COLETÂNEA DE ARTIGOS

EDIÇÃO VI - 2023

SUMÁRIO

SUMÁRIO

INTRODUÇÃO

Mariana da Silveira, DIDS, MBCR, CPSI, CEGRC, CIGR, CISI,
CIEIE, DPO, ISO | Divisão Cibernética da Brasiliano INTERISK

Acelerado nos últimos anos, trazendo novas perspectivas às organizações. Apesar desta evolução, nos cabe fazer a seguinte pergunta: de que maneira o sistema de segurança gera vantagem competitiva.

Para construirmos esta resposta precisamos levar em conta três premissas. A primeira é que o sistema de segurança é uma unidade de apoio, unidade meio ou de serviço compartilhado, tal como recursos humanos, finanças e jurídico. Os produtos do sistema de segurança, assim como de outras unidades de apoio, são geralmente intangíveis, pois é uma prestação de serviço. É difícil quantificar esses produtos quando as empresas tentam avaliar a eficácia e a eficiência dessas unidades.

A segunda premissa é que o sistema de segurança precisa adotar um conjunto sistemático de processos a fim de criar valor por meio do alinhamento. Inicialmente, é necessário alinhar as estratégias do sistema de segurança com as estratégias das unidades de negócio e da corporação, definindo o conjunto de serviços estratégicos a serem oferecidos. Posteriormente, o sistema de segurança precisa alinhar seus processos, de maneira que sejam capazes de executar a estratégia. Para tanto, é necessário desenvolver um plano estratégico que descreva como adquirir, desenvolver e prestar serviço estratégico às unidades operacionais, o qual passa a ser a base do mapa estratégico, do Balanced Scorecard (BSC), da iniciativa estratégica e do orçamento do sistema de segurança. Finalmente, o sistema de segurança deve fechar o ciclo, avaliando o desempenho de sua iniciativa, mediante técnicas como acordo de nível de serviço (SLA), feedback dos

clientes internos, avaliações pelos clientes e auditorias internas.

A terceira premissa é perceber o sistema de segurança como um sistema aberto, ou seja, um conjunto de elementos dinamicamente relacionados que desenvolvem atividades para atingir determinado objetivo. Como sistema apresenta seis elementos: objetivos, entradas, processos, saídas e feedback.

O sistema de segurança cria vantagem competitiva se for excelente em qualquer dos arquétipos estratégicos adotados pelas unidades de negócio: baixo custo, liderança de serviço, soluções completas para os clientes internos. As estratégias de intimidade ou de soluções para os clientes exigem do sistema de segurança construir parcerias com os clientes internos, sendo necessário mudar de especialistas funcionais para assessores de confiança e parceiros do negócio.

O sistema de segurança reforça a estratégia empresarial por meio do portfólio de serviços que oferecem aos clientes internos. Depois de definir os serviços estratégicos, o sistema de segurança precisa desenvolver sua estratégia de prestação dos serviços prometidos, a qual, deve ser traduzida em mapa estratégico e em BSC. Ao se desenvolver o mapa estratégico e o BSC do sistema de segurança, é útil vê-lo como um negócio dentro de um negócio.

O BSC apresenta quatro perspectivas: financeira, cliente, processo interno e aprendizado e crescimento. A perspectiva financeira do BSC do sistema de segurança apresenta dois componentes: eficiência e eficácia. O primeiro envolve questões tradicionais, como o custo dos serviços prestados e a observância do orçamento. O segundo é medido pelo impacto sobre a estratégia empresarial.

Em relação à perspectiva dos clientes, devemos levar em conta que o sistema de segurança tem dois tipos de clientes:

- Os gestores das unidades de negócio a quem prestam serviços diretamente.
- Os colaboradores ou clientes externos, que são beneficiários e destinatários dos serviços.

O sistema de segurança deve compreender as estratégias dos clientes internos e usar sua expertise funcional para criar e propor soluções que contribuam para o sucesso desses clientes.

A perspectiva dos processos internos apresenta três temas. O primeiro é a concentração na excelência operacional que impulsionará o objetivo de eficiência da perspectiva financeira. O segundo tema trata da maneira como o sistema de segurança gerencia o relacionamento com os clientes internos. E o último tema aborda o apoio estratégico à organização, impulsionando o componente de eficácia da estratégia, ao fornecer aos clientes internos novas capacidades que reforçam suas estratégias.

A perspectiva do aprendizado e crescimento trata das necessidades específicas dos recursos humanos do sistema de segurança, em termos de treinamento, tecnologia e clima de trabalho solidário. Em relação aos recursos humanos é necessário a preocupação com três componentes: programas de desenvolvimento de competências estratégicas; desenvolvimento da organização e da liderança; processo de gestão de desempenho.

Podemos perceber que se os objetivos do sistema de segurança forem desdobramentos dos objetivos de longo prazo desenvolvidos no planejamento estratégico da empresa, o sistema de segurança terá os seus processos relacionados com o negócio. Desta forma, o sistema de segurança terá a importância na obtenção do sucesso corporativo. Com esta potencialização, fez surgir a necessidade de departamentos de segurança com atuação científica, ou seja, não se admite mais o empirismo ou o "achismo" nas ações de segurança. Este contexto fez elevar o nível da prestação de serviços terceirizados de segurança ou de sistemas orgânicos de segurança. Para gerir o Sistema de Segurança é necessário um profissional altamente qualificado. Uma pessoa que gerencie de forma científica. Que saiba interagir a teoria com a prática. Alguém que tenha as competências (conhecimento, habilidade e comportamento) necessárias para ajudar a empresa a ser altamente competitiva. Esta necessidade criou a base para o surgimento dos cursos de graduação e pós-graduação na área de Segurança Empresarial. Cursos que são multidisciplinares e focados na prática. Mas para que os cursos cumpram com a sua missão é fundamental a existência de fontes de consulta. Baseado no exposto acima, é que estamos lançando mais uma edição da COLETÂNEA DE ARTIGOS. Uma coletânea de artigos que busca dotar os gestores dos conhecimentos necessários para serem capazes de fazer uma gestão científica e alinhada com a estratégia da empresa. Não queremos afirmar que os assuntos abordados nos diversos artigos estão esgotados, mas pontos importantes foram abordados. Além de abordarmos os pontos principais, temos o objetivo de despertar nos leitores a percepção da importância de aprofundamento dos diversos temas. São artigos produzidos por nossos sócios.

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

4 FALHAS COMETIDAS PELOS PROFISSIONAIS NO PROCESSO DE GESTÃO DE RISCOS

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.

Em razão do avanço tecnológico experimentado nos últimos anos, muitas funções que eram feitas de maneira manual já estão sendo realizadas de forma automatizada. Analisando o atual cenário empresarial, especificamente nas áreas de Gestão de Riscos, Governança, Compliance e Auditoria, percebemos uma grande evolução nos quesitos de Praticidade e Rapidez na execução das mais diversificadas tarefas.

No entanto, mesmo com o exponencial avanço das ferramentas de tecnologia, notamos que a ausência de uma metodologia eficaz pode refletir negativamente no desempenho profissional da equipe e da organização.

A partir disso, trazemos algumas falhas que podem atrapalhar o desempenho da organização quando são cometidas pela área de gerenciamento de riscos. Vale ressaltar que as atividades desenvolvidas pelos profissionais que fazem a Gestão de Riscos e Auditoria Interna nas empresas exigem muita perícia e competência.

Tecnologia e automação são duas importantes ferramentas de trabalho, mas de nada adianta sua organização dispor de software top de linha se não conta com uma metodologia eficiente.

Confira as principais falhas dos profissionais dos segmentos de Riscos, Governança e Compliance:

Mitigação de riscos em excesso

A falta de foco na gestão de riscos atrapalha o tratamento dos riscos que realmente são críticos, ao dedicar esforços no trato de riscos em que o custo/esforço de tratamento não excede o prejuízo do evento, levando em conta seu impacto e probabilidade;

APLICAÇÃO DE METODOLOGIA INADEQUADA

A metodologia na gestão dos riscos e suas respectivas ferramentas precisam ser selecionadas com assertividade, sendo definidas de acordo com o escopo e a natureza do projeto. A escolha inadequada resulta em excesso, escassez ou incoerência no tratamento de riscos adotado.

Não considerar a interconectividade entre riscos

Sem o cálculo da motricidade entre os riscos não sabemos quanto um risco pode influenciar os outros. Uma vez que um risco moderado influencia a ocorrência de um risco crítico, este deve ser tratado com prioridade.

Não fazer o registro e relato

A Gestão de Riscos precisa ser documentada, não podendo ficar só na fase das ideias ou no entendimento pessoal dos gestores. É preciso que ela esteja arquivada em um lugar de fácil acesso e que o relato seja realizado para os responsáveis. Assim, quando necessário, todos ficam cientes e sabem onde consultar.

Tendo em vista que o cenário de Riscos Corporativos no Brasil é volátil e está sempre enfrentando mudanças, os executivos estão começando a dar mais importância a perdas e reforçaram a importância das áreas de Riscos, Governança e Compliance, mas a carência de profissionais capacitados é um fator que pode vir a ter reflexos no futuro. Quando citamos capacitação, falamos de profissionais treinados para manusear ferramentas que vão agregar valor ao processo de gestão da empresa.

Conhecendo as dificuldades enfrentadas no dia a dia pelos profissionais de gestão de Riscos, Governança e Compliance, a Brasiliano INTERISK desenvolveu uma solução integrada que tem como objetivo estimular o aculturamento dos profissionais da área nas organizações, trazendo automação e praticidade. Comprovação deste fato são os seus diferenciais de mercado. Diferentemente da maioria das ferramentas de gerenciamento de riscos, a Brasiliano 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 SEGURANÇA PRIVADA COMO ESTRATÉGIA PARA PROTEGER EMPRESAS E PATRIMÔNIOS

Dr. Hebert Magno, CPSI, CIGR, CIEIE. Doutor Internacional
em Ciencias de la Seguridad, pela Corporación
Euro-Americana de Seguridad – Espanha.

INTRODUÇÃO

A segurança privada é uma área que tem ganhado cada vez mais destaque na proteção de empresas e patrimônios, principalmente em um cenário de crescente violência e insegurança nas cidades brasileiras. Empresas de diversos setores têm buscado investir em soluções de segurança para garantir a proteção de seus negócios e minimizar riscos.

A segurança privada se apresenta como uma estratégia eficaz para proteger empresas e patrimônios, já que oferece serviços especializados de vigilância patrimonial, monitoramento eletrônico, escolta armada, entre outros. Esses serviços são prestados por empresas de segurança privada que têm como objetivo garantir a proteção do patrimônio e das pessoas que trabalham ou frequentam o ambiente empresarial.

A contratação de serviços de segurança privada pode trazer diversos benefícios para as empresas. Além de reduzir riscos de roubo, invasão, vandalismo e outros crimes, a segurança privada também aumenta a sensação de segurança dos funcionários, clientes e visitantes, o que pode contribuir para melhorar a imagem e reputação da empresa.

No entanto, a contratação de serviços de segurança privada também apresenta desafios e cuidados que devem ser considerados pelas empresas. A privacidade e proteção de dados dos clientes e funcionários, o compliance com a legislação que regulamenta a segurança privada no Brasil e os custos e orçamento para implementação de soluções de segurança são alguns dos pontos que devem ser avaliados antes da contratação.

Nesse contexto, este artigo tem como objetivo apresentar a segurança privada como estratégia para proteger empresas e patrimônios, destacando seus benefícios e desafios. Serão abordados também os tipos de serviços oferecidos pelas empresas de segurança privada, como escolher o serviço adequado para as necessidades da empresa e os cuidados que devem ser considerados antes da contratação.

Por meio desse artigo, pretende-se contribuir para uma maior compreensão sobre a importância da segurança privada como estratégia para proteger empresas e patrimônios, além de fornecer informações relevantes para as empresas que desejam investir em soluções de segurança.

Além disso, a tecnologia tem sido uma grande aliada da segurança privada, permitindo a implementação de soluções de segurança mais eficientes e avançadas. Câmeras de vigilância com reconhecimento facial, sistemas de monitoramento remoto, sensores de presença e alarmes são algumas das tecnologias que têm sido utilizadas para aumentar a segurança de empresas e patrimônios.

Outro ponto importante a ser considerado é a escolha da empresa de segurança privada. É fundamental que a empresa contratante faça uma pesquisa prévia sobre a reputação e qualidade dos serviços prestados pela empresa, além de verificar se ela possui todas as autorizações e licenças necessárias para atuar no mercado.

Por fim, é importante destacar que a segurança privada deve ser vista como um investimento para a proteção do patrimônio e das pessoas, e não como um gasto desnecessário. A contratação de serviços de segurança privada pode evitar prejuízos financeiros e até mesmo salvar vidas em casos de emergência.

Diante desse cenário, este artigo tem como objetivo apresentar a segurança privada como estratégia para proteger empresas e patrimônios, abordando seus benefícios, desafios e cuidados a serem considerados. Através desse conteúdo, espera-se fornecer informações relevantes para as empresas que desejam investir em soluções de segurança e contribuir para uma maior compreensão sobre a importância da segurança privada como um recurso para garantir a proteção dos negócios e pessoas.

1. A IMPORTÂNCIA DA SEGURANÇA PRIVADA NA PROTEÇÃO DE EMPRESAS E PATRIMÔNIOS

1.1. Cenário atual de insegurança e violência nas cidades e seus impactos nas empresas

O cenário atual de insegurança e violência nas cidades tem gerado um impacto significativo nas empresas e investidores. A falta de segurança nas ruas, o aumento dos assaltos e roubos e a crescente incidência de crimes violentos têm levado empresários a buscar alternativas para proteger seus patrimônios e colaboradores. Nesse contexto, a segurança privada se apresenta como uma opção cada vez mais viável e eficiente.

As empresas enfrentam diversos desafios em relação à segurança, como a proteção de seus bens e equipamentos, a segurança de seus colaboradores e a prevenção de roubos e furtos. Além disso, a violência nas cidades pode afetar diretamente o desempenho das empresas, causando prejuízos financeiros e danos à imagem da empresa.

Por isso, a segurança privada é fundamental para a proteção de empresas e patrimônios. A contratação de serviços de segurança privada permite que as empresas contem com profissionais especializados na prevenção e reação a situações de risco, além da utilização de tecnologias avançadas de segurança, como câmeras de vigilância, sistemas de alarme e sensores de presença.

A segurança privada também é importante para a proteção dos colaboradores das empresas, garantindo um ambiente seguro e protegido para o trabalho. Isso contribui para o aumento da produtividade, motivação e bem-estar dos colaboradores, que se sentem mais seguros em seus locais de trabalho.

Vale ressaltar que a segurança privada no Brasil é regulamentada por leis específicas que estabelecem normas e regras para a atuação dos profissionais de segurança privada. É importante que as empresas contratantes estejam cientes das regulamentações aplicáveis e verifiquem se a empresa contratada cumpre todos os requisitos legais para atuar no mercado.

Porém, é importante destacar que a segurança privada deve ser vista como um complemento às medidas de segurança adotadas pelas empresas e não como uma solução isolada. As adoções de medidas preventivas, como a implementação de protocolos de segurança e treinamentos para colaboradores, também são fundamentais para garantir a proteção de empresas e patrimônios.

Por fim, é importante destacar que a segurança privada é um investimento para a proteção do patrimônio e das pessoas, e não um gasto desnecessário. A contratação de serviços de segurança privada pode evitar prejuízos financeiros e até mesmo salvar vidas em casos de emergência. Por isso, é fundamental que as empresas considerem a segurança privada como uma estratégia importante para a proteção de seus negócios e colaboradores.

1.2. Necessidade da segurança privada na proteção

do patrimônio, funcionários e clientes

A segurança privada é uma necessidade para muitas empresas que buscam proteger seus patrimônios, funcionários e clientes. Com o aumento da violência e criminalidade nas cidades, as empresas enfrentam cada vez mais desafios para manter seus negócios seguros. Além disso, o roubo de informações confidenciais e a ameaça de ataques cibernéticos também se tornaram uma preocupação para muitas empresas.

Nesse contexto, a segurança privada se torna uma estratégia eficaz para garantir a proteção dos bens e pessoas envolvidas nos negócios. A presença de profissionais de segurança, equipamentos de monitoramento e tecnologias avançadas ajuda a prevenir e responder a incidentes de segurança, reduzindo os riscos de prejuízos financeiros e danos à imagem da empresa.

Além disso, a segurança privada também desempenha um papel importante na proteção dos funcionários e clientes da empresa. Com a implementação de medidas de segurança, como a instalação de câmeras de segurança e sistemas de controle de acesso, é possível garantir a segurança de todos que frequentam o local, evitando incidentes que possam colocar em risco a integridade física das pessoas.

Outro fator importante é a proteção do patrimônio da empresa, que muitas vezes envolve ativos valiosos, como equipamentos, produtos, informações e propriedades. A segurança privada pode ajudar a prevenir roubos e vandalismo, garantindo a continuidade dos negócios e a preservação do patrimônio da empresa.

Além disso, a segurança privada também pode ser uma forma de aumentar a confiança dos clientes na empresa. Ao saber que a empresa se preocupa com a segurança de seus clientes e funcionários, os clientes podem se sentir mais seguros em frequentar o local, o que pode levar a um aumento nas vendas e na fidelização dos clientes.

Outra vantagem da segurança privada é a flexibilidade que ela oferece às empresas. Os serviços de segurança podem ser personalizados de acordo com as necessidades específicas de cada empresa, permitindo que elas escolham as medidas de segurança que melhor se adequem às suas atividades e riscos. Isso significa que as empresas podem contar com soluções de segurança sob medida, garantindo uma proteção mais eficaz e eficiente.

Por fim, a segurança privada também pode ser uma forma de cumprir obrigações legais e regulatórias. Algumas empresas, como as que atuam em setores financeiros, de saúde e de tecnologia, precisam cumprir requisitos específicos de segurança, visando a proteção de informações confidenciais e a prevenção de fraudes. Nesses casos, a segurança privada pode ser uma forma de atender a essas exigências e evitar sanções legais.

1.3. Como a segurança privada pode ser uma estratégia para

reduzir riscos e aumentar a efetividade dos negócios

A segurança privada pode ser uma estratégia efetiva para reduzir riscos e aumentar a efetividade dos negócios. Isso porque, além de proteger o patrimônio e os funcionários de uma empresa, a segurança privada também pode ajudar a evitar perdas financeiras e garantir a continuidade das operações.

Uma das principais maneiras pelas quais a segurança privada pode reduzir os riscos de uma empresa é por meio da prevenção de crimes. Os profissionais de segurança privada são treinados para identificar e lidar com possíveis ameaças, o que pode ajudar a evitar roubos, furtos, vandalismo e outras formas de crime.

Além disso, a presença de profissionais de segurança privada pode aumentar a sensação de segurança de funcionários e clientes, o que pode melhorar a reputação da empresa e aumentar a satisfação dos clientes. Isso pode, por sua vez, levar a um aumento nas vendas e na fidelidade do cliente.

Outra maneira pela qual a segurança privada pode ser uma estratégia para reduzir riscos e aumentar a efetividade dos negócios é por meio da proteção de informações confidenciais e de propriedade intelectual. Os profissionais de segurança privada podem ajudar a garantir que as informações e propriedade intelectual de uma empresa sejam mantidas em segurança, o que pode evitar perdas financeiras e a perda de vantagem competitiva.

Além disso, a segurança privada também pode ajudar a aumentar a eficiência das operações de uma empresa. Isso pode ser alcançado por meio da monitorização de equipamentos e do uso de tecnologia de segurança avançada, como câmeras de vigilância e sistemas de controle de acesso.

A segurança privada também pode ajudar a reduzir a responsabilidade legal de uma empresa. Isso porque, ao tomar medidas preventivas para garantir a segurança de funcionários e clientes, a empresa pode evitar possíveis ações legais por negligência.

Por fim, a segurança privada também pode ser uma estratégia efetiva para lidar com situações de emergência, como incêndios, desastres naturais e ataques terroristas. Os profissionais de segurança privada são treinados para lidar com essas situações de maneira eficaz, o que pode minimizar os danos e garantir a segurança de todos os envolvidos.

Em resumo, a segurança privada pode ser uma estratégia efetiva para reduzir riscos e aumentar a efetividade dos negócios. Além de proteger o patrimônio e os funcionários de uma empresa, a segurança privada pode ajudar a evitar perdas financeiras, proteger informações confidenciais, aumentar a eficiência das operações, reduzir a responsabilidade legal e lidar com situações de emergência de maneira eficaz.

2. TIPOS DE SERVIÇOS OFERECIDOS PELAS EMPRESAS DE SEGURANÇA PRIVADA

2.1. Vigilância patrimonial, escolta armada, monitoramento eletrônico, entre outros serviços.

As empresas de segurança privada oferecem diversos tipos de serviços para atender as necessidades de proteção de empresas e patrimônios. Entre os principais serviços oferecidos estão a vigilância patrimonial, escolta armada, monitoramento eletrônico, entre outros.

A vigilância patrimonial é um serviço muito comum, no qual os vigilantes fazem a segurança dos locais em que são designados, como prédios comerciais, condomínios, indústrias e eventos. Os profissionais responsáveis pela vigilância patrimonial são treinados para realizar rondas, controlar o acesso de pessoas e veículos, verificar o funcionamento dos equipamentos de segurança, dentre outras atividades.

Já a escolta armada é um serviço voltado para a proteção de cargas e valores, sendo muito utilizado por empresas que realizam transporte de valores, como bancos e empresas de segurança. Os profissionais que atuam nesse serviço são altamente treinados e capacitados para lidar com situações de risco, sempre acompanhados por veículos equipados com tecnologia de ponta para garantir a segurança.

O monitoramento eletrônico também é um serviço bastante procurado pelas empresas, consistindo na instalação de câmeras de segurança e outros dispositivos eletrônicos para detectar e prevenir invasões, furtos e outros tipos de delitos. As empresas de segurança privada podem oferecer desde o monitoramento remoto desses equipamentos até mesmo a presença física de profissionais especializados para realizar a vigilância em tempo real.

A segurança pessoal é uma das principais preocupações das pessoas que buscam os serviços de segurança privada. Ela abrange a proteção de indivíduos em situações de risco, como empresários, celebridades, políticos e outras pessoas que precisam de proteção especial. Os serviços de segurança pessoal podem incluir escolta armada, segurança em residências, segurança em eventos públicos, entre outros.

O serviço de transporte de valores é uma das principais atividades da segurança privada, que consiste no deslocamento de valores, como dinheiro, joias e documentos importantes, de um local para outro, com o objetivo de garantir a segurança desses bens. A segurança nesse tipo de transporte é fundamental, uma vez que os valores transportados podem ser alvo de roubo ou furto. As empresas especializadas em transporte de valores oferecem serviços de escolta armada, utilizando veículos equipados com sistemas de segurança avançados, além de profissionais altamente treinados e capacitados para lidar com situações de risco. A segurança nesse tipo de

transporte é regulada por normas específicas, que visam garantir a proteção dos valores transportados e a segurança dos profissionais envolvidos na atividade. O transporte de valores é uma atividade de alto risco, que exige muito cuidado e atenção por parte dos profissionais de segurança, além de equipamentos e tecnologias de ponta para garantir a segurança e efetividade do serviço.

Os grandes eventos, como shows, festivais e competições esportivas, atraem um grande número de pessoas e, portanto, exigem medidas de segurança especiais. As empresas de segurança privada oferecem serviços para garantir a segurança dos participantes e do público em geral. Isso inclui a supervisão de entradas e saídas, a identificação de pessoas suspeitas, o monitoramento de multidões e a coordenação com as forças policiais locais.

A formação de vigilantes é um processo essencial para garantir a qualidade dos serviços de segurança privada. Os cursos de formação são oferecidos por empresas especializadas e são obrigatórios para quem deseja trabalhar na área. Eles incluem aulas teóricas e práticas, abordando temas como segurança patrimonial, primeiros socorros, defesa pessoal, armamento e tiro, entre outros. Os cursos de formação de vigilantes são regulamentados pela Polícia Federal e devem ser renovados periodicamente.

É importante ressaltar que os serviços oferecidos pelas empresas de segurança privada são fundamentais para a proteção de empresas e patrimônios. Esses serviços podem ser personalizados de acordo com as necessidades de cada cliente, garantindo uma proteção eficiente e adequada para cada situação.

Além disso, a contratação de serviços de segurança privada pode ajudar a reduzir riscos e prejuízos para as empresas, contribuindo para a manutenção de um ambiente seguro e tranquilo para os funcionários e clientes.

Entretanto, é importante lembrar que a escolha de uma empresa de segurança privada deve ser feita com cautela e atenção. É preciso buscar empresas idôneas, que atuem de forma ética e que possuam profissionais capacitados e treinados para oferecer serviços de qualidade.

Por fim, a segurança privada pode ser vista como uma estratégia para reduzir riscos e aumentar a efetividade dos negócios, oferecendo serviços de proteção personalizados para cada situação e garantindo a tranquilidade e segurança de empresas, funcionários e clientes.

2.2. Como escolher o serviço de segurança privada adequado para as necessidades da empresa.

A escolha de um serviço de segurança privada para a proteção de uma empresa é uma tarefa importante e que exige uma análise criteriosa para garantir a efetividade do serviço prestado. Existem diversas empresas de segurança privada no mercado, e cada

uma oferece diferentes serviços e níveis de qualidade, o que pode gerar dúvidas na hora de escolher o prestador de serviço adequado.

O primeiro passo para escolher um serviço de segurança privada é avaliar as necessidades específicas da empresa. Isso envolve identificar os pontos críticos do negócio, como áreas com alto fluxo de pessoas, pontos de acesso a bens de valor, horários de maior risco, entre outros fatores relevantes. Com essa análise em mãos, é possível buscar um prestador de serviços que atenda às necessidades específicas da empresa.

Outro aspecto importante a ser considerado é a reputação da empresa de segurança privada. Para isso, é fundamental verificar se a empresa possui licença para operar, bem como sua regularidade junto aos órgãos de fiscalização. Além disso, é possível pesquisar a reputação da empresa por meio de avaliações de clientes e verificar se ela está associada a entidades de classe.

A qualificação dos profissionais que compõem o serviço de segurança privada também é um fator relevante. Verificar se a empresa possui um programa de treinamento constante para seus funcionários e se estes são capacitados para lidar com situações de risco é fundamental. Além disso, a experiência dos profissionais em situações similares às que a empresa enfrenta é um ponto a ser avaliado.

Outra questão importante é o tipo de tecnologia utilizada pela empresa de segurança privada. Verificar se a empresa possui equipamentos modernos e eficientes, como câmeras de alta resolução e sistemas de monitoramento avançados, é fundamental para garantir a efetividade do serviço.

O tipo de contrato de prestação de serviços é outro aspecto relevante a ser considerado. É importante avaliar se o contrato oferece flexibilidade para a empresa, permitindo ajustes e adaptações conforme as necessidades mudam. Além disso, é fundamental verificar as condições de pagamento e as penalidades em caso de descumprimento do contrato.

A transparência é um aspecto relevante na escolha de uma empresa de segurança privada. Verificar se a empresa apresenta clareza em relação aos serviços oferecidos, valores cobrados, e se oferece um canal de comunicação direta com os clientes é fundamental para garantir uma relação de confiança.

Por fim, é importante avaliar os custos envolvidos na contratação de um serviço de segurança privada. É preciso considerar os valores cobrados pela empresa, bem como os investimentos necessários em tecnologia e treinamento de funcionários. É fundamental buscar um equilíbrio entre o valor investido e a qualidade do serviço prestado.

2.3. Importância de avaliar a reputação e a experiência da empresa de segurança privada

Ao buscar um serviço de segurança privada para proteger a sua empresa, é importante

avaliar a reputação e a experiência da empresa que irá contratar. Afinal, a segurança de seu negócio estará nas mãos desses profissionais.

Uma das primeiras coisas que você pode fazer é pesquisar sobre a empresa em questão. Busque informações sobre sua atuação no mercado, sua história e seus clientes atendidos. É importante também verificar se a empresa possui certificações e licenças necessárias para atuar no setor.

Além disso, é importante avaliar a experiência dos profissionais que serão responsáveis pela segurança de sua empresa. Verifique se a empresa possui um processo seletivo rigoroso e investe em treinamento e capacitação contínua de seus funcionários.

Outro aspecto a ser considerado é a tecnologia utilizada pela empresa. Verifique se ela está sempre atualizada e se a empresa investe em inovações que possam trazer mais eficiência e segurança ao serviço prestado.

Além disso, avalie a flexibilidade da empresa em se adaptar às necessidades específicas de sua empresa. Cada negócio possui suas particularidades e é importante que o serviço de segurança seja personalizado e adequado às suas demandas.

Também é importante avaliar a transparência da empresa em relação aos seus processos e contratos. Verifique se as condições e valores acordados estão claros e bem definidos, evitando possíveis surpresas no futuro.

Ao considerar esses aspectos ao escolher um serviço de segurança privada, você estará tomando medidas importantes para garantir a proteção de sua empresa e de seus colaboradores.

Além de avaliar a reputação e a experiência da empresa de segurança privada, também é importante considerar a capacidade técnica da empresa. Isso envolve verificar se a empresa tem tecnologia de ponta para garantir a segurança dos clientes, como câmeras de vigilância, alarmes, sensores, entre outros. Além disso, é importante avaliar se a empresa tem uma equipe bem treinada e capacitada para lidar com situações de risco e garantir a segurança dos clientes.

Outro aspecto a considerar ao escolher um serviço de segurança privada é o custo. É importante avaliar as diferentes opções de serviços disponíveis e comparar os preços oferecidos pelas empresas de segurança privada. É importante lembrar que o custo não deve ser o único fator a ser considerado na escolha da empresa de segurança privada, pois a segurança não é um aspecto que deve ser negligenciado.

Também é importante considerar a flexibilidade da empresa de segurança privada em relação aos serviços oferecidos. Cada empresa tem necessidades específicas de segurança, e é importante que a empresa de segurança privada ofereça soluções personalizadas de acordo com as necessidades de cada cliente. Isso inclui serviços

como escolta armada, segurança em eventos, vigilância patrimonial, entre outros.

Por fim, é importante verificar se a empresa de segurança privada tem uma cultura de segurança forte e se está comprometida com a segurança dos clientes. Isso inclui a realização de treinamentos regulares para a equipe, a implementação de políticas e procedimentos de segurança, e a manutenção de uma cultura de segurança forte em toda a empresa.

Em suma, escolher o serviço de segurança privada adequado para as necessidades da empresa requer uma análise cuidadosa de vários fatores, incluindo a reputação e experiência da empresa, capacidade técnica, custo, flexibilidade, capacidade de adaptação, cultura de segurança e compromisso com a segurança dos clientes. Ao avaliar cuidadosamente esses fatores, é possível encontrar uma empresa de segurança privada confiável e eficaz para proteger os negócios e o patrimônio da empresa.

3. BENEFÍCIOS DA SEGURANÇA PRIVADA PARA EMPRESAS E PATRIMÔNIOS

3.1. Redução de riscos de roubo, invasão, vandalismo e outros crimes.

A segurança privada é uma estratégia importante para proteger empresas e patrimônios, e traz consigo uma série de benefícios significativos. Um dos principais benefícios é a redução de riscos de roubo, invasão, vandalismo e outros crimes que podem afetar as empresas e seus ativos. Com a presença de seguranças capacitados e equipamentos de monitoramento de alta tecnologia, a segurança privada pode ajudar a prevenir e reduzir a incidência desses crimes.

Além disso, a segurança privada também pode ajudar a melhorar a eficiência e produtividade das empresas, ao permitir que os funcionários trabalhem em um ambiente seguro e livre de distrações externas. Isso pode levar a uma redução do tempo de inatividade e a uma maior qualidade do trabalho realizado.

Outro benefício importante da segurança privada é a proteção da imagem da empresa. A ocorrência de incidentes de segurança pode ter um impacto significativo na reputação da empresa e na percepção de seus clientes e parceiros. Ao investir em segurança privada, as empresas podem garantir a proteção de sua imagem e reputação, bem como a confiança de seus stakeholders.

Além disso, a segurança privada também pode ser uma maneira eficaz de evitar perdas financeiras. Através de medidas de segurança adequadas, como monitoramento de acesso, vigilância e patrulha, as empresas podem proteger seus ativos financeiros e evitar perdas decorrentes de roubos e outras atividades criminosas.

Outro benefício importante da segurança privada é a capacidade de personalização dos serviços prestados. Cada empresa tem necessidades únicas em termos de segurança, e as empresas de segurança privada podem adaptar seus serviços para atender a essas necessidades específicas. Isso significa que as empresas podem escolher os serviços de segurança que melhor se adequam às suas necessidades e orçamento.

Além disso, a segurança privada também pode trazer benefícios em termos de segurança pessoal. Muitas empresas oferecem serviços de escolta pessoal para executivos e outras pessoas de alto nível, garantindo sua segurança em situações de risco. Isso pode ser especialmente importante em áreas de alta criminalidade ou em situações de ameaças de sequestro e extorsão.

Outro benefício da segurança privada é a disponibilidade de tecnologias de monitoramento avançadas. Empresas de segurança privada podem oferecer uma variedade de soluções tecnológicas, como câmeras de vigilância, sistemas de alarme e rastreamento de veículos. Essas tecnologias podem ajudar a monitorar as atividades dentro e ao redor das empresas, melhorando a capacidade de resposta a incidentes de segurança.

A segurança privada também pode ajudar a prevenir conflitos internos nas empresas. Por exemplo, a presença de segurança em eventos corporativos pode ajudar a manter a ordem e a evitar conflitos entre funcionários ou entre funcionários e clientes.

Além da redução de riscos, a segurança privada também pode trazer outros benefícios para as empresas e patrimônios. Um deles é a sensação de segurança para funcionários e clientes. Quando há uma equipe de segurança presente, as pessoas se sentem mais tranquilas e confiantes para frequentar o local, o que pode aumentar o fluxo de clientes e melhorar a imagem da empresa.

Outro benefício é a prevenção de perdas financeiras. A segurança privada pode ajudar a identificar e deter fraudes, roubos internos e outras atividades ilegais que possam estar ocorrendo dentro da empresa. Isso pode resultar em economias significativas para a organização a longo prazo.

Além disso, a segurança privada também pode contribuir para a eficiência operacional da empresa. Com a presença de uma equipe de segurança, os funcionários podem se concentrar em suas tarefas sem se preocupar com possíveis ameaças de segurança. Isso pode aumentar a produtividade e melhorar a qualidade do trabalho realizado.

Outro benefício é a flexibilidade de atuação. As empresas de segurança privada podem oferecer uma variedade de serviços para atender às necessidades específicas de cada cliente. Isso inclui desde serviços de vigilância patrimonial até monitoramento eletrônico e escolta armada. A flexibilidade de atuação permite que as empresas escolham o tipo de serviço que melhor se adapta às suas necessidades.

Além disso, as empresas de segurança privada costumam ter uma ampla gama de recursos e tecnologias disponíveis para ajudar na proteção de seus clientes. Isso pode

incluir câmeras de segurança, sistemas de alarme, sistemas de controle de acesso, entre outros recursos. Essas tecnologias podem aumentar a eficácia da equipe de segurança e oferecer um nível mais alto de proteção para as empresas e patrimônios.

Por fim, é importante mencionar que a segurança privada também pode ajudar a cumprir obrigações legais e regulatórias. Empresas em determinados setores, como bancos e empresas de transporte de valores, são obrigadas a contratar serviços de segurança privada para cumprir as regulamentações. Ao contratar uma empresa de segurança privada, essas empresas podem garantir que estão cumprindo com todas as obrigações legais e regulatórias pertinentes.

4. DESAFIOS E CUIDADOS NA CONTRATAÇÃO DE SERVIÇOS DE SEGURANÇA PRIVADA

4.1. Privacidade e proteção de dados dos clientes e funcionários.

A contratação de serviços de segurança privada traz inúmeras vantagens para empresas e patrimônios, mas também é preciso levar em consideração os desafios e cuidados necessários para garantir a segurança e proteção dos clientes e funcionários.

Um dos principais desafios na contratação de serviços de segurança privada é a privacidade e proteção de dados dos clientes e funcionários da empresa contratante. É importante que a empresa de segurança privada siga as normas e leis de proteção de dados, garantindo que as informações não sejam divulgadas ou utilizadas de forma inadequada.

Além disso, é preciso considerar a segurança e proteção dos próprios funcionários da empresa de segurança privada. É necessário garantir que eles tenham treinamento adequado, equipamentos de segurança e condições de trabalho satisfatórias para que possam desempenhar suas funções com eficácia e segurança.

Outro desafio é a seleção adequada dos profissionais que irão compor a equipe de segurança privada. É necessário que a empresa de segurança privada realize uma rigorosa seleção e treinamento dos profissionais, verificando suas qualificações, antecedentes criminais e conduta ética.

Ainda na questão de seleção de profissionais, é importante que a empresa de segurança privada tenha uma política clara de diversidade e inclusão, buscando a representatividade de diferentes grupos e garantindo um ambiente de trabalho inclusivo e respeitoso.

Outro cuidado importante é a escolha do tipo de serviço de segurança privada adequado para as necessidades da empresa. É preciso avaliar as particularidades do patrimônio, as necessidades de proteção dos funcionários e clientes e os riscos envolvidos antes de contratar um serviço específico.

Além disso, é fundamental que a empresa contratante esteja atenta às condições contratuais e às obrigações da empresa de segurança privada. É importante que as cláusulas do contrato sejam claras e objetivas, estabelecendo as responsabilidades de cada parte envolvida e as obrigações que devem ser cumpridas.

Outro cuidado importante é a fiscalização constante do serviço prestado pela empresa de segurança privada. A empresa contratante deve estabelecer um canal de comunicação para reportar qualquer irregularidade ou problema, garantindo que o serviço seja prestado de forma eficaz e segura.

Com o crescente aumento da criminalidade e da violência, a contratação de serviços de segurança privada tem se tornado cada vez mais comum. Entretanto, essa prática demanda cuidados e atenção especial, principalmente quando se trata de privacidade e proteção de dados dos clientes e funcionários.

É importante ressaltar que, ao contratar uma empresa de segurança privada, é preciso estar ciente dos tipos de informações que serão compartilhadas com ela. Dados pessoais sensíveis, como nome completo, endereço, RG, CPF e informações bancárias, devem ser protegidos e utilizados somente para fins de segurança. É necessário que a empresa contratada tenha políticas e procedimentos adequados de proteção de dados e que siga as normas e legislações aplicáveis.

Outro ponto importante é a conscientização dos funcionários da empresa contratante e da empresa de segurança privada em relação à privacidade e proteção de dados. Os colaboradores devem estar cientes das políticas de privacidade e segurança da empresa, além de receberem treinamentos sobre a importância da proteção de dados.

Além disso, é fundamental que a empresa contratada esteja em conformidade com as normas e regulamentações do setor. É importante verificar se a empresa possui as devidas licenças e autorizações para atuar na área de segurança privada, além de verificar se ela segue as normas de segurança estabelecidas pelo setor.

Por fim, é importante que a empresa contratante tenha uma postura ética e responsável em relação à contratação de serviços de segurança privada. É fundamental que a empresa respeite as leis e normas vigentes e que não utilize a segurança privada como meio de repressão ou intimidação de funcionários ou clientes.

Em resumo, a contratação de serviços de segurança privada é uma prática comum, mas que demanda atenção e cuidado especial com a privacidade e proteção de dados dos clientes e funcionários. É fundamental que as empresas contratantes e contratadas sigam as normas e regulamentações do setor, além de conscientizar os funcionários sobre a importância da proteção de dados e privacidade. A avaliação dos riscos e a elaboração de um plano de segurança adequado também são essenciais para garantir a segurança e privacidade dos envolvidos.

4.2. Compliance com a legislação que regulamenta a segurança privada no Brasil.

O Brasil possui uma legislação bastante rigorosa para a segurança privada, com o objetivo de garantir a proteção da população e a integridade das empresas. As empresas que atuam nesse setor precisam estar em compliance com as leis e regulamentações aplicáveis, o que exige um cuidado especial com a gestão de riscos e a elaboração de planos de segurança adequados.

A legislação que regulamenta a segurança privada no Brasil é composta por diversas normas e regulamentações, como a Lei nº 7.102/83, que estabelece as diretrizes para a segurança privada e os serviços de transporte de valores, além de normas da Polícia Federal e da Agência Nacional de Vigilância Sanitária (Anvisa), que regulamentam o porte de armas, o treinamento dos vigilantes e a segurança em hospitais, por exemplo.

Entre os principais pontos que as empresas de segurança privada devem observar para estar em compliance com a legislação estão: obter as devidas licenças e autorizações para atuar no setor, seguir as normas de segurança estabelecidas pelas autoridades competentes, manter os registros atualizados e em conformidade com a legislação, e contratar apenas profissionais treinados e capacitados para atuar na área.

Outro aspecto importante é a gestão de riscos. As empresas de segurança privada devem realizar uma avaliação dos riscos para identificar possíveis vulnerabilidades e ameaças e elaborar um plano de segurança adequado para cada situação. Além disso, é preciso ter políticas e procedimentos de segurança que garantam a integridade dos dados e a privacidade dos clientes e funcionários.

A adoção de práticas de compliance na segurança privada é fundamental para evitar riscos e prevenir incidentes. As empresas que adotam uma cultura de compliance têm mais chances de serem bem-sucedidas em um mercado altamente competitivo, além de estarem mais preparadas para enfrentar crises e situações de emergência.

A implementação de um programa de compliance na segurança privada pode incluir a criação de um código de conduta, a realização de treinamentos regulares, a revisão constante das políticas e procedimentos de segurança, a avaliação de riscos e a revisão das licenças e autorizações necessárias para a atuação no setor.

A segurança privada é um setor fundamental para a proteção de empresas e pessoas no Brasil, e por isso é essencial que as empresas desse ramo estejam em conformidade com a legislação e regulamentações aplicáveis. Além disso, a compliance na segurança privada também pode trazer diversos benefícios, como a melhoria da reputação da empresa, o aumento da confiança dos clientes e a redução de custos com processos legais e multas.

Uma das principais preocupações das empresas de segurança privada em relação à

compliance é a segurança da informação. Com a crescente digitalização dos processos e a coleta de dados cada vez mais relevantes para a segurança, a privacidade e proteção de dados dos clientes e funcionários se tornou uma questão crítica. Por isso, é necessário que as empresas tenham políticas claras de proteção de dados e privacidade, além de mecanismos de segurança adequados para garantir a integridade dos dados.

Outro desafio para a compliance na segurança privada é a constante atualização das normas e regulamentações. As empresas precisam estar atentas às mudanças na legislação e regulamentação, além de se adaptarem às novas exigências de segurança e proteção de dados. Isso requer um investimento constante em treinamentos e capacitação dos profissionais envolvidos na gestão de riscos e na implementação dos planos de segurança.

Para garantir a compliance na segurança privada, as empresas também devem ter um sistema eficiente de monitoramento e auditoria interna. Isso permite que possíveis violações ou irregularidades sejam identificadas rapidamente e corrigidas antes que se tornem problemas mais graves. Além disso, a auditoria interna também pode ajudar a empresa a identificar possíveis áreas de melhoria e implementar novas políticas e procedimentos de segurança.

A compliance na segurança privada também pode ser um desafio em relação ao treinamento e capacitação dos profissionais. É essencial que os vigilantes e demais profissionais envolvidos na segurança privada tenham treinamentos regulares e estejam capacitados para lidar com as diversas situações de risco que podem ocorrer. Isso inclui desde o treinamento no uso de armas até a gestão de crises e o atendimento ao público.

Por fim, a compliance na segurança privada requer um compromisso constante da empresa com a ética e a transparência. É essencial que a empresa mantenha uma cultura de integridade e honestidade, além de estar comprometida com a prevenção de crimes e irregularidades. Isso pode ser alcançado por meio da adoção de políticas claras de conduta, da promoção de um ambiente de trabalho saudável e da transparência nas relações com clientes e autoridades reguladoras.

Em resumo, a compliance na segurança privada é um desafio constante, mas é essencial para garantir a proteção da população e das empresas. As empresas que atuam nesse setor devem estar em conformidade com as leis e regulamentações aplicáveis, além de investir em treinamentos e capacitação dos profissionais envolvidos na gestão de riscos e na implementação dos planos de segurança. Com uma cultura de ética e transparência, as empresas

4.3. Custos e orçamento para implementação de soluções de segurança privada.

A segurança privada é um investimento importante para empresas e indivíduos que desejam proteger seus bens e garantir a segurança pessoal. No entanto, a implementação

de soluções de segurança privada pode envolver custos significativos e é importante que as empresas e indivíduos levem em conta esses custos ao planejar sua estratégia de segurança.

O primeiro passo para estimar os custos da segurança privada é avaliar as necessidades específicas da empresa ou indivíduo. Isso envolve uma análise detalhada dos riscos envolvidos e das soluções de segurança necessárias para mitigá-los. Dependendo das necessidades de segurança, os custos podem variar significativamente.

Uma das soluções de segurança privada mais comuns é a contratação de vigilantes armados ou desarmados. Os custos dessa solução podem variar de acordo com a localização, tamanho e complexidade das instalações a serem protegidas. Além disso, a necessidade de vigilância 24 horas por dia pode aumentar significativamente os custos.

Outra solução de segurança privada é a instalação de sistemas de monitoramento, como câmeras de segurança e alarmes. Esses sistemas podem ser uma alternativa mais econômica à contratação de vigilantes, mas ainda envolvem custos significativos, como a compra e instalação dos equipamentos, a manutenção e a operação dos sistemas.

A terceira opção de segurança privada é a contratação de serviços de escolta e proteção pessoal, que é uma solução mais voltada para a segurança pessoal do que para a proteção de bens. Esses serviços geralmente envolvem um único agente de segurança para acompanhar uma pessoa em viagens ou eventos, e os custos podem variar dependendo do nível de treinamento e experiência do agente

É importante ressaltar que, além dos custos diretos, a implementação de soluções de segurança privada também pode envolver custos indiretos, como a necessidade de treinamento e capacitação dos funcionários, a implementação de políticas de segurança e a atualização regular dos sistemas de segurança. Esses custos podem ser considerados um investimento para garantir a efetividade da segurança privada.

Outro fator que pode influenciar os custos da segurança privada é a reputação e a qualidade dos serviços prestados pelas empresas de segurança privada. É importante escolher uma empresa que seja confiável e tenha uma boa reputação no mercado, o que pode significar custos mais elevados, mas também pode garantir uma solução de segurança mais eficaz.

Para ajudar a gerenciar os custos da segurança privada, as empresas e indivíduos podem considerar a terceirização dos serviços de segurança privada. Isso pode trazer benefícios significativos, como redução de custos com funcionários e treinamento, além de garantir acesso a profissionais altamente capacitados e equipamentos de segurança de última geração.

Finalmente, é importante lembrar que o orçamento para soluções de segurança privada deve ser visto como um investimento na proteção dos bens e da segurança pessoal. Portanto, é fundamental que as empresas e indivíduos

Considerem o custo-benefício das soluções de segurança privada escolhidas, avaliando não apenas os custos envolvidos, mas também os benefícios em termos de proteção e redução de riscos.

Além disso, as empresas e indivíduos devem estar cientes das possíveis mudanças nos custos da segurança privada ao longo do tempo. Por exemplo, o aumento da criminalidade em uma determinada região pode levar a um aumento nos custos da segurança privada, à medida que a demanda por esses serviços aumenta. Portanto, é importante monitorar regularmente os custos da segurança privada e revisar periodicamente as soluções de segurança implementadas para garantir sua eficácia e adequação.

Outra maneira de gerenciar os custos da segurança privada é considerar a implementação de soluções de segurança em fases, priorizando as áreas ou bens que apresentam maior risco. Isso pode ajudar a reduzir os custos iniciais e permitir que as empresas e indivíduos implementem soluções de segurança mais abrangentes ao longo do tempo, conforme o orçamento permitir.

Além dos custos diretos envolvidos na implementação de soluções de segurança privada, as empresas e indivíduos também devem considerar os custos associados à não implementação de medidas de segurança adequadas. A falta de segurança pode resultar em perdas financeiras significativas, danos à reputação da empresa e, em casos extremos, colocar em risco a segurança pessoal.

Por fim, é importante lembrar que o sucesso da segurança privada depende não apenas das soluções de segurança implementadas, mas também da conscientização e envolvimento dos funcionários e usuários das instalações protegidas. Portanto, as empresas e indivíduos devem investir em treinamento e conscientização em segurança, a fim de garantir que todos os envolvidos estejam cientes dos riscos envolvidos e das medidas de segurança apropriadas a serem tomadas.

Em resumo, os custos envolvidos na implementação de soluções de segurança privada devem ser cuidadosamente avaliados e gerenciados, a fim de garantir a eficácia e adequação dessas soluções. As empresas e indivíduos devem considerar suas necessidades específicas de segurança, bem como o custo-benefício das soluções de segurança implementadas, e monitorar regularmente os custos e a eficácia dessas soluções ao longo do tempo. Com o planejamento adequado e o gerenciamento efetivo de custos, a segurança privada pode ser uma solução eficaz para proteger bens e garantir a segurança pessoal.

CONCLUSÃO

A segurança privada é uma estratégia cada vez mais importante para proteger empresas e patrimônios em um mundo cada vez mais complexo e perigoso. Como vimos, existem muitos desafios e cuidados a serem considerados na contratação de serviços de segurança privada, desde a conformidade com as leis e regulamentações até a gestão

efetiva de custos e orçamentos.

No entanto, quando implementados corretamente, os serviços de segurança privada podem fornecer proteção efetiva contra riscos como roubo, vandalismo e violência, bem como oferecer tranquilidade e paz de espírito para as empresas e indivíduos envolvidos.

Ao escolher soluções de segurança privada, é importante considerar as necessidades específicas de segurança e avaliar cuidadosamente os custos e benefícios de diferentes opções. Além disso, é essencial garantir que todas as soluções de segurança sejam conformes com as leis e regulamentações aplicáveis e que a conscientização em segurança seja promovida em toda a organização.

Em última análise, a segurança privada é uma ferramenta valiosa para proteger empresas e patrimônios e deve ser considerada como parte de uma estratégia de gestão de riscos abrangente. Com planejamento cuidadoso e implementação eficaz, as soluções de segurança privada podem ajudar a garantir a segurança pessoal e financeira, permitindo que as empresas e indivíduos se concentrem em suas atividades principais e alcancem seus objetivos com confiança.

Pode se dizer que, a segurança privada também pode ser uma ferramenta importante para proteger a reputação de uma empresa. A imagem de uma empresa pode ser prejudicada se ela for vítima de um crime ou incidente de segurança. Por isso, investir em soluções de segurança privada pode ser visto como um sinal de comprometimento com a proteção de seus funcionários e clientes, bem como do patrimônio e dos ativos da empresa.

Outro benefício importante da segurança privada é a capacidade de personalizar as soluções de segurança de acordo com as necessidades específicas de cada empresa. Por exemplo, algumas empresas podem precisar de segurança de acesso restrito para suas instalações, enquanto outras podem precisar de soluções de segurança para proteger a cadeia de suprimentos ou gerenciar riscos de segurança digital. As soluções de segurança privada podem ser adaptadas para atender a essas necessidades exclusivas, proporcionando uma camada adicional de proteção personalizada.

Com isso, a segurança privada também pode ser um fator importante na melhoria da produtividade e do bem-estar dos funcionários. Funcionários que se sentem seguros em seu ambiente de trabalho são mais propensos a serem produtivos e a terem uma atitude positiva em relação à empresa. A segurança privada também pode ajudar a reduzir o estresse e a ansiedade dos funcionários, permitindo que se concentrem em suas tarefas principais sem se preocupar com a segurança.

A segurança privada também pode ser vista como um investimento estratégico para o futuro. Com a crescente complexidade dos riscos de segurança, as empresas precisam estar preparadas para lidar com ameaças em constante evolução. As soluções de segurança privada podem fornecer proteção contra riscos emergentes, permitindo que as empresas se adaptem às mudanças do ambiente de segurança e estejam preparadas

para enfrentar os desafios futuros.

Em resumo, a segurança privada pode ser uma estratégia valiosa para proteger empresas e patrimônios. Embora haja desafios e cuidados a serem considerados, as soluções de segurança privada podem fornecer proteção efetiva, melhorar a reputação da empresa, personalizar soluções de segurança, melhorar a produtividade e o bem-estar dos funcionários e preparar a empresa para enfrentar os desafios futuros. Portanto, é importante considerar a segurança privada como parte de uma estratégia de gestão de riscos abrangente e investir em soluções de segurança personalizadas e eficazes para proteger os ativos e as pessoas da empresa.

A IMPORTÂNCIA DA PREVENÇÃO DE FRAUDES NO AMBIENTE CORPORATIVO

Dr. Hebert Magno, CPSI, CIGR, CIEIE. Doutor Internacional
em Ciencias de la Seguridad, pela Corporación
Euro-Americana de Seguridad – Espanha.

Como um assistente que está sempre buscando ajudar, acredito que é importante abordar um tema muito relevante para as empresas atualmente, que é a prevenção de fraudes no ambiente corporativo. Neste artigo, vamos discutir sobre a importância da prevenção de fraudes, entender o que é a fraude corporativa, seus tipos, impactos e melhores práticas para prevenção. Acompanhe!

Introdução à prevenção de fraudes no ambiente corporativo

O ambiente corporativo é um ambiente propício para a ocorrência de fraudes. Com o avanço tecnológico, a sofisticação dos fraudadores aumenta, tornando-se cada vez mais difícil identificar e prevenir a fraude. Além disso, as empresas estão sempre em busca de crescimento e lucratividade, o que muitas vezes pode acabar comprometendo a segurança e integridade da empresa. Por isso, é fundamental que as empresas invistam em medidas preventivas para evitar a ocorrência de fraudes.

Entendendo a fraude corporativa

A fraude corporativa é um ato ilegal realizado por um indivíduo ou grupo, com o objetivo de obter vantagem financeira ou benefícios pessoais em detrimento da empresa ou de seus acionistas. A fraude pode ser cometida por funcionários, fornecedores, clientes ou qualquer pessoa que tenha acesso aos dados da empresa.

Existem diversos tipos de fraude corporativa, alguns dos mais comuns são: desvio de

dinheiro, corrupção, falsificação de documentos, roubo de informações, entre outros. A fraude pode ser realizada de forma oculta ou explícita, sendo que algumas vezes os próprios colaboradores da empresa podem estar envolvidos.

O impacto da fraude corporativa nas empresas

A fraude corporativa pode ter um impacto significativo na empresa, podendo levar a perdas financeiras, danos à reputação, perda de clientes, entre outros. Além disso, a ocorrência de fraudes pode levar a processos judiciais, multas e penalidades, o que pode comprometer ainda mais a saúde financeira da empresa. Por isso, é fundamental que as empresas adotem medidas preventivas para evitar a ocorrência de fraudes.

A importância da prevenção de fraudes no ambiente corporativo

A prevenção de fraudes é fundamental para garantir a integridade e segurança das empresas. Investir em medidas preventivas pode ajudar a evitar a ocorrência de fraudes, reduzir riscos e proteger a empresa contra possíveis perdas financeiras. Além disso, a prevenção de fraudes pode ajudar a fortalecer a cultura ética da empresa, demonstrando aos colaboradores, clientes e fornecedores que a empresa tem um compromisso com a integridade e transparência.

Implementação de um programa de prevenção de fraudes

Para implementar um programa de prevenção de fraudes, é fundamental que as empresas adotem medidas preventivas eficazes. Algumas das melhores práticas incluem a identificação de riscos, treinamento de funcionários, monitoramento de atividades, auditoria interna, definição de políticas e procedimentos, entre outras.

É importante lembrar que a prevenção de fraudes é uma tarefa contínua, que deve ser realizada de forma sistemática e estratégica. A empresa deve estar sempre atenta aos possíveis riscos e adotar as medidas preventivas necessárias para evitar a ocorrência de fraudes.

Técnicas e melhores práticas para prevenção de fraudes

Existem diversas técnicas e melhores práticas que podem ser adotadas pelas empresas para prevenir a fraude corporativa. Algumas das principais incluem:

- Identificação de riscos: é fundamental que a empresa identifique e avalie os possíveis riscos de fraude, a fim de adotar medidas preventivas eficazes.
- Treinamento de funcionários: é importante que os colaboradores da empresa estejam conscientes dos riscos de fraude e saibam como identificar possíveis irregularidades.

- Monitoramento de atividades: a empresa deve monitorar as atividades dos colaboradores, fornecedores e clientes, a fim de identificar possíveis irregularidades.
- Auditoria interna: a realização de auditorias internas pode ajudar a identificar possíveis fraudes e irregularidades.
- Políticas e procedimentos: a empresa deve definir políticas e procedimentos claros e objetivos, a fim de garantir a integridade e transparência da empresa.

O papel da tecnologia na prevenção de fraudes

A tecnologia tem um papel fundamental na prevenção de fraudes. Existem diversas ferramentas tecnológicas que podem ser utilizadas pelas empresas para identificar e prevenir a fraude corporativa. Alguns exemplos incluem a implementação de sistemas de monitoramento, ferramentas de análise de dados, sistemas de detecção de anomalias, entre outros. É importante que a empresa esteja sempre atualizada em relação às novas tecnologias e ferramentas disponíveis para prevenção de fraudes.

Os benefícios da prevenção de fraudes para as empresas

Investir em prevenção de fraudes pode trazer diversos benefícios para as empresas, como:

- Redução de riscos e perdas financeiras;
- Proteção da reputação da empresa;
- Fortalecimento da cultura ética da empresa;
- Aumento da confiança de clientes e fornecedores;
- Cumprimento de leis e regulamentos.

Conclusão

A prevenção de fraudes é fundamental para garantir a integridade, segurança e saúde financeira das empresas. Investir em medidas preventivas pode ajudar a proteger a empresa contra possíveis perdas financeiras, além de fortalecer a cultura ética da empresa. É importante que as empresas adotem as melhores práticas e estejam sempre atualizadas em relação às novas tecnologias disponíveis para prevenção de fraudes.

Se você gostou deste conteúdo e deseja saber mais sobre como proteger sua empresa contra fraudes, entre em contato conosco. Estamos à disposição para ajudá-lo.

COMO A TECNOLOGIA ESTÁ TRANSFORMANDO A SEGURANÇA PRIVADA

Dr. Hebert Magno, CPSI, CIGR, CIEIE. Doutor Internacional
em Ciencias de la Seguridad, pela Corporación
Euro-Americana de Seguridad – Espanha.

INTRODUÇÃO

Nos últimos anos, a tecnologia tem sido uma força disruptiva em vários setores, e a segurança privada não é exceção. A tecnologia está revolucionando a maneira como as empresas de segurança privada trabalham, criando novos desafios e oportunidades. Neste artigo, exploraremos as tendências que estão moldando a segurança privada no século XXI e como as empresas de segurança estão se adaptando a elas.

Um dos desenvolvimentos mais importantes na tecnologia de segurança privada é a utilização de câmeras de segurança. As câmeras de segurança são cada vez mais acessíveis com uma qualidade de imagem melhor do que nunca, o que permite que as empresas de segurança monitorem as áreas de maneira mais eficiente. Além disso, a tecnologia de reconhecimento facial está se tornando cada vez mais sofisticada, permitindo que as empresas identifiquem pessoas em tempo real e identifiquem indivíduos suspeitos.

Outra tendência importante na tecnologia de segurança é o uso de drones. Os drones conseguem voar em áreas de difícil acesso, o que os torna ideais para monitorar grandes áreas, como estacionamentos ou terrenos industriais. Além disso, a tecnologia de drone está melhorando a cada ano, o que significa que eles estão se tornando mais precisos e fáceis de controlar.

A inteligência artificial (IA) é outro avanço tecnológico importante que está transformando

a segurança privada. A IA pode ajudar as empresas de segurança a analisar grandes quantidades de dados em tempo real, permitindo que elas identifiquem padrões e anomalias que poderiam passar despercebidos por humanos. Além disso, a IA também pode ser usada para automatizar tarefas de segurança, como monitoramento de câmeras ou patrulhas de segurança.

A tecnologia móvel também está mudando a maneira como as empresas de segurança trabalham. Os smartphones permitem que os guardas de segurança acessem informações em tempo real sobre as áreas que estão protegendo, permitindo que eles respondam rapidamente a ameaças. Além disso, os aplicativos móveis podem ser usados para monitorar as atividades de segurança e gerar relatórios em tempo real.

Finalmente, a tecnologia está permitindo que as empresas de segurança privada ofereçam novos serviços aos seus clientes. Por exemplo, as empresas podem oferecer monitoramento remoto de alarmes, o que significa que elas podem monitorar o sistema de alarme de um cliente a partir de um local remoto. Além disso, as empresas também podem oferecer serviços de monitoramento de saúde e segurança, que utilizam sensores para monitorar o ambiente de trabalho e detectar potenciais riscos à saúde e à segurança.

Essas são apenas algumas das maneiras pelas quais a tecnologia está transformando a segurança privada. Embora essas inovações ofereçam muitas oportunidades para empresas de segurança, elas também apresentam desafios significativos, como a necessidade de proteger dados sensíveis e garantir a privacidade dos indivíduos. No entanto, com a abordagem correta, a tecnologia pode ser uma força poderosa para melhorar a segurança privada e manter as pessoas e as propriedades seguras.

Câmeras de segurança e sistemas de monitoramento: como a tecnologia está mudando a vigilância

A tecnologia tem avançado rapidamente e a vigilância não é exceção. Câmeras de segurança e sistemas de monitoramento estão se tornando cada vez mais sofisticados e eficientes, permitindo que as empresas de segurança e os proprietários de imóveis monitorem suas propriedades de maneira mais eficiente e segura. Neste tópico, exploraremos como a tecnologia está mudando a vigilância, quais são as novas tendências em câmeras de segurança e sistemas de monitoramento, e como as pessoas estão usando essas tecnologias para garantir a segurança de suas propriedades.

Uma das principais tendências em câmeras de segurança é a crescente utilização de câmeras com inteligência artificial (IA) e aprendizado de máquina. Essas câmeras são capazes de identificar objetos e pessoas em tempo real, além de monitorar as atividades em uma determinada área e detectar anomalias ou comportamentos suspeitos. As câmeras com IA também podem ser programadas para reconhecer indivíduos específicos e permitir ou negar o acesso a uma área com base nessa identificação.

Outra tendência importante é a utilização de câmeras térmicas. Essas câmeras são capazes de detectar o calor emitido por objetos e pessoas e, portanto, são particularmente úteis para monitorar áreas escuras ou com baixa visibilidade, como estacionamentos e áreas externas à noite. As câmeras térmicas também são frequentemente usadas em ambientes industriais para monitorar equipamentos e detectar falhas antes que elas ocorram.

Além das câmeras de segurança, os sistemas de monitoramento também estão se tornando cada vez mais sofisticados. Os sistemas de monitoramento com inteligência artificial são capazes de analisar grandes quantidades de dados em tempo real e detectar anomalias ou padrões suspeitos. Esses sistemas podem ser usados para monitorar uma ampla gama de atividades, desde o tráfego em uma rodovia até as transações em um caixa eletrônico.

Os sistemas de monitoramento também estão se tornando mais conectados e integrados com outras tecnologias. Por exemplo, as câmeras de segurança e os sistemas de alarme podem ser integrados para detectar intrusos e alertar automaticamente as autoridades competentes. Além disso, muitos sistemas de monitoramento podem ser acessados remotamente por meio de aplicativos para dispositivos móveis, permitindo que os usuários monitorem suas propriedades em tempo real a partir de qualquer lugar.

No entanto, o uso de câmeras de segurança e sistemas de monitoramento também apresenta desafios importantes. Um desses desafios é garantir a privacidade das pessoas que são monitoradas. Muitas pessoas têm preocupações sobre a coleta e o uso de dados pessoais, especialmente se esses dados forem usados por terceiros para fins comerciais ou de vigilância. Além disso, o uso indevido ou abusivo dessas tecnologias pode levar a violações de privacidade e até mesmo ações judiciais.

Outro desafio importante é garantir a segurança dos dados coletados. As câmeras de segurança e os sistemas de monitoramento coletam uma grande quantidade de dados, muitos dos quais são sensíveis e confidenciais.

Esses dados incluem informações pessoais, como rostos, nomes e endereços, bem como informações financeiras e de segurança. É crucial que esses dados sejam protegidos contra ameaças de segurança, como ataques cibernéticos, invasões de hackers e vazamentos de dados.

Além disso, muitas vezes é difícil determinar quem é responsável pelo uso e armazenamento desses dados. Muitos sistemas de monitoramento são operados por empresas de segurança privada ou agências governamentais, mas essas entidades podem ter diferentes políticas de privacidade e segurança de dados. Isso pode levar a conflitos de interesse e incertezas legais sobre quem é responsável por garantir a segurança e privacidade dos dados coletados.

Outro desafio é a implementação e manutenção desses sistemas. Embora as câmeras de segurança e os sistemas de monitoramento sejam cada vez mais acessíveis e fáceis

de usar, muitas vezes é necessário conhecimento técnico para instalar e configurar esses sistemas corretamente. Além disso, esses sistemas requerem manutenção regular, incluindo atualizações de software, limpeza e substituição de peças, o que pode ser caro e demorado.

Por fim, é importante reconhecer que a tecnologia de câmeras de segurança e sistemas de monitoramento não é uma solução mágica para todos os problemas de segurança. Embora essas tecnologias possam ser úteis para detectar e prevenir crimes, elas também têm limitações. Por exemplo, as câmeras de segurança não podem prever ou prevenir todos os tipos de crimes, e a vigilância constante pode gerar um sentimento de desconfiança e insegurança entre as pessoas.

Em resumo, as câmeras de segurança e os sistemas de monitoramento estão mudando rapidamente a forma como as pessoas monitoram suas propriedades e mantêm a segurança. Embora essas tecnologias ofereçam muitos benefícios, elas também apresentam desafios importantes em relação à privacidade, segurança de dados, implementação e manutenção, e eficácia geral. É importante considerar cuidadosamente esses desafios e oportunidades antes de investir em sistemas de câmeras de segurança e monitoramento, a fim de garantir a segurança e privacidade de todos os envolvidos.

Inteligência artificial e análise de dados: como a tecnologia está melhorando a prevenção e resposta a ameaças

A inteligência artificial (IA) e a análise de dados estão se tornando cada vez mais importantes para melhorar a prevenção e a resposta a ameaças. A IA permite que os sistemas de segurança processem grandes quantidades de dados em tempo real, o que ajuda a identificar ameaças em potencial e a tomar medidas preventivas antes que ocorram incidentes. A análise de dados, por sua vez, ajuda a identificar padrões e tendências que podem ser usados para melhorar a segurança.

Uma das maneiras pelas quais a IA e a análise de dados estão melhorando a prevenção e a resposta a ameaças é através do monitoramento de redes de computadores e sistemas. A IA pode detectar anomalias no tráfego da rede e nos padrões de comportamento dos usuários, o que pode indicar uma possível violação de segurança. A análise de dados também pode ser usada para identificar tendências de ataques cibernéticos, o que pode ajudar as equipes de segurança a se preparar melhor e a implementar medidas preventivas.

Outra área em que a IA e a análise de dados estão sendo usadas é na prevenção de fraudes. As empresas podem usar a IA para identificar padrões suspeitos de comportamento, como tentativas de login de locais geográficos incomuns ou transações incomuns em contas bancárias. A análise de dados pode ajudar a identificar padrões de fraude em transações anteriores, o que pode ser usado para prever e prevenir futuras fraudes.

Além disso, a IA e a análise de dados também estão sendo usadas para melhorar a segurança física. Por exemplo, a análise de vídeo pode ser usada para detectar atividades suspeitas em áreas monitoradas por câmeras de segurança. A IA pode identificar comportamentos incomuns, como a presença de uma pessoa em uma área restrita, e alertar a equipe de segurança para investigar.

A IA também está sendo usada em sistemas de reconhecimento facial, o que permite que as equipes de segurança identifiquem pessoas suspeitas em tempo real. Isso pode ser particularmente útil em grandes eventos ou locais com alto tráfego de pessoas, como aeroportos ou estações de trem.

No entanto, é importante reconhecer que a IA e a análise de dados também apresentam desafios em relação à privacidade e segurança de dados. A coleta e análise de grandes quantidades de dados pessoais pode levar a violações de privacidade, bem como a riscos de segurança de dados. É importante implementar medidas de segurança adequadas para garantir que os dados coletados sejam protegidos contra ameaças.

Em resumo, a inteligência artificial e a análise de dados estão mudando a forma como as equipes de segurança previnem e respondem a ameaças. Essas tecnologias permitem que as equipes de segurança processem grandes quantidades de dados em tempo real e identifiquem padrões e tendências que podem ser usados para melhorar a segurança. No entanto, é importante reconhecer e abordar os desafios em relação à privacidade e segurança de dados ao usar essas tecnologias.

Sensores e dispositivos IoT: como a tecnologia está permitindo a automação e monitoramento de ambientes

Os sensores e dispositivos IoT (Internet das Coisas) estão transformando a segurança privada e permitindo a automação e monitoramento de ambientes de forma mais eficiente. A tecnologia IoT está tornando possível conectar dispositivos, sensores e equipamentos em uma rede, permitindo a comunicação entre eles e fornecendo informações valiosas para os sistemas de segurança.

Os sensores são dispositivos que podem detectar e medir mudanças em um ambiente, como temperatura, umidade, movimento e presença. Eles são amplamente utilizados em sistemas de segurança para monitorar e controlar os ambientes. Por exemplo, sensores de movimento podem ser instalados em portas e janelas para detectar tentativas de intrusão. Sensores de temperatura podem ser usados para monitorar as condições de armazenamento de produtos sensíveis, como alimentos e medicamentos.

Os dispositivos IoT, por outro lado, são equipamentos que podem ser controlados e monitorados remotamente pela internet. Isso significa que as equipes de segurança podem controlar e monitorar sistemas de segurança de qualquer lugar com acesso à internet. Por exemplo, um gerente de segurança pode verificar as imagens de uma câmera de segurança em tempo real em seu celular, mesmo estando em outra cidade.

Além disso, os sensores e dispositivos IoT estão permitindo a automação de ambientes. Por exemplo, um sistema de segurança pode ser programado para desligar as luzes e o ar condicionado em uma sala após o último usuário sair, reduzindo o consumo de energia e aumentando a eficiência do sistema. A automação também permite que as equipes de segurança monitorem sistemas de segurança de forma mais eficiente, eliminando a necessidade de realizar tarefas repetitivas manualmente.

A tecnologia IoT também está permitindo que as empresas monitorem seus ativos em tempo real. Sensores podem ser instalados em equipamentos e máquinas para monitorar seu status, detectar falhas e prever a necessidade de manutenção. Isso ajuda as empresas a tomar decisões informadas sobre quando substituir ou consertar equipamentos, reduzindo o tempo de inatividade e os custos de manutenção.

No entanto, a utilização de sensores e dispositivos IoT também apresenta desafios, como a necessidade de proteger os dados coletados e garantir que os dispositivos sejam seguros. É importante implementar medidas de segurança adequadas, como criptografia de dados, autenticação de usuários e atualizações de firmware regulares.

Em resumo, os sensores e dispositivos IoT estão permitindo a automação e monitoramento de ambientes de forma mais eficiente. Eles permitem a comunicação entre dispositivos, fornecem informações valiosas para os sistemas de segurança e permitem a automação de tarefas repetitivas. No entanto, é importante abordar os desafios em relação à segurança de dados e dispositivos ao usar essas tecnologias.

Reconhecimento facial e outras tecnologias biométricas: como a tecnologia está transformando o controle de acesso e identificação

As tecnologias biométricas, como o reconhecimento facial, estão transformando o controle de acesso e identificação na segurança privada. Essas tecnologias permitem que as empresas verifiquem a identidade de indivíduos com base em características físicas únicas, como rosto, impressão digital, voz e íris. O reconhecimento facial é uma das tecnologias biométricas mais populares e está sendo amplamente utilizada em sistemas de segurança em todo o mundo.

O reconhecimento facial é uma tecnologia que utiliza algoritmos para analisar as características faciais de um indivíduo e compará-las com uma base de dados. Essa tecnologia é capaz de identificar pessoas em tempo real e fornecer alertas instantâneos sobre pessoas suspeitas ou indesejadas. Além disso, o reconhecimento facial pode ser usado para controlar o acesso a áreas restritas, como salas de servidores, laboratórios e áreas de armazenamento.

Outras tecnologias biométricas, como a impressão digital e a íris, também são utilizadas para controle de acesso e identificação. A impressão digital é uma das tecnologias biométricas mais antigas e é amplamente utilizada em sistemas de segurança em todo o mundo. A íris é outra tecnologia biométrica que está se tornando mais popular, devido

à sua alta precisão e rapidez na identificação de indivíduos.

No entanto, o uso de tecnologias biométricas, como o reconhecimento facial, também apresenta desafios em relação à privacidade e segurança de dados. É importante garantir que essas tecnologias sejam usadas de maneira ética e transparente, com o consentimento explícito dos usuários. Também é importante proteger os dados biométricos coletados e garantir que eles sejam armazenados e usados de maneira segura.

Além disso, a tecnologia biométrica pode ser cara de implementar e manter. A compra e instalação de scanners biométricos, equipamentos de armazenamento de dados e sistemas de software podem ser muito caros. Também pode ser necessário treinar pessoal para usar e manter esses sistemas.

Em resumo, o reconhecimento facial e outras tecnologias biométricas estão transformando o controle de acesso e identificação na segurança privada. Essas tecnologias permitem que as empresas verifiquem a identidade de indivíduos com base em características físicas únicas e estão sendo amplamente utilizadas em sistemas de segurança em todo o mundo. No entanto, é importante abordar os desafios em relação à privacidade e segurança de dados e os custos associados à implementação e manutenção desses sistemas.

Cloud Computing e Armazenamento de Dados: Como a Tecnologia está permitindo o Armazenamento Seguro e Acessível de Grandes Quantidades de Informações.

Nos últimos anos, a tecnologia de computação em nuvem tem revolucionado a forma como as empresas e indivíduos armazenam e gerenciam seus dados. O armazenamento em nuvem permite que grandes quantidades de informações sejam armazenadas de forma segura e acessível a partir de qualquer dispositivo com conexão à internet. Isso torna o armazenamento de dados muito mais prático e econômico do que as opções tradicionais de armazenamento, como discos rígidos e servidores locais.

A computação em nuvem também oferece maior segurança aos dados armazenados, já que os provedores de nuvem geralmente têm medidas de segurança mais avançadas do que as empresas individuais. Isso inclui medidas como criptografia, autenticação de dois fatores e backups regulares. Além disso, a computação em nuvem permite que os usuários personalizem as configurações de segurança de acordo com suas necessidades específicas.

Outra vantagem da computação em nuvem é a sua escalabilidade. Os usuários podem facilmente aumentar ou diminuir a quantidade de armazenamento necessária, sem precisar investir em hardware adicional ou atualizar seus sistemas. Isso é especialmente útil para empresas em crescimento ou projetos que requerem um grande volume de armazenamento temporário.

A computação em nuvem também oferece uma maior acessibilidade aos dados. Os usuários podem acessar seus dados de qualquer lugar do mundo com conexão à internet, o que é especialmente útil para equipes distribuídas ou usuários móveis. Além disso, muitos provedores de nuvem oferecem aplicativos móveis e ferramentas de colaboração, tornando mais fácil para as equipes trabalharem juntas em um projeto.

Apesar de todos esses benefícios, a computação em nuvem ainda tem algumas limitações e preocupações de segurança. A privacidade dos dados é uma preocupação frequente, especialmente quando se trata de dados confidenciais ou de propriedade exclusiva. Também existe a preocupação com a disponibilidade dos dados em caso de falhas no serviço ou interrupções de rede.

Por fim, é importante lembrar que a computação em nuvem é uma tecnologia em constante evolução e que os provedores de nuvem estão constantemente melhorando suas medidas de segurança e funcionalidades. Como resultado, a computação em nuvem é uma opção de armazenamento cada vez mais popular e viável para empresas e indivíduos que precisam gerenciar grandes quantidades de dados de forma segura e acessível.

CONCLUSÃO

Em conclusão, a tecnologia está trazendo mudanças significativas para a segurança privada e oferecendo novas oportunidades para melhorar a segurança de empresas e indivíduos. As câmeras de segurança e sistemas de monitoramento, inteligência artificial e análise de dados, sensores e dispositivos IoT, bem como o reconhecimento facial e outras tecnologias biométricas estão transformando a forma como a segurança é gerenciada e como as ameaças são detectadas e respondidas.

No entanto, é importante que as empresas e profissionais de segurança privada estejam cientes dos desafios que acompanham essa transformação. A proteção da privacidade e dos dados pessoais é uma preocupação importante, especialmente no que diz respeito à coleta, armazenamento e uso de informações por meio de tecnologias de vigilância e análise de dados.

É fundamental que as empresas estejam em conformidade com as regulamentações e leis relevantes, além de garantir que os sistemas de segurança implementados sejam éticos e transparentes. Além disso, é importante que as empresas se concentrem em treinar seus funcionários em relação ao uso dessas novas tecnologias, garantindo que a privacidade e segurança de dados sejam consideradas em todas as fases do processo.

A tecnologia também apresenta oportunidades para as empresas melhorarem seus processos de segurança e aumentarem a eficácia de seus sistemas. Ao usar as tecnologias disponíveis, as empresas podem implementar sistemas mais rápidos, precisos e automatizados, permitindo uma resposta mais rápida e eficiente a possíveis ameaças.

Em última análise, é importante que as empresas e profissionais de segurança privada estejam abertos à adoção de novas tecnologias e sejam proativos na busca de soluções que melhor atendam às suas necessidades específicas. Com a combinação certa de tecnologia e abordagens de segurança tradicionais, as empresas podem aumentar sua segurança e proteção, oferecendo maior tranquilidade e segurança a seus funcionários e clientes.

CONSIDERAÇÕES SOBRE AS FONTES DE RISCOS CIBERNÉTICOS

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

Em textos anteriores, verificamos a necessidade e a conveniência do trabalho metódico na tarefa nem sempre simples de determinar o conjunto de riscos de toda ordem que povoam a vida administrativa das organizações, sejam elas governamentais, sejam pertencentes a qualquer um dos diferentes ramos da iniciativa privada.

Vimos que sistemas de gerenciamento de riscos visam, idealmente, à prevenção, isto é, a evitar que o risco se materialize. Caso essa ação não obtenha o efeito desejado e o risco venha a se concretizar, deve-se de imediato partir para a sua mitigação, de modo a reduzir o impacto dele na empresa. Essencial para que esta segunda linha de conduta possa ter lugar é a existência de toda uma sistemática de gerenciamento de riscos planejada, implantada, praticada.

Vimos que o risco nada mais é que a consequência indesejável da presença de seus dois componentes: as fontes de risco (também conhecidas como fatores de risco ou causas de risco) e a exposição do alvo a essas fontes. Quando se fala de prevenção do risco, existem basicamente duas linhas de conduta: pode-se, de um lado, eliminar ou reduzir a expressão das fontes de risco; do outro lado, pode-se eliminar ou reduzir a exposição do alvo aos efeitos delas.

Para clarificar a questão das fontes de risco, vamos fazer uso do risco cibernético mais falado em nossos dias, qual seja o ataque cibernético. O phishing, comumente citado como um risco cibernético, nada mais é que uma fonte desse risco – uma devastadora fonte de riscos cibernéticos que tantos danos vem causando às corporações em todo

o mundo. A mensagem de phishing pode ser recebida pelo funcionário da empresa e permanecer na caixa de entrada por tempo indefinido, sem causar qualquer dano. O ataque cibernético só se processa quando ocorre a exposição: o operador pouco cuidadoso, curioso ou dotado de boa-fé que decide clicar no link para abri-lo e libera o trojan (cavalo de troia) que desencadeia, a partir dali a infecção do computador e da rede a que ele está conectado. Na sequência, pode-se esperar a criptografia e o sequestro de dados e, um pouco mais adiante, a exigência do pagamento de um resgate, no desenrolar do ataque cibernético conhecido como ransomware. Ficou aí evidenciada uma segunda e determinante fonte de risco cibernético, qual seja, o despreparo dos colaboradores das empresas para o trabalho em rede.

O tratamento das fontes de riscos cibernéticos (com a implantação dos chamados controles), nesse caso, impõe ação muito proativa, no âmbito da TI, para impedir a entrada nos sistemas corporativos de mensagens cuja origem não seja perfeitamente reconhecida e cujo conteúdo não tenha sido avaliado e reconhecido como inofensivo à integridade dos sistemas. Outra medida impositiva, tratando agora da segunda fonte de risco mencionada, é a capacitação dos colaboradores em todos os níveis, do chão de fábrica à alta administração, para que não abram, de forma alguma, mensagens suspeitas ou de que não conheçam a procedência.

É necessário que se determinem, de forma sistemática, as fontes de risco, sem esquecer que algumas delas são comuns a diversos riscos. A uma primeira análise, salta aos olhos que quanto maior o número de riscos originados da mesma fonte de risco, mais relevante ela será.

A seguir, iremos citar algumas das fontes de riscos cibernéticos mais comuns e tecer ligeiros comentários sobre elas, com a ressalva de que esta lista não é, de forma alguma, exaustiva.

- A ampla disseminação do uso da internet em todas as áreas da atividade humana, abrindo oportunidades de atuação aos criminosos do espaço cibernético.
- A falta de atualização dos equipamentos de informática e dos sistemas de TI e TO, muitas vezes por desleixo ou falta de atenção de usuários e administradores.
- A utilização de senhas fracas, mantendo-as por longos períodos, para acessar os diversos sistemas e aplicativos utilizados pelo usuário.
- A utilização das mesmas senhas e credenciais em diferentes sistemas e aplicativos.
- A inexistência ou fragilidade dos sistemas de gestão de riscos cibernéticos utilizados pelas corporações.

A pouca atenção dedicada aos riscos cibernéticos pelos integrantes da alta administração das empresas, muitas vezes movidos pela falta de conhecimento técnico, o que os compele a “deixar esse assunto por conta de quem entende”. Acontece que o pessoal técnico muitas vezes não tem conhecimento de quais são os sistemas críticos para o negócio e, na tentativa de defender toda a frente, acaba enfraquecendo todo o perímetro. É necessário que as chefias nos níveis operacional e estratégico trabalhem em estreita ligação com os especialistas de TI, para que os processos e os sistemas de criticidade mais elevada recebam a devida prioridade na aplicação de recursos.

As deficiências na capacitação do pessoal em todas as áreas sobre a maneira adequada de operar os equipamentos conectados à rede constituem uma das fontes de riscos mais exploradas. Essas lacunas de capacitação proporcionam ao intruso a oportunidade de ter acesso aos sistemas e apoderar-se do controle de todas as operações daquela organização. É desnecessário dizer que a fonte de risco aqui mencionada tem sua relevância potencializada pelas conexões cada vez mais estreitas entre os sistemas de TI e os de TO, o que pode franquear ao hacker acesso pleno às linhas de produção e aos demais sistemas finalísticos das corporações.

Pudemos assim verificar algumas noções importantes sobre fontes de riscos e estabelecer a diferença desse conceito para o conceito de risco. Da correta e exaustiva análise das fontes de riscos, dos riscos que a partir delas podem se concretizar, dos controles a serem estabelecidos para eliminar ou minimizar umas e outros resultará, certamente, a confecção de planos de ação eficientes, eficazes e que atendam ao interesse das organizações.

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 e disciplinas – entre eles, a disciplina Gestão de Riscos Cibernéticos – compostos de diferentes disciplinas. Isso garante a abrangência e a integração de todos os processos em um único framework.

Solicite uma demonstração!

SEGURANÇA E RESILIÊNCIA – SISTEMAS DE GESTÃO DE CONTINUIDADE DE NEGÓCIOS (ABNT NBR ISO 22301:2020)

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

A Norma ABNT NBR ISO 22301:2020 define os aspectos necessários para que um sistema de gestão previna e proteja empresas diante de contingências como desastres naturais e situações que possam causar a interrupção de seus processos e negócios.

Esta norma traz as especificações, a estrutura e os requisitos para que seja implementado e mantido um sistema de gestão de continuidade de negócios (SGCN) que tem por objetivo manter uma operação após um evento disruptivo, independentemente de este ser decorrente de falha de segurança digital, de desastre ou de qualquer outro motivo.

Entre os vários benefícios dessa certificação, está o diferencial competitivo. Comparando com concorrentes sem essa chancela, uma empresa credenciada pela ISO 22301 terá melhor visibilidade no mercado – principalmente quando se trata de clientes sensíveis à manutenção da continuidade de suas operações e à entrega de seus produtos e serviços.

Além disso, essa ISO pode melhorar a reputação e ajudar a conquistar novos clientes, tornando mais fácil demonstrar que determinado negócio está entre os melhores do setor. Afinal, o negócio dispõe de uma documentação que comprova isso.

Os resultados de um SGCN devem ser modulados por requisitos legais, regulatórios, organizacionais e operacionais da organização e de suas partes interessadas e, para ser eficaz deve-se entender quais são as necessidades da organização e a imprescindibilidade do estabelecimento de uma política e de objetivos para a continuidade de negócios.

É preciso que os processos sejam operados e mantidos, incorporando capacidades e estruturas de pronta resposta para que a organização sobreviva a eventos disruptivos.

O SGCN deve ser monitorado e seu desempenho avaliado de forma crítica para que seja eficaz. Além disso deve ser melhorado continuamente com base em medições qualitativas e quantitativas.

A implementação de um SGCN não é uma tarefa fácil. São várias etapas que devem ser cumpridas, de forma obrigatória, conforme determinado pela Norma ABNT NBR ISO 22301:2020. Dentre elas, temos:

1) Apoio dos gestores - para iniciar qualquer tipo de projeto dessa magnitude, os gestores da empresa precisam estar dispostos a investir em recursos humanos, financeiros e tecnológicos.

2) Identificação dos requisitos – inicialmente, é preciso ter certeza de que essa ação está em conformidade com tudo o que as partes interessadas desejam. Não são apenas as leis e regulamentos, mas também os requisitos nos acordos já firmados com os clientes e os desejos dos proprietários da empresa, dentre outros.

3) Política e objetivos de continuidade de negócios - é preciso implantar uma política de continuidade de negócios e os diretores precisam determinar exatamente o que se espera dessa continuidade, definindo metas objetivas.

4) Avaliação e tratamento de risco - é preciso descobrir quais problemas podem ocorrer com mais frequência e definir os controles que podem ser aplicados para mitigá-los.

5) Análise de impacto nos negócios - o objetivo da análise de impacto nos negócios é definir o tempo disponível para a recuperação e os recursos necessários para isso.

6) Estratégia de continuidade de negócios – definir meios para conseguir o que foi listado nas etapas anteriores com um nível mínimo de investimento, evitando gastos desnecessários que podem fazer a diferença nos estágios seguintes.

7) Plano de continuidade de negócios - planos de resposta inicial a incidentes e planos de recuperação que detalhem o que precisa ser feito para iniciar as atividades.

8) Treinamento e conscientização - é preciso capacitar os colaboradores sobre como executar determinadas etapas do plano, enfatizando a razão pela qual tudo isso é tão importante.

9) Manutenção da documentação – toda estratégia precisa estar refletida em

documentos.

10) Exercício e teste – é preciso criar situações nas quais se possa testar os planos no modo mais realista possível. Quem não puser os planos à prova para descobrir como eles se comportam em situações reais nunca descobrirá os pontos que precisam ser aperfeiçoados.

11) Comunicação com as partes interessadas - a continuidade dos negócios pode depender também de órgãos reguladores, autoridades, proprietários, empregados e fornecedores.

12) Medição e avaliação – é preciso saber se as metas estão sendo atingidas. Os objetivos definidos na etapa 3 têm que ser verificados para entendermos se estão sendo atingidos de acordo com algum tipo de métrica.

15) Auditoria interna - outras pessoas da empresa devem revisar o projeto e sugerir melhorias – é essa a função da auditoria interna. Embora muitas vezes seja considerada uma sobrecarga, uma auditoria interna é realmente muito útil quando se trata de enfrentar a realidade e integrar equipes.

16) Ações corretivas – a Norma ABNT NBR ISO 22301 traz melhorias diárias que acabam sendo conduzidas sistematicamente. É o que conduz uma empresa a descobrir por que determinado problema aconteceu, garantindo que nunca aconteça novamente. O próprio texto da ISO fala sobre “garantir que as não conformidades não se repitam”. É algo que precisa ser feito de forma sistemática e transparente.

17) Revisão - concluídas todas as etapas, a alta administração precisa avaliá-las e tomar algumas decisões cruciais – como atualizar os objetivos, liberar verbas, fazer melhorias adicionais, entre outros. Afinal, é deles a responsabilidade final sobre a capacidade que a empresa tem de sobreviver a incidentes maiores.

SEGURANÇA CIBERNÉTICA ZERO TRUST E O DESAFIO DA IMPLEMENTAÇÃO NA ORGANIZAÇÃO

Mariana da Silveira, DIDS, MBCR, CPSI, CEGRC, CIGR, CISI, CIEIE, DPO, ISO | Divisão Cibernética da Brasiliano INTERISK

A Segurança Cibernética Zero Trust é uma filosofia baseada na premissa de que nenhuma parte do ambiente de rede deve merecer confiança total até que seja devidamente verificada. Significa que a autenticação e os controles de acesso são fundamentais para proteger sistemas e informações críticas. Esta abordagem deve ser aplicada desde a infraestrutura até as aplicações e usuários, para garantir que apenas aqueles autorizados possam acessar os recursos.

Além disso, a Zero Trust visa fornecer proteção de ponta a ponta de todas as conexões de rede e atividades, proporcionando acompanhamento contínuo para detectar atividade suspeita e bloquear qualquer acesso não autorizado. A proteção proativa permite a análise de comportamento contínua, o monitoramento e a avaliação das atividades dos atores de rede e o envio de alertas de segurança ao detectar qualquer situação suspeita.

O monitoramento de equipamentos de rede de forma proativa é uma prática de segurança que envolve a monitorização contínua para detectar padrões de comportamento anômalos ou outras formas de atividade maliciosa. Esta prática ajuda a identificar possíveis ameaças, que possam explorar as vulnerabilidades do ambiente, antes que causem danos, contribuindo assim, para a manutenção da segurança cibernética.

Medidas de segurança proativas exigem a realização de monitoramento on-line, em tempo real, para a identificação e a detecção de ameaças e intrusões, por intermédio de soluções de antivírus, antimalwares, backups periódicos, auditorias regulares, incorporação de melhoria contínua e de lições aprendidas. Tais medidas devem ser

suficientes para contribuir com a proteção do ambiente cibernético.

Tecnologias robustas de autenticação e controle de acesso são ferramentas que podem ser usadas para autenticar e controlar os usuários e dispositivos na rede. Estas ferramentas incluem, mas não se limitam, a firewall, antivírus, autenticação multifator, lógica de negócios, configurações de política de acesso, controle de acesso de escopo de rede, criptografia, licenças, atualização de patches.

As ameaças cibernéticas são qualquer tipo de ameaça que se manifeste no âmbito da segurança cibernética. Tais ameaças podem incluir vírus, phishing, backdoor, malware, interceptação de dados e ataques de negação de serviços. Seus resultados podem causar danos à confidencialidade, integralidade e disponibilidade das informações. A adoção de medidas técnicas adequadas e proativas contribui para a prevenção de tais ameaças.

Os incidentes cibernéticos podem ser causados por uma variedade de fatores, incluindo descobertas de vulnerabilidades de software exploradas por crackers, falhas na segurança computacional, controles de acesso inapropriados ou inexistentes e configuração de senhas fracas. Além disso, uso inadequado da tecnologia, comportamento e negligência dos usuários podem contribuir para a ocorrência de tais incidentes.

Para a abordagem de Confiança Zero, todo usuário, dispositivo ou serviço de rede são considerados não confiáveis, por padrão. O conceito aplica-se a todos os elementos relevantes em uma infraestrutura de rede, exigindo, portanto, soluções de autenticação fortes, autorizações granulares e segurança multicamada para a proteção das ameaças cibernéticas. Assim, ainda que a ameaça se concretize, seu impacto deverá ser isolado, controlado e mitigado.

Dos padrões e normas mais utilizados para o fornecimento das diretrizes de implementações práticas de segurança que podem auxiliar no estabelecimento de um ambiente Zero Trust, citamos a ISO 27001, a ISO 27032 e o NIST. Eles fornecem uma abordagem segura para a implementação de técnicas e gestão da segurança cibernética, com requisitos específicos para os processos que suportam a segurança no ambiente cibernético.

Independentemente da estrutura utilizada, ponto importante é verificar se os arcabouços técnico, organizacional e físico, de segurança cibernética, estão voltados para identificar, proteger, detectar, responder e recuperar, no contexto da exploração de vulnerabilidades, por parte das ameaças presentes no espaço cibernético. Nesse sentido, essas funções precisam abranger, necessariamente, os quesitos a seguir.

Estrutura da gestão e de serviços de segurança da informação e seus controles, controle de acesso e responsabilidades, controle de rede, gestão de aplicações e softwares, segurança no uso dos sistemas, gestão de dispositivos móveis, segurança em estações de trabalho e servidores, gestão de identidade e acesso, gestão de contingência, segmentação de rede, monitoramento e análise de risco da segurança da informação.

Para alcançar o Zero Trust, são necessárias as ações de segurança discutidas ao longo do texto, cujos resultados perpassam pela tentativa de evitar a visibilidade de sistemas e de aplicativos na internet, e assim minimizar ações de ataque; melhorar a experiência de navegação do usuário na rede, concedendo acesso seguro, rápido, ininterrupto e remoto a SaaS; segmentação da rede corporativa, oferecendo segurança cibernética, dentre inúmeras outras vantagens.

O desafio da implementação da Confiança Zero, nos procedimentos de segurança da informação, pertinentes ao ambiente cibernético, consiste em realizar investimentos de recursos em medidas técnicas, físicas e organizacionais. Dentre elas, a cultura organizacional em segurança cibernética, o investimento financeiro em tecnologias, a capacitação de usuários e, principalmente, a liderança e o comprometimento da Alta Direção.

O caminho a ser percorrido não é fácil, tampouco é rápido, contudo, a organização precisa tomar imediatamente a iniciativa de sua caminhada rumo à Confiança Zero. Começar pelo começo pode ser considerado pleonasmo, mas, neste aspecto, é a melhor forma de agir. A organização deve tomar ações logicamente estruturadas, ao esbarrar nos percalços, a serem superados, precisa vencer a dificuldade e seguir com consistência para os próximos obstáculos.

Dessarte, a organização guiada por um framework direcionado, que ofereça a estrutura concatenada para o estabelecimento do sistema de gestão de segurança cibernética, poderá conquistar um ambiente Zero Trust, por intermédio de medidas técnicas, organizacionais e físicas, conquistando assim a maturidade em segurança cibernética, com solidez e perspicácia, num processo de melhoria contínua e de lições aprendidas incorporadas.

ESG E TRABALHO ANÁLOGO À ESCRAVIDÃO

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

No início deste ano, uma notícia triste e preocupante veio somar-se aos acontecimentos que movimentavam o nosso universo político.

A informação da descoberta de numerosos trabalhadores submetidos a condições de trabalho análogas à escravidão em conceituadas vinícolas do Rio Grande do Sul causou espanto e indignação à parcela esclarecida da população que tem consciência dos direitos humanos e da necessidade do respeito ao próximo em qualquer situação.

Logo a incredulidade cedeu lugar à curiosidade por conhecer as motivações e as circunstâncias de tal procedimento. Não demorou muito para que a situação fosse esclarecida pela força-tarefa montada com esse objetivo, envolvendo integrantes da Polícia Rodoviária Federal (PRF), da Polícia Federal (PF) e do Ministério do Trabalho e Emprego (MTE).

Versões e realidade

O comunicado emitido pelas empresas denunciadas, embora reconhecesse a ocorrência do evento, procurava desviar a responsabilidade, descarregando-a sobre a terceirizada que contratava os trabalhadores, colocava-os a trabalhar e os mantinha submetidos àquelas deploráveis condições.

É de todo interessante verificar o quanto essa realidade era diferente do apregoado nos meios de comunicação e nas declarações postadas nas mídias das empresas.

Por exemplo, reportagem publicada no jornal O Estado de São Paulo de 06/10/2022, assinada pelo jornalista Luis Filipe dos Santos, traz como título: “Vinícola Salton aposta em juventude e ESG por competitividade”.

Diferentemente do que se é levado a crer pelo conteúdo da manchete acima transcrita, uma simples passada de olhos pela matriz de materialidade da empresa (https://www.salton.com.br/jornada-consciente) nos informa que os aspectos sociais e ambientais não ocupavam alta prioridade para as suas Lideranças.

Ao contrário, a matriz de materialidade mostra os aspectos ambiental e social ocupando níveis de prioridade médio e baixo para as Lideranças, embora os demais stakeholders ofereçam uma visão mais consentânea com os tempos atuais e atribuam a esses aspectos um nível de materialidade alto. Para as Lideranças da empresa em questão, apenas o Produto e a Segurança Cibernética ocupavam uma posição de alta relevância entre os temas submetidos à análise de materialidade ESG.

Como costuma acontecer, as decisões são, no final das contas, tomadas pela Alta Administração da organização. Assim é que, pelo visto, as opiniões dos demais stakeholders não foram muito valorizadas, pelo menos no que toca aos aspectos a que estamos nos referindo.

Com o aspecto social negligenciado na cadeia de valor e sem ter sido contido ou mitigado por qualquer controle, o risco de trabalho escravo veio a se materializar. As consequências não se fizeram esperar e trouxeram consigo uma fatura pesada em termos legais, financeiros e de imagem para as empresas.

Em resumo...

De toda essa triste história, é possível concluir sobre a necessidade de as empresas encararem de forma positiva a gestão da Agenda ESG. É fundamental estabelecer, de forma precisa e coerente, os temas ESG relevantes para a empresa e levantar os riscos que o fato de não os levar em consideração acarretará. A partir daí, caberá à Alta Administração decidir se esses riscos cabem no apetite ao risco da empresa ou se será necessário tratá-los.

É público e notório que os investimentos em ESG têm alta probabilidade de trazer retornos financeiros positivos, embora nem sempre no ritmo desejado. Todavia, mais importante que o retorno financeiro é exatamente a circunstância de esses investimentos, quando conduzidos de forma planejada e estruturada, reduzirem drasticamente as probabilidades de materialização de riscos de impacto muito alto que podem acarretar até mesmo a inviabilização do negócio.

Conclusão

Tivemos assim, em poucas palavras, uma visão da importância, para qualquer organização, do atendimento dos princípios que regem a Agenda ESG, a partir de um caso ocorrido há pouco em nosso país.

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 Gestão de Riscos ESG – compostos de diferentes disciplinas. Isso garante a abrangência e a integração de todos os processos em um único framework.

DA CONSCIENTIZAÇÃO AO ENVOLVIMENTO NA SEGURANÇA CIBERNÉTICA

Manuel Sánchez Gómez-Merelo | 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. Miembro experto de la Comisión Mixta Central de Seguridad Privada del Ministerio del Interior. España. http://www.manuelsanchez.com

Nos últimos anos, a cibersegurança tem vindo a assumir o protagonismo que merece, mas os níveis de sensibilização e envolvimento ainda estão longe de serem adequados.

As pessoas são o elo mais fraco da cadeia de segurança da informação, e as comunicações representam a porta de entrada para mais de 90% dos ataques cibernéticos que sofremos por meio dos meios digitais.

94% das empresas na Espanha sofreram um incidente de segurança cibernética no ano passado. Um fato alarmante, segundo estudo recente divulgado pela rede internacional de atendimento Deloitte.

De fato, a Espanha se posicionou em 2022 como o terceiro país do mundo em termos de ataques cibernéticos, depois de ter sofrido mais de 300.000 crimes de informática em 2021, o que é considerado a maior onda de cibercrimes no país até o momento.

Os ataques cibernéticos supõem uma vulnerabilidade muito grande nas organizações e, as perdas econômicas e de informação, além de serem muito importantes, representam danos à imagem e reputação pessoal e institucional.

Os cibercriminosos se aproveitam da ignorância, exposição e vulnerabilidades dos usuários para acessar as informações em nossos dispositivos, a fim de utilizá-las contra pessoas e organizações.

Quando uma organização sofre um incidente, as consequências são imediatamente

conhecidas e o próprio impacto do ataque coloca em risco a confiança, a reputação, a credibilidade e o desenvolvimento da atividade da organização atacada. Consequentemente, os órgãos de governo das organizações devem fortalecer sua capacidade de resiliência no mesmo ritmo que fazem com a segurança cibernética, o que representa um desafio significativo.

Objetivos de conscientização

Os pilares fundamentais da segurança cibernética são pessoas, processos e sistemas e tecnologias.

Nesse sentido, o objetivo da conscientização das pessoas não é transformar os funcionários em especialistas em segurança da informação, mas sim transferir as melhores práticas em termos de prevenção e proteção para que adotem diretrizes de comportamento seguro nos diversos ambientes em que aqueles que exercem fora a sua atividade.

Desta forma, não só se melhora a cultura de segurança da organização, como também se otimizam os processos com garantias de proteção. Assim, identificará facilmente os riscos e ameaças a que está exposto, bem como as suas potenciais consequências.

Da mesma forma, é um objetivo importante saber como agem os cibercriminosos, suas motivações e modus operandi para saber como aplicar as medidas de segurança adequadas e, assim, prevenir a maioria dos ataques cibernéticos.

A comunicação de todos os aspetos relacionados com a cibersegurança de uma organização é também um objetivo importante.

Por fim, os processos de controle, supervisão e inteligência devem estar sempre atualizados, permitindo medir os resultados e desvios de forma a manter uma análise confiável e constante das informações provenientes da operação e estado de segurança de todos os processos derivados da atividade da organização.

Conscientização e participação

De forma a sensibilizar e envolver eficazmente todos os colaboradores, a política de segurança deve ser previamente definida na própria estrutura da organização.

Para isso, a primeira fase para evitar a materialização do risco ou qualquer ameaça cibernética é identificá-los ou conhecê-los para estabelecer medidas de prevenção.

Uma vez identificados os riscos e ameaças, estabeleceremos as medidas de conscientização e prevenção que devemos aplicar para minimizar ou, no melhor dos casos, eliminar as vulnerabilidades, riscos e ameaças aos quais estamos expostos.

Nesse sentido, o envolvimento da alta direção tem papel fundamental no fortalecimento

do estabelecimento de medidas de segurança.

A sensibilização é, em todo o caso, uma prioridade maior do que nunca e exige o lançamento de iniciativas de sensibilização e formação para todos os colaboradores.

Segurança e cibersegurança

Por muito tempo, a segurança foi estabelecida com uma visão abrangente e integrada de segurança física e lógica, para a proteção dos ativos e informações das organizações.

Esta integração deve assentar numa perfeita sinergia também entre operações e segurança, garantindo assim que esta última, para além de garantir e proteger os interesses e ativos da organização, proporcione valor acrescentado, diferencial e competitivo. Esta circunstância só é possível quando os departamentos e gestores de segurança têm um conhecimento aprofundado da atividade e dos seus riscos.

Para tal, na definição de um plano de segurança, devem ser previamente identificados e quantificados os riscos, ameaças e vulnerabilidades implícitas na atividade e as pessoas e bens ou ativos a proteger.

Em seguida, devemos definir as políticas de segurança necessárias para proteger e prevenir as possíveis consequências dos riscos identificados, e que estas estejam alinhadas com a atividade.

Por todas estas razões, as medidas e meios de cibersegurança deixam de ser uma opção, devem ser integrados no Plano de Segurança para garantir a salvaguarda da informação e proteger ativos intangíveis, como a reputação da organização.

Neste sentido, o Conselho de Administração deve envolver-se e transmitir o seu compromisso à Direção de Segurança e restantes colaboradores, de forma a minimizar o impacto na sua organização e modelo de funcionamento.

Comunicação e Informação

Através desta formação, serão detectadas as vantagens e desvantagens do meio digital e como está a evoluir a prevenção e proteção na organização.

É essencial acompanhar todas estas políticas de segurança com medidas e protocolos complementares, tanto para controlo, verificação e monitorização, como para identificação de novos riscos e ameaças.

A título de conclusões

A tarefa de sensibilização exige o esforço e o envolvimento de todos na cibersegurança, pois tanto os cidadãos como as administrações, agências e organizações empresariais são responsáveis pelo comportamento nas comunicações, portanto, todas as ações têm

consequências diretas sobre os demais atores que participam e só através do trabalho comum e da responsabilidade partilhada se pode garantir uma maior proteção dos meios de gestão e comunicação.

A utilização de novas tecnologias e equipamentos na realização de nossas atividades digitais, aliada à facilidade de acesso à Internet, tornou nossos trabalhos versáteis, podendo trabalhar de qualquer lugar e nos comunicar a qualquer hora.

Isso torna a conscientização e o envolvimento com a segurança da informação tratada pelos funcionários uma questão pendente no campo da cibersegurança, e é o elemento que causa inúmeras brechas de insegurança capazes de afetar organizações de qualquer porte.

Em resumo, vamos rediscutir sobre os pontos básicos que qualquer responsável pela segurança da informação deve ter em conta para minimizar o risco de insegurança causado pelo fator humano e são os seguintes:

- Devemos estabelecer políticas de conscientização para facilitar o envolvimento das pessoas na segurança cibernética.
- Avaliações periódicas e ações de conscientização devem ser realizadas entre os colaboradores para conhecer o nível e a cultura de proteção das informações que possuem.
- Periodicamente, simulações de ataques a informações e dados devem ser realizadas e os resultados analisados.
- É fundamental que todos os colaboradores conheçam a política de segurança da organização, e saibam muito bem o que se espera deles em termos de proteção de informações e dados online.
- Cada colaborador deve dispor dos meios e protocolos necessários para realizar o seu trabalho e manter a sua sensibilização e envolvimento.
- Os funcionários devem ser estabelecidos e incentivados a usar senhas fortes e alterá-las com frequência, fornecendo ferramentas e controles adequados que facilitem o cumprimento dos protocolos para alterá-las.
- Temos que garantir que os funcionários entendam as consequências de violações de segurança ou ataques de cibercriminosos, a fim de aumentar seu nível de alerta e preparação adequada para identificar qualquer ataque de engenharia social.

Em suma, vamos tornar a sensibilização e o envolvimento na cibersegurança uma parte importante da cultura organizacional, criando desafios que tornem visíveis os colaboradores que têm as melhores práticas.

ESTUDO DA SEGURANÇA COMO DEVE SER CONDUZIDO

Dr. Fabiano Sérgio Paiva Dias de Sá, CPSI | Doctor
en Ciencias de la Seguridad (Espanha).

No mundo em que vivemos, a enorme competitividade entre as empresas, independentemente de seu ramo de atuação ou tamanho, além das incertezas e riscos naturais inerentes ao seu negócio e ainda o crescimento da violência, ascensão do crime organizado, desequilíbrio social e atuação abaixo do desejável dos órgãos de segurança pública, as obriga a se organizarem e planejarem da forma mais eficiente possível todas as despesas e custos. Nesse contexto não se pode mitigar a segurança empresarial**.** Não se deve ver a segurança apenas como a protetora de pessoas e ativos, pelo menor custo possível e sim como ferramenta fundamental para agregar competitividade e estabilidade aos processos empresariais.

Baseado no contexto acima, a realização de um estudo voltado para a segurança em uma instituição pública ou privada, será de suma importância.

Apresentaremos neste artigo, algumas orientações que poderão nortear o profissional de segurança durante o processo de construção de um Estudo de Segurança, objetivando conhecer uma série de questionamentos fundamentais para alcançar um resultado de sucesso.

A segurança nasce quando um indivíduo apresenta um sentimento do **"medo de perder"**, podendo ser um produto ou até mesmo a própria vida, em cima de uma ameaça em potencial.

Em seu conceito mais tradicional, segurança é a **"ausência de um risco"**, enquanto que em um conceito mais atualizado, poderíamos definir como **"o conjunto de riscos controlados adequadamente"**.

O presente artigo apresentará aos profissionais de segurança questionamentos voltados

para a elaboração de um Estudo de Segurança mais apurado, neste caso, alguns tópicos devem ser analisados para efetividade do referido estudo, vamos a eles:

O que venha ser um Estudo de Segurança?

É o resultado do exame de fatores que afetam ou favorecem a segurança, através de um documento que deverá servir de guia para o desenvolvimento de programas de segurança e os planos subsequentes da mesma instalação.

Compreende um estudo, onde iremos reconhecer os riscos e vulnerabilidades da empresa ou instituição, onde o objetivo é recomendar medidas de segurança necessárias para proteção de ativos e de pessoas.

Quando é necessário um Estudo de Segurança?

- Antes da construção de uma nova instalação.

- No processo de remodelação ou mudanças na infraestrutura das instalações.

- Quando a organização está operando e não foi realizado anteriormente nenhum estudo previamente de segurança.

- Quando da mudança ou expansão do negócio.

- Quando as condições de segurança apresentam deficiências ou surgem suspeitas de falhas em seu sistema.

- Quando não tenha havido nenhuma auditoria de segurança e/ou estudo está desatualizado.

Quem necessita o Estudo de Segurança?

- Empresas privadas

- Empresas públicas

- Instituições de diferentes fins (Financeira, médicas, educação, ONG, outras)

Sequência para realização de um Estudo de Segurança?

- Negociação e definição do âmbito do Estudo.

- Coleta de dados e trabalho de campo.

- Processamento de dados.

- Formulação do Estudo.

- Apresentação preliminar e revisão com contrapartidas.

- Apresentação final e entrega do Estudo.

Quem realiza um Estudo de Segurança?

O Estudo deverá ser realizado por um Profissional em Segurança que de acordo com a complexidade da instalação pode constituir uma equipe multidisciplinar com especialistas, para atender as seguintes áreas:

- Proteção física de instalações.

- Segurança Pessoal.

- Sistemas de segurança eletrônica.

- Sistema de detecção e combate a incêndios.

- Engenharia Industrial.

- Segurança da Informação.

- Outras modalidades de acordo com o âmbito do estudo.

Quais as responsabilidades para um Estudo de Segurança? Pela Organização (Contratante pelo Estudo)	Quem realiza o Estudo (Profissional de Segurança)
- Compromisso da alta administração	- Profissionalismo
- Designar colaboradores para atuar como contraparte	- Ética
- Facilitar o acesso e coordenação interna necessária	- Confidencialidade
- Fornecer as informações necessárias de maneira ampla e abrangente.	- Cumprimento dos prazos e escopo

Quais os documentos básicos de uma Organização em matéria de segurança?

- Legislações e regulamentos relacionados com a segurança privada.

- Estudo de Segurança.

- Plano Integral de segurança.

- Planos para situações de emergências.

- Plano de Gestão de Crises.

- Plano de Continuidade de Negócios.

EVITE FALHAS NA SEGURANÇA PATRIMONIAL - A IMPORTÂNCIA DO ENGAJAMENTO

Olavo Tokutake, CIGR, CPSI, CIEIE, MBS | Consultor em Gestão de Riscos e Especialista em Endomarketing da Brasiliano INTERISK

Quem é o responsável pela Segurança Patrimonial de uma empresa?

A resposta a essa pergunta, para muitas pessoas, é rápida e direta: “a área de Segurança Patrimonial!”. Porém, tão rápida quanto essa resposta equivocada, pode ser a materialização de riscos contra a empresa e suas pessoas, em consequência das brechas causadas por essa visão.

A Segurança Patrimonial é responsabilidade de todas as pessoas da empresa, sem exceção. Desde a presidência até os colaboradores da limpeza, todos têm obrigação de conhecer as regras de conduta e agir de acordo com elas, para a criação e a manutenção de um ambiente seguro para todos e para os ativos da organização.

Num mundo com tantos equipamentos eletrônicos a serviço da Segurança e com a Internet das coisas possibilitando, a cada dia, inovações que reforçam a capacidade de trabalho da área de Segurança Patrimonial, é fácil acontecer de as pessoas não se darem conta da própria importância para a Segurança. Muitas vezes, há colaboradores que chegam a reclamar da necessidade de certos procedimentos que, invariavelmente, são implantados visando evitar riscos não só para a empresa, mas para as pessoas. Por exemplo, o controle de acesso, com vistoria nos porta-malas dos veículos, a necessidade de cadastramento de visitantes, o treinamento de evacuação das instalações para caso de incêndio ou até mesmo a instalação de câmeras de CFTV nos ambientes de trabalho.

Para que as ações implementadas em prol da Segurança Patrimonial obtenham êxito,

o fator humano, o engajamento e o comportamento das pessoas são fundamentais. Sem isso, abrem-se brechas na Segurança Patrimonial que, em questão de tempo, serão utilizadas por pessoas mal-intencionadas em suas tentativas de agir contra o patrimônio ou as pessoas da empresa. De nada servirá o uso de crachá eletrônico, se ele for emprestado para outra pessoa entrar no ambiente da empresa; os detectores de abertura de porta perderão sua utilidade se os colaboradores mantiverem a porta permanentemente aberta; o portão não impedirá a entrada de pessoa não autorizada se for deixado destrancado. E por aí vai.

Por isso, é fundamental que a empresa tenha e divulgue amplamente, a todos os stakeholders, a sua política de segurança corporativa, com diretrizes e procedimentos claros, e utilize as ferramentas de endomarketing para enfatizar os pontos que a Gestão de Riscos julgar mais importantes. Para evitar a materialização de riscos, faz-se necessário o pleno entendimento da importância da participação de todos, de modo a obter-se o desejado e necessário engajamento dos colaboradores em todos os níveis da organização.

Com o bom entendimento e aplicação das diretrizes de segurança pelo público interno, integrados a processos bem estruturados e tecnologia eficaz, a segurança patrimonial terá muito mais chances de sucesso.

Não temos dúvidas, aliás, de que a tecnologia tem ajudado muito a otimizar a Gestão dos Riscos de Segurança Patrimonial, trazendo mais eficiência e eficácia nos resultados, mitigando os riscos e evitando falhas, que é o objetivo principal, assim como a diminuição dos custos. Por isso, recomendamos o Software INTERISK, uma solução que integra as diversas disciplinas de riscos e que é perfeitamente personalizável para cada cliente. Entre em contato conosco para conhecer a nossa solução, seus diferenciais e benefícios que trarão mais facilidade, agilidade e eficiência para a sua Gestão de Riscos.

GESTÃO DA SEGURANÇA PATRIMONIAL: APLICAÇÃO DO MÉTODO PDCA

Carlos Köhler, CPSI, CISI, MBS e CRA | Graduado em Segurança Pública, Pós Graduando em Segurança Privada, CEO do Grupo CINDAPA

Temos observado que muitos gestores de segurança patrimonial estão insatisfeitos com sua atuação devido à falta de investimentos em segurança e que o seu setor só é visto quando alguma grande perda ocorre.

Por que isso acontece? Será que os diretores não sabem os riscos que a empresa está exposta, bem como as perdas que podem ocorrer, gerando prejuízos? Ou há outros motivos para essa "falta" de investimentos na área de segurança patrimonial?

Sabe-se que em muitas empresas não há preocupação com essa área e o motivo é que existe pouca oferta de profissionais qualificados com experiência no segmento. O fato é que a grande maioria desses profissionais não está preocupada com o resultado financeiro do negócio das empresas em que trabalham, não sabem qual é o custo efetivo que o seu setor representa no contexto geral e estão focados somente na operação em si e não nos processos gerenciais e não possuem a capacidade de fazer análises gerenciais e estratégicas, enfim, possuem perfis operacionais. Para corroborar a isso, a maioria das formações acadêmicas do setor ainda acompanham esse modelo antigo, ou seja, abordam somente disciplinas operacionais, não apresentando no mínimo questões básicas de gestão de processos administrativos e gerenciais.

Nesse contexto, é importante situar e clarificar onde a Gestão da Segurança Patrimonial se encontra no organograma de uma empresa. Destacar qual é a função dela e sinalizar como ela ajuda toda empresa alcançar os resultados das metas estratégicas.

Se por um lado, há empresas que pouco ou nada observam em relação à segurança patrimonial, vale lembrar que, por outro lado, há empresas organizadas que têm esse setor específico e com metas bem definidas e que são muito bem vistos, recebendo recursos para uma excelente gestão.

O Mestre em administração, professor Falconi enfatiza que o sucesso de uma gestão depende de três fatores: conhecimento, liderança e método. O método PDCA tem sido utilizado pela maioria das empresas de sucesso, obtendo excelentes resultados. O método é simples, porém poucas empresas conseguem aplicar, pela dificuldade em ter um ritual.

Quando se fala em Segurança Patrimonial, a inteligência em riscos é a chave necessária do conhecimento e a utilização de ferramentas e metodologias do Prof. Dr. Antônio Celso Ribeiro Brasiliano são um atalho para quem almeja uma Gestão de Resultados.

A Gestão em Segurança Patrimonial tem como objetivo a redução das perdas, para que a empresa possa ser mais competitiva e alcançar os resultados das metas estratégicas. Brasiliano classifica as perdas em quatro categorias: financeiro, imagem, “compliance” e operacional. Perdas em qualquer uma dessas categorias, afeta o resultado estratégico da empresa e por isso a importância do gerenciamento de riscos corporativos, que abrange todos os campos de uma empresa no qual a segurança patrimonial está inserida.

A maneira prática de utilização dos métodos para se alcançar as metas da Segurança Patrimonial requer um bom planejamento. Recomenda-se iniciar pelo entendimento das diretrizes, políticas, estratégias e negócios da empresa, entre outros pontos importantes que explicam o negócio, para daí criar um organograma específico e localizar a Segurança Patrimonial na hierarquia da empresa. Complementarmente, faz-se necessário a criação de fluxogramas para deixar claro os processos e subprocessos da Segurança Patrimonial, assim como a confecção de Procedimentos Operacionais – POP´S para que o cada integrante da equipe saiba o que se espera dele, especificando quais são suas atribuições. Outra ação necessária dentro do planejamento é a elaboração de metas para cada processo e subprocesso de todos envolvidos.

Feito isso, é hora de aplicar o que foi planejado nas atividades de rotina, seguido pela verificação dos indicadores para sabermos se o que está sendo realizado está conforme o previsto. A partir disso, seguindo na metodologia do PDCA, devemos ajustar os procedimentos que não alcançaram as metas, e que precisam de ajustes, ou no planejamento ou na execução.

Aos interessados que queiram se destacar nesse mercado que cresce de forma exponencialmente, cabe as seguintes reflexões:

Você já tem no seu planejamento as metas estratégicas da Gestão da Segurança Patrimonial, bem como metas para os níveis gerenciais e operacionais? Se não, faça quanto antes, pois sem metas claras e definidas, dificilmente se alcançarão os objetivos.

Qual a importância do líder para que todos os integrantes sejam membros de um único time? Como ser um verdadeiro Líder que motiva as pessoas a alcançarem metas e serem felizes? O Líder tem um papel fundamental para o sucesso de uma Gestão eficaz.

O livro “GESTÃO DA SEGURANÇA PATRIMONIAL: aplicação do método PDCA”, aborda todos estes temas de forma simples, ensinando a utilização do método PDCA nos processos da Gestão de Segurança Patrimonial.

HABILIDADES TÉCNICAS DOS PROFISSIONAIS DE SEGURANÇA EMPRESARIAL

Dr. Hebert Magno, CPSI, CIGR, CIEIE, DIDS | Delegado CEAS Regional- MG, Doutor Internacional en Ciencias de la Seguridad, pela Corporación Euro-Americana de Seguridad – Espanha.

No mundo empresarial contemporâneo, a segurança tornou-se um aspecto crucial para as organizações em todos os setores. Com o avanço da tecnologia e a crescente dependência de sistemas digitais, as empresas estão cada vez mais conscientes dos riscos de violações de segurança e dos impactos negativos que podem resultar dessas ameaças. Diante desse cenário, a busca por profissionais especializados em segurança empresarial tem se intensificado, com as empresas reconhecendo a importância de proteger seus ativos e informações sensíveis.

Desenvolver uma estratégia de segurança empresarial eficaz requer uma abordagem abrangente e proativa. Os profissionais de segurança são responsáveis por identificar, avaliar e mitigar os riscos associados às operações empresariais. Eles devem estar atualizados sobre as últimas tendências e ameaças em segurança cibernética, física e de dados, bem como possuir habilidades técnicas para implementar e gerenciar sistemas de segurança.

Além disso, as empresas estão buscando profissionais com capacidade de análise e tomada de decisões rápidas, capazes de responder a incidentes de segurança de forma eficiente. A capacidade de antecipar e prevenir ameaças, bem como de identificar e investigar possíveis violações de segurança, é valorizada pelos empregadores.

As competências técnicas são essenciais, mas as habilidades interpessoais também são cada vez mais valorizadas. Profissionais de segurança empresarial devem ser capazes de comunicar efetivamente com diferentes partes interessadas, incluindo funcionários,

gerentes e parceiros externos. Eles devem ser capazes de articular as medidas de segurança de forma clara e concisa, a fim de obter apoio e cooperação de todos os envolvidos.

No atual ambiente empresarial altamente conectado e vulnerável a ameaças, a segurança tornou-se uma prioridade estratégica para as empresas. A busca por profissionais especializados em segurança empresarial reflete o compromisso das organizações em proteger seus ativos e garantir a continuidade dos negócios. Os profissionais que possuem conhecimentos atualizados, habilidades técnicas e competências interpessoais estão em alta demanda, e a sua contribuição é fundamental para garantir a segurança e o sucesso das empresas na atualidade.

Para atender às demandas atuais de segurança empresarial, as empresas estão buscando profissionais que sejam versáteis e adaptáveis. A natureza em constante evolução das ameaças exige que os especialistas em segurança empresarial estejam dispostos a aprender e se atualizar constantemente. A capacidade de se manter informado sobre as últimas tendências em segurança, participar de treinamentos especializados e obter certificações relevantes é altamente valorizada.

Com isso, as empresas também estão interessadas em profissionais que possuam uma mentalidade proativa em relação à segurança. Isso significa que eles devem ser capazes de antecipar possíveis vulnerabilidades e implementar medidas preventivas antes que as ameaças se materializem. A capacidade de realizar avaliações de risco abrangentes, identificar pontos fracos e implementar soluções de segurança adequadas são características essenciais que as empresas buscam nos profissionais de segurança empresarial. Em resumo, as empresas estão em busca de especialistas em segurança empresarial que sejam ágeis, adaptáveis, bem informados e proativos, capazes de garantir a proteção dos ativos e a continuidade dos negócios em um ambiente empresarial cada vez mais desafiador.

PLANO DE RESPOSTA A INCIDENTES CIBERNÉTICOS

Mariana da Silveira, DIDS, MBCR, CPSI, CEGRC, CIGR, CISI, CIEIE, DPO, ISO | Divisão Cibernética da Brasiliano INTERISK

Antes de o incidente cibernético ocorrer, é preciso que a organização possua um processo estabelecido, chamado Plano de Continuidade de Negócios – PCN, contendo as informações necessárias para mitigar os danos a ela causados. No processo do PCN existe o PRI. Se você ainda não sabe o que deve conter no PRI, certamente também não saberá o que fazer para realizar a melhoria contínua, bem como para assimilar as lições aprendidas após o incidente.

O ponto importante do PRI é focar na infraestrutura crítica de TI, composta basicamente de redes, hardware, software e bancos de dados. A organização precisará realizar ações para provisionar recursos, recuperar os negócios e retornar à normalidade. Assim, é preciso definir como será o fluxo de resposta a incidentes, ou ajustar o fluxo atual, caso haja, que contêm os critérios de acionamento do PCN, devendo ser periodicamente revisado.

Um plano de recuperação de incidentes é um conjunto de procedimentos documentados que descrevem como responder a um incidente de segurança. Os passos para construir um PRI consistem em identificar o Cenário Prospectivo, estabelecer a Política Diretriz e o Protocolo de Resposta, realizar o Registro de Incidente de Segurança da Informação e o Cadastro de Teste e Revisão do Plano.

Para tanto, é preciso o estabelecimento prévio de um conjunto de subprocessos e procedimentos, tais como a identificação dos ativos críticos, a identificação de informações, processos, softwares e aplicativos críticos para o negócio, que devem ser protegidos. gerir as ameaças, que possam afetar tais ativos críticos, definir as medidas de segurança apropriadas para proteger esses ativos críticos contra as ameaças identificadas.

A preparação é a chave para a resposta efetiva a incidentes cibernéticos. Isso inclui a formação de uma equipe de resposta a incidentes, a identificação dos principais ativos e sistemas de informação, a documentação de processos e procedimentos de segurança, e a implementação de controles de segurança adequados. Bem como a detecção, com a análise de incidentes e o monitoramento de logs e alertas de segurança.

A equipe de resposta a incidentes deve ser capaz de identificar o tipo e a extensão do incidente e avaliar o impacto sobre os sistemas e dados da organização. Uma vez que o incidente foi identificado, é importante conter e mitigar os danos. Isso pode incluir a desativação de softwares afetados, a aplicação de patches de segurança, a restauração de backups de dados e a implementação de controles adicionais de segurança.

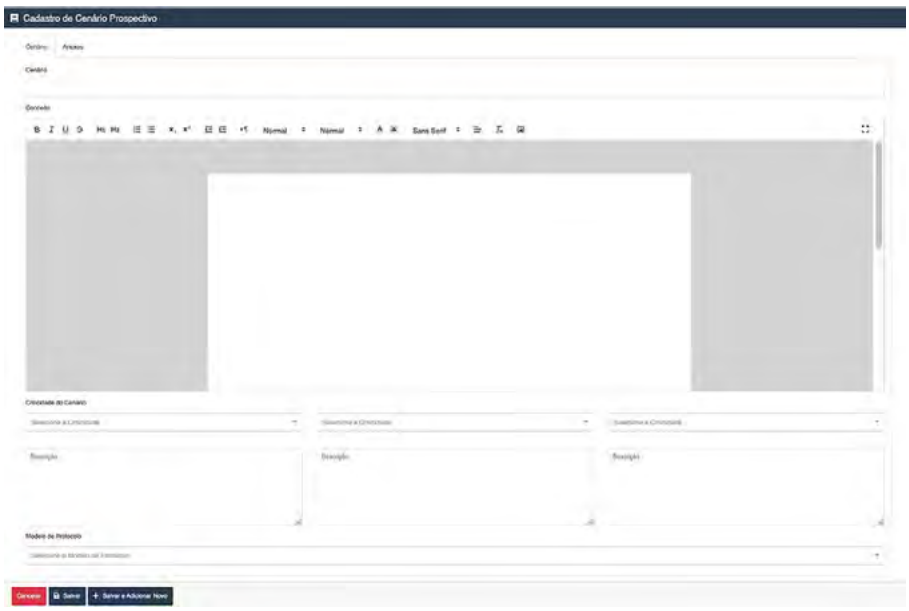
Deve ser conduzida uma investigação completa do incidente com análise forense para determinar a causa raiz, o escopo do incidente e quaisquer medidas adicionais que devem ser tomadas para evitar futuros incidentes. A equipe de resposta a incidentes deve notificar as partes afetadas, como clientes, fornecedores e órgãos reguladores, e elaborar um relatório detalhado do incidente e das medidas tomadas para sanar ou mitigar os danos.

A restauração da estrutura afetada deve ocorrer alinhada com o Plano elaborado, validado, testado e melhorado, por intermédio da implementação de medidas adicionais de segurança e do aperfeiçoamento das já existentes, após a verificação da necessidade de melhoria contínua, quando identificada, durante testes de eficácia do PRI com a incorporação das lições aprendidas, assim o retorno aos níveis aceitáveis de segurança ocorrerá em menor tempo.

Uma vez controlada a contingência e passada a crise, a organização inicia o retorno aos seus níveis originais de operação, pois as prioridades foram definidas anteriormente, os protocolos de retomada acionados de maneira organizada e concatenada, os papéis e as responsabilidades estabelecidos, as pessoas estão treinadas e preparadas, os recursos e os meios disponibilizados, as lições aprendidas incorporadas, para o retorno à normalidade.

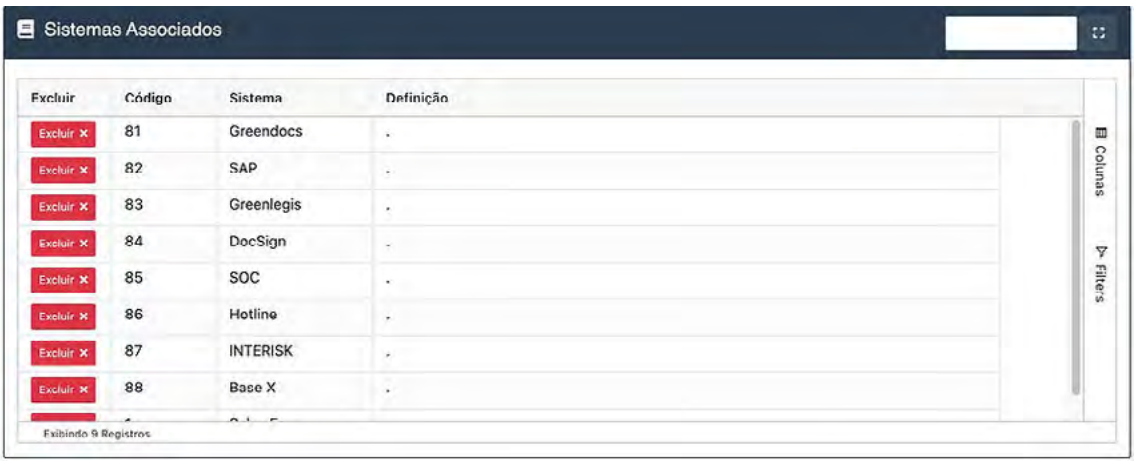
De todas as etapas a serem percorridas durante a execução de um PRI, o processo de melhoria contínua e a incorporação de lições aprendidas devem ser destacados neste momento. Pois, de pouco adiantaria aperfeiçoar as medidas técnicas de segurança, já existentes, em redes, hardware, software e bancos de dados, e novas medidas técnicas de segurança se as lições apresentadas, na ocasião do incidente, não fossem assimiladas.

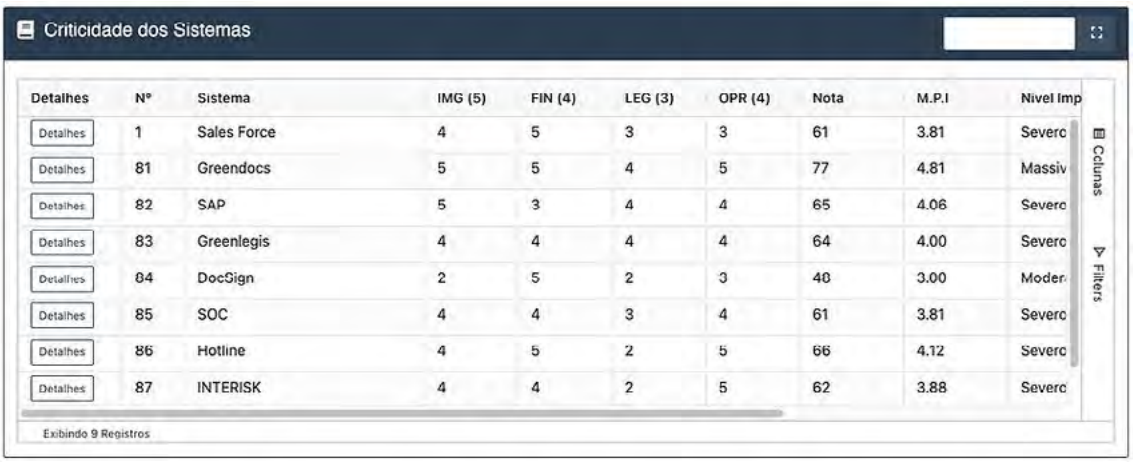
O método Brasiliano de PRI, utilizado no Software INTERISK, consiste em algumas etapas, detalhadas a seguir. A primeira é a identificação do Cenário Prospectivo, na qual é realizado o Cadastro de Cenários Prospectivos:



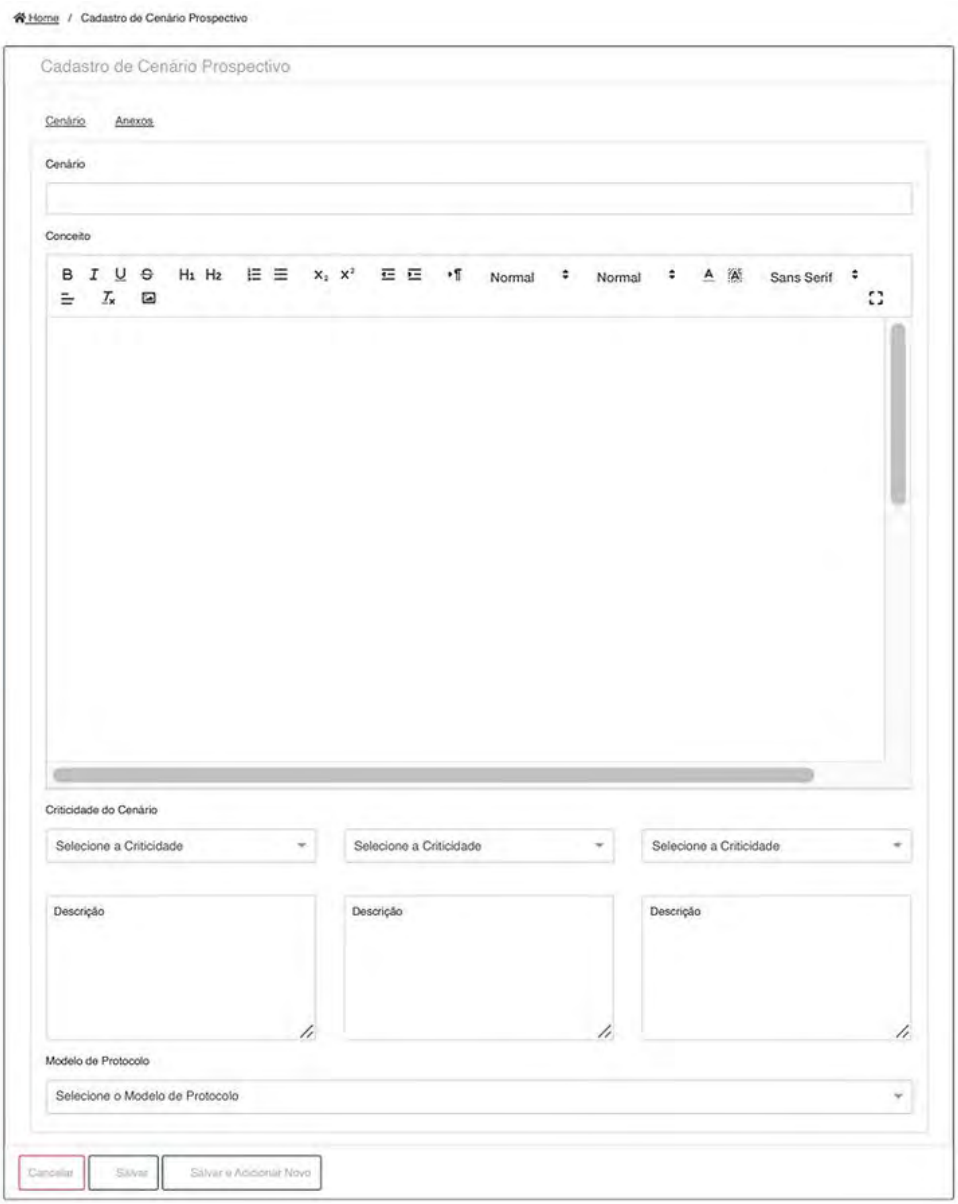
Assim, é possível visualizar todos os cenários prospectivos para sua organização:

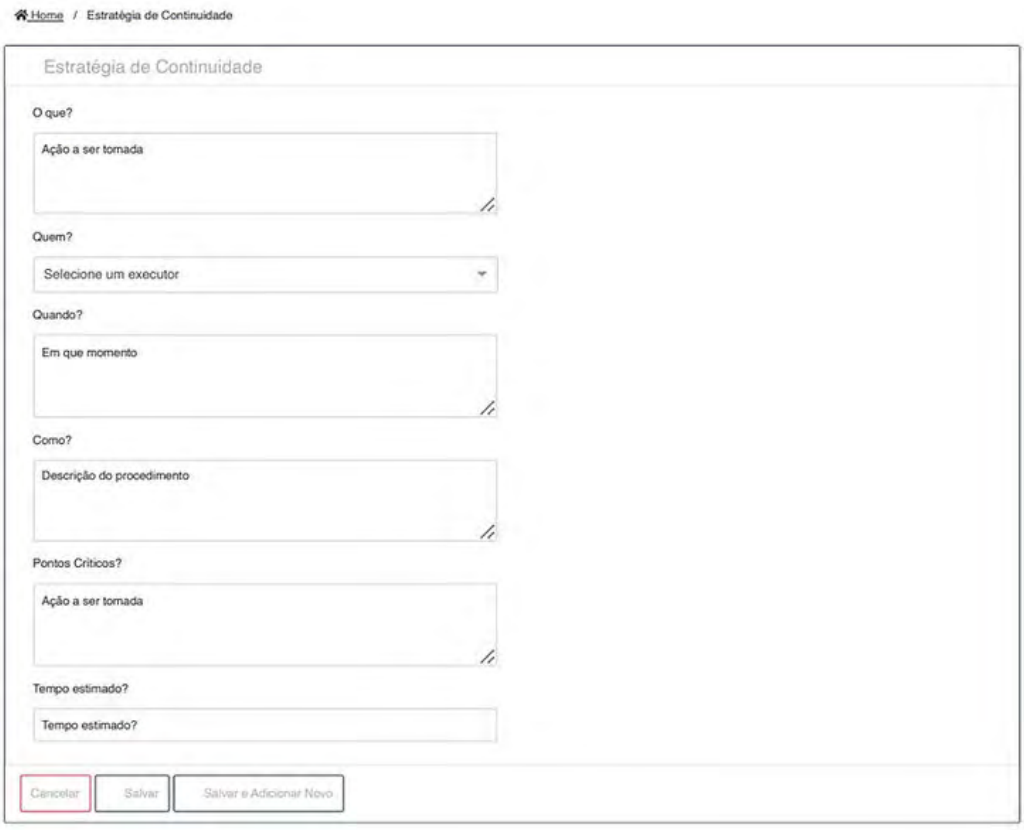
Na etapa do Business Impact Analysis – BIA, responsáveis, unidades de negócio, processos e sistemas críticos são mapeados, priorizados e validados pela alta direção:

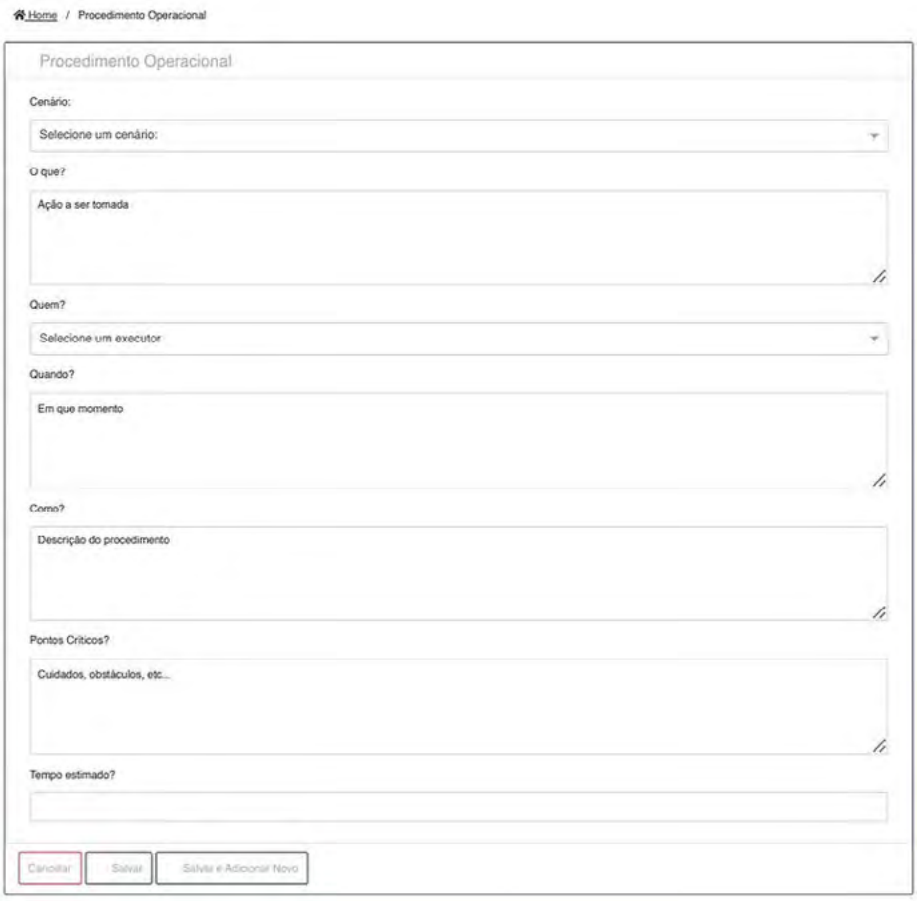




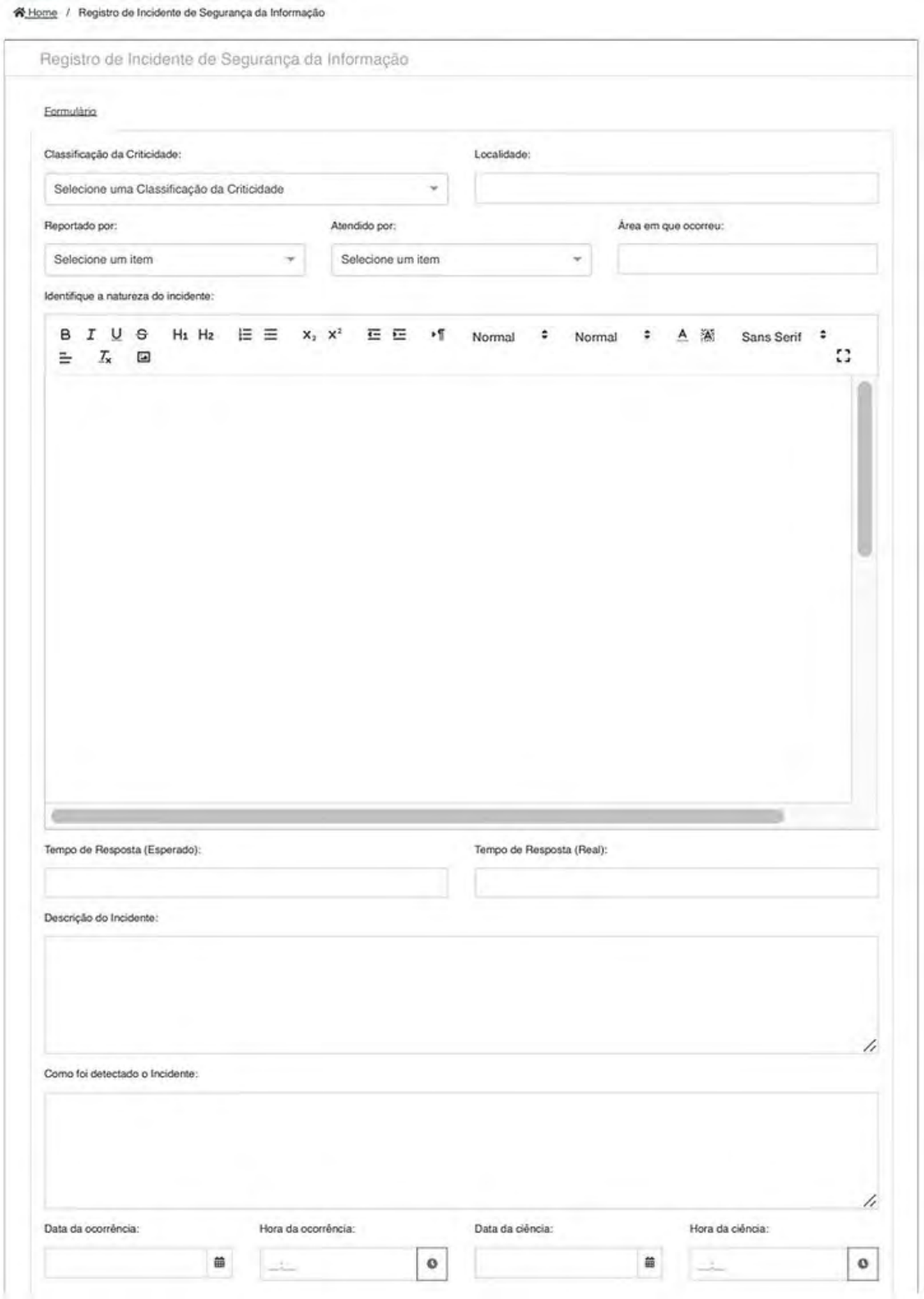
As criticidades são estabelecidas, os cenários críticos são elaborados, as estratégias de continuidade definidas, e os Planos de Continuidade Operacionais, estruturados.


Home / Cadastro de Cenário Prospectivo
Cadastro de Cenário Prospectivo
Cenário
Anexos
Cenário
Conceito
Normal
Normal
Sans Serif
Criticidade do Cenário
Selecione a Criticidade
Selecione a Criticidade
Selecione a Criticidade
Descrição
Descrição
Descrição
Modelo de Protocolo
Selecione o Modelo de Protocolo
Cancelar
Salvar
Salvar e Adicionar Novo

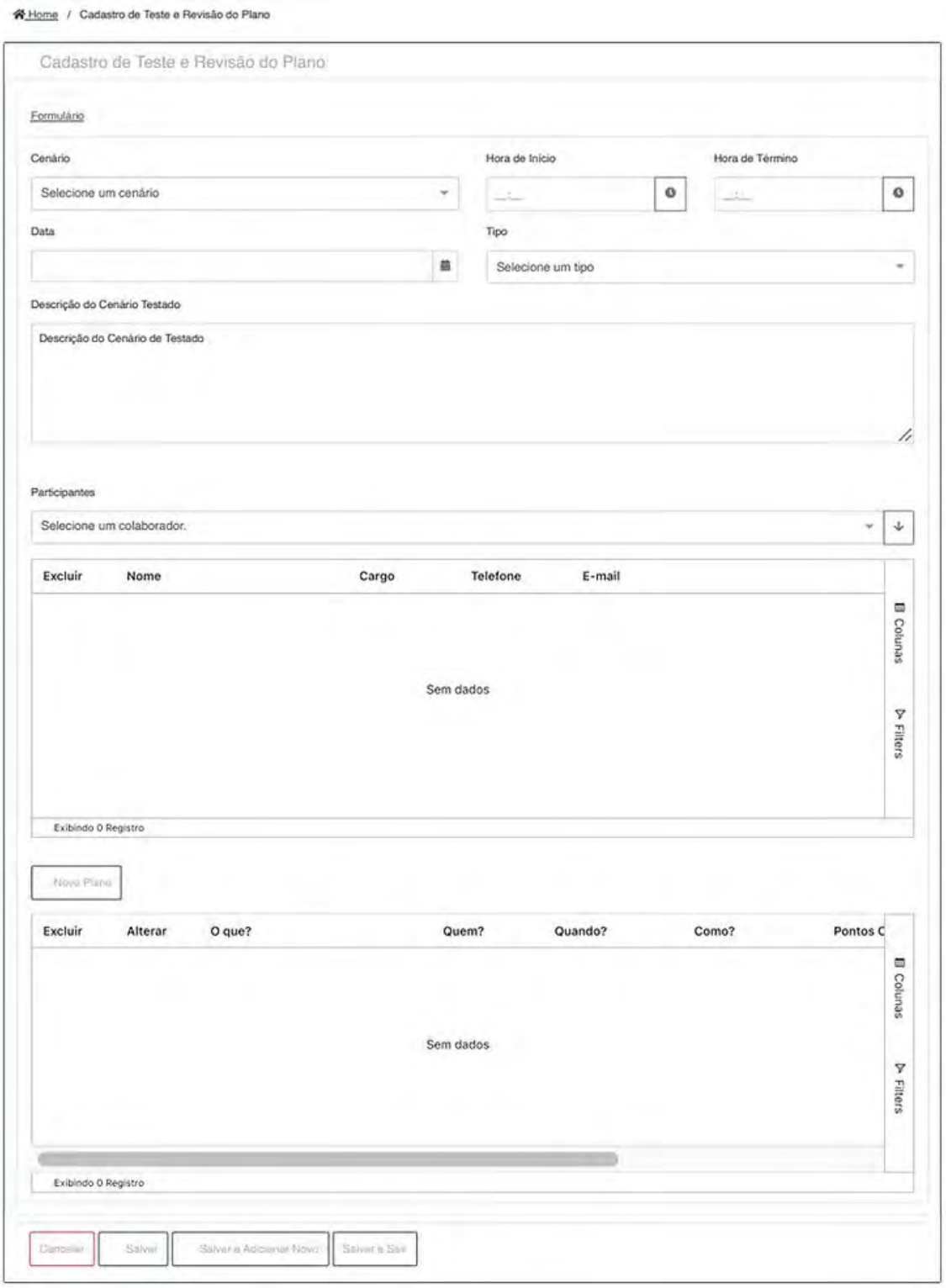

Home / Estratégia de Continuidade
Estratégia de Continuidade
O que?
Ação a ser tomada
Quem?
Selecione um executor
Quando?
Em que momento
Como?
Descrição do procedimento
Pontos Criticos?
Ação a ser tomada
Tempo estimado?
Tempo estimado?
Cancelar
Salvar
Salvar e Adicionar Novo


Home / Procedimento Operacional
Procedimento Operacional
Cenário:
Selecione um cenário:
O que?
Ação a ser tomada
Quem?
Selecione um executor
Quando?
Em que momento
Como?
Descrição do procedimento
Pontos Criticos?
Cuidados, obstáculos, etc...
Tempo estimado?
Cancelar
Salvar
Salvar e Adicionar Novo

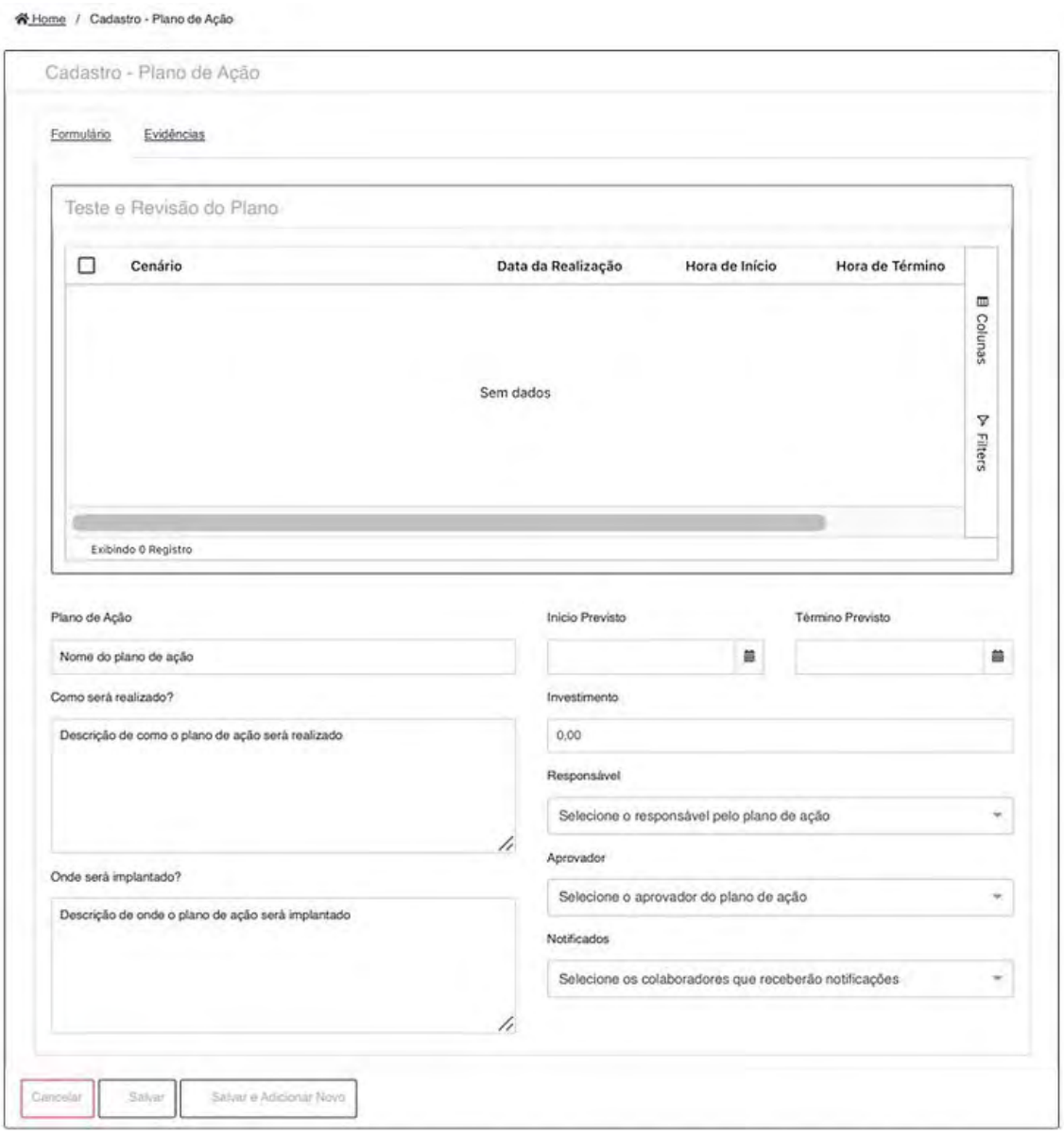
Quando um Cenário Prospectivo é materializado, as diretrizes da Política são executadas, a fim de orientar as tomadas de decisão. O acionamento do Protocolo de Resposta a Incidentes é realizado para, em seguida, iniciar o Registro de Incidente de Segurança da Informação com a comunicação às autoridades.



O Cadastro de Teste é realizado, bem como a Revisão do Plano em um processo de melhoria contínua:



Por fim, é realizado o cadastro do Plano de Ação a fim de atuar com medidas corretivas para preencher lacunas, possíveis distorções ou melhorias identificadas durante a execução dos testes:



Quer conhecer com profundidade o framework exclusivo da Brasiliano INTERISK? Inspirado no COSO, nas Normas ISO 31.000/2018, 22.301/2020, 22.317/2023 e 27.031/2023, é um modelo em constante atualização e baseado nos frameworks e estruturas mais aceitos mundialmente, assim como nas melhores práticas do mercado, graças à vanguarda, em Gestão de Riscos no Brasil, do nosso presidente e fundador da Brasiliano INTERISK.

Entre em contato e solicite uma demonstração do Software INTERISK - Módulo GCN para visualizar na prática a elaboração do Plano de Resposta a Incidentes - PRI.

POLÍTICAS DE CONTINUIDADE DE NEGÓCIOS - ISO 22313

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

Política de continuidade de negócios é um conjunto de padrões e diretrizes que uma organização elabora para garantir a resiliência e o gerenciamento adequado de riscos. Essa política varia de acordo com a organização e demanda atualizações constantes, de acordo com a evolução das tecnologias e a mudança dos riscos comerciais.

Essa política tem por objetivo a documentação do que é necessário para manter a organização funcionando, tanto no dia a dia quanto nos momentos de emergência. Com uma política bem definida e cumprida claramente, a empresa pode definir expectativas realistas para processos de continuidade de negócios e recuperação perante desastres. Essa política também pode ser usada para determinar o que deu errado para que os problemas possam ser resolvidos.

Embora as políticas de continuidade de negócios sejam diferentes para cada empresa, todas incluem componentes básicos. Os principais incluem equipe, métricas e requisitos padrão.

A Organização Internacional de Normalização (ISO) e a Instituição de Normas do Reino Unido (BSI) emitem padrões comuns de continuidade de negócios. No Brasil, atualmente, a Norma ABNT NBR ISO 22313:2020 é a diretriz para a elaboração de uma política de continuidade de negócios. Esses padrões são atualizados de tempos em tempos, portanto, as mudanças devem ser monitoradas.

A elaboração da política de continuidade de negócios deve ser estabelecida em termos

objetivos, sendo assegurado pela alta direção que:

- É uma declaração concisa e de alto nível da intenção de direcionamento da alta direção para o Sistema de Gestão de Continuidade de negócios (SGCN);
- É apropriada para a finalidade da organização frente ao seu tamanho, natureza e complexidade, refletindo sua cultura, dependências e ambiente de funcionamento
- Fornece estrutura para definir objetivos;
- Inclui compromissos claros para atender requisitos aplicáveis, incluindo obrigações legais e regulamentares;
- Inclui comprometimento com a melhoria contínua do SGCN.

A política de continuidade de negócios deve especificar claramente o escopo e os limites do programa de continuidade de negócios da organização, incluindo suas limitações e exclusões. Ela deve identificar todas a autoridades e delegações necessárias, incluindo os responsáveis pelo SGCN da organização, além de incluir referências às normas, diretrizes, regulamentos e políticas que o SGCN deve considerar e cumprir.

Uma boa política de continuidade de negócios deve estabelecer um comprometimento de financiamento e o compromisso de exercitar e manter a continuidade de negócios, bem como fazer referências a outras políticas relacionadas.

No caso de existirem outros sistemas de gestão, é conveniente que a política seja integrada àquelas com as quais manterá algum tipo de relacionamento.

Devem ser tomadas medidas para aprovar a política, reter informações documentadas sobre ela e fazer análises críticas de forma periódica. Além disso, sempre que ocorrerem mudanças significativas em fatores internos ou externos, ela deve ser atualizada.

A política de continuidade de negócios deve ser documentada, comunicada, compreendida e aplicada dentro da organização, sendo ainda disponibilizada a todas as partes interessadas.

A alta direção da organização deve assegurar que haja a comunicação das responsabilidades e autoridades dentro do SGCN e estabelecer quem será o responsável e o responsabilizado neste processo.

Caso seja de interesse da organização, poderá ser nomeado um comitê para supervisionar a implementação e o monitoramento contínuo do SGCN. Seus representantes serão nomeados com papéis, responsabilidades e autoridade definidas para:

- assegurar que o SGCN esteja em conformidade com a política de continuidade de negócios;

- relatar o desempenho do SGCN à alta direção da organização para análise crítica e como base para melhorias;
- promover a conscientização sobre a continuidade de negócios através de toda organização;
- assegurar a eficácia dos procedimentos desenvolvidos para responder a incidentes.

O representante da alta direção poderá receber um título específico, ter outras responsabilidades dentro da organização e pertencer a qualquer área da organização.

Por fim, destacamos que todos os papéis, responsabilidades e autoridades do SGCN devem ser definidos e documentados e estar sujeitos a auditoria.

O Software INTERISK contém um módulo específico de Gestão de Continuidade de Negócios e, sendo totalmente parametrizável para atender às necessidades do cliente, pode se tornar um grande aliado ao SGCN da organização.

PREVENÇÃO DE PERDAS - PLANEJAMENTO

Dr. Sérgio Caldas CRA, MBA, MBR, CPSI, CIEIE, CIEAC, CIGR, DIDS, MSDIS, DICS | Doctor en Ciencias de la Seguridad (España) | Gestão Empresarial e Corporativa | Prevenção e Controle de Perdas | Riscos Corporativos
Prof. Dr. Nino Meireles, CPSI, CIGR, CIEIE, CIEAC, CISI, DIDS | Doctor en Ciencias de la Seguridad (España); Diretor de Formação e Extensão Universitária da CEAS-BRASIL e Coordenador e professor do MBA em Gestão Estratégica da Segurança Corporativa da Faculdade FACEI.

O planejamento pode ser definido de diversas maneiras. Resumidamente poderíamos dizer que planejar é definir metas e os meios necessários para alcançá-las.

Além de processo de tomar decisões e competência intelectual, planejar é uma questão de atitude.

PLANEJAMENTO

O processo de planejar é composto de três passos:

- aquisição de entrada;
- processamento de dados; e
- elaboração de plano.

Cada um desses passos é um processo em si, envolvendo diagnóstico, avaliação de alternativas e escolha de um caminho.

A obtenção de dados de entrada são informações sobre o presente, passado ou futuro dos ambientes externo e interno (subsistemas da empresa). Os dados mostram pontos

fortes, pontos fracos, ameaças e oportunidades.

O segundo passo (processamento de dados) significa transformar informação para produzir novas informações e decisões. A transformação é feita por meio de:

- Interpretação do significado das informações;
- Identificação de alternativas para lidar com os pontos fortes, pontos fracos, ameaças e oportunidades; e
- Avaliação das alternativas e escolha do caminho.

O resultado do planejamento é a elaboração de planos. Em essência, um plano é o registro das decisões resultantes do processamento dos dados de entrada. De uma maneira geral, um plano apresenta no mínimo os seguintes pontos:

- metas;
- definição de meios para realizar as metas; e
- previsão dos meios de controle.

As metas normalmente desdobram-se em outras metas. Uma sucessão de metas interligadas forma uma cadeia de meios e fins. Sempre que for possível, as metas devem ser quantitativas. Devem ser desenvolvidas em termos numéricos, associadas aos indicadores de desempenho.

> "Para a concretização de metas, é necessário estabelecer cursos de ação, executar atividades e empregar recursos."

Os meios de controle são informações para avaliar até que ponto as metas estão sendo atingidas e os cursos de ação escolhidos são apropriados.

Os planos podem ser classificados de diversas maneiras. Uma das formas mais comuns de classificação é o critério da permanência, que classifica os planos em temporários e permanentes. Os temporários extinguem-se quando as metas são alcançadas e contêm decisões não programadas.

Já os planos permanentes contêm as decisões programadas, que devem ser usadas em situações predefinidas. Exemplos deste tipo de plano são as políticas e os procedimentos.

O planejamento não deve ser confundido com previsão, projeção, predição, resolução de problemas ou plano, pois:

- Previsão – É o esforço para verificar quais serão os eventos que poderão ocorrer;
- Predição – É a situação em que o futuro tende a ser diferente do passado,

mas a empresa não tem nenhum controle sobre seu processo;

- Projeção – É a situação em que o futuro tende a ser igual ao passado;
- Resolução de problemas – Corresponde a aspectos imediatos que procuram a correção de certas descontinuidades e desajustes entre a empresa e as forças externas;
- Plano – Documento formal que se constitui na consolidação das informações das atividades desenvolvidas no processo de planejamento.

Dependendo da abrangência e do impacto que têm sobre a organização, os planos podem ser classificados em três níveis principais:

- estratégico;
- tático; e
- operacional.

CICLO PDCA

Esta ferramenta deve ser utilizada por todas as empresas e gestores, pois gerenciar sem planejamento é fazer a gestão de forma empírica e com grande probabilidade dos objetivos não serem alcançados. Apesar deste capítulo tratar do P deste ciclo, é importante fazermos uma breve abordagem completa.

Este ciclo é composto de quatro fases: planejar (P), executar (D), controlar (C) e ação corretiva (A).

Na fase do planejamento (primeira etapa) as atividades a serem desenvolvidas são:

- diagnóstico;
- estabelecimento de metas;
- estabelecimento de medidas; e
- elaboração dos planos de ação (5W 2H).

Na segunda fase, execução (do), as atividades são:

- atuação de acordo com os planos de ação,
- coletar informações dos resultados do processo; e
- treinamento das pessoas.

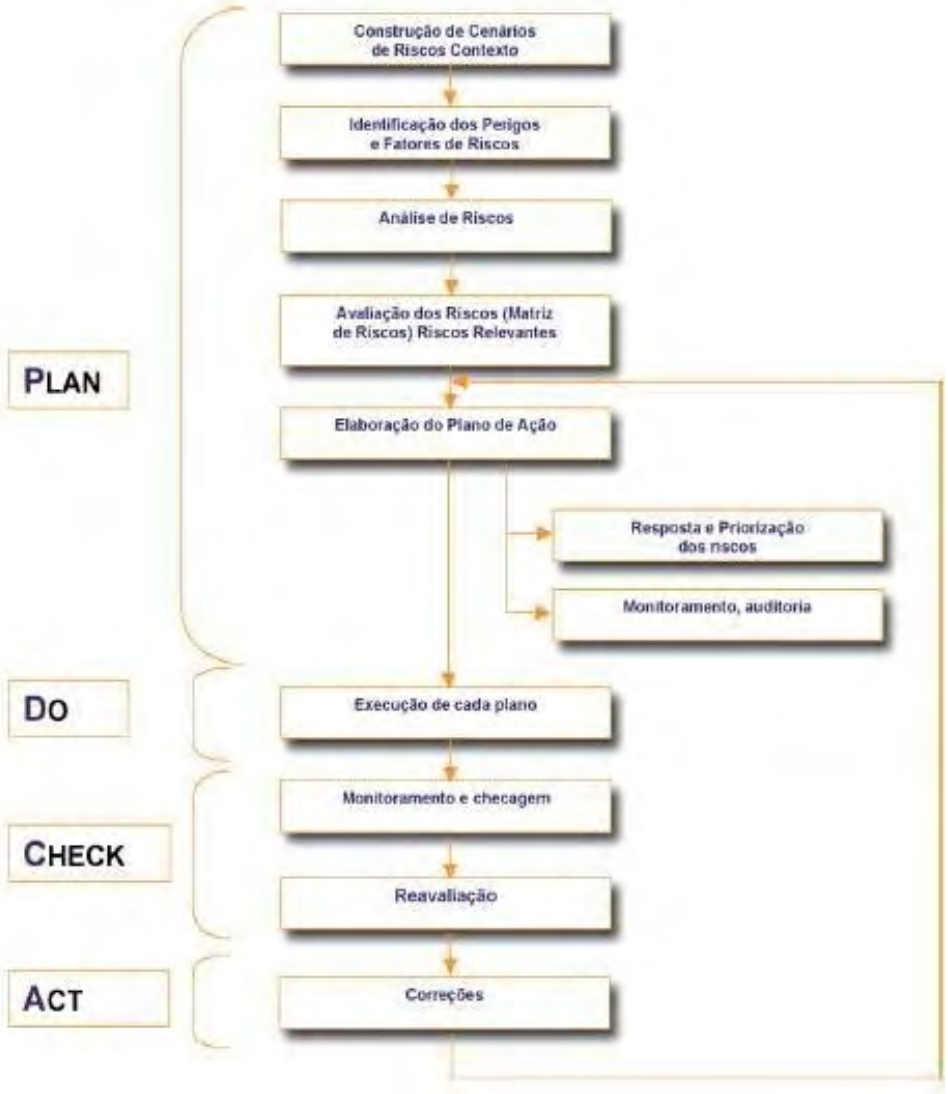
Na fase (C) as atividades são:

- avaliar o alcance das metas; e
- utilizar as informações obtidas durante a execução.

Na última fase (A), as atividades são:

- padronização;
- treinamento;
- revisão das atividades; e
- planejamento para trabalho futuro.

Se for observado desvio em relação à meta (problema), serão buscadas as causas geradoras e serão estabelecidas as contramedidas necessárias.



Ciclo DDCA

Os planos de ação devem ser desenvolvidos com base na técnica conhecida por 5W2H, sendo:

- What (O que fazer?) – Quais ações serão implementadas;
- Who (Quem?) – Quem é o responsável, podendo ser uma pessoa ou um grupo;
- When (Quando?) – Horizonte temporal de implementação de cada ação;
- Where (Onde?) – Quais serão os setores e locais da empresa nos quais as ações serão implantadas;
- Why (Por que?) – Quais são as justificativas;
- How (Como?) – De que forma será implantada a ação (em fases ou de uma única vez);
- How Much (Quanto custa?) – Projeção de investimento.

WHAT	WHO	WHEN	WHERE	WHY	HOW	HOW MUCH
O QUE	QUEM	QUANDO	ONDE	POR QUE	COMO	QUANTO CUSTA

Plano de Ação 5W 2H

A depender da situação pode ser utilizado 5W1H e o segundo H (quanto custa) é feito em separado. Outra alternativa é a utilização de mais uma coluna, a de STATUS ou ACOMPANHAMENTO. É uma forma de controle para saber se a ação foi realizada ou não. A legenda que pode ser utilizada é:

- vermelho não realizado;
- verde realizado; e
- amarelo em execução.

É importante também a definição de meta. Meta é um ponto a ser atingido e é constituída de três partes:

- objetivo gerencial;
- valor; e
- prazo.

Ela é estabelecida sempre sobre os fins, nunca sobre os meios.

As metas normalmente desdobram-se em outras metas. Uma sucessão de metas interligadas forma uma cadeia de meios e fins. Para a concretização de metas, é necessário estabelecer cursos de ação, executar atividades e empregar recursos.

Os meios de controle são informações para avaliar até que ponto as metas estão sendo atingidas e os cursos de ação escolhidos são apropriados. Quando adicionamos à meta as medidas necessárias para alcança-la, temos a diretriz.

PRINCÍPIOS

Os princípios do planejamento podem ser divididos em: gerais e específicos.

Os princípios gerais são:

- Contribuição – Visa os objetivos máximos da empresa;
- Precedência – Função administrativa que antecede às outras (organização, direção e controle);
- Maior penetração – Pode provocar várias mudanças nas características e atividades da empresa. As modificações nas pessoas podem gerar necessidades de: treinamento, substituição, transferências etc;
- Maior eficácia, eficiência e efetividade – Maximizar os resultados e minimizar as deficiências.

Os princípios específicos são:

- participativo;
- coordenado;
- integrado; e
- permanente.

O primeiro estabelece que todos os setores devem ser envolvidos. Pelo segundo princípio devemos ter uma visão da empresa como sistema, sinergia. O terceiro estabelece que os diversos níveis devem ter seus planejamentos integrados. O último princípio afirma que nenhum plano mantém seu valor com o tempo.

PREVENÇÃO DE PERDAS – PLANEJAMENTO ESTRATÉGICO

Dr. Sérgio Caldas CRA, MBA, MBR, CPSI, CIEIE, CIEAC, CIGR, DIDS, MSDIS, DICS | Doctor en Ciencias de la Seguridad (España) | Gestão Empresarial e Corporativa | Prevenção e Controle de Perdas | Riscos Corporativos
Prof. Dr. Nino Meireles, CPSI, CIGR, CIEIE, CIEAC, CISI, DIDS | Doctor en Ciencias de la Seguridad (España); Diretor de Formação e Extensão Universitária da CEAS-BRASIL e Coordenador e professor do MBA em Gestão Estratégica da Segurança Corporativa da Faculdade FACEI.

Através do planejamento estratégico, a organização busca cinco objetivos:

- conhecer e melhor utilizar seus pontos fortes;
- conhecer e eliminar ou adequar seus pontos fracos;
- conhecer e usufruir as oportunidades;
- conhecer e evitar as ameaças; e
- ter um efetivo plano de trabalho.

PLANEJAMENTO ESTRATÉGICO

É importante que seja bem compreendido o que vem a ser ponto fraco, ponto forte, oportunidade e ameaça:

- Ponto forte – Variável controlável, pois está relacionada ao ambiente interno da empresa. É a diferenciação conseguida pela empresa e que lhe proporciona uma vantagem operacional;
- Ponto fraco – Variável controlável, pois está relacionada ao ambiente

interno da empresa. É uma situação inadequada que proporciona uma desvantagem operacional;

- Oportunidade – Variável incontrolável, pois está relacionada ao ambiente externo. Pode favorecer à empresa, desde que conhecida e aproveitada;
- Ameaça – Variável incontrolável, pois está relacionada ao ambiente externo. Cria obstáculos à ação estratégica da empresa, mas poderá ser evitada ou não, desde que conhecida em tempo hábil.

Conforme colocado anteriormente, o quinto objetivo do planejamento estratégico é ter um plano de trabalho efetivo. Segundo Oliveira (2004), para alcançar este objetivo é necessário estabelecer:

- As premissas básicas que devem ser consideradas no processo;
- As expectativas de situações almejadas pela organização;
- Os caminhos a serem seguidos pela organização.
- 5W 2H; e
- Como e onde alocar recursos.
- De acordo com Oliveira (2004), o planejamento deverá apresentar como resultados finais:
- Direcionamento de esforços para pontos comuns;
- Consolidação do entendimento por todos os colaboradores da missão, das macroestratégias, das micropolíticas, dos objetivos gerais, dos objetivos funcionais, das metas e dos projetos; e
- Estabelecimento de uma agenda de trabalho por um período de tempo que permita à organização trabalhar levando em conta as prioridades estabelecidas.

O conhecimento de uma metodologia de elaboração e implementação do planejamento estratégico dá ao gestor o embasamento teórico necessário para otimizar sua aplicação. O gestor deve ter domínio tanto da teoria quanto da prática, ou ser assessorado por quem tem o conhecimento.

O planejamento estratégico possui três dimensões operacionais:

- delineamento;
- elaboração; e
- implementação.

A primeira dimensão compreende a estruturação do processo de planejamento, ou seja, neste momento o gestor deve escolher a estrutura metodológica e o profissional que irá ajudá-lo (interno ou externo).

A segunda dimensão inclui a identificação das oportunidades e ameaças do ambiente externo e a adoção de estimativas de risco para as alternativas estabelecidas. Antes da escolha da alternativa, o gestor deve avaliar os pontos fortes e fracos do seu ambiente interno.

A terceira e última dimensão envolve assuntos organizacionais, os sistemas de informações, os sistemas de incentivos, a competência operacional, o treinamento e a liderança necessária ao desenvolvimento do processo.

O planejamento estratégico é composto de:

- plano de longo prazo;
- plano de médio prazo; e
- plano anual.

No plano de longo prazo (5 a 10 anos) são definidas as estratégias (meios) para se atingir a visão de futuro (fins). No plano de médio prazo (3 anos) devemos estabelecer metas sobre as estratégias do plano de longo prazo e fazer projeções financeiras que suportem as medidas. Já no plano anual devemos detalhar o primeiro ano dos planos de longo e médio prazo, com metas concretas, até o ponto de se terem os planos de ação e o orçamento anual.

BASES ESTRATÉGICAS

As bases estratégicas são:

- visão;
- missão;
- abrangência;
- princípios;
- valores; e
- escolha estratégica.

A visão é o modelo mental de uma realidade futura possível para a empresa. Deve ser definida de maneira simples, objetiva, abrangente, mas compreensível para todos os colaboradores. Uma visão compartilhada é essencial, pois sua função é explicitar o que a empresa quer ser.

A segunda base é a missão, ela é a razão de ser da empresa. Deve ser compartilhada com todos os colaboradores.

A abrangência trata das limitações existentes para a atuação da empresa. As limitações podem estar no ambiente externo (leis, geografia etc) e no ambiente interno.

Os princípios são coisas que a empresa não muda. São as crenças básicas e não pode existir meio termo, ou seja, são respeitados ou não. Já os valores são qualidades da empresa. Poderíamos fazer a seguinte analogia:

- os princípios seriam as bases de um edifício; e
- os valores o acabamento interno e externo.

As escolhas estratégicas podem ser:

- fornecimento de produtos e ou serviços de ponta;
- busca da excelência operacional; e
- estreitamento da relação com os clientes.

A empresa precisa definir uma das escolhas para ser o seu foco.

A escolha da opção estratégica deve ter por base: visão, missão, abrangência, valores e princípios. Além disso, a escolha estratégica irá influenciar: estratégias, programas de capacitação e investimentos prioritários.

TRIÂNGULO ESTRATÉGICO

Cada vértice do triângulo busca responder uma pergunta:

- o que a empresa quer ser,
- o que é permitido fazer; e
- o que a empresa sabe fazer.

A primeira pergunta, o que a empresa quer ser, tem resposta nas bases estratégicas: visão, missão, valores, princípios, abrangência e escolha estratégica.

A segunda pergunta, o que é permitido fazer, terá resposta no ambiente externo. A terceira pergunta, o que a empresa sabe fazer, tem a resposta na capacitação.

No centro do triângulo estão as estratégias, que respondem à pergunta: o que a empresa vai fazer.

PREVENÇÃO DE PERDAS – PLANEJAMENTO ESTRATÉGICO DE RECURSOS HUMANOS

Dr. Sérgio Caldas CRA, MBA, MBR, CPSI, CIEIE, CIEAC, CIGR, DIDS, MSDIS, DICS | Doctor en Ciencias de la Seguridad (España) | Gestão Empresarial e Corporativa | Prevenção e Controle de Perdas | Riscos Corporativos
Prof. Dr. Nino Meireles, CPSI, CIGR, CIEIE, CIEAC, CISI, DIDS | Doctor en Ciencias de la Seguridad (España); Diretor de Formação e Extensão Universitária da CEAS-BRASIL e Coordenador e professor do MBA em Gestão Estratégica da Segurança Corporativa da Faculdade FACEI.

Como a gestão de pessoas é uma das bases de sustentação do programa de gestão de perdas, iremos abordar, neste tópico, o planejamento estratégico de recursos humanos.

PLANEJAMENTO ESTRATÉGICO DE RECURSOS HUMANOS

Segundo Lucena (1999), este planejamento é o processo gerencial de identificação e análise das necessidades empresariais de recursos humanos e o consequente desenvolvimento de:

- políticas;
- programas;
- sistemas; e
- atividades.

De acordo com Silva (2003), planejamento estratégico de pessoas é o conjunto de

ações planejadas e organizadas de maneira estratégica para identificar necessidades da empresa quanto ao gerenciamento eficaz de recursos humanos, visando possibilitar ganhos reais de produtividade, qualidade e competitividade, bem como satisfazer os anseios pessoais e profissionais de seus colaboradores.

A elaboração deste planejamento possui duas etapas:

- previsão das necessidades de recursos humanos; e
- análise dos recursos humanos.

Na primeira etapa as ações são:

- impacto das decisões estratégicas nos recursos humanos;
- impactos das mudanças organizacionais previstas; e
- análise do ambiente e do mercado de trabalho.

A segunda etapa, análise dos recursos humanos, é composta das seguintes atividades:

- análise da capacidade instalada quantitativa e qualitativamente;
- identificação dos cargos chaves e críticos;
- metodologia para elaboração de planos de sucessão; e
- informações gerenciais sobre recursos humanos.

Existem algumas resistências a este planejamento que precisam ser entendidas para serem eficazmente tratadas.

As principais resistências são:

- Encarar as pessoas como um custo inevitável;
- Ações de recursos humanos com o objetivo de atender reivindicações e ou solucionar conflitos internos;
- Gestores sem o preparo para gerir pessoas;
- Decisões isoladas de recursos humanos; e
- Ausência de visão, formação ou experiência do gestor de pessoas.

Os modelos de planejamento são:

- baseado na procura estimada do produto ou serviço;
- baseado em segmentos de cargos;

- substituição de postos-chave;
- baseado no fluxo de pessoal; e
- planejamento integrado.

O modelo baseado na procura estimada do produto ou serviço parte do princípio de que as necessidades de pessoal são uma variável dependente desta procura. Esta relação é influenciada por:

- variações de produtividade;
- tecnologia;
- disponibilidade financeira; e
- disponibilidade de pessoas na empresa.

Este modelo está focado no nível operacional e é limitado em virtude de ter como base aspectos quantitativos (quantas pessoas x quantidade).

O modelo baseado em segmentos de cargos também está focado no nível operacional e consiste em:

- Escolher um fator estratégico (vendas, volume de produção, expansão etc) cuja variação afete proporcionalmente a necessidade de pessoas;
- Estabelecer os níveis históricos e futuro para cada fator estratégico;
- Determinar os níveis históricos de recursos humanos; e
- Projetar os níveis futuros.

O terceiro modelo, substituição de postos-chave, é conhecido por mapa de substituição ou organogramas de encarreiramento. Cada colaborador é classificado em três alternativas de promoção:

- colaborador pronto para promoção imediata;
- colaborador que requer maior experiência; e
- colaborador com substituto já preparado.

O desempenho da cada colaborador é avaliado com base na seguinte gradação:

- excepcional;
- satisfatório;
- regular; e

- fraco.

Para este modelo é necessário o programa de preparação e desenvolvimento de pessoas e funciona como plano de carreira.

O modelo baseado no fluxo de pessoal é um modelo quantitativo. Ele mapeia o fluxo de pessoas para dentro, através e para fora da empresa e leva em consideração o histórico de entradas, saídas, promoções e transferências. Este histórico permite uma predição de curto prazo. É um modelo adaptável para empresas estáveis e sem plano de expansão.

O último modelo, planejamento integrado, leva em conta quatro fatores:

- volume de produção planejado pela empresa;
- mudanças tecnológicas que alterem a produtividade das pessoas;
- condições de oferta e procura no mercado; e
- comportamento do cliente e planejamento de carreira.

PREVENÇÃO DE PERDAS E AS ORGANIZAÇÕES

Dr. Sérgio Caldas CRA, MBA, MBR, CPSI, CIEIE, CIEAC, CIGR, DIDS, MSDIS, DICS | Doctor en Ciencias de la Seguridad (España) | Gestão Empresarial e Corporativa | Prevenção e Controle de Perdas | Riscos Corporativos
Prof. Dr. Nino Meireles, CPSI, CIGR, CIEIE, CIEAC, CISI, DIDS | Doctor en Ciencias de la Seguridad (España); Diretor de Formação e Extensão Universitária da CEAS-BRASIL e Coordenador e professor do MBA em Gestão Estratégica da Segurança Corporativa da Faculdade FACEI.

Neste artigo, iremos trabalhar os conceitos básicos sobre as organizações, desempenho, eficiência, produtividade, eficácia, competitividade, processo decisório, diagnóstico, identificação dos problemas e/ou oportunidades, diagrama de causa e efeito, além de princípio de Pareto.

> "É muito importante a compreensão destes conceitos, pois estamos buscando entender como as perdas ocorrem nas empresas."

A nossa sociedade é feita de organizações que fornecem os meios para que as pessoas possam satisfazer as suas necessidades. Salários, abonos, lucros distribuídos e outras formas de remuneração são fornecidos às pessoas, em retribuição por seu trabalho ou seu investimento.

Uma organização é um sistema de recursos que procura realizar algum tipo de objetivo. Além dos objetivos e dos recursos, existem mais dois componentes importantes:

- processos; e
- divisão do trabalho.

As organizações estão por toda parte, tais como:

- faculdade;
- universidade;
- prefeitura;
- supermercado etc.

Elas existem com a finalidade de fornecer alguma combinação de produtos e serviços.

Por meio dos processos, a organização transforma os recursos para produzir os resultados. Um processo é um conjunto de atividades interligadas, com começo, meio e fim, que utiliza recursos para fornecer produtos e serviços.

A divisão do trabalho é o processo que permite superar as limitações individuais por meio da especialização. Quando se juntam as tarefas especializadas, realizam-se produtos e serviços que uma pessoa não seria capaz de fazer sozinha.

DESEMPENHO

O desempenho de uma organização pode ser avaliado pela medida em que as metas são alcançadas e pela forma como os recursos são utilizados.

Eficiência e eficácia são dois conceitos usados para fazer a avaliação do desempenho. Uma organização é eficaz quando alcança suas metas e eficiente quando utiliza corretamente seus recursos. De uma maneira geral, a eficiência é determinante da eficácia, pois se houver recursos disponíveis, utilizados corretamente, a probabilidade de atingir as metas aumenta.

Algumas organizações, além de eficientes e eficazes, precisam ser competitivas, porque enfrentam outras organizações que perseguem os mesmos objetivos.

> "O desempenho de uma organização reflete o desempenho de seus gestores."

EFICIÊNCIA

Depende de como os recursos são utilizados. Eficiência significa: realizar atividades de maneira certa, realizar tarefas de maneira inteligente (mínimo de esforço e melhor aproveitamento) e realizar tarefas de maneira econômica.

O princípio da eficiência é da relação entre esforço e resultado. Quanto menor o esforço necessário para produzir um resultado, mais eficiente é o processo. O contrário da eficiência é o desperdício.

Eliminar desperdícios significa reduzir ao mínimo a atividade que não agrega valor ao produto e/ou serviço, ou seja, perdas.

Depois de eliminados ou reduzidos os desperdícios, o que resta é atividade que agrega valor ao produto. Agregar valor significa realizar operações estritamente relacionadas com a elaboração do produto e/ou serviço. Um produto e/ou serviço sem desperdícios tem o máximo possível de valor agregado ao cliente.

PRODUTIVIDADE

O critério mais simples para avaliar uma organização é a produtividade. Segundo Maximiano (2004), produtividade é a relação entre os recursos utilizados e os resultados obtidos.

A produtividade tem diversas variações:

- Entre dois sistemas que utilizam a mesma quantidade de recursos, é mais produtivo aquele que produz maior quantidade de resultados.
- Entre dois sistemas que produzem a mesma quantidade de resultados, é mais produtivo aquele que o faz com menor quantidade de recursos.

A produtividade pode ser calculada para fatores de produção isolados. Poderíamos citar como exemplos:

- alunos por professor;
- vendas por metro quadrado; e
- produção por quilowatt/hora.

A produtividade também pode ser calculada para diversos fatores simultaneamente.

Quando se consideram produtividade e qualidade ao mesmo tempo, mede-se o desempenho não apenas da quantidade total produzida em relação aos recursos utilizados, mas também dos produtos que são aproveitados em relação ao total fornecido.

EFICÁCIA

É o conceito de desempenho que envolve a comparação entre objetivos (desempenho esperado) e resultados (desempenho realizado). Eficácia significa o grau de realização dos objetivos finais da organização:

- satisfação dos clientes;
- satisfação dos acionistas;

- impacto na sociedade; e
- aprendizagem organizacional.

COMPETITIVIDADE

É a tradução particular da ideia de eficácia, que se aplica particularmente a empresas. As empresas têm natureza competitiva. A mais competitiva é aquela que consegue transformar grande número de pessoas em seus clientes, obter lucro e sobreviver com isso.

Para ser competitiva a empresa precisa ter desempenho melhor que outras que disputam os mesmos clientes, ou seja, tem que ter vantagem sobre seus concorrentes.

As vantagens competitivas estão embutidas nos indicadores de eficiência e eficácia. Uma organização eficiente e eficaz tem alta probabilidade de ser competitiva. Existem outras vantagens competitivas: qualidade do produto e/ou serviço, domínio de fontes de matéria-prima e domínio de tecnologia.

PROCESSO DECISÓRIO

Uma decisão é uma escolha entre alternativas. As decisões são tomadas para resolver problemas ou aproveitar oportunidades. O processo decisório é a sequência de etapas que vai da identificação de uma situação que oferece ameaça ou oportunidade, até a escolha e colocação em prática de uma ação. Quando a decisão é colocada em prática, o ciclo se fecha. Uma decisão que se coloca em prática cria uma situação nova, que pode gerar outras decisões ou processos de resolver problemas.

De acordo com Simom, as decisões nas empresas dividem-se em duas categorias: programadas e não programadas. As programadas fazem parte do acervo de decisões da organização. Resolvem problemas que já foram enfrentados antes e que se comportam sempre da mesma maneira.

As não programadas são preparadas uma a uma, para fazer frente a problemas que as soluções padronizadas não conseguem resolver. Situações desta natureza precisam de um processo de análises sucessivas, desde o entendimento das causas geradoras do problema até a tomada de uma decisão.

De acordo com Maximiano (2004), o processo de tomada de decisão tem cinco fases:

- identificação do problema ou oportunidade,
- diagnóstico;

- geração de alternativas;
- escolha de uma alternativa; e
- avaliação da decisão.

IDENTIFICAÇÃO DO PROBLEMA OU OPORTUNIDADE

Nesta fase percebe-se que o problema está ocorrendo e que é necessário tomar uma decisão.

DIAGNÓSTICO

Consiste em procurar entender a ameaça ou oportunidade e identificar suas causas e consequências. Algumas técnicas foram desenvolvidas para ajudar os gestores a analisar problemas de forma sistemática, estudando suas causas, consequências e prioridades. Dentre as técnicas existentes, destacamos duas:

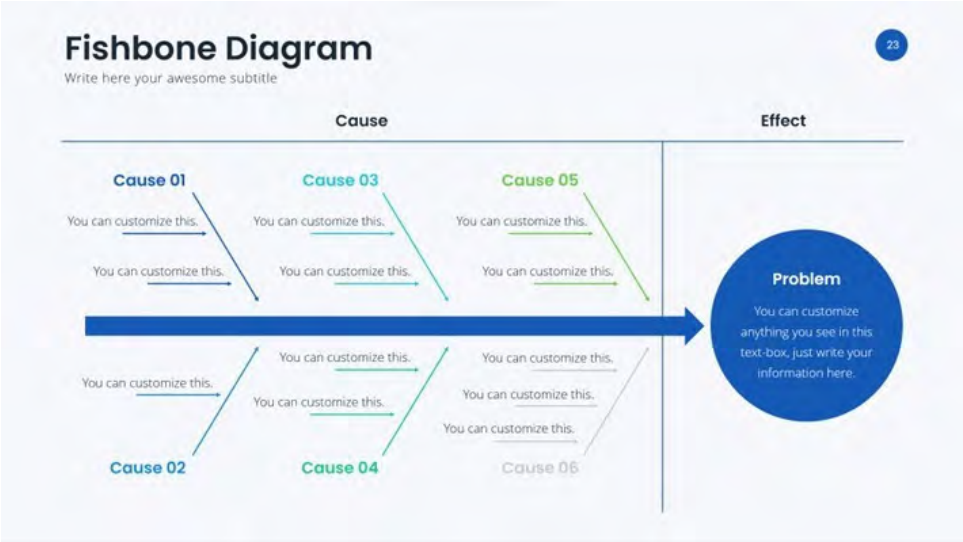
- diagrama de causa e efeito; e
- princípio de Pareto.

Diagrama de causa e efeito

Este diagrama, que também tem o nome do seu criador (Ishikawa), tem a forma de uma espinha de peixe. É um gráfico que tem por finalidade organizar o raciocínio e a discussão sobre as causas de um problema.

Para identificar as causas, três caminhos devem ser seguidos:

- levantamentos no local da ocorrência;
- análise de documentos; e
- entrevista com pessoas.



Modelo de Diagrama de Causa e Efeito Ishikawa

RISCO OPERACIONAL: O QUE É, QUAIS SÃO, CLASSIFICAÇÃO, TIPOS

José Sérgio Marcondes – CES | Especialista em Segurança Empresarial. Consultor em Segurança Privada. Diretor do IBRASEP

O Risco operacional pode representar uma ameaça significativa para a saúde financeira e a reputação de uma organização. Afinal, qualquer problema que afete as operações ou capacidade de uma empresa de realizar suas atividades com eficiência pode ter efeitos negativos na qualidade do produto ou serviço oferecido, além de impactar a confiança dos clientes e investidores.

Ignorar o risco operacional pode ter consequências significativas para as operações de uma empresa, sua reputação e seus resultados financeiros. Por isso, é fundamental que as empresas estejam cientes dos riscos operacionais que enfrentam e tomem medidas proativas para gerenciá-los adequadamente.

Neste artigo, você encontrará a definição e os conceito relacionados ao risco operacional, incluindo o que é, quais são os diferentes tipos de riscos operacionais. Além disso, abordarei as melhores práticas de gerenciamento de riscos operacionais e as estratégias que você pode adotar para mitigá-los. Espero que este artigo forneça insights valiosos para você melhorar sua capacidade de avaliar e gerenciar adequadamente os riscos operacionais.

O que é Risco Operacional?

O risco operacional é um tipo de risco associado às falhas nos processos, sistemas, pessoas ou eventos externos que podem afetar negativamente uma organização. Em outras palavras, é o risco de perda decorrente de falhas em processos internos, pessoas

ou sistemas, ou de eventos externos que fogem ao controle da organização.

Essas falhas operacionais podem ser causadas por diversos fatores, como erros humanos, problemas de tecnologia, eventos naturais, mudanças regulatórias, entre outros. As perdas decorrentes do risco operacional podem ser financeiras ou não financeiras, incluindo, por exemplo, multas regulatórias, danos à reputação, interrupções nos negócios, entre outros.

O risco operacional é aquele que afeta as operações de uma organização. Ele se refere ao risco de perda resultante de falhas ou inadequações em processos internos, pessoas, sistemas ou eventos externos, incluindo riscos legais e de conformidade.

Os riscos operacionais podem impactar negativamente as operações de uma organização, bem como sua reputação, levando a perdas financeiras, litígios, multas regulatórias e outros danos. Portanto, é essencial que as organizações identifiquem e gerenciem adequadamente o risco operacional para garantir a continuidade dos negócios e a proteção dos interesses dos stakeholders.

Definições e conceitos relacionados ao Risco Operacional

O risco operacional é inerente à execução dos processos e negócios de qualquer empresa. Segundo Jorion (2003), o risco operacional é talvez a forma mais nociva de risco, pois ele é indiretamente responsável por numerosas falhas nas instituições.

Jorion (1997) considera que os riscos operacionais “referem-se às perdas potenciais resultantes de sistemas inadequados, má administração, controles defeituosos ou falha humana […] também inclui fraude […] e risco tecnológico.”

O Comitê da Basiléia (The new Basel capital accord, 2001), similarmente ao conceito de Jorion, definiu risco operacional como “o risco de perda direta ou indireta, resultante de inadequações ou falhas de processos internos, pessoas e sistemas, ou de eventos externos.”

Segundo Deloach (2001), o risco operacional é “o risco de que as operações sejam ineficientes e ineficazes para executar o modelo de negócios da empresa, satisfazer seus clientes e atender os objetivos da empresa em termos de qualidade, custo e desempenho temporal.”

A Resolução 4.557 do Banco Central conceitua risco operacional como sendo a possibilidade de perdas resultantes de eventos externos ou de falha, deficiência ou inadequação de Processos Internos, Pessoas ou Sistemas. Esta definição inclui a possibilidade de perdas decorrentes do risco legal.

Quais são os riscos operacionais?

Os riscos operacionais são aqueles que podem surgir de falhas ou inadequações nos processos, sistemas internos, pessoas ou eventos externos, que podem levar a perdas financeiras, danos à reputação da empresa, ou impactos na continuidade das operações. Exemplos: erros de processos, falhas em controles internos, problemas com tecnologia, danos ao meio ambiente, à saúde e à segurança.

Como o Risco Operacional pode ser classificado?

Os riscos operacionais podem ser classificados /categorizados em várias subcategorias, incluindo riscos de processos, riscos de pessoas, riscos de sistemas e riscos externos.

Riscos de processos: referem-se a riscos relacionados a processos de negócios da empresa. Eles podem incluir falhas em processos de fabricação, erros em sistemas de gerenciamento de inventário, erros de produção, problemas de qualidade do produto e problemas de gerenciamento de projetos.

Riscos de pessoas: referem-se a riscos relacionados a funcionários, clientes ou terceiros envolvidos nas atividades da empresa. Eles podem incluir comportamento inadequado de funcionários, falta de treinamento, negligência ou erro humano.

Riscos de sistemas: referem-se a riscos relacionados a sistemas de informação e tecnologia da empresa. Eles podem incluir falhas de segurança cibernética, falhas de sistemas de pagamento, problemas de rede e problemas de software.

Riscos externos: referem-se a riscos relacionados a fatores externos à empresa, incluindo condições macroeconômicas, mudanças regulatórias e riscos de mercado. Eles podem incluir mudanças nas taxas de juros, flutuações cambiais, desastres naturais e crises políticas.

O que são Eventos de Risco Operacional?

Eventos de risco operacional são acontecimentos decorrentes de falhas ou inadequações de pessoas, processos, sistemas e eventos externos e podem provocar impactos indesejáveis no resultado da organização, seja por meio de despesas incorridas ou pela diminuição de receita. Entre os eventos de risco operacional, incluem-se:

- Fraudes internas;
- Fraudes externas;
- Demandas trabalhistas e segurança deficiente do local de trabalho;

- Práticas inadequadas relativas a clientes, produtos e serviços;
- Danos a ativos físicos próprios ou em uso pela instituição;
- Eventos que acarretem na interrupção das atividades da instituição;
- Falhas em sistemas de tecnologia da informação;
- Falhas na execução, cumprimento de prazos e gerenciamento das atividades da instituição.

O que são Fatores de Risco Operacional?

Os Fatores de Risco Operacional são características, condições ou eventos que aumentam a probabilidade de ocorrência de um determinado risco operacional. Eles podem ser agrupados em quatro grandes grupos de fatores causadores do risco operacional: pessoas, sistemas, processos e eventos externos.

Fator de risco pessoas está ligado às falhas nas decisões, nos projetos, nos processos e nos controles causadas por competência, informação e habilitação física ou emocional insuficientes no trabalhador. São componentes desse fator de risco: habilidade específica (conhecimento adquirido, experiência, competência); desempenho (honestidade, comportamento ético); ambiente de trabalho (cultura organizacional, motivação).

Fator de risco sistemas está ligado à tecnologia existente na instituição. Como componentes desse fator de risco, destacam-se a estrutura tecnológica e a falha tecnológica. A estrutura tecnológica refere-se à capacidade de desempenho dos sistemas, inclusive a estrutura da rede de comunicação entre os sistemas utilizados pela instituição.

Fator de risco processos considera a ocorrência de perdas por problemas ligados aos processos internos que constituem as atividades das instituições. Os principais componentes desse fator de risco são modelagem (processos internos modelados incorretamente) e conformação com a legislação (processos internos não-conformes com a legislação atual do sistema financeiro).

Fator de risco eventos externos pode ser subdividido em três componentes principais: força maior, quando as perdas sofridas pela instituição são decorrentes, por exemplo, de enchentes, terremotos ou outros desastres naturais; ambiente externo, quando as perdas são ocasionadas por degradação no meio-ambiente, alterações no ambiente econômico, político e social; e agente externo, quando as perdas são frutos de atos praticados por agentes externos à organização, como clientes, fornecedores e concorrentes.

Qual a importante de avaliar e gerenciar adequadamente os riscos operacionais?

É importante para as empresas avaliar e gerenciar adequadamente os riscos operacionais por várias razões. Em primeiro lugar, o risco operacional pode levar a perdas financeiras significativas para a empresa, afetando sua rentabilidade e reputação. Em segundo lugar, o risco operacional pode prejudicar a eficiência e eficácia das operações de uma empresa, resultando em atrasos, erros e retrabalho desnecessário. Além disso, o risco operacional pode ter um impacto negativo nas relações com clientes e stakeholders, pois a falta de conformidade com leis e regulamentos pode resultar em multas, sanções e litígios.

Ao identificar e gerenciar adequadamente os riscos operacionais, as empresas podem tomar medidas proativas para mitigar esses riscos, melhorar a eficiência operacional e garantir a conformidade com leis e regulamentos.

Quais são as melhores práticas de gerenciamento de riscos operacionais?

Existem várias melhores práticas que as empresas podem adotar para gerenciar eficazmente os riscos operacionais. Aqui estão algumas delas:

Identificar, analisar e avaliar os riscos: é importante que as empresas realizem uma avaliação sistemática de seus processos, sistemas e pessoas para identificar os possíveis riscos operacionais.

Implementar controles internos: os controles internos são medidas preventivas ou corretivas que ajudam a evitar ou minimizar os riscos operacionais. As empresas devem implementar controles internos adequados, como políticas e procedimentos, para gerenciar e mitigar esses riscos.

Monitorar e revisar regularmente: as empresas devem monitorar regularmente seus processos e controles internos para garantir que eles estejam funcionando efetivamente e atualizados com as mudanças na organização e no ambiente externo. As empresas também devem revisar periodicamente seus planos de gerenciamento de riscos operacionais para garantir que eles estejam alinhados com as mudanças na estratégia e nos objetivos da empresa.

Estabelecer uma cultura de gerenciamento de riscos: é importante que as empresas estabeleçam uma cultura de gerenciamento de riscos em toda a organização. Isso pode incluir treinamento para os funcionários em todos os níveis sobre a importância do gerenciamento de riscos e a responsabilidade de todos em contribuir para a gestão de riscos operacionais.

Manter comunicação clara e transparente: as empresas devem manter uma comunicação clara e transparente com os stakeholders sobre seus riscos operacionais e como eles

estão sendo gerenciados. Isso pode incluir relatórios regulares sobre o status dos riscos operacionais, bem como discussões sobre medidas para mitigar esses riscos.

Ao adotar essas melhores práticas de gerenciamento de riscos operacionais, as empresas podem minimizar o impacto de possíveis perdas financeiras, melhorar a eficiência operacional e garantir a conformidade com leis e regulamentos, aumentando a resiliência da organização a longo prazo.

O que é gestão de Risco Operacional?

A gestão de risco operacional é o processo pelo qual uma organização identifica, avalia, monitora e gerencia os riscos associados às suas atividades operacionais. Esses riscos podem incluir falhas em processos, sistemas, pessoas ou cultura organizacional, eventos imprevistos, mudanças regulatórias, desastres naturais e outros fatores que possam afetar adversamente as atividades da organização.

A gestão de risco operacional tem como objetivo garantir que a organização tenha processos adequados para identificar e avaliar os riscos, bem como implementar medidas para mitigá-los ou transferi-los. Isso ajuda a organização a proteger sua reputação, sua estabilidade financeira e a manter a continuidade das operações.

A gestão de risco operacional geralmente envolve a implementação de políticas e procedimentos para gerenciar os riscos, o estabelecimento de controles internos, a análise de dados para identificar padrões e tendências de risco e a realização de auditorias e testes de estresse para avaliar a eficácia das medidas de gestão de risco. Além disso, é importante que haja uma cultura de gestão de risco dentro da organização, com uma conscientização geral sobre a importância da identificação e gestão dos riscos operacionais.

Quais são as estratégias que podem ser usadas para mitigar os riscos operacionais?

Existem várias estratégias que as empresas podem adotar para mitigar os riscos operacionais, incluindo:

Diversificação: As empresas podem diversificar suas operações em diferentes áreas geográficas, setores ou linhas de produtos para reduzir a exposição a um único risco operacional.

Automação: A automação de processos pode reduzir a chance de erros humanos e aumentar a eficiência operacional.

Terceirização: A terceirização de processos para empresas especializadas pode transferir parte do risco operacional para essas empresas. No entanto, a empresa deve garantir que a terceirização seja realizada com empresas confiáveis e que haja uma estratégia

de monitoramento adequada.

Treinamento: O treinamento adequado dos funcionários em relação aos processos e controles internos pode reduzir a chance de erros e aumentar a efetividade dos controles internos.

Monitoramento contínuo: As empresas devem monitorar continuamente seus processos e controles internos para garantir que estejam funcionando efetivamente e identificar possíveis problemas antes que se tornem grandes riscos operacionais.

Políticas e procedimentos claros: As empresas devem estabelecer políticas e procedimentos claros para guiar as operações e minimizar a possibilidade de erros e falhas.

Análise de causa raiz: As empresas devem conduzir análises de causa raiz sempre que ocorrer um incidente operacional para entender as causas principais e implementar medidas preventivas para evitar incidentes semelhantes no futuro.

Ao adotar essas estratégias, as empresas podem mitigar os riscos operacionais e reduzir a probabilidade de perdas financeiras e reputacionais.

Exemplos de Riscos Operacionais

Falhas no processamento de transações financeiras, como erros de entrada de dados, que podem resultar em perdas financeiras para a empresa e seus clientes.

Interrupções na infraestrutura de tecnologia, como falhas no servidor ou na rede, que podem resultar em tempo de inatividade do sistema, perda de dados e impactar negativamente as operações comerciais.

Roubo interno, como fraude de funcionários, que pode levar á perda financeira, danos à reputação e perda de confiança dos clientes.

Incapacidade de cumprir regulamentações governamentais ou padrões de segurança, que podem resultar em multas e penalidades, bem como danos à reputação da empresa.

Desastres naturais, como terremotos ou inundações, que podem danificar as instalações físicas da empresa, interromper as operações comerciais e levar a perda financeira.

Conclusão

O gerenciamento eficaz de riscos operacionais é crucial para a saúde financeira e a reputação de uma empresa. As empresas que implementam práticas sólidas de gerenciamento de riscos operacionais são mais capazes de identificar e mitigar os riscos potenciais que enfrentam, minimizando a probabilidade de perdas financeiras e de reputação.

Neste artigo, abordei o conceito de risco operacional, os diferentes tipos de riscos operacionais e as melhores práticas de gerenciamento de riscos operacionais. Assim como, estratégias eficazes para mitigar esses riscos e insights valiosos para ajudá-lo a gerenciar melhor os riscos operacionais.

Espero que este artigo tenha sido informativo e útil para você. Se você deseja saber mais sobre gestão de riscos, recomendo a leitura do artigo “Avaliação de Riscos: O que é, para que serve, Tipos e Métodos ”, que aborda definições, conceitos e práticas eficazes para avaliação de riscos.

SEGURANÇA CIBERNÉTICA ZERO TRUST E O DESAFIO DA IMPLEMENTAÇÃO NA ORGANIZAÇÃO

Mariana da Silveira, DIDS, MBCR, CPSI, CEGRC, CIGR, CISI, CIEIE, DPO, ISO | Divisão Cibernética da Brasiliano INTERISK

A Segurança Cibernética Zero Trust é uma filosofia baseada na premissa de que nenhuma parte do ambiente de rede deve merecer confiança total até que seja devidamente verificada. Significa que a autenticação e os controles de acesso são fundamentais para proteger sistemas e informações críticas. Esta abordagem deve ser aplicada desde a infraestrutura até as aplicações e usuários, para garantir que apenas aqueles autorizados possam acessar os recursos.

Além disso, a Zero Trust visa fornecer proteção de ponta a ponta de todas as conexões de rede e atividades, proporcionando acompanhamento contínuo para detectar atividade suspeita e bloquear qualquer acesso não autorizado. A proteção proativa permite a análise de comportamento contínua, o monitoramento e a avaliação das atividades dos atores de rede e o envio de alertas de segurança ao detectar qualquer situação suspeita.

O monitoramento de equipamentos de rede de forma proativa é uma prática de segurança que envolve a monitorização contínua para detectar padrões de comportamento anômalos ou outras formas de atividade maliciosa. Esta prática ajuda a identificar possíveis ameaças, que possam explorar as vulnerabilidades do ambiente, antes que causem danos, contribuindo assim, para a manutenção da segurança cibernética.

Medidas de segurança proativas exigem a realização de monitoramento on-line, em tempo real, para a identificação e a detecção de ameaças e intrusões, por intermédio

de soluções de antivírus, antimalwares, backups periódicos, auditorias regulares, incorporação de melhoria contínua e de lições aprendidas. Tais medidas devem ser suficientes para contribuir com a proteção do ambiente cibernético.

Tecnologias robustas de autenticação e controle de acesso são ferramentas que podem ser usadas para autenticar e controlar os usuários e dispositivos na rede. Estas ferramentas incluem, mas não se limitam, a firewall, antivírus, autenticação multifator, lógica de negócios, configurações de política de acesso, controle de acesso de escopo de rede, criptografia, licenças, atualização de patches.

As ameaças cibernéticas são qualquer tipo de ameaça que se manifeste no âmbito da segurança cibernética. Tais ameaças podem incluir vírus, phishing, backdoor, malware, interceptação de dados e ataques de negação de serviços. Seus resultados podem causar danos à confidencialidade, integralidade e disponibilidade das informações. A adoção de medidas técnicas adequadas e proativas contribui para a prevenção de tais ameaças.

Os incidentes cibernéticos podem ser causados por uma variedade de fatores, incluindo descobertas de vulnerabilidades de software exploradas por crackers, falhas na segurança computacional, controles de acesso inapropriados ou inexistentes e configuração de senhas fracas. Além disso, uso inadequado da tecnologia, comportamento e negligência dos usuários podem contribuir para a ocorrência de tais incidentes.

Para a abordagem de Confiança Zero, todo usuário, dispositivo ou serviço de rede são considerados não confiáveis, por padrão. O conceito aplica-se a todos os elementos relevantes em uma infraestrutura de rede, exigindo, portanto, soluções de autenticação fortes, autorizações granulares e segurança multicamada para a proteção das ameaças cibernéticas. Assim, ainda que a ameaça se concretize, seu impacto deverá ser isolado, controlado e mitigado.

Dos padrões e normas mais utilizados para o fornecimento das diretrizes de implementações práticas de segurança que podem auxiliar no estabelecimento de um ambiente Zero Trust, citamos a ISO 27001, a ISO 27032 e o NIST. Eles fornecem uma abordagem segura para a implementação de técnicas e gestão da segurança cibernética, com requisitos específicos para os processos que suportam a segurança no ambiente cibernético.

Independentemente da estrutura utilizada, ponto importante é verificar se os arcabouços técnico, organizacional e físico, de segurança cibernética, estão voltados para identificar, proteger, detectar, responder e recuperar, no contexto da exploração de vulnerabilidades, por parte das ameaças presentes no espaço cibernético. Nesse sentido, essas funções precisam abranger, necessariamente, os quesitos a seguir.

Estrutura da gestão e de serviços de segurança da informação e seus controles, controle de acesso e responsabilidades, controle de rede, gestão de aplicações e softwares, segurança no uso dos sistemas, gestão de dispositivos móveis, segurança em estações

de trabalho e servidores, gestão de identidade e acesso, gestão de contingência, segmentação de rede, monitoramento e análise de risco da segurança da informação.

Para alcançar o Zero Trust, são necessárias as ações de segurança discutidas ao longo do texto, cujos resultados perpassam pela tentativa de evitar a visibilidade de sistemas e de aplicativos na internet, e assim minimizar ações de ataque; melhorar a experiência de navegação do usuário na rede, concedendo acesso seguro, rápido, ininterrupto e remoto a SaaS; segmentação da rede corporativa, oferecendo segurança cibernética, dentre inúmeras outras vantagens.

O desafio da implementação da Confiança Zero, nos procedimentos de segurança da informação, pertinentes ao ambiente cibernético, consiste em realizar investimentos de recursos em medidas técnicas, físicas e organizacionais. Dentre elas, a cultura organizacional em segurança cibernética, o investimento financeiro em tecnologias, a capacitação de usuários e, principalmente, a liderança e o comprometimento da Alta Direção.

O caminho a ser percorrido não é fácil, tampouco é rápido, contudo, a organização precisa tomar imediatamente a iniciativa de sua caminhada rumo à Confiança Zero. Começar pelo começo pode ser considerado pleonasmo, mas, neste aspecto, é a melhor forma de agir. A organização deve tomar ações logicamente estruturadas, ao esbarrar nos percalços, a serem superados, precisa vencer a dificuldade e seguir com consistência para os próximos obstáculos.

Dessarte, a organização guiada por um framework direcionado, que ofereça a estrutura concatenada para o estabelecimento do sistema de gestão de segurança cibernética, poderá conquistar um ambiente Zero Trust, por intermédio de medidas técnicas, organizacionais e físicas, conquistando assim a maturidade em segurança cibernética, com solidez e perspicácia, num processo de melhoria contínua e de lições aprendidas incorporadas.

A forma mais segura de alcançar a maturidade necessária para que as ameaças não explorem as vulnerabilidades, é unindo tecnologia e conceito. Com a Divisão de Segurança Cibernética da Brasiliano INTERISK, você consegue mesurar sua maturidade com o objetivo desenvolver sua organização de forma constante, possibilitando também análises dos resultados e melhores decisões através de agrupamentos e filtros de informações.

SEGURANÇA E RESILIÊNCIA – SISTEMAS DE GESTÃO DE CONTINUIDADE DE NEGÓCIOS - ISO 22301

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

A Norma ABNT NBR ISO 22301:2020 define os aspectos necessários para que um sistema de gestão previna e proteja empresas diante de contingências como desastres naturais e situações que possam causar a interrupção de seus processos e negócios.

Esta norma traz as especificações, a estrutura e os requisitos para que seja implementado e mantido um sistema de gestão de continuidade de negócios (SGCN) que tem por objetivo manter uma operação após um evento disruptivo, independentemente de este ser decorrente de falha de segurança digital, de desastre ou de qualquer outro motivo.

Entre os vários benefícios dessa certificação, está o diferencial competitivo. Comparando com concorrentes sem essa chancela, uma empresa credenciada pela ISO 22301 terá melhor visibilidade no mercado – principalmente quando se trata de clientes sensíveis à manutenção da continuidade de suas operações e à entrega de seus produtos e serviços.

Além disso, essa ISO pode melhorar a reputação e ajudar a conquistar novos clientes, tornando mais fácil demonstrar que determinado negócio está entre os melhores do setor. Afinal, o negócio dispõe de uma documentação que comprova isso.

Os resultados de um SGCN devem ser modulados por requisitos legais, regulatórios, organizacionais e operacionais da organização e de suas partes interessadas e, para ser eficaz deve-se entender quais são as necessidades da organização e a imprescindibilidade do estabelecimento de uma política e de objetivos para a continuidade de negócios.

É preciso que os processos sejam operados e mantidos, incorporando capacidades e estruturas de pronta resposta para que a organização sobreviva a eventos disruptivos.

O SGCN deve ser monitorado e seu desempenho avaliado de forma crítica para que seja eficaz. Além disso deve ser melhorado continuamente com base em medições qualitativas e quantitativas.

A implementação de um SGCN não é uma tarefa fácil. São várias etapas que devem ser cumpridas, de forma obrigatória, conforme determinado pela Norma ABNT NBR ISO 22301:2020. Dentre elas, temos:

1) Apoio dos gestores - para iniciar qualquer tipo de projeto dessa magnitude, os gestores da empresa precisam estar dispostos a investir em recursos humanos, financeiros e tecnológicos.

2) Identificação dos requisitos – inicialmente, é preciso ter certeza de que essa ação está em conformidade com tudo o que as partes interessadas desejam. Não são apenas as leis e regulamentos, mas também os requisitos nos acordos já firmados com os clientes e os desejos dos proprietários da empresa, dentre outros.

3) Política e objetivos de continuidade de negócios - é preciso implantar uma política de continuidade de negócios e os diretores precisam determinar exatamente o que se espera dessa continuidade, definindo metas objetivas.

4) Avaliação e tratamento de risco - é preciso descobrir quais problemas podem ocorrer com mais frequência e definir os controles que podem ser aplicados para mitigá-los.

5) Análise de impacto nos negócios - o objetivo da análise de impacto nos negócios é definir o tempo disponível para a recuperação e os recursos necessários para isso.

6) Estratégia de continuidade de negócios – definir meios para conseguir o que foi listado nas etapas anteriores com um nível mínimo de investimento,

evitando gastos desnecessários que podem fazer a diferença nos estágios seguintes.

7) Plano de continuidade de negócios - planos de resposta inicial a incidentes e planos de recuperação que detalhem o que precisa ser feito para iniciar as atividades.

8) Treinamento e conscientização - é preciso capacitar os colaboradores sobre como executar determinadas etapas do plano, enfatizando a razão pela qual tudo isso é tão importante.

9) Manutenção da documentação – toda estratégia precisa estar refletida em documentos.

10) Exercício e teste – é preciso criar situações nas quais se possa testar os planos no modo mais realista possível. Quem não puser os planos à prova para descobrir como eles se comportam em situações reais nunca descobrirá os pontos que precisam ser aperfeiçoados.

11) Comunicação com as partes interessadas - a continuidade dos negócios pode depender também de órgãos reguladores, autoridades, proprietários, empregados e fornecedores.

12) Medição e avaliação – é preciso saber se as metas estão sendo atingidas. Os objetivos definidos na etapa 3 têm que ser verificados para entendermos se estão sendo atingidos de acordo com algum tipo de métrica.

15) Auditoria interna - outras pessoas da empresa devem revisar o projeto e sugerir melhorias – é essa a função da auditoria interna. Embora muitas vezes seja considerada uma sobrecarga, uma auditoria interna é realmente muito útil quando se trata de enfrentar a realidade e integrar equipes.

16) Ações corretivas – a Norma ABNT NBR ISO 22301 traz melhorias diárias que acabam sendo conduzidas sistematicamente. É o que conduz uma empresa a descobrir por que determinado problema aconteceu, garantindo que nunca aconteça novamente. O próprio texto da ISO fala sobre “garantir que as não conformidades não se repitam”. É algo que precisa ser feito de forma sistemática e transparente.

17) Revisão - concluídas todas as etapas, a alta administração precisa avaliá-las e tomar algumas decisões cruciais – como atualizar os objetivos, liberar verbas, fazer melhorias adicionais, entre outros. Afinal, é deles a responsabilidade final sobre a capacidade que a empresa tem de sobreviver a incidentes maiores.

O Software INTERISK possui o Módulo de Gestão de Continuidade de Negócios – GCN que auxilia a sua organização na elaboração e automação de um processo que garante

a continuidade do seu negócio, mediante a uma eventual paralização.

SEGURANÇA. PENSE GLOBALMENTE, AJA LOCALMENTE

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

A segurança é uma necessidade básica de todos os cidadãos e um bem coletivo exigido e reconhecido. Por esta razão, a sua melhoria e manutenção ocupa um lugar de destaque na escala de valores e objetivos da população.

Mas, segurança também é um direito, mantê-la tem um custo e, para alcançá-la, temos que abrir mão de uma parte de nossa liberdade e assumir um conjunto de regras, deveres e restrições em nossas atividades diárias.

Combater a insegurança é tarefa do Estado e das Forças e Corpos de Segurança. No entanto, perante os novos e crescentes desafios dos atos antissociais (tráfico de drogas, crime organizado, branqueamento de capitais, terrorismo internacional, vandalismo etc.), as instituições estatais nem sempre têm capacidade para responder adequadamente a estes riscos e ameaças, sendo cada vez mais limitados quando se trata de desenhar estratégias eficazes.

Todos estes aspectos são ingredientes que alimentam a insegurança cidadã, tanto percebida como real, contra a qual os políticos devem buscar respostas eficazes, procurando oferecer o bem-estar mais estável possível, nos aspectos econômico, político e social, começando por dar prioridade à atenção local áreas.

Por isso, agora que em Espanha entramos no período de eleições autárquicas e gerais, um programa de modernização e reinvenção da segurança só pode ser assente e planeado a pensar no global para atuar eficazmente localmente.

Pense globalmente e aja localmente. Conceitos

Em geral, e nas instituições públicas em particular, existe uma natural fricção entre a mentalidade global e a mentalidade local, que é seu dever resolver.

A segurança (e muitos outros conceitos) deve ser transmitida do pensamento global para o local, ou seja, do nível europeu, do país, da comunidade, da cidade e do bairro.

Pensar globalmente e agir localmente deve ser um acordo político e social inteligente diante dos problemas de insegurança e emergência que põe em movimento e otimiza o uso dos valores e recursos disponíveis.

Bases de trabalho

Estruturas locais de segurança:

A Constituição Espanhola, no seu artigo 148.1.22, atribui às Comunidades Autónomas competência em matéria de coordenação e outras competências em relação à Polícia Local e serviços de emergência.

A Lei Orgânica 2/1986, das Forças e Órgãos de Segurança (LOFCS) regula esta vertente estabelecendo, no seu artigo 39.º, que compete às Comunidades Autónomas, coordenar a atuação da Polícia Local no âmbito territorial da Comunidade, através o exercício das seguintes funções:

- Estabelecimento de normas-quadro às quais deve obedecer o Regulamento da Polícia Local.
- Estabelecer ou promover, conforme o caso, a homogeneização das diferentes Forças Policiais Locais, em termos de meios técnicos para aumentar a sua eficiência e colaboração, uniformes e remunerações.
- Definir os critérios de seleção, formação, promoção e mobilidade da Polícia Local, determinando os diferentes níveis de escolaridade exigidos para cada categoria, sem que em nenhum caso o nível seja inferior a Licenciatura Escolar.
- Coordenar a formação profissional da Polícia Local através da criação de Escolas de Formação de Comando e Formação Básica.

As políticas nacionais nas áreas tradicionais da segurança já não são suficientes para a salvaguardar no século XXI. Só uma abordagem abrangente, que conceba a segurança de forma ampla e interdisciplinar, a nível nacional, europeu e internacional, pode responder aos complexos desafios que enfrentamos.

A Estratégia Espanhola de Segurança (EES) baseia a política de segurança em uma série de conceitos básicos, tais como: abordagem integral das várias dimensões da segurança, coordenação entre as administrações públicas e com a sociedade, eficiência

no uso de recursos e antecipação e prevenção de ameaças e riscos.

Espera-se que o desenvolvimento de uma progressiva reorganização do Sistema de Segurança Nacional, com base nas estruturas e organismos que têm vindo a desempenhar funções de segurança, viabilize, através das devidas modificações legislativas, a tão referida integração de todos os intervenientes públicos e privados da segurança, favorecendo que a sua gestão seja, como tantas vezes se tem proclamado, mais ágil e eficiente.

Ao mesmo tempo, nas Estratégias elaboradas até o momento, falta uma alusão mais clara e dinâmica ao mundo local, às suas estruturas, partícipes da segurança justamente no ambiente mais diretamente percebido pela sociedade.

Evolução e desenvolvimento

O objetivo é propor a cultura de segurança como um bem público, promovendo a evolução e o desenvolvimento de um paradigma de segurança compartilhada, que abrange do global ao local. As principais organizações voltadas para a análise do conceito de segurança deixaram claro seu caráter evolutivo e a necessidade de adequá-lo às transformações ocorridas com a crescente globalização.

A necessária integração, definida nas sucessivas Estratégias de Segurança adoptadas a nível internacional e nacional, exige que se tenha em consideração a perspectiva local, tornando-a participante dos objetivos traçados aos diferentes níveis e estratégias. Neste sentido, recorde-se que em Espanha, mais de 85% da população reside em 16% dos municípios, que representam aqueles com um censo superior a 5.000 habitantes e que o grupo de polícias locais, estimado entre 70.000 e 80.000 efetivos, estão distribuídos, justamente, nesses mesmos municípios.

Entre as propostas indicadas relativamente aos processos de melhoria e adaptação da Polícia ao atual contexto global, destacam-se as seguintes:

- Fomentar a criação de uma consciência coletiva identitária em matéria de segurança, reforçando os órgãos de coordenação existentes e promovendo a criação de órgãos, comandos e estruturas comuns.

- Atualizar as leis policiais, de forma a regular e racionalizar a atual realidade policial.

- Desenvolver um modelo de Segurança Local, em linha com as competências assumidas, privilegiando a elevada especialização das polícias locais na segurança cidadã, desenvolvendo o modelo de policiamento comunitário e aperfeiçoando a função preventiva.

Nesta perspectiva, a segurança local tem de responder a um conjunto de áreas ou desafios que são vividos com especial intensidade em ambientes urbanos, configurando

o que se designa por

Estratégia de segurança local:

- Segurança Cidadã, tendo em conta a ideia de que a prevenção da criminalidade é uma prioridade do sistema penal, estabelecendo mecanismos de colaboração e coordenação entre as diferentes forças policiais.

- Violência de Género, com o objetivo de prevenir e detectar a violência de género, assistir e proteger as vítimas, contribuir para a reparação dos danos que lhes são causados e melhorar os mecanismos para evitar a vitimização secundária.

- Mobilidade Sustentável e Segura, contribuindo para a melhoria da mobilidade urbana de acordo com os parâmetros e compromissos estabelecidos na Carta Europeia de Segurança Rodoviária e nos Planos de Sustentabilidade (Agenda 21).

- Segurança Escolar, com o objetivo de melhorar a segurança dos escolares influenciando seu entorno imediato e contribuindo pedagogicamente para a configuração de atitudes favoráveis à segurança, tanto no trânsito quanto na convivência cidadã.

- Proteção Civil Municipal, de forma a pôr em prática os diferentes Planos Municipais de Proteção Civil e monitorizá-los e atualizá-los.

- Segurança nas Atividades, Instalações e Dependências, conhecer e fiscalizar os planos de autoproteção dos estabelecimentos obrigados a tê-los, estabelecendo as medidas de segurança adequadas quando for o caso.

- Saúde Pública, com o objetivo de prevenir e garantir a segurança e saúde das pessoas em diversos aspectos da vida cotidiana, como segurança alimentar, hídrica e ambiental; a posse de animais domésticos e exóticos; controle de pragas; as condições higiênico-sanitárias das residências e instalações etc.

- Riscos Sociais, dando cobertura a pessoas que apresentem problemas de desproteção e/ou exclusão social ou que, em consequência de uma situação de emergência, se encontrem em situação de risco passível de atendimento pelo poder público.

- Assistência Psicológica, estabelecendo os mecanismos para poder dar uma primeira resposta psicológica às vítimas e familiares em catástrofes e acidentes graves.

- Convivência e Cidadania, de forma a contribuir para a melhoria da convivência cidadã, priorizando determinados conteúdo das portarias de convivência e civilidade, que afetam diretamente o campo das relações interpessoais e a qualidade de vida dos cidadãos, bem como implementando serviços de mediação específicos para resolução de conflitos.

- Segurança Urbana, com o objetivo de contribuir para as boas práticas no domínio da construção de habitações e aglomerados populacionais, garantindo o cumprimento da regulamentação urbanística e das condições específicas dos respetivos alvarás.

- Segurança em Espaços de Especial Interesse, garantindo a segurança de determinados ambientes que pelas suas características o exijam. Assim, por exemplo, o bairro antigo das vilas e cidades, onde se situa a maior parte do património arqueológico e monumental.

Em todo o caso, tendo em conta que as abordagens devem ser global, ou seja, aplicar esquemas globais de segurança ao local, e abrangentes e integradas entre recursos de segurança pública e privada, conforme também estabelece a Lei de Segurança Cidadã e a Lei de Segurança Privada.

Por fim, para pensarmos globalmente e agirmos localmente, devemos tomar consciência da nossa própria responsabilidade de procurar aprofundar e compreender a realidade que nos rodeia e a urgência das suas ameaças, partilhando o nosso conhecimento como forma de contribuir para uma sociedade baseada na segurança e o bem comum. Para criar as condições para uma mudança sustentável, é preciso tecer redes colaborativas, e nossas relações pessoais e profissionais também podem constituir um ecossistema de transformação. Nesta linha, queremos convidar as pessoas a pensar globalmente, gerando um marco de desenvolvimento exportável que nos permita atuar localmente. Aos poucos vamos mudando o paradigma e a cultura de segurança em nossa sociedade, até conseguirmos integrar essa estrutura que facilita nosso bem-estar de forma tão silenciosa e eficiente que, como o próprio esqueleto que sustenta nosso corpo, nem se nota que se integra sob a pele que nos cobre, permitindo-nos experimentar a tranquilidade de existir em paz como sociedade e como pessoas, numa harmonia codependente e sinérgica.

ESTUDOS DE SEGURANÇA

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.

No cenário atual, podemos notar que o Estudo de Segurança é de suma importância para que possamos ter um diagnóstico eficaz para a identificação das condições de vulnerabilidade e riscos potenciais que podemos enfrentar em nossas instalações, pessoa ou processo objeto da avaliação.

Pois desta forma podemos melhor ordenar nossas fraquezas e nossas vulnerabilidades, tanto nos ambientes internos e externos em nossa área circunvizinhas, após este levantamento podemos de forma estratégica conduzir da melhor forma os recursos financeiros disponíveis e obter a melhor performance nas ações necessárias e imediatas.

No ESTUDO DE SEGURANÇA (ES) conseguimos ter uma avaliação tanto subjetiva quanto qualitativa que permite determinar o estado atual em que se encontra os recursos de segurança (humanos, físicos, eletrônicos, tecnológicos, organizativos) de uma determinada pessoa, organização, instalação ou operação. Formando assim um documento técnico produto do processo metodológico do estudo de fatores internos e externos que se relacionam com a segurança de uma instalação especifica. No

processo de execução de um Estudo de Segurança é importante avaliar a informação obtida para estabelecer o problema operativo de segurança, agrupando-os em riscos contra pessoas, valores, instalações, processos, meio ambiente e informação, com tudo isso poderemos emitir as recomendações especificas, além do mais deverá sugerir a formulação de "UMA ANALISE DE RISCOS", para aqueles casos que mereçam um exame minucioso e detalhado por sua complexidade.

O treinamento nos mostrou a Matriz de análise, determinada FODA:

- Fortalezas

- Oportunidades

- Debilidades

- Ameaças

O treinamento nos trouxe um novo método para uma análise de riscos, mostrando que não existe nenhuma matriz universal e que as instituições, empresas ou organizações possuem particularidades diferentes e que devem ser sempre consideradas nos levantamentos e diagnósticos, realizados pelo Gestor de Segurança.

O treinamento também ressaltou a importância de todo estudo ser realizado por Profissional Segurança Privada, e, que ele sempre o faça com:

1. Profissionalismo

2. Ética

3. Confidencialidade

4. Cumprimento de prazos e alcances das metas

Assim sendo podemos resumir que devemos sempre escolher o método que melhor se adequa as nossa realidade e nossas condições de assimilar os conceitos, facilitando assim nosso poder de persuasão, frente a alta direção.

Não podemos deixar de sempre utilizar equipes multidisciplinares para Estudos de Segurança, pois as visões de prismas diferentes engrandecem e deixam o projeto mais robusto e com mais efetividade nos resultados propostos.

Para o êxito no projeto ou estudo de segurança:

Devemos dividir em 4 Etapas distintas:

- Diagnóstico é um processo inicial o qual o especialista obtém uma apreciação subjetiva inicial e de forma geral das condições de segurança do objeto a proteger, o que permitirá orientar da melhor maneira o planejamento,

estabelecer um cronograma de trabalho, executar ordenadamente o trabalho de campo e a elaboração do relatório. O diagnóstico é obrigatório para elaboração do ES.

- Planejamento, precisa ser respeitado alguns passos:

  A) Definição do Método de Estudo;

  B) Cronograma de atividades;

  C) Desenvolvimento de formatos de aplicação.

- Trabalho de Campo, precisa responder a algumas perguntas básicas:

  - O quero proteger?

  - Como estão distribuídos meus recursos?

  - Contra o que quero proteger?

  - Quais são meus Meios Técnicos Ativos e Passivos, Recursos Humanos, Meios Organizacionais, o Ambiente Interno e Externo?

- A Elaboração do Informe é o documento de trabalho e consulta, como é uma ferramenta de administração dos riscos, deve ser confiável, pois é apresentada a alta direção.

Concluímos, portanto que o Estudo de Segurança – ES é indispensável e leva em consideração os recursos humanos, materiais e financeiros, dando a direção e elencando as camadas de segurança a serem priorizadas, respeitando as restrições de tempo, perda e custo, para atingir uma mudança benéfica definida por meios de objetivos. Assim sendo o ES é caracterizado pela temporalidade, objetividade, singularidade e recursos limitados.

Os objetivos de um ES consistem no que se planeja alcançar ao final do estudo. Pode ser definido como um resultado a que o trabalho ou serviço será orientado, de uma posição estratégica a ser alcançada ou um propósito a ser atingido, mitigando os riscos e as perdas financeiras de uma empresa, organização ou instituição.

COMPUTAÇÃO QUÂNTICA: UM NOVO PARADIGMA PARA A SEGURANÇA CIBERNÉTICA

Mariana da Silveira, DIDS, MBCR, CPSI, CEGRC, CIGR, CISI, CIEIE, DPO, ISO | Divisão Cibernética da Brasiliano INTERISK

Nas últimas décadas fomos apresentados a diversas novas tecnologias. Dentre elas, a mais impactante, arrisco-me a apontar, é a computação quântica. Ao menos, propõe-se a realizar a maior transformação da ciência computacional hodierna e requer maior preparação para utilizar a nova tecnologia, seja pelos desenvolvedores, prestadores de serviços ou usuários. Os computadores quânticos foram propostos na década de 1980 por Richard Feynman e Yuri Manin.

A mecânica quântica foi desenvolvida no início do século XX e, cem anos depois, continua sendo o fundamento das tecnologias atualmente utilizadas e desenvolvidas. Percebeu-se, no entanto, que a modelagem dos sistemas mais simples, nas máquinas atuais, ainda que sejam "supercomputadores", torna-se praticamente impossível utilizando a mecânica quântica.

Isso porque a matéria, em nível quântico, pode assumir um número infinito de configurações e assim realizar uma interconectividade que interfere na utilização do método de amostragem estatística para analisar um determinado conjunto de possibilidades de configurações. Assim, para compreender a evolução quântica, seria necessário identificar essas possibilidades de configurações num sistema quântico.

Esse "problema" passou a ser considerado uma oportunidade científica. Para isso, ao longo desses cem anos desde a descoberta da mecânica quântica, foram desenvolvidos computadores quânticos que codificam exponencialmente mais informações do que bits, por meio de qubits. Dessarte, os cientistas podem produzir soluções imediatas, de alta qualidade, para problemas difíceis.

A expectativa, no tocante à segurança cibernética, é que os computadores quânticos possibilitem, por exemplo, a resolução de problemas de otimização que envolvam a escolha da melhor alternativa entre uma grande variedade de opções. Serão capazes, ainda, de decifrar os algoritmos de criptografia mais sofisticados, o que é considerado atualmente como algo impossível de acontecer em tempo hábil.

O intuito da computação quântica é realizar o armazenamento de informações em configurações quânticas da matéria e usar operações do "gate quântico", circuito quântico básico, para calcular essas informações e, ao mesmo tempo, aprender a programar a interferência quântica. Em caráter experimental, os "protótipos de computadores quânticos", demonstram progresso rápido e satisfatório.

O algoritmo de Shor, desenvolvido pelo matemático Peter Shor na década de 1990, é baseado em propriedades da mecânica quântica e resolve o problema de fatoração de um número "N" em tempo polinomial, sendo capaz de quebrar toda a criptografia existente atualmente, com a utilização da criptoanálise em computadores quânticos. Em resposta, surge a criptografia pós-quantum.

A criptografia pós-quantum estuda classes de algoritmos criptográficos resistentes à criptoanálise quântica, tais como os baseados em hash. Assim, demoraria um tempo exponencial para tais algoritmos serem quebrados, ainda que em computadores quânticos. A ciência demonstra, portanto, que é possível à Segurança Cibernética manter-se na dianteira em face de novos paradigmas.

Como os responsáveis pela Segurança Cibernética devem atuar diante das ameaças iminentes apresentadas? Ressaltam-se alguns percalços no caminho dessa revolução tecnológica: os computadores quânticos ainda estão em fase de desenvolvimento, o planejamento da produção para fins comerciais ainda não é uma realidade, o desempenho prometido pelo algoritmo de Shor pode não superar algoritmos clássicos que ainda possam surgir.

É mister ressaltar os recursos que a computação quântica oferece à Segurança Cibernética. Além da criptografia pós-quantum, podemos citar a comunicação quântica, capaz de criar redes de comunicações altamente seguras que poderão formar a base da internet quântica. Por possibilitar integralidade e confidencialidade durante a transferência de dados, é considerada ultrassegura.

A tecnologia atual permite que os dados confidenciais sejam criptografados e enviados juntamente com as chaves criptográficas para decodificar as informações. Esse envio conjunto torna a transmissão de dados vulnerável, possibilitando que crackers acessem e capturem os dados em trânsito sem deixar vestígios. Já com a alteração de estado da matéria, em nível quântico, essa possibilidade deixaria o rastro de suas ações.

Ainda que sejam criadas redes de transmissão de dados, extremamente sensíveis, com base em distribuição quântica de chaves, ou QKD, em tese, altamente seguras, há problemas envolvendo a Segurança Cibernética. Isso acontece porque a realização da

transmissão com bits criptografados, em redes convencionais, permite a interceptação, a captura dos dados e a quebra da chave criptográfica. Computadores quânticos devem estar conectados em redes quânticas.

Para tanto, a transmissão de dados deverá ocorrer na forma quântica, por teletransporte quântico, por meio de emaranhamento de fótons em pares. Durante a assunção das infinitas possibilidades de configurações, somada à interconectividade realizada pelos transmissores e receptores, cada um com seu par de fótons, mudariam o estado dos pares de fótons de ambos, possibilitando a segurança necessária.

O maior desafio da rede quântica é o emprego de recursos científicos, financeiros, de inteligência humana, tecnológicos, de produção de equipamentos, de energia, de resfriamento e de escalabilidade. Assim, classificar as informações e atribuir-lhes valor é uma das primeiras ações que a organização deve realizar, pois as medidas de controle levam em consideração a relação entre o valor do ativo a ser protegido e o valor da proteção a ele proporcionada.

Dessarte, as informações críticas de negócio devem ser protegidas quanto à confidencialidade, integralidade, disponibilidade e autenticidade. As medidas técnicas de Segurança Cibernética devem ser consideradas investimento com geração de valor para a organização. Ainda que a computação quântica não seja uma realidade de mercado, a tecnologia da informação atual permite a segurança da informação proporcional às ameaças enfrentadas.

Assim, a organização deverá, na medida da tecnologia disponível, atuar para que as ameaças não explorem suas vulnerabilidades, e que estas sejam mitigadas. Seus negócios estão protegidos? Saiba como a Brasiliano INTERISK pode contribuir com a Segurança Cibernética de sua organização.

AGENDA ESG: PILARES, RISCOS E GERENCIAMENTO

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

A Agenda ESG, tão debatida em nossos dias, é composta basicamente de três pilares. A organização que se propõe a implantar essa agenda como parte de sua estratégia de negócios deve fazer com que todos os integrantes de seus quadros tenham uma visão bastante clara do que são esses pilares e de como eles se relacionam entre eles mesmos e com os diversos setores da organização.

O pilar Ambiental trata, preponderantemente do impacto que a organização provoca sobre o planeta. Esse impacto pode influenciar nas mudanças climáticas; nas emissões de gases de efeito estufa (GEE); no desmatamento; na perda de biodiversidade; na poluição da água, solo e atmosfera; na geração de resíduos e assim por diante.

O pilar Social analisa o impacto da organização sobre as pessoas. Diretamente afetados por esse impacto estão os funcionários da empresa; os clientes e a comunidade a que a organização pertence; os direitos humanos; a saúde e segurança ocupacional; a cadeia de suprimentos etc.

Já o pilar Governança Corporativa diz respeito à maneira como a organização é gerenciada. Englobadas neste pilar estão as práticas de gestão do conselho; o planejamento sucessório; a remuneração; a diversidade, a equidade e a inclusão; a conformidade legal; as medidas de prevenção e combate à corrupção e à fraude; a segurança dos dados, entre outros itens.

Nos últimos anos, tem havido um foco crescente em questões ambientais e as preocupações com a sustentabilidade vêm se se intensificando no mundo inteiro, em razão de mudanças climáticas hoje de todo evidentes e da perspectiva de escassez de recursos naturais em curto prazo. Também vêm ganhando realce os aspectos sociais

e de governança corporativa, na medida em que os investidores buscam colocar seus recursos em empresas comprometidas em impactar positivamente a sociedade.

A implementação de uma estratégia ESG pode ser uma forma de as empresas sinalizarem seu compromisso com essas questões e assim atraírem investimentos. Esses investimentos em ESG podem ajudar as organizações a reduzir seu impacto ambiental, a melhorar os resultados sociais e a construir melhores estruturas de governança.

Resulta daí a necessidade imperiosa de que a alta direção das empresas tenha plena consciência, não apenas do conceito de ESG, como também de suas diversas implicações na estratégia a ser executada, tendo em vista o forte impacto financeiro que pode resultar da observância ou não-observância desses princípios. Em outras palavras, os riscos ESG envolvidos são de grande envergadura e podem resultar tanto da inação por parte da organização em aderir aos princípios e práticas ESG quanto de ações em direção a essas práticas de forma não assentada em uma metodologia adequada.

Uma tendência que vem sendo observada nos últimos tempos, em nível global, é a entrada em vigor de uma regulamentação ambiental cada vez mais rigorosa, o que fatalmente irá sujeitar as empresas que adotam procedimentos não conformes ao risco de multas e outras penalidades, numa escalada que pode ao final tornar o negócio inviável. O mesmo acontece com relação às práticas no pilar Social, submetidas de forma progressiva ao escrutínio dos órgãos fiscalizadores e ao olhar atento da opinião pública. Práticas inadequadas nesses campos, se não forem detectadas e corrigidas de início, podem levar a empresa a enfrentar danos à reputação, o que certamente terá como consequência a perda de clientes e de receita.

Como é natural, o pilar Governança Corporativa, além de sua expressão própria, é também o condutor dos outros dois pilares, uma vez que no âmbito dele são geradas as decisões e as ações em todo o espectro de atividades da empresa. Além de tudo, práticas de governança fracas podem ensejar a ocorrência de fraudes, desvios financeiros, não conformidades jurídicas e todo o rol de riscos que a elas se associam.

A implementação de uma estratégia ESG pode ser um desafio para as empresas por vários motivos. Muitas vezes há falta de dados e de transparência sobre questões ambientais e sociais, o que carrega implícito o risco de não se estabelecerem as metas com a clareza necessária. Em segundo lugar, as iniciativas ESG podem exigir um investimento inicial significativo, o que implica muitas vezes contingenciar as despesas em outras áreas do negócio. Também por isso, a mudança radical das práticas de negócios para alinhá-las a uma estratégia ESG carrega o risco de causar desconforto para as partes interessadas, em particular entre clientes e funcionários.

Para fazer face a esses riscos, a empresa pode estabelecer parceria com ONGs ou outras organizações com experiência em questões ESG específicas. Dados de mídias sociais e de outras fontes podem ser coletados para obter informações sobre o sentimento das

partes interessadas em relação à implantação de uma Agenda ESG na empresa. Todavia, o mais importante é desenvolver gradualmente os planos de implementação, distribuindo as diversas ações em fases sucessivas e com grau crescente de complexidade. Dessa forma, minimizam-se os riscos de serem tomadas decisões não alinhadas com os interesses dos acionistas e de ser dedicada uma excessiva atenção às questões ESG, desviando a atenção dos principais objetivos do negócio.

Tendo em vista esses riscos e condicionantes, o conselho de administração deve garantir que o processo de tomada de decisão da empresa seja transparente e que os acionistas sejam mantidos a par do progresso no cumprimento das metas ESG. Relatórios periódicos atualizarão as partes interessadas sobre o andamento do processo e permitirão o seu ajuste, a partir de uma comunicação bem estruturada.

As pessoas às vezes perguntam se a Agenda ESG não é só mais um modismo, alguma coisa de que muito se fala hoje mas que daqui a alguns anos estará relegada aos livros de história. Na verdade, os benefícios de tomarem-se a sério esses princípios e colocá-los em execução, integrando-os às práticas de negócio, já são bem perceptíveis, como podemos verificar nos tópicos a seguir.

1. Relações com investidores: atualmente os investidores em geral, mas especialmente as instituições, esperam ver políticas e práticas ESG na empresa em que planejam investir, incluindo boa governança (planejamento de sucessão, independência de auditores, verificações de conformidade) e perspectivas de liderança no setor refletidas no balanço.

2. Redução de custos: os programas ESG reduzem os custos de RH, por exemplo, atraindo talentos a partir de um grupo mais amplo de funcionários em potencial e limitando despesas relacionadas à alta rotatividade de colaboradores na empresa.

3. Valorização de mercado: pesquisas vêm demonstrando que as empresas com um menor número de incidentes ESG têm superado por larga margem as concorrentes nos mercados de ações globais e que as práticas ESG podem levar a um melhor desempenho financeiro e, em consequência, a um maior valor para o acionista.

4. Acesso a novos mercados: as evidências sugerem que as empresas com forte histórico ESG têm acesso facilitado a novos mercados, como aquele representado pelos integrantes da Geração Millennials ou dos consumidores ambientalmente conscientes.

5. Gerenciamento de riscos eficaz: o gerenciamento de riscos é facilitado em empresas dotadas de boas práticas ESG. A menor exposição a demandas e interrupções na cadeia de suprimentos é um exemplo de resultado positivo trazido por essas boas práticas. Outro ponto digno de nota é a necessidade de entender que as questões ESG são questões comerciais regulares e que o gerenciamento de riscos ESG faz parte do gerenciamento de riscos padrão.

Desse modo, uma metodologia moderna e eficaz de gestão de riscos corporativos será,

sem dúvida, de grande valia para a empresa evoluir na direção da conquista de seus objetivos estratégicos. Essa metodologia trará em seu bojo um módulo específico sobre riscos ESG, tratados de forma interativa com os demais riscos, de modo a evitar as miopias da administração.

Além de atrair investimentos, a correta implementação de uma estratégia ESG também pode ajudar a melhorar a eficiência operacional, o gerenciamento de todo o portfólio de riscos e o engajamento dos funcionários.

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.

DATA LOSS PREVENTION – DLP

Mariana da Silveira, DIDS, MBCR, CPSI, CEGRC, CIGR, CISI,
CIEIE, DPO, ISO | Divisão Cibernética da Brasiliano INTERISK

A DLP é uma estratégia adotada pelas organizações para assegurar que as informações confidenciais permaneçam em segurança na rede corporativa. Para isso, um conjunto de ferramentas e processos são empregados para garantir que dados confidenciais não sejam perdidos ou acessados indevidamente. Incidentes podem gerar graves consequências, incluindo perdas financeiras e violação de dados pessoais.

Ponto importante a salientar é que as informações devem ser classificadas na organização, seja segundo uma norma de classificação da informação, seja em atendimento a uma política de DLP sólida e consistente. Para proteger, é necessário saber o valor do bem a ser protegido. Esse ponto vem sendo frisado há tempo em nossas postagens, haja vista que os controles implementados não podem ser mais caros que o próprio ativo a ser assegurado.

As políticas de DLP definem os tipos de dados considerados confidenciais e como eles devem ser protegidos. Isso pode incluir restrições de acesso, criptografia de dados, monitoramento de redes e outras medidas de segurança. As ferramentas de DLP são usadas para monitorar o uso de dados sensíveis e prevenir o seu acesso não autorizado. Exemplos de ferramentas de DLP são os softwares de monitoramento, de criptografia e de controle de acesso.

A implementação de uma estratégia de DLP envolve a identificação de dados sensíveis, a definição de políticas de segurança e a implementação de ferramentas e técnicas de segurança. É importante lembrar que o DLP não é uma solução completa de segurança da informação e deve ser usado em conjunto com outras medidas de segurança, como firewalls, antivírus e autenticação de usuários.

Os sistemas de DLP monitoram continuamente as atividades de dados em busca de possíveis incidentes. Isso pode incluir o monitoramento de dados em repouso, em trânsito e em utilização. O objetivo é detectar atividades suspeitas, como tentativas de ações não autorizadas, acesso a informações confidenciais, inclusive fora do horário

convencional de operação. Os sistemas de DLP são capazes de detectar e classificar, em tempo real, dados confidenciais.

Tais sistemas de DLP impedem, ainda, a transferência não autorizada de informações confidenciais para dispositivos externos, serviços em nuvem ou aplicativos não autorizados. Isso pode incluir restrições de acesso a dispositivos USB, acessos a redes wi-fi, transferências de dados via bluetooth, bloqueio de transferências de arquivos grandes ou restrições de acesso a serviços em nuvem conhecidos por terem vulnerabilidades de segurança.

Em 2022, o Gartner publicou[1] uma pesquisa oferecendo orientações sobre as tendências do mercado e seus impactos nas estratégias de segurança de dados, o "Market Guide for Data Loss Prevention", cujas recomendações ao mercado replicaremos brevemente neste artigo. A última previsão do Gartner sobre segurança da informação estimou a taxa de crescimento para DLP de 6,6% para o ano de 2022.

A pesquisa destacou que os gastos mundiais dos usuários finais em serviços de nuvem pública cresceram 20,4% em 2022 para US$ 494,7 bilhões, acima dos US$ 410,90 bilhões em 2021. Em 2023, segundo o Gartner, espera-se que os gastos dos usuários finais atinjam quase US$ 600 bilhões. Essa previsão positiva também criou desafios de segurança adicionais, já que as equipes de segurança não têm visibilidade dos dados armazenados na nuvem.

O Gartner recomenda que, antes de selecionar uma solução de DLP, os líderes de segurança e gerenciamento de riscos identifiquem os recursos de DLP para lidar com riscos de dados e necessidades de negócios, considerando a utilização das ferramentas atuais (como produtos SEG e SSE e aqueles em ambientes de nuvem), bem como as opções existentes para obter melhor visibilidade do uso e movimento de dados no ecossistema da organização.

A utilização de tecnologia de classificação de dados é recomendada, por ser fundamental aos esforços de segurança e conformidade de dados. O processo de classificação ajuda a identificar informações confidenciais em um ambiente, o que facilita a definição de políticas de DLP. A classificação precisa evitar os falsos positivos que criam problemas de negócios, obstruem a implantação de controles preventivos e impedem a eficácia dos controles.

Recomenda ainda a utilização de soluções DLP focadas na nuvem para proteção de dados em nuvem pública em organizações com uma estratégia híbrida ou em nuvem. O fornecimento AaS também pode oferecer segurança de dados em várias plataformas para repositórios de dados não estruturados e estruturados. O monitoramento dos limites desses serviços e pontos de contato asseguram os benefícios a longo prazo.

Em suma, destacamos que a implementação de uma solução de DLP envolve, ao menos, 7 etapas importantes, cujo planejamento e execução devem assegurar que a solução atenda às necessidades da sua organização. A seguir, descrevemos as fases

que podem ser estabelecidas para implementar uma solução de DLP confiável.

1. Identifique os dados críticos da sua organização - Inicie identificando quais são os dados críticos da sua organização, como informações financeiras, dados pessoais de clientes ou informações de propriedade intelectual.

2. Avalie os riscos - Avalie os riscos associados à perda ou vazamento desses dados, identificando as ameaças e vulnerabilidades em sua rede e sistemas.

3. Defina as políticas de DLP - Com base nos dados críticos e nos riscos identificados, defina políticas claras de DLP para proteger esses dados. As políticas podem incluir restrições ao acesso, monitoramento de atividades suspeitas e bloqueio de transferências de dados confidenciais.

4. Escolha uma solução de DLP - Escolha uma solução de DLP que atenda às necessidades da sua organização. Certifique-se de que a solução seja compatível com os sistemas existentes e que possa ser configurada de acordo com as políticas de DLP definidas.

5. Implemente a solução - Configure a solução de DLP de acordo com as políticas definidas e teste-a para garantir que esteja funcionando corretamente.

6. Capacite os usuários - Treine os usuários da sua organização sobre as políticas de DLP e como usar a solução de DLP para proteger os dados confidenciais.

7. Monitore e atualize - Monitore continuamente a solução de DLP e atualize as políticas de acordo com as mudanças nas necessidades da sua organização e nas ameaças de segurança.

6 DICAS PARA POTENCIALIZAR O SUCESSO DA GESTÃO DE RISCOS COM A AJUDA DO ENDOMARKETING

Olavo Tokutake, CIGR, CPSI, CIEIE, MBS |
Consultor em Gestão de Riscos e Especialista
em Endomarketing da Brasiliano INTERISK

Se você é profissional da área de Gestão de Riscos, já sabe bem que a Comunicação tem papel muito importante em seu dia a dia, em todas as fases do trabalho. Tanto é que a ISO 31000 e o COSO a têm como fundamental, desde o início até a implementação e monitoramento das ações de gerenciamento dos riscos. O framework desenvolvido pela Brasiliano Interisk, inclusive, possui uma área específica para documentar as ações de comunicação previstas.

Porém, apesar de saber da importância da Comunicação para a Gestão de Riscos, talvez você não saiba de alguns detalhes que podem fazer a sua comunicação interna alcançar melhores resultados. Por isso vou passar, para você, algumas dicas que a experiência me mostrou serem bastante úteis para o trabalho ser desenvolvido de maneira mais prática, objetiva e, claro, com eficiência.

#1 – Um briefing com boas informações possibilita uma comunicação mais eficiente.

Parece óbvio, né? Mas muitas vezes, se não na maioria delas, o desenvolvimento de uma campanha de Endomarketing fica muito prejudicada porque as informações passadas para os criadores não eram corretas, eram insuficientes ou não chegaram com antecedência. Não é necessário passar uma enciclopédia de informações, mas, para o desenvolvimento de um bom trabalho, é importante que você informe:

- O problema ou oportunidade a ser tratado;
- Quem é o seu público-alvo e onde ele está;
- O que eu quero/preciso passar de informação para o público-alvo;
- Qual atitude que o público-alvo precisa/deve adotar;
- Qual o budget para a realização da campanha;
- Book da marca;
- Período da campanha;
- Objetivos da Gestão de Riscos;
- Outras informações que você achar importante.

#2 – Crie, junto da equipe de Endomarketing, um cronograma de trabalho, com cada fase da campanha – desde o briefing até a entrega da campanha.

#3 – Fazer reuniões presenciais, principalmente para o briefing e para as apresentações de planejamento e de criação. Certamente, as chances de acerto serão bem maiores, pois a interação presencial facilita a troca de informações, assim como o entendimento de detalhes, muito mais que numa reunião virtual – tanto para a equipe de Comunicação quanto para a da Gestão de Riscos.

#4 – Se tiver qualquer dúvida, exponha-a assim que ela surgir. Deixar para depois pode levar a um grande retrabalho, que não será necessário se a dúvida for sanada logo que apareceu. E retrabalhos podem gerar atrasos no cronograma.

#5 – Se a campanha criada ficou confusa para você, ela também pode parecer confusa para o público-alvo. Peça a opinião de outras pessoas e, caso a sensação persista, solicite que a equipe do Endomarketing reavalie e retrabalhe as peças; mensagens que não são claras não trazem resultado.

#6 – Procure responder às perguntas da equipe de Endomarketing com rapidez. A informação solicitada pode ser um fator chave para o desenvolvimento da campanha e, assim como no caso de retrabalhos, uma demora pode gerar atrasos no cronograma.

Essas são as seis primeiras dicas para ajudar você a solicitar uma campanha de Endomarketing. Claro que não pretendo, aqui, esgotar o assunto. Afinal, não chegamos nem perto disso. Mas creio que podem iluminar um pouco do caminho. Até a próxima, com mais algumas dicas para ajudar você com o Endomarketing na Gestão de Riscos.

DICAS PARA POTENCIALIZAR O SUCESSO DA GESTÃO DE RISCOS COM A AJUDA DO ENDOMARKETING - PARTE 2

Olavo Tokutake, CIGR, CPSI, CIEIE, MBS |
Consultor em Gestão de Riscos e Especialista
em Endomarketing da Brasiliano INTERISK

Vamos dar continuidade às dicas que a experiência me mostrou serem bastante úteis para que o trabalho de Endomarketing seja desenvolvido de maneira prática, objetiva e, claro, com eficiência. Como mencionado anteriormente, a Comunicação com os colaboradores é fundamental para que o trabalho da Gestão de Riscos obtenha os resultados necessários e esperados.

Na newsletter anterior, passei as seis primeiras dicas e, com as que seguem abaixo, espero poder ajudar a Gestão de Riscos da sua empresa a dispor de uma Comunicação ainda mais eficaz.

Seguem as novas dicas:

#7 – Imagens que ilustrem bem o conceito do que se quer transmitir são muito importantes, pois ajudam o público-alvo a entender, rapidamente, do que você está falando. Como as pessoas estão, atualmente, expostas a muitas informações (pode-se dizer até que de maneira excessiva), a comunicação tornou-se muito visual. Já diz o velho ditado: "uma imagem vale mais do que mil palavras".

#8 – Chamadas curtas e objetivas são outra dica que, assim, como a anterior, são importantes para que o público-alvo entenda rapidamente o que é de fato a sua

comunicação. Essas chamadas devem apontar, de maneira concisa, direta e, se possível marcante, o núcleo do conteúdo que se quer passar. Pode ser um convite irrecusável à leitura do texto que acompanha a peça ou que, por si só, já permita a compreensão do conceito principal.

#9 – Evite textos longos. Caso sua matéria pareça muito extensa, faça um esforço para encurtá-la, cortando palavras que não sejam absolutamente necessárias para a compreensão. Textos curtos são mais atraentes. Use frases diretas, ordenadas de acordo com o raciocínio que você quer que o leitor siga, até a conclusão.

#10 – Uma dica para iniciar a confecção de um texto é, primeiramente, listar palavras e conceitos ligados ao que se quer passar para o leitor. Com a lista feita, vá utilizando as palavras anotadas, costurando-as para redigir a sua mensagem. Isso ajuda a não deixar de lado pontos importantes e, também, a não repetir as mesmas palavras e expressões.

#11 – Por mais que você escreva bem, peça sempre para outra pessoa revisar o seu texto. Afinal, todos são passíveis de cometer pequenos erros, inclusive os de digitação, e quem escreve dificilmente consegue encontrar os próprios deslizes.

#12 – Procure dar celeridade ao processo de avaliação/aprovação do trabalho proposto pela equipe de planejamento/criação da campanha. Lembre-se de que a Comunicação é um ponto muito importante para a Gestão de Riscos: sem ela, todo o restante do trabalho pode ficar enfraquecido, sem o engajamento do público-alvo. Isso pode muito bem acontecer se os colaboradores não forem impactados pela informação no momento correto e de maneira eficaz.

Até a próxima, com mais algumas dicas.

DICAS PARA POTENCIALIZAR O SUCESSO DA GESTÃO DE RISCOS COM A AJUDA DO ENDOMARKETING - PARTE 3

Olavo Tokutake, CIGR, CPSI, CIEIE, MBS |
Consultor em Gestão de Riscos e Especialista
em Endomarketing da Brasiliano INTERISK

Dando prosseguimento às dicas para que o trabalho de Endomarketing seja realizado de maneira prática, objetiva e eficiente, seguem mais seis orientações para que a comunicação ajude a Gestão de Riscos a alcançar os resultados necessários e esperados.

#13 Aproveite e respeite as características dos meios de comunicação. Por exemplo, um cartaz de mural pode ser usado para causar impacto visual, com chamadas curtas e diretas; em meios que possibilitem o uso de vídeos, você pode ganhar a atenção por meio de emoção e/ou mostrar um passo a passo; em outros, em que é possível utilizar áudios, a força da trilha sonora pode ajudar a envolver a audiência e a modulação de voz pode ajudar no entendimento e retenção da atenção. Como disse o filósofo e teórico da comunicação canadense Marshall McLuhan, em 1967, "o meio é a mensagem".

#14 Se a estratégia de comunicação permitir e a verba também, avalie a utilização de meios fora do formato usual, como adesivos em espelhos ou elevadores, apliques na borda de monitores, distribuição de brindes etc. Faça um brainstorming com sua equipe e pensem em ideias fora da caixa. Surpreender é uma ótima maneira de ganhar a atenção e angariar

engajamento.

#15 Eventos também funcionam muito bem. E para isso, nem sempre é preciso montar grandes estruturas nem contratar atrações badaladas. Por exemplo, pode-se organizar um quiz, estendendo um pouco a hora do almoço, para os colaboradores responderem sobre um tema específico, com entrega de prêmios (que podem ser simbólicos) aos vencedores; dependendo do tamanho da empresa e do número de colaboradores, um telão ou tv de tela grande, um microfone e a animação dos participantes já são suficientes.

#16 Interações com o público interno também são sempre bem-vindas. Convidar os colaboradores a darem suas opiniões sobre determinados assuntos, ainda que de maneira anônima, ajuda muito no mapeamento de pontos de interesse. Isso pode ser feito por meio de urnas espalhadas pela empresa, nas quais cada um pode depositar sua opinião, por e-mail ou até por meio de uma empresa terceirizada que coletará as informações sem passar os dados do colaborador à empresa, garantindo o seu anonimato. Mas lembre-se de que é fundamental uma campanha de comunicação para convidar o público interno à participação e para dizer como ele pode tomar parte.

#17 Comunicar sempre os resultados das ações da Gestão de Riscos. Isso sempre ajuda no engajamento dos colaboradores, seja pelo orgulho de participar de algo que está dando certo, seja por perceber que é preciso que todos façam um algo a mais para o sucesso das ações.

#18 A Comunicação é dinâmica, como deve ser para poder acompanhar as necessidades de mudanças que os trabalhos da Gestão de Riscos possam demandar. Por isso, ao planejar as fases da sua campanha de Endomarketing, pense também nos possíveis cenários. Assim será mais fácil e ágil realizar alterações no seu planejamento e nas ações.

Espero que as dicas estejam sendo úteis para você e à Comunicação na Gestão de Riscos. Se tiver alguma dúvida em relação a elas, envie um e-mail para otokutake@brasiliano.com.br.

FONTES DE RISCOS ESG

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

A finalidade de qualquer sistema de gerenciamento de riscos será sempre a prevenção ou, caso esta não seja possível, a mitigação dos riscos para o negócio, seja ele qual for.

Uma maneira adequada para iniciar um trabalho de gerenciamento de riscos ESG será pela determinação dos temas relevantes para a organização, mediante a construção da matriz de dupla materialidade ou relevância, assunto que já debatemos neste mesmo espaço em outra ocasião.

Após terem sido compreendidos perfeitamente os aspectos macro da organização, quais sejam a sua política, as diferentes estratégias e seus correspondentes objetivos estratégicos, parte-se para a identificação dos riscos estratégicos, aqueles que, uma vez materializados, ameaçam o atingimento dos objetivos estratégicos da empresa.

A origem dos Riscos

Uma análise aprofundada revelará que os riscos estratégicos decorrem, normalmente, de outros riscos menos relevantes, muitas vezes combinados. Na dissecação da cadeia de riscos, chegaremos às chamadas fontes de risco(*), isto é, às próprias origens dos riscos. É fundamental para o correto gerenciamento de riscos que as fontes dos riscos sejam determinadas com precisão, bem como os eventos ou exposições que possam vir a transformá-las em riscos.

Um exemplo muito conhecido é o que trata do buraco sem sinalização deixado na rua por uma empresa que faz a manutenção da rede de esgotos. O buraco em si não constitui um risco – é apenas a fonte do risco, pois para gerar dano é necessário que haja um evento ou exposição. Esse evento pode ser uma criança se deslocando sem prestar atenção, que pode cair no buraco e vir a se machucar. Pode ser também um carro passando à noite por aquele trecho e sofrendo um acidente.

Outro exemplo é o phishing, a conhecida técnica utilizada pelos criminosos cibernéticos. O fato de a pessoa receber a mensagem maliciosa ainda não é um risco, mas apenas a fonte de risco, pois a mensagem em si é inofensiva. Ela poderá permanecer na caixa de entrada por muito tempo sem causar transtornos. O problema começa quando ocorre o evento ou exposição: o operador pouco cuidadoso, curioso ou dotado de boa-fé que decide clicar no link e que propicia, a partir dali a infecção do computador e da rede a que está conectado, com todas as consequências que conhecemos muito bem.

Que fazer depois de determinar as fontes de risco?

A determinação precisa das fontes de risco torna-se relevante para que se examinem com cuidado todas as hipóteses de os riscos se materializarem. Algumas fontes de risco são comuns a diversos riscos e é intuitivo que, quanto maior o número de riscos originados da mesma fonte de risco, mais relevante ela será. O perigo de tomarem-se riscos por fontes de risco é que algumas destas últimas possam nos passar despercebidas. Daí a necessidade de uma análise cuidadosa desses aspectos.

Após detida análise e identificação das fontes de risco, o próximo passo será o estabelecimento de controles, de modo a evitar que, surgindo o evento ou a exposição, o risco venha a se caracterizar.

No caso do buraco na rua, poderíamos pensar em um alambrado para impedir o acesso de pessoas ou viaturas às proximidades da fossa. Placas alertando para a existência do perigo constituem outro controle sobre essa mesma fonte de risco.

Já no caso do phishing, o controle mais eficaz será certamente a prevenção, mediante a orientação e capacitação da força de trabalho da empresa sobre o significado dos riscos cibernéticos e da necessidade de todos prestarem atenção a qualquer mensagem recebida via internet, mesmo àquelas provindas das fontes mais confiáveis.

Fontes de riscos ESG

As fontes de riscos ESG serão determinadas com o emprego da mesma metodologia. Tomemos como exemplo um risco ambiental bastante comum: o derrame de efluentes líquidos gerados durante o processo produtivo. Esse é um risco de primeira ordem e que pode dar origem a diversos outros: poluição ambiental, passando pelas multas aplicadas pelo órgão ambiental, pelos danos à imagem da empresa, pela cassação da licença ambiental e chegando até à falência da empresa. As possíveis fontes desse risco de primeira ordem seriam, por exemplo: a produção de efluentes químicos poluentes pela empresa; a falta de monitoramento ambiental; a inexistência de tanques de retenção de efluentes; a falta de capacitação das equipes de monitoramento; o uso de equipamentos obsoletos; a previsão orçamentária insuficiente; e assim por diante.

É interessante observar que cada uma das fontes de riscos ESG se aninha em uma das tradicionais macrocausas, quais sejam: Processos, Pessoal, Infraestrutura, Tecnologia

ou Ambiente Externo.

Controles ESG

Prosseguindo com o nosso exemplo, verificamos as seguintes possibilidades de controles: providências para eliminar ou reduzir a geração de efluentes químicos poluentes; criação de uma equipe de monitoramento ambiental e capacitação de seus integrantes; construção de tanques ou lagoas de retenção de efluentes; capacitação das equipes de monitoramento; previsão de recursos no orçamento anual da empresa para fazer face às despesas com a capacitação de pessoal e com aquisições e manutenção de equipamentos.

O Plano de Ação

O documento que especifica os controles é o chamado Plano de Ação. Da análise da existência e da conformidade dos controles retiram-se conclusões sobre o Risco Inerente, o Risco Residual e sobre o Apetite ao Risco da empresa, dados esses essenciais para a prática do gerenciamento de riscos em qualquer organização.

Conclusão

Tivemos assim uma ideia, ainda que ligeira, da relevância que assume a determinação das **fontes de risco** no trabalho de **gerenciamento de riscos** em geral e dos **riscos ESG** em particular.

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 **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. Solicite uma demonstração:

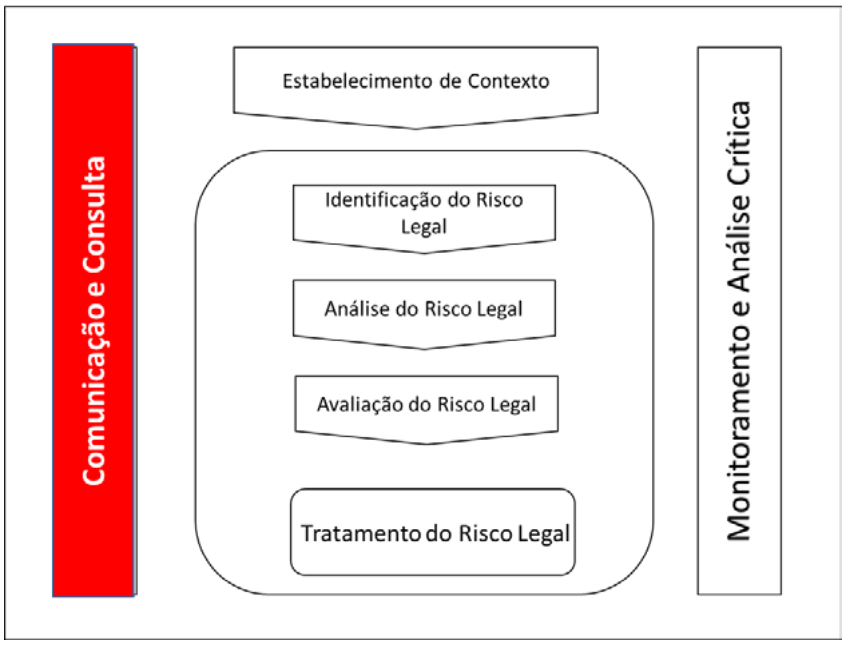
(*) Também conhecidas como “fatores de risco”

OS MECANISMOS DE COMUNICAÇÃO, CONSULTA E RELATO PARA GESTÃO DE RISCOS LEGAIS DE ACORDO COM AS NORMAS ABNT NBR ISO 31000:2018 E ABNT NBR ISO 31022:2020

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

A norma ABNT NBR ISO 31000:2018, complementada pela ABNT NBR ISO 31022:2020, estabelece que uma organização deve desenvolver mecanismos de comunicação e relato para assegurar que haja comunicação adequada dos principais elementos da gestão de riscos legais, em tempo e níveis apropriados.

PROCESSO DE AVALIAÇÃO DE RISCO LEGAL



É preciso que haja uma conexão entre estes mecanismos, a forma de comunicação e as outras fontes de informação de riscos, de forma que os fluxos de comunicação entre a organização e as partes interessadas externas sejam assegurados.

A confidencialidade, o privilégio profissional legal, bem como o privilégio advogado-cliente – ou quaisquer formas equivalentes de proteção de jurisdição pertinente – devem ser garantidas entre a comunicação externa e o relato.

É oportuno que a organização, em cada etapa do processo de gestão de riscos legais, estabeleça a comunicação e consulta, em tempo hábil, entre as partes interessadas pertinentes, para que estas compreendam integralmente quais são esses riscos e que efeitos serão produzidos. Neste contexto, as partes interessadas devem conhecer seus papéis no processo de tomada de decisões para a gestão de riscos legais e devem estar aptas, de maneira eficiente e eficaz, a tomar decisões apropriadas com base em informações pertinentes .

Considerando que a organização e as partes interessadas, de maneira geral, possuem valores, perspectivas e focos diversos, suas preferências e expectativas em relação à gestão de riscos legais provavelmente serão divergentes, causando um importante efeito na tomada de decisões no que diz respeito ao gerenciamento desses riscos. Frente a isto, a comunicação e a consulta às partes interessadas pertinentes, durante o processo de tomada de decisões e implementação do tratamento desses riscos, devem incluir um processo vigoroso de monitoramento e análise crítica, mantendo registros das práticas dessa gestão.

Para facilitar a comunicação eficaz e efetiva, a organização deve fornecer todas as informações necessárias a todos os envolvidos com responsabilidade, responsabilização e autoridade pela gestão e supervisão dos riscos legais.

A direção deve estar plenamente apta a se comunicar com as partes interessadas pertinentes, aí incluídas as autoridades regulatórias, legislativas, judiciárias e outra partes interessadas externas.

A construção de uma cultura de gestão de riscos na organização depende, então, de que a comunicação ocorra em todos os estágios da gestão de riscos legais. Tal cultura deve promover a conscientização e a compreensão sobre a exposição aos riscos e ser usada para permitir clareza sobre a governança e liderança, sobre o mandato, as metas e objetivos, o envolvimento das partes interessadas, seus papéis e responsabilidades, e a conformidade com políticas, processos e procedimentos.

INTRODUÇÃO AO SISTEMA DE CONTROLE INDUSTRIAL

Mariana da Silveira, DIDS, MBCR, CPSI, CEGRC, CIGR, CISI, CIEIE, DPO, ISO | Divisão Cibernética da Brasiliano INTERISK

O sistema de controle industrial (ICS) é usado para administrar processos industriais, como fabricação, manuseio de produtos, produção e distribuição. Ele inclui sistemas de supervisão e de aquisição de dados usados para monitorar ativos geograficamente dispersos, bem como sistemas de controle distribuídos e sistemas de controle menores usando controladores lógicos programáveis para fiscalizar processos localizados.

O ICS abrange vários tipos de sistemas, incluindo sistemas de controle de supervisão e aquisição de dados, sistemas de controle distribuído e outras configurações de sistema de controle, como controladores lógicos programáveis frequentemente encontrados nos setores industriais e de infraestruturas críticas.

Segundo o National Institute of Standards and Technology (NIST), agência estadunidense de padrões e tecnologia, um sistema de controle industrial consiste em combinações de componentes de controle elétrico, mecânico, hidráulico e pneumático que atuam juntos para atingir um objetivo industrial, quer seja fabricação, transporte de matéria ou energia.

O ICS é essencial para as operações das infraestruturas críticas, dos setores industrial e automotivo. Além disso, é constituído de sistemas altamente interconectados e interdependentes. No Brasil, a segurança na interface da tecnologia da informação com a tecnologia operacional é, muitas vezes, negligenciada. Consequentemente, os investimentos necessários para mitigar as vulnerabilidades e ameaças são insuficientes.

Muitos dos sistemas de controle industrial evoluíram a partir da inserção de recursos de TI em sistemas físicos existentes, muitas vezes substituindo ou complementando os mecanismos de controle físico. Assim, os controles digitais incorporados substituíram os controles mecânicos analógicos em máquinas, motores e equipamentos.

Os investimentos em tecnologias de ponta e as melhorias em custo e desempenho estimularam essa evolução, resultando em muitas das tecnologias inteligentes, como rede elétrica, transporte, construção e manufatura. Embora tenha aumentado a conectividade e a criticidade desses sistemas, houve o surgimento de uma maior necessidade de adaptabilidade, resiliência, proteção e segurança.

Nos primórdios, o ICS era composto de sistemas isolados que executavam protocolos de controle proprietários usando hardware e software especializados. Muitos componentes do sistema de controle industrial estavam em áreas fisicamente protegidas e os componentes não estavam conectados a redes ou sistemas de TI.

Os dispositivos de Protocolo de Internet (IP) de baixo custo e largamente disponíveis têm substituído soluções proprietárias, aumentando a ocorrência de vulnerabilidades e incidentes de segurança cibernética. Tem ocorrido a adoção de soluções em TI nos sistemas de controle industrial para promover conectividade de sistemas de negócios corporativos e recursos de acesso remoto.

Os sistemas operacionais (SO) estão sendo projetados e implementados com protocolos de rede padrão da indústria. Essa integração oferece suporte a novos recursos de TI e estabelece comunicação integrada, permitindo o compartilhamento de informações. A partir daí, aumenta a exposição a riscos oriundos do ambiente externo, trazendo a necessidade de aumentar a proteção para esses sistemas.

O uso crescente de redes sem fio expõe o ICS a incidentes, o que torna a segurança cibernética elemento essencial para a operação segura e confiável de processos industriais modernos. As ameaças aos sistemas de controle industrial podem surgir de qualquer origem, assim, medidas técnicas e administrativas devem ser tomadas a fim de proteger a confidencialidade, disponibilidade e integridade das informações.

Quanto às possíveis ameaças que um ICS pode enfrentar, considera-se: fluxo de informações bloqueado ou atrasado; acesso não autorizado, destruição, divulgação, modificação de informações, negação de serviço; alterações não autorizadas em instruções, comandos ou limites de alarme; informações imprecisas enviadas aos operadores do sistema; software infectado ou definições de configuração modificados; interferência na operação dos sistemas de proteção do equipamento ou no funcionamento dos sistemas de segurança.

As medidas técnicas e organizacionais que podem ser tomadas a fim de mitigar a probabilidade de as ameaças explorarem as vulnerabilidades do ICS, são: segmentação e segregação de redes; estratégia de defesa em profundidade; restrição do acesso lógico e à atividade da rede; restrição do acesso físico à rede, aos componentes individuais e dispositivos; restrição ao acesso e à modificação não autorizada de dados; detecção de eventos e incidentes de segurança e manutenção das funcionalidades durante

condições adversas.

Um ponto fundamental a ser considerado é a existência de diferentes cenários de ataques, ameaças, níveis de risco, impacto e probabilidade nos sistemas de controle industrial. Cada setor específico, quer sejam as infraestruturas críticas, as indústrias de manufatura, distribuição e fabricação, e cada organização possuem suas próprias peculiaridades, que devem ser respeitadas e estudadas, para que ações efetivas sejam realizadas e medidas técnicas e organizacionais sejam tomadas em cada caso específico.

IMPORTÂNCIA DO GERENCIAMENTO DE OCORRÊNCIA NA SEGURANÇA

José Sérgio Marcondes, CES | Especialista em Segurança Empresarial, Consultor de Segurança e Diretor do IBRASEP.

A segurança é uma das principais preocupações das organizações em todo o mundo. E, para garantir a proteção das pessoas e do patrimônio, é essencial ter um bom sistema de Gerenciamento de Ocorrência de Segurança. Mas o que é exatamente gerenciar ocorrências na segurança e por que é tão importante?

O Gerenciamento de Ocorrência na Segurança envolve o registro e tratamento de eventos que possam afetar a segurança da organização. Desde pequenos incidentes até grandes ameaças, como invasões e roubos. Neste artigo, vou explorar a importância do Gerenciamento de Ocorrência na Segurança e como ele pode ser usado para melhorar a qualidade da gestão da segurança.

O que é uma Ocorrência na Segurança?

Ocorrência na segurança pode ser definida como qualquer evento que ameace a segurança de um determinado ativo, incluindo pessoas, bens, instalações e equipamentos. Esses eventos podem ser intencionais ou acidentais e geralmente requerem ações imediatas para mitigar os danos.

Algumas das ocorrências mais comuns na segurança incluem acesso indevido, roubo, furto, vandalismo, sabotagem, incêndios, desastres naturais, falhas no sistema de segurança, entre outros. Essas ocorrências podem acontecer em qualquer setor, como indústrias, comércio, hospitais, escolas e condomínios residenciais e comerciais.

É importante ressaltar que a identificação, registro e gerenciamento adequado dessas

ocorrências são cruciais para a segurança da organização. Além disso, a coleta e análise de dados sobre esses eventos podem ajudar na tomada de decisões mais informadas sobre as estratégias de segurança a serem adotadas.

O que é Gerenciamento de Ocorrências na Segurança?

O Gerenciamento de Ocorrência na Segurança pode ser definido como o processo de registrar as ocorrências na segurança e tratar esse registro de forma a gerar conhecimentos que possam ser aplicados a melhoria da segurança da organização.

O processo de Gerenciamento de ocorrência na segurança envolve o registro da ocorrência, a criação de banco de dados, a avaliação dos eventos, a criação de estatísticas, a geração de informação e o aprendizado com as ocorrências registradas. O objetivo é prevenir ocorrências, reduzir riscos e aumentar a eficiência e efetividade da segurança.

A gestão de ocorrências envolve a criação de um sistema de registro de ocorrências que permita documentar todas as informações relevantes sobre o incidente, bem como o estabelecimento de procedimentos claros para armazenamento e tratamento desses registros.

Relatório de Ocorrência

O registro das ocorrências, através do Relatório de Ocorrência, é uma das principais ferramentas do gerenciamento de ocorrências na segurança, pois permite que as informações sobre os eventos ocorridos sejam registradas de forma clara e precisa.

Esses relatórios devem conter detalhes sobre a natureza da ocorrência, as circunstâncias em que ocorreu e outras informações importantes que possam ser usadas para avaliação

e compreensão do evento.

O Relatório de Ocorrência é uma ferramenta valiosa para o gerenciamento de ocorrências na segurança, pois permite que as informações importantes sejam registradas, analisadas e utilizadas para aprimorar continuamente o sistema de segurança existente.

Para que serve o Gerenciamento de Ocorrência na Segurança?

O Gerenciamento de Ocorrência na Segurança serve para registrar, avaliar e tratar as ocorrências relacionados à segurança, a fim de prevenir futuras ocorrências e melhorar a segurança existente

Esse gerenciamento permite que os gestores de segurança avaliem as ameaças e os riscos à segurança, identifiquem tendências e padrões de comportamento, e implementem medidas preventivas e corretivas para minimizar o impacto das ocorrências na segurança.

Além disso, o Gerenciamento de Ocorrência ajuda a manter um registro preciso de todas as ocorrências, fornecendo informações importantes para a tomada de decisões e melhoria contínua do programa de segurança existente.

Importância do Gerenciamento de Ocorrências na Segurança

O processo de Gerenciamento de Ocorrências na Segurança é uma ferramenta crucial para o aprendizado com as falhas e erros cometidos. Ao revisar e avaliar as ocorrências, é possível identificar padrões de comportamento, pontos fracos e falhas no sistema de segurança, e outras áreas que precisam ser aprimoradas para prevenir futuras ocorrências.

Um sistema de gerenciamento de ocorrência bem estruturado pode oferecer vários benefícios para a segurança. Ele pode identificar tendências e padrões nas ocorrências, permitindo que a empresa tome medidas preventivas para evitar incidentes futuros.

Outro benefício do gerenciamento de ocorrência na segurança é a melhora do direcionamento de investimentos. Ao documentar todas as ocorrências, é possível identificar áreas que estão mais propensas a problemas de segurança e, assim, tomar medidas para fortalecer a segurança dessas áreas especificas.

Além disso, a análise dos dados de ocorrências pode ajudar a identificar padrões de comportamento dos infratores, o que pode levar à implementação de medidas preventivas mais efetivas.

Conclusão

O Gerenciamento de Ocorrências na Segurança é uma prática fundamental para garantir a proteção das pessoas e bens. Com um sistema bem estruturado de registro, tratamento

e aprendizado com as ocorrências, é possível identificar falhas e oportunidades de melhorias, reduzir riscos e prevenir eventos futuros.

Nesse contexto, não deixe de conferir o meu artigo sobre “Relatório de Ocorrência”, onde abordo a importância desse documento para o gerenciamento de ocorrências na segurança. Através do relatório de ocorrência, é possível registrar e documentar todas as informações relevantes sobre as ocorrências, permitindo a criação de estatísticas e análises para aprimorar ainda mais o sistema de segurança.

BENEFÍCIOS E VANTAGENS DE UMA CERTIFICAÇÃO PROFISSIONAL

Dr. Renato Figueiredo, CPSI, CIGR, CISI, CIEIE, CEGRC, CIEAC, CIPSI, MBS, DIDS. Doctorado Internacional en Ciencias de la Seguridad (CEAS-INTERNACIONAL). Presidente CEAS-BRASIL e Secretário Geral CEAS-INTERNACIONAL

O que uma certificação garante ao profissional de segurança?

Uma certificação aumenta as possibilidades, por exemplo, de que a pessoa que a obtenha tenha certos conhecimentos e habilidades em segurança, tais como:

- Melhorar a sua imagem dentro da sua organização.
- Aumentar o potencial de crescimento e oportunidades dentro da empresa.
- Acelerar seu desenvolvimento profissional.
- Obter reconhecimento profissional e pessoal.
- Capacidade de desenvolver programas de treinamento interno com pessoal qualificado.
- Participar de um grupo de profissionais reconhecidos.
- Reconhecimento de suas habilidades como Especialista por colegas de profissão e diretores.
- Promover a sua carreira profissional pelo reconhecimento como profissional da área de segurança.
- A satisfação pessoal de obter a certificação em sua carreira.
- A certificação pode melhorar o desempenho geral, eliminar a incerteza e

expandir as oportunidades de mercado.

- O processo de obtenção e manutenção da certificação ajuda a garantir que você esteja continuamente aprimorando e refinando suas habilidades e conhecimentos.

- Você receberá benefícios potencialmente maiores ao ser formalmente reconhecido como um profissional experiente.

Uma certificação é uma declaração formal de uma instituição (pública ou privada, nacional ou internacional) que atesta que o candidato foi aprovado com sucesso em um exame ou em uma série de procedimentos estabelecidos pela instituição.

É interessante que algumas organizações que coordenavam uma ou duas certificações, viram uma oportunidade de mercado e ampliaram sua oferta, mas para obter uma base de certificados rapidamente implementaram o que eu traduziria como fábrica de certificação. Isto significa que, ao conceder uma certificação, a certificadora permite que o candidato receba a sua certificação,

mediante o cumprimento de determinados requisitos que incluem experiência comprovada em determinadas áreas e sem apresentação de qualquer exame, uma vez que me parece que não ajuda a homogeneizar o nível dos certificados.

O problema é esperar a certeza total sobre esses conhecimentos e habilidades. Por exemplo, se uma pessoa é um profissional certificado com a certificação CPSI, podemos supor (com uma alta porcentagem de probabilidade, mas não como garantia) que ela tenha um bom nível de conhecimento geral de segurança e alguns anos de experiência, pois caso contrário seria quase impossível obter a certificação CPSI. Por outro lado, pudemos ter a certeza de que tal profissional está qualificado para ocupar um cargo gerencial em uma empresa da área de segurança, tanto nacional quanto internacionalmente.

Na minha opinião, um dos maiores pontos fracos de muitas certificações é que elas estão mais focadas em testar os conhecimentos dos candidatos, do que em qualificar suas habilidades para enfrentar e resolver problemas cotidianos de trabalho. Algumas certificações não avaliam, por exemplo, se essa pessoa será capaz de realizar com sucesso uma análise de risco ou apresentar satisfatoriamente os resultados de uma auditoria de segurança. Por esse motivo, é muito importante uma rigorosa análise curricular, onde o avaliado deve possuir determinadas qualificações e cursos em diversas áreas do conhecimento.

Existem profissionais que não possuem conhecimentos prévios de alguns sistemas gerais de segurança e que não possuem habilitações em diversas áreas de segurança, obtendo a sua certificação.

Embora o exposto acima possa parecer óbvio para alguns, a verdade é que muitas

vezes as empresas contratam candidatos às cegas, confiando principalmente em seus certificados.

Devo dizer que concordo que a equipe seja certificada; há duas coisas que não me parecem adequadas: (1) que pensamos que ao ter uma determinada certificação a pessoa automaticamente tem competências ou experiências para o trabalho que vai realizar, e (2) que vemos as certificações como objetivo. Em outras palavras, acho que devemos nos preocupar mais em aprimorar nossos conhecimentos de segurança, incluindo conhecimentos técnicos bem específicos de temas como Gestão de Riscos Empresarial, Riscos Cibernéticos, Segurança Pessoal Privada, Segurança Corporativa, Gestão de Riscos de Fraudes e Compliance, Análise de Inteligência, Segurança Industrial ou os detalhes de uma determinada tecnologia, para posteriormente obter uma certificação.

Os certificados profissionais permitem validar as competências e habilidades de um profissional em diferentes áreas de especialização que muitas empresas eles precisam. Esse tipo de certificação pode ser obtido por meio da certificação de competências, ou por meio de treinamentos específicos, presenciais, ou por meio de cursos online voltados para a obtenção de uma certificação profissional específica.

A obtenção de um certificado profissional supõe o reconhecimento oficial de que uma pessoa possui competências específicas, pelo que é muito importante para o crescimento profissional e a procura de colocação qualificada. Mas a certificação profissional contribui não só para o desenvolvimento profissional, mas também para o desenvolvimento pessoal, dando aos profissionais a garantia de que as suas competências são reconhecidas. Nesse sentido, os certificados profissionais permitem que você se diferencie e seja mais competitivo.

A certificação contribui tanto para o desenvolvimento pessoal quanto profissional, dando ao profissional a segurança de ter as diretrizes adequadas para a realização de seu trabalho. Os profissionais certificados devem estar sempre atualizados em novos conhecimentos e estratégias de gestão, tendo as ferramentas ideais para continuar melhorando.

A cada momento que passa, o mercado de trabalho fica mais exigente, e isso torna os profissionais cada vez mais preparados para esses avanços que ocorrem quase que diariamente. A obtenção de uma certificação profissional surge assim como uma ferramenta fundamental para os profissionais da área da segurança que ambicionam o sucesso na sua carreira profissional.

Após a obtenção de sua certificação, o profissional deve sempre buscar sua qualificação profissional, pois é uma ferramenta de fundamental importância para seu contínuo crescimento profissional e até mesmo realizar a renovação de sua certificação, pois o profissional deve atingir um determinado número de créditos, através de determinados

formas de qualificação, que vão desde cursos de segurança até os famosos MBA`s, Congressos, Seminários, etc. O importante é que o profissional certificado esteja sempre se atualizando.

Obtenha reconhecimento profissional e faça parte do grupo de profissionais que já se beneficiaram das vantagens concedidas por uma certificação profissional da Corporación Euro-Americana de Seguridad (CEASINTERNACIONAL).