movimentação, importância económica e estratégica do porto, etc.).

Manuel Sánchez Gómez-Merelo

Consultor de Segurança Internacional

A descrição da Infraestrutura, bem como a sua localização e características geográficas do porto, juntamente com a descrição das instalações (docas, terminais, armazéns, etc.), bem como dos equipamentos de movimentação de carga e sistemas de controle, infraestrutura de transporte e acesso etc.), incluindo sistemas de comunicação e tecnologias de informação, são igualmente básicos.

Análise do ambiente e das atividades, identificação de ameaças potenciais (terrorismo, pirataria, crime organizado, roubo, sabotagem, etc.), avaliação de riscos e vulnerabilidades, análise de incidentes de segurança anteriores, interação com autoridades e empresas locais Segurança e cooperação com outros portos e organizações do setor são igualmente essenciais.

Esta secção é completada pela descrição das medidas de segurança existentes, dos sistemas de controlo de acessos e de identificação, vigilância e monitorização, dos sistemas de segurança física, dos sistemas de cibersegurança e proteção da informação e de segurança marítima e proteção de navios, bem como de resposta a emergências. planos e gestão de crises.

Por fim, a implementação de planos de contingência e resiliência, a gestão de crises, a incerteza e a agilidade na tomada de decisões são recomendações para reforçar a proteção num ambiente de volatilidade e insegurança.

Política de segurança

As novas exigências, desafios e necessidades de segurança exigem adaptação e alterações normativas e regulatórias na segurança portuária, e a resposta às novas ameaças emergentes e às mudanças no panorama de risco exigem a implementação de novas tecnologias e soluções de prevenção e proteção e melhoria contínua dos processos de segurança. e procedimentos, bem como maior colaboração e troca de informações com todas as partes interessadas e envolvidas.

Assim, um novo planeamento deve ser feito com base na prevenção e no desenvolvimento de um plano abrangente de segurança portuária com identificação e priorização de medidas preventivas, na alocação de recursos e orçamento para iniciativas de segurança, no estabelecimento de objetivos e métricas de desempenho em segurança, implementando formação. e programas de conscientização para funcionários, realizando avaliações periódicas de risco e auditorias de segurança, além de resposta a incidentes e planejamento de continuidade de negócios.

Da mesma forma, deve ser proposta uma nova otimização da proteção para fortalecer a segurança física e lógica e o controle de acesso, melhorias na vigilância e monitoramento em tempo real, implementação de sistemas avançados de detecção de ameaças, integração de tecnologias de segurança (IoT, IA, análise de dados, etc.), otimizando a resposta a incidentes e a gestão de crises, bem como promovendo uma cultura de segurança proativa em toda a organização com maior colaboração operacional entre a segurança pública e a privada.

Gerenciamento de riscos

A identificação e classificação exaustiva de potenciais riscos e ameaças é fundamental, bem como a sua categorização por nível de criticidade ou potencial impacto é essencial para a análise e avaliação, da sua probabilidade de ocorrência, do seu potencial impacto nas operações, reputação, finanças, etc.

A determinação do nível de risco (baixo, médio, alto, crítico), a sua priorização com base na probabilidade e impacto e a consideração de fatores de risco específicos do porto revelarão o nível das suas vulnerabilidades e fragilidades físicas, operacionais e de segurança. cibernética. A análise de vulnerabilidades em processos, pessoas e tecnologia, a descrição detalhada de cada

vulnerabilidade identificada no ambiente portuário possibilitarão efeitos em cascata.

A gestão abrangente dos riscos, o desenvolvimento de uma estrutura de gestão dos riscos a nível organizacional, a integração da gestão dos riscos na tomada de decisões e nas operações, bem como a atribuição de funções e responsabilidades pela gestão desses riscos, em conjunto. otimizarem esta gestão, elevarão o nível de segurança para níveis aceitáveis.

Por último, a identificação de estratégias de tratamento (evitar, mitigar, transferir, aceitar), o desenvolvimento de planos de ação para mitigar riscos prioritários, a implementação de controlos e medidas de segurança adicionais, bem como a transferência de riscos através de seguros ou outros mecanismos, como bem como a aceitação informada dos riscos residuais, reforçarão o ajustamento contínuo das estratégias de tratamento dos riscos.

Medidas de segurança

Os principais objetivos da segurança nas instalações portuárias são a proteção da vida e segurança das pessoas, a salvaguarda dos ativos físicos e das infraestruturas, a garantia da continuidade operacional e a resiliência do porto no cumprimento dos requisitos legais e regulamentos de segurança, juntamente com a proteção de sistemas de informação e tecnológicos para a confiança das partes interessadas.

Com base na matriz de riscos, ameaças e vulnerabilidades estabelecida e na sua atualização periódica, será descrito o sistema de segurança abrangente de medidas físicas, operacionais e cibernéticas com integração de tecnologias e sistemas, funções e responsabilidades do pessoal de segurança e processos e procedimentos operacionais de segurança.

A concepção basear-se-á na avaliação de riscos e nos requisitos de segurança, na incorporação de princípios de defesa em profundidade e resiliência, na integração dos sistemas de segurança com outros sistemas portuários, bem como no planeamento de redundância e nas capacidades de backup com validação e testes da concepção de segurança.

Os meios de controle de segurança, controlos de acesso físico (cercas, barreiras, portas, etc.), sistemas de vídeo vigilância e monitorização, sensores, drones, etc.), bem como controlos de segurança para cargas e navios, incluindo medidas de segurança para instalações críticas e infraestruturas serão complementadas pelas correspondentes medidas organizacionais, desenvolvimento de políticas e procedimentos de segurança, bem como programas de formação e sensibilização em segurança.

Planos de segurança

Os objetivos e otimização mensuráveis dos planos de segurança são o alinhamento dos objetivos com a estratégia e prioridades do porto, a otimização dos recursos e orçamento atribuídos à segurança. A identificação de oportunidades para melhorar a eficiência e eficácia, bem como o estabelecimento de mecanismos de monitoramento e revisão de objetivos e ajustes com base em mudanças no ambiente de risco.

Os planos de segurança serão desenvolvidos com uma visão global de prevenção e proteção para reduzir a probabilidade de incidentes através de avaliações de risco e vulnerabilidade e da implementação de controlos e medidas de segurança proativas, programas de formação e sensibilização em medidas de segurança e proteção para mitigar o impacto dos incidentes. com planos de resposta a emergências e gestão de crises, em coordenação com empresas de segurança e primeiros socorros e integração com outros planos operacionais portuários, sem esquecer a revisão e atualização periódica dos planos com base nas lições aprendidas.

Serão desenvolvidos planos de contingência e continuidade de negócio para cenários de interrupção de processos críticos da atividade, implementando estratégias de manutenção das operações durante as interrupções e estabelecimento de enclaves e sistemas de backup, planos de comunicação e gestão de crises.

Serão desenhados procedimentos para recuperação e retomada das operações normais, bem como testes regulares e exercício de planos de contingência e exercícios de contingência com planos de segurança e operações.

Como comportamento organizacional, será estabelecida a promoção de uma cultura de segurança e resiliência na organização, com liderança visível e comprometimento da alta administração com a segurança, comunicação aberta e transparente e aprendizado contínuo para compartilhar conhecimentos sobre segurança portuária.

Monitoramento e controle

A implementação eficaz das medidas preventivas identificadas nos planos de Segurança, o reforço contínuo da segurança física, operacional e cibernética, a manutenção e atualização regular dos sistemas e equipamentos de segurança serão estabelecidos através da monitorização e controlo proativo dos riscos e

ameaças emergentes, em colaboração com partes interessadas a melhorar as medidas de prevenção e proteção com avaliações periódicas para identificar oportunidades de melhoria.

Uma estrutura organizacional e protocolos serão estabelecidos para o gerenciamento de segurança com definição de funções, responsabilidades e linhas de subordinação para o pessoal de segurança, com desenvolvimento e implementação de protocolos e procedimentos operacionais padronizados para garantir consistência e conformidade com os protocolos em toda a organização, incluindo revisão periódica e atualizar protocolos com base nas mudanças e lições aprendidas e treinar regularmente a equipe em protocolos e procedimentos de segurança.

A gestão abrangente de riscos e segurança será implementada em todos os níveis da organização com a alocação de recursos apropriados para apoiar uma gestão eficaz de riscos e segurança. Serão realizadas auditorias internas regulares e revisões do sistema de gestão de segurança com participação em auditorias externas e certificações de segurança reconhecidas pela indústria, revisão periódica de políticas, procedimentos e controles de segurança, realização de testes e exercícios para avaliar a eficácia dos planos e segurança. capacidades, bem como a identificação e monitoramento de ações corretivas e oportunidades de melhoria com comunicação dos resultados das auditorias e revisões às partes interessadas.

Treinamento e comunicação

Será desenvolvido um plano abrangente de formação em segurança para todo o pessoal interno e externo, com identificação das necessidades de formação com base nas funções e responsabilidades e incorporação de diversas metodologias de formação (presencial, online, treinos, exercícios, etc.) com o estabelecimento de um programa regular e recorrente. cronograma de treinamento e avaliação da eficácia do treinamento e ajuste dos programas conforme necessário.

Será estabelecido um plano de comunicação para promover a sensibilização para a segurança com a utilização de diversos canais de comunicação (intranet, newsletters, sinalização, etc.) e a promoção de uma cultura de segurança através de comunicações regulares e consistentes.

Será implementado um processo de avaliação contínua das competências de segurança, com a definição de padrões e critérios claros para a avaliação periódica de conhecimentos, competências e atitudes e com a utilização dos resultados da avaliação para identificar lacunas e necessidades de formação e reconhecimento e premiar o elevado desempenho e melhorar as competências de segurança.

Legislação e regulamentos

Será estabelecida uma identificação abrangente de todas as leis, regulamentos e normas de segurança aplicáveis às instalações portuárias de requisitos internacionais, nacionais e locais, com análise detalhada de sua aplicabilidade às operações portuárias e com atribuição de responsabilidades pelo monitoramento e cumprimento de cada norma, através de mecanismos para manter as alterações legislativas e regulamentares atualizadas, garantindo a comunicação regular dos requisitos legais e regulamentares relevantes a todo o pessoal de segurança.

O compromisso da alta administração deve ir além do mero cumprimento da Legislação com a adoção de uma abordagem proativa e preventiva de segurança em todas as operações e o estabelecimento de padrões e melhores práticas que superem os requisitos mínimos, promovendo uma cultura de segurança que valorize prevenção e melhoria contínua e a alocação de recursos adequados para apoiar medidas preventivas fortes, juntamente com o reconhecimento e recompensa de iniciativas e realizações de prevenção notáveis.

Manuel Sánchez Gómez-Merelo

Consultor Internacional de Seguridad Pública y Privada

Presidente e Diretor Geral de Grupo Estudios Técnicos (GET)

Diretor de Círculo de Seguridad

Sócio-Consultor de ComOutGlobal

“A Importância da Gestão de Perdas Integrada a Gestão de Riscos nas Empresas”

Marcos Alves Junior, CIEIE, CIGR, CPSI

É comum que todas as empresas enfrentem riscos e lidem com perdas. Devemos encarar a materialização dos riscos como uma realidade concreta. O Antonio Celso Ribeiro Brasiliano, PhD, defende a ideia de que não há garantia de segurança total. Por isso, consideramos essencial que as empresas estejam preparadas para lidar com as perdas, sejam elas quais forem. Portanto, é importante sabermos o que é a gestão de perdas em sua essência e qual sua importância para as organizações. Dessa forma teremos clareza em saber como ela surgiu e ajuda a garantir um futuro mais próspero para as empresas.

A gestão de perdas surgiu da necessidade das empresas de reduzir perdas financeiras decorrentes de furtos, quebras, danos e erros operacionais. Inicialmente, focava-se na prevenção de furtos no varejo, ganhando destaque nos Estados Unidos durante o século XX. Com o tempo, evoluiu para abranger uma gama mais ampla de atividades, incluindo gestão de riscos operacionais, otimização de processos e proteção dos ativos da empresa. Isso reflete a importância crescente atribuída à gestão eficiente dos recursos e à proteção dos ativos das empresas.

A gestão de perdas se tornou essencial em diversos setores empresariais, envolvendo estratégias para minimizar perdas financeiras e operacionais, garantir a segurança dos colaboradores e clientes, além de proteger o patrimônio da empresa.

Ao reconhecer a inevitabilidade dos riscos, as empresas podem se tornar mais resilientes e capazes de superar adversidades, garantindo sua sustentabilidade a longo prazo.

A **Brasiliano INTERISK** trabalha a abordagem da gestão de perdas integrada à gestão de riscos; ao unir essas duas áreas, as empresas podem identificar, avaliar e mitigar possíveis perdas decorrentes de eventos adversos, sejam eles relacionados a aspectos financeiros, operacionais, estratégicos e/ou reputacionais.

A gestão de riscos traz uma visão de antecipação e prevenção de eventos que possam impactar negativamente a organização, enquanto a gestão de perdas se concentra na minimização dos impactos decorrentes desses eventos, caso ocorram. A integração dessas duas abordagens permite uma visão abrangente e proativa, possibilitando a identificação precoce de potenciais perdas, bem como a implementação de medidas para reduzir sua probabilidade e impacto.

Ao adotar uma abordagem integrada, as empresas podem otimizar seus recursos, promover uma cultura organizacional mais resiliente e ágil, e fortalecer sua capacidade de recuperação diante de adversidades. Além disso, a

integração da gestão de perdas à gestão de riscos demonstra um compromisso com a excelência operacional, a responsabilidade corporativa e o cuidado com os stakeholders.

Em suma, a gestão de perdas integrada à gestão de riscos representa uma abordagem estratégica e holística que contribui significativamente para a proteção do valor do negócio e para o alcance dos objetivos organizacionais em um ambiente cada vez mais desafiador e dinâmico.

O processo de gestão das perdas através do **Software INTERISK** é bastante intuitivo e dividido nas seguintes etapas:

1. Registro: Realiza a abertura da ocorrência e classifica em qual disciplina de riscos o evento ocorreu, fazendo uma descrição dos danos, dos envolvidos, repercussão na mídia, paralisação da operação e notificação do grupo de emergência.

2. Análise e Parecer: Lista as fragilidades da ocorrência, controles, envolvidos, registro oficial das áreas, impacto real e potencial, fornecendo informações estruturadas para embasar a tomada de decisões após uma investigação eficaz.

3. Investigação: A investigação consiste na inspeção dos fatos, identificando a causa raiz das perdas, com a aplicação da ferramenta Diagrama de Causa e Efeito (DCE), permitindo uma visão dos fatores de riscos identificados pelo gestor da área e a possibilidade de acrescentar novos fatores de riscos mediante a apuração dos fatos.

4. Encerramento / Conclusão: Com base no resultado da investigação, é necessário realizar um plano de ação para atuar na causa raiz do problema, aplicando a ferramenta 5W2H e otimizando recursos com uma gestão automatizada do plano de ação.

O INTERISK é uma ferramenta inovadora e automatizada que tem como objetivo facilitar o gerenciamento das perdas, caso algum risco se materialize. O **Software de Gestão de Perdas** opera de forma integrada ao **Software de Gestão de Riscos Corporativos** e oferece diversos benefícios à sua empresa, capacitando-a a superar as difíceis eventualidades decorrentes de riscos que se tornem realidade.

Entre em contato com um especialista e agende uma demonstração de como o sistema pode atuar na sua organização.

Marcos Alves Junior, CIEIE, CIGR, CPSI, Redator, Editor de texto, Criador de vídeos. Cursou Gestão Empresarial na Anhanguera. Formado pela Uninove – Universidade Nove de Julho em Comunicação Social – Jornalismo. Assistente de Comunicação e Marketing na Brasiliano INTERISK.


CORPORACIÓN EURO-AMERICANA DE SEGURIDAD
CEAS - INTERNACIONAL