FIESP | DEPARTAMENTO DE DEFESA E SEGURANÇA

GUIA PRÁTICO DE AÇÕES DE SEGURANÇA EMPRESARIAL FRENTE À COVID-19

Maio 2020

FIESP

O mundo enfrenta o maior desafio de sua história recente: a pandemia do novo coronavírus. Essa crise está impactando toda a sociedade. E desde o primeiro momento, a indústria tem atuado com coragem e determinação, para proteger a saúde de todos os brasileiros, e reduzir o impacto sobre empresas e empregos.

Fiesp, Ciesp, Sesi, Senai e IRS assumiram o protagonismo nessa luta contra a Covid-19. Suas muitas frentes de atuação vêm servindo de balizamento pra empresas e poder público, neste momento de pandemia.

Nas áreas de defesa e segurança, mobilizamos nossa rede de parceiros para criar um Comitê de Crise para pensar, discutir e propor medidas capazes de minimizar os riscos e os impactos da pandemia do Coronavírus na segurança dos ativos de indústrias e empreendimentos.

Um dos resultados dessa iniciativa é o **Guia Prático de Ações de Segurança Empresarial frente à COVID-19**, que apresenta uma sucessão de conteúdos voltados para profissionais de todas as cadeias produtivas da indústria. Os textos a seguir jogam luz sobre temas pertinentes à realidade que temos enfrentado, como segurança de instalações, armazenamento e distribuição de insumos, e gestão de continuidade de negócios.

Entendemos que as circunstâncias geradas pela pandemia da Covid-19 são excepcionais e demandam a integração de esforços para que contribuições sejam realizadas e experiências e conhecimentos sejam trocados. É com esse objetivo que disponibilizamos essa série de conteúdos produzidos por especialistas que são autoridades em suas áreas de atuação. Ao final de cada artigo, foram disponibilizados dados de contato dos autores, proporcionando a você, leitor, acesso direto a cada um deles, caso deseje se aprofundar em qualquer uma das questões tratadas.

Esperamos que esses conteúdos possam trazer esclarecimentos e orientações sobre como cada um de nós, colaborador da indústria, pode enfrentar esse momento de dúvidas e inquietações.

Ainda não chegamos ao fim desta jornada tão desafiadora. Mas temos a convicção de que estamos no caminho certo para atravessar a tempestade. Mais do que isso, estamos certos de que estamos fazendo tudo ao nosso alcance para ajudar nosso país e todos os brasileiros a fazer o mesmo.

Essa é a missão da indústria contra o coronavírus.

Paulo Skaf
Presidente da Fiesp, do Ciesp, Sesi, Senai e IRS

SUMÁRIO

1. COMITÊ DE GERENCIAMENTO DE CRISE

ENTENDA O QUE É UM COMITÊ DE GERENCIAMENTO DE CRISES E COMO ELE PODE AJUDAR SUA EMPRESA A ENFRENTAR MOMENTOS DE INSTABILIDADE

Empresas de todo o mundo passam por um momento delicado, diante da eclosão da pandemia do Coronavírus. Desafiadas por uma ameaça até então inédita, elas se veem obrigadas a organizar suas operações para enfrentar não apenas os impactos causados pela COVID-19, mas também os desdobramentos que surgirão durante o pós-crise.

Uma das ferramentas de resposta mais eficazes a uma crise, independentemente do seu grau de gravidade, é a criação de um Comitê de Crises. Ele costuma ser o primeiro recurso acionado em momentos críticos e faz parte do Plano de Gerenciamento de Crises, recurso indispensável para empresas e organizações de qualquer porte. Esse Comitê é composto por um pequeno grupo de profissionais da empresa – geralmente os principais executivos da corporação – que será responsável pela tomada de decisões. Caberá a cada integrante direcionar sua respectiva expertise às áreas afetadas e, eventualmente, solicitar apoio externo.

Se a empresa for pequena ou média, o grupo pode ser ainda mais reduzido. O importante é manter um núcleo que possa pautar decisões e ações. Tanto quanto possível, para cada função exercida no Comitê de Crises, deve haver um membro substituto com atribuições delegadas, na impossibilidade de o titular estar presente ou participar por via remota. Isto vale também para eventuais revezamentos necessários quando falamos de crises de longa duração. Todos devem conhecer bem as suas funções em cenários de anormalidade e serem acionáveis a qualquer tempo, devendo haver para isso um aplicativo ou uma lista com a chamada árvore de acionamento.

A empresa deve garantir que seja criado um Termo de Confidencialidade, e que todos os membros convocados para o Comitê de Crises o assinem, para controlar potenciais vazamentos de informações. A implantação de uma rígida política de segurança da informação é crucial. Anotações não devem ser descartadas na lixeira e documentos, registros, anotações de lousa, pen drives ou HDs externos não devem ser deixados na sala, após a reunião. Limite o acesso a esse local apenas às pessoas membros do Comitê de Crises, evitando assim o vazamento de informações e estratégias adotadas. Registre sempre em uma lista assinada as presenças de todos, preferencialmente com horário de chegada e saída.

O funcionamento do Comitê de Crises é simples. Cada integrante do comitê manifesta-se para cada decisão importante, cabendo ao secretário a consignação das respectivas opiniões e a anotação de todas as decisões e justificativas, a fim de proporcionar o registro dos fatos para aprendizados e eventuais auditorias e investigações.

É função do gerente da crise não apenas tomar a decisão final, mas também moderar as discussões para que as melhores decisões sejam obtidas e assegurar que os envolvidos mantenham certo grau de distanciamento do problema discutido, a fim de evitar desconfortos, além daqueles já causados pela crise. O ambiente de discussão é árido pela natureza das próprias circunstâncias, por isso, é

necessário que haja extrema atenção aos humores de cada integrante. Dessa forma, será possível garantir um desempenho colaborativo e harmônico.

Outros pontos aos quais os membros do comitê devem permanecer atentos são a autenticidade e a veracidade das informações analisadas para que decisões não sejam tomadas com base em algo não concreto ou fora de contexto. É importante ressaltar que na dinâmica de uma crise é preciso trabalhar com a melhor informação validada disponível para subsidiar a melhor tomada de decisão possível.

Plano de Retorno

É importante que todos reservem ainda durante a crise um horário diário para preparar o retorno à "nova" normalidade. É a chance de o grupo refletir sobre os negócios, avaliar mudanças nos produtos e na estrutura da empresa, possíveis contratações, demissões, ajustes nos controles e certificações. O ajuste no Plano de Negócios permitirá perceber todas as necessidades. A capacidade de enxergar rotinas como flexíveis para fazer frente à situação em tela é uma capacidade essencial, pois nem todas as respostas estarão nas rotinas estabelecidas, ou mesmo nos planos de crises, contingência e continuidade.

Plano de Desmobilização

A crise chegará ao final e, quando este momento chegar, ele deverá ser declarado para os parceiros, fornecedores, acionistas, público interno, comunidade local, e todos aqueles ligados direta ou indiretamente ao negócio. Será o momento para rescindir os contratos emergenciais e revisar os existentes e os que vão continuar. Também é a etapa em que finalizamos o documento da gestão da crise, fotos, vídeos, atas de reunião, comprovantes, justificativas, dentre outros. Assim, a empresa estará preparada para continuar as suas operações.

Ao menos uma reunião pós-crise ou *debriefing* é essencial para que não se percam aprendizados importantes, acertos e erros, não com propósito de juízo de valor, mas de melhoria de processos. Este conhecimento fortalece a memória institucional da organização e as soluções encontradas, ajudando a manter ou cultivar uma cultura de gerenciamento de crises para o futuro.

AUTORES

Diógenes Viegas Dalle Lucca, MSc, Tenente-Coronel Veterano da Polícia Militar do Estado de São Paulo. Especialista em Gestão de Crises e Proteção Executiva.
Contato: lucca@thefirst.com.br
Jeová Ferreira Cardoso Júnior, PFSO, Consultor Sênior em Segurança Empresarial.
Contato: jeova.cardoso@hotmail.com
Mauricio Franklin Pontes, empresário. Especialista em Gestão de Crises e Ciência da Complexidade.
Contato: mauricio.pontes@c5i.com.br
Roberto Zapotoczny Costa, MSc, empresário. Especialista em Gestão de Crises e Proteção Executiva.
Contato: robertocosta@thefirst.com.br

2. COMUNICAÇÃO NA GESTÃO DE CRISES

GERENCIAMENTO DE CRISE: 13 PASSOS PARA IMPLANTAR UMA COMUNICAÇÃO EFICIENTE E DECISIVA

A Comunicação transparente, constante e correta é uma das mais eficientes armas de defesa em uma gestão de crise. Comunicar a todo momento, mesmo que a empresa ainda esteja estruturando as suas ações para enfrentar a crise, reflete o comprometimento da instituição em passar pelos desafios com o mínimo de danos possíveis para seus públicos: empregados, fornecedores, clientes e parceiros.

É por isso que as autoridades governamentais estão em constante diálogo com a imprensa e formadores de opinião. Não se manifestar neste momento pode vir a ser crítico à empresa, sendo indispensável a atenção a informações e opiniões incertas ou que não estejam alinhadas à imagem pública daquela instituição.

Sim, é importante comunicar, mas a comunicação precisa levar em conta os valores da empresa e os de seu público para que a informação atinja seus objetivos. A coerência entre o discurso e o posicionamento tem que estar refletida na comunicação institucional, principalmente em um ambiente de crise. Nessa hora, tudo o que uma determinada instituição comunicar será analisado com lupa pelo seu público.

O roteiro abaixo, com algumas sugestões, pode servir de inspiração sobre como estruturar a Comunicação para enfrentar situações críticas:

1. **Crie um comitê de crise, formado pelos principais gestores e pessoas chave da empresa**. O CEO deve dividir com os pares a responsabilidade pelas decisões para que haja o engajamento necessário e o alinhamento das mensagens emitidas pela empresa. Haverá desgaste de imagem, caso o CEO passe uma mensagem e seus diretores outra, além de diminuir a credibilidade das informações e da corporação;

2. **Seja claro, não esconda a verdade.** Explique o problema e sua real dimensão, como o negócio poderá ser impactado, assim como empregos e contratos. Demonstre a preocupação e o comprometimento em encontrar soluções. A empatia gerada acalmará os ânimos, ao mesmo tempo em que sinaliza a complexidade e a gravidade do novo cenário;

3. **Aumente consideravelmente os canais de comunicação e a frequência das mensagens**, mesmo que não haja nada novo para comunicar. Repita as mensagens, explique novamente por outro ângulo, convide especialistas sobre diversos assuntos, mas não pare de dialogar com seus diversos públicos. A enorme quantidade de eventos online que surgiu nos últimos 30 dias aconteceu justamente para as instituições continuarem próximas de seus públicos, levando serviços e informações de forma constante;

4. **Quando errar, admita o erro e comunique a correção das ações**. Em um momento tão tenso quanto de uma crise, os erros vão acontecer, seja pela ânsia de solucionar o problema, seja pela

rapidez da tomada de decisões. O motivo e o erro não importam, mas a vontade de corrigir, sim. Corrija a rota e informe seus públicos;

5. **Comunique com clareza e segurança**. Se o CEO não é eloquente, a comunicação deve ser delegada a um porta-voz, a um diretor, a alguém que transmita confiança e tranquilidade ao passar as informações. Nada desgasta mais um líder do que passar a imagem incorreta diante de uma crise. E mesmo que um dos líderes seja extremamente bom em falar em público, construa um roteiro em equipe e treine-o antes. Se o gestor participar de entrevistas jornalísticas, o melhor é passar por um *media training* ou, pelo menos, ser sabatinado pelos pares antes de conceder a entrevista;

6. **Use e abuse das ferramentas digitais, preferencialmente as que transmitam imagens**, como *lives*, videoconferências, mensagens em vídeo. Seus funcionários, clientes e fornecedores querem ver a pessoa por trás da informação, querem o olho no olho para poderem confiar mais no que está sendo dito;

7. **Explique minuciosamente**. Todas as novas leis e determinações governamentais que impactarem diretamente o negócio ou a forma de trabalho ou remuneração de seus empregados devem ser comunicadas de forma detalhada e adaptada à realidade da empresa. Simplesmente reproduzir leis e decretos não é o bastante. Explique até ser compreensível a todos os níveis da empresa;

8. **Crie vários canais de atendimento para os seus colaboradores**. Em um momento de alta tensão, de incerteza na continuidade dos contratos de trabalho e remunerações, é importante ouvir empaticamente seus funcionários, através de diversos canais: e-mails, WhatsApp, *chats* institucionais, redes sociais, telefones ou outros meios disponíveis;

9. **Faça reuniões de status com as equipes diariamente**. Através de videoconferências, realize reuniões de atualização das decisões e rotinas. Dessa forma, as equipes ficam mais engajadas, sabendo exatamente qual a situação da empresa naquele momento e o papel de cada colaborador no novo cenário. As reuniões devem ser rápidas, mas constantes para criar a sinergia necessária;

10. **Incentive seus colaboradores a desenvolver novas habilidades**. Além de ser uma grande arma contra a ansiedade e a sensação de impotência diante de um cenário descontrolado, adquirir novos conhecimentos e habilidades pode ser extremamente útil em situações de crise. A criatividade e inovação comumente são os diferenciais que levam uma empresa ao sucesso mesmo nos piores momentos;

11. **Seja empático**. Em todas as comunicações da empresa, pense no bem-estar de seus públicos. Coloque-se como receptor daquela informação e verifique qual o sentimento que ela desperta. Se a emoção for negativa, procure mudar o ângulo da informação até conseguir passar a mesma mensagem, de forma positiva;

12. **Sites e redes sociais precisam estar atualizados e com informações corretas.** Uma das maiores fontes de estresse em crises é a desinformação. Não permita que sua empresa tenha uma comunicação deficiente, com dados antigos ou imprecisos;

13. **Revise seus materiais de comunicação**: **folders, anúncios, redes sociais etc**. Evite associar a marca de sua corporação à lembrança de eventos negativos como acidentes, pandemias, mortes. Uma imagem despretensiosa como a de um reflexo de um avião nas janelas de um edifício pode ser bonita graficamente, mas se a peça publicitária for divulgada dias após um ataque terrorista ao *World Trade Center*, por exemplo, o sentimento negativo pode "contaminar" a imagem de sua empresa.

AUTORA

Lilian Ferracini, Jornalista, Especializada em Gestão de Mercado pela FGV – Fundação Getúlio Vargas.
Contato: lilianviviane.ferracini@gmail.com

3. ARMAZENAMENTO E DISTRIBUIÇÃO DE INSUMOS E PRODUTOS

SAIBA COMO GARANTIR A SEGURANÇA DO ARMAZENAMENTO E DA DISTRIBUIÇÃO DE SEUS PRODUTOS

No atual momento de crise provocado pela pandemia do novo coronavírus, é esperado que haja um aumento do material armazenado nas empresas, seja pela dificuldade na distribuição, seja pela falta de mão de obra ou de destinatários com capacidade limitada de recebimento. O problema é que esse alto volume de carga amontoados em depósitos gera uma série de desdobramentos, como o crescimento do risco de roubo de materiais de valor e a maior exposição de trabalhadores a produtos contaminados pelo vírus.

Por esses motivos, é fundamental que as mercadorias sejam separadas e protegidas, especialmente insumos hospitalares ou equipamentos usados no combate à COVID-19, como máscaras, ventiladores, testes e álcool em gel e medicamentos que tenham conexão com a profilaxia ou tratamento da doença, além de insumos para o agronegócio e para a produção de alimentos. Também é essencial que os depósitos tenham a segurança reforçada, os colaboradores cumpram medidas de proteção - como higienização das mãos, e uso de luvas e máscaras – e a atenção com as medidas de controle, preenchimento de inventários e alocação de produtos seja redobrada. Qualquer relaxamento na execução desses produtos pode abrir margem para a ocorrência de possíveis furtos e desvios.

Em todos os cenários, é comum planejar o sistema de proteção levando-se em consideração o contexto externo, porém, em um momento como esse, é extremamente importante pensar no contexto interno de risco e focar em quais partes dos processos e quais atores neles envolvidos poderão romper a cadeia de segurança e proteção.

Agora que você já sabe quais medidas protetivas deve tomar para garantir o armazenamento seguro dos seus produtos, é hora de conhecer as normas que podem garantir a segurança da distribuição dos seus insumos. No cenário atual de restrições e confinamento, a área de transporte é a mais crítica. Medicamentos e material de higienização, equipamentos de proteção individual, insumos para fábricas e serviços de transporte para compras online não podem parar. Porém, os cuidados com os funcionários envolvidos e o manuseio correto das cargas devem ser observados para que não haja casos de contaminação. Um colaborador contaminado pelo vírus pode ter contato com outros funcionários e, inclusive clientes, causando um forte impacto na operação e até mesmo na imagem da empresa.

Além das medidas de armazenamento já mencionadas, há outras recomendações aplicáveis ao processo de distribuição e transporte de mercadorias. O plano de gerenciamento de riscos da carga em trânsito, por exemplo, deve prever as medidas de proteção necessárias para preservar altos valores em circulação.

Em razão do volume liberado e da urgência dos clientes em receber as mercadorias, gargalos no recebimento de destino, como filas na descarga e falha na conferência de entrega, devem ser esperados. Um plano simples, mas objetivo, deve ser feito com antecedência, considerando o alinhamento com o recebedor final e os outros atores envolvidos.

Antecipar-se e rever os planos de gerenciamento de riscos com a seguradora a fim de enfrentar o retorno à normalidade também é indispensável. Neste novo cenário, haverá um crescimento no número das viagens e no volume de distribuição, aumentando as oportunidades na estrada para roubos de carga e aumentando a quantidade de veículos monitorados nos grids das centrais, para quem conta com esse serviço.

AUTORES

Maciel Lastoria, LatAm Safety and Security Head at Diebold Nixdorf.
Contato: maciel.lastoria@dieboldnixdorf.com
Maurício de Faria, DSE, CRMP. Gerente de Inteligência da Sensitech.
Contato: mauricio.defaria@carrier.com

4. SEGURANÇA PESSOAL

22 DICAS PARA GARANTIR A SUA SEGURANÇA PESSOAL, A DO SEU PATRIMÔNIO E A DA SUA EMPRESA

Neste momento, praticamente todas as atenções estão voltadas para as questões relativas à COVID-19, o que provoca tensão, incertezas e alterações nas emoções e na capacidade de tomada de decisão das pessoas.

Isto aumenta a possibilidade dos crimes de estelionato, golpes e fraudes de um modo geral e, embora o crime de extorsão mediante sequestro não esteja causando uma preocupação em nosso país, dadas as medidas de repressão a este tipo de problema, as orientações que daremos a seguir contribuirão para reduzir ainda mais os riscos à sua proteção e à dos seus colaboradores. Confira:

Ameaças às pessoas de forma indiscriminada:

1. Caso necessite sair de casa, mantenha especial cuidado ao chegar e sair de sua residência – atenção a atitudes suspeitas por parte de qualquer pessoa;

2. Revise o que você transporta. Lembre-se de que ao ter consigo objetos e documentos importantes, tenderá à reação, o que pode piorar a situação;

3. Falar ao celular enquanto caminha ou dirige amplia bastante os seus riscos – *smartphones* são potencialmente objetos de grande interesse por parte de criminosos. Oriente a sua família sobre este risco;

4. Ao dirigir, mantenha sempre vidros fechados, portas travadas e distância do veículo à sua frente. Ao utilizar transporte público, mantenha bolsa, mochila e carteira à sua frente, sempre sob sua vigilância;

5. Para saques em caixas eletrônicos, assegure-se de que não há ninguém em atitude suspeita por perto e não aceite ajuda de estranhos;

6. O confinamento (distanciamento social) fez elevar o uso da internet com mais frequência e intensidade. Abra apenas links que você tenha absoluta confiança, mantenha muita atenção quanto à proteção das suas senhas e obtenha informações mais acuradas a respeito dos aplicativos sugeridos. Mais do que nunca é importante você proteger as suas informações pessoais, sobretudo as disponíveis nas redes sociais. De posse dessas informações os criminosos praticam extorsões diversas. Oriente a sua família quanto a esses cuidados;

Ameaças às pessoas de forma seletiva:
As ações governamentais, que estimulam o confinamento diante da COVID-19, causam impactos na circulação das pessoas, o que colabora para uma possível diminuição dos crimes de roubo em via pública e, possivelmente, uma redução dos indicadores no tráfico de entorpecentes. Por outro lado, há a possibilidade de invasão a residências por conta do aumento das atividades na modalidade "*delivery*" e falsas prestações de serviços. Veja como você pode se proteger adotando estas simples precauções:

1. Certifique-se da procedência daquilo que foi solicitado sobre identificação do condutor e da mercadoria a ser recebida antes de facilitar seu acesso;

2. Tenha cuidado com visitas de supostos prestadores de serviços, inclusive de órgãos públicos (vigilância sanitária, vacinação itinerante e outras). Exija a identificação dos colaboradores e a documentação oficial de seus respectivos órgãos antes de aceitar qualquer tipo de acesso;

3. Crie um procedimento para avaliar o momento exato de receber um *delivery* e só o faça quando o local estiver seguro (criminosos podem se aproveitar de uma vulnerabilidade criada para invadir uma residência nos momentos de entrega).

Caso a empresa possua serviços de segurança pessoal privada:

1. Crie canais de comunicação com seu time de segurança pessoal. Estabeleça o compartilhamento de informações importantes: ocorrências nos bairros onde residem os executivos, ocorrências na região de seus respectivos escritórios e fábricas, bem como aquelas nos itinerários diários de deslocamento para o cumprimento das agendas, ainda que elas estejam restritivas neste momento;

2. Ainda que as agendas dos executivos estejam restritas, mantenha os profissionais de proteção executiva (VSPPs – Vigilantes em Segurança Pessoal Privada) preparados e estrategicamente alocados (nas residências, por exemplo) para que a logística em casos de deslocamentos seja a mais prática possível. Mantenha esse mesmo procedimento para os motoristas executivos;

3. Considere a possibilidade de utilizar o VSPP embarcado (na função de motorista) a fim de viabilizar com maior rapidez os deslocamentos com um nível de segurança aceitável para a atual situação;

4. Mantenha os canais de comunicação com secretárias executivas e outros serviços de apoio, ainda que estejam trabalhando remotamente;

5. Reforce seu Centro de Controle Operacional (local ou da matriz), bem como seu parceiro contratado para a proteção de executivos e expatriados quanto às contingências que estão sendo adotadas por parte de sua empresa. Estabeleça pontos de apoio mútuo em casos de ocorrências (seu CCO e o Parceiro, por exemplo, na resposta a um alarme de pânico) no intuito de reforçar monitoramento e pronta resposta em casos de emergência;

6. Considere a possibilidade de reforço na sua estrutura de proteção pessoal, procedendo a potencial contratação de VSPPs e a incorporação de veículos blindados;

7. Promova inspeções técnicas nos sistemas de segurança: controles de acesso, iluminação, câmeras, muros, armazenamento e distribuição de imagens, fechaduras e controle de chaves e senhas;

8. Prepare cenários de contingências em decorrência de eventual contaminação pela COVID-19 dos executivos e sua estrutura de proteção pessoal;

9. Crie um plano de contingências para o transporte das equipes de proteção pessoal, em caso de interrupção nos serviços de transporte público;

10. Assegure-se da disponibilidade de insumos de proteção sanitária às equipes, bem como o rigor na sua utilização;

11. Alinhe com seu time de Centro de Controle de Operações (CFTV, telefones de emergência, sistema de controle de acesso etc.) ações de monitoramento e rastreamento;

12. Verifique a possibilidade de contratação de monitoramento remoto de seus sistemas eletrônicos de segurança;

13. Estabeleça um contato mais frequente com os órgãos de segurança pública de sua região (Polícia Militar, Civil, Guarda Civil) no sentido de proporcionar apoio mútuo em emergências.

AUTORES

Diógenes Viegas Dalle Lucca, MSc, Tenente-Coronel Veterano da Polícia Militar do Estado de São Paulo. Especialista em Gestão de Crises e Proteção Executiva.
Contato: lucca@thefirst.com.br
Leandro Fortes, Gerente de Segurança Corporativa da Mercedes Benz do Brasil.
Contato: leandro.fortes@daimler.com
Roberto Zapotoczny Costa, MSc, empresário. Especialista em Gestão de Crises e Proteção Executiva.
Contato: robertocosta@thefirst.com.br

5. SEGURANÇA PRIVADA

DESCUBRA COMO A SEGURANÇA PRIVADA PODE SER ALIADA DA SUA EMPRESA NO COMBATE AOS RISCOS CAUSADOS PELA COVID-19

Os serviços de proteção da integridade física das pessoas e do patrimônio, conhecidos como segurança privada, são regulamentados no Brasil pela Lei nº 7.102/83 que, por meio do Ministério da Justiça e do Departamento da Polícia Federal, disciplina as atividades de vigilância (armada ou desarmada), transporte de valores, segurança pessoal privada (*bodyguard*), escolta armada e cursos de formação de vigilantes.

A legislação atual é obsoleta perante os anseios da sociedade, porém, as empresas prestadoras de serviços de segurança têm se adaptado na tentativa de trazer ao cliente o que há de melhor em serviços de vigilância, aliados às melhores práticas mundiais e à tecnologia de ponta. A legislação supracitada descreve os requisitos mínimos para o exercício da profissão de vigilante, como idade, formação, reciclagem, exigência de não ter condenação criminal etc.

Na indústria, as principais funções desempenhadas pelo vigilante são prevenir riscos, proteger vidas e patrimônio, promover a revista em pessoas e veículos, realizar rondas (inspeções) nas áreas internas, combater princípios de incêndio, realizar os primeiros socorros, controlar o acesso de pessoas e materiais, entre outras. Em muitas delas, os vigilantes têm ainda a missão da segurança pessoal, acompanhando diariamente a rotina dos executivos e de suas famílias.

A COVID-19 que atingiu o mundo no final de 2019 e foi constatada no Brasil em 26 de fevereiro de 2020 trouxe problemas não só para o sistema de saúde, mas também para a economia, a logística, a justiça, as relações internacionais e a segurança. Quando dizemos segurança, nos referimos ao sentido mais amplo que podemos pensar, desde a defesa nacional, a segurança pública e a segurança privada (*security*) até a autodefesa do próprio cidadão.

Em um contexto extraordinário de mobilidade nacional, o papel da segurança privada torna-se ainda mais importante. O contingente de vigilantes trabalhando em 2018 era de 553.900. Destes, 31,3% estavam situados apenas no estado de São Paulo. Dados do IBGE sobre o Perfil dos Estados e dos Municípios Brasileiros indicam que, em 2013, o Brasil tinha o efetivo de 425.248 policiais militares. Já as Forças Armadas, somam 327 mil militares na ativa, de acordo com informações da Global FirePower.

Os vigilantes são profissionais habilitados e capacitados para manusear armas de fogo, possuem experiência na proteção de bens e pessoas e são um reforço às forças de segurança pública. Em épocas de crise e instabilidades, tornam-se indispensáveis. Em alguns países, em caso de guerra ou graves crises, a segurança privada chega a assumir algumas atividades antes exclusivas da segurança pública.

No contexto atual, a gestão da indústria deve somar esforços junto à liderança da empresa de segurança privada para garantir que as equipes sejam revistas de modo a protegerem as sedes, os centros de distribuição, os escritórios e os galpões de armazenamento. Sendo necessária a ampliação emergencial das equipes, permanece a necessidade de que os postos de vigilância sejam cobertos

por profissionais habilitados e treinados para a operação, uma vez que uma crise desse porte tende a aumentar os riscos contra o patrimônio.

Neste momento, a segurança privada é necessária para garantir a ordem na indústria, preservar o patrimônio e ajudar a restaurar o *status* de normalidade da forma mais rápida possível. A necessidade de manutenção dos serviços de segurança é vital para a indústria. Recomenda-se muita cautela na redução de postos de vigilantes e sistemas de apoio à segurança. Uma economia hoje pode representar uma perda maior num futuro próximo.

Novas análises de risco se fazem necessárias para adaptar as equipes à realidade emergencial. Iniciar o plano de contingência também demanda, via de regra, realocação das equipes, que deixam de ser necessárias em alguns pontos e passam a ser fundamentais em outros. Toda e qualquer redução de escopo deve ser embasada por uma análise de risco, realizada por profissional com expertise e técnica para avaliação com base na norma ISO 31.000.

Nas negociações entre a indústria (contratante) e empresa de segurança privada (contratada), deve-se ter claramente a composição dos custos de um posto de vigilante, levando-se em conta salários, benefícios, insumos, taxa de administração, equipamentos e impostos. Para que as negociações ocorram na rigidez que o momento exige, mas no limite do equilíbrio financeiro entre as partes.

Veja 10 medidas de segurança privada que você deve colocar em prática durante a pandemia da COVID-19:

1. Ative o Plano de Contingência. Na falta de um, reavalie os riscos contra a segurança da indústria no cenário de pandemia, bem como os sistemas de proteção para tratamento das ameaças;

2. Reforce a segurança das áreas de armazenamento de produtos acabados ou insumos de interesse, com a devida atenção para produtos que se tornaram visados neste momento de crise, como medicamentos, equipamentos médicos, produtos de higienização, EPI, alimentos, entre outros;

3. Tendo em vista o possível aumento de demissões e renegociações de salários, estresse mental e problemas financeiros, dê ainda mais apoio às ações das áreas de Recursos Humanos, Departamento Pessoal e Segurança, Saúde e Meio Ambiente;

4. Fique atento ao aumento dos riscos de incêndio no armazenamento de materiais;

5. Mantenha atualizados os planos de chamada, contingências e de auxílio mútuo;

6. Suprima a operação saque nos caixas eletrônicos ou postos bancários;

7. Conheça a saúde financeira da empresa de segurança contratada a fim de evitar o pagamento futuro de responsabilidade subsidiárias;

8. Solicite à empresa de segurança as opções de escalas de serviços para garantir o efetivo mínimo na unidade, assim como os planos de contingências para casos de falta de colaborador, supressão do serviço público de transporte e tratamento dos colaboradores com COVID-19;

9. Cumpra a previsão contratual de aviso prévio com antecedência, uma vez que o maior custo das empresas de segurança são salários, encargos e tributos. Não esqueça que elas terão que cumprir aviso de 30 dias com os seus colaboradores;

10. Junto à seguradora, atualize qualquer mudança no plano de gerenciamento de risco.

Já passamos por outros períodos difíceis. Temos certeza de que também sairemos deste, e com segurança.

AUTORES

Michel Pipolo de Mesquita – Vice-presidente da ABSEG e Diretor do Grupo GPS.
Contato: michel.pipolo@gpssa.com.br
Roberto Coletti – Presidente da ASIS/Chapter Rio e Diretor da Verzani & Sandrini.
Contato: roberto.coletti@verzani.com.br
Tatiana Diniz, CPP, ASE – Presidente da Comissão Especial de Segurança Privada da OAB/SP e Diretora da Cadiz Segurança.
Contato: tatiana@cadiz.com.br

6. SEGURANÇA CIBERNÉTICA

HOME OFFICE COM SEGURANÇA: VEJA 10 MANEIRAS DE PROTEGER AS INFORMAÇÕES COMPARTILHADAS NO MUNDO VIRTUAL

Com o crescimento do número de pessoas fazendo home office, usando softwares de videoconferência e acessando e-mails de casa, indivíduos e corporações tornaram-se mais vulneráveis a ataques cibernéticos. Entretanto, a adoção de controles e ações básicas por parte de empresas e colaboradores pode garantir a segurança dos sistemas operacionais e das informações compartilhadas no mundo digital. Veja dicas de como evitar a materialização de riscos virtuais e/ou mitigar seus impactos.

1. O BACKUP PODERÁ SALVAR O SEU NEGÓCIO

Realize regularmente o backup de todas as informações importantes para o seu negócio e para a sua vida. Lembre-se que muitos processos de seu negócio e recordações da sua vida estão armazenados em meios digitais. Você já refletiu sobre quanto custaria a perda de todos esses dados?

2. SENHAS FORTES, INDIVIDUAIS E INTRANSFERÍVEIS

Sua senha é o que te representa no mundo digital. Garanta que ela seja forte, utilize a regra de quanto maior, melhor. Ser forte não significa ser difícil, utilize uma frase que seja simples de recordar. E lembre-se, a senha deve ser individual para cada sistema e intransferível, você não poderá emprestá-la. Quando possível, ative a autenticação de dois fatores em todos os sistemas e sites que solicitarem senha.

3. MANTENHA-SE ATUALIZADO

A maioria dos ataques acontecerá por falhas em softwares que você utiliza. Por isso, garanta que os softwares de todos os seus dispositivos – computador, *smartphone*, *access point*, roteador *wireless*, e *smart TV*, estejam atualizados.

4. O ANTIVÍRUS AJUDARÁ NA SUA PROTEÇÃO

Mantenha um antivírus instalado e atualizado no computador de sua casa, no computador de sua empresa e em seus dispositivos móveis, como *smartphone* e *tablets*. Em sua empresa, garanta que a proteção do antivírus esteja ativa para e-mail e acessos à internet.

5. PROTEJA A SUA REDE WI-FI

Na empresa ou em casa, garanta a segurança de sua rede. Utilize o padrão de proteção WPA2 em conjunto com uma senha forte para a rede WI-FI. Evite acessar redes WI-FI públicas e desconhecidas, mas se precisar acessá-las, utilize sempre uma solução de VPN.

6. CRIPTOGRAFIA PARA PROTEGER O QUE É IMPORTANTE

Assegure-se de que todas as informações sensíveis contidas nos computadores e nos dispositivos móveis de sua empresa e sua casa estejam criptografadas.

7. PROTEJA-SE AO USAR SOFTWARES DE COMUNICAÇÃO INSTANTÂNEA E E-MAILS

Se você utiliza softwares de comunicação instantânea como WhatsApp e Telegram, não esqueça

de ativar a verificação em duas etapas. Evite entrar em grupos e abrir arquivos ou links duvidosos. A mesma orientação vale para e-mails com anexos e links enviados por desconhecidos. Na dúvida, não abra.

8. TENHA CUIDADO AO USAR SOFTWARES DE VIDEOCONFERÊNCIA

Devido à grande demanda de uso, estão sendo identificadas novas vulnerabilidades que podem permitir a invasão de seu computador e o roubo de suas informações. Certifique-se de que a última versão do programa esteja sendo utilizada e evite abrir links e arquivos de terceiros enviados pelo software de videoconferência.

9. COMPRAS PELA INTERNET COM SEGURANÇA

Antes de concretizar qualquer compra pela Internet, garanta que ela seja realizada pela plataforma (site ou aplicativo) do vendedor. No caso de compra pelo navegador de internet, verifique a utilização de um certificado digital confirmando se o site inicia com *https* e se possui o ícone de um cadeado próximo da url. Desconfie se o preço do produto vendido for muito menor do que o valor de mercado. Em caso de dúvida, entre em contato com o fornecedor.

10. PROTEJA-SE AO USAR AS REDES SOCIAIS

Nas redes sociais, verifique os controles de privacidade e defina-os para que apenas seus amigos e familiares possam ver todos os seus detalhes. Não insira muitas informações pessoais em suas contas de redes social. Lembre-se de nossas dicas sobre senhas. Se você compartilhar fotos dos seus animais, não utilize o nome deles como senha.

AUTOR

Ricardo Ribeiro Tavares – CISM, CRISC, CGEIT, CGIH, GPEN, ISO 27001 Lead Auditor, TOGAFC. Especialista em segurança cibernética e forense digital. Coordenador e professor do curso de pós-graduação em segurança cibernética na Faculdade Impacta e diretor da consultora GEMINA Threat Intelligence.
Contato: ricardo@tavares.io

7. SEGURANÇA DE CONDOMÍNIOS INDUSTRIAIS LOGÍSTICOS E EMPRESARIAIS

CONHEÇA ALGUNS CUIDADOS PARA MANTER SEU SISTEMA INTEGRADO DE SEGURANÇA ATUALIZADO E QUALIFICADO PARA PROTEGER SEU CONDOMÍNIO INDUSTRIAL

A incerteza causada pela proliferação da COVID-19 causou impactos na segurança das pessoas e dos patrimônios. Contudo, a adoção de algumas medidas preventivas e a execução de algumas respostas imediatas podem ajudar as empresas a gerenciar a atual crise e preparar-se para responder às consequências da pandemia e manter as atividades rotineiras com segurança. Dentre todas essas medidas, destaca-se a adoção de um Sistema Integrado de Segurança (SIS), e é sobre ela que jogaremos luz neste artigo. Sua empresa conhece as premissas de um SIS e sabe como implementá-lo?

Confira o passo a passo da execução desta ferramenta que pode garantir a segurança dos condomínios industriais logístico e empresariais, a partir das perspectivas dos recursos humanos, recursos técnicos e recursos organizacionais.

RECURSOS HUMANOS

- **Serviços de vigilância, recepção e portaria:**
  1. Verifique se os EPIs utilizados pela equipe são adequados e se a higienização do posto de trabalho foi intensificada;
  2. Certifique-se de que os profissionais com postos na segurança, portaria e recepção estão respeitando a distância recomendada pelas autoridades;
  3. Nos casos de serviço próprio ou orgânico, assegure-se de que haja um plano de contingência formalizado, revisado, atualizado e que tenha sido previamente simulado**;**
  4. No caso de serviço terceirizado, solicite formalmente ao prestador de serviço um plano para a contingência de algum tipo de interrupção ou impedimento. Com o plano em mãos, teste sua eficácia, por meio da realização de simulações.

- **Treinamento:**
  1. Revise seus procedimentos de rotina e de contingência;
  2. Recicle sua equipe periodicamente.

- **Apoio individual:**
  1. Afaste das atividades os membros da equipe que estão no grupo de risco, apresentaram algum tipo de sintoma da COVID-19 ou vivem com familiares que foram contaminados;
  2. Mapeei as modalidades de transporte usadas pelos funcionários e ofereça uma alternativa àqueles que fazem o trajeto até o trabalho de transporte público;
  3. Atente-se ao processo de seleção (*assessment* e *background checking*) e capacitação de novos colaboradores. Um processo de avaliação cíclica de conhecimento é recomendado através da aplicação de simulações verbais ou de surpresa e auditorias, que abordem as pessoas de todos os turnos.

BARREIRAS FÍSICAS

1. Certifique-se de que sua barreira perimetral está em ordem, e de que vistorias foram realizadas conforme o prazo estabelecido. Tenha em mãos os relatórios de cada uma das vistorias;
2. A segurança de locais que sofreram redução das atividades está adequada? Eles contam com ronda e cobertura por sistema de alarme e/ ou imagens de CFTV?
3. Lance mão de bloqueios físicos, como grades, tapumes, cavaletes, cordas e cones, para em casos de manifestação desordenada.

RECURSOS TECNOLÓGICOS

1. Analise a fonte de fornecimento de iluminação e certifique-se se alternativas devem ser adotadas. Faça o mesmo para iluminação de emergência e de reforço;
2. Garanta que o alarme perimetral, o controle de pedestres e veículos, o circuito fechado de TV e o monitoramento remoto estão funcionando. Teste esses recursos periodicamente e tenha um técnico residente, peças sobressalentes ou assistência técnica para o caso de eles apresentarem falhas. Também tenha alternativas na manga para o caso de eles entrarem em pane e mantenha um back-up de dados e imagens. No caso de impedimento da sua Central de Comando e Controle, identifique empresas que possam servir de *backup* ou reforço para manutenção de imagens de segurança (*Cloud*) e monitoramento;
3. Verifique a rotina de abastecimento do seu gerador e teste-o regularmente, assegurando o pleno atendimento aos pontos de segurança.

RECURSOS ORGANIZACIONAIS

1. Revise ou elabore uma Análise dos Riscos de seu negócio. Ela deve estar atualizada e seguir os critérios da norma ISO 31.000;
2. Teste regularmente um plano de contingências que siga a Norma ISO 22.390 e preveja interrupções de processos críticos capazes de impedir a execução dos serviços;
3. Elabore um Plano de Auxílio Mútuo (PAM). Busque contato com prédios e condomínios vizinhos para estabelecer formas de apoio integrado entre os participantes (ambulância, estacionamento, bombeiros, comunicação, imagens etc.);
4. Acompanhe as ocorrências (livro de ocorrência e passagem de serviço (impresso ou informatizado);
5. Assegure que os dados cadastrais dos funcionários, usuários, fornecedores e demais necessários estejam atualizados;
6. Elabore um sistema e uma forma de comunicação centralizada e unificada junto ao público interno.

AUTORES

Eytan Magal – Sócio Diretor da Eytan Magal – Risks & Secutity solutions.
Contato: em@eytanmagal.com.br
João Jaouiche – Consultor em Segurança Empresarial – ADS.
Contato: jj@nucleoconsult.com.br
Laércio Soares – Empresário da área de tecnologia e segurança logística.
Contato: laercio@emepar.com.br
Marcela Vasconcellos – Gestora de Facilities – Ecorodovias/Concessões.
Contato: marcella.vasconcelos@ecorodovias.com.br
Marcy José Campos Verde, CPP, ADS – Consultor sênior em segurança empresarial.
Contato: falecom@marcy.com.br

8. GESTÃO DE CONTINUIDADE DE NEGÓCIOS

GESTÃO DE CONTINUIDADE DE NEGÓCIOS: COMO ADMINISTRAR SUA EMPRESA EM ÉPOCAS DE CRISE

Uma organização precisa estar preparada para situações adversas, como crises ou desastres, protegendo vidas, patrimônio e garantindo sua sobrevivência. Diante de incertezas em relação ao desenvolvimento de uma vacina capaz de prevenir os indivíduos do novo coronavírus ou de um medicamento capaz de tratar pessoas contaminadas pela COVID-19, é difícil prever quando as atividades serão retomadas na sua totalidade. Contudo, os negócios não podem parar. Fazer uma gestão de continuidade de negócios nunca foi tão fundamental como agora. Veja como o emprego de algumas ações simples podem proteger sua empresa de dificuldades e prepará-la para o retorno à normalidade.

1. **Estabeleça uma Equipe de Gerenciamento de Crises (EGC)**. É recomendável a participação da Presidência, Comunicação, Recursos Humanos (RH), Jurídico, Tecnologia da Informação (TI), Segurança da Informação e Cibersegurança, Vendas/Relacionamento com Clientes, Seguros, Produção/Indústria/Fábrica(s), Logística, Segurança Empresarial e Saúde (leia o artigo "Entenda o que é um comitê de gerenciamento de crises e como ele pode ajudar sua empresa a enfrentar momentos de instabilidade");

2. **Institua um Centro de Operação de Emergência (COE).** O COE, presencial ou remoto, deverá ser o meio oficial de relacionamento da EGC, ponto focal para a comunicação, centralização da tomada de decisões e relacionamento com as autoridades e a imprensa;

3. **Defina uma liderança para a crise.** Um líder e um substituto precisam ser definidos, e isto vale para todos os membros da EGC. No caso de reuniões do COE ocorrerem presencialmente, não esqueça de cumprir as recomendações sanitárias de distanciamento social;

4. **Ative o Plano de Continuidade (PCN).** Caso tenha um PCN, contendo Planos de Gerenciamento (PGC) e de Comunicação em Crises (PCOM), inicie a ativação dessas ferramentas;

5. **Realize reuniões diárias da EGC**. Atualize a liderança sobre estatísticas e fatos relacionados à pandemia, à situação dos colaboradores, e às reinvindicações de clientes, governo e outras partes interessadas;

6. **Prepare um Plano de Comunicação em Crises (PCOM)**, **caso não tenha um**. Defina um porta-voz e mantenha consistência. Atente-se aos fatos, siga as orientações das autoridades de saúde e defina os canais de comunicação oficiais da organização;

7. **Realize reuniões semanais com os colaboradores**. Comunique-se adequadamente, de forma clara e objetiva, minimizando boatos e informações não oficiais sobre a organização. Transmita uma mensagem positiva e otimista;

8. **Promova o distanciamento social para minimizar o contágio.** Em casos pandêmicos, ofereça condições para trabalho remoto *(home office)*. Ensino ou atendimento a distância também é recomendável e estratégico;

9. **Identifique pessoal crítico**. Liste os colaboradores que são fundamentais para determinadas funções ou atividades e que fazem parte do grupo de risco informados pelas autoridades de saúde. Prepare substitutos para essas funções e monitore periodicamente;

10. **Avalie proteção e benefícios emergenciais**. Antecipação de período de férias e antecipações de salários e verbas adicionais de ajuda podem ser necessárias. Se possível, prepare um *kit* de proteção (máscara, luvas descartáveis e álcool em gel) para os colaboradores e suas famílias;

11. **Prepare o atendimento presencial.** Para equipes que precisam continuar interagindo presencialmente com os clientes, recomenda-se distribuir máscaras e álcool em gel, realizar limpeza constante dos locais e orientar para o distanciamento social. Se possível, instale barreiras de proteção entre atendentes e clientes;

12. **Contate os principais clientes.** Entre em contato com os principais clientes semanalmente, e lhes dê apoio e suporte. Entenda as necessidades específicas de cada um, identificando oportunidades e mantendo os negócios atuais durante a crise;

13. **Mapeie impactos nos clientes, por segmento.** Reavalie riscos e prováveis impactos decorrentes da paralisação e desaceleração socioeconômica causadas pela crise. O alinhamento das informações entre as equipes de Vendas e Financeiro é fundamental;

14. **Ajuste a logística para a crise.** É recomendável uma avaliação de riscos completa da cadeia de suprimentos, bem como adaptações para o recebimento e o atendimento aos principais clientes, mantendo entregas que garantam o fluxo de caixa;

15. **Projete impactos financeiros.** O Financeiro deve informar imediatamente a EGC acerca de projeções de reservas e impactos para os próximos 3, 6 e 12 meses, sempre orientadas ao "pior cenário";

16. **Prepare recursos financeiros de emergência**. Identifique fundos de reserva já existentes, seguros, linhas de emergência e crédito governamentais, opções para protelamento de impostos e renegociações de pagamentos. Liste despesas não essenciais para suspensão, valide necessidades de conformidade legal e regulamente as obrigatórias;

17. **Promova a resiliência e a sobrevivência da organização.** A EGC deve manter a viabilidade econômica da organização e estudar possíveis acelerações de projetos que possam trazer recursos e receitas durante e após a crise.

AUTOR

Jeferson D'Addario – CBCP, CRISC, ISO 22301 e 27001 Lead Auditor. Representante e Instrutor do Disaster Recovery Institute International, coordenador e professor de MBA em Gestão de Riscos, Continuidade de Negócios e Segurança da Informação. CEO e sócio da DARYUS Consultoria e Treinamentos. Contato: jeferson@daryus.com.br

9. SEGURANÇA DA INFORMAÇÃO

ENTENDA POR QUE CRIAR UM PROGRAMA ORGANIZACIONAL DE SEGURANÇA DA INFORMAÇÃO NA SUA EMPRESA

Com o surgimento da pandemia da COVID-19, a maioria das organizações mostrou fragilidade na implantação de controles que poderiam garantir uma funcionalidade operacional menos traumática. A organização deve ter controles estruturados aprovados pelo seu corpo diretivo e capazes de absorver impactos de ações criminosas e enfrentar situações de indisponibilidade de recursos.

A informação é um dos fatores críticos para a existência, operacionalização e planejamento de qualquer organização. Portanto, a segurança da informação é um controle organizacional que deve abarcar não apenas a tecnologia, mas também os colaboradores, os clientes e o mercado. A existência de um Programa Organizacional de Segurança da Informação é responsabilidade do Corpo Diretivo.

Os controles descritos neste artigo formam um conjunto mínimo e prioritário de ações que deve fazer parte de um plano estruturado de segurança da informação. Veja como dar o primeiro passo e estabelecer uma estrutura adequada de proteção das informações dentro da sua empresa.

Confira algumas sugestões de ações e procedimentos:

1. Somente usuários colaboradores (funcionários, prestadores serviços) e usuários clientes ativos e válidos deverão estar na lista de usuários autorizados a acessar informações compartilhadas pela empresa;

2. A comunicação remota dos usuários colaboradores deve ser realizada utilizando um canal seguro, tipo padrão técnico VPN, que impede que criminosos interfiram nesta comunicação;

3. O equipamento utilizado pelo usuário colaborador é equipamento profissional da organização ou autorizado pela organização com programas padrões da organização;

4. Os horários de acesso permitidos para os usuários colaboradores devem ser controlados, considerando a sua função e a sua relação profissional com a organização. Monitore este comportamento de uso;

5. Se existe uma Central de Atendimento para o Usuário Colaborador, coloque nesta central os melhores profissionais de suporte técnico e de negócio. O usuário não pode ter dúvidas;

6. Certifique-se de que somente programas e produtos autorizados pela organização estão implantados nos computadores utilizados pelos usuários e de que suas versões estão atualizadas;

7. Verifique se existem cópias de segurança (backups) atualizados no ambiente centralizado. Não devem ser permitidas cópias nos equipamentos remotos utilizados pelos usuários colaboradores;

8. Os programas e produtos utilizados pela organização devem ser na modalidade corporativa (paga). Não permita o uso desses serviços na opção gratuita;

9. Oriente seus usuários colaboradores a utilizarem a autenticação em duas etapas. Ela deve ser realizada de quatro em quatro horas;

10. Ofereça um treinamento sobre prática de segurança da informação no formato EAD para o usuário colaborador;

11. Os Gestores da Informação são obrigados a revisar a cada 30 dias a autorização de acessos a sistemas, programas, aplicativos, transações, pastas e demais recursos de informação;

12. Certifique-se da conformidade com a Lei de Proteção de Dados Pessoais – LGPD, concluída ou em andamento, com cronograma de conhecimento do Corpo Diretivo;

13. Reforce a Gestão de Riscos de Segurança da Informação, considerando os controles de tratamento da informação, continuidade do negócio e dependência com os fornecedores;

14. Atualize ou crie os Planos de Continuidade de Negócio. Certifique-se de que eles cobrem todos os ambientes de informação e são testados a cada período máximo de 12 (doze) meses;

15. Seu negócio conta com uma efetiva Gestão de Incidentes? Reportes semanais para o Corpo Diretivo e reportes diários para os gerentes e os superiores são fundamentais. Caso, esses processos não existam em sua empresa, esta é uma boa hora para criá-los;

16. Existem regulamentos de segurança da informação na sua organização? Não existindo, emita um documento emergencial definindo os principais controles obrigatórios de segurança da informação;

AUTOR

Edison Luiz Gonçalves Fontes – CISM, CRISC, CISA, Ms, Gestor, Professor e Consultor em Segurança da Informação e Proteção de Dados Pessoais. Sócio Consultor da Núcleo Consultoria.
Contato: edison.fontes@uol.com.br

10. INVESTIGAÇÕES CORPORATIVAS

APRENDA A CONDUZIR UMA INVESTIGAÇÃO CORPORATIVA EM UM CENÁRIO DE CRISE

Em tempos de crise, é comum sermos bombardeados por uma enxurrada de dados e informações. Por isso é tão importante que o comitê de crise tenha discernimento para tomar decisões coerentes, amparadas em fatos e fontes fidedignas, a fim de evitar erros ou desgastes desnecessários para a corporação. Em cenários de crise, é recomendado que as empresas iniciem um processo de coleta de dados, análise de riscos e estudo de cenários. Mesmo em momentos como este, denúncias ou suspeitas internas de irregularidades devem ser investigadas e falhas, apuradas.

Devemos entender que o tomador de decisão não tem muito tempo para decidir. Normalmente, a janela de tempo para as ações necessárias é muito curta, e cada etapa decisória acaba sendo validada com a melhor informação disponível naquele momento. A informação vigente é aquela que serviu a um propósito, mesmo que momentâneo, podendo ser alterada quando outras informações puderem ser obtidas.

Portanto, o tomador de decisão deve ser moderado na intensidade de suas ações quando a informação vigente criar condicionantes que exijam grandes recursos que, se não estiverem sendo direcionados para o vetor correto da crise, podem limitar as ações corretivas necessárias a um ajuste de rumo futuro.

Moderação não é hesitação, mas sim, o cuidado necessário que se deve tomar em qualquer plano de ação. Estamos vivenciando um momento caótico, de muitas incertezas. Ele exige que a coleta de dados e as análises decorrentes produzam informações consistentes para o tomador de decisão enquanto o Comitê de Crises estiver trabalhando.

Para tanto, descrevemos a seguir o processo técnico de análise das fontes para validarmos os fatos recebidos.

- Quando um suposto fato nos chega, não importa o meio, primeiro deve ter sido observado por alguém, que pode apresentar parcialidade, expectativa e mesmo displicência em sua observação, o que influenciará a sua memorização e posterior descrição do fato, influenciando assim, muitos aspectos relevantes do mesmo;
- A fonte que descreveu o fato, gerando um dado, pode ser uma organização, uma pessoa ou um documento. Precisamos então avaliar sua autenticidade, competência e confiança através de seus antecedentes, vida, contribuição e motivação para formarmos um julgamento de valor;
- Partindo do fato que gerou um dado que foi avaliado quanto ao valor, precisamos agora julgar o conteúdo. Saber se existe semelhança, coerência e compatibilidade deste dado com outros previamente conhecidos ou validados;
- Após termos julgado a fonte e o conteúdo, podemos creditar um grau de credibilidade para o fato relatado, gerando um informe. A informação pode ser produzida através da somatória de vários informes com diferentes graus de credibilidade. Sendo assim, o conhecimento produzido deve responder às perguntas “O que? Quando? Como? Onde? Quem? Por quê?” e ser acompa-

nhado de uma análise final do grau de certeza para que o tomador de decisão possa avaliar os riscos das ações a serem tomadas.

Não basta obter dados ou acumular informes, uma investigação requer capacidade técnica na análise do fato ou denúncia, buscando as respostas e evidências, que servirão como base comprobatória, seja no âmbito legal ou para tomada de decisões.

AUTORES

Leonardo Simão – Diretor de Segurança-Latam da DSM Nutritional Products, especialista em Gestão de Crises e Segurança Corporativa.
Contato: leonardo.simao@dsm.com
Aureo Miraglia de Almeida – MBS, Consultor em Gestão de Riscos Operacionais e Investigações de Fraudes.
Contato: aureo745@gmail.com
Flávio Ainbinder – CPP, ASE, MBA, Executivo de Segurança.
Contato: fainbinder@hotmail.com

11. TECNOLOGIA EM SEGURANÇA

VEJA COMO ENFRENTAR OS RISCOS DE SEGURANÇA CAUSADOS PELA PANDEMIA DA COVID-19 EMPREGANDO TECNOLOGIA NOS PROCESSOS DE PROTEÇÃO PATRIMONIAL

Durante a crise provocada pela COVID-19, a segurança patrimonial poderá ser objeto de redução de custos em seu ponto mais sensível, o dos recursos humanos. Por esse motivo, é tão fundamental ter atenção aos recursos tecnológicos. Em épocas de crise como a que estamos vivenciando, eles são capazes de manter o equilíbrio do chamado tripé da segurança, formado pelos recursos humanos, os recursos organizacionais e os recursos tecnológicos.

Veja abaixo dicas de como enfrentar riscos de segurança causados pela pandemia do novo coronavírus e preparar o seu negócio para lidas com as consequências geradas por essa crise, sob o ponto de vista do emprego da tecnologia nos processos de proteção patrimonial.

BARREIRAS FÍSICAS

Como pode haver um aumento do risco de invasão para prática de furtos e da ocorrência de crimes de pequena escala e comportamentos antissociais, é necessário fazer a manutenção de muros e a limpeza da área, além de pinturas e cortes da vegetação.

PROTEÇÃO PERIMETRAL

Com a possibilidade de redução ou eliminação da ronda perimetral, é importante implementar um sistema de detecção de invasão através do sensoriamento do perímetro com monitoramento local e, se possível, remoto.

CONTROLE DE ACESSO

A portaria remota já é uma realidade em condomínios residenciais e comerciais. O mesmo princípio pode ser aplicado às empresas com automação parcial ou total das portarias. Com relação ao risco de contaminação por contato, há dispositivos de validação de identidade que minimizam essa possibilidade, como leitores de biometria sem contato ou por reconhecimento facial, além de catracas com dispositivos de abertura lateral. Sua empresa também pode considerar o fechamento de algum ponto de acesso, mesmo que temporário.

SISTEMA DE CFTV

As áreas que passaram por reconfiguração de layout e formas de utilização podem se tornar pontos críticos. Portanto, as câmeras do circuito fechado de televisão podem contribuir tanto para a detecção de uma ocorrência e a checagem de disparos de alarmes, quanto para a identificação de situações indesejadas através de análise de vídeo. O monitoramento remoto também pode ser uma contribuição importante na redução de custos, assim como no reforço a um sistema já existente.

SISTEMAS DE ALARME

O sistema de alarme precisa ser revisado e testado periodicamente. Identificar um sinistro no perímetro ou no ambiente interno deve fazer parte da estratégia da empresa. Ela deve levar em conta o risco, o tempo de resposta, e o custo x benefício de ampliar a área que precisa ser protegida. Mere-

cem atenção os recursos de retardo (ex: cortinas de fumaça) e a sua integração com aplicativos de auto monitoramento integrado às imagens.

SISTEMAS DE RASTREAMENTO E MONITORAMENTO PESSOAL

É importante prover o rastreamento de veículos com inteligência embarcada. Ele pode detectar algum comportamento ou rota anormal e fora da programação, e notificar os responsáveis para que a equipe de segurança possa tomar providências.

Para o monitoramento pessoal é necessária a instalação de aplicativos direcionados para essa atividade, proporcionando a rastreabilidade através do celular do executivo, assim como a possibilidade de acionamento da função Emergência/Pânico.

CENTRAL DE MONITORAMENTO

Centrais modernas precisam trazer a inteligência para dentro dos seus processos, automatizando todas as tarefas possíveis e reposicionando as pessoas para um papel mais analítico e otimizado. A detecção do problema ou do risco precisa ser feita pela máquina (nível 1), e o ser humano deve exercer o papel mais tático e estratégico (nível 2). Sob o ponto de vista da redução de recursos humanos, é necessário analisar a real necessidade de mantê-las nas dependências da empresa ou adotar um modelo novo de contratação remota, diluindo assim esse custo com outras empresas.

SISTEMA DE INFORMAÇÕES

A prestação de serviços não pode acontecer sem informações. Para tal, um bom sistema de informações é necessário para a sua gestão. Ele vai coletar dados e processá-los, além de gerar, armazenar e disseminar informações, com o objetivo de dar suporte à tomada de decisões, à coordenação, ao controle, à medição, à análise e à visualização do desempenho das entregas dos serviços.

Outro requisito importante para o sistema de informações é o fornecimento de subsídios para reflexões que possibilitem a saída dessa crise com boas lições aprendidas. Um caminho a ser trilhado pode ser a avaliação da situação atual, com o aparato tecnológico disponível, para que os melhores ensinamentos possam ser extraídos.

Reunir os dados gerados pelo aparato tecnológico e usar ferramentas próprias para analisá-los constituirá um ativo importantíssimo para os negócios. Estar à frente com inovações na segurança e na transformação digital da organização é outro grande passo para o enfrentamento da crise e a sua recuperação.

MEIOS DE COMUNICAÇÃO

Um ponto comum de vulnerabilidade a todos sistemas de segurança eletrônica são os meios de comunicação. Uma interrupção provocada deliberadamente de forma bastante simples pode tornar o sistema de proteção inoperante.

Com a evolução em capacidade e estabilidade das bandas largas, antenas de rádio frequência, tecnologias IP e *wireless* cada vez mais confiáveis, faz-se necessária a utilização de redundância nos sistemas de comunicação, com preferência na contratação de provedor diferente do sistema principal e, se possível, com meio físico diferente de transmissão.

SISTEMAS DE BACKUP

O backup das informações dos sistemas de segurança é premissa básica em qualquer sistema. E, como princípio, deve-se adotar a regra de backup 3-2-1:

- Ter pelo menos 3 cópias dos seus dados
- Armazenar essas cópias em 2 mídias diferentes
- Manter 1 cópia de backup fora do site

MANUTENÇÃO

A disponibilidade do parque instalado deve ser objeto de monitoramento constante pela equipe de segurança para que medidas de contingência possam ser acionadas, caso algum equipamento ou sistema esteja danificado ou em reparo programado.

Os contratos de manutenção devem ser revistos e baseados em acordos de nível de serviço (ANS). Isso possibilita que a empresa tenha uma prévia do tempo em que o sistema ficará indisponível e receba um prazo de atendimento e solução, de acordo com o nível de criticidade de cada sistema ou equipamento.

AUTORES

Alexandre Chaves – CEO da C4i Inteligência em Segurança e Diretor do Departamento de Defesa e Segurança da FIESP.
Contato: achaves@c4i.com.br
Fernando Só e Silva – CEO da PerformanceLab e Diretor do Departamento de Defesa e Segurança da FIESP.
Contato: fso@performancelab.com.br
Luciano Caruso – Diretor Geral da Haganá Tecnologia e Diretor de Tecnologia da ASIS International – American Society for industrial Secutity.
Contato: luciano.caruso@hagana.com.br
Marcos Serafim – Diretor de Desenvolvimento de Negócios da PerformanceLab e Diretor do Departamento de Defesa e Segurança da FIESP.
Contato: marcos.serafim@performancelab.com.br

12. MEDIÇÃO DE SERVIÇOS

A IMPORTÂNCIA DA ANÁLISE DOS NÚMEROS NA TOMADA DE DECISÃO: ENTENDA POR QUE A MEDIÇÃO DOS SERVIÇOS DE SEGURANÇA EMPRESARIAL DEVE FAZER PARTE DO DNA DA SUA ORGANIZAÇÃO

Muitas questões nas atividades profissionais, particularmente quando tratamos de contratos entre organizações, devem ser baseadas em números, ou, no mínimo, no formato de um valor a receber ou a pagar no final do mês. Estes números podem responder questões e auxiliar líderes empresariais a tomar melhores decisões. Mais do que nunca, é o momento das organizações fazerem as contas, avaliarem suas necessidades e se prepararem para eventuais reduções ou ampliações nos contratos.

A expectativa das empresas em relação à adoção de medições em seus processos está relacionada à diminuição de incertezas. Muitas vezes, os líderes se questionam: O que eu dimensionei é suficiente para fazer frente aos riscos? A contratação dos serviços é adequada e dimensionada para a necessidade? Consigo fazer mais com menos? Vamos alcançar os resultados programados?

Sob um estado de incerteza, as decisões podem ser tomadas de forma mais assertiva quando houver números e estatísticas disponíveis. Veja, abaixo, como pode ser fácil fazer a medição dos serviços de segurança da sua empesa.

SLA - SERVICE LEVEL AGREEMENT

Dentro dos conceitos da medição em serviços, o SLA (Acordo de Nível de Serviço) assume um papel preponderante pois, como o próprio nome diz, é um acordo, entre duas ou mais partes, sendo geralmente um cliente e o outro um prestador de serviços. Este documento visa estabelecer uma compreensão mútua das atividades prioritárias, responsabilidades, planejamento, soluções contratadas, métodos de medição e desempenho dos serviços contratados.

A redação de todo SLA deve descrever de maneira clara e objetiva os padrões dos serviços desejados, incluindo seus custos assim como as consequências geradas pela não execução dos níveis previamente acordados. O SLA deve auxiliar tanto a organização que contrata, como a empresa que presta serviços, em razão de ele permitir a cada uma das partes ser específica sobre suas expectativas e necessidades.

SLM – SERVICE LEVEL MANAGEMENT

O SLM, ou gerenciamento da entrega dos serviços, é outra ferramenta importante para a medição em serviços, projetado para monitorar o dia a dia, medindo o tempo todo a eficiência da estrutura operacional de entrega dos serviços e, periodicamente, sua eficácia. Com essas medições, os gestores dos serviços podem associar os números projetados aos serviços entregues, permitindo as devidas correções se necessárias.

O SLM é o acompanhamento do que está sendo entregue pela prestação de serviços. Ele pode ser comparado a um "filme da ação", onde a sequência de fotos ganha um movimento, retratando a ação operacional. Nesta analogia, a sequência de fotos do SLM significa a dinâmica da prestação de serviços, ao longo de um horizonte temporal. Já o SLA é uma foto que, por sua natureza, retrata uma situação estática do que foi contratado (e o contrato), ficando no passado, mas projetando o desejado para o futuro.

MEDIÇÃO E INDICADORES DE DESEMPENHO

Indicadores são ferramentas gerenciais poderosas e essenciais em ambientes de negócios competitivos e em momentos de crises. Eles não representam apenas um avanço na prestação de serviços, mas têm se tornado recursos altamente demandados pela alta gestão. O gerenciamento do nível de entrega dos serviços (SLM) tira proveito de dados operacionais para produzir informações e "insights" que apoiam o processo de tomada de decisões.

A medição do desempenho pode ser conceituada objetivamente como "o processo de quantificar a ação". Com mais detalhes, define-se como o processo de associar quantidades às atividades operacionais e sua comparação com padrões pré-estabelecidos ou também, o resultado das ações tomadas pelos diferentes níveis de colaboradores e expressas em números.

Medição do desempenho está relacionada a determinação dos "sinais vitais" dos processos operacionais. Ela pode qualificar e quantificar a entrega dos serviços, e apontar se os objetivos e metas pactuados estão sendo atingidos. O desempenho da entrega de um serviço, medido através de indicadores, é a relação entre uma quantidade e o nível de satisfação dos requisitos, das necessidades e expectativas dos clientes.

Para cada tipo de serviço poderá existir um conjunto específico de indicadores. No setor de segurança empresarial, os principais indicadores que se destacam são a prevenção de perdas, o absenteísmo nos postos de serviços, o "turnover" na equipe, a apresentação pessoal, a regularidade jurídica frente os órgãos de fiscalização, a disponibilidade dos sistemas de segurança, a pronta resposta aos chamados e a confiabilidade na capacidade de cumprir a missão.

Aos indicadores exemplificados para os serviços de segurança empresarial, para melhor ser tratada a avaliação da qualidade de sua entrega, se faz necessário incorporar a dimensão do risco. Pois, por melhor qualidade que o serviço possa ter, evidenciada e medida através de indicadores robustos, havendo uma ocorrência, o desempenho dos serviços prestados ficará comprometido.

Outro destaque, aplicado ao processo de medição de serviços de segurança, está relacionado a uma das maneiras de avaliação de sua entrega: a comparação, com saldo positivo para a prevenção, entre potenciais ocorrências neutralizadas (prevenção) e ocorrências efetivas (perdas com saldo negativo), quantificadas em valores monetários. Se forem acompanhados sistematicamente com indicadores, para a medição deste trabalho preventivo, os investimentos na prestação de serviços poderão ser justificados. O sucesso estará em o tomador de serviços investir um determinado montante na prestação de serviço e receber, em contrapartida, o retorno na forma de prevenção de perdas de possíveis ocorrências. Em especial, para este caso, o índice de prevenção de perdas, tal como um indicador econômi-

co-financeiro, traduzirá o resultado obtido pelos serviços de segurança. Sem dúvida, este é um número importante, capaz de expressar os esforços das equipes operacional e de gestão, que permite também a justificativa dos investimentos nas atividades de tratamento dos riscos.

Finalmente, deixamos aqui uma reflexão relacionada à medição do desempenho, principalmente em tempos muito difíceis como agora: “Estamos diante de uma verdadeira hecatombe, ceifando vidas humanas e a saúde econômica de muitas empresas, das quais, provavelmente, muitas não sobreviverão. É momento de sentarmos e negociarmos, baseando-se em números para chegarmos aos melhores acordos, onde devemos ter mutuamente as mãos estendidas, na linha de quem pode mais põe mais, quem pode menos põe menos. Em passada a crise, certamente, com este posicionamento, as parcerias se tornarão mais sólidas e os benefícios para os negócios e para nossa sociedade serão grandes”.

AUTOR

Eng. Fernando Só e Silva – MSc. CEO da Performancelab Sistemas e Diretor do Departamento de Defesa e Segurança da FIESP.
Contato: fso@performancelab.com.br

13. SEGURANÇA DA CADEIA PRODUTIVA DE EVENTOS

TRABALHA NA ÁREA DE EVENTOS? SAIBA COMO GARANTIR A SEGURANÇA DESSA CADEIA PRODUTIVA DURANTE A PANDEMIA DA COVID-19

A economia mundial entrou em colapso em um reflexo direto da proliferação da COVID-19 por todo o mundo. Alguns setores produtivos foram mais impactados, como é o caso do setor de eventos, que traz consigo uma cadeia extensa de áreas direta ou indiretamente ligadas à sua dinâmica. A sustentabilidade de inúmeros negócios, sobretudo dos menores, foi impactada. Colaboradores estão sujeitos a demissões e empresas, ao fechamento das operações.

No Brasil somente o segmento hoteleiro projeta mais de 100.000 demissões. No segmento aéreo, apenas 10% dos 2,8 mil voos diários estão ativos. Os prejuízos ao setor de eventos ainda estão sendo contabilizados, porém, a condição informal de muitos prestadores de serviços e o grande número de colaboradores terceirizados dificultam a obtenção de dados.

Temos ainda um período de maior necessidade de isolamento físico, e certamente as crises, de todas as facetas, serão ampliadas. Pressupõem-se maiores preocupações, sobretudo, de ordem de segurança pública e privada.

As angústias e sofrimentos coletivos poderão desencadear atos de violência gratuitos ou orquestrados sob a fragilidade de cenários expostos, o que demandará maior atenção e precaução de todos, particularmente dos empresários. Nessa situação, é mais que recomendada a preservação de todo o plano de segurança no intuito de não permitir que espaços de eventos, galpões de estoques de materiais de locação e artefatos de construção de estandes sejam invadidos ou saqueados.

Não é hora de realizar *saving* no aspecto da segurança, porque mais do que nunca ela poderá mitigar ainda mais prejuízos de ordem material. Independentemente do tamanho, as empresas precisam estar preparadas para situações adversas, como crises ou desastres, protegendo as vidas dos seus colaboradores e o seu patrimônio.

É muito importante que as empresas do setor de eventos entendam os riscos do aumento da insegurança em nosso país a cada dia que o *isolamento físico* é estendido. Estamos diante dos seguintes cenários:

1. Trabalhadores que dependiam do trabalho diário para o sustento de suas famílias não estão conseguindo ter receita e tendem a buscar alimentos da forma que for possível, nem que para isso tenham que participar de grupos de saques. Ações como essas já estão acontecendo em diversas localidades pelo país;
2. A justiça de diversos estados está liberando presos sem o devido cumprimento de suas penas. Isso impacta diretamente no crescimento da criminalidade e, por consequência, aumenta o risco de invasões e furtos nos mais variados ambientes;
3. A segurança pública no Brasil vive uma situação de colapso no sistema de segurança há muitos anos, e com a crise da COVID-19, essas estruturas ficam ainda mais sobrecarregadas. Existe o risco do afastamento de profissionais em decorrência de contaminação, o que pode gerar uma

diminuição dos efetivos policiais, que já não são suficientes para atender as demandas comuns da sociedade;
4. Os órgãos de segurança estão identificando tipos de crimes que não eram comuns no Brasil, como assaltos para suprimir sacolas de comidas e compras nas proximidades de supermercados e armazéns, o que demonstra que a tendência do aumento de crimes é real;
5. Como as cargas de maior atratividade estão contando com um maior aparato de segurança – e em muitos casos gozando de apoio dos órgãos de segurança pública - quadrilhas especializadas em roubo a bancos e roubo de cargas estão efetivamente invadindo e furtando depósitos;

Como pode ver, os riscos são reais, mas você pode minimizá-los reforçando a segurança física e eletrônica da sua empresa. Veja algumas dicas que podem ser aplicadas pelo setor de eventos:

1. Proteja e garanta seus ativos e patrimônio contra roubos, furtos, golpes e desvios internos;
2. Procure estar com os sistemas de segurança física e eletrônica adequados, garantindo que se algo acontecer nesse período, não afetará seu patrimônio;
3. Revise e ajuste seu Plano de Segurança física;
4. Crie e/ou revise o Manual de Segurança para Espaços e Funcionários;
5. Teste todos os seus mecanismos de segurança eletrônica (alarmes, cercas energizadas, câmeras, luzes e outros);
6. Identifique, corrija, renove e faça a manutenção de seguros de equipamentos e espaços, incluindo usuários e suas devidas contratações. Identifique a possibilidade de contratar apólices específicas;
7. Invista em treinamento das equipes, dando maior ênfase à segurança;
8. Simule falhas nos seus sistemas para confirmar a funcionalidade das sirenes, luzes, sensores e demais acionamentos remotos;
9. Revise a efetividade de seus procedimentos de controle de acesso;
10. Mantenha seus ambientes físicos monitorados por uma central de monitoramento 24/7 (sem interrupção);
11. Esteja preparado para retomada das suas atividades assim que as autoridades permitirem;
12. Estabeleça normas sanitárias, como lavagem obrigatória das mãos, uso de álcool em gel e máscaras de proteção, para todos usuários do estabelecimento, incluindo clientes e convidados, enquanto a pandemia existir.
13. Esteja ciente das determinações, licenças e legislações locais, a respeito da operação de sua atividade de negócio;
14. Faça a manutenção geral de equipamentos e espaços, enquanto aguarda a autorização para a realização de novos eventos;
15. Mantenha-se informado sobre a legislação em sua região. Saiba quais autorizações de funcionamento e licenças são obrigatórias;
16. No retorno das atividades, disponibilize álcool em gel em locais chave dos eventos (acessos, banheiros, cozinha, pontos de alimentação), já prevendo fornecedores e tipos de produtos a serem adquiridos;
17. Garanta que toda a cadeia de fornecedores esteja treinada e cumprindo com as exigências de higiene que serão determinadas pelos órgãos de saúde regionais e locais;
18. Eventos que contam com revista pessoal deverão se preparar para utilizar novos mecanismos e novas formas de revista;
19. Identifique boas práticas adotadas pelas empresas congêneres e adote-as na sua companhia;
20. Desenvolva com os fornecedores formatos mais rígidos de segurança, controle de acessos e identificação de funcionários, incluindo recursos eletrônicos e a distância;

21. Participe de grupos de discussões e de entidades representativas do setor que abordem o assunto “segurança”;
22. Exija dos fornecedores a lista completa dos seus prepostos para que eles sejam cadastrados. Analise se os colaboradores têm registro em carteira para procederem a prestação de serviços e se as empresas de segurança têm registro ativo na Polícia Federal.

A pandemia do coronavírus obrigou os negócios a se reinventar, e com a indústria de eventos não foi diferente. O setor passou a oferecer serviços pela internet, e assim se tornou vulnerável a riscos próprios do universo virtual. Veja algumas precauções que devem ser tomadas pelos promotores de eventos nas plataformas online:

1. Os promotores de eventos devem avaliar os riscos de vazamento de informações tratadas e geradas no evento e de possíveis gravações realizadas por participantes não autorizados;
2. É de extrema importância identificar os riscos de imagem pessoal, considerando os direitos de imagem de quem está participando do evento, e as autorizações concedidas para utilização das imagens geradas no evento;
3. É fundamental estar atento aos recursos de segurança oferecidos pela plataforma utilizada para transmissão, identificando as possibilidades de gravação de eventos e pessoas não autorizadas, principalmente quando houver troca de imagens por diversas câmeras e compartilhamento de telas;
4. Os responsáveis pelos conteúdos que serão distribuídos em larga escala (global, nacional, regional ou local) deverão se adaptar à LGPD (Lei Geral de Proteção de Dados). Embora ainda não tenha entrado em vigor, ela terá impactos diretor nessa nova realidade;
5. A privacidade de pessoas, mesmo que dentro de suas próprias residências, será impactada diretamente e isso exigirá uma reeducação das pessoas a uma nova cultura. Os riscos de vazamento de informações e de exposição de imagem não autorizadas pelos usuários também aumentam em grande escala;
6. Promotores de “webinars” e outras modalidades de eventos a distância deverão se adaptar muito rapidamente às novas regras, exigências e riscos de seus negócios. O mercado deverá criar mecanismos de análise, gestão e controle desses novos riscos;
7. Esteja atento às regras de acesso, gravação, divulgação e armazenamento de todos os conteúdos que foram gerados por plataformas de comunicação de áudio e vídeo em tempo real.

AUTORES

Andrea Nakane – Doutora em Comunicação Social, com 28 anos de experiência profissional acumulada em vivências nas áreas de hotelaria, turismo, indústria, cerimonial e educação. É sócia-diretora da Mestres da Hospitalidade, cuja expertise é focada na inteligência estrategista de eventos corporativos, Cerimonial e Protocolo e capacitação do talento humano na área da Hospitalidade. É autora de diversos capítulos e livros na área de Turismo e Eventos e colaboradora do site Diário do Turismo, do Portal Eventos e Promoview. Foi condecorada com a outorga de Embaixadora do RJ e o Prêmio Joana Palhares.
Contato: mestresdahospitalidade@uol.com.br.

Igor de Mesquita Pipolo, ADS, ASE – Fundador e CEO da Núcleo Consultoria, Bacharel em Direito, pós-graduado em Alta Direccion de Securidad pela Universidad Pontificia Comillas de Madrid.

Diretor do DESEG - Departamento de Segurança da FIESP. Ex-presidente da American Society for Industrial Security (Chapter Brasil). Fundador, ex-presidente e diretor da Associação Brasileira de Profissionais de Segurança – ABSEG, Autor de vários artigos e de 3 livros sobre Segurança de Eventos.
Contato: lp@nucleoconsult.com.br.

Gustavo Caleffi, DSE – Fundador e Sócio diretor da Squadra Gestão de Riscos, Fundador e CEO APP Be On – Segurança Colaborativa, Administrador de empresas, com MBA em *Direccion de Seguridad en Empresas* (Comillas), Certificado pela universidade Israelense ICT (International Institute for Counter-Terrorism) em *"Segurança Global e Antiterrorismo",* certfificado em "*Advanced VIP Protection Course*" em Israel, especialista em gestão de riscos estratégicos, crises e segurança, autor do livro *"Caos Social – A Violenta Realidade Brasileira".*
Contato: gustavo@squadraconsultoria.com.br.

José Roberto Sevieri – Administrador de empresas e técnico de segurança do trabalho, participou do projeto de lei que criou as profissões do Técnico de Segurança do Trabalho e do Engenheiro de Segurança do Trabalho, através da Lei 7.410 e do Decreto 92.530, em 1985. Produziu 34 exposições, bem como 68 congressos que aconteciam simultaneamente. Foi diretor da FIESP, no DESEG – Departamento de Segurança, ex-Presidente da ABEOC NACIONAL - Associação Brasileira das Empresas de Eventos, foi fundador e Tesoureiro da ABS - Agência Brasil de Segurança, foi Vice-Presidente da UBRAFE – União Brasileira das Empresas Promotoras de Feiras, é chanceler da Ordem do Mérito Prevencionista e recebeu várias honrarias pela ABRAPHISET, CETESB, ANIMASEG e ABESE, criou vários prêmios para destacar profissionais e empresas, é Diretor Operacional de Gerenciamento de Riscos da Abimex – Associação Brasileira das Indústrias de Materiais Explosivos e Agregados.
Contato: sevieri@sevieri.com.br.

EXPEDIENTE

Fiesp

Roberto Zapotoczny Costa
Ricardo Coelho
Igor de Mesquita Pipolo
Flávio Porto
Adalmir Manoel Domingos
Luciano Villela Coelho

Parceiros

Diógenes Viegas Dalle Lucca
Jeová Ferreira Cardoso Júnior
Mauricio Franklin Pontes
Lilian Ferracini
Maciel Lastoria
Maurício de Faria
Leandro Fortes
Michel Pipolo de Mesquita
Roberto Coletti
Tatiana Diniz
Ricardo Ribeiro Tavares
Eytan Magal
João Jaouiche
Laércio Soares
Marcela Vasconcellos
Marcy José Campos Verde
Jeferson D'Addario
Edison Luiz Gonçalves Fonte
Leonardo Simão
Aureo Miraglia de Almeida
Flávio Ainbinder
Alexandre Chaves
Fernando Só e Silva
Luciano Caruso
Marcos Serafim
Andrea Nakane
Gustavo Caleffi
José Roberto Sevieri

FIESP
Federação das Indústrias
do Estado de São Paulo

Av. Paulista, 1313
São Paulo - SP | CEP: 01311-923
deseg@fiesp.com.br
www.fiesp.com.br