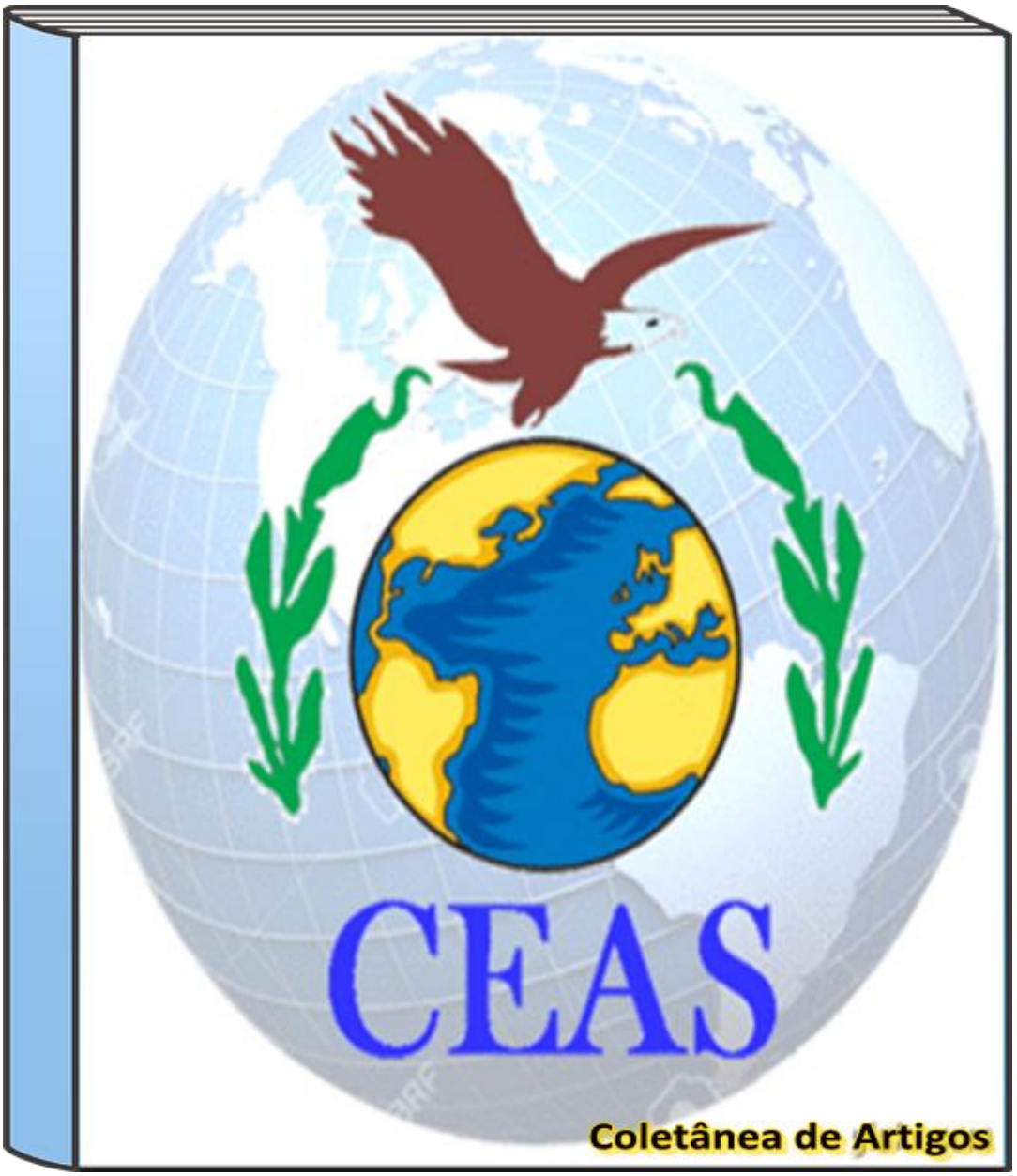


Edição VII - 2023

contato@ceasbrasil.com.br

SUMÁRIO

INTRODUÇÃO

Décio Luís Schons, CIEAI, CEGRC, CIGR, CISI

Em resposta à carência, em nosso país, de publicações relacionadas à gestão de riscos e segurança empresarial especializada, a Corporação Euro-Americana de Segurança (CEAS) no Brasil presenteia seus associados e parceiros com o 7º volume de sua Coletânea de Artigos sobre esses temas.

Já de longa data, a CEAS-Brasil vem envidando 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.

Não é segredo para ninguém que as atividades de segurança e gestão de riscos assumiram, em nossos dias, um caráter estritamente profissional, em que não mais se admitem amadorismos. A evolução dos recursos tecnológicos colocados à disposição de toda a sociedade, inclusive das organizações criminosas, impõe aos responsáveis pelas áreas correspondentes, nas empresas e organizações em geral, um estado de permanente prontidão. Esse estado de prontidão não se refere apenas à área de máquinas e equipamentos, mas diz respeito, sobretudo, à capacitação de recursos humanos. Neste último ponto, entra em pauta o serviço prestado pela CEAS-BRASIL à nossa sociedade.

Conforme reza um velho adágio, bom negócio é aquele em que todas as partes saem ganhando. Esse é, precisamente, o caso das atividades da CEAS no Brasil. Os resultados dessas atividades são facilmente percebidos e todas as partes interessadas acabam sendo beneficiadas: os profissionais de segurança, estimulados e amparados na busca de seus objetivos de qualificação; as instituições de ensino, que passam a desfrutar de fontes de consulta adicionais para levar a bom termo suas tarefas de capacitação; as empresas dedicadas à atividade de segurança empresarial, que podem contar com um número expressivo de profissionais preparados para o desempenho de suas atividades; as empresas usuárias desses serviços, que dispõem de melhorias significativas

nas suas condições de segurança e na gestão de riscos de toda ordem; e a população em geral, em lugar de destaque como beneficiária indireta de todo o processo.

Dessa forma, a CEAS-BRASIL escreve mais um capítulo de sua história em nosso país, no caminho do pleno cumprimento de sua missão, qual seja, a de contribuir para o fortalecimento integral das organizações prestadoras de serviços de segurança pública e privada no Brasil, por meio de serviços de excelência em termos de consultoria e assistência técnica, bem como de capacitação técnica e profissional.

O presente volume apresenta uma coletânea de textos muito bem selecionados e que irão, certamente, acrescentar novos elementos de valor à formação de todos os interessados no tema que tiverem a oportunidade de percorrer suas páginas.

Nossos cumprimentos, portanto, ao Professor Dr. Renato Figueiredo, Presidente da CEAS-BRASIL, Secretário-Geral da CEAS-INTERNACIONAL e Coordenador da CEAS-INTERNACIONAL no âmbito do MERCOSUL, pela inestimável contribuição prestada à sociedade brasileira a partir desta iniciativa que teve seus primórdios no ano de 2012 – cumprimentos que estendo a sua valorosa equipe.

Boa leitura a todos.

**** General-de-Exército da Reserva, é Presidente da Associação dos Ex-Alunos e Amigos da Escola Preparatória de Cadetes do Exército (AEsPCEx), Membro do Conselho Acadêmico do Instituto de Estudos Estratégicos da UFF e Vice-Presidente de Operações de Consultoria da empresa Brasiliano Interisk***

]

CENTRO DE CONTROLE (CECON) DA SEGURANÇA EMPRESARIAL

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

Ao contrário do que muitos imaginam, um Centro de Controle (CECON) de Segurança pode propiciar muito mais do que o monitoramento de imagens, acessos, alarmes e rastreadores, bem como o atendimento e registro de incidentes. O professor Mestre **Antonio Celso Ribeiro Brasiliano** na sua obra **"Manual de Planejamento Tático e Técnico em Segurança Empresarial"** afirma que: ***"A central de segurança é o cérebro e o centro nervoso de qualquer organização. A central otimiza os recursos empregados, além de coordenar de forma ágil e em tempo real as contingências na edificação".***

Nesse contexto o CECON constitui recurso fundamental na estratégia da Segurança Empresarial de uma Empresa. Portanto, é importante refletir acerca dos requisitos fundamentais para obtenção da melhor performance.

Infraestrutura

Quando é tratado o tema infraestrutura de um CECON logo são citados itens como: controle de acesso com blindagem das portas e eclusa, sistemas redundantes, vias alternativas de comunicação e energia elétrica, monitores de alta definição e vídeo wall. Porém, nesta discussão se faz necessário incluir itens que farão muita diferença no dia a dia da operação, como:

- Mesas com regulagem de altura: visando redução de dores nas costas, pois os operadores não passarão horas seguidas na mesma posição e versatilidade para ajuste da mesa ao formato mais confortável para o momento;

- Cadeiras ergonômicas: propiciando aos operadores se manterem na posição adequada durante suas atividades, prevenindo lesões e conferindo mais conforto;

- Iluminação adequada: aumentando acuidade visual e, a velocidade da leitura e da concentração, reduzindo a fadiga ocular sonolência, consequentemente o aumento da performance do operador.

Manual

Todas as atividades a serem executadas deverão estar redigidas no Manual do CECON. Nenhuma ação e/ou decisão poderá ser tomada pelo operador, inspetor, supervisor ou coordenador de forma subjetiva, ou seja, todos procedimentos deverão estar escritos.

É recomendável que no Manual do CECON conste, mas não se limite, aos itens

à saber:

- Objetivo;
- Matriz de responsabilidade;
- Descrição da atividade de cada cargo;
- Orientações técnicas/operacionais: dos sistemas de segurança eletrônica integrados; supervisão dos postos de vigilância e serviços; premissas para o acesso ao CECON, plano das atividades frente incidentes de segurança, plano de acionamento em caso de emergências, procedimento operacional padrão (POP), passagem de posto etc
  .

Não obstante, o CECON deve possuir o *Book* de cada unidade (instalação) contendo: endereço com coordenadas geográficas, pontos de referências, número de colaboradores efetivos (próprios e terceiros), colaborador responsável pela unidade, croqui, efetivo de segurança e instrução de trabalho de cada posto de serviço (vigilância, portaria e recepção) e etc.

É fundamental ter de forma digital e física o manual do CECON e os dados das unidades de segurança pública e serviços de emergência localizados no entorno de cada instalação.

Em virtude disso, é vital que o gestor de segurança tenha em mente que “tudo que não é escrito fica subentendido”.

Seleção

Frente a importância do CECON para área Segurança Empresarial, se faz necessária dedicação de tempo do gestor nesta atividade. Apesar de existirem diversas premissas, muitas delas expostas neste artigo, o CECON estará sempre em linha com as políticas e os sistemas integrados da Empresa. Assim sendo, recomenda-se que a seleção dos profissionais que atuarão no CECON considere como “fiel da balança” o comportamento do candidato.

Isso, porque a questão técnica (o saber fazer) poderá ser lapidada com treinamentos específicos, sendo certo que o comportamento não, pois é a maneira de se portar de cada pessoa. Trata-se da máxima “contrata-se pela competência técnica e demite-se pela comportamental”.

O comportamento em linha com a função exercida é fundamental para performance individual e, por consequência da equipe no setor tão sensível e específico da segurança.

Treinamentos

É sabido que o treinamento visa qualificar o profissional para algo específico das suas tarefas. Nesse diapasão, tendo o CECON como “***cérebro e o centro nervoso”***, visando **“*coordenar de forma ágil e em tempo real as contingências”*** se faz necessário que todos os integrantes da equipe, operadores e liderança, estejam capacitados através de treinamentos específicos e customizados, conforme sugestões abaixo:

- Temas técnicos: treinamentos específicos e reciclagens no sistema de segurança integrado;

- Temas operacionais: políticas internas, manuais, instruções de trabalho e procedimentos operacionais padrão (POP);

- Simulados: treinamentos práticos que simulam, de forma realista, incidentes de segurança, situações de risco e emergência, fazendo com que todos os operadores do CECON saibam exatamente as ações a serem adotadas frente um caso real;

- Lei Geral de Proteção de Dados (LGPD): treinamento voltado para conformidade da legislação no que tange ao tratamento de dados pessoais, dispostos em meio físico ou digital, no CECON.

Atribuições

Visando obter melhor performance da equipe do CECON, agregando valor a Segurança Empresarial, recomenda-se as seguintes pertinências:

- Monitoramento do sistema integrado de segurança eletrônica: imagens, analíticos, alarmes, acessos, rastreadores etc.;

- Monitoramento e controle da vigilância e serviços: confirmações dos postos, acompanhamento, direcionamento e orientação do efetivo;

- Coordenação, tratamento, comunicação e registro de incidentes de segurança nas unidades da Empresa;

- Relatórios estatísticos;

- Monitoramento do cenário de segurança pública através de *Clipping*: seleção das notícias em sites e outros meios de comunicação, digitais ou impressos, resultando num apanhado de informações sobre assuntos de total interesse da área de Segurança Empresarial da Empresa.

Segurança dos Dados

Pelo princípio da necessidade de conhecimento os operadores do CECON detêm diversas informações da Empresa e dos seus colaboradores. Além do mais, são criadores de informações e dados sensíveis. Por isso, é imprescindível que todos os colaboradores do CECON leiam, entendam, concordem e assinem um Termo de Confidencialidade e Sigilo das informações que terão acesso para realização das suas atividades.

Em suma, os requisitos sugeridos neste artigo visam de forma objetiva melhorar a performance do CECON a qual poderá ser percebida ao passar do tempo pela eficiência, eficácia e efetividade. Com a utilização adequada deste recurso a Segurança Empresarial ganha confiabilidade, amplitude, agilidade e qualidade nas suas atividades.

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

A IMPORTÂNCIA DAS MEDIDAS DE SEGURANÇA NO AMBIENTE ESCOLAR

Walter Oliveira, CPSI, MBA

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| 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.

Agenda ESG no Brasil

Décio Luís Schons, CIEAI, CEGRC, CIGR, CISI

Para iniciar, diremos, contrariando o pensamento de alguns estudiosos do assunto, que a sustentabilidade não é um modismo. Trata-se de uma pauta atual e que reúne boas condições para ganhar um caráter de permanência, exatamente por tratar de temas vitais para a saúde e o bem-estar das pessoas e das comunidades, agregando uma noção de grande abrangência. Assim sendo, toda vez que uma empresa se alinha às práticas socioambientais e apresenta bons indicadores ESG, é normal que passe a desfrutar de melhor aceitação por parte do mercado e da sociedade em geral.

Sucesso do Negócio

Quando focamos no Brasil, vemos que, de forma progressiva, o uso dos indicadores ESG vem recebendo maior atenção, não apenas do mercado, mas também de boa parte da população em geral. Há, pelo lado dos consumidores, uma renovada consideração pelos aspectos socioambientais, que hoje constituem parcela importante na avaliação da imagem e da reputação de qualquer empresa. Um dos resultados palpáveis, ao motivar os consumidores a se conectar e permanecer em sintonia com a marca e seus propósitos, é a fidelização da clientela, com o consequente aumento na previsibilidade das receitas e dos lucros do empreendimento.

Redução de Custos

O correto entendimento e aplicação dos princípios da Agenda ESG é de grande valor no momento de selecionar e empregar as matérias-primas utilizadas pela empresa de maneira consciente e otimizada.

Aparecem assim oportunidades de reduzir os custos pelo melhor aproveitamento de matérias-primas, melhorando os resultados financeiros e obtendo vantagens competitivas em face dos concorrentes. Isso significa, em síntese, melhorias de vulto na saúde financeira do empreendimento.

Como não poderia deixar de ser, essas considerações devem se estender a toda a cadeia de fornecimento, sob pena de invalidar os esforços realizados no interior das instalações da organização considerada.

Oportunidades de Negócios

O correto entendimento e aplicação dos princípios ESG funciona à semelhança de uma lente que permite identificar gargalos de naturezas variadas. A implementação de um sistema de compliance completo e bem divulgado atrairá, com certeza, a boa vontade de um público crescentemente interessado nos princípios do consumo consciente. Ética nos negócios, política de inovação e efetividade formam a tríade que possibilitará o aperfeiçoamento no

relacionamento com stakeholders internos e externos e, em consequência, o aumento na lucratividade em todos os campos.

Redução de Desperdícios

Há cerca de dois anos, chamou a atenção a notícia de que, na capital de determinado estado brasileiro, famílias de pessoas necessitadas estariam "assaltando" caminhões de lixo para obter restos de alimentos. Essas sobras de produtos de consumo eram oriundas de conhecida rede de supermercados que divulgava como um de seus princípios mercadológicos a sustentabilidade. Com a publicação da notícia, incluindo filmagens dos eventos, a empresa foi acusada de praticar green washing. A solução para o problema foi bastante criativa: os caminhões de coleta de lixo, deixaram de recolher os resíduos às 8 horas da manhã e passaram a fazê-lo às 3 horas da madrugada.

Aspecto muitas vezes não mencionado pela literatura especializada é a importância na redução de desperdícios por parte das empresas. Esse é um problema que não se restringe ao Brasil. Calcula-se que cerca de 1 bilhão de toneladas de alimentos são desperdiçados globalmente. Enquanto os aterros sanitários transbordam de alimentos que poderiam ter sido reaproveitados, doados ou compostados, milhões de pessoas não dispõem do básico para o consumo de suas famílias.

Nosso país atravessa situação de vulnerabilidade alimentar para um número recorde de famílias. Reduzir o desperdício e aproveitar as sobras de forma consciente, não só em feiras e supermercados, como também nas cozinhas das residências, constitui muito mais que um gesto de caridade – constitui, sim, necessidade absoluta para melhorar a qualidade de vida em dois pilares básicos da Agenda ESG: o Social e o Ambiental. Além de tudo, as sobras não aproveitadas e destinadas aos aterros sanitários acabam se transformando em gases poluentes, o que agrava o problema.

Partindo para a ação

Colocar em execução a Agenda ESG no âmbito de uma empresa não é tarefa das menos complexas. Tendo em vista a extensão da gama de temas abrangidos, é necessário, antes de tudo, selecionar aqueles que podem fazer a diferença para a organização e para seus stakeholders. Nesse passo, ganha importância o emprego da chamada matriz de dupla relevância ou dupla materialidade.

Dentre os temas relevantes, estariam, por exemplo:

- Gerenciamento dos resíduos e efluentes sólidos, líquidos e gasosos, em particular dos gases de efeito estufa;

- Racionalização do consumo de recursos naturais;

- Redução do emprego de materiais não degradáveis em embalagens;

- Elaboração de programas voltados à saúde física e mental dos trabalhadores;

- Qualificação, capacitação e desenvolvimento de mão de obra;

- Providências visando à independência do CA;

- Gestão da cadeia de suprimento incluindo parâmetros ESG;

- Prática da diversidade, inclusão e equidade nas diversas posições no âmbito da força de trabalho;

Gestão de Riscos

Ao evidenciar os objetivos estratégicos a serem conquistados e mantidos em cada uma das dimensões e em cada um dos temas considerados relevantes, a correta gestão dos temas ESG facilita a visualização dos riscos potenciais que se antepõem à conquista e manutenção dos objetivos e metas correspondentes. A sistemática de gerenciamento de riscos da organização proporciona ao corpo operacional e administrativo a tranquilidade de trabalhar sem o perigo de violar a legislação e os padrões de procedimento. Além disso, a empresa aperfeiçoa sua capacidade de prevenir os riscos antes que eles se concretizem. Caso isso seja de todo impossível, uma competente preparação dará à empresa a agilidade para responder aos riscos já materializados, colocando em execução os planos de resposta adequados.

Caso haja interesse de sua empresa em aprofundar-se nesse ou em outros temas afetos ao gerenciamento de riscos, contate a Brasiliano INTERISK, uma empresa que oferece soluções de Inteligência e Gestão de Riscos com base na Interconectividade, conferindo total transparência aos processos de Governança, Riscos e Compliance.

Conheça o **Software INTERISK**, trata-se de uma plataforma tecnológica e automatizada que une vários módulos, incluindo o **Módulo Environmental, Social and Governance – ESG**, que garante a abrangência e a integração de todos os processos em um único framework de forma otimizada. Solicite uma demonstração para se inteirar referente aos benéficos que o sistema pode disponibilizar a sua empresa.

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

Alarme Residencial: O que é, Como Funciona, por que é essencial para sua residência!

José Sérgio Marcondes, CES, CPSI

Saiba como o alarme residencial pode ser uma solução de segurança inteligente e vantajoso para aumentar o nível de segurança da sua residência.

Alarme residencial é um sistema de segurança projetado para proteger as residências contra riscos de intrusões e situações de perigo, fornecendo um alerta imediato em caso de atividade suspeita e de riscos. É composto por dispositivos eletrônicos interconectados que detectam e sinalizam eventos indesejados, como invasões, tentativas de arrombamento, incêndios, vazamentos de gás, entre outros.

Você já parou para pensar na segurança da sua casa? Atualmente, proteger a residência é uma preocupação cada vez mais presente na mente das pessoas. Afinal, nossa casa é o refúgio onde buscamos conforto, paz e segurança. É o lugar onde guardamos nossos bens mais valiosos e, acima de tudo, onde nossos entes queridos estão presentes.

No entanto, infelizmente, a tranquilidade da nossa casa pode ser ameaçada por diversos fatores. É nesse contexto que entra a importância do alarme residencial. Investir em soluções de segurança adequadas é essencial para garantir a tranquilidade e a proteção de nossa família.

Neste artigo, vamos explorar em detalhes os principais conceitos do alarme residencial. Vamos descobrir o que são alarmes residenciais, como funcionam e quais são os diferentes tipos disponíveis. Além disso, vamos explorar os benefícios de usar um sistema de alarme e dicas para escolher o sistema mais adequado.

O que é um alarme residencial?

Um alarme residencial é um sistema de segurança projetado para proporcionar segurança residencial ou seja, para proteger as residências contra riscos de intrusões e situações de perigo, fornecendo um alerta imediato em caso de atividade suspeita e de riscos. Ele é composto por dispositivos eletrônicos interconectados que detectam e sinalizam eventos indesejados, como invasões, tentativas de arrombamento, incêndios, vazamentos de gás, entre outros

Um alarme é um dispositivo eletrônico que emite um sinal sonoro, visual ou ambos, com o objetivo de alertar as pessoas sobre uma determinada situação ou evento. Eles podem variar em termos de tamanho, design e funcionalidade, mas sua finalidade principal é chamar a atenção das pessoas e notificá-las sobre algo importante ou urgente.

Os alarmes são amplamente utilizados em diferentes contextos para fins de segurança, emergência, monitoramento e aviso. No caso do alarme residencial, além de proteger contra roubos e invasões, alguns sistemas podem incluir

recursos adicionais, como detecção de incêndio, vazamento de água ou monóxido de carbono, aumentando ainda mais a proteção das casas e apartamentos.

Para que serve e qual o objetivo do alarme residencial?

O alarme residencial serve para proteger casas e apartamentos (residências) contra invasões, furtos, roubos, incêndio e outros riscos e perigos, tendo como objetivo principal aumentar a segurança dos moradores e de seus valores e bens. Ele desempenha várias funções importantes como:

1. Dissuasão: A simples presença de um alarme residencial visível, como câmeras de segurança, sensores de presença e placas de advertência, pode dissuadir potenciais invasores. Saber que uma casa está protegida por um alarme cria uma barreira psicológica e faz com que os criminosos pensem duas vezes antes de tentar invadir.

2. Detecção precoce de intrusões: Os sensores de movimento e sensores de abertura dos alarmes de cada e apartamento detectam atividades suspeitas, como movimentos não autorizados ou abertura de portas e janelas. Isso permite que os moradores sejam alertados imediatamente sobre qualquer tentativa de invasão.

3. Alerta sonoro ou visual: Quando um sensor é acionado, a central de controle do alarme dispara um alarme sonoro ou visual, como uma sirene alta, luzes piscando ou notificações sonoras no aplicativo móvel. Esse alerta chama a atenção dos moradores e vizinhos, alertando sobre a possível intrusão e solicitando ação imediata.

4. Notificação a empresa de monitoramento: A maioria dos alarmes residenciais podem ser conectados a uma empresa de monitoramento. Isso permite uma resposta rápida e eficaz em situações de emergência.

5. Tranquilidade e paz de espírito: O objetivo final de um alarme residencial é proporcionar tranquilidade aos moradores, permitindo que se sintam seguros em sua própria residência. Saber que há um sistema de segurança confiável em vigor aumenta a sensação de proteção e reduz o medo de invasões e roubos.

Em resumo, o objetivo principal do alarme residencial é proteger a residência, os moradores e seus pertences, fornecendo uma camada adicional de segurança, detecção precoce de intrusões e uma resposta rápida em caso de eventos indesejados.

Qual a importância do alarme residencial?

O alarme residencial desempenha um papel fundamental na segurança da sua residência e na proteção dos moradores e de seus bens. Aqui estão algumas das principais razões pelas quais o alarme residencial é importante:

1. Deter e prevenir intrusões: A presença visível de um sistema de alarme pode fazer com que os criminosos pensem duas vezes antes de tentar invadir a propriedade.

2. Alertar os moradores e vizinhos: permite que os moradores ajam rapidamente, tomando as medidas apropriadas para garantir sua segurança e chamar as autoridades, se necessário.

3. Proteger contra incêndios e vazamentos: Ao detectar ameaças precocemente, o alarme residencial pode alertar os moradores e ajudar a minimizar os danos causados por incêndios ou vazamentos.

4. Monitoramento remoto e resposta rápida: Em caso de violação, a central de monitoramento residencial pode tomar medidas imediatas, como contatar as autoridades locais ou enviar uma equipe de segurança para verificar a situação.

5. Tranquilidade e sensação de segurança: Saber que um sistema de segurança está em vigiando a residência pode reduzir o estresse e a ansiedade relacionados à segurança residencial, especialmente quando os moradores estão em viagem.

Em resumo, o alarme residencial desempenha um papel essencial na proteção da residência, dos moradores e dos bens. Ele dissuade intrusos, alerta os moradores e vizinhos, protege contra incêndios e vazamentos, oferece monitoramento remoto e proporciona tranquilidade.

O que é Alarme residencial não monitorados?

Os alarmes residenciais não monitorados ou autônomo são sistemas eletrônicos de segurança instalados em residências que não estão conectados a uma central de monitoramento residencial. Não enviam sinais de alerta para uma equipe de monitoramento 24 horas por dia.

Os alarmes residenciais não monitorados funcionam de forma autônoma e dependem dos dispositivos instalados para detectar atividades suspeitas. Esses dispositivos podem incluir sensores de movimento, sensores de abertura de portas e janelas, câmeras de vigilância, sirenes, entre outros.

Quando ocorre uma violação ou atividade suspeita, o alarme residencial não monitorado é ativado e emite um sinal sonoro alto para alertar os moradores, vizinhos e possíveis intrusos. Eles são uma opção mais barata para aqueles que desejam ter algum nível de proteção e alerta de baixo custo.

O que é alarme residencial monitorado?

Um alarme residencial monitorado é um sistema de segurança que está conectado a uma empresa de monitoramento residencial. Quando ocorre uma atividade suspeita, como uma intrusão ou disparo de um sensor, o alarme envia um sinal para a central de monitoramento residencial.

A equipe da central de monitoramento avalia o sinal recebido e toma as medidas apropriadas, como entrar em contato com os moradores, verificar a situação e, se necessário, enviar ajuda de emergência, como a polícia.

O que é uma empresa monitoramento residencial?

Uma empresa de monitoramento residencial é uma empresa especializada na prestação de serviços de monitoramento de alarmes residências. O serviço de monitoramento de alarme consiste em uma central de monitoramento de alarmes instalada na sede da empresa que acompanha os sinais enviados pelos alarmes instalados nas residências.

A central de monitoramento da empresa opera 24 horas por dia, 7 dias por semana. Ela recebe e monitora os sinais enviados pelos dispositivos de segurança instalados na residência. Isso inclui a detecção de atividades suspeitas, como violação de portas, janelas, movimentos não autorizados, entre outros.

Quando ocorre uma atividade suspeita ou uma violação é detectada, a central de monitoramento residencial toma as medidas apropriadas. Isso pode envolver a comunicação com os moradores, notificação das autoridades locais de segurança ou envio de uma equipe de resposta para verificar a situação.

Quais são os componentes do alarme residencial?

Um sistema de alarme residencial básico inclui os seguintes componentes:

1. Sensores de movimento: São dispositivos que detectam movimentos dentro de áreas específicas da casa. Quando um movimento é detectado, eles enviam um sinal para a central de monitoramento de alarme.

2. Sensores de abertura: São sensores colocados em portas e janelas para detectar quando são abertos ou violados. Eles também enviam sinais para a central de controle do alarme.

3. Teclado de controle: É um painel onde o proprietário pode ativar e desativar o sistema de alarme inserindo um código de segurança.

4. Sirene: É um dispositivo sonoro que emite um alarme alto quando ativado, com o objetivo de alertar os moradores e afastar possíveis intrusos.

5. Central de controle: É o cérebro do sistema de alarme, responsável por receber os sinais dos sensores e tomar as ações apropriadas. Pode ser programada para acionar uma sirene alta, enviar notificações para o proprietário e, em alguns casos, entrar em contato com uma empresa de monitoramento.

6. Empresa monitoramento residencial: Responsável por acompanhar os sinais enviados pelos alarmes instalados nas residências e tomar as medidas apropriadas

Além desses componentes básicos, os sistemas de alarme residenciais modernos podem incluir recursos adicionais, como câmeras de vigilância,

integração com celulares para controle remoto e notificações, detecção de fumaça, por exemplo.

Quais são os tipos de alarme residencial?

Existem vários tipos de alarmes residenciais disponíveis, cada um com características e funcionalidades distintas. Aqui estão alguns dos tipos mais comuns de alarmes residenciais:

1. Alarme residencial com fio: são conectados por fios aos sensores e à central de controle. Eles são conhecidos por sua confiabilidade, pois a comunicação é realizada através de conexões físicas.

2. Alarmes residenciais sem fio: utilizam tecnologia sem fio, como rádio frequência, para se comunicar entre os sensores e a central de controle. Eles são mais fáceis de instalar e não requerem a passagem de fios.

3. Alarme residencial com câmera: combinam recursos de detecção de intrusão com câmeras de segurança. Além de acionar os alarmes, eles também capturam imagens ou vídeos das atividades suspeitas, permitindo uma visualização remota em tempo real ou posteriormente.

4. Alarme residencial com sensor de presença interno: utiliza sensores de movimento instalados dentro da residência para detectar atividades suspeitas ou movimentos no interior do ambiente monitorado.

5. Alarme residencial com sensor de presença externo – utiliza um sensor de movimento específico para monitorar a área externa da residência. Os sensores de presença externos são projetados para detectar movimentos do lado de fora da casa, como no jardim, quintal, entrada ou perímetro da propriedade.

6. Alarmes com sensor de fumaça: Além da detecção de intrusão, eles também possuem sensores de fumaça integrados. Eles podem emitir um alarme sonoro e enviar notificações em caso de detecção de fumaça, permitindo uma resposta rápida a incêndios ou situações de emergência relacionadas a fogo.

Esses são apenas alguns exemplos dos tipos de alarmes residenciais disponíveis no mercado. Cada tipo possui suas vantagens e considerações específicas, e a escolha dependerá das necessidades de segurança da sua residência, do seu orçamento e das funcionalidades desejadas.

Como funciona alarme residencial?

O funcionamento de um alarme residencial pode variar dependendo do tipo específico de sistema que está sendo utilizado. No entanto, a seguir uma visão geral de como um alarme residencial funciona:

1. Detecção de intrusão: O alarme residencial é equipado com sensores de intrusão, como sensores de movimento, sensores de abertura de portas/janelas, sensores de quebra de vidro, entre outros. Esses sensores são responsáveis por monitorar a presença de atividades suspeitas na residência.

2. Sinalização para a central de alarme: Quando um sensor é acionado, ele envia um sinal para a central de alarme, que é o “cérebro” do sistema. Essa comunicação pode ser feita com fios, através de uma rede sem fio ou por meio de tecnologias como radiofrequência.

3. Avaliação da central de alarme: A central de alarme recebe os sinais dos sensores e avalia a situação com base nas configurações pré-programadas.

4. Ativação dos alarmes: Se a central de alarme avaliar que há uma intrusão ou uma violação de segurança, ela aciona os alarmes. Isso pode incluir sirenes sonoras, luzes e/ou notificações visuais em um painel de controle.

5. Notificação aos moradores: Além dos alarmes sonoros e visuais, alguns sistemas de alarme residencial podem enviar notificações aos moradores através de dispositivos móveis, telefones fixos ou por meio de um serviço de monitoramento profissional.

6. Desativação do alarme: Após a detecção de uma intrusão, o alarme residencial geralmente permite que os moradores desativem o sistema digitando um código de acesso em um teclado de controle ou através de um aplicativo móvel, caso o sistema possua essa funcionalidade.

7. Monitoramento profissional (opcional): Alguns sistemas de alarme residencial podem estar conectados a uma empresa de monitoramento residencial. Nesses casos, quando o alarme é ativado, a central de monitoramento residencial é notificada e toma medidas apropriadas, como entrar em contato com os moradores ou enviar ajuda de emergência.

É importante observar que as etapas e os recursos citados podem variar dependendo do sistema de alarme que está sendo utilizado.

Qual o melhor alarme residencial?

Não existe um único melhor alarme residencial no mercado, atualmente existem diversas marcas e modelos disponíveis no mercado, cada um com características e recursos diferentes. O que pode ser considerado o “melhor” alarme residencial para uma pessoa pode não ser o mesmo para outra.

A escolha do melhor alarme para uma residência depende de vários fatores como necessidade de segurança da residência, equipamento disponíveis no mercado, e condição financeiro do proprietário da residência.

Recomenda-se pesquisar várias opções, comparar recursos, preços e avaliações antes de tomar uma decisão. Além disso, sugiro que consulte um especialista em segurança residencial para obter recomendações personalizadas com base nas necessidades específicas da sua residência.

Como escolher o alarme mais adequado para minha residência?

Ao escolher o alarme mais adequado para a sua residência, é importante considerar alguns aspectos específicos para garantir a melhor proteção e

atender às suas necessidades de segurança. Aqui estão algumas etapas que você pode seguir para fazer uma escolha informada:

1. Avalie as necessidades de segurança da sua residência: comece fazendo uma avaliação de risco da sua residência. Isso ajudará a determinar os recursos e dispositivos necessários para atender as necessidades específicas de segurança da sua casa.

2. Defina um orçamento: Estabeleça um orçamento realista para o seu sistema de alarme residencial. Isso ajudará a limitar suas opções e garantir que você encontre uma solução que atenda às suas necessidades sem exceder suas possibilidades financeiras.

3. Pesquise diferentes marcas e modelos: Faça uma pesquisa detalhada sobre as marcas e modelos de alarmes residenciais disponíveis no mercado que atendam a sua necessidade de segurança.

4. Considere os recursos e funcionalidades: Avalie os recursos e funcionalidades oferecidos pelos diferentes sistemas de alarme. Escolha um sistema que ofereça os recursos que melhor se adequem às suas necessidades de segurança.

5. Pense na facilidade de uso e instalação: Verifique se o sistema de alarme é de fácil instalação e uso intuitivo. Alguns sistemas possuem interfaces amigáveis e oferecem configurações simplificadas, facilitando a operação e a personalização do sistema.

6. Considere a escalabilidade e a expansibilidade: Avalie se o sistema de alarme permite a expansão futura. Por exemplo, se você planeja adicionar mais dispositivos ou aumentar a cobertura da segurança em sua residência, certifique-se de que o sistema possa ser facilmente expandido.

7. Consulte um profissional especializado: Se possível, consulte um profissional especializado em segurança residencial. Eles podem fazer uma avaliação personalizada da sua residência e recomendar soluções de segurança adequadas às suas necessidades específicas.

Quais são os benefícios do alarme residencial?

O uso de um alarme residencial oferece uma série de benefícios significativos para a segurança e proteção da sua residência. Aqui estão alguns dos principais benefícios de usar um alarme residencial:

1. Reduz as possibilidades de perdas e danos em relação a residência e os bens e valores do seu interior.

2. Proporciona tranquilidade aos moradores, permitindo que se sintam seguros em sua própria residência.

3. Muitos sistemas de alarme residencial podem ser integrados a dispositivos inteligentes, como smartphones, tablets ou assistentes de voz. Isso permite que você monitore e controle seu sistema de segurança remotamente, recebendo notificações em tempo real e ajustando as configurações conforme necessário.

4. Descontos no seguro residencial: Ao instalar um alarme residencial, você pode reduzir os custos do seguro residencial e, ao mesmo tempo, aumentar a segurança da sua propriedade.

5. A presença de um sistema de alarme residencial pode aumentar o valor percebido da sua propriedade. Potenciais compradores ou inquilinos podem considerar um sistema de segurança como um benefício adicional ao avaliar a residência.

Conclusão

Ao longo deste artigo, exploramos os principais conceitos de alarme residencial e sua importância para proteção do seu lar e da sua família. Vimos os diferentes tipos de alarmes residenciais, como esses sistemas funcionam, os benefícios que oferecem e como escolher o mais adequado para suas necessidades específicas.

Ficou claro que investir em um sistema de alarme residencial vai além de simplesmente proteger seus bens materiais. É uma medida essencial para garantir a segurança de seus entes queridos e proporcionar uma sensação de tranquilidade em seu lar.

Os alarmes residenciais oferecem uma camada adicional de proteção, podendo detectar intrusões, incêndios, vazamentos de gás e outras ameaças potenciais, enquanto fornecem uma resposta rápida e eficiente.

Para aprofundar ainda mais seus conhecimentos nesse assunto e facilitar a sua escolha do alarme mais adequado para sua casa sugiro a leitura do meu artigo sobre segurança residencial. Nele, você encontrará mais informações, dicas e estratégias eficazes para garantir a segurança da sua residência.

José Sergio Marcondes, CES, CPSI - Gestor, Consultor e Diretor do IBRASEP. Profissional com competências sólidas na área de segurança privada e gestão empresarial.

Atividades de Segurança Privada: Conheça quais são e como contribuem para proteção da sociedade

José Sergio Marcondes, CES, CPSI

Saiba como as atividades de segurança privada desempenham um papel fundamental na preservação da ordem e proteção. Descubra suas áreas de atuação e benefícios.

As Atividades de Segurança Privada abrangem aquelas autorizadas pela Lei 7.103 para serem executadas por empresas privadas, que empregam profissionais devidamente capacitados para oferecer uma variedade de serviços de proteção a pessoas, áreas, estabelecimentos, numerários, bens e valores. Essas atividades se referem às diversas áreas de atuação dentro do campo da segurança privada.

A segurança privada evoluiu para áreas de atuações altamente especializadas, onde profissionais extremamente treinados e equipes dedicadas se unem para enfrentar desafios complexos. As Atividades de Segurança Privada desempenham um papel crucial na definição dos padrões da segurança privada, operando dentro de rigorosas normativas legais.

No cerne dessas atividades de segurança está o compromisso inabalável de assegurar a proteção, tranquilidade e ordem, onde a segurança é mais do que uma simples observação, é uma arte meticulosa de antecipar riscos, mitigar ameaças e preservar a incolumidade de pessoas, bens e valores.

Neste artigo, exploraremos o universo das atividades de segurança privada, desvendando as diversas áreas de atuação desse campo. Abordaremos a maneira pela qual essas atividades são conduzidas, as regulamentações que as orientam e o impacto que exercem em nossa vida cotidiana.

O que são as Atividades de Segurança Privada?

Atividades de Segurança Privada são aquelas autorizadas pela Lei 7.103 para serem executadas por empresas privadas, empregando profissionais devidamente capacitados para oferecer serviços de proteção a pessoas, áreas, estabelecimentos, numerários, bens e valores.

Essas atividades podem ser exercidas de forma armada ou desarmada, e abrangem diversos ambientes, como empresas, residências, condomínios, eventos e outros. Elas desempenham um papel fundamental na prevenção e repressão do crime, garantindo a segurança dos locais e das pessoas envolvidas.

As Atividades de Segurança Privada são regulamentadas pela Lei nº 7.102, de 20 de junho de 1983. Essa legislação estabelece os requisitos para o exercício das atividades de segurança privada e impõe sanções para quem a exerce sem a devida autorização.

A Polícia Federal desempenha um papel essencial como órgão regulador e fiscalizador, sendo responsável por disciplinar as atividades de segurança privada através de suas Portarias, além de regular a fiscalização dos planos de segurança dos estabelecimentos financeiros.

As áreas de atuação da segurança privada abrangem uma ampla gama de serviços voltados para proteção, prevenção e resposta a situações de risco. Essas atividades são executadas por empresas privadas devidamente autorizadas e por profissionais altamente capacitados.

Qual a Importância das Atividades de Segurança Privada?

As Atividades de Segurança Privada têm como principal objetivo garantir a proteção e segurança de pessoas, áreas, estabelecimentos, bens e valores. Isso proporciona um ambiente mais seguro para a população em geral, reduzindo a exposição a riscos e ameaças.

Essas atividades de segurança são consideradas atividades complementares às forças de segurança pública. Enquanto as forças de segurança pública têm a responsabilidade primária de manter a ordem, prevenir crimes e lidar com situações de emergência em âmbito público, as atividades de segurança privada atuam em parceria para reforçar esses esforços e oferecer uma camada adicional de proteção.

É importante destacar que as Atividades de Segurança Privada devem operar dentro dos limites da legislação e em colaboração com as forças de segurança pública. A parceria entre essas duas esferas contribui para a construção de uma sociedade mais segura e protegida, onde os esforços combinados ajudam a prevenir e combater a criminalidade e a responder eficazmente a situações de risco.

Quais são as Atividades de Segurança Privada?

As Atividades de Segurança Privada são diversas e abrangem diferentes áreas da segurança, para efeito legal, elas são agrupadas em 4 tipos:

1. Vigilância Patrimonial: Consiste na proteção de áreas e estabelecimentos públicos ou privados, com a finalidade de garantir a incolumidade física das pessoas e a integridade do patrimônio.

2. Transporte de Valores: Envolve o transporte seguro de numerário, bens e valores, realizado por meio de veículos especiais e profissionais capacitados para garantir a segurança durante o trajeto.

3. Segurança Pessoal: Oferece proteção e garantia da integridade física de pessoas específicas, geralmente indivíduos que necessitam de segurança pessoal devido a suas funções, cargos, status ou exposição a riscos.

4. Escolta Armada: Envolve o acompanhamento e proteção de cargas, valores ou pessoas durante o transporte, especialmente em situações de maior risco, utilizando equipes de profissionais habilitados.

5. Cursos de Formação: Os cursos de formação destinados à capacitação de profissionais de segurança privada, como vigilantes, que são obrigatórios para ingresso nessa área e são oferecidos por empresas especializadas devidamente autorizadas.

Como funciona a Atividade de Vigilância Patrimonial?

A atividade de vigilância patrimonial consiste em prover proteção a áreas e estabelecimentos urbanos ou rurais, sejam eles públicos ou privados, com o objetivo de garantir a integridade física das pessoas e a segurança do patrimônio.

As pessoas que desejam atuar nessa área devem passar por um Curso de Formação de Vigilante, ministrado por empresas autorizadas, que os prepara de forma específica para a atividade de vigilância patrimonial, fornecendo capacitação teórica e prática para um desempenho eficiente e profissional.

A vigilância patrimonial tem a importante responsabilidade de zelar pela segurança das pessoas que frequentam ou trabalham em um determinado local, assim como proteger os bens e o patrimônio da instituição contratante.

Dentre as funções desempenhadas pela vigilância patrimonial, destacam-se:

1. Rondas ostensivas de segurança;

2. Controle de acessos;

3. Atendimento de emergências.

A atuação da vigilância patrimonial é fundamental para garantir a tranquilidade e a proteção das pessoas e do patrimônio, seguindo sempre os princípios da legalidade, ética e profissionalismo. Com Vigilantes devidamente capacitados e tecnologias apropriadas, essa atividade contribui significativamente para a prevenção de incidentes e a segurança de diversos ambientes e estabelecimentos.

Como funciona a Atividade de Transporte de Valores?

A atividade de transporte de valores é uma das principais vertentes da segurança privada, que consiste em realizar o transporte seguro de numerário, bens ou objetos de valor. Essa atividade é de suma importância para assegurar que o transporte de dinheiro e itens valiosos ocorra de forma eficiente e protegida contra possíveis riscos, como assaltos ou roubos.

O transporte de valores é executado por meio de veículos especialmente projetados e equipados para garantir a segurança durante todo o percurso. Esses veículos (carro-forte) são robustos e contam com dispositivos de segurança, como cofres, trancas eletrônicas e sistemas de monitoramento.

Cada operação de transporte de valores é acompanhada por uma equipe de vigilantes especialmente treinados para essa atividade. Esses Vigilantes

possuem a responsabilidade de assegurar a proteção do numerário e dos objetos de valor durante todo o trajeto.

Antes do início do transporte, é realizado um planejamento detalhado, levando em consideração a segurança das rotas, possíveis pontos de risco e a logística envolvida. Para elevar ainda mais a segurança do transporte, é comum que as empresas adotem estratégias como a utilização de rotas e horários aleatórios, dificultando a previsibilidade e minimizando a exposição excessiva.

A atividade de transporte de valores é de extrema importância para garantir a segurança das instituições financeiras, empresas e estabelecimentos que lidam com grandes volumes de dinheiro ou objetos de valor.

Como funciona a Atividade de Segurança Pessoal?

A atividade de segurança pessoal tem como objetivo prover proteção e garantir a integridade física de pessoas específicas, frequentemente indivíduos que necessitam de segurança devido a suas funções, cargos, status ou exposição a riscos. Essa é uma das vertentes mais especializadas da segurança privada e requer Vigilantes altamente capacitados e treinados para assegurar a segurança de seus clientes.

Antes de iniciar os serviços de segurança pessoal, é realizada uma análise minuciosa dos riscos enfrentados pelo cliente. Essa avaliação leva em consideração fatores como o perfil do cliente, suas atividades diárias e a exposição a possíveis ameaças, dentre outros aspectos relevantes.

Com base na avaliação de riscos, é elaborado um plano de segurança personalizado para atender às necessidades específicas do cliente. Esse planejamento inclui estratégias para evitar situações de risco, medidas preventivas, definição de rotas seguras e procedimentos a serem seguidos em caso de emergência.

A segurança pessoal é executada por uma equipe de profissionais altamente treinados e especializados em proteção pessoal. Essa equipe pode é composta por vigilantes especialmente habilitados para essa atividade.

A atividade de segurança pessoal é de suma importância para garantir a integridade física de indivíduos que enfrentam riscos em função de suas atividades profissionais, públicas ou pessoais. A atuação desses profissionais deve ser pautada na eficiência, discrição e capacidade de reação, buscando sempre a proteção e o bem-estar do cliente.

Como funciona a Atividade de Escolta Armada?

A atividade de escolta armada é uma das modalidades da segurança privada que consiste no acompanhamento e proteção de cargas e valores durante o transporte. Seu foco é garantir a segurança e integridade dos itens transportados, especialmente em situações de maior risco.

Essa atividade é realizada por empresas especializadas, contando com profissionais devidamente treinados e habilitados para essa função. Esses profissionais são armados e capacitados para reagir a possíveis situações de risco durante o transporte.

A equipe de escolta armada acompanha o transporte da carga ou dos valores desde o local de origem até o destino final. Durante o trajeto, os vigilantes estão atentos a possíveis ameaças e atuam para prevenir ou neutralizar qualquer tentativa de assalto ou roubo.

Antes de iniciar o transporte, é realizado um planejamento detalhado das rotas a serem seguidas, levando em consideração a segurança e eficiência do trajeto. As rotas podem ser variadas para evitar a previsibilidade e reduzir os riscos.

A atividade de Escolta Armada é fundamental para assegurar o transporte seguro de cargas e valores de alto risco. Os vigilantes que atuam nessa atividade devem possuir treinamento especializado, agindo com responsabilidade, eficiência e prontidão para enfrentar possíveis ameaças e garantir o sucesso da missão de proteção.

Como funciona a Atividade de Curso de Formação?

Os cursos de formação são ministrados por escolas de formação e destinados à capacitação dos profissionais de segurança privada, condição obrigatória para ingresso nessa área. A formação profissional é uma etapa essencial na segurança privada, visa capacitar os profissionais para atuarem de forma adequada e responsável em suas respectivas funções.

Para oferecer esses cursos, as empresas devem obter autorização prévia da Polícia Federal e serem credenciadas para ministrarem os treinamentos. Essa autorização é concedida somente após o cumprimento de requisitos específicos, o que garante que a empresa possui as condições adequadas para fornecer o treinamento de forma competente e responsável.

Além disso, é imprescindível que as empresas de curso de formação disponham de infraestrutura adequada para ministrar as aulas. Isso inclui a disponibilidade de salas de aula bem estruturadas, espaços apropriados para práticas de tiro, e instrutores devidamente capacitados e experientes e credenciados na Policia Federal.

Os cursos de formação exercem um papel fundamental para assegurar que os profissionais da segurança privada possuam o conhecimento e as competências necessárias para atuarem de maneira ética, responsável e eficiente, com foco constante na segurança e proteção dos clientes e do patrimônio.

A capacitação oferecida durante o curso contribui para o aprimoramento da segurança privada como um todo e para o cumprimento das diretrizes estabelecidas pela legislação, garantindo um serviço de qualidade e profissionalismo na área de segurança.

Principais Benefícios das Atividades de Segurança Privada

As Atividades de Segurança Privada oferecem uma série de benefícios para a sociedade, empresas e indivíduos. Esses serviços são projetados para complementar as ações de segurança pública, proporcionando uma proteção adicional e contribuindo para um ambiente mais seguro.

Abaixo estão alguns dos principais benefícios das atividades de segurança privada:

1. Proteção e Segurança: Os vigilantes trabalham para prevenir e responder a incidentes de segurança, reduzindo riscos e protegendo tanto pessoas como propriedades.

2. Prevenção de Crimes: A simples presença dos vigilantes e a realização de patrulhas em áreas sensíveis podem inibir a ocorrência de crimes, como roubos, furtos e invasões.

3. Rapidez na Resposta: Em situações de emergência, os serviços de segurança privada podem responder rapidamente, notificar as autoridades competentes e agir de forma coordenada para mitigar os danos e reduzir os impactos negativos.

4. Tranquilidade para Empresas e Clientes: Empresas que contratam serviços de vigilância patrimonial podem oferecer um ambiente mais seguro e protegido para seus funcionários, clientes e visitantes, gerando maior confiança e tranquilidade.

5. Atenção Personalizada: A segurança pessoal fornece uma atenção direcionada e proteção especializada para indivíduos como executivos, celebridades ou pessoas sob ameaças potenciais.

6. Redução de Perdas Financeiras: O transporte de valores e a escolta armada contribuem para a redução de perdas financeiras causadas por roubos e furtos, especialmente em estabelecimentos financeiros e nas rodovias.

7. Suporte em Eventos e Situações Especiais: As atividades de segurança privada também são essenciais para fornecer suporte em eventos especiais, como shows, eventos esportivos e feiras, garantindo a segurança dos participantes e do público.

É importante destacar que os benefícios das atividades de segurança privada estão intimamente ligados à qualidade, eficiência e conformidade com as regulamentações e normas vigentes. Quando realizadas por empresas e profissionais confiáveis, essas atividades podem ter um impacto positivo significativo na proteção da sociedade, do patrimônio e dos indivíduos.

Conclusão

Em um mundo em constante evolução, as Atividades de Segurança Privada desempenham um papel fundamental. Ao abranger uma ampla área de atuação, essas atividades se estabeleceram como uma peça crucial no quebra-cabeça da segurança moderna. Desde a vigilância patrimonial até o transporte de valores,

elas oferecem um suporte valioso para garantir a tranquilidade de indivíduos e organizações.

À medida que exploramos as diversas áreas de atuação da segurança privada, fica evidente que essas atividades não apenas complementam, mas também colaboram ativamente com as forças de segurança pública. Juntas, elas formam um sistema interligado de proteção, trabalhando em harmonia para enfrentar os desafios complexos que a nossa sociedade enfrenta atualmente.

No entanto, essa é apenas uma visão geral do vasto mundo da segurança privada. Se você deseja aprofundar ainda mais nesse assunto, sugiro a leitura do meu artigo sobre as Empresas Especializadas em Segurança Privada. Nele, exploraremos o papel vital que essas empresas desempenham na garantia da segurança e como suas práticas especializadas contribuem para moldar um ambiente mais seguro e protegido para todos.

José Sergio Marcondes, CES, CPSI - Gestor, Consultor e Diretor do IBRASEP. Profissional com competências sólidas na área de segurança privada e gestão empresarial.

Benefícios da Gestão de Riscos para a estratégia do seu Negócio

Marcos Alves Junior, CIEIE, CIGR, CPSI

A gestão de riscos é uma abordagem essencial para garantir o sucesso e a sustentabilidade das empresas em um ambiente cada vez mais complexo e competitivo. O processo inclui a identificação, análise, avaliação e mitigação dos riscos que podem afetar o cumprimento dos objetivos organizacionais. Ao adotar uma cultura de gestão de riscos, as empresas podem obter diversos benefícios significativos que impactam positivamente sua performance e longevidade.

1. Tomada de decisão mais informada: a gestão de riscos proporciona uma visão clara dos desafios e oportunidades enfrentados pela empresa, permitindo que os gestores tomem decisões mais fundamentadas. Ao entender os riscos potenciais associados a uma determinada estratégia, os líderes podem ajustá-la ou optar por alternativas mais adequadas.

2. Prevenção de perdas financeiras: ao identificar e gerenciar proativamente os riscos financeiros, como flutuações cambiais, taxas de juros ou volatilidade do mercado, a empresa está mais preparada para evitar perdas financeiras significativas e garantir sua estabilidade econômica.

3. Resiliência em tempos de crise: a gestão de riscos prepara a empresa para enfrentar situações de crise, sejam elas econômicas, desastres naturais, pandemias ou outros eventos inesperados. As empresas com uma estrutura sólida de gestão de riscos estão mais bem equipadas para resistir a adversidades e se recuperar rapidamente.

4. Fortalecimento da reputação da empresa: a percepção dos stakeholders sobre uma empresa é crucial para sua imagem e reputação. A gestão de riscos ajuda a garantir a conformidade com as regulamentações, ética nos negócios e a proteção do meio ambiente, o que contribui para uma imagem mais positiva no mercado.

5. Otimização de recursos: a identificação de riscos potenciais permite que a empresa aloque seus recursos de forma mais eficiente, focando nas áreas de maior impacto e minimizando o desperdício. Isso resulta em uma alocação mais eficaz dos investimentos e maior produtividade operacional.

6. Cumprimento de normas e regulamentações: a gestão de riscos auxilia as empresas a atender às normas e regulamentações governamentais e do setor em que atuam. Isso reduz o risco de penalidades e sanções, além de garantir um ambiente de negócios mais seguro e ético.

7. Estímulo à inovação: a gestão de riscos não se limita à identificação de riscos negativos. Ela também incentiva a busca por oportunidades e riscos positivos que possam ser explorados estrategicamente, fomentando a inovação e o crescimento sustentável.

Resumidamente, a gestão de riscos é um elemento crítico para a saúde e o sucesso das empresas. Ela oferece uma abordagem proativa para lidar com incertezas e desafios, fortalecendo a resiliência e a capacidade de adaptação das organizações em um mundo em constante mudança. Ao incorporar a gestão de riscos em sua cultura organizacional, as empresas podem melhorar sua tomada de decisão, proteger seus ativos, construir uma reputação sólida e promover um crescimento sustentável.

A maneira mais correta de implementação da cultura de gestão de riscos, é através de uma metodologia eficaz alinhada a uma ferramenta teológica que ajude sua organização a otimizar esses processos de forma automatizada, evitando as falhas que poderiam ser cometidas através de uma análise feita em planilhas de Excel. Por meio do Software INTERISK o processo de gestão de riscos trabalha de maneira interconectada, trazendo uma visão mais ampla dos riscos e seus impactos. Veja como o INTERISK atua nos processos da 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.

Cenários de Gestão de Riscos Cibernéticos que sua organização deve mapear

Mariana da Silveira, DIDS, MBCR, CPSI, CEGRC, CIGR, CISI, CIEIE, DPO, ISO

A Gestão de Riscos Cibernéticos deve ser constantemente monitorada e revisada, em um processo de melhoria contínua. Os atacantes cibernéticos possuem motivações e técnicas próprias e atuam de diversas maneiras. As formas mais comuns de atuação são apresentadas a seguir.

- Crackers: são hackers que se envolvem em atividades ilegais, como invasão de sistemas ou distribuição de software pirateado ou adulterado. Hackers éticos: diferentemente dos hackers maliciosos, esses profissionais de segurança cibernética utilizam suas habilidades para ajudar empresas e organizações a identificar vulnerabilidades, testar a segurança dos sistemas e propor melhorias.
- Engenheiros sociais: não utilizam necessariamente conhecimentos técnicos avançados, mas sim técnicas de manipulação psicológica para obter informações confidenciais. Eles podem se passar por outras pessoas, criar e-mails falsos e convincentes, links maliciosos ou realizar ligações telefônicas fraudulentas a fim de enganar e obter vantagens de suas vítimas.
- Grupos de crime organizado: esses grupos estão envolvidos em atividades criminosas que também incluem ataques cibernéticos. Podem se especializar em roubo de dados, extorsão, tráfico de informações ou cibercrimes mais complexos.
- Infiltradores internos: esses são indivíduos com acesso privilegiado a sistemas e redes por meio de suas posições dentro de uma organização. Seja por motivos pessoais ou financeiros, eles podem realizar sabotagens, roubo de informações, vazamento de dados ou outros tipos de ataques.

Ponto importante a ressaltar é que essas categorias não são mutuamente exclusivas e que muitas vezes as motivações e técnicas dos atacantes cibernéticos se sobrepõem. A segurança cibernética é um desafio em constante evolução. É fundamental, portanto, que a organização esteja atenta às ameaças, adote medidas técnicas, físicas e administrativas adequadas a fim de mitigar os riscos cibernéticos aos quais está suscetível.

Os atacantes cibernéticos têm diversas motivações, métodos e alvos. Suas motivações podem variar amplamente, desde ganhos financeiros, espionagem industrial, ativismo político até o simples prazer de causar danos. Em relação aos métodos, eles exploram vulnerabilidades em sistemas e redes de computadores para comprometer a segurança e obter acesso não autorizado a informações sensíveis.

Tais ameaças podem se concretizar por meio de ataques de phishing, ransomware, ataque de negação de serviço, vazamento de dados, ataques à Internet das Coisas (IoT), ataque de envenenamento da tabela ARP, ataques de injeção de código no BIOS, ataque de transmissão de pulso eletromagnético (EMP), ataque de air-gap, como sinais de rádio, ondas sonoras ou até mesmo dispositivos USB, para comprometer o sistema, ou ataque por ultrassom.

Para combater essas ameaças, é fundamental ter uma abordagem de segurança cibernética abrangente, incluindo medidas de prevenção, identificação, detecção e resposta a incidentes. Manter sistemas atualizados, implementar firewalls, antivírus e outras soluções de segurança, além de educar os usuários sobre as melhores práticas de segurança online, são medidas importantes para reduzir o risco de ataques cibernéticos.

Destarte, para uma Gestão de Riscos Cibernéticos efetiva, é necessário identificar os cenários que podem se apresentar para a organização. Sendo assim, a abordagem e as medidas a serem tomadas são determinadas de acordo com os cenários concretizados:

- Mercenário: refere-se a atividades maliciosas realizadas por indivíduos ou grupos, violando sistemas de computadores, redes ou dispositivos para obter informações confidenciais, causar danos ou interromper operações normais, com a finalidade de extorquir e cobrar resgate.
- Hacktivista: são indivíduos ou grupos que invadem sistemas com o objetivo de promover uma causa (política, social, ambiental). É comum a realização de ataques de negação de serviço (DDoS) em sites ou o vazamento de informações sensíveis.
- Sequestrador: O sequestro cibernético, também conhecido como ransomware, é um tipo de ataque cibernético em que os invasores bloqueiam o acesso a sistemas, arquivos ou dispositivos digitais e exigem um resgate para restabelecer o acesso. Os sequestros cibernéticos são geralmente realizados por meio de um malware que criptografa os arquivos da vítima, tornando-os inacessíveis.
- Hackers Internos: são funcionários de uma organização que, por vários motivos, decidem comprometer os sistemas internos. Eles podem roubar informações confidenciais, sabotar operações ou causar danos à infraestrutura.
- Script Kiddies: são indivíduos com habilidades técnicas básicas que usam ferramentas e scripts disponíveis na Internet para realizar ataques simples. Eles geralmente não têm motivação específica além de ganhar notoriedade na internet.
- Terrorista Cibernético: indivíduo ou grupo que utiliza ataques cibernéticos como parte de uma estratégia terrorista. Procura causar danos a infraestruturas críticas, sistemas governamentais ou afetar a confiança pública.

Diante de tais cenários, a organização deve recorrer às medidas técnicas, administrativas e físicas adequadas. A Brasiliano INTERISK possui um time altamente qualificado e experiente, pronto a oferecer consultoria em segurança

cibernética e o software INTERISK, propiciando a gestão de riscos cibernéticos que pode ser a solução ideal para a sua organização. Quer conhecer nossos produtos e serviços? Agende uma apresentação.

Mariana da Silveira, DIDS, MBCR, CPSI, CEGRC, CIGR, CISI, CIEIE, DPO, ISO

Especialista de Segurança da Informação, Privacidade e Proteção de Dados Pessoais

CEO da RUT Information Security Audit

Certificação Profissional: O que significa, qual sua importância e benefícios para os profissionais

Descubra como a Certificação Profissional valida seus conhecimentos e habilidades, e como ela pode ser um diferencia importante para sua carreira profissional.

José Sergio Marcondes, CES, CPSI

No mundo profissional altamente competitivo de hoje, é essencial encontrar maneiras de se destacar e avançar em sua carreira. Uma das maneiras mais eficazes de alcançar esse impulso é através da obtenção da Certificação Profissional.

As certificações não apenas validam suas habilidades e conhecimentos em uma área específica, mas também abrem portas para oportunidades promissoras e oferecem uma vantagem competitiva no mercado de trabalho.

Cada vez mais os empregadores estão em busca de profissionais qualificados e experientes que possam agregar valor às suas equipes e organizações. Nesse contexto, a obtenção de uma Certificação Profissional pode ser uma estratégia eficaz para se destacar no mercado de trabalho e abrir portas para novas oportunidades.

Neste artigo, exploraremos a importância das certificações profissionais e como elas podem impulsionar o crescimento em sua carreira, e aumentar sua credibilidade profissional, e como podem abrir portas para novas oportunidades.

O que é uma Certificação Profissional?

Uma Certificação Profissional é um reconhecimento oficial de que um indivíduo possui habilidades e conhecimentos específicos em um determinado campo de atuação. Geralmente, as certificações são concedidas por instituições especializadas e reconhecidas na sociedade, e são projetadas para validar as competências técnicas e práticas necessárias para exercer uma profissão ou ocupação específica.

A Certificação Profissional demonstra que um profissional possui um conjunto de competências específicas, o que pode aumentar sua credibilidade numa determinada área. Além disso, as certificações podem ajudar os profissionais a se manterem atualizados em suas áreas de atuação, uma vez que muitas delas exigem a conclusão de cursos de atualização e a recertificação periódica.

As áreas em que as certificações profissionais são comumente encontradas são diversas, incluindo tecnologia da informação, finanças, saúde, gerenciamento de projetos, recursos humanos, marketing, segurança privada, entre outras. Cada campo pode ter suas próprias certificações reconhecidas e requisitos específicos para obtê-las.

Qual a diferença entre certificação e certificado?

É importante destacar que as certificações profissionais são diferentes dos certificados e diplomas de conclusão de cursos acadêmicos, como graduação, pós-graduação e outros cursos.

Enquanto os diplomas de conclusão de cursos atestam a conclusão de um programa de estudos em uma instituição educacional, as certificações profissionais focam em habilidades e conhecimentos específicos para o exercício de uma profissão ou ocupação.

A diferença entre certificação e certificado está relacionada ao propósito e ao alcance de cada um. A seguir as distinções entre os dois conceitos:

Certificação:

Uma certificação é um processo formal no qual uma instituição, reconhecida na sociedade, avalia e valida as competências (conhecimentos e habilidades) de um indivíduo em um determinado campo de atuação. A certificação geralmente envolve a conclusão de requisitos específicos, como exames teóricos e práticos, experiência profissional ou educação formal.

O objetivo da certificação é atestar a proficiência do indivíduo em um campo de atuação específico e é geralmente concedida por organizações profissionais, associações ou instituições regulatórias.

As certificações são frequentemente voltadas para áreas profissionais específicas e podem exigir uma manutenção regular, como a recertificação periódica, para garantir que os profissionais certificados estejam atualizados com as últimas práticas e conhecimentos da área.

Certificado:

Um certificado, por outro lado, é um documento emitido para atestar a conclusão bem-sucedida de um curso, programa de estudos ou treinamento específico.

Os certificados são concedidos por instituições educacionais, como escolas, universidades, provedores de treinamento ou empresas. Eles comprovam que o indivíduo participou e completou um determinado curso ou programa de estudos, mas não necessariamente garantem um nível de proficiência em uma área específica.

Os certificados podem abranger uma ampla variedade de áreas, desde cursos profissionalizantes, workshops e treinamentos até programas de desenvolvimento pessoal e habilidades técnicas.

Para que serve a Certificação Profissional?

A certificação profissional é uma credencial que atesta que um indivíduo possui um conjunto específico de competências (conhecimentos e habilidades) em uma determinada área de atuação, é utilizada para validar e reconhecer

competências profissionais numa determinada área. Ela é concedida por organizações ou instituições especializadas e reconhecidas, como associações profissionais, institutos de certificação ou órgãos reguladores.

Exemplos de Certificação Profissional

1. **Certificação Project Management Professional (PMP)**: é reconhecida globalmente e valida as habilidades em gerenciamento de projetos. Ela demonstra a capacidade de liderar equipes, planejar, executar e entregar projetos de forma eficiente e eficaz.
2. **SHRM-CP** – Voltada para profissionais de média gerência de RH
3. **CISSP – Certified Information Systems Security Professional**: voltada para profissionais que atuam na segurança da tecnologia da informação.
4. **CPSI – Certificado Profesional en Seguridad Internacional** – é uma certificação especializada no campo da segurança. Essa certificação é destinada a profissionais que desejam ter validados seus conhecimentos e habilidades na proteção e gestão de riscos em contextos globais e na área de segurança internacional.

Quais os benefícios de um Certificação Profissional?

Uma certificação profissional serve para diversas finalidades e pode trazer vários benefícios para os profissionais. A seguir algumas das principais razões pelas quais as certificações profissionais são importantes:

1. **Reconhecimento de habilidades**: Uma Certificação Profissional valida as competências (conhecimentos e habilidades) adquiridas em um determinado campo de atuação. Ela demonstra que o profissional possui um conjunto de competências específicas e atende aos padrões estabelecidos pelo mercado de trabalho para aquela atividade.
2. **Credibilidade e confiança**: Ao obter uma Certificação Profissional, o indivíduo ganha credibilidade e confiança dos empregadores, clientes e colegas de trabalho. A certificação mostra que o profissional está comprometido com o aprimoramento de suas habilidades e práticas, tornando-o mais confiável e respeitado no mercado de trabalho.
3. **Vantagem competitiva**: No mercado de trabalho competitivo, as certificações podem fornecer uma vantagem significativa. Elas podem diferenciar um profissional dos concorrentes, aumentando suas chances de obter empregos, promoções e oportunidades de carreira.
4. **Desenvolvimento profissional contínuo**: Muitas certificações profissionais requerem que os profissionais participem de programas de atualização e recertifiquem-se periodicamente. Isso incentiva o desenvolvimento profissional contínuo e a atualização de habilidades, mantendo-os atualizados com as tendências e avanços em sua área de atuação.

5. **Acesso a redes profissionais**: Ao obter uma certificação, os profissionais geralmente se tornam parte de uma comunidade ou associação profissional. Isso proporciona oportunidades de networking, conexões com outros profissionais da área e acesso a recursos exclusivos, como eventos, fóruns e materiais de estudo.
6. **Melhores oportunidades de emprego e remuneração**: As certificações profissionais podem abrir portas para melhores oportunidades de emprego. Muitas vezes, as empresas procuram profissionais certificados para preencher cargos específicos. Além disso, as certificações também podem estar associadas a salários mais altos e benefícios adicionais.

No entanto, é importante lembrar que as certificações profissionais não são uma garantia automática de emprego ou sucesso na carreira. Elas são complementares à experiência e outras qualificações, e os profissionais devem continuar investindo em seu crescimento e desenvolvimento profissional de maneiras abrangentes.

Conclusão

Ao longo deste artigo, exploramos a importância e os benefícios da Certificação Profissional. Vimos que as certificações podem proporcionar uma vantagem competitiva no mercado de trabalho, validando habilidades e conhecimentos específicos em uma área de atuação. Elas são um meio de comprovar sua expertise, aumentar a credibilidade e abrir portas para melhores oportunidades de carreira.

Investir em certificações profissionais é essencial para o crescimento profissional contínuo. Elas permitem que você se mantenha atualizado com as melhores práticas, desenvolva habilidades relevantes e esteja em sintonia com as demandas do mercado. Além disso, as certificações podem impulsionar sua confiança e autoestima, fornecendo um senso de conquista e reconhecimento.

Como profissional em busca de excelência, não deixe de considerar as certificações relevantes para sua área de atuação. Pesquise as certificações reconhecidas e respeitadas, avalie seus requisitos e benefícios, e planeje estrategicamente sua jornada de certificação.

José Sérgio Marcondes, CES, CPSI - Especialista em Segurança Empresarial - Consultor em Segurança Privada - Diretor do IBRASEP

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

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

Que segurança deve ter um hotel?

Um hotel ou centro turístico necessita de vários sistemas de gestão de segurança abrangentes, como controle de acessos, automação, CCTV, proteção contra incêndios, alarmes, sistemas de estacionamento etc.
O conceito de segurança em Hotéis engloba um leque de atividades cujo objetivo final é a integridade, primeiro das pessoas e depois das instalações. Ao conceber um projeto de segurança integral em um hotel, é essencial fazer um compromisso entre os dois aspectos materiais e pessoais.

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

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

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

A partir do confronto entre optar por uma mudança ou manter-se apegado a esquemas antigos, surgirá uma nova cultura na empresa. A mudança proposta de acordo com uma visão sistêmica não deve ser gerada verticalmente (topo da pirâmide para a base operacional), mas sim, a mudança deve ser operada e assumida em todas as áreas da empresa e todos os seus membros devem cooperar. Exemplo: a recepção do hotel geralmente está mais em contato com o hospede do que o Gerente Geral, para quem o hóspede faz comentários, reclamações.

É necessário criar a consciência da empresa como um todo, vista como um sistema, onde todas as pessoas devem contribuir para eliminar as falhas que podem surgir. A pessoa que recebe a reclamação deve informar ao setor correspondente de tal forma que, no menor tempo possível, o problema seja

resolvido. Esta concepção da empresa como sistema, onde todos seus setores estão vinculados e cada área está capacitada para cumprir sua função, com um satisfatório grau de comunicação entre eles, é o que forma as bases para materializar o objetivo proposto, isto é: CONHECER O HOSPEDE E FIDELIZÁ-LO.

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

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

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

Se na área da segurança não forem implementadas medidas de controle para reduzir os riscos, quem corre o risco não será somente o hóspede, mas também o hotel, e o risco pode ser alto.

Para reforçar a segurança, alguém (ou todos), em algum momento deve ter que denunciar algo ou dizer não. Isso pode ser difícil, especialmente se for percebido que o colega de trabalho poderá ficar ressentido. Agora, se as mudanças forem implementadas corretamente, o funcionário deve saber que se ele denunciar a reclamação, por exemplo, para a área de manutenção, isso não causará a demissão de um funcionário.

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

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

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

caso a mudança se torna anárquica, mas uma vontade de ouvir as necessidades do hóspede no momento certo.

Cada funcionário deve ter conhecimento claro de qual é o seu papel, seu espaço dentro da empresa e sua função. Afirmar que a opinião de todos é necessária para gerenciar uma mudança de paradigma não implica ignorar que as decisões são feitas apenas por alguns. A decisão nunca é da ordem da horizontalidade, alguém deve assumi-la e torná-la concreta.
Aquele que toma a decisão de uma mudança, orientada para implementar uma política de segurança, deve ter a capacidade de liderar o caminho, e isso não significa apenas comando. Toda empresa deve estar ciente de seus pontos fortes e fracos, reforçar o primeiro e eliminar ou reduzir o último.

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

CONCLUSÃO

Um hotel tem muitas peculiaridades, não só pelo grande número de usuários que nela convergem durante as 24 horas do dia, contando convidados e diferentes funcionários contratados por um curto período, mas também para o número de portas, escadas e corredores existentes. Por esta razão, a segurança em hotéis é um princípio fundamental para alcançar a satisfação do cliente, objetivo principal de qualquer estabelecimento turístico, e para os funcionários realizarem seu trabalho de forma eficaz e eficiente.

Dr. Renato Santos Figueiredo, CPSI, CISI, CIGR, CIEIE, CEGRC, CIPSI, CISI, CIEAC, MBS, DIDS.
Presidente CEAS-BRASIL / CEAS ANGOLA e Secretário Geral CEAS-INTERNACIONAL, capítulos CEAS-BRASIL/CEAS- ANGOLA/MERCOSUL E PAÍSES ASSOCIADOS.

Entenda o porquê a Governança Corporativa é tão importante nas organizações

Marcos Alves Junior, CIEIE, CIGR, CPSI

Recentemente ocorreu o que consideramos o maior descaso com a Governança Corporativa de todos os tempos, envolvendo a Americanas, quinta maior empresa varejista do Brasil. Resumidamente, esse escândalo teve início no dia 11 de janeiro. Naquela data, a empresa anunciou irregularidades no seu balanço. Cinco meses depois, a varejista admitiu fraude nas contas e desde então os prejuízos financeiros somam cerca de 43 bilhões de reais.

Dito isso, fica claro que após esse escândalo com o prejuízo bilionário iremos frisar a importância da Governança Corporativa nas organizações.

A palavra Governança vem do vocabulário grego, e seu significado trata do ato de governar. Especificamente, a governança corporativa diz respeito a controlar e/ou dirigir uma companhia; é uma estrutura com regras e processos de gerenciamento e monitoramento que regem a organização, para que ela alcance suas metas e objetivos.

É de conhecimento de todos que as decisões que uma organização toma não se baseiam na concepção de uma única pessoa, ou seja, cada decisão é tomada a partir da concordância de um grupo de pessoas envolvidas no processo que está sendo discutido.

A Gestão de Riscos da organização é uma grande aliada neste processo e sugere que haja a distribuição de responsabilidades e liberdade de opinião de todos os colaboradores envolvidos.

De acordo com o IBGC (Instituto Brasileiro de Governança Corporativa), os princípios fundamentais da governança corporativa são: Transparência, Prestação de contas, Equidade e Responsabilidade Corporativa.

O objetivo da Governança Corporativa é a criação de um sistema de gestão transparente e inclusivo a todos os colaboradores envolvidos, bem como a outras partes interessadas. É importante ressaltar que não é um processo que irá criar mais burocracia para as empresas, pois tem como propósito ajudar a aperfeiçoar seus processos de administração, para que eles se tornem mais objetivos e imparciais.

Ou seja, o motivo para a governança ser tão importante é ser ela um conjunto de normas e boas condutas que auxiliam na direção e nas decisões dentro da organização, ajudando diretamente na transparência das ações.

Dessa forma, um dos principais benefícios para a organização é a prevenção contra possíveis fraudes, pois as normas motivam os agentes dos processos a serem mais conscientes.

Uma vez que sua organização esteja pronta para desencadear este processo, é importante tentar otimizar uma boa alternativa. Nesse ponto, ganham importância as soluções de TI, desde que sejam compatíveis com os processos que já existem na sua organização, pois isso facilitará em muito a vida dos envolvidos no trabalho. O Software INTERISK, por exemplo, é uma solução integrada que tem como objetivo estimular o aculturamento da Gestão de Riscos, Governança e Compliance nas organizações, incorporando automação e praticidade.

Diferentemente da grande maioria das ferramentas de gerenciamento de riscos, governança e compliance, o Software INTERISK não cobra licenças em função do número de usuários, ou seja, não importa o número de colaboradores que irão utilizar a solução, o custo da licença será sempre o mesmo.

Se você tem alguma dúvida sobre outros diferenciais do Software INTERISK e até mesmo sobre a otimização de processos que ele pode proporcionar a sua organização, acesse aqui e solicite uma demonstração com um de nossos especialistas.

#gestãoderiscos #metodologia #processos #otimizacao #tecnologia #ti #so ftware #governaça #integração #compliance #riscos #inteligenciaemriscos #inovação #governança #agilidade #solução #softwareinterisk #news

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. Atualmente trabalha como Assistente de Comunicação e Marketing na Brasiliano INTERISK.

ESG e Risco de Reputação. Como Prevenir ou Mitigar?

Décio Luís Schons, CIEAI, CEGRC, CIGR, CISI

Introdução

A reputação ou “o bom nome da empresa” constitui um dos ativos mais valiosos de qualquer organização. Em outras palavras, a manutenção de uma percepção positiva da empresa e de seu papel na sociedade por parte dos stakeholders (partes interessadas) ocupa um ponto muito elevado na escala de prioridades a serem tomadas em consideração pela Alta Gestão empresarial.

Antes de prosseguirmos, será de todo interessante estabelecer a diferença entre os conceitos de reputação e de imagem, muitas vezes tomados um pelo outro.

Imagem é como uma foto, um instantâneo da empresa. A divulgação de uma imagem negativa da organização pode frequentemente ser ultrapassada mediante o emprego de ações rápidas e eficazes de contenção de danos, mediante planos de mitigação.

Já a reputação é algo construído ao longo do tempo, muitas vezes através de gerações.

É intuitivo que a ocorrência de sucessivos incidentes de danos à imagem acabará por afetar de forma decisiva a reputação corporativa.

Os riscos (sempre eles...) e o estrago que provocam

Dessa forma, o Risco de Reputação (ou Risco Reputacional) constitui um dos escolhos mais graves com que as organizações se deparam em nossos dias. Seu impacto pode levar à falência ou à extinção da empresa. Por tal motivo, o tratamento dessa categoria de riscos requer especial atenção da parte dos gestores.

Sabemos que o Risco de Reputação constitui geralmente uma consequência da materialização de outros riscos. Dentre estes, ocupam posição de destaque os Riscos ESG.

Uma providência seminal para a não materialização dos riscos reputacionais é justamente evitar as chances de que os Riscos ESG, em seu devido tempo, se materializem. Ganha importância aí o estabelecimento de controles eficazes sobre as fontes de risco, de maneira a reduzir significativamente as probabilidades de ocorrência dos Riscos ESG.

Riscos ESG comuns, como a liberação de efluentes sólidos, líquidos ou gasosos, estão entre aqueles que geram as mais daninhas consequências para a imagem e a reputação da organização. A mortandade de peixes em um rio, causada por efluentes atribuídos a determinada empresa; a percepção da poluição

atmosférica por gases emitidos pela empresa e consequente degradação das condições de habitabilidade de locais antes caracterizados pela pureza do ar; a notícia de que a organização conta em sua cadeia de fornecedores com empresas que se valem de mão de obra escrava – são exemplos de eventos que afetam de imediato a imagem e, em médio prazo, irão comprometer a reputação da empresa.

É melhor prevenir que remediar

A correta gestão dos Riscos ESG exige o estabelecimento, por parte do negócio em tela, de uma governança corporativa desses riscos, mediante o trabalho de pessoas dotadas de conhecimento sobre o tema e de liberdade de ação para assessorar corretamente a Alta Gestão com relação às medidas a adotar.

Nessa área crucial da Governança Corporativa, ganham realce, dentre outras, as atividades de monitoramento da cadeia produtiva, a colocação em prática de um código de conduta para todos os profissionais da companhia, a criação e estruturação de um canal de denúncias eficaz e efetivo e a prestação de contas, periódica e transparente, a todos os stakeholders.

Somente a correta e eficaz gestão dos Riscos ESG terá o condão de reduzir sensivelmente as probabilidades de materialização de consequências daninhas como, num primeiro momento, prejuízos à imagem e, em casos mais agudos ou repetitivos, sérios danos à reputação da companhia.

Conclusão

Procuramos, de uma forma simplificada, proporcionar uma visão da importância da gestão do Risco Reputacional e de sua interconexão com os Riscos ESG, dos quais é, frequentemente, consequência.

Caso haja interesse de sua empresa em aprofundar-se nesse ou em outros temas relacionados ao gerenciamento de riscos, contate a Brasiliano INTERISK, uma empresa que oferece soluções de Inteligência e Gestão de Riscos com base na Interconectividade, conferindo total transparência aos processos de Governança, Riscos e Compliance.

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

Venha conhecer nosso sistema e solicite uma demonstração

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

FORMAÇÃO DO PROFISSIONAL DE SEGURANÇA

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

Nos últimos anos, tem havido um aumento na amplitude de atuação e importância do segmento de segurança. No entanto, muitas organizações ainda não incluem esse segmento nas decisões estratégicas, limitando-o ao nível operacional. Os Gestores de Segurança nesse nível têm pouca autonomia, uma vez que estão vinculados a uma gerência existente ou não há uma gerência de segurança dedicada. No entanto, no mercado, já há gestores com cargos de gerência média ou diretoria de alta administração, embora essa evolução seja lenta.

É fundamental que as empresas e os profissionais de segurança compreendam a segurança de maneira ampla. O Gestor de Segurança é, de fato, um gestor de riscos, que engloba diversas vertentes de ações de segurança, gerenciamento de riscos e gerenciamento de perdas.

No Brasil, há um erro comum na separação entre segurança empresarial (security) e segurança do trabalho (safety). Embora a legislação torne essa interação mais difícil, essa separação é equivocada, pois a Gestão de Risco (ISO 31000) abrange todos os riscos empresariais. Mesmo que haja a obrigatoriedade da existência de técnicos e engenheiros de segurança do trabalho, esses profissionais devem estar vinculados à área de Gestão de Riscos e não a outro departamento, a exemplo de RH, Infraestrutura, Engenharia, Patrimônio, dentre outros.

As empresas estão começando a perceber gradualmente a importância da área de segurança para a realização das Diretrizes Estratégicas, mesmo que seja uma atividade de suporte à atividade principal. Essa compreensão, juntamente com a formação adequada do Gestor de Segurança por meio de graduação e pós-graduação específicas, bem como a formação e cursos de aprimoramento para os operacionais, ajudarão a elevar a segurança do nível operacional para o nível tático.

A atividade de consultoria em segurança, por exemplo, ainda está em fase de amadurecimento em muitos estados. A falta de Cultura de Segurança das empresas e a formação inadequada dos profissionais são alguns dos motivos para essa realidade. Na maioria das vezes, as empresas não percebem a importância do planejamento de um sistema de segurança, optando por soluções isoladas, como a contratação de mais pessoas ou tecnologia, sem uma visão sistêmica.

“Além disso, há empresas especializadas em tecnologia ou segurança (conforme a Lei 7.102 de 1983) que priorizam a venda de equipamentos ou pessoal em vez de uma solução de segurança eficaz.”

O caminho correto seria a contratação de um consultor para realizar um diagnóstico e desenvolver uma solução de segurança completa (incluindo planejamento preventivo e contingencial) e, em seguida, a contratação de empresas especializadas para a implementação da solução.
O novo cenário da segurança exige um aprimoramento contínuo de todos os profissionais envolvidos no sistema, desde o gestor até o operacional (vigilante). Atuar empiricamente, baseado apenas em conhecimento tácito, não é mais suficiente.

Como já mencionado anteriormente, o Gestor de Segurança deve possuir graduação superior específica em gestão de segurança privada e, preferencialmente, pós-graduação lato sensu em área correlata. Já o operacional, além do curso de formação obrigatório por lei, deve buscar constantemente atualizações por meio de cursos não previstos na Legislação Específica.

Outro ponto crucial para a qualificação contínua dos profissionais é a necessidade de cursos específicos para o tipo de negócio do cliente.
É importante compreender que o Sistema de Segurança deve estar alinhado com o negócio, sendo que a segurança em hotéis é diferente da segurança em shoppings e condomínios. A qualificação contínua é essencial em qualquer área profissional, mas na segurança é ainda mais importante devido à sua dinamicidade.

Dr. Sérgio Leônidas Dias Caldas, CPSI, CIGR
Doutor Ciências da Segurança | Gestão Empresarial e Corporativa | Prevenção e Controle de Perdas | Riscos Corporativos

“O papel da Auditoria Investigativa frente as fraudes nas organizações”

Gláucia Maria da Silva, MBS, CPSI, CIGR, CIEIE

As fraudes não são prerrogativas apenas da sociedade atual, são lamentáveis acontecimentos que se perpetuam pela história do homem e de todas as suas civilizações. Atualmente, as empresas estão percebendo cada vez mais que as fraudes também não são exclusividade de determinadas entidades, atacam qualquer tipo de organização.

Elas provocam, além das altas perdas financeiras, outras consequências por demais devastas, tanto no ambiente interno como externo e a imagem da empresa.

ASPECTOS CONCEITUAIS

Na busca do significado da palavra fraude, comumente se depara com o sentido de: burlar, enganar, espoliar, roubar, falsificar, adulterar, sonegar e lesar. Já erro, do latim “error”, enganar-se, desviar-se. Conforme os Dicionários da Língua Portuguesa, a palavra erro pode ter os seguintes significados: “equívoco, uso impróprio ou indevido, doutrina falsa”.

Das diversas classificações históricas de fraudes, já efetuadas, reveste-se de interesse a que as dividem em: a) Não encobertas; b) Encobertas temporariamente; c) Encobertas permanentemente.

Os estudiosos de comportamento criminal acham que teoricamente todas as pessoas, se forem motivadas suficientemente, e o ambiente for propício a isto, vão cometer uma fraude ou irregularidade.

FRAUDES X AUDITORIA

A primeira responsabilidade na prevenção e identificação de fraudes e/ou erros é da Administração e da área de Governança da empresa, mediante a manutenção de adequados sistemas de controles internos, que, entretanto, não eliminam a possibilidade e/ou o risco de sua ocorrência.

O auditor, particularmente no âmbito contábil, “não é responsável nem pode ser responsabilizado pela prevenção de fraudes ou erros. Entretanto, deve planejar seu trabalho avaliando o risco da sua ocorrência, de forma a ter grande probabilidade de detectar aqueles que impliquem efeitos relevantes nas demonstrações contábeis” (CFC, 1999, p. 208).

O profissional de auditoria sempre deve informar à alta Administração da organização auditada descobertas factuais envolvendo fraude.

A adoção de controles que previnam quanto à ocorrência de fraudes contra o patrimônio, ou permitam detectá-las quando ocorrerem, é uma responsabilidade tanto gerencial quanto diretiva. Cabe aos auditores verificar e comprovar a

adequação das medidas tomadas pela administração para cumprir suas responsabilidades nesse particular.

As fraudes, atualmente, assumem inúmeras e diversas formas, modalidades e características dentro e fora das empresas. Tornaram-se complexas e sofisticadas, acompanhando o progresso tecnológico, sendo realizadas por gestores, empregados, clientes e/ou terceiros. Com esta triste realidade, tornam-se cada vez mais necessárias ações, medidas e controles internos eficazes, que as possam prevenir e/ou rapidamente identificar.

Outro fator importante no contexto Estratégico significa a identificação dos processos da empresa, segue algumas diretrizes estratégicas que devem serem seguidas: Análise Lógica; Compreensão histórica; Percepção Psicológica e Visão Sociológica.

Importante sempre fazer o cruzamento de dados, considerando 4 itens: Motivação do Ator; Causas do Delito; Lógica da Agressão; Consequências do delito.

Enfim, não basta ter somente alguns bons controles internos. É necessário sempre atualizá-los e adaptá-los à realidade. A prevenção é um trabalho contínuo e ininterrupto. A Auditoria Interna, neste aspecto, tem um papel de extrema importância na avaliação permanente destes controles internos dentro das organizações; tem ainda um papel decisivo na prevenção, identificação e/ou apuração das fraudes, bem como na coleta e seleção de provas e evidências, que possam ser apresentados contra os fraudadores, tanto na esfera civil como na esfera criminal.

Gláucia Maria da Silva, MBS, CPSI, CIGR, CIEIE; Especializada em Gestão de Pessoas – Master Business Administration – MBA pela Faculdade ISCA – Instituto Superior de Ciências Aplicadas; Graduada em Serviço Social pela Faculdade ISCA - Instituto Superior de Ciências Aplicadas; Técnica em Enfermagem pela UNIPAC; Auditora das ISO´s 9001, 31.000 e OHAS 18.001. Analista de Inteligência Estratégica e Segurança Corporativa e Empresarial - ADESG-CPS; CURSO INTERNACIONAL DE “ANALISIS DE INTELIGENCIA” pelo CEAS; Curso de Continuidade de Negócio – GCN pelo Brasiliano; Curso de Gestão de Riscos e Fraudes pelo Brasiliano; Curso de Identificação de possíveis suspeitos pela Polícia Federal; Cursos de Capacitação para habilitação e instrução do uso do DEA, padrão AHA 2018; Curso de Aspectos Práticos da Aplicação da Legislação e de Política Judiciária pelo Departamento de Polícia Civil de SP. Atualmente Inspetora de Segurança Orgânica do Shopping Iguatemi Campinas.

Funções, responsabilidades do vigilante de acordo com a legislação atual

José Sérgio Marcondes, CES, CPSI

Saiba quais são as funções e responsabilidades do vigilante. Qual a importância de conhecer e pôr em prática essas atribuições e como elas impactam na profissão.

As Funções e responsabilidades do Vigilante são a descrição do conjunto de atividades e tarefas atribuídas aos vigilantes no exercício da sua profissão, visando alcançar um objetivo de segurança necessário e desejado. Refere-se às tarefas e responsabilidades específicas associadas ao cargo de vigilante.

No mundo atual, onde a segurança é uma preocupação constante, as funções do vigilante desempenham um papel essencial na proteção de pessoas, bens, propriedades e eventos. Eles são responsáveis por garantir a tranquilidade e a integridade daqueles que necessitam de uma proteção especializada.

Os vigilantes desempenham um papel de destaque na segurança privada, complementando o trabalho das forças de segurança pública. Sua presença e atuação eficiente contribuem diretamente para a tranquilidade de pessoas, empresas e instituições.

Mas você já parou para pensar quais são exatamente as funções e responsabilidades do vigilante? Neste artigo, iremos explorar as principais atribuições dos vigilantes no exercício da sua profissão.

O que são funções e responsabilidades do vigilante?

As Funções e responsabilidades do Vigilante são a descrição do conjunto de atividades e tarefas atribuídas aos vigilantes no exercício da sua profissão, visando alcançar um objetivo de segurança necessário e desejado. Refere-se às tarefas e responsabilidades específicas associadas a profissão do Vigilante.

As Funções e responsabilidades do Vigilante são definidas com base na lei 7.10, e em normas e regulamentações específicas estabelecidas pelos órgãos competentes, como a Polícia Federal. Essas normas estabelecem as responsabilidades e atividades que um vigilante pode realizar de acordo com sua formação e especialização.

Além disso, as funções dos vigilantes também podem variar de acordo com o local de atuação e as necessidades específicas de segurança envolvidas. Por exemplo, em uma empresa, as responsabilidades do vigilante podem envolver controle de acesso de funcionários e visitantes, vigilância perimetral, rondas preventivas, entre outras atividades relacionadas à segurança da empresa.

Fontes que definem as funções e responsabilidades do vigilante

As funções e responsabilidades do vigilante poderão estar contidas nas previsões legais a seguir:

LEI Nº 7.102, DE 20 DE JUNHO DE 1983 – Que dispõe sobre segurança para estabelecimentos financeiros, estabelece normas para constituição e funcionamento das empresas particulares que exploram serviços de vigilância e de transporte de valores, e dá outras providências.

DECRETO Nº 89.056, DE 24 DE NOVEMBRO 1983 – Que regulamenta a Lei nº 7.102, de 20 de junho de 1983.

PORTARIA Nº 18.045, DE 17 DE ABRIL DE 2023 – Que disciplina as atividades de segurança privada e regula a fiscalização dos Planos de Segurança dos estabelecimentos financeiros.

Contrato de prestação de serviço – Acordo formal estabelecido para prestação dos serviços de segurança privada, o qual deve respeitar as normas e diretrizes estabelecidas nas legislações citadas anteriormente.

Quais as principais atividades do vigilante previstas na legislação?

O vigilante desempenha uma série de atividades de segurança privada, que são autorizadas pela Lei 7.102 e regulamentadas pela Portaria DG/PF nº 18.045, de 17 de abril de 2023. Essas atividades são fundamentais para garantir a segurança das pessoas e a integridade do patrimônio em diversos contextos.

A seguir as principais atividades desenvolvidas pelo vigilante, conforme legislação pertinente:

Vigilância patrimonial: O vigilante exerce a vigilância patrimonial em eventos sociais, bem como dentro de estabelecimentos urbanos ou rurais, públicos ou privados. Essa atividade tem como objetivo garantir a incolumidade física das pessoas presentes e a proteção do patrimônio.

Transporte de valores: O transporte de valores é outra atividade desempenhada pelo vigilante. Essa função envolve o transporte seguro de numerário, bens ou valores utilizando veículos especiais. Essa atividade requer especialização em curso específico e medidas de segurança rigorosas para garantir a proteção do dinheiro e dos objetos de valor.

Escolta armada: A escolta armada consiste em garantir a segurança durante o transporte de cargas ou valores de qualquer tipo. O vigilante realiza a proteção do veículo e de sua carga, assegurando que o transporte ocorra de forma segura e protegida. Essa atividade requer especialização em curso específico e medidas de segurança especificas para garantir a proteção da carga valiosa.

Segurança pessoal: O vigilante também pode atuar na segurança pessoal, que tem como objetivo garantir a incolumidade física de pessoas específicas, envolve a proteção e o acompanhamento de indivíduos em situações que requerem segurança especial. Essa atividade requer especialização em curso específico e medidas de segurança especiais para garantir a integridade física da pessoa protegida.

Quais as principais funções e responsabilidades do vigilante?

No desempenho das atividades permitidas pela legislação o vigilante desempenha várias funções conforme o tipo de atividade que desempenha. Dentre as principais funções e responsabilidades do vigilante podemos destacar:

1. Prevenção de crimes: O vigilante atua como um agente dissuasor, evitando a ocorrência de crimes por meio de sua presença visível e vigilância constante.

2. Complemento da segurança pública: A legislação considera a atividade do vigilante complementar as atividades da segurança pública, pois seria inviável ao Estado assumir todas as funções da segurança, o que geraria grande dificuldade em promover a proteção da população no geral.

3. Controle de acesso: Faz parte da função do vigilante controlar o acesso de pessoas e veículos em determinados locais, verificando identificações, autorizações e realizando procedimentos de revista quando necessário.

4. Proteção de áreas edificações: O vigilante também pode ser responsável pela proteção de áreas específicas dentro de um local, como salas restritas, depósitos, armazéns e zonas de acesso controlado.

5. Proteção de bens e patrimônio: É responsabilidade do vigilante resguardar e preservar os bens materiais de um local, como equipamentos, maquinários, estoques, veículos e instalações físicas.

6. Proteção de valores e numerários: Em locais como instituições financeiras, empresas de transporte de valores e estabelecimentos comerciais que manipulam dinheiro, o vigilante desempenha um papel crucial na proteção desses valores e numerários.

7. Proteção de pessoas: Além da proteção de bens materiais, o vigilante também atua na função de proteção de pessoas para garantir a integridade física e emocional dos indivíduos.

8. Atendimento ao público: Além de suas funções de segurança, o vigilante também desempenha um papel fundamental de atendimento ao público, seja para dar informações, orientar comportamentos ou realizar controle de acessos.

9. Monitoramento de alarmes e câmeras: Faz parte da função do vigilante supervisor sistemas de alarme e câmeras de segurança, detectando qualquer sinal de intrusão ou atividade suspeita.

10. Segurança em eventos: Em eventos de grande porte, como shows, feiras, festivais ou conferências, o vigilante desempenha um papel essencial na segurança dos participantes.

11. Intervenção em casos de ações violentas: Faz parte da função segurança do vigilante intervir em casos de tentativas de roubo ou outras ações agressivas de força adversa, sendo seu principal objetivo, nessas situações, garantir a segurança das pessoas e proteger o patrimônio, agindo de forma adequada e dentro dos limites legais e de sua capacidade e treinamento.

12. Resposta a emergências: Também faz parte das funções do vigilante agir em caso de emergências como incêndios, acidentes ou desastres. Ele pode auxiliar na prestação de primeiros socorros, na evacuação do local, combater princípios de incêndio e acionar/colaborar com equipes de emergência.

Quais as principais tarefas do vigilante?

No exercício das suas funções e responsabilidades, os vigilantes desempenham diversos tipos de tarefas, entre as quais podemos destacar:

- Controlar acesso a área controladas e restritas;
- Atender, identificar, orientar, encaminhar, acompanhar e fiscalizar pessoas;
- Gerenciar e registrar a movimentação de pessoas, veículos e objetos;
- Controlar, fiscalizar e orientar a movimentação interna de pessoas, veículos, objetos e bens;
- Conferir e inspecionar a integridade de mercadorias, equipamentos, materiais e cargas;
- Revistar pessoas, veículos, objetos e recintos;
- Auxiliar idosos, deficientes físicos e demais pessoas necessitadas;
- Abordar pessoas e veículos em atitude suspeita;
- Ocupar postos de vigilâncias e de controle de acesso;
- Realizar rondas de segurança;
- Ligar e desligar sistemas de iluminação;
- Ligar, operar e desligar sistemas eletrônicos de segurança;
- Orientar e fiscalizar o cumprimento de políticas, normas e procedimentos de segurança;
- Prestar primeiros socorros e providenciar socorros médicos;
- Prevenir e combater princípios de incêndio;
- Confeccionar relatórios de ocorrência;
- Confeccionar livro de ocorrência;
- Interagir com órgãos de segurança pública, e solicitar apoio quando necessário;
- Identificar e tratar as vulnerabilidades e riscos de segurança;
- Intervir em situações de ameaça ou tentativas de cometimento de crimes.

Funções e atividades do Vigilante

Como deve ser a postura do vigilante com relações as suas funções e responsabilidades?

A postura do vigilante em relação às suas funções e responsabilidades deve ser profissional, diligente e responsável. O vigilante é um profissional dedicado à segurança e proteção de pessoas e patrimônios, e sua postura reflete diretamente na eficiência e credibilidade de seu trabalho. A seguir alguns aspectos importantes da postura do vigilante:

Conhecimento das funções e responsabilidades: O vigilante deve ter um entendimento claro de suas funções e responsabilidades. Deve buscar se informar sobre as diretrizes da empresa, procedimentos operacionais, e as políticas de segurança relevantes.

Domínio das habilidades necessárias: Cada função específica dentro da segurança privada requer habilidades particulares. Neste contexto, o vigilante deve buscar constantemente aprimorar suas habilidades e conhecimentos por meio de treinamentos e capacitações adequadas.

Manutenção da preparação física: A preparação física adequada é importante para o vigilante, pois suas funções muitas vezes exigem esforço físico e resistência. Manter uma boa condição física ajuda o vigilante a lidar com situações desafiadoras, a realizar suas atividades de forma eficiente e a garantir sua própria segurança, bem como a segurança daqueles sob sua proteção.

Profissionalismo: O vigilante deve agir de forma profissional em todos os momentos, mantendo uma conduta ética, respeitando as leis e regulamentos aplicáveis e seguindo os procedimentos estabelecidos pela empresa.

Atitude vigilante: O vigilante deve estar atento e vigilante em seu ambiente de trabalho, identificando potenciais ameaças, observando comportamentos suspeitos e tomando as medidas adequadas para prevenir incidentes de segurança. Ele deve ser proativo, antecipando-se a situações de risco e agindo de forma preventiva.

Comunicação eficaz: O vigilante deve ser capaz de se comunicar de maneira clara e eficaz com colegas de trabalho, autoridades competentes, clientes e o público em geral. Isso inclui relatar incidentes, fornecer informações relevantes, transmitir instruções de segurança e responder a perguntas ou solicitações de forma adequada.

Respeito e empatia: O vigilante deve tratar todas as pessoas com respeito e empatia, independentemente de sua origem, posição social ou outras características. Ele deve ser capaz de lidar com diferentes situações de forma calma, cortês e profissional, mesmo em momentos de tensão.

Responsabilidade e confiabilidade: O vigilante deve assumir a responsabilidade por suas ações e cumprir com suas obrigações e deveres com diligência. Ele deve ser confiável e estar comprometido com a segurança e o bem-estar das pessoas e do patrimônio que lhe foram confiados. Isso envolve cumprir os

protocolos de segurança, realizar suas tarefas de forma adequada, reportar incidentes e cumprir com as normas legais e regulamentares.

Conclusão:

Ao longo deste artigo, exploramos minuciosamente as principais funções desempenhadas pelos vigilantes em diferentes áreas de atuação. Ficou claro que esses profissionais desempenham um papel fundamental na garantia da segurança e proteção de pessoas, bens, áreas, propriedades e eventos.

É importante ressaltar a importância dessas funções e o impacto positivo que os vigilantes têm na sociedade. Eles são os guardiões da tranquilidade, dedicados a prevenir e intervir nas situações de risco, garantindo a segurança daqueles que confiam em seus serviços.

Considerando todos os aspectos abordados, fica evidente que os vigilantes desempenham um papel de destaque na segurança privada, complementando o trabalho das forças de segurança pública. Sua presença e atuação eficiente contribuem diretamente para a tranquilidade de pessoas, empresas e instituições.

Diante desse panorama, é fundamental reconhecer e valorizar o trabalho desses profissionais, bem como conhecer os direitos e deveres que os cercam. Para aprofundar seu conhecimento sobre esse tema relevante, convido você a ler o meu artigo sobre “Os Direitos e Deveres do Vigilante. Nele, você encontrará informações importantes que todo vigilante e aqueles interessados na área devem conhecer.

José Sérgio Marcondes, CES, CPSI

Especialista em Segurança Empresarial, Consultor em Segurança Privada e Diretor do IBRASEP, com amplo conhecimento em Gestão Empresa.

INTRODUÇÃO A ISO 31000 - REPUTAÇÃO E IMAGEM

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

INTRODUÇÃO A ISO 31000

A ISO 31000 é uma norma internacional que estabelece os princípios e as diretrizes para a gestão de riscos em uma organização. Ela foi desenvolvida para ajudar as empresas a lidar de forma mais eficaz com os riscos que enfrentam em suas operações diárias.

O risco é uma parte intrínseca de qualquer negócio. Ele surge devido à incerteza associada a eventos futuros e pode ter um impacto negativo na performance da empresa. A gestão de riscos é, portanto, uma parte crucial da estratégia de qualquer organização.

A ISO 31000 é uma ferramenta essencial para a gestão de riscos. Ela fornece uma estrutura para a identificação, avaliação e tratamento dos riscos que uma organização enfrenta. Isso ajuda a minimizar a possibilidade de perda financeira, dano à reputação ou qualquer outro tipo de impacto negativo.

A norma ISO 31000 é baseada em três princípios fundamentais: integração, inclusão e melhoria contínua.

· A integração envolve a incorporação da gestão de riscos em todos os processos da empresa;

· A inclusão refere-se à participação de todas as partes interessadas na gestão de riscos;

· E a melhoria contínua envolve a análise constante dos resultados da gestão de riscos e a busca de maneiras de melhorar o processo.

No entanto, é importante lembrar que a ISO 31000 não elimina completamente o risco. Ela apenas fornece uma estrutura para a sua gestão. É responsabilidade da empresa implementar as diretrizes estabelecidas e garantir que a gestão de riscos seja uma parte integral da sua estratégia.

A gestão de riscos bem-sucedida requer uma abordagem multidisciplinar. É importante envolver todas as partes interessadas, incluindo:

· Funcionários;

· Clientes; e

· fornecedores, todos na identificação e avaliação dos riscos.

Além disso, as empresas devem estar dispostas a investir tempo e recursos na gestão de riscos, a fim de minimizar os impactos negativos que os riscos podem ter.

INTEGRAÇÃO DA GESTÃO DE RISCO EM PROCESSOS EMPRESARIAIS

Digamos que você tenha uma empresa de manufatura que produz uma variedade de produtos. Um dos riscos que você enfrenta é a possibilidade de um produto apresentar defeito e causar danos a um cliente.

Para integrar o gerenciamento de riscos em seus processos, você pode seguir os seguintes passos:

· Implementar plano de gerenciamento de risco;

· Identifique o risco: Identifique os riscos potenciais associados aos seus produtos, como fabricação defeituosa, falhas de projeto ou testes inadequados de produtos;

· Avalie o risco: Avalie o impacto potencial de cada risco e a probabilidade de ocorrência. Por exemplo, uma falha de projeto que pode causar danos a um cliente tem alta probabilidade de ocorrer e alto impacto;

· Desenvolver um plano de gerenciamento de riscos: Desenvolva um plano que descreva como você reduzirá os riscos identificados. Isso pode envolver melhorar o design do produto e aprimorar o processo de fabricação;

· Monitorar, mitigar, contingenciar, reparar, tratar, corrigir, reter ou transferir o risco.

PARTES INTERESSADAS E A GESTÃO DE RISCOS

A gestão de riscos é uma atividade crucial para garantir a segurança e a sustentabilidade de uma organização. É importante que as partes interessadas, ou seja, as pessoas ou grupos que são afetuosos pelas atividades da empresa, estejam envolvidos nesse processo. Isso pode incluir funcionários, clientes, fornecedores, acionistas e até mesmo a comunidade local. Ao envolver as partes interessadas na gestão de riscos, a empresa pode obter uma visão mais ampla dos riscos potenciais e das consequências associadas a eles. Além disso, a participação das partes interessadas pode aumentar a transparência da gestão de riscos e ajudar a criar um ambiente de confiança e colaboração.

A participação das partes interessadas deve ocorrer para que se evite os seguintes pontos:

· Recursos limitados: o gerenciamento de riscos pode ser demorado e exigir recursos significativos, incluindo financeiros, humanos e tecnológicos. Organizações menores podem lutar para alocar esses recursos de forma eficaz.

Além de:

· Resistência dos participantes;

· Falta de engajamento;

· Dados insuficientes:

· Outros.

RESISTÊNCIA DAS PARTES INTERESSADAS

A resistência das partes interessadas é um incentivo comum em muitos projetos e iniciativas corporativas. Quando as partes envolvidas se sentem ameaçadas por mudanças ou percebem que seus interesses não estão sendo considerados, é natural que possam resistir às mudanças propostas. Para superar essa resistência, é importante adotar uma abordagem colaborativa, envolvendo as partes interessadas desde o início do processo. Isso pode incluir a comunicação clara e transparente sobre os objetivos e benefícios da iniciativa, a escuta ativa das preocupações e sugestões das partes interessadas e a busca de soluções conjuntas para abordar as questões levantadas. Ao adotar uma abordagem colaborativa, é possível construir um ambiente de confiança e cooperação, encorajar a resistência e aumentar as chances de sucesso da iniciativa.

Principais abordagens colaborativas são:

· Treinar funcionários: Fornecer treinamento e educação aos funcionários sobre a importância da gestão de riscos e como isso beneficia a empresa. Isso pode ajudar os funcionários a entender a necessidade de mudança e incentivá-los a apoiar a implementação dos planos de gerenciamento de riscos;

· Educar os funcionários: É importante educar os funcionários sobre a iniciativa proposta, explicando claramente os objetivos e os benefícios. Quando os funcionários entendem a importância da iniciativa, eles se tornam mais tolerantes a apoiá-la e trabalhar para que ela tenha sucesso;

· Envolve-los do início ao fim do processo;

· Comunicar efetivamente cada ação durante o processo;

· Liderá-los ao bem comum:

· Alinhar as ações e expectativas do processo.

CASES DE SUCESSO GESTÃO DE RISCO

Aqui estão alguns exemplos de empresas que implementaram com sucesso planos de gerenciamento de riscos:

· IBM: tem um programa abrangente de gerenciamento de risco projetado para identificar e mitigar os riscos associados às suas operações de negócios. O programa inclui uma robusta função de auditoria interna, avaliações de risco e foco na melhoria contínua;

· Apple: implementou um plano de gerenciamento de riscos que se concentra em garantir a segurança de seus produtos e serviços. A empresa implementou medidas de segurança rigorosas para proteger os dados do cliente e também implementou um programa de segurança de produtos para garantir que seus produtos sejam seguros para uso;

· Procter & Gamble: tem um programa de gerenciamento de risco projetado para identificar e mitigar os riscos associados à sua cadeia de suprimentos. A empresa implementou ferramentas e processos para monitorar os fornecedores e garantir o cumprimento dos padrões de qualidade e segurança;

· Boeing: implementou um plano de gerenciamento de riscos que se concentra em garantir a segurança de suas aeronaves. A empresa implementou testes rigorosos e medidas de controle de qualidade para garantir que suas aeronaves atendam aos mais altos padrões de segurança;

· Pfizer: tem um programa de gestão de risco que é projetado para identificar e mitigar os riscos associados com seus processos de desenvolvimento e fabricação de medicamentos. A empresa implementou medidas rigorosas de controle de qualidade para garantir que seus medicamentos sejam seguros e eficazes.

Essas empresas demonstram que o gerenciamento eficaz de riscos é essencial para o sucesso no ambiente de negócios atual. Ao implementar planos abrangentes de gerenciamento de riscos, essas empresas conseguiram identificar e mitigar riscos, proteger sua reputação e garantir a segurança de seus produtos e serviços.

RISCOS REPUTACIONAIS EMPRESARIAIS

Existem muitos riscos que as empresas enfrentam, e os riscos específicos dependerão do setor, do tamanho da empresa e de outros fatores. Aqui estão alguns riscos comuns que muitas empresas enfrentam:

· Riscos financeiros: as empresas podem enfrentar riscos financeiros, como desacelerações econômicas, flutuações cambiais, mudanças nas taxas de juros e risco de crédito;

· Riscos operacionais: Os riscos operacionais surgem das atividades diárias do negócio e podem incluir interrupções na cadeia de suprimentos, falhas de equipamentos e erros de funcionários;

· Riscos legais e regulatórios: As empresas podem enfrentar riscos legais e regulatórios, como ações judiciais, multas e penalidades por não conformidade com leis e regulamentos;

· Riscos de reputação: Os riscos de reputação surgem de publicidade negativa, reclamações de clientes e outros fatores que podem prejudicar a marca e a reputação da empresa;

· Riscos de segurança cibernética: as empresas enfrentam riscos de segurança cibernética, como violações de dados, hackers e outras ameaças cibernéticas que podem comprometer dados de clientes e outras informações confidenciais;

· Riscos ambientais: as empresas podem enfrentar riscos ambientais, como poluição, mudanças climáticas e desastres naturais;

· Riscos estratégicos: Os riscos estratégicos surgem da estratégia de longo prazo da empresa e podem incluir mudanças no mercado, concorrência e outros fatores que podem afetar o sucesso futuro da empresa.

Estes são apenas alguns exemplos dos muitos riscos que as empresas enfrentam. É importante que as empresas identifiquem e avaliem esses riscos e

implementem estratégias para mitigá-los para proteger seus negócios e garantir o sucesso a longo prazo.

MITIGAÇÃO RISCOS REPUTACIONAIS

As empresas podem ser proativas na mitigação de riscos reputacionais adotando diversas medidas preventivas. Uma delas é priorizar a ética e a transparência em todas as suas operações, evitando práticas que possam ser percebidas como antiéticas ou ilegais.

Além disso, é importante monitorar ativamente a crença da empresa nas redes sociais e em outros canais de comunicação, a fim de identificar e responder a quaisquer problemas ou críticas.

As empresas também podem investir em programas de treinamento e conscientização para seus funcionários, garantindo que todos estejam cientes das políticas e procedimentos da empresa e possam agir de forma adequada em situações de risco.

Afinal, é importante ter um plano de gerenciamento de crises em vigor, para que a empresa possa responder rapidamente e de forma eficaz a qualquer problema que possa surgir.

Ao adotar essas práticas, as empresas podem ser proativas na mitigação de riscos reputacionais e proteger sua imagem perante o público e seus stakeholders.

MEDIÇÃO RISCOS REPUTACIONAIS

Medir a eficácia das estratégias de gerenciamento de reputação de uma empresa é essencial para garantir que elas alcancem os resultados desejados.

Aqui estão algumas maneiras pelas quais as empresas podem medir a eficácia de suas estratégias de gerenciamento de reputação:

· Pesquisas: as empresas podem realizar pesquisas para medir as percepções dos clientes sobre sua marca e reputação. As pesquisas podem avaliar fatores como reconhecimento da marca, fidelidade do cliente e satisfação geral;

· Monitoramento de mídia social: as empresas podem monitorar canais de mídia social para rastrear menções de sua marca e reputação. Isso pode ajudar a identificar qualquer comentário ou feedback negativo que possa afetar sua reputação e permitir que eles respondam prontamente;

· Análise da cobertura da mídia: as empresas podem analisar a cobertura da mídia para rastrear a visibilidade de sua marca e avaliar o tom da cobertura. Isso pode ajudar a identificar qualquer publicidade negativa e permitir que eles tomem medidas para resolvê-la;

· Índice de reputação: as empresas podem usar índices de reputação, como o sistema RepTrak, para medir sua reputação em relação aos concorrentes. Esses índices avaliam fatores como confiança, liderança e responsabilidade social;

· Feedback dos funcionários: as empresas podem coletar feedback dos funcionários para avaliar a eficácia de suas estratégias de gerenciamento de reputação. Isso pode ajudar a identificar áreas de melhoria e garantir que os funcionários estejam alinhados com as metas de reputação da empresa.

ERROS COMUNS DE RISCOS REPUTACIONAIS

Existem vários erros comuns que as empresas podem cometer ao medir suas estratégias de gestão de reputação. aqui estão alguns exemplos:

· Concentrar-se apenas em métricas quantitativas: embora as métricas quantitativas, como vendas e crescimento de receita, sejam importantes, elas não fornecem uma imagem completa da reputação de uma empresa. As empresas também devem considerar métricas qualitativas, como reconhecimento da marca, fidelidade do cliente e envolvimento dos funcionários;

· Negligenciar o estabelecimento de metas claras: as empresas devem definir metas claras para suas estratégias de gerenciamento de reputação e medir seu sucesso em relação a essas metas. Sem objetivos claros, pode ser um desafio avaliar a eficácia das estratégias de gerenciamento de reputação;

· Deixar de medir as métricas corretas: as empresas devem garantir que estão medindo as métricas mais relevantes para seus objetivos de gerenciamento de reputação. Medir as métricas erradas pode levar a avaliações imprecisas de eficácia e desperdício de recursos;

· Confiar demais em pesquisas: as pesquisas podem ser uma ferramenta útil para medir a reputação, mas não devem ser a única ferramenta usada. As empresas também devem considerar outras métricas, como cobertura da mídia, monitoramento de mídia social e feedback dos funcionários;

· Deixar de avaliar a concorrência: as empresas devem avaliar sua reputação em relação a seus concorrentes para determinar sua posição no mercado. Deixar de fazer isso pode levar a avaliações imprecisas de eficácia e oportunidades perdidas de melhoria;

· Não revisar e ajustar estratégias regularmente: as estratégias de gerenciamento de reputação devem ser revisadas e ajustadas regularmente com base nas mudanças nas condições do mercado e no feedback das partes interessadas. Deixar de fazer isso pode resultar em estratégias desatualizadas que não são mais eficazes.

Ao evitar esses erros comuns e adotar uma abordagem abrangente para medir as estratégias de gerenciamento de reputação, as empresas podem garantir que estão avaliando com precisão a eficácia e identificando áreas para melhoria.

EXEMPLOS DE MEDIÇÃO DE MÉTRICAS CERTAS

Além das pesquisas, monitoramento, análise e avaliação que podemos ser realizadas para medir a reputação de uma empresa, podemos dizer que:

· Índice de crédito: é uma medida quantitativa do crédito de uma empresa, que leva em consideração diversos fatores, como qualidade dos produtos e serviços, responsabilidade social e ambiental, governança corporativa, entre

outros. Empresas como a Reputation Institute e Forbes publicam índices de confiança de empresas em todo o mundo.

MÉTRICAS ESTRATÉGICAS GERENCIAMENTO DE REPUTAÇÃO

Medir corretamente a opinião de uma empresa é fundamental para entender como a empresa é percebida por seus clientes, partes interessadas e público em geral. A seguir, apresentamos 5 exemplos de métricas que podem ser usados para medir a acreditar de uma empresa:

· Net Promoter Score (NPS): O NPS é uma métrica que avalia a lealdade e satisfação dos clientes com uma empresa. Os clientes são questionados a respeito de sua disposição em recomendar a empresa a outras pessoas, em uma escala de 0 a 10. A partir das respostas, é possível calcular o NPS, que varia de -100 a 100. Quanto maior o NPS, maior a lealdade e satisfação dos clientes e, consequentemente, o potencial de crédito positivo da empresa;

· Índice de acreditar: O índice de acreditar é uma métrica que avalia a acreditar de uma empresa em relação a seus concorrentes. É possível acreditar em diversos aspectos, como qualidade dos produtos e serviços, responsabilidade social e ambiental, governança corporativa, entre outros. Empresas como a Reputation Institute e Forbes publicam índices de confiança de empresas em todo o mundo;

· Taxa de retenção de clientes: A taxa de retenção de clientes é uma métrica que avalia a capacidade de uma empresa em manter seus clientes fiéis. Quanto maior a taxa de retenção de clientes, maior a confiança e satisfação dos clientes em relação à empresa, e, consequentemente, maior probabilidade de credibilidade positiva;

· Análise de sentimento: A análise de sentimento é uma métrica que avalia a percepção do público em relação à empresa, identificando comentários positivos e negativos em redes sociais, fóruns e outros canais de comunicação. A partir da análise, é possível identificar tendências e oportunidades de melhoria;

· Índice de engajamento: O índice de engajamento é uma métrica que avalia a interação do público com a empresa em canais de comunicação, como redes sociais. É possível medir o número de seguidores, curtidas, comentários e compartilhamentos, entre outros aspectos. Quanto maior o índice de engajamento, maior a visibilidade e a audiência da empresa.

NET PROMOTER SCORE

Para calcular o Net Promoter Score (NPS), você precisará realizar uma pesquisa ou pedir a seus clientes que avaliem sua empresa em uma escala de 0 a 10 com base na pergunta "Qual a probabilidade de você recomendar nossa empresa a um amigo ou colega?"

Depois de coletar as respostas, você pode agrupá-las em três categorias:

· Promotores (9-10): Clientes com alta probabilidade de recomendar sua empresa a outras pessoas;

· Passivos (7-8): Clientes que estão satisfeitos com sua empresa, mas podem não necessariamente recomendá-la a outras pessoas;

· Detratores (0-6): clientes que provavelmente não recomendam sua empresa a outras pessoas e podem ter tido uma experiência negativa.

Para calcular o NPS, subtraia a porcentagem de detratores da porcentagem de promotores. O resultado será um número entre -100 e 100. Um NPS mais alto indica um nível mais alto de fidelidade e satisfação do cliente.

Veja um exemplo de como calcular o NPS:

Suponha que você tenha pesquisado 100 clientes e recebido as seguintes respostas:

· 60 promotores (classificação de 9-10);

· 20 passivas (classificação de 7-8);

· 20 detratores (avaliação de 0-6).

Para calcular o NPS, primeiro calcule a porcentagem de promotores e detratores:

· Promotores: 60/100 = 60%;

· Detratores: 20/100 = 20%.

Em seguida, subtraia a porcentagem de detratores da porcentagem de promotores:

· NPS = 60% - 20% = 40

Neste exemplo, o NPS é 40, o que indica um nível relativamente alto de fidelidade e satisfação do cliente.

MELHORIA NPS

Melhorar o Net Promoter Score (NPS) é importante para aumentar a fidelidade e a satisfação do cliente. Aqui estão algumas maneiras de melhorar o NPS:

· Aborde as preocupações dos clientes: responda de forma rápida e eficaz às preocupações e reclamações dos clientes. Isso pode ajudar a resolver problemas e evitar feedback negativo de detratores;

· Forneça um excelente atendimento ao cliente: certifique-se de que sua equipe de atendimento ao cliente esteja bem treinada e equipada para lidar com as dúvidas e preocupações dos clientes. Oferecer um serviço excepcional pode ajudar a aumentar a satisfação e a fidelidade do cliente;

· Personalize a experiência do cliente: personalize a experiência do cliente ao entender suas necessidades e preferências. Isso pode ajudar a construir uma conexão mais forte com os clientes e aumentar a probabilidade de recomendar sua empresa a outras pessoas;

· Ofereça incentivos: ofereça incentivos aos clientes que recomendam sua empresa a outras pessoas, como descontos ou recompensas. Isso pode incentivar os clientes a compartilhar suas experiências positivas com outras pessoas e aumentar a probabilidade de novos clientes;

· Meça e melhore continuamente: Meça e monitore continuamente o NPS e identifique áreas para melhoria. Use o feedback do cliente para melhorar produtos, serviços e a experiência geral do cliente;

· Envolva-se com os clientes: envolva-se com os clientes por meio de mídias sociais, e-mail ou outros canais para construir um relacionamento e criar uma impressão positiva. Isso pode ajudar a aumentar a fidelidade do cliente e a probabilidade de recomendar sua empresa a outras pessoas.

Ao implementar essas estratégias, você pode melhorar o Net Promoter Score e aumentar a fidelidade e a satisfação do cliente.

RESUMO

Como vimos, a gestão de riscos é uma prática essencial para garantir a sustentabilidade e o sucesso de uma organização. Além do que foi dito até aqui, a seguir, apresento 12 caminhos que devem ser observados na gestão de riscos corporativos:

· Identificação de riscos: Identificar os riscos que podem afetar a organização, como riscos financeiros, operacionais, regulatórios, entre outros;

· Análise de riscos: Analisar a probabilidade e o impacto dos riscos identificados, a fim de priorizar e planejar as ações de mitigação;

· Avaliação de riscos: Avaliar a eficácia das ações de mitigação incorporadas e implementadas, a fim de garantir que os riscos sejam legados gerenciados;

· Monitoramento de riscos: Monitorar continuamente os riscos, a fim de identificar novos riscos ou mudanças nos riscos existentes;

· Plano de contingência: Desenvolver um plano de contingência para lidar com possíveis eventos adversos, minimizando seus impactos na organização;

· Comunicação de riscos: Comunicar os riscos identificados e as ações de mitigação iniciadas e integradas para as partes interessadas, a fim de aumentar a transparência e a confiança;

· Gerenciamento de crises: Desenvolvedor de um plano de gerenciamento de crises, que inclui ações de comunicação, medidas de contingência e procedimentos para lidar com situações de emergência;

· Treinamento em gestão de riscos: Treinar os funcionários e colaboradores da organização em gestão de riscos, a fim de aumentar sua conscientização e capacidade de identificar e gerenciar riscos;

· Governança corporativa: Implementar práticas de governança corporativa eficazes, a fim de garantir a transparência, responsabilidade e conformidade com as leis e regulamentos;

· Tecnologia e segurança da informação: gerir os riscos relacionados com a tecnologia e segurança da informação, garantindo a proteção dos dados, sistemas e infraestrutura da organização;

· Responsabilidade social e sustentabilidade: gerenciar os riscos relacionados à responsabilidade social e sustentabilidade, garantindo que uma organização opere de forma ética e sustentável;

· Parcerias e terceirização: gerenciar os riscos relacionados a parcerias e terceirização, garantindo que as atividades terceirizadas sejam realizadas de forma eficaz e em conformidade com as políticas e regulamentos da organização.

CONCLUSÃO

Em resumo, a gestão de riscos é uma prática fundamental para garantir a sustentabilidade e o sucesso de uma organização. A ISO 31000 estabelece os princípios e diretrizes para a gestão de riscos em organização, visando ajudá-las a implementar um sistema de gestão de riscos eficaz e integrado. A implementação da ISO 31000 pode trazer vários benefícios para as organizações, incluindo a melhoria da tomada de decisões, a redução de perdas e danos, a maximização de oportunidades, entre outros. Para implementar a ISO 31000, as organizações devem seguir um processo sistemático e contínuo de avaliação e gestão de riscos, envolvendo todas as partes interessadas e enfatizando a importância da comunicação e consulta.

Dr. Sérgio Caldas CRA, MBA, MBR, CPSI, CIEIE, CIEAC, CIGR, DIDS, MSDIS, DICS. Prevenção e Controle de Perdas | Riscos Corporativos | Doctor en Ciencias de la Seguridad (España) | Gestão Empresarial e Corporativa.

A importância de um Plano de Segurança e Emergência no Ambiente Escolar

Dr. Fabiano Sérgio Paiva Dias de Sá, CPSI

A segurança e o bem-estar dos estudantes e funcionários são prioridades fundamentais em qualquer ambiente escolar. A falta de cultura no Brasil, no tocante a segurança no ambiente escolar, por exemplo, leva a uma sensação de insegurança e abandono. Um plano de segurança e emergência eficaz desempenha um papel crucial na preparação e resposta a situações de risco, ajudando a minimizar danos e proteger a vida.

O presente artigo, decorre da expertise adquirida na consultoria realizada na Maple Bear Canadian School Porto Velho, para nos conduzir a uma reflexão acerca da importância da existência de um plano de segurança e emergência no ambiente escolar e os benefícios que ele pode trazer para a comunidade escolar.

A elaboração de um plano de segurança e emergência no ambiente escolar, deve abranger pontos que possam direcionar ações, visando mitigar ou eliminar os riscos levantados. Apresento alguns pontos trabalhados na referida consultoria, para melhor entendimento:

Prevenção e Mitigação de Riscos: um plano de segurança e emergência permite identificar e avaliar os riscos potenciais dentro e ao redor da escola, acerca de ameaças como incêndios, desastres naturais, atiradores ativos e outros incidentes. Ao antecipar e compreender esses riscos, a escola pode adotar medidas preventivas e implementar estratégias de mitigação adequadas para reduzir a probabilidade de ocorrência desses eventos.

Resposta Rápida e Coordenada: um plano de segurança e emergência estabelece procedimentos claros e orientações para ação durante uma emergência. Todos os membros da comunidade escolar devem estar familiarizados com esses procedimentos e saber como responder de forma rápida e eficiente. Isso inclui evacuação segura, comunicação interna e externa, primeiros socorros básicos e outros protocolos específicos para cada tipo de incidente. A resposta coordenada e eficaz pode salvar vidas e minimizar o impacto de um incidente.

Tranquilidade para Estudantes, Pais e Funcionários: a existência de um plano de segurança e emergência oferece tranquilidade para os estudantes, pais e funcionários da escola. Saber que existem medidas de segurança em vigor e que a escola está preparada para lidar com emergências, reduz a ansiedade e promove um ambiente de aprendizado seguro. Demonstrando compromisso da escola em garantir a segurança de todos os envolvidos.

Treinamento e Conscientização: um plano de segurança e emergência não é eficaz apenas em sua existência, mas requer treinamento contínuo e conscientização por parte de todos os membros da comunidade escolar. Realizar exercícios de simulação, treinamentos regulares e campanhas de conscientização, ajuda a reforçar os protocolos de segurança e garantir que

todos estejam preparados para agir em caso de emergência. Alunos, professores, funcionários e até mesmo os pais, desempenham um papel importante no apoio ao plano de segurança.

Atualização e Melhoria Contínua: a implementação de um plano de segurança e emergência não deve ser vista como um evento único, mas sim como um processo contínuo de atualização e melhoria. À medida que novas ameaças surgem ou informações relevantes são adquiridas, o plano deve ser revisado e aprimorado para se manter relevante e eficaz. A colaboração com autoridades locais, especialistas em segurança e a comunidade escolar em geral, pode contribuir para o desenvolvimento de um plano de segurança abrangente e adaptado à realidade específica da escola.

Enfim, um plano de segurança e emergência é essencial para garantir um ambiente escolar seguro e protegido. Ele não apenas ajuda a prevenir e mitigar riscos, mas também permite uma resposta rápida e coordenada em emergências. Além disso, promove tranquilidade para estudantes, pais e funcionários, enquanto fomenta uma cultura de segurança e conscientização. Ao implementar e manter um plano de segurança e emergência eficaz, a escola demonstra seu compromisso com o bem-estar de todos os membros da comunidade escolar e reforça a importância da segurança como um valor fundamental na educação.

Dr. FABIANO SÉRGIO PAIVA DIAS DE SÁ, CPSI - Doutor em Ciencias de La Seguridad (Espanha). Mastér Superior en Direccion Internacional de Seguridad (Espanha). Pós-graduado em Planejamento e Gestão Estratégica. Pós-graduado em Administração e Logística. Diplomado Superior en Direccion Internadional Seguridad "DSDIS" (Espanha). Pós-graduado em Filosofia: Ensino da Filosofia pela Faculdade Católica de Rondônia. Pós-graduado em História e Arqueologia do Oriente Antigo e Mediterrâneo pela UNASP/Engenheiro Coelho - São Paulo. Certificado Profesional en Seguridad Internacional "CPSI" (Espanha). Diplomado Director Internacional de Seguridad "DIDS" (Espanha). Graduado em Processos Gerenciais pela Universidade Norte do Paraná - UNOPAR. Professional in Intelligence Analysis (CPAI). Extensão em Gestão Estratégica de Riscos: Interface da Norma ABNT ISO 31.000 e Ferramentas de Avaliação de Riscos da Norma ABNT ISO 31.010. BSC e a Gestão do Sistema de Segurança pela UNIVERSIDAD INTERNACIONAL DE SEGURIDAD (UNIVERIS - Espanha). Inteligencia y Contrainteligencia Empresarial. Seguridad Instalaciones Vitales pela Corporación Euro-Americana de Seguridad/CEAS-Brasil. Professor, palestrante e consultor.

Risco de Conformidade: Descubra como impacta nos negócios da empresa e como gerenciá-lo

José Sergio Marcondes, CES, CPSI

Conheça as consequências de ignorar o Risco de Conformidade e saiba quais são as melhores estratégias prevenir e fazer o gerenciamento desses tipos de riscos.

Risco de Conformidade refere-se à possibilidade de uma organização enfrentar consequências negativas devido ao não cumprimento de leis, regulamentos, normas e padrões relevantes que se aplicam às suas operações. É o risco associado a não aderir aos requisitos legais e éticos que governam a conduta e as atividades da empresa.

No mundo empresarial em constante evolução, a busca por excelência não se limita apenas ao crescimento financeiro e à inovação. A conformidade com as leis, regulamentos e padrões éticos é um pilar fundamental para a sustentabilidade e o sucesso a longo prazo de qualquer organização.

O Risco de Conformidade pode surgir de uma variedade de fatores que tornam as organizações suscetíveis a violações de regulamentos, normas e padrões. Esses fatores podem variar dependendo da indústria, localização e natureza das operações da organização.

No entanto, à medida que as regulamentações se tornam mais complexas e abrangentes, o desafio de gerenciar o “Risco de Conformidade” torna-se cada vez mais crucial. Este artigo de blog explora profundamente o universo do Risco de Conformidade empresarial, desvendando suas nuances, impactos e estratégias para mitigá-lo de maneira eficaz.

Definição de Conformidade

Conformidade, no contexto de gerenciamento de riscos empresariais, refere-se à aderência de uma organização às leis, regulamentos, normas, políticas internas e padrões relevantes que se aplicam às suas operações. Trata-se de garantir que a empresa esteja operando de acordo com as diretrizes estabelecidas, evitando infrações legais e riscos associados a não cumprir essas obrigações.

Além disso, a conformidade também envolve a adoção de práticas éticas e responsáveis, garantindo que a organização siga os princípios de integridade e transparência em todas as suas atividades. Isso não apenas ajuda a prevenir multas e penalidades, mas também contribui para a reputação positiva da empresa e para a confiança dos clientes, parceiros e stakeholders.

Quais são os fatores de influenciam a Conformidade Organizacional?

A conformidade organizacional é influenciada por uma variedade de fatores que interagem entre si para moldar a abordagem de uma empresa em relação ao cumprimento de regulamentos, normas e padrões. Esses fatores podem variar

de acordo com a indústria, o tamanho da organização e o contexto regulatório em que ela opera.

A seguir alguns dos principais fatores que influenciam a conformidade organizacional:

Regulamentações e Normas: As leis e regulamentos específicos que se aplicam à indústria e à localização da empresa têm um papel central na determinação dos requisitos de conformidade.

Complexidade Regulatória: Algumas indústrias enfrentam um conjunto intrincado de normas, enquanto outras têm requisitos mais simples. A complexidade afeta a quantidade de esforço necessário para garantir a conformidade.

Tamanho e Estrutura da Organização: Empresas maiores geralmente têm mais recursos para dedicar ao gerenciamento da conformidade, enquanto empresas menores podem enfrentar desafios adicionais na alocação de recursos.

Cultura Organizacional: Uma cultura que valoriza a ética e a responsabilidade tende a se alinhar mais naturalmente com esforços de conformidade.

Liderança e Engajamento: Quando a liderança demonstra a importância da conformidade e dá o exemplo, isso incentiva toda a organização a seguir os mesmos padrões.

Treinamento e Educação: A disponibilidade de treinamento adequado para os funcionários em relação às políticas e regulamentações é crucial para garantir que eles compreendam as regras e os requisitos que devem ser seguidos.

O que é Risco de Conformidade?

O Risco de Conformidade refere-se à possibilidade de uma organização enfrentar consequências negativas devido ao não cumprimento de leis, regulamentos, normas e padrões relevantes que se aplicam às suas operações. É o risco associado a não aderir aos requisitos legais e éticos que governam a conduta e as atividades da empresa.

Em outras palavras, é a ameaça de prejuízos resultantes da falha em aderir aos requisitos legais e regulatórios que governam as operações e conduta da empresa. O gerenciamento eficaz do risco de conformidade envolve a identificação, avaliação, mitigação e monitoramento contínuo das potenciais violações, visando garantir a conformidade constante e a minimização de impactos negativos.

Quais são as principais origem dos Risco de Conformidade?

Esse tipo de risco pode surgir de diversas origens, incluindo:

Regulamentações Governamentais: Violações de leis federais, estaduais ou locais podem resultar em multas, penalidades financeiras ou outras ações legais.

Normas Setoriais: Muitas indústrias têm normas específicas que as empresas devem seguir para operar de maneira segura e ética. O não cumprimento dessas normas pode levar a consequências negativas.

Padrões Internacionais: Em um cenário globalizado, empresas que operam em várias jurisdições podem enfrentar desafios de conformidade com diferentes normas e regulamentos em cada país.

Contratos e Acordos: Violações de contratos com clientes, fornecedores ou parceiros podem resultar em litígios legais e danos à reputação.

Questões Ambientais: Não cumprir regulamentos ambientais pode resultar em multas e responsabilidades legais, além de danos à imagem da empresa.

Proteção de Dados: No contexto da privacidade e proteção de dados, o não cumprimento das leis de privacidade pode levar a multas substanciais e perda de confiança do cliente.

Segurança do Trabalho: O não cumprimento das normas de segurança e saúde ocupacional pode resultar em acidentes, ações legais e penalidades.

Ética Empresarial: O não cumprimento de padrões éticos pode prejudicar a reputação da empresa e afetar a confiança dos stakeholders.

Quais são os fatores geradores de Risco de Conformidade?

O Risco de Conformidade pode surgir de uma variedade de fatores que tornam as organizações suscetíveis a violações de regulamentos, normas e padrões. Esses fatores podem variar dependendo da indústria, localização e natureza das operações da empresa.

A seguir alguns dos principais fatores geradores de Risco de Conformidade:

Rápidas Mudanças Regulatórias: Alterações frequentes nas leis e regulamentos podem pegar as organizações desprevenidas, dificultando a adaptação rápida e completa.

Falta de Conhecimento: Funcionários não familiarizados com as regulamentações e políticas da empresa podem inadvertidamente violar regras por falta de conhecimento.

Falta de Treinamento: Treinamento inadequado sobre políticas, regulamentações e procedimentos pode levar a erros de conformidade.

Falta de Supervisão: Falhas na supervisão e monitoramento das atividades dos funcionários podem resultar em práticas não conformes.

Cultura Organizacional: Uma cultura que não valoriza a conformidade e a ética pode levar a comportamentos de alto risco.

Pressão por Resultados: Expectativas não realistas de desempenho podem levar os funcionários a contornar regulamentos para atingir metas.

Falta de Recursos: Recursos financeiros, humanos e tecnológicos insuficientes podem prejudicar os esforços de conformidade.

Mudanças na Equipe: Rotatividade de funcionários ou mudanças de liderança podem afetar a consistência das práticas de conformidade.

Falhas em Processos Internos: Processos internos mal projetados ou ineficientes podem levar a erros de conformidade.

Quais são os principais Tipos de Risco de Conformidade?

Existem diversos tipos de Risco de Conformidade que uma organização pode enfrentar, cada um associado a diferentes aspectos regulatórios, normativos e éticos. Aqui estão alguns dos principais tipos de Risco de Conformidade:

Risco Legal: Refere-se à possibilidade de enfrentar processos legais, multas ou penalidades por violar leis e regulamentos governamentais.

Risco Regulatório: Está relacionado à falta de aderência às normas e regulamentos específicos do setor em que a organização opera.

Risco de Privacidade de Dados: Relacionado à não conformidade com regulamentações de proteção de dados.

Risco Ambiental: Envolve o não cumprimento das regulamentações ambientais, resultando em multas, sanções e danos à reputação.

Risco de Concorrência: Refere-se a violações das leis de competição, que podem resultar em multas substanciais e ações judiciais.

Risco de Lavagem de Dinheiro: Está associado à falta de conformidade com regulamentações que visam evitar o uso indevido de fundos para atividades ilegais.

Risco de Saúde e Segurança Ocupacional: Envolve a não conformidade com normas de saúde e segurança no local de trabalho, resultando em acidentes e litígios.

Risco de Fraude e Corrupção: Refere-se a práticas fraudulentas ou corruptas que podem levar a penalidades e danos à reputação.

Risco de Publicidade e Marketing: Refere-se ao não cumprimento das regulamentações de publicidade e marketing, resultando em penalidades e danos à reputação.

Risco de Fraude Financeira: Está ligado a práticas financeiras fraudulentas, que podem levar a litígios legais e perda de confiança dos investidores.

Quais são as principais Consequências do Risco de Conformidade?

O Risco de Conformidade pode resultar em uma série de consequências negativas para uma organização, abrangendo desde impactos financeiros até danos à reputação. A seguir algumas das principais consequências que podem surgir do não cumprimento das regulamentações, normas e padrões:

Multas e Penalidades: A violação de regulamentações pode levar a multas substanciais impostas por autoridades regulatórias, o que pode impactar diretamente as finanças da empresa.

Litígios Legais: A não conformidade pode resultar em ações legais movidas por reguladores, clientes, fornecedores ou outras partes afetadas.

Danos Financeiros: Além de multas, as consequências financeiras podem incluir custos legais, indenizações e despesas relacionadas à correção de problemas de conformidade.

Perda de Receita: Ações legais, multas e uma má reputação podem afetar negativamente a capacidade da empresa de atrair clientes e parceiros, levando a perda de receita.

Danos à Reputação: A perda de confiança dos clientes, parceiros e stakeholders devido a violações de conformidade pode ter um impacto duradouro na reputação da empresa.

Restrições Operacionais: Reguladores podem impor restrições ou exigir mudanças nas operações da empresa como resultado de violações de conformidade.

Perda de Licenças e Autorizações: Violações graves de conformidade podem resultar na perda de licenças, permissões ou certificações necessárias para operar.

Perda de Clientes e Parceiros: Clientes e parceiros podem optar por não fazer negócios com uma empresa que demonstrou problemas de conformidade.

Essas consequências podem variar de acordo com a gravidade das violações de conformidade e o setor em que a empresa opera. Portanto, a gestão eficaz do Risco de Conformidade é essencial para evitar ou mitigar essas consequências potencialmente prejudiciais.

Como prevenir o risco o Risco de Conformidade?

Prevenir o Risco de Conformidade é uma parte essencial do gerenciamento de riscos empresariais. Implementar medidas proativas para garantir a aderência às leis, regulamentos, normas e padrões relevantes é fundamental para evitar consequências negativas. A seguir algumas estratégias e práticas para prevenir o Risco de Conformidade:

Conhecimento das Regulamentações: Mantenha-se atualizado sobre as leis, regulamentos e normas que se aplicam ao seu setor e localização. Isso inclui regulamentações governamentais, normas setoriais e normas internacionais.

Programas de Conformidade: Desenvolva e implemente programas de conformidade robustos, incluindo políticas claras, procedimentos detalhados e orientações para funcionários.

Treinamento e Educação: Forneça treinamento regular e educação aos funcionários sobre as regulamentações e políticas da empresa, garantindo que eles compreendam as expectativas de conformidade.

Cultura de Ética: Promova uma cultura organizacional que valoriza a ética e a responsabilidade, incentivando os funcionários a agir de maneira ética em todas as situações.

Auditorias Internas: Realize auditorias internas regulares para avaliar a eficácia dos programas de conformidade e identificar áreas de melhoria.

Avaliação de Riscos: Identifique, avalie e trate os riscos de conformidade específicos associados às operações da sua organização, considerando fatores internos e externos.

Ao adotar uma abordagem abrangente de prevenção de Risco de Conformidade, as empresas podem reduzir significativamente a probabilidade de violações, multas, penalidades e danos à reputação, garantindo operações mais éticas, eficientes e sustentáveis.

Como gerenciar o Risco de Conformidade?

O gerenciamento de riscos de conformidade é um processo estruturado que envolve a identificação, avaliação, tratamento e monitoramento dos riscos associados à não conformidade com leis, regulamentos, normas e padrões éticos. Aqui estão as etapas-chave desse processo:

Identificação de Riscos: A primeira etapa envolve a identificação de todos os possíveis riscos de conformidade que a organização pode enfrentar. Isso inclui a análise das regulamentações aplicáveis ao setor, bem como a compreensão das vulnerabilidades internas que podem resultar em não conformidade.

Avaliação de Riscos: Nesta etapa, os riscos identificados são avaliados quanto à sua probabilidade de ocorrência e ao impacto potencial. Isso permite priorizar os riscos com base em sua gravidade e urgência.

Tratamento de Riscos: Com base na avaliação, os riscos são tratados por meio da implementação de estratégias apropriadas. Isso pode incluir ações para evitar, mitigar, transferir ou aceitar os riscos. Por exemplo, implementar controles internos, revisar processos ou buscar seguro para cobrir certos riscos.

Monitoramento de Riscos Residuais: Depois que as estratégias de tratamento são implementadas, é crucial monitorar os riscos residuais que permanecem. Isso envolve avaliar regularmente a eficácia dos controles implementados e identificar quaisquer mudanças nas circunstâncias que possam afetar a exposição aos riscos.

Programas Implementados: Durante todo o processo de gerenciamento de riscos de conformidade, programas específicos são implementados para garantir a aderência contínua às regulamentações. Esses programas podem incluir políticas, procedimentos, treinamentos, auditorias e sistemas de monitoramento.

O objetivo final do gerenciamento de riscos de conformidade é garantir que a organização esteja em conformidade com todas as regulamentações relevantes, minimizando os riscos de multas, penalidades e danos à reputação. Ao seguir essas etapas de forma contínua, as organizações podem criar uma cultura de conformidade sólida e eficaz.

Cite exemplos práticos de risco de conformidade?

Certamente, aqui estão alguns exemplos práticos de Risco de Conformidade em diferentes setores:

Risco de Privacidade de Dados (GDPR): Uma empresa de tecnologia coleta dados pessoais de clientes sem o devido consentimento ou não protege

adequadamente esses dados, resultando em multas substanciais de acordo com o Regulamento Geral de Proteção de Dados.

Risco de Ética Empresarial: Uma empresa de manufatura não segue práticas éticas em suas operações, incluindo o uso de trabalho infantil, resultando em investigações regulatórias, boicotes de clientes e danos à reputação.

Risco de Saúde e Segurança Ocupacional: Uma construtora não fornece equipamentos de segurança adequados para seus trabalhadores, resultando em acidentes e lesões graves, levando a multas e litígios.

Risco Ambiental: Uma empresa química descarta resíduos tóxicos de maneira inadequada, poluindo os recursos hídricos locais e enfrentando multas regulatórias e custos de limpeza.

Risco de Publicidade Enganosa: Uma empresa de produtos de saúde faz alegações exageradas sobre os benefícios de seus produtos em suas campanhas de marketing, resultando em multas e ações legais por publicidade enganosa.

Conclusão:

Em um mundo onde a transparência e a responsabilidade são cada vez mais valorizadas, o Risco de Conformidade emerge como um desafio incontornável para organizações de todos os tamanhos e setores. Reconhecer a importância de manter a conformidade é um passo fundamental para o sucesso sustentável.

Como vimos ao longo deste artigo, as consequências de não gerenciar adequadamente o Risco de Conformidade podem ser graves. No entanto, a boa notícia é que existem estratégias eficazes de prevenção, monitoramento e correção que podem ser implementadas para mitigar esses riscos e manter uma cultura de conformidade robusta.

À medida que avançamos em direção a um ambiente de negócios cada vez mais complexo e regulamentado, o conhecimento sobre o Risco de Conformidade se torna um pré-requisito para o sucesso. Empresas de sucesso adotam as melhores práticas de gerenciamento de riscos para se manterem protegidas dos diversos tipos de risco existentes no seguimento que atuam.

José Sergio Marcondes, CES, CPSI – Gestor, Consultor e Diretor do IBRASEP.

Segurança Global e Infraestruturas Críticas

Manuel Sánchez Gómez-Merelo

A globalização tem marcado o ritmo das capacidades do Estado e da comunidade e das suas infraestruturas, que vivem este processo com um aumento da insegurança.

Hoje, os riscos e ameaças vêm em muitas dimensões e formas, decorrentes da instabilidade geopolítica, crime e terrorismo, catástrofes naturais e, mais recentemente, pandemias globais e a guerra na Ucrânia.

Temos de estudar as grandes mudanças e tendências que vivemos, diferenciando os riscos económicos, políticos e de segurança que nos esperam, de forma a desenhar um novo cenário futuro em que um modelo de governação de segurança global seja capaz de responder aos novos desafios e requisitos de prevenção e proteção.

A segurança deve ser entendida, portanto, como um processo global, integral e integrado, constituído por todos os elementos técnicos, materiais, humanos e organizacionais relacionados ao sistema e seu funcionamento.

Infraestruturas Críticas e Estratégicas

Conforme definição prévia, entende-se por infraestruturas críticas e estratégicas "Aquelas instalações, redes, serviços e equipamentos físicos e tecnologias sobre os quais assenta o funcionamento de serviços essenciais e cuja interrupção ou destruição produziriam maior impacto na saúde, na segurança ou na economia e bem-estar social dos cidadãos ou no efetivo funcionamento da Administração".

Com o objetivo de alcançar um grau adequado de proteção em instalações estratégicas classificadas como infraestruturas críticas, contra os riscos ou ameaças de eventos ou atos ilícitos deliberados que afetem a proteção do sistema, o Secretário de Estado da Segurança aprova as revisões dos Planos de Proteção, competência atribuída ao Ministério do Interior.

Segurança global

Nas últimas décadas, a segurança global tornou-se uma prioridade fundamental na Espanha. Desafios como o combate ao terrorismo e ao crime organizado ou o especial impacto na cibersegurança são fundamentais na nossa política interna e externa.

A segurança global é um dos pilares fundamentais sobre os quais as organizações devem assentar, devendo ser entendida como um objetivo abrangente e integrado cuja finalidade é a proteção de pessoas e bens ou bens, para além de servir para proteger interesses e objetivos estratégicos ou de funcionamento essencial.

O contexto em que se insere e a importância que a segurança global assume e assumirá exigem novos tipos de análise e conhecimento multidisciplinar das soluções a aplicar.

Deve-se levar em consideração que o conceito de segurança global é especialmente importante no campo da proteção de infraestrutura crítica (CIP). Para isso, deve ser estabelecida uma Política Geral de Segurança Global, onde aspectos fundamentais devem ser levados em consideração, como: a proteção de serviços essenciais; gestão estratégica de segurança alinhada com a política de riscos; a estrutura organizacional e as responsabilidades em termos de segurança integral; a responsabilidade, empenho 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; conformidade regulatória e aplicação de boas práticas; e a melhoria contínua dos processos de segurança implementados.

A prevenção no sistema PIC contra ataques deliberados é a espinha dorsal sobre a qual assenta o enquadramento dos diferentes planos que os chamados operadores críticos devem elaborar para garantir a segurança das infraestruturas. Assim, o impacto será priorizado sobre a probabilidade, garantindo que qualquer infraestrutura seja prevenida de um ataque deliberado, independentemente da probabilidade de sofrer.

Por isso, os Planos de Segurança do Operador (PSO) e os Planos de Proteção Específica (PPE), coordenados pelo Centro Nacional de Proteção de Infraestruturas Críticas (CNPIC) e fiscalizados pelas Forças e Corpos de Segurança, que também cooperam na preparação e a avaliação dos Planos Estratégicos Setoriais e Planos de Apoio Operacional, constituem o elemento essencial da prevenção de riscos e ameaças.

Infraestruturas críticas e segurança global

Do ponto de vista da segurança global, temos que ajudar as organizações públicas e privadas a desenhar novas estratégias em um mundo globalizado que continua a se desenvolver.

Só a segurança global, integral e integrada garante uma proteção eficaz contra ameaças globais e, para isso, temos de redefinir as políticas de segurança, criar uma nova cultura de segurança integral, estabelecer mecanismos de controlo e gestão da segurança física e lógica, monitorizar o sistema de segurança e avaliar a resiliência.

Uma nova redefinição e uma nova oportunidade de avançar em Segurança Global em um mundo de desafios e demandas coletivas e um futuro incerto, com a necessidade de entender as novas dinâmicas sociais, econômicas, energéticas e tecnológicas para promover o desenvolvimento desse conceito amplo de nova cultura de segurança que está se tornando cada vez mais presente.

Os desafios sugeridos pelo novo contexto global de riscos e ameaças exigem soluções inovadoras de segurança, tanto na esfera pública quanto na privada, que incorporem inteligência e tecnologia como base de uma estratégia de segurança necessária para operar nas organizações e na sociedade como um todo, mas sem esquecendo que o valor social contribui para a criação de valor econômico, e vice-versa, sendo indesculpável considerar os dois tipos de valores como um todo.

Com isso, podemos oferecer soluções holísticas para a Gestão de Riscos de Infraestruturas Críticas e Estratégicas que, sem dúvida, requerem produtos e serviços de segurança adequados aos seus riscos, ameaças e vulnerabilidades específicos.

Devemos ser capazes de entender o atual ecossistema de segurança global e realizar uma análise aprofundada de suas falhas e dos desafios mais importantes que enfrenta. Para isso, o impacto da globalização e das mudanças sociais e econômicas que estamos vivendo na segurança e suas organizações devem ser estudados em profundidade. É necessário identificar as grandes tendências de segurança, além de alguns dos riscos em infraestruturas críticas, avaliar o seu possível impacto e poder analisar as complexidades na tomada de decisões, sem esquecer a importância da liderança em segurança a nível internacional, calculando as suas capacidades e resiliência.

A Comissão Europeia propôs o reforço da resiliência da infraestrutura da UE através de um "Plano de Cinco Pontos para Infraestrutura Crítica Resiliente" , apresentado no Parlamento Europeu. Este plano visa proteger infraestruturas críticas em três áreas prioritárias: preparação, resposta e cooperação internacional. Para o efeito, prevê um papel de apoio e coordenação da Comissão, para melhorar a preparação e resposta às ameaças atuais mais importantes, bem como uma cooperação reforçada entre os Estados-Membros e com os países terceiros vizinhos. Deve-se notar que é priorizado nos setores-chave de energia, infraestrutura digital, transporte e espaço.

Novos desafios e novas respostas globais que exigem também uma visão partilhada, a par da preparação adequada de cada vez mais profissionais, executivos e operacionais, que devem credenciar formação e formação especializada, não linear, assente em estratégias e pensamentos exponenciais e abertos. flexíveis, o que os torna os líderes de segurança de que precisamos.

Os Administradores de Segurança (CSO e CISO), marcados por diversas situações como a recente pandemia, a aceleração da transformação digital, a globalização dos riscos e ameaças, etc., encontram-se motivados a continuar a desenvolver as suas carreiras face a novos desafios, problemas globais com um horizonte maior e uma visão cooperativa.

A implementação e gestão da Segurança Integral e Integrada requer uma nova figura com uma visão holística e executiva, um novo Diretor de Segurança Global.

Até recentemente, integrar a segurança física e lógica sob um único responsável como Diretor de Segurança era uma decisão voluntária com vista à otimização de recursos, que algumas organizações têm vindo a adotar, mas, sobretudo pelo

que aconteceu nos últimos anos, já não é uma questão de otimização, mas tornou-se inevitável e irreversível, especialmente quando se trata de entidades ou infraestruturas críticas ou estratégicas.

Por tudo isto, é necessário rever as políticas de segurança, criando uma nova cultura de segurança global, abrangente e integrada, estabelecendo mecanismos de controlo e gestão da segurança física e lógica e, sobretudo, tendo em conta a implementação dos novos sistemas e o reforço da resiliência.

O objetivo é propor a nova cultura da segurança como bem público, fomentando a evolução e o desenvolvimento de um paradigma de segurança de valor compartilhado, que vai do global ao local.

No campo da cultura de segurança nacional, o ano de 2022 fica marcado pela consolidação da estrutura que permitirá o desenvolvimento do Plano Integral de Cultura de Segurança Nacional. Assim, o Conselho de Ministros acordou as regras de funcionamento, tanto do Grupo Interministerial de Acompanhamento e Avaliação da Cultura de Segurança Nacional, como do Fórum Integral de Cultura de Segurança Nacional.

Estamos diante de uma nova mudança de paradigma na Segurança Global (integral e integrada, pública e privada) como resposta aos novos e grandes desafios e demandas decorrentes do avanço da globalização.

Queremos progresso e bem-estar para todos, mas não podemos esquecer o seu preço. Qualquer novo empreendimento implica o custo de sua implantação, mais o de seus estudos de impacto e consequências, seu cuidado, seu bom uso, sua manutenção e a capacitação permanente das pessoas que garantem o perfeito funcionamento e proteção das vidas e bens envolvidos.

Dimensionar a segurança que cada inovação, evolução ou investigação requer deve ser um requisito essencial, sem o qual nenhum progresso pode ser feito.

Vamos crescer, mas não verticalmente ou horizontalmente, mas de forma esférica, integradora e consciente, para que o bem do todo seja antecipadamente contemplado e detectados os riscos e ameaças que qualquer desarmonia pode produzir. Só assim a segurança adquire a sua dimensão mais importante, que, tal como na medicina, é preventiva.

Manuel Sánchez Gómez-Merelo

Consultor Internacional de Seguridad. Presidente · Director General de GET – Grupo Estudios Técnicos. Director de Programas de Protección de Infraestructuras Críticas en el Instituto Universitario General Gutierrez Mellado IUGM-UNED. http://www.manuelsanchez.com

Sistemas de Gestão de Continuidade de Negócios – ISO 22313: Liderança e Comprometimento

Flavio Fleury de Souza Lima, MBCR, CEGRC, CIEAC, CISI, CIGR

Liderança e comprometimento

A liderança e o comprometimento são elementos fundamentais para o sucesso da continuidade de negócios.

Neste sentido, é essencial que a alta administração demonstre um comprometimento claro com a continuidade de negócios. Isso envolve a alocação de recursos adequados, a definição de metas e objetivos claros e a comunicação regular sobre sua importância para a organização.

Nomear um líder responsável pela continuidade de negócios é crucial. Essa pessoa deve ter autoridade e recursos para implementar e manter esses planos, além de coordenar as atividades relacionadas.

A liderança deve envolver no processo de continuidade de negócios todas as partes interessadas relevantes, tais como funcionários, fornecedores e clientes. Isso pode ser feito por meio de treinamentos, workshops e comunicação regular para garantir que todos estejam cientes de suas responsabilidades e do papel que desempenham no processo.

Cabe à liderança promover uma cultura organizacional que valorize a continuidade de negócios. Isso pode ser alcançado por meio da conscientização, educação e incentivos para a conformidade com os planos de continuidade.

A liderança deve, ainda, estar comprometida com a revisão e melhoria contínua dos planos. Isso envolve a análise regular dos resultados dos testes, a identificação de áreas de melhoria e a implementação de ações corretivas.

Liderança e comprometimento são fundamentais para estabelecer uma cultura de continuidade de negócios e garantir que os planos sejam eficazes e atualizados.

Estabelecendo uma Política de GCN

Assim como uma liderança e o comprometimento são elementos fundamentais para o sucesso da continuidade de negócios, uma política de continuidade de negócios é essencial para garantir que uma organização possa continuar operando mesmo diante de interrupções ou desastres.

É necessário que se identifiquem os riscos que podem afetar a continuidade dos negócios, como desastres naturais, falhas de infraestrutura, ataques cibernéticos, entre outros, avaliando também o impacto que cada risco

identificado pode ter nas operações da empresa. Isso ajudará a priorizar os esforços de continuidade.

Os planos de continuidade devem ser criados de forma detalhada para lidar com cada risco identificado. Isso pode incluir planos de recuperação de desastres, planos de resposta a incidentes de segurança cibernética, planos de contingência, entre outros.

Devem ser realizados testes regulares desses planos para garantir que eles sejam eficazes. Além disso, é importante treinar os funcionários para que saibam como agir em caso de interrupções.

Deve-se revisar e atualizar regularmente os planos de continuidade para que eles permaneçam alinhados com as mudanças na organização e no ambiente de negócios.

Comunicando a Política de Continuidade de Negócios

A comunicação da política de continuidade de negócios é um aspecto fundamental para garantir que todos os envolvidos na organização estejam cientes das diretrizes e procedimentos a serem seguidos em caso de interrupções ou crises.

A comunicação eficaz dessa política envolve a disseminação clara e abrangente das informações relevantes para todos os funcionários, parceiros de negócios e partes interessadas. Isso pode ser feito por meio de diferentes canais de comunicação, como reuniões, treinamentos, intranet, e-mails, boletins informativos, entre outros.

É importante que sua comunicação seja feita de forma regular e consistente, para que todos estejam atualizados sobre as medidas de continuidade de negócios e saibam como agir em situações de crise. A comunicação deve também ser adaptada ao público-alvo, utilizando uma linguagem clara e acessível, de modo a garantir que todos compreendam as informações transmitidas.

Além disso, a comunicação deve incluir a divulgação dos planos de ação e procedimentos a serem seguidos em casos de interrupções ou crises. Isso pode envolver a criação de manuais de referência, fluxogramas e outros materiais que auxiliem os funcionários a entender como agir em diferentes cenários.

A comunicação também desempenha um papel importante na conscientização e engajamento dos funcionários em relação à política de continuidade de negócios. É essencial que todos os colaboradores compreendam a importância da continuidade das operações e estejam motivados a seguir as diretrizes estabelecidas.

Em resumo, a comunicação eficaz da política de continuidade de negócios é essencial para garantir que todos os funcionários e partes interessadas estejam cientes das diretrizes e procedimentos a serem seguidos em caso de

interrupções ou crises. Isso ajuda a minimizar os impactos e garantir a continuidade das operações da empresa.

É importante ter em mente que uma política de continuidade de negócios deve ser adaptada às necessidades específicas da sua organização. É recomendável buscar a orientação de especialistas em continuidade de negócios para garantir que todos os aspectos relevantes sejam considerados.

O **Software INTERISK** dispõe de um **Módulo específico de Gestão de Continuidade de Negócios** totalmente parametrizável em função das necessidades do cliente. Essa ferramenta pode se tornar uma grande aliada na estruturação de um Sistema de Gestão de Continuidade de Negócios para sua organização.

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

Vigilante Condutor de Cães: Conheça as características e atribuições dessa função

José Sergio Marcondes, CES, CPSI

Descubra como é a função de vigilante condutor de cães. Saiba o que é necessário para atuar na função, o que faz, responsabilidades e importância p/ segurança.

O Vigilante Condutor de Cães é um profissional de segurança privada, devidamente habilitado para a condução cães, que atua em conjunto com cães adestrados para a proteção de pessoas, patrimônios e áreas específicas. Esses profissionais são responsáveis por conduzir e controlar os cães adestrados durante as operações de vigilância privada.

No universo dinâmico da segurança privada, existe um profissional especializado que desempenha um papel essencial no reforço da proteção patrimonial: o vigilante condutor de cães. Combinando a eficiência da vigilância humana com o instinto protetor dos cães treinados, essa função tem se tornado cada vez mais relevante no cenário atual.

Os cães, por sua natureza leal e instintos protetores, têm sido parceiros valorosos dos seres humanos há séculos. Na segurança privada, essa parceria evoluiu para uma estratégia de segurança patrimonial. Onde o vigilante condutor de cães é a figura central nessa abordagem, combinando o adestramento do animal com a experiência e conhecimento do profissional de segurança.

Neste artigo, abordaremos a função do Vigilante Condutor de Cães, conheceremos os requisitos necessários para ingressar nessa função, suas atribuições e responsabilidades, estratégias de emprego e importância estratégica para a atividade da vigilância patrimonial.

O que é um Vigilante Condutor de Cães?

O Vigilante Condutor de Cães é um profissional de segurança privada, devidamente habilitado para conduzir cães adestrados e atuar em conjunto com eles para a proteção de pessoas, patrimônios e áreas específicas. Esses profissionais são responsáveis por conduzir e controlar os cães adestrados durante as operações de vigilância patrimonial.

A Portaria Nº 18.045, de 17 de abril de 2023, autoriza e disciplina a utilização de cães na segurança privada, desde que o cão seja adequadamente adestrado e sempre acompanhado por vigilantes devidamente habilitados para a condução do animal.

Os cães utilizados na segurança privada devem ser adequadamente treinados para identificar e responder a situações de risco, detectar intrusos, realizar rondas e auxiliar em ações de intervenção em situações de emergência.

O Vigilante Condutor de Cães deve trabalhar em conjunto com esses animais, estabelecendo uma parceria que potencialize a eficiência e a capacidade de dissuasão, detecção de ameaças e resposta efetiva em diversas situações. Os cães podem ser empregados para atividades de vigilância patrimonial em empresas, condomínios, eventos ou outros locais, proporcionando um nível adicional de segurança.

O que faz um Vigilante Condutor de Cães?

Um Vigilante Condutor de Cães tem como principal função conduzir e controlar cães adestrados nas atividades de vigilância patrimonial. Suas responsabilidades incluem:

1. Realizar rondas de segurança em áreas específicas, utilizando o cão para auxiliar na detecção de intrusos ou atividades suspeitas.
2. Empregar o cão como um recurso adicional de proteção e detecção, potencializando a eficiência das ações de segurança.
3. Colaborar com a equipe de segurança, comunicando informações relevantes obtidas por meio do cão durante as rondas.
4. Participar de ações de intervenção em situações de emergência ou risco, com o auxílio do cão para imobilizar possíveis ameaças.
5. Reciclar o adestramento dos cães para responder a comandos e situações de risco, garantindo que o animal esteja preparado para agir de forma adequada durante as operações.
6. Cuidar da saúde e bem-estar do cão, garantindo que ele esteja em boas condições para o trabalho e receba os cuidados necessários.
7. Seguir os protocolos, normas e procedimentos de segurança estabelecidos pela empresa ou contratante, no que se refere ao emprego do cão, garantindo o cumprimento das diretrizes do serviço.

O Vigilante Condutor de Cães desempenha um papel fundamental na segurança patrimonial, utilizando a habilidade e instintos do cão aliados ao seu conhecimento técnico e habilidades para garantir um ambiente mais seguro e protegido.

Qual a importância do Vigilante Condutor de Cães?

O Vigilante Condutor de Cães desempenha um papel de extrema importância na segurança patrimonial. A presença de um cão adestrado e conduzido por um vigilante habilitado traz diversos benefícios, que incluem:

1. **Eficiência na detecção**: Os cães têm um olfato apurado e aguçado senso de audição, o que os torna excelentes na detecção de intrusos ou atividades suspeitas. Eles podem identificar pessoas ou objetos ocultos, mesmo em locais de difícil acesso.

2. **Aumento do perímetro de segurança**: Com a ajuda dos cães, o vigilante consegue cobrir uma área maior durante as rondas, proporcionando uma proteção mais abrangente.
3. **Desestímulo aos infratores**: A presença de cães devidamente treinados é uma forte medida dissuasória contra possíveis invasores ou criminosos, reduzindo a probabilidade de incidentes.
4. **Resposta rápida**: Os cães respondem prontamente a comandos do vigilante, permitindo uma reação rápida em situações de emergência ou risco.
5. **Parceria leal**: O vínculo entre o vigilante e o cão é de confiança e lealdade, criando uma parceria que contribui para o trabalho de segurança de forma mais efetiva.
6. **Melhoria do bem-estar no ambiente**: A presença amigável e ao mesmo tempo imponente dos cães pode proporcionar maior sensação de segurança a funcionários, moradores e frequentadores de determinado local.
7. **Trabalho em equipe**: O vigilante condutor de cães trabalha em estreita colaboração com o animal, reforçando a interação e garantindo o bom desempenho das atividades.

Portanto, o vigilante condutor de cães é uma ferramenta valiosa para otimizar a segurança, proteger propriedades e garantir a tranquilidade das pessoas envolvidas em ambientes que necessitam de uma vigilância mais aprimorada.

Quem pode ser Vigilante Condutor de Cães?

Para ser um vigilante condutor de cães, é necessário atender a alguns requisitos específicos previstos na legislação que disciplina as atividades da segurança privada no País, que incluem:

1. **Formação como vigilante:** O candidato deve ter concluído o Curso de Formação de Vigilantes, que é obrigatório para exercer a profissão.
2. **Habilitação específica**: Deve ser aprovado em Curso de Vigilante Condutor de Cães em órgão militar ou policial, Kennel Club ou empresa de curso de formação, onde deverá ser ministrado treinamento prático para condução do cão em serviço.
3. **Aptidão física e emocional**: A atividade de conduzir cães de segurança exige boa aptidão física e controle emocional, uma vez que o trabalho pode envolver situações desafiadoras e de alto estresse.
4. **Afinidade com cães**: A afinidade com cães é um fator importante para o sucesso da atuação desse profissional, pois ele estará trabalhando diretamente com os animais e será responsável pelo treinamento, manejo e cuidado dos cães de guarda, para tanto deve sentir vontade e prazer em trabalhar com cães.

Quais sãos as responsabilidades de um Vigilante Condutor de Cães?

As responsabilidades de um Vigilante Condutor de Cães são variadas e envolvem cuidar e utilizar os cães adestrados de forma adequada para garantir a segurança do local ou evento onde atua. Algumas das principais responsabilidades desse profissional incluem:

1. **Adestramento dos cães**: O vigilante condutor é responsável por revisar periodicamente o adestramento dos cães de segurança para que respondam corretamente aos comandos e sejam eficazes em suas funções de proteção.
2. **Manutenção da saúde dos cães**: Cuidar da saúde e bem-estar dos cães é essencial. Isso inclui garantir que recebam alimentação adequada, cuidados veterinários, exercícios físicos e condições adequadas de alojamento.
3. **Patrulhas e rondas**: O vigilante condutor realiza patrulhas e rondas no perímetro designado, acompanhado pelos cães. Essas rondas são fundamentais para detectar qualquer atividade suspeita ou ameaça.
4. **Intervenção em situações de risco**: Quando necessário, o vigilante condutor utiliza os cães adestrados para intervir em situações de risco, como abordagem de pessoas suspeitas ou tentativas de invasão em áreas protegidas.
5. **Trabalho em equipe**: O vigilante condutor trabalha em conjunto com outros vigilantes e equipe de segurança para garantir a eficiência e o sucesso das operações.
6. **Registro de ocorrências**: Manter registros precisos de ocorrências, atividades realizadas e qualquer incidente relevante é parte importante das responsabilidades do vigilante condutor.
7. **Segurança do público e dos cães**: Assegurar a segurança não apenas do local onde atua, mas também do público presente, é uma das principais preocupações do vigilante condutor.
8. **Cumprimento das normas**: O vigilante condutor deve cumprir todas as normas e regulamentos relacionados ao uso e condução de cães de segurança, bem como respeitar as leis aplicáveis ao exercício de suas funções.

É importante destacar que as responsabilidades do Vigilante Condutor de Cães podem variar de acordo com a empresa de segurança, o tipo de local ou evento onde atua e as regulamentações locais vigentes. O profissional deve sempre atuar com ética, responsabilidade e dedicação para garantir a segurança de todos os envolvidos.

Qual o salário de um Vigilante Condutor de Cães?

O salário de um Vigilante Condutor de Cães pode variar de acordo com a região do País em função de acordos coletivos de trabalho, Além do piso base da categoria, de acordo com a Convenção Coletiva de Trabalho da região o vigilante condutor pode receber uma gratificação de função de 10% sobre o piso base.

Por exemplo: No estado de São Paulo, o piso base do Vigilante/Condutor de Cães é de R$1.845,56 + 10% = R$ 2.030,116

As gratificações de função descritas são devidas somente durante o período em que o empregado exercer a função gratificada e não são cumulativas, de forma que, em caso de exercício de mais de uma função gratificada, o empregado perceberá o valor correspondente àquela de maior valor, somente durante o período em que perdurar o exercício da referida função

Conclusão

Ao longo deste artigo abordamos a função do “Vigilante Condutor de Cães”. Exploramos como essa profissão especializada combina habilidades humanas com o companheirismo canino para proporcionar uma camada a mais de segurança e proteção.

Descobrimos os requisitos para exercer a função de vigilante condutor, suas funções, responsabilidades, e a importância para segurança privada. Vimos que os cães são uma ferramenta valiosa na prevenção de incidentes e na identificação de riscos em diversos cenários.

Se você se interessou por esse assunto importante para vigilância patrimonial e deseja se aprofundar ainda mais, não perca a oportunidade de ler nosso próximo artigo sobre o “Curso de Vigilante Condutor de Cães“. Descubra como é a capacitação do vigilante para condução de cães adestrados na segurança privada,

José Sergio Marcondes, CES, CPSI - Gestor, Consultor e Diretor do IBRASEP. Profissional com competências sólidas na área de segurança privada e gestão empresarial.

Condutor de Veículos: Saiba o que faz e como contribui para eficácia da segurança Vigilante

José Sérgio Marcondes, CES, CPSI

Conheça o papel do Vigilante Condutor de Veículos na segurança privada. Saiba o que faz, as responsabilidades e contribuições para uma proteção mais eficaz

O Vigilante Condutor de Veículos é um profissional da área de segurança privada que possui a função de dirigir veículos motorizados, como carros e motos, para desempenhar atividades de vigilância e proteção. Ele combina as habilidades de vigilância com a capacidade de conduzir veículos de forma segura e eficiente, tornando-se essencial para garantir rondas e deslocamentos rápidos em diferentes cenários.

O vigilante condutor de veículos desempenha uma série de funções relacionadas à segurança e à mobilidade, combinando habilidades de vigilância com a capacidade de veículos como carros e motos, garantindo a eficiência das operações de segurança.

Para se tornar um vigilante condutor de veículo motorizado, o indivíduo precisa cumprir alguns requisitos e seguir determinados procedimentos estabelecidos pela legislação e órgãos reguladores da segurança privada.

Neste artigo, abordaremos a função do Vigilante Condutor de Veículos Motorizados, explorando suas funções, treinamento e a importância vital que desempenham na vigilância patrimonial. Além disso, descobriremos como a utilização estratégica de carros e motos na vigilância pode otimizar a segurança de áreas extensas e sensíveis.

O que é um Vigilante Condutor de Veículos Motorizados?

Um Vigilante Condutor de Veículos é um profissional da área de segurança privada que possui a função de dirigir veículos motorizados, como carros e motos, para desempenhar atividades de vigilância e proteção. Ele combina as habilidades de vigilância com a capacidade de conduzir veículos de forma segura e eficiente, tornando-se essencial para garantir rondas de segurança e deslocamentos rápidos em diferentes cenários.

As responsabilidades de um Vigilante Condutor de Veículos variam de acordo com o local de atuação. Ele pode ser empregado para realizar rondas de segurança em empresas, condomínios, áreas industriais, shoppings, entre outros locais, com o objetivo de prevenir incidentes e garantir a proteção de pessoas e patrimônios.

Quais são os tipos de vigilantes condutores e o que fazem?

Os tipos de vigilantes condutores de veículos motorizados podem variar de acordo com as especializações e funções específicas em que atuam. Alguns dos principais tipos de vigilantes condutores são:

Vigilante Condutor de Carro Forte: São responsáveis por conduzir veículos especiais de segurança, como carros-fortes, para transportar valores. Eles garantem a integridade dos valores e a segurança da equipe durante o trajeto.

Vigilante Condutor de Ambulância: Atuam conduzindo ambulâncias para prestar atendimento de emergência em casos de acidentes ou outras situações que necessitem de assistência médica.

Vigilante Condutor de Veículo de Patrulha: Realizam rondas motorizadas em veículos como carros ou motocicletas para monitorar a segurança de determinadas áreas e patrimônios, garantindo a presença ostensiva e inibindo possíveis ações criminosas.

Vigilante Condutor de Veículo de Escolta: São responsáveis por escoltar cargas valiosas ou sensíveis durante o transporte, garantindo a segurança do trajeto e a integridade da carga.

Vigilante Condutor de Veículo de Segurança Pessoal: São responsáveis por conduzir veículos utilizados para atividade de segurança pessoal privada.

Independentemente do tipo de vigilante condutor, suas principais atribuições incluem zelar pela segurança e integridade do veículo sob sua responsabilidade, cumprir os protocolos e procedimentos estabelecidos pela empresa de segurança, comunicar qualquer ocorrência ou incidente à supervisão, e garantir a integridade física da equipe e das pessoas envolvidas no transporte ou atendimento.

O que faz um vigilante condutor de veículos

Um Vigilante Condutor de Veículos desempenha uma série de funções relacionadas à segurança e à mobilidade, combinando habilidades de vigilância com a capacidade de conduzir veículos de forma segura e eficiente. Algumas das principais atividades desse profissional incluem:

Rondas de Segurança: Realiza rondas de segurança com veículos motorizados para monitorar e inspecionar áreas, identificar possíveis ameaças ou atividades suspeitas e garantir a integridade do patrimônio e das pessoas.

Transporte de vigilantes: Faz transporte de outros vigilantes para postos de vigilância ou locais de operações.

Resposta Rápida a Ocorrências: Presta apoio rápido para situações de emergência, como tentativas de invasão, furtos, incêndios ou acidentes.

Suporte Operacional: Colabora com a equipe de segurança em operações específicas, fornecendo apoio e auxílio nas atividades que requerem mobilidade e agilidade.

Condução de veículos de emergência: Conduz veículos de emergência, como ambulância, para locomoção de pessoas vítimas de acidentadas ou mal súbito.

Qual a importância do condutor de veículos motorizados?

O Vigilante Condutor de Veículos Motorizados desempenha um papel de extrema importância na segurança patrimonial e pessoal. Sua atuação é fundamental em diversos aspectos:

Mobilidade e Agilidade: O condutor de veículos permite que a equipe de segurança se desloque rapidamente e de forma eficiente entre diferentes áreas, possibilitando a realização de rondas mais abrangentes e o atendimento ágil a emergências.

Resposta Rápida a Ocorrências: Em situações de emergência, como tentativas de invasão, furtos, incêndios ou acidentes, a presença de um vigilante condutor de veículos é crucial para uma resposta rápida, minimizando danos e garantindo a segurança de pessoas e patrimônios.

Suporte em Operações Específicas: Em atividades que demandam mobilidade, como transporte de valores ou escolta de cargas, o vigilante condutor de veículos desempenha um papel estratégico, garantindo a segurança do deslocamento e dos bens.

Prevenção de Incidentes: A realização de rondas motorizadas permite a identificação precoce de situações suspeitas ou ameaças potenciais, possibilitando a adoção de medidas preventivas antes que problemas maiores ocorram.

Eficiência na Segurança: Com o uso de veículos, o vigilante pode cobrir áreas extensas em um curto espaço de tempo, otimizando a eficiência da equipe de segurança e garantindo uma cobertura mais ampla do perímetro a ser protegido.

Presença Dissuasória: A presença de veículos de vigilância patrimonial em locais estratégicos pode funcionar como um elemento dissuasório para potenciais infratores, reduzindo o risco de ocorrências criminosas.

Ampliação da Área de Cobertura: Veículos possibilitam o acesso a locais mais distantes e de difícil acesso, expandindo a área de atuação da equipe de segurança e tornando possível a vigilância de grandes perímetros.

Vigilante Condutor de Veículos Motorizados

Quem pode ser vigilante condutor de veículo motorizado?

Para se tornar um Vigilante Condutor de Veículos, o indivíduo precisa cumprir alguns requisitos estabelecidos pela legislação e órgãos reguladores da segurança privada. Os principais requisitos incluem:

Formação como Vigilante: É necessário ter concluído o curso de formação de vigilante em instituição devidamente autorizada pela Polícia Federal.

Habilitação (CNH): O candidato deve possuir Carteira Nacional de Habilitação (CNH) válida para a categoria do veículo que pretende conduzir, seja moto ou automóvel.

Vínculo empregatício: Deve ser registrado como empregado de uma empresa especializada ou possuidora de serviço orgânico de segurança.

É fundamental ressaltar que a função de Vigilante Condutor de Veículos envolve grande responsabilidade e requer capacitação adequada para garantir a segurança do profissional, da equipe e das pessoas e bens sob sua proteção durante o desempenho das atividades de vigilância e condução de veículos.

Quais são as responsabilidades do vigilante condutor

As responsabilidades do vigilante condutor em relação ao veículo utilizado no exercício de sua função são amplas e envolvem cuidados com a segurança, manutenção, cumprimento de normas e regulamentos, e a garantia de que o veículo esteja sempre em condições adequadas para o desempenho das atividades de vigilância.

Algumas das principais responsabilidades são:

Segurança do Veículo: O vigilante condutor é responsável por garantir a segurança do veículo em todos os momentos, evitando situações de risco e adotando medidas de prevenção de acidentes. Isso inclui seguir as regras de trânsito, não ultrapassar limites de velocidade e utilizar equipamentos de segurança, como cinto de segurança, capacete (no caso de motocicletas), entre outros.

Manutenção Preventiva: O vigilante condutor deve realizar a manutenção preventiva do veículo de forma regular, verificando e garantindo que todos os sistemas do veículo estejam funcionando corretamente, como freios, pneus, luzes, sistema elétrico, entre outros.

Zelar pela Limpeza e Conservação: O profissional deve zelar pela limpeza e conservação do veículo, mantendo-o em boas condições de higiene e aparência.

Registro de Ocorrências: Caso ocorra algum problema, dano ou incidente com o veículo durante o trabalho, o vigilante condutor deve fazer o registro da ocorrência e comunicar à empresa, seguindo os procedimentos estabelecidos.

Respeito às Normas da Empresa: É responsabilidade do vigilante condutor seguir as normas, procedimentos e instruções de trabalho estabelecidas pela empresa para o uso e condução dos veículos durante as atividades de vigilância.

Comunicação de Irregularidades: Caso identifique alguma irregularidade ou necessidade de reparo no veículo, o vigilante condutor deve comunicar imediatamente aos superiores ou setores responsáveis para que sejam tomadas as devidas providências.

Essas responsabilidades são essenciais para garantir a segurança do vigilante, da equipe e dos bens que estão sob sua proteção durante o exercício de suas funções como condutor de veículo motorizado na atividade de vigilância patrimonial.

Quanto ganha um vigilante condutor de veículo?

O salário de um vigilante condutor de veículo pode variar de acordo com a região dos Pais em função de acordos coletivos de trabalho, Além do piso base da categoria, de acordo com a Convenção Coletiva de Trabalho da região o vigilante condutor pode receber uma gratificação de função de 10% sobre o piso base.

Por exemplo: No estado de São Paulo, o piso base do Vigilante/Condutor de Veículos Motorizados é de R$1.845,56 + 10% = R$ 2.030,116

As gratificações de função descritas são devidas somente durante o período em que o empregado exercer a função gratificada e não são cumulativas, de forma que, em caso de exercício de mais de uma função gratificada, o empregado perceberá o valor correspondente àquela de maior valor, somente durante o período em que perdurar o exercício da referida função

Conclusão

Ao longo deste artigo, abordamos a atuação dos Vigilantes Condutores de Veículos Motorizados na segurança privada. Com suas habilidades de condução e capacitação em segurança, esses profissionais desempenham um papel vital na proteção de patrimônios e pessoas. Seja conduzindo carros de segurança ou motos, sua presença estratégica otimiza a vigilância de áreas extensas e sensíveis.

A importância desses vigilantes reside não apenas na mobilidade proporcionada por veículos motorizados, mas também na capacidade de agir prontamente em situações críticas, garantindo a segurança de pessoas e bens.

Se você deseja aprender mais sobre as atividades do vigilante condutor, sugiro a leitura do meu artigo sobre a “Vigilância Patrimonial“. Este conteúdo complementar permitirá uma visão mais ampla sobre a relevância do vigilante condutor e suas atribuições.

José Sérgio Marcondes, CES, CPSI - Especialista em Segurança Empresarial

Consultor em Segurança Privada - Diretor do IBRASEP

Empatia Assertiva” – “Como ser um líder incisivo sem perder a humanidade”

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

A obra de Kim Scott, traz uma nova filosofia de liderança baseada na empatia e assertividade.

Neste artigo você encontrará dicas práticas para se tornar um líder mais eficiente e humano ao mesmo tempo.

Resumo

"Empatia Assertiva, é um livro que apresenta uma nova filosofia de gestão baseada em quatro princípios: desenvolver relacionamentos assertivamente empáticos, receber, dar e encorajar o feedback, saber o que motiva cada membro da equipe e trabalhar em colaboração para atingir resultados. A autora defende que a empatia assertiva é a habilidade de entender e responder às necessidades dos outros de forma eficaz, sem deixar de lado as próprias necessidades. Ao desenvolver essa habilidade, os líderes podem criar um ambiente de trabalho mais colaborativo, onde a comunicação flui com mais facilidade e as pessoas se sentem mais motivadas e engajadas. O livro apresenta ferramentas e técnicas para colocar em prática esses princípios, como uma abordagem para conquistar a confiança da equipe e criar uma cultura de comunicação aberta. Além disso, a obra traz casos reais de liderança e exemplos práticos para ajudar os leitores a se tornarem líderes mais eficazes e humanos. Portanto, "Empatia Assertiva" é um guia completo para quem deseja desenvolver suas habilidades de liderança e criar um ambiente de trabalho mais produtivo e colaborativo.

Os Quatro Princípios

- Desenvolver relacionamentos assertivamente empáticos: se baseia na habilidade de entender e responder às necessidades dos outros de forma eficaz, sem deixar de lado as próprias necessidades. A empatia assertiva busca equilibrar a compreensão das necessidades dos outros com a defesa das próprias necessidades, criando um ambiente de trabalho mais colaborativo e produtivo;

- Receber, dar e encorajar o feedback: se refere à importância da comunicação aberta e honesta na equipe. A autora defende que o feedback é essencial para o desenvolvimento dos membros da equipe e para a melhoria contínua do trabalho. Ela apresenta ferramentas e técnicas específicas para facilitar o processo de dar e receber feedback de forma construtiva;

- Saber o que motiva cada membro da equipe: fundamenta na ideia de que cada pessoa tem seus próprios sonhos e objetivos, e que o líder deve ajudar a equipe a realizá-los. A autora apresenta técnicas para descobrir o que motiva cada membro da equipe e como usar essa informação para criar um ambiente de trabalho mais engajador e bem-sucedido;

- Trabalhar em colaboração para atingir resultados: menciona à relevância da colaboração e do trabalho em equipe para atingir os objetivos da empresa. A autora defende que o líder deve trabalhar em conjunto com a equipe, em vez de apenas dar ordens e esperar que as coisas aconteçam. Ela apresenta técnicas para criar um ambiente de trabalho mais colaborativo e produtivo, onde todos trabalham juntos para atingir os resultados desejados.

Líder Criativo

O líder pode criar um ambiente de trabalho mais colaborativo de diversas maneiras. Uma delas é incentivando a comunicação aberta e honesta entre os membros da equipe, por meio do feedback e da escuta ativa.

Outra forma é promovendo a diversidade e a inclusão, valorizando as diferenças e criando um ambiente onde todos se sintam respeitados e valorizados. Além disso, o líder pode incentivar a colaboração por meio de projetos em equipe, onde cada membro tem um papel importante a desempenhar e todos trabalham juntos para atingir um objetivo comum.

- Um exemplo prático é por meio de reuniões regulares de equipe, onde todos têm a oportunidade de compartilhar suas ideias e opiniões. O líder pode incentivar a participação de todos, criando um ambiente seguro e acolhedor para que as pessoas se sintam à vontade para falar.

- Outro exemplo é por meio de projetos em equipe, onde cada membro tem um papel importante a desempenhar e todos trabalham juntos para atingir um objetivo comum. O líder pode incentivar a colaboração, definindo claramente as responsabilidades de cada membro e promovendo a comunicação aberta e honesta entre eles.

Comunicação Liderança e Equipe

O líder pode adotar algumas práticas, como:

- Escuta ativa: o líder deve estar presente e atento durante as conversas, demonstrando interesse e compreensão. Ele deve fazer perguntas abertas e claras para incentivar a participação dos membros da equipe e evitar interrupções;

- Feedback construtivo: o líder deve dar feedbacks construtivos e específicos, destacando os pontos positivos e apontando áreas de melhoria. Ele deve ser claro e objetivo, evitando críticas pessoais e focando no desempenho;

- Comunicação clara: o líder deve ser claro e objetivo ao se comunicar, evitando jargões e termos técnicos que possam confundir os membros da equipe. Ele deve usar uma linguagem simples e direta, e estar disponível para esclarecer dúvidas;

- Incentivo à participação: o líder deve incentivar a participação dos membros da equipe, criando um ambiente seguro e acolhedor para que todos se sintam à vontade para falar. Ele deve valorizar as opiniões e ideias de todos, e promover a diversidade e a inclusão;

- Reconhecimento e celebração: o líder deve reconhecer e celebrar as conquistas da equipe, valorizando o esforço e o empenho de cada membro. Ele deve ser grato e demonstrar apreciação pelos resultados alcançados, incentivando a continuidade do trabalho.

Ferramentas e Técnicas

Para pôr em prática os princípios de empatia assertiva e criar uma cultura de comunicação aberta, algumas ferramentas e técnicas são necessárias.

Algumas delas são:

- Técnica: “feedback radical", que consiste em dar feedbacks claros e específicos, destacando os pontos positivos e apontando áreas de melhoria. Ela também apresenta uma técnica para receber feedbacks, chamada "escuta ativa", que consiste em ouvir atentamente e fazer perguntas para entender melhor a perspectiva do outro;

- Comunicação: "comunicação clara", que versa em usar uma linguagem simples e direta, evitando jargões e termos técnicos que possam confundir os membros da equipe. Ela também apresenta uma técnica para promover a diversidade e a inclusão, chamada "escuta empática", que consiste em ouvir atentamente e valorizar as diferenças;

- Motivação: "motivação intrínseca", que incide em ajudar os membros da equipe a encontrar significado e propósito no trabalho. Ela também apresenta uma técnica para descobrir o que motiva cada membro da equipe, chamada "perguntas poderosas", que consiste em fazer perguntas abertas e claras para entender melhor as necessidades e desejos de cada um;

- Colaboração: "colaboração eficaz", que se refere em trabalhar em conjunto com a equipe, em vez de apenas dar ordens e esperar que as coisas aconteçam. Ela também apresenta uma técnica para promover a colaboração, chamada "projetos em equipe", que consiste em definir claramente as responsabilidades de cada membro e promover a comunicação aberta e honesta entre eles.

Além das ferramentas e técnicas mencionadas anteriormente, outros temas também são relevantes, como a importância da confiança na equipe, a necessidade de estabelecer limites claros e a importância de manter um equilíbrio entre a empatia e a assertividade.

Ao longo da obra, Kim Scott compartilha suas próprias experiências como líder e apresenta exemplos de outras empresas que adotaram essa filosofia de liderança com sucesso. Ela também inclui exercícios práticos para ajudar o leitor a aplicar os conceitos em sua própria vida profissional e pessoal.

Se você procura uma abordagem mais humana e eficiente para liderar sua equipe, este livro certamente é para você. Com empatia assertiva, você pode conquistar a confiança da equipe, criar uma cultura de comunicação aberta e alcançar resultados excepcionais.

Exemplo de empresas que adotaram a filosofia de empatia assertiva com sucesso:

- Google: A Google é uma das empresas mais conhecidas por sua cultura de comunicação aberta e colaboração. A empresa incentiva seus funcionários a dar feedbacks claros e específicos uns aos outros, e a liderança é treinada para ouvir atentamente e valorizar as opiniões de todos os membros da equipe;

- Apple: A Apple é outra empresa que adota a filosofia de empatia assertiva em sua liderança. Steve Jobs, o fundador da empresa, era conhecido por sua habilidade em dar feedbacks claros e específicos, e por sua capacidade de inspirar e motivar sua equipe;

- Airbnb: A Airbnb é uma empresa que valoriza a diversidade e a inclusão em sua cultura. A empresa incentiva seus funcionários a ouvir atentamente e valorizar as diferenças, e a liderança é treinada para promover a colaboração e a comunicação aberta entre os membros da equipe.

Esses são apenas alguns exemplos de empresas que adotaram a filosofia de empatia assertiva com sucesso. Cada uma delas tem sua própria abordagem e cultura, mas todas compartilham a mesma visão de liderança baseada na empatia e assertividade.

Exercícios Práticos

- Pratique a escuta ativa: A escuta ativa é uma habilidade fundamental para a empatia assertiva. Para praticá-la, Kim Scott sugere que você se concentre em ouvir atentamente o que as pessoas estão dizendo, sem interrompê-las ou julgá-las. Tente fazer perguntas abertas para entender melhor o ponto de vista da outra pessoa e demonstre que você está realmente interessado em ouvi-la;

- Dê feedbacks claros e específicos: Dar feedbacks é uma parte importante da empatia assertiva. Para praticar essa habilidade, a sugestão é você escolher uma pessoa em sua vida profissional ou pessoal e dê a ela um feedback claro e específico sobre algo que ela fez bem ou que precisa melhorar. Certifique-se de que o feedback seja construtivo e que você esteja disposto a ouvir a resposta da outra pessoa;

- Estabeleça limites claros: Estabelecer limites claros é outra habilidade importante da empatia assertiva. Para praticá-la, identifique uma situação em que precisa estabelecer um limite claro e específico. Em seguida, pratique a comunicação clara e assertiva para estabelecer esse limite de forma respeitosa e eficaz.

Cada um destes exercícios é detalhado e explicado em mais profundidade ao longo da obra, com exemplos práticos e dicas para ajudar o leitor a aplicar os conceitos em sua vida pessoal e profissional.

Concluindo, a liderança assertiva é uma abordagem que traz muitas vantagens e ganhos para líderes, equipes e empresas. Ao adotar essa filosofia, os líderes podem criar uma cultura de comunicação aberta e colaboração, o que leva a uma maior confiança e engajamento da equipe. Além disso, a liderança assertiva ajuda a resolver conflitos de forma mais eficaz e a tomar decisões mais informadas e bem-sucedidas.

Para os líderes, a empatia assertiva pode ajudar a desenvolver habilidades de liderança mais fortes e a se tornar mais eficazes em sua função. Para as equipes, a empatia assertiva pode ajudar a criar um ambiente de trabalho mais positivo e produtivo, onde todos se sentem valorizados e respeitados. E para as empresas, a empatia assertiva pode ajudar a melhorar a satisfação do cliente, a retenção de funcionários e a rentabilidade geral.

Por fim, convidamos todos os líderes a colocar em prática os conceitos de empatia assertiva apresentados neste livro. Com a prática e o comprometimento, você pode se tornar um líder mais eficiente e humano, e ajudar sua equipe a alcançar resultados excepcionais. Então, comece agora mesmo e descubra como a empatia assertiva pode transformar sua liderança e sua vida profissional.

Quais são os principais conceitos abordados no livro?

Os principais conceitos abordados no livro são apresentados em duas partes. A Parte I traz uma nova filosofia de gestão baseada em quatro princípios: desenvolver relacionamentos assertivamente empáticos, receber, dar e encorajar o feedback, saber o que motiva cada membro da equipe e trabalhar em colaboração para atingir resultados. Já a Parte II apresenta ferramentas e técnicas para colocar em prática esses princípios, como uma abordagem para conquistar a confiança da equipe e criar uma cultura de comunicação aberta.

Como a empatia pode ajudar a melhorar a liderança?

Segundo o livro, a empatia assertiva é a habilidade de entender e responder às necessidades dos outros de forma eficaz, sem deixar de lado as próprias necessidades. Ao desenvolver essa habilidade, os líderes podem criar um ambiente de trabalho mais colaborativo, onde a comunicação flui com mais facilidade e as pessoas se sentem mais motivadas e engajadas. Além disso, a empatia pode ajudar a construir relacionamentos mais fortes e duradouros com a equipe, o que pode levar a melhores resultados e maior satisfação no trabalho.

O que diferencia a abordagem de Kim Scott de outras teorias de liderança?

A abordagem de Kim Scott se diferencia de outras teorias de liderança por combinar a empatia com a assertividade. Segundo o livro, muitas teorias de liderança enfatizam apenas um desses aspectos, o que pode levar a problemas como falta de comunicação, conflitos e baixa produtividade. A empatia assertiva, por outro lado, busca equilibrar a compreensão das necessidades dos outros com a defesa das próprias necessidades, criando um ambiente de trabalho mais colaborativo e produtivo. Além disso, a abordagem de Kim Scott é baseada em experiências reais de liderança, tanto dela própria quanto de outras pessoas que ela conheceu ao longo da carreira.

Dr. Sérgio Leônidas Dias Caldas, CRA, MBA, MBR, CPSI, CIEIE, CIEAC, CIGR, DIDS, MSDIS, DICS - Doutor Ciências da Segurança | Gestão Empresarial e Corporativa | Prevenção e Controle de Perdas | Riscos Corporativos

Faça Auditoria com eficiência: a abordagem Baseada em Riscos para maximizar recursos!

Marcos Alves Junior, CIEIE, CIGR, CPSI

Não podemos começar a falar da Auditoria Baseada em Riscos sem ao menos citar a Auditoria Interna tradicional. Por isso, vamos falar um pouco dela e como foi o seu início.

A auditoria interna se iniciou no século XIX, nos Estados Unidos, como uma resposta às necessidades de controle e transparência nas empresas. Na época, as organizações cresciam rapidamente e enfrentavam desafios na gestão de riscos e na área operacional.

A partir daí surgiram as práticas de controle interno, destinadas a garantir a integridade dos registros contábeis, a proteção dos ativos da empresa e o cumprimento das normas e regulamentos. Os primeiros auditores geralmente eram funcionários da própria organização, responsáveis por validar os processos internos, atestando que eles estavam sendo seguidos adequadamente.

Com o tempo, a auditoria interna foi se profissionalizando. Já no século XX, surgiram as primeiras associações profissionais de auditores internos, que buscavam estabelecer padrões e melhores práticas para a atividade. Com o crescimento das empresas multinacionais, a auditoria interna ganhou ainda maior importância, pois era necessária para garantir a conformidade com todas as normas e regulamentos.

A auditoria interna se tornou cada vez mais elaborada, incorporando técnicas avançadas de análise de dados e avaliação de riscos. Além disso, passou a desempenhar um papel estratégico nas organizações, fornecendo insights valiosos para a alta administração sobre a eficácia dos controles internos e o atingimento dos objetivos da empresa.

Nos dias atuais, a auditoria interna está presente em todas as organizações que têm os processos definidos, independentemente do tamanho ou setor de atuação. Seu principal objetivo é fornecer uma avaliação independente dos processos e controles internos, contribuindo para a governança corporativa, a gestão de riscos e a melhoria contínua das operações. A auditoria interna continua evoluindo para acompanhar as mudanças no ambiente de negócios e as demandas por transparência. Em uma dessas evoluções, nasceu a Auditoria Baseada em Riscos que traz uma visão holística dos processos.

A abordagem da Auditoria Baseada em Riscos é uma estratégia eficiente e que abrange auditorias internas e externas. Em vez de conduzir uma auditoria generalizada, essa metodologia se concentra nos principais riscos enfrentados pela organização, aqueles mais relevantes e significativos.

Ao adotar a Auditoria Baseada em Riscos, os auditores identificam e avaliam os riscos que podem impactar negativamente os objetivos da organização. Esses riscos podem ser de natureza financeira, operacional, de conformidade, de

reputação, entre outros. A compreensão desses riscos permite que os auditores concentrem seus esforços nas áreas críticas e priorizem suas atividades.

Para implementar a Auditoria Baseada em Riscos, é necessário realizar uma análise detalhada dos processos de negócios da organização para identificar as áreas mais suscetíveis a riscos. Isso envolve identificar possíveis falhas nos controles internos, lacunas na conformidade com regulamentações externas e vulnerabilidades operacionais.

Com base nessa análise de riscos, os auditores podem desenvolver um plano de auditoria que priorize as áreas críticas. Eles podem ajustar a frequência e profundidade das auditorias nessas áreas específicas e alocar recursos adequados para mitigar os riscos identificados.

A abordagem da Auditoria Baseada em Riscos traz diversos benefícios para as organizações. Primeiramente, ela permite direcionar os recursos de auditoria para onde são mais necessários, maximizando o impacto das atividades realizadas pelos auditores.

Além disso, essa estratégia auxilia na detecção e gestão antecipada dos riscos, diminuindo as chances de prejuízos financeiros, danos à reputação e descumprimento de leis e regulamentos.

No entanto, é importante ressaltar que a Auditoria Baseada em Riscos não elimina a necessidade de auditorias abrangentes e regulares em todas as áreas da organização. Ela é uma abordagem complementar que visa otimizar os recursos de auditoria, priorizando os riscos mais significativos.

Em resumo, a Auditoria Baseada em Riscos é uma metodologia eficaz para direcionar as atividades de auditoria para as áreas mais relevantes de uma organização. Ao identificar e tratar os riscos de forma proativa, ela contribui para melhorar a governança, o controle interno e o desempenho global da organização.

Com o intuito de automatizar processos em diferentes partes das organizações, o **Software INTERISK** contém o **Módulo de Auditoria Baseada em riscos – ABR**, que trabalha em conjunto com o **Módulo Gestão de Riscos Corporativos - GRC**, integrando a Auditoria Interna, Gestor da Área e Gestão de Riscos Corporativos para avaliar processos críticos, fontes de risco, controles e seus impactos (eficazes ou ineficazes), além dos riscos inerente e residual. Isso permite que a Auditoria Interna foque nos riscos e agregue mais valor à empresa do que uma auditoria focada apenas em controles. O Módulo ABR segue as melhores práticas como ISO 31000, COSO I, COSO ERM, Três Linhas de Defesa, ISO 31010 e IPPF.

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.

Sistema de Gestão de Continuidade de Negócios – Recursos e Competências: ISO 22313

Flavio Fleury de Souza Lima, MBCR, CEGRC, CIEAC, CISI, CIGR

Recursos e Competências Necessários para um Eficiente Sistema de Gestão de Continuidade de Negócios

De acordo com a norma ABNT NBR ISO 22313:2020, um sistema de gestão de continuidade de negócios (SGCN) requer recursos e competências para garantir que a organização esteja preparada para lidar com interrupções e crises. Vejamos:

Recursos

Um Sistema de Gestão de Continuidade de Negócios (SGCN) é uma abordagem estruturada para garantir que uma organização possa continuar suas operações mesmo diante de interrupções ou desastres. Para implementar um SGCN eficaz, é necessário contar com uma série de recursos. Aqui estão alguns dos principais recursos necessários:

- Avaliação de riscos: um recurso fundamental para um SGCN é a capacidade de realizar uma avaliação abrangente dos riscos que podem afetar a continuidade dos negócios. Isso envolve identificar e analisar os riscos potenciais, como desastres naturais, falhas de infraestrutura, interrupções de fornecedores, ciberataques, entre outros.

- Plano de continuidade de negócios: um plano de continuidade de negócios é um documento que descreve as ações a serem tomadas para garantir a continuidade das operações em caso de interrupção. Esse plano deve incluir procedimentos detalhados para lidar com diferentes cenários de crise, como realocação de pessoal, backup de dados, comunicação com partes interessadas, entre outros.

- Infraestrutura de TI resiliente: a tecnologia da informação desempenha um papel crucial na continuidade dos negócios. Portanto, é necessário contar com uma infraestrutura de TI resiliente, incluindo sistemas de backup e recuperação de dados, servidores redundantes, planos de contingência para falhas de hardware ou software, entre outros recursos tecnológicos.

- Recursos humanos capacitados: uma equipe qualificada e treinada é essencial para a implementação de um SGCN eficaz. Isso inclui profissionais com conhecimentos em gestão de riscos, continuidade de negócios, segurança da informação e recuperação de desastres. Esses profissionais devem estar preparados para agir rapidamente e tomar decisões informadas durante uma crise.

- Testes e exercícios de simulação: testar regularmente o plano de continuidade de negócios é fundamental para garantir sua eficácia. Isso envolve a realização de exercícios de simulação, como simulações de desastres, para identificar

falhas e áreas de melhoria. Os testes ajudam a garantir que todos os recursos e procedimentos estejam funcionando corretamente e que a equipe esteja preparada para lidar com uma crise real.

- Parcerias e acordos de fornecedores: estabelecer parcerias e acordos com fornecedores é importante para garantir a continuidade dos negócios. Isso inclui ter fornecedores alternativos em caso de interrupção, acordos de nível de serviço (SLAs) que garantam a disponibilidade de serviços essenciais e a colaboração com outras organizações para compartilhar recursos em situações de crise.

Em resumo, recursos como avaliação de riscos, plano de continuidade de negócios, infraestrutura de TI resiliente, equipe capacitada, testes e exercícios de simulação e parcerias com fornecedores são essenciais para a implementação de um SGCN eficaz. Ao reuni-los, uma organização pode estar preparada para enfrentar interrupções e garantir a continuidade de suas operações.

Competências

As competências são fundamentais para que um Sistema de Gestão de Continuidade de Negócios (SGCN) possa garantir que a organização estará preparada para enfrentar interrupções e crises. Algumas competências essenciais para um SGCN eficaz são:

- Liderança: a competência de liderança é crucial para estabelecer uma cultura de continuidade de negócios na organização. Os líderes devem demonstrar comprometimento e fornecer direção clara para a implementação e manutenção do SGCN.

- Gestão de riscos: a competência em gestão de riscos envolve a capacidade de identificar, avaliar e mitigar os riscos que podem afetar a continuidade dos negócios. Isso inclui a compreensão dos diferentes tipos de riscos, a análise de impacto nos negócios e a implementação de medidas preventivas e de mitigação.

- Planejamento estratégico: a competência em planejamento estratégico é essencial para desenvolver e implementar estratégias de continuidade de negócios alinhadas aos objetivos organizacionais. Isso envolve a definição de metas e objetivos claros, a identificação de atividades críticas, a alocação de recursos adequados e a definição de indicadores de desempenho.

- Gestão de crises: a competência em gestão de crises é necessária para lidar com emergências e interrupções. Isso inclui a capacidade de tomar decisões rápidas e assertivas, coordenar equipes de resposta, comunicar-se efetivamente com as partes interessadas internas e externas e mitigar os impactos negativos.

- Comunicação eficaz: a competência em comunicação é fundamental para garantir que as informações sejam transmitidas de forma clara e oportuna durante uma interrupção ou crise. Isso inclui a capacidade de se comunicar com diferentes públicos, adaptar a mensagem de acordo com as necessidades e utilizar diferentes canais de comunicação.

- Gestão de projetos: a competência em gestão de projetos é importante para planejar, executar e monitorar as atividades relacionadas ao SGCN. Isso envolve a definição de escopo, cronograma e recursos, o acompanhamento do progresso, a resolução de problemas e a garantia de que os objetivos sejam alcançados dentro dos prazos estabelecidos.

- Conhecimento técnico: a competência em conhecimento técnico abrange o domínio de áreas relevantes, como tecnologia da informação, segurança física, gestão de fornecedores, entre outras. Isso permite que os profissionais envolvidos no SGCN entendam os requisitos e as melhores práticas em cada área e apliquem as medidas adequadas para garantir a continuidade dos negócios.

- Pensamento estratégico: a competência em pensamento estratégico é necessária para antecipar e planejar a longo prazo. Isso envolve a capacidade de considerar diferentes cenários e possíveis interrupções, identificar oportunidades de melhoria e tomar decisões informadas para garantir a resiliência organizacional.

- Tomada de decisão: a competência em tomada de decisão é fundamental durante uma crise. Isso inclui a capacidade de avaliar rapidamente as informações disponíveis, considerar diferentes opções, pesar os riscos e benefícios e tomar decisões eficazes para minimizar os impactos negativos.

- Aprendizado contínuo: A competência em aprendizado contínuo é essencial para um SGCN eficaz. Isso envolve a disposição de aprender com experiências passadas, avaliar o desempenho do SGCN, identificar áreas de melhoria e atualizar constantemente os planos e procedimentos com base em lições aprendidas e melhores práticas.

Essas competências são fundamentais para garantir a eficácia e a resiliência de um Sistema de Gestão de Continuidade de Negócios. Cada organização pode ter requisitos específicos adicionais, dependendo de sua área, tamanho e complexidade.

O Software INTERISK dispõe de um módulo específico de Gestão de Continuidade de Negócios totalmente parametrizável em função das necessidades do cliente. Essa ferramenta pode se tornar uma grande aliada na identificação dos recursos e competências necessários para um Sistema de Gestão de Continuidade de Negócios para sua organização.

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

Interconectividade entre riscos: o que é e qual sua importância para as organizações

Olavo Tokutake. CIGR, CPSI, CIEIE, MBS

Você já deve ter visto, muitas e muitas vezes, o efeito dominó não é mesmo? Pois a imagem desse efeito em cadeia, gerado pela queda da primeira peça, combina muito bem com a situação em que a materialização de um risco influencia diretamente na materialização de outros. É isso o que chamamos de interconectividade entre riscos, ou motricidade entre riscos.

Claro que, ao se realizar uma análise de riscos, a interconectividade entre eles não se apresenta de maneira tão evidente como na brincadeira com as peças de dominó; talvez por isso, mais o fato de as ferramentas tradicionais de gestão de riscos não abordarem esta variável, a grande maioria dos gestores de risco não se atenta para a importância da motricidade dos riscos. Eles se dedicam a analisar a criticidade dos riscos isoladamente, obtendo, em consequência, um resultado à primeira vista certeiro, mas que, na verdade, trata-se apenas de um trabalho parcial, em consequência da visão míope a que foram induzidos pela falta da análise da interdependência.

Para se obter a visão completa dos riscos, é preciso analisar, risco a risco, o potencial de influência de uns sobre os outros, bem como em que grau essa influência se manifesta.

Para realizar essa tarefa, é possível utilizar a ferramenta de avaliação da motricidade dos riscos, fornecida com exclusividade pelo prático e abrangente Software INTERISK. Com essa análise feita, podem-se identificar os quatro tipos de riscos, em relação à interconectividade:

- Riscos de ligação, que influenciam e são influenciados por riscos motrizes;
- Riscos motrizes, que influenciam outros riscos mas não sofrem influência;
- Riscos Dependentes, que são influenciados mas não influenciam; e
- Riscos Independentes, que não influenciam nem são influenciados.

De posse dos resultados da análise de interconectividade dos riscos, fica fácil compreender a dinâmica dos e entre os riscos e, assim, visualizar os riscos que podem, apesar de aparentemente modestos, provocar a materialização de grandes riscos, ou ainda desencadear uma reação em sequência de outros.

O estudo da motricidade dos riscos é fundamental para que se possa enxergar, de maneira completa, os riscos corporativos e seu alcance sobre a instituição; não realizá-lo, apoiando-se apenas na tradicional matriz de riscos, é deixar uma importante brecha aberta para grandes problemas e, o pior, sem nem mesmo ter a ideia de que essa brecha existe.

Garanta uma análise de riscos estruturada e que leva em consideração a interconectividade entre os riscos, adotando o INTERISK. Além de ser uma plataforma integrada, que traz uma visão holística dos riscos e suas fontes, a ferramenta possibilita a avaliação da motricidade entre os riscos, trazendo maior eficácia às análises, de modo a facilitar a vida do gestor e otimizar os processos na organização.

A plataforma INTERISK conta com 14 módulos, visando atender plenamente às diferentes áreas do processo. **Conheça o Módulo de Gestão de Riscos Corporativos – GRC**, nosso carro chefe, e veja como ele atua na otimização de inúmeras áreas na sua organização.

Olavo Tokutake. CIGR, CPSI, CIEIE, MBS | Consultor em Gestão de Riscos e Especialista em Endomarketing da Brasiliano INTERISK

Consequências que a falta de Gestão de Riscos pode trazer para sua organização

Marcos Alves Junior, CIEIE, CIGR, CPSI

Anteriormente falamos dos benefícios que uma boa gestão de riscos pode trazer para sua empresa. Agora, vamos falar das consequências que a falta e/ou uma gestão de riscos mal estruturada pode levar para sua organização e como pode impactá-la.

Uma gestão de riscos míope e/ou mal estruturada pode ter consequências profundamente negativas para as empresas. Ela expõe a organização a uma série de ameaças que, se materializadas, podem resultar em danos financeiros, operacionais e reputacionais significativos. Confira algumas das principais consequências de uma gestão de riscos míope:

1. **Perdas Financeiras: Uma gestão de riscos inconveniente pode levar a perdas financeiras substanciais. Isso pode ocorrer devido a flutuações adversas nos mercados financeiros, falhas em estratégias, investimentos de alto risco não avaliados especificamente, ou mesmo fraudes internas não bloqueadas. Tais perdas podem comprometer a estabilidade da empresa e afetar sua capacidade financeira de investir e crescer.**

2. **Impacto Operacional: Riscos operacionais, como falhas em processos, falta de contingência ou desastres não planejados, podem resultar em incidentes significativos nos negócios. Isso não apenas prejudica a produtividade, mas também afeta a entrega de produtos ou serviços aos clientes, levando à insatisfação e perda de receita.**

3. **Impacto na reputação: Uma gestão de riscos insuficiente pode resultar em escândalos, ações judiciais, revelações de regulamentações e incidentes de segurança que prejudicam a privacidade da empresa. A perda de confiança dos clientes, investidores e partes interessadas pode ser difícil de recuperar e ter um impacto duradouro nos negócios.**

4. **Consequências Legais e Regulatórias: Violações de leis e regulamentações devido a uma gestão de riscos ineficaz podem levar a julgamentos substanciais, multas e processos legais. Além disso, as empresas podem ter custos adicionais para corrigir infrações e se adequar às regulamentações, o que aumenta os custos operacionais.**

5. **Desafios de Recuperação: Em situações de crise, como desastres naturais, pandemias ou crises econômicas, uma gestão de riscos deficiente torna a recuperação da empresa mais difícil. Isso pode resultar em uma recuperação mais lenta,**

perda de participação no mercado para concorrentes mais preparados e custos de reestruturação elevados.

6. **Erosão do Valor do Mercado: A falta de uma gestão eficaz de riscos pode levar a uma queda no valor do mercado das ações da empresa. Os investidores tendem a fugir de empresas com riscos percebidos como não gerenciados, ou que afetam o preço das ações.**

7. **Custos de Seguro Mais Altos: Se uma empresa não demonstra uma gestão de riscos eficazes, as seguradoras consideram um risco maior e aumentam os prêmios de seguro. Isso, por sua vez, aumenta os custos operacionais da empresa.**

Em resumo, uma gestão de riscos ineficaz pode ter consequências graves para a saúde e a sustentabilidade de uma empresa. Além das consequências financeiras imediatas, ela pode minar a confiança das partes interessadas. A Brasiliano INTERISK sempre primou por disseminar a cultura de gestão de riscos, governança e compliance. Levando em consideração que cenário do Brasil é volátil e está sempre enfrentando mudanças, os executivos estão começando a dar mais importância a perdas e reforçaram a importância para essas áreas, mas a carência de profissionais capacitados é um fator que pode vir a ter reflexos no futuro. Quando citamos capacitação, falamos de profissionais treinados em metodologias eficazes e para manusear ferramentas que vão agregar valor ao processo de gestão da empresa.

Tendo a experiência de mais de 30 no setor corporativo e conhecendo a fundo as dificuldades enfrentadas no dia a dia pelos gestores, nós desenvolvemos o Software INTERISK, uma solução integradora que traz automação e praticidade. Os seus diferenciais são únicos no mercado e, diferentemente da maioria das ferramentas de gerenciamento de riscos, o INTERISK não cobra licenças em função do número de usuários, ou seja, não importa o número de colaboradores que irão utilizar a solução, o valor será sempre o mesmo. A nossa plataforma conta com 14 módulos, visando atender diferentes áreas do processo com maestria. **Conheça o Módulo de Gestão de Riscos Corporativos – GRC, nosso carro chefe, e veja como ele atua na otimização de inúmeras áreas 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.

Como o investimento em ESG pode prevenir ou mitigar desastres?

Décio Luís Schons, CIEAI, CEGRC, CIGR, CISI

O primeiro pensamento que ocorre a qualquer um de nós quando tratamos de riscos, seja de modo genérico, seja de riscos ESG em particular, vai comumente na direção da prevenção, deixando a mitigação como um último recurso, quando todas as medidas possíveis para evitar a concretização do desastre foram ultrapassadas e o pior já ocorreu.

Mesmo tendo ciência da relevância da prevenção, equipes de gestão de riscos que se prezam não podem, em hipótese nenhuma, deixar de considerar as possibilidades de mitigação, ou seja, o tratamento do risco após a sua materialização, sob pena de serem responsabilizadas nos casos em que o pior venha a suceder. Essa afirmação encaixa-se muito bem na gestão dos riscos ESG, uma vez que esses riscos têm o potencial de afetar, de forma direta ou indireta, modos de vida e a própria sobrevivência de comunidades inteiras, por períodos prolongados e até mesmo de forma permanente.

Lamentavelmente, temos acompanhado o desenrolar de impactos ambientais muito mais graves do que se poderia esperar. Aí estão as memórias do rompimento das barragens de Mariana (2015) e Brumadinho (2019), com pesadas perdas em vidas humanas e toda a destruição ambiental que se seguiu. Esses são apenas os eventos mais recentes de uma série de tragédias elencando derrames de quantidades imensas de óleo no mar, incêndios devastadores, destruição da fauna e flora e assim por diante.

É senso comum que em todos esses casos houve falhas, tanto na prevenção dos riscos quanto no estabelecimento de medidas eficazes que pudessem, na eventualidade da concretização do risco em si, minorar os seus impactos.

Resulta daí a necessária conclusão de que investimentos na Agenda ESG são praticamente mandatórios para as empresas que, pela própria natureza de suas atividades, geram riscos relevantes ao meio ambiente e aos grupos sociais que o habitam. Esses investimentos, mais do que simplesmente contemplar atividades de preservação ambiental aleatórias, precisam estar alinhados aos propósitos da gestão de riscos, de modo a satisfazer às condições da eficiência, eficácia e efetividade.

O processo, um tanto trabalhoso, inicia-se com a determinação dos temas relevantes (ou de alta materialidade) para a empresa e para as suas partes interessadas internas e externas. A partir do conhecimento desses temas, serão montados os planos de ação que orientarão a busca dos objetivos correspondentes. Os indicadores chaves de desempenho (KPIs) constituem ferramenta importante para a avaliação periódica da situação, no que se refere às metas e objetivos estabelecidos em cada plano de ação.

À luz dos temas relevantes, serão levantados os riscos ESG estratégicos e operacionais que podem pôr em cheque o atingimento dos objetivos do negócio.

Como se pode perceber, há necessidade de investimentos tanto na área de implementação dos planos de ação quanto no que respeita à prevenção e mitigação de riscos. Providência interessante será exatamente fazer com que a equipe responsável pelo planejamento e implantação dos planos de ação trabalhe em estreita coordenação com a equipe de gestão de riscos, de modo a evitar gastos redundantes e a estabelecer iniciativas que atendam às duas frentes, o que proporcionará sensível economia de recursos.

Todavia, o resultado mais importante será percebido com o passar do tempo, com o aprofundamento dos estudos dos temas e tópicos relevantes para a organização e para seus stakeholders. Como é natural, a gestão dos riscos ESG irá, no mesmo passo, se tornando mais eficiente, eficaz e capaz de prevenir os riscos, de modo que eles não se materializem e, na eventualidade de uma materialização, que sejam prontamente mitigados.

É intuitivo que riscos de tal magnitude precisam ser tratados no mais curto prazo. Todavia, se alguma dúvida restar quanto à conveniência e oportunidade da implantação de um processo de gestão de riscos, a simples montagem de uma matriz Business Impact Analysis (BIA) será suficiente para esclarecer a questão.

Caso haja interesse de sua empresa em aprofundar-se nesse ou em outros temas afetos ao gerenciamento de riscos, contate a Brasiliano INTERISK, uma empresa que oferece soluções de Inteligência e Gestão de Riscos com base na Interconectividade, conferindo total transparência aos processos de Governança, Riscos e Compliance.

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

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

PROTEÇÃO DE INFRAESTRUTURAS CRÍTICAS. Do global ao setorial

Manuel Sánchez Gómez-Merelo

Vivemos num panorama globalizado de novas ameaças e maiores riscos sociais, industriais e comerciais, que ratificam novas exigências e exigências da sociedade para a proteção das suas atividades com plenas garantias para a sua segurança.

Sinais de alarme contínuos que aumentam as percepções (e mais do que percepções) de insegurança chegam-nos de todas as frentes, causando um sentimento generalizado de insegurança, múltiplas preocupações e problemas globais.

A Segurança Nacional e as Infraestruturas Críticas podem ser consideradas um problema global muito especial, que deve ser abordado a nível institucional, seguindo políticas nacionais, bem como uma abordagem internacional.

A Proteção de Infraestruturas Críticas. Novo quadro de cooperação europeu

A guerra na Ucrânia e as suas atuais ameaças, sabotagens e consequências estão a provocar uma nova abordagem à Segurança Global e à Proteção de Infraestruturas Críticas, principalmente na União Europeia.

Perante novas exigências e desafios constantes, as organizações públicas e privadas devem assumir a circunstância agora irreversível de que face às infraestruturas críticas devem avançar e, para tal, alinhar e integrar sistemas e planos de segurança físicos e lógicos, incluindo a cibersegurança, necessários proteger as suas atividades contra riscos e ameaças em constante evolução, bem como cumprir os novos regulamentos que as diferentes instituições nacionais e internacionais estão a implementar para proteger a segurança global de tais elementos estruturais essenciais.

Em junho de 2022, realizou-se em Madrid a XXX Cimeira da Aliança Atlântica (NATO) com a presença de 40 líderes internacionais. Durante esta reunião de alto nível, foi aprovado o novo “Conceito Estratégico da NATO”, um documento fundamental que define os desafios da organização internacional para a próxima década, e que culminou com um acordo para reforçar as capacidades da Aliança.

Para fazer jus a estes novos objetivos, devemos redefinir as políticas de segurança, criar uma nova cultura de segurança abrangente e integrada, estabelecer mecanismos de controlo e gestão da segurança física e lógica, monitorizar o sistema de segurança e, acima de tudo, enfatizar a resiliência.

Os novos desafios e exigências que surgem também para a Segurança Pública e Privada e a sua especial integração operacional exigem uma revisão e atualização dos meios tecnológicos e das medidas organizacionais disponíveis para responder a estes novos riscos e ameaças.

O Programa Europeu para a Proteção de Infraestruturas Críticas (PEPIC), que foi criado em 2006 com base na Comunicação da Comissão, é o principal veículo da UE para garantir a sua salvaguarda e resiliência.

Com as novas diretivas, a Comissão procura reforçar a capacidade dos Estados-Membros para proteger e recuperar as suas infraestruturas e serviços críticos nacionais e, progressivamente, avançar na harmonização dos recursos e planos europeus. Para tal, aumenta as obrigações dos membros de desenvolver estratégias, realizar análises de risco e identificar e supervisionar entidades críticas, entre outras.

Catálogo de Infraestrutura e Setores Estratégicos e Críticos

Por definição, as infraestruturas críticas são vitais para o funcionamento da sociedade. Sem fornecimentos fiáveis de energia ou transporte ou o funcionamento seguro das suas estruturas essenciais (saúde, financeira, abastecimento, etc.), o nosso modo de vida atual não seria possível. Por esta razão, a UE e as suas Comissões há muito que se dedicam a promover a proteção e a resiliência das infraestruturas críticas contra todos os tipos de riscos naturais e provocados pelo homem.

Assim, foram determinados os Sectores Estratégicos e Críticos, tais como infraestruturas relacionadas com Serviços Essenciais: Sector Energético (Eléctrica, hidrocarbonetos, gás); Setor de Tecnologia da Informação (Telefonia, rádio, televisão); Setor de Transportes (Aeroportos, portos, ferrovias, estradas); Setor de Água. Água (Depósitos, reservatórios, estações, tratamento); Setor Saúde (Biológico, assistência hospitalar, vacinas); Setor Alimentar (Produção, armazenamento e distribuição); Setor Financeiro (Entidades bancárias, títulos e investimentos).

Da mesma forma, infraestruturas sensíveis relacionadas com a segurança merecem especial atenção, tais como: Sector Nuclear (Produção e armazenamento de resíduos); Setor Químico (substâncias químicas, armas e explosivos); Setor de Instalações de Pesquisa (materiais químicos, biológicos, etc.); Setor Espacial (Cecom, telecomunicações); Sector da Administração (Instituições Superiores do Estado, Defesa, Interior, Serviços de Emergência, Património Nacional).

Setores, localização e segurança

Hoje a insegurança e a violência estão globalizadas e refletem uma organização social também em crise, que envolve indivíduos e instituições. É preciso dizer que os cidadãos perderam as referências para encontrar soluções para os problemas mais comuns, entre outras razões, porque a segurança fica turva por não ser globalizada ou suficientemente organizada.

Temos que pensar globalmente como cidadãos do mundo, mas temos que agir localmente, na nossa dimensão cidadã porque as fragilidades e vulnerabilidades se tornaram evidentes e, para abordar a segurança das Infraestruturas Críticas e Estratégicas, é essencial ter uma visão abrangente de o ambiente, interno e externo, que leva em consideração todos os aspectos da atividade e seus objetivos com uma perspectiva panorâmica, identificando todos os riscos, ameaças e vulnerabilidades da organização.

Quanto ao que a segurança deve ser considerada, deve-se notar que deve haver um único sistema abrangente de segurança e proteção em cada organização que inclua:

- A segurança física de edifícios e instalações.
- A segurança das infraestruturas e dos abastecimentos.
- Segurança corporativa e proteção de pessoas e bens.
- Segurança e privacidade da informação.
- Segurança lógica e de software e cibersegurança.
- Segurança contra fraudes operacionais e internas.
- Segurança ocupacional, prevenção e meio ambiente.
- Segurança jurídica e conformidade regulatória.

Assim, as medidas a adotar e os meios a disponibilizar estarão diretamente relacionados com:

- O perigo óbvio para as pessoas.
- O perigo imediato ou importante para a atividade.
- A gravidade das consequências.
- A influência social ou política do impacto.
- As possibilidades de repetição.

Segurança global, abrangente e integrada

Devemos redefinir a Segurança porque os desafios sugeridos pelo novo contexto global de riscos e ameaças exigem soluções inovadoras que incorporem inteligência e tecnologia como bases de uma estratégia de segurança necessária para operar nas organizações e na sociedade como um todo.

Em especial, precisamos analisar o impacto potencial em termos de riscos e ameaças às infraestruturas essenciais e reexaminar as complexidades da

tomada de decisões e da liderança em segurança global como uma tarefa essencial para um futuro esperado de prevenção e proteção.

Só a implementação de uma segurança global, abrangente e integrada pode garantir uma proteção eficiente contra ameaças globais, e isso significa ter em conta os aspectos geoestratégicos, humanos, jurídicos, sociais, económicos e técnicos de todos os riscos e ameaças que possam surgir. e ativos envolvidos nas atividades dos países aliados para o bem comum e a segurança conjunta.

Dada a grande variedade de riscos inerentes às Infraestruturas Críticas, a sua proteção deve ter uma abordagem baseada na segurança abrangente, e ser abordada como gestão de risco, implementando um modelo de segurança holístico, incorporando uma cultura proativa de prevenção e proteção.

Sem dúvida, hoje devemos responder com uma Segurança Única com letra maiúscula, abrangente e integrada, pública e privada.

Em suma, devemos promover uma cultura de segurança, identificando as oportunidades e fraquezas dos diferentes autores que cobrem o espectro global, nacional e local da segurança pública e privada.

Tudo isto sem esquecer que uma organização e gestão de segurança moderna deve hoje estar estruturada em torno de valores e a sua liderança deve ser consequência da expressão destes.

Não podemos esperar ter organizações seguras e resilientes se as pessoas que fazem parte delas não o fizerem. Portanto, devemos trabalhar a resiliência individual proativa, aproveitando os recursos e a experiência que já possuímos, aplicando os bons resultados já obtidos com eles e apoiando-nos nos valores dos modelos de sucesso já implementados.

Planos e soluções de segurança

Todo o desenvolvimento é baseado no Plano Nacional PIC (Proteção de Infraestruturas Críticas) e no seu desenvolvimento:

PES – Plano Estratégico Setorial: instrumentos de estudo e planeamento para todo o território nacional, que permitirão conhecer, em cada um dos sectores contemplados, quais são os serviços essenciais prestados à sociedade, o seu funcionamento, as vulnerabilidades do sistema, a potenciais consequências da sua inatividade e as medidas estratégicas necessárias à sua manutenção.

PSO – Plano de Segurança do Operador: documentos estratégicos que definem as políticas gerais dos operadores críticos para garantir a segurança do conjunto de instalações ou sistemas por eles detidos ou geridos.

EPI – Planos Específicos de Proteção: documentos que definem as medidas específicas já adotadas e as que serão implementadas pelos operadores críticos para garantir a segurança integral (física e lógica) das suas infraestruturas críticas.

PAO – Plano de Apoio Operacional: documentos que devem refletir as medidas organizacionais e operacionais específicas a implementar pelas Administrações Públicas para apoiar os operadores críticos, para a melhor proteção das suas infraestruturas.

Tudo isto com uma abordagem abrangente da segurança física e da segurança lógica, tendo como missão fundamental coordenar as atividades dos agentes envolvidos na proteção de infraestruturas essenciais ou críticas, tanto no setor público como no privado, adotando medidas legislativas, regulamentares, boas práticas, planos gerais e específicos para cada setor, em coordenação com as Forças e Corpos de Segurança e a cooperação internacional

Neste sentido, o Ministério do Interior de Espanha renovou o site do Centro Nacional de Proteção de Infraestruturas Críticas (CNPIC) com melhorias na sua acessibilidade e segurança. Entre as principais novidades, oferecerá o Nível de Alerta de Infraestruturas Críticas (NAIC), uma escala de cinco níveis complementares associados aos níveis de alerta do Plano de Prevenção e Proteção Antiterrorismo.

Com tudo isto, e como recomendações finais, devemos promover uma nova cultura de segurança com uma visão holística baseada em ameaças complexas; aumentar os recursos de análise e libertá-los de antigas patologias e rigidezes; e desenvolver o esquema abrangente de gestão de riscos e segurança, partindo de esquemas básicos ou decálogos para o desenvolvimento do pensamento global e da ação local.

Manuel Sánchez Gómez-Merelo - Presidente · Director General de ET. Estudios Técnicos, s.a. - Director de Programas de Protección de Infraestructuras Críticas del Instituto Universitario General Gutiérrez Mellado IUGM-UNED. Ministerio de Defensa. Miembro Permanente Experto de la Comisión de Seguridad Privada. Ministerio del interior.

Riscos ESG: Negar ou Tratar?

Décio Luís Schons, CIEAI, CEGRC, CIGR, CISI

Durante um largo período, desde que a temática da sustentabilidade começou a ganhar espaço no debate público, as dúvidas sobre a sua permanência no tempo vêm assaltando investidores, homens de negócios e a população em geral. Seria esse mais um modismo passageiro, desenhado por alguns espertos para faturar à custa de preocupações artificialmente provocadas? Seria toda essa conversa a respeito de mudanças climáticas uma imensa coleção de fake news construídas para causar confusão, iludir a população e assim facilitar a manipulação das massas desorientadas?

O tempo passou e o suposto modismo veio adquirindo cada vez mais ares de permanência no tempo. As supostas fake news mostraram a sua verdadeira cara à custa do sofrimento de muita gente. Desastres climáticos tornaram-se corriqueiros no Brasil e no mundo, haja vista o acontecido no ano passado em Petrópolis (RJ) e, neste ano de 2023, na Baixada Santista (SP) e no Vale do Jacuí (RS). Isso sem esquecer os incêndios recentes no Havaí, no Canadá, na Califórnia e em diversos países europeus, além da inundação ocorrida na Líbia e o calor fora de época que estamos enfrentando por aqui mesmo.

As mudanças climáticas estão ligadas ao chamado aquecimento global, como passou a ser conhecido o aumento da temperatura média superficial da Terra. As numerosas consequências que daí derivam, como as secas frequentes, os incêndios florestais, o derretimento das calotas polares, as tempestades catastróficas, a escassez de água e o aumento do nível dos oceanos, já se tornaram por demais evidentes para serem ignoradas.

Ao que se sabe, o processo todo teve início com a Revolução Industrial, agravado progressivamente pelo aumento da queima de combustíveis fósseis como o petróleo, o gás natural e o carvão. As causas raízes disso são interligadas, começando pelo aumento constante da população mundial e o correspondente aumento na demanda por alimentos e produtos manufaturados, trazendo atrelados o desmatamento, o aumento das atividades industriais e as mudanças de formas do uso do solo. Esses são aspectos contribuintes para o aumento da temperatura, por englobarem atividades emissoras de grande quantidade de gás carbônico, o principal componente do chamado efeito estufa.

Desde 1972, na Conferência de Estocolmo, os países vêm debatendo a esse respeito, sem que se chegue a um consenso capaz de transformar as boas intenções em realidade. Assim foi na Rio-92, na Conferência de Paris em 2015 e na Assembleia Geral da ONU que acaba de se encerrar. Por exemplo, hoje já é ponto pacífico que, dos 17 Objetivos de Desenvolvimento Sustentáveis (ODS) propostos pela ONU em 2015 para serem atingidos até 2030, somente 15% serão cumpridos. Da mesma forma, o compromisso firmado naquela mesma conferência, com a assinatura do famoso Acordo de Paris, prevê parâmetros para o aumento das temperaturas médias no planeta que, hoje já se tem como certo, não serão nem de longe alcançados.

A pergunta que neste momento pode assaltar a mente dos cidadãos de bem é esta: que podemos fazer, em nossa insignificância, para colaborar nessa tarefa hercúlea e certamente muito acima das nossas possibilidades de fazer alguma diferença sensível?

A primeira parte da resposta diz respeito ao cidadão comum, que pode conformar seus atos e atitudes às regras da sustentabilidade, fazendo a sua parte, proporcionando exemplos e colaborando no processo educativo das gerações que nos irão substituir ou que já nos estão substituindo.

Já com relação aos cidadãos que ocupam cargos de relevo, seja no poder público, seja na iniciativa privada, seja ainda nas organizações da sociedade civil, a estes cabe, sim, uma responsabilidade maior, pois de suas palavras e ações dependerá o sucesso ou o fracasso de tudo o que diz respeito ao futuro sustentável da humanidade.

A conscientização dos que estão à nossa volta surge aqui como fator chave de sucesso para essas iniciativas. Mudar hábitos arraigados, sabe-se muito bem, é processo difícil que depende de pelo menos uma das seguintes circunstâncias: em primeiro lugar, o sofrimento ou a perspectiva dele; em segundo lugar, a tomada de consciência de que é necessário mudar, para o próprio bem e para o bem do grupo a que se pertence. Sendo assim, que possamos escolher voluntariamente a segunda maneira, levando a nossos colaboradores, companheiros de jornada, amigos e familiares, a mensagem e o exemplo da sustentabilidade.

Adoção de hábitos de vida saudáveis, disposição adequada de resíduos, cuidados com a vegetação e com os animais, plantio de mudas de árvores em locais disponíveis – esses são alguns passos que permitem a qualquer um de nós, na qualidade de cidadãos comuns, evidenciar a nossa seriedade em relação ao tema. Já como gestores de negócios, de organizações da administração pública ou da sociedade civil, é provável que recaia sobre nós uma responsabilidade maior e para isso devemos estar preparados.

É fora de questão que as mudanças climáticas constituem riscos importantes, não apenas para os negócios, mas sobretudo para a humanidade. Hoje os Riscos ESG são tratados nas empresas como mais uma disciplina da Gestão de Riscos Corporativos. As empresas que não aderirem de todo à pauta da sustentabilidade ou tentarem ganhar tempo e algum dinheiro praticando o famigerado green washing passam a correr um risco muito maior, uma vez que o poder público já despertou para a importância do tema e condutas irresponsáveis tendem a ser punidas com rigor.

Mesmo contrariando as conclusões da grande maioria dos cientistas e estudiosos do tema (e concordando com os chamados negacionistas), vamos admitir que a fase de aquecimento que atravessamos é natural, ou seja, um reflexo dos ciclos característicos do nosso planeta. Mesmo assim, os esforços de preservação ambiental não terão sido desperdiçados. Não há dúvida de que a ação predatória do ser humano vai aos poucos desfigurando a superfície da Terra e tornando-a cada vez mais insalubre. Podemos e devemos deixar para os que vierem depois de nós um planeta habitável. Depende de nós.

Basta olhar à nossa volta para perceber o muito que precisamos fazer nessa seara, seja como cidadãos comuns, seja como depositários de responsabilidade sobre uma empresa, associação ou autarquia.

Caso haja interesse de sua empresa em aprofundar-se nesse ou em outros temas afetos ao gerenciamento de riscos, contate a Brasiliano INTERISK, uma empresa que oferece soluções de Inteligência e Gestão de Riscos com base na Interconectividade, conferindo total transparência aos processos de Governança, Riscos e Compliance.

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

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

Como mitigar riscos de imagem e reputação durante atuação dos agentes de segurança

Adenilson Campos Guedes

Uma abordagem focada na segurança em sistemas de transporte sobre trilhos

O trabalho dos **agentes de segurança** em geral, sobretudo, aqueles que atuam em sistemas de transporte sobre trilho, não é algo simples e por isso exige habilidades que vão muito além da capacidade física. Humanização, estratégia e inteligência, são habilidades fundamentais para os profissionais de segurança do século XXI e fazem toda a diferença na mitigação de riscos, especialmente, aqueles ligados à imagem e reputação das empresas. Mas, como lidar com exposição midiática e/ou pessoas filmando ações dos agentes? Como mitigar riscos de imagem e reputação durante as abordagens e condução de ocorrências nas estações, trens e demais locais sob domínio da concessionária responsável? Neste artigo, irei discorrer sobre alguns aspectos que podem potencializar riscos, bem como algumas formas mitigadoras sob a ótica do uso progressivo da força e os pilares psicológicos essenciais para os Agentes de Segurança.

O contexto atual

Atualmente vivemos um dos fenômenos contemporâneos: Repórteres anônimos e agenda diária da imprensa cada vez mais sedenta por furo de reportagem, principalmente as de cunho político e social com aspecto de tragédia, do negativo. Tudo isso somado às pessoas em geral com os seus smartphones, com câmeras cada vez melhores e conectados às redes sociais, blogs e canais da grande mídia, bastando apenas um clique para postarem vídeos, textos e fotos. Para se ter uma ideia, somente o Brasil possui 234 milhões de dispositivos digitais em uso, revela a 31ª Pesquisa Anual do FGVcia, ou seja, mais dispositivos que habitantes. O fato é que, gostando ou não, tudo que acontece nas estações de metrô e trens podem ser captadas pelas lentes, seja da imprensa ou do cidadão repórter anônimo, não há como escapar disso. Dentro deste contexto, quase sempre quando ocorre alguma atuação por parte dos agentes de segurança, com emprego da força física, as notícias logo se proliferam nas redes sociais e na imprensa. Quase sempre negativas para a imagem da empresa.

“a confiança é como um vaso de cristal, quando quebrado, por mais que tentemos colar, jamais voltará a ser como antes”

Na frase “a confiança é como um vaso de cristal, quando quebrado, por mais que tentemos colar, jamais voltará a ser como antes”, significa dizer que, por exemplo, uma notícia falsa ou exposição midiática negativa da empresa, poderá “quebrar o

vazo", e isso pode custar muito caro para a empresa consertar. O abalo na imagem pode impactar na perda de receita e, no caso das concessionárias com ações na Bolsa de Valores, assustar os investidores. Podemos citar algumas das principais consequência que o risco de imagem pode trazer à organização:

- A empresa terá mais dificuldades no relacionamento com o mercado, e consequentemente em gerar novos negócios.
- Queda nos lucros.
- O mercado pode se fechar para a empresa, gerando um desgaste na imagem. Para recolocá-la novamente no mercado, o trabalho é dobrado, assim como o custo.
- Criar má reputação, podendo comprometer severamente a vida da empresa.

Especialmente às concessionárias de transporte público sobre trilhos, é necessário olhar com muita atenção para o time de operações, pois uma simples ação do agente de segurança, que tenha ampla repercussão midiática negativa, poderá causar um grande estrago na imagem da empresa. Veja o caso do Carrefour em 2020, onde seguranças foram presos acusados de agredir e matar João Alberto Silveira Freitas. Com grande repercussão na imprensa, isso custou muito caro para a empresa. Não cabe aqui avaliar o grau de excesso dos agentes do Carrefour, mas em geral é importante destacar que, muitas vezes a ação dos agentes pode até ser correta, mas aos olhos do público, é algo incorreto ou inaceitável, por isso lidar com tais variáveis é algo muito complexo e exige grande capacidade de adaptação.

Humanização na abordagem do agente de segurança

De acordo com o Manual Básico de Abordagem Policial da Polícia Militar da Bahia, a abordagem é o ato de aproximar-se e interpelar uma pessoa com o intuito de identificar, orientar, advertir, assistir, deter etc. (MBAP/PMBA/2000, p. 32). No caso dos agentes de segurança metroviária, a abordagem é o momento em que o agente se aproxima de uma pessoa para exercer uma obrigação, socorrer ou impedir algum mal feito, se comportando como um mantenedor da lei dentro dos limites da concessionária, investido do poder-dever que compete ao agente por força da Lei 6.149/74 e os respectivos Decretos (Regulamentos de Viagens dos sistemas de Transporte sobre Trilhos no Brasil).

O agente de segurança que realiza abordagens durante o exercício de sua função, possui limites estabelecidos no ordenamento jurídico, para não incorrer em abuso e consequentemente responder por crimes previstos no Código Penal. Tão importante quanto examinar os aspectos legais, é a consciência de que lidam com pessoas que têm sonhos, necessidades, família e buscam segurança, conforto e qualidade no sistema metroviário. Por isso, é imperioso que os agentes reflitam sempre: Somos todos seres humanos, somos todos iguais. Neste sentido, o modelo de segurança adequado aos tempos atuais, é aquele composto por profissionais capazes de entender a fundo a vida dos clientes, fazendo o exercício da empatia, servindo-os,

protegendo-os, promovendo uma experiência boa, inesquecível, para que eles voltem, falem bem do sistema de transporte e o quanto foram bem atendidos. Desta forma, além de potencializar a fidelização dos clientes, minimiza reclamações e até comportamentos agressivos. Neste sentido, é possível afirmar que, embora os agentes de segurança possam atuar em determinadas circunstâncias, de maneira repressiva, sua ação é essencialmente preventiva. Portanto, quanto mais desenvolver habilidades para atuar em ações preventivas, menor a probabilidade do emprego efetivo da força física numa ocorrência.

Ações com emprego do uso efetivo da força custa caro, pois além dos riscos de repercussão midiática negativa, haverá emprego de mais de um agente de segurança na ocorrência (emprego de viaturas, tempo na Delegacia), além de riscos judiciais inerentes à ocorrência.

Mesmo diante de situações em que o agente de segurança precise abordar algum cliente em eventual descumprimento do regulamento de viagem ou flagrante delito, é fundamental observar os Direitos e Garantias Fundamentais, previsto na Constituição Brasileira, bem como o Uso Progressivo (seletivo) da Força de acordo as normas da ONU (Organização das Nações Unidas). Quando realmente for necessário o emprego efetivo da força por parte do agente de segurança, precisa atuar obrigatoriamente dentro da lei, ou seja, revestido de legalidade, necessidade, proporcionalidade e conveniência na ação. Estes são os pilares psicológicos essenciais para os agentes de segurança.

Pilares psicológicos essenciais para o Agente de Segurança

a) Legalidade

O agente de segurança precisa buscar respaldo legal na sua ação. Antes, deve refletir: A ação está justificada de acordo a lei? Deve amparar legalmente a sua ação, devendo ter conhecimento da lei e está preparado tecnicamente, através da sua formação e do treinamento recebido.

b) Proporcionalidade

A força emprega pelo agente de segurança precisa ser adequada para conter o ofensor, nem mais, nem menos. O uso excessivo da força poderá caracterizar abuso e incorrer em crime.

c) Conveniência

Mesmo que a ação do agente de segurança esteja respaldada pela legalidade e a força empregada seja adequada, é importante verificar: Será que o momento é conveniente para o uso da força? Será que a sua ação naquele momento não poderá trazer consequências maiores? Ou seja, se houver mais riscos do que benefícios, o

emprego na força não será conveniente naquele momento. Podemos dizer que “o remédio não pode ser pior do que a própria doença”.

Uso Progressivo (seletivo) da Força

O termo uso seletivo da força é algo mais apropriado tendo em vista que o agente de segurança deve selecionar o nível de força adequado conforme a situação. Sendo assim, segue um modelo básico para utilização dos Níveis de utilização da força adaptado para a realidade do agente de segurança das Concessionárias de Transporte Público Sobre Trilhos:

1º Nível – Presença física: é a simples presença do agente de segurança, diante de uma situação onde alguém está descumprindo alguma regra ou na iminência de cometer algum ilícito. Muitas vezes, a simples ação de presença é suficiente para cessar um mal feito.

2º Nível – Verbalização: É a comunicação, orientação por parte do agente de segurança, na fase em que o ofensor é cooperativo, não oferece resistência ao agente. É muito importante se esforçar na orientação.

3º Nível – Controle de contato: Neste caso, já ocorre o uso da força por parte do Agente, com utilização de técnicas de conduções e imobilizações, inclusive por meios de algemas quando justificáveis. Técnicas empregadas diante da resistência passiva do agressor, que age em um nível preliminar de desobediência (ele não acata as determinações, fica simplesmente parado).

4º Nível – Controle físico: É o emprego da força suficiente para superar a resistência ativa do indivíduo. O ofensor não está passivo, desafia fisicamente o Agente, como por exemplo num caso de fuga. Uso de tonfa e agentes químicos podem ser utilizados.

Muito importante! Para o emprego dos últimos níveis de força (3 e 4), deve ser considerado que já existe um grau elevado de risco de exposição midiática, por isso, sem o flagrante delito, não é algo justificável. Há exceções, por exemplo, nos casos em que o indivíduo ofereça risco à integridade física do próprio ofensor ou de terceiros; não havendo outra maneira, este nível de força poderá ser aplicado. Alguns exemplos: Alguém com surto psicótico, que ameaça a sua vida ou de outros etc.).

Agora que já conhecemos um pouco sobre os níveis para o emprego do Uso Progressivo (seletivo) da Força e os pilares psicológicos essenciais para o Agente de Segurança, trarei algumas dicas que poderão mitigar ainda mais os riscos de exposição midiática e/ou de reputação.

- **Sem flagrante delito na origem –** Não utilizar o nível 3 de força (controle físico), quando na origem do problema não houve flagrante de crime. Ex.:

Alguém pedindo dinheiro ou vendendo dentro do trem. Há um descumprimento do regulamento de viagem, mas não crime. Evitar a banalização do crime de ameaça nestas situações, pois é comum nestes casos o ofensor proferir algum tipo de ameaça verbal.

- **Avaliação de riscos –** Antes de fazer o uso efetivo da força, deve-se analisar o ambiente, verificar se é conveniente o emprego do nível 3 ou 4 de força. Avaliar quais as consequências poderão advir desta ação. Por exemplo: Há riscos do público se revoltar contra os Agentes ou pode ter alguém filmando a ocorrência. Pode ocorrer a presença de grupo de ofensores violentos em maior número do que os Agentes etc.
- **Mediação de conflitos –** Desprender energia para mediar conflitos; ser empático, buscar soluções inteligentes, não deixar a emoção sobrepor a razão; se necessário, outro Agente poderá assumir a ocorrência.
- **Uso de câmeras corporais –** O uso deste equipamento durante a atuação dos Agentes de Segurança traz vários benefícios. Neste caso, o fato de estar captando áudio e vídeo da ocorrência, potencializa maiores cautelas, tanto por parte do ofensor, quanto dos próprios agentes. Essas imagens poderão, por exemplo, ajudar a esclarecer dúvidas sobre a ação dos Agentes durante as ocorrências, resultando em maior transparência nas ações, inibindo ou confirmando se houve ou não excessos no atendimento das ocorrências. As gravações também poderão ser utilizadas como prova judicial, demonstrando que a ação da equipe foi correta diante de uma possível denúncia de irregularidade. As imagens poderão ajudar ainda no aperfeiçoamento de técnicas a serem utilizadas no treinamento dos agentes de segurança.
- **Narrar os fatos/ação –** Durante a atuação, preferencialmente com uso da câmera corporal, narrar os fatos, explicar o que está fazendo, citar que o bem do coletivo deve estar acima do individual, sempre tratando todos com cordialidade. Dependendo da forma de atuação, o público poderá ficar a favor do agente de segurança.
- **Evitar tocar na pessoa** – Conforme citado anteriormente, em situações que não foi originada por flagrante delito, não tocar no ofensor. Insistir nos níveis 1 e 2 de força. Se aproximar e orientar incansavelmente.
- Realização de diálogos com time de agente de segurança – Criar agenda e lista de temas com foco na mitigação de riscos de imagem e reputação. O papel da liderança é fundamental neste processo, inclusive, incentivando a equipe a trazer novas alternativas.
- **Comunicação ou área de Inteligência:** Monitoramento constante das notícias negativas, nas redes sociais, mídia falada e escrita, incluindo notícias falsas pois esta tem um poder de propagação muito grande e consequentemente poderá trazer consequências ruins em termos de imagem e reputação para a empresa.

- Cuidado com indivíduos que possam provocar situações para levantar bandeiras relacionadas a tema sensíveis: racismo, homofobia etc. Usar sempre a coerência e dentro dos Direitos e Garantias Fundamentais.
- **Área de Comunicação:** Soltar notas impactantes, legitimando a atuação do time de segurança. Para que a atuação seja rápida, as informações deverão ser checadas e levantadas para a área de Comunicação de forma muito rápida, para que seja possível de forma imediata, produzir informações (contramedidas) para inibir a proliferação da notícia, mostrando o lado dos fatos pela ótica da concessionária, não apenas do ofensor.
- **Apoio da área jurídica –** Se necessário, a área jurídica deverá ser acionada. Podendo até acompanhar eventuais conduções de ocorrências na Delegacia de Polícia. Neste caso é recomendado a presença de Advogado da área penal.

Considerações finais:

É necessário elevar os padrões de segurança, colocando-a em um novo patamar: Segurança humanizada, estratégica e inteligente, agentes que olham o todo, o ser humano em primeiro lugar.

Apesar na amplitude do tema, os conceitos e dicas aqui expostos devem contribuir para que os agentes de segurança possam lidar melhor com as situações adversas, sobretudo, aquelas com maior potencial de impacto negativo de imagem e reputação. Que, a utilização dos conceitos apresentados possam ajudar as equipes a potencializarem ainda mais as ações exitosas e mitigar riscos, sempre observando os pilares psicológicos essenciais para o Agente e lembrar que o uso efetivo da força custa caro, por isso vale muito à pena os esforços nas ações preventivas, observar, especialmente, o princípio da conveniência. Mesmo assim, se tiver que fazer o uso da força, que seja rápida, cirúrgico, pautada na lei e em observância aos pilares psicológicos essenciais para o uso da força.

REFERÊNCIAS BIBLIOGRÁFICAS:

Brasil tem 424 milhões de dispositivos digitais em uso, revela a 31ª Pesquisa Anual do FGVcia. Portal FGV. 20 de jun. de 2020. Disponível em: <https://portal.fgv.br/noticias/brasil-tem-424-milhoes-dispositivos-digitais-uso-revela-31a-pesquisa-anual-fgvcia>. Acesso em: 30 de mar. de 2021.

Lei 6.149, de 2 de dezembro de 1974. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/1970-1979/L6149.htm>. Acesso em: 30 de mar. de 2021.

Princípios básicos sobre o uso da força e armas de fogo pelos funcionários responsáveis pela aplicação da lei. Defensoria Pública do Mato Grosso do Sul.. Disponível em:

<http://www.defensoria.ms.gov.br/images/nudedh/sistemas_onu/33_-_principios_basicos_sobre_o_uso_da_for%C3%A7a_e_arma_fogo_pelos_funcion%C3%A1rios__respons%C3%A1veis_pela_eplica%C3%A7%C3%A3o_da_lei__1990.pdf>. Acesso em: 30 de mar. de 2021.

BÖING, Cláudio. 2010. 95 f. Trabalho de conclusão de curso (monografia) – Curso de Formação de Oficiais, Centro de Ensino da Polícia Militar, Florianópolis, Santa Catarina, 2010.

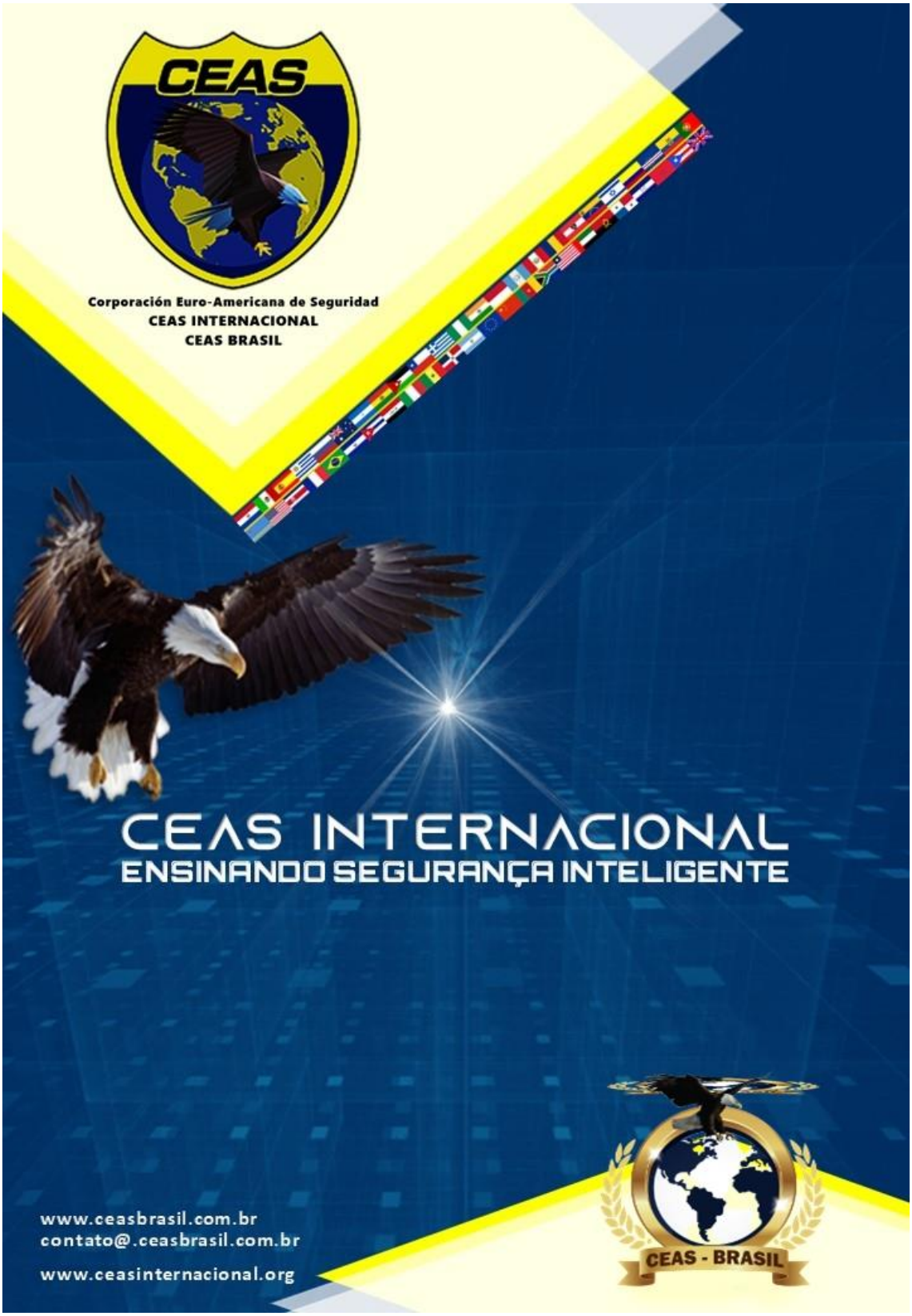
BÖING, Cláudio. 2010. 95 f. Trabalho de conclusão de curso (monografia) – Curso de Formação de Oficiais, Centro de Ensino da Polícia Militar, Florianópolis, Santa Catarina, 2010.
Entrevista, o Fenômeno das notícias falsas. Revista PUC Minas. 20 de jun. de 2020. Disponível em: <http://www.revista.pucminas.br/materia/fenomeno-noticias-falsas/>. Acesso em: 30 de mar. de 2021.

DI PIETRO. Maria Sylvia Zanella. Direito Administrativo. 8A Ed. São Paulo. Atlas, 1997.
MANUAL BÁSICO DE ABORDAGEM POLICIAL. Polícia Militar da Bahia.2000. Acesso:http://pt.scribd.com/doc/18589797/Manual-Basico-Abordagem-Policial#scribd de 2015/>. Acesso em 30 de mar. De 2021.

BRASIL, Glauciria Mota. Direitos Humanos e formação policial: reflexões sobre limites e possibilidade. Público e Privado. Revista semestral. UECE, N.18 – Julho/Dezembro, 2011.

ONU. Organização das Nações Unidas. Código de Conduta para os Funcionários Responsáveis pela Aplicação da Lei. Assembleia Geral das Nações Unidas, resolução 34/169, de 17 de Dezembro de 1979. Disponível em: <https://flitparalisante.wordpress.com/2010/06/10/resolucao-onu-n%C2%BA-34169-de-17121979-codigo-de-conduta-para-os-policiaiscode-of-conduct-for-law-enforcement-officials-os-policiais-que-tiverem-motivos-para-acreditar-que-se-produziu-ou-ir/>. Acesso em: 15 de mar. de 2021.

Adenilson Campos Guedes - Graduado em Gestão de Segurança Empresarial, possui Especialização em Consultoria Empresarial com Ênfase em Segurança Corporativa, MBA em Gestão Política e Planejamento Estratégico e MBA em Gestão da Inteligência Estratégica pela Associação dos Diplomados da Escola Superior de Guerra – ADESG-BA, certificado Six-Sigma Green Belt da Escola EDTI. É idealizador e responsável pelo site www.folhadaseguranca.com.br. Linkedin: https://www.linkedin.com/in/adenilsonguedes/ e Twitter: https://twitter.com/deseguranca Canal Instagram: https://www.instagram.com/folhadaseguranca.com.br/


CEAS
Corporación Euro-Americana de Seguridad
CEAS INTERNACIONAL
CEAS BRASIL
CEAS INTERNACIONAL
ENSINANDO SEGURANÇA INTELIGENTE
www.ceasbrasil.com.br
contato@.ceasbrasil.com.br
www.ceasinternacional.org
CEAS - BRASIL