Planejamento Estratégico em Segurança Empresarial

Objetivo geral:

Identificar o processo de Gestão de Segurança e os procedimentos preventivos capazes de mitigar os riscos inerentes ao negócio

Espera-se que ao final do estudo deste tema você possa:

- Relacionar a necessidade de segurança com a criminalidade na sociedade atual.
- Identificar a necessidade da gestão de segurança nas empresas e Instituições financeiras.
- Identificar a contribuição da gestão de segurança para os negócios.
- Identificar os aspectos regulatórios da gestão de segurança.
- Identificar os fatores considerados no processo de gestão de segurança.
- Relacionar risco operacional e segurança

Com planejamento cuidadoso e detalhado, pode-se vencer; com planejamento descuidado e menos detalhado, não se pode vencer. A derrota é mais do que certa se não se planeja nada! Pela maneira como o planejamento antecipado é feito, podemos predizer a vitória ou a derrota."

Sun Tzu

A Arte da Guerra

Introdução ao tema:

Para ser efetivo e alcançar os objetivos sociais e empresariais desejados, qualquer negócio ou empreendimento deve ser estruturado levando-se em conta diversos fenômenos ou fatores de influência, entre outros, os sociais, econômicos, psicológicos, políticos e tecnológicos. Quando pesquisamos, delimitamos e controlamos esses aspectos, podemos definir estratégias para minimizar os seus efeitos no ambiente produtivo e social ou mesmo utilizá-los como fontes geradoras de benefícios.

Desde os primórdios, por exemplo, percebeu-se que o crime e a violência eram fenômenos de causa social que, sem estar devidamente controlados, poderiam causar sérias repercussões ou mesmo neutralizar o crescimento econômico e afetar a estabilidade social em qualquer contexto.

Esses aspectos devem ser levados em conta em todos os ambientes (pessoal, familiar, social, empresarial, etc.), sendo hoje uma preocupação de governos em todo o mundo. É nesse sentido que incluímos o tema segurança no escopo da governança corporativa. Qualquer instituição, para garantir sua efetividade, tem o dever de mapear de forma adequada os riscos inerentes aos negócios e mercados com os quais atua ou pretende atuar. Quanto ao ambiente interno, deve-se ter em vista que a segurança é essencial para garantir um ambiente saudável, ético, propício à motivação pessoal, à integração e à geração de resultados.

Com as profundas mudanças que ocorreram nas últimas décadas em todo o planeta, a globalização, a rápida proliferação da internet, a

multiplicação de ações terroristas, a modernização do crime organizado, o surgimento de tratados internacionais para combate à lavagem de dinheiro e ao terrorismo e outros fenômenos, provocaram grandes alterações na visão de governos e corporações em todo o mundo sobre o tema segurança.

No ambiente corporativo, ainda que haja muito a realizar, especialmente por ser um processo vivo e dinâmico, a segurança passou a ser vista como uma área de abrangência multidisciplinar que, embora conduzida com base em pressupostos respaldados por ciências humanas (sociologia, psicologia etc.), deve ser suportada por governança qualificada, integração com o negócio, equipes de excelência, tecnologias de ponta e inteligência estratégica, com programas permanentes de educação e cultura, considerando que a eficácia do processo de segurança depende do envolvimento de todas as pessoas.

VISÃO ATUAL DA SEGURANÇA

Temas estratégicos de governança corporativa estão diretamente relacionados com as atividades de segurança. Ao trabalhar para o lançamento de um produto inédito, por exemplo, uma empresa procura garantir que não haja divulgação externa do trabalho, especialmente que nenhum concorrente tenha conhecimento prévio da novidade. Para que isso ocorra é necessário adotar uma série de medidas internas relacionadas à segurança da informação, de tal maneira que, ao ser lançado no mercado, o novo produto seja reconhecido como novidade, inclusive pelos concorrentes.

Da mesma forma, quando o produto é posto à venda, o cumprimento de requisitos de segurança vai ajudar na garantia da rentabilidade das vendas ao evitar ou reduzir perdas com falhas, fraudes, roubos e outros problemas. Ao sermos omissos quanto à segurança estamos, de alguma forma, trabalhando contra nós mesmos, contra a nossa empresa e a sociedade de um modo geral. A omissão pode facilitar a ocorrência de ações ilícitas e alimentar o mercado do crime que, atualmente, movimenta bilhões de dólares em todo o mundo, comprometendo a vida, a estabilidade social e a economia de muitas pessoas, comunidades e nações.

Uma gestão eficaz de riscos é fator preponderante para uma boa posição no mercado e tranquilidade de acionistas. Em empresas sujeitas a regulamentação, a eficácia das atividades de gestão de riscos, de controle e de segurança é uma preocupação permanente dos respectivos órgãos reguladores.

Estima-se que o crime movimenta anualmente cerca de US$ 3 trilhões em todo o mundo, representando, segundo a Organização das Nações Unidas, de 2% a 5% do PIB mundial. As fontes geradoras desses recursos são diversas, passando por crimes como o narcotráfico, corrupção, contrabando, pirataria, fraudes, roubos, sequestros, tráfico de armas, tráfico de pessoas e órgãos humanos, prostituição, pornografia, entre outros. De acordo com os mesmos estudos, pelo menos US$ 1,5 trilhão circulam pelo sistema financeiro.

SEGURANÇA NAS EMPRESAS

As empresas mantêm, necessariamente, compromissos tácitos com seus empregados, fornecedores, clientes, acionistas, com a sociedade e com o meio ambiente. Exige-se que, ao menos, busquem proteger seus ativos contra riscos previsíveis que podem não só comprometer o negócio, mas causar os danos sociais e políticos anteriormente citados.

Ressalta-se que a melhor forma de prevenir riscos é o constante exame dos processos, o monitoramento do negócio, a percepção de cenários e a manutenção permanente das pessoas mobilizadas contra eventuais ocorrências.

Para tanto é necessária a participação integrada e sistematizada de toda a empresa, de forma global e corporativa.

Mais do que apenas buscar reduzir ocorrências de danos isoladamente, é necessário também organizar e coordenar todo o esforço corporativo no sentido de:

- avaliar as ameaças ao negócio e o nível de segurança da organização;

- introduzir a discussão sobre o custo que eventuais danos poderão ocasionar;

- identificar os recursos necessários para evitar as possíveis ocorrências, cujas perdas repercutem diretamente nos negócios, no resultado econômico e na imagem da organização.

Nesse contexto, a segurança não pode mais ser tratada apenas como uma estrutura específica, mas como uma atividade sistematizada, pressupondo integração em todos os níveis e segmentos institucionais.

A gestão de segurança constitui um processo contínuo, dinâmico e flexível, de permanente avaliação e adequação das medidas e procedimentos de segurança das pessoas e dos ativos, contra os riscos e ameaças reais ou potenciais.

As empresas estão conscientes da necessidade da segurança para a preservação de seus valores, uma vez que as perdas podem influenciar diretamente no resultado financeiro. Por outro lado, a legislação também obriga a adoção de requisitos de segurança. Dessa forma, as organizações são levadas a investir continuamente em soluções de segurança.

FATORES DO PROCESSO DE Gestão de segurança

O objetivo da segurança é resguardar a integridade das pessoas, das informações, dos ativos físicos e financeiros e da imagem da empresa. Consideremos os seguintes fatores do processo de gestão de segurança:

Valores

Os valores são os "objetos" da proteção. Representam tudo o que deve ser protegido para assegurar a continuidade dos negócios e contribuir para o resultado financeiro da empresa.

Pessoas: este primeiro grupo de valores é composto diretamente pelos funcionários da organização, contratados diversos, clientes e usuários. Indiretamente devem ser incluídos os familiares dos funcionários, que podem ser vítimas de ocorrências relacionadas com a atividade dos funcionários, a exemplo da extorsão mediante sequestro.

■ **Ativos físicos e financeiros:** podem ser citados o numerário (moeda nacional em espécie) e outros valores (moeda estrangeira, equipamentos, instalações físicas.

■ **Imagem:** qualquer tipo de vinculação do nome da instituição e/ou de seus funcionários com fatos ou notícias de caráter negativo pode provocar sérios danos à sua imagem - um ativo intangível - e, por isso, necessita de mecanismos eficientes de proteção.

■ **Informações:** as informações merecem alto nível de proteção, pois sua perda pode gerar prejuízos incalculáveis às organizações. Podem ser citados alguns exemplos de informações cujo vazamento pode gerar, direta ou indiretamente, transtornos às organizações: dados pessoais de funcionários e clientes, informações sigilosas sobre clientes, assuntos estratégicos (projetos, negócios, valores, plano de segurança etc.), rotinas de serviços e funções específicas de funcionários. Deve ficar claro que criminosos procuram conhecer as informações e rotinas das unidades para subsidiar as ações contra a empresa.

Ocorrências e agentes

As organizações estão sujeitas a inúmeros tipos de ocorrências, que variam de acordo com o tipo de negócio e com as fragilidades encontradas em cada local. Vale lembrar que os criminosos também procuram correr sempre o menor risco, portanto a tendência é que a vítima seja sempre a empresa ou unidade mais despreparada, não só sob aspecto de equipamentos, mas principalmente quanto ao comportamento de seus funcionários.

As ocorrências podem ser provocadas ou facilitadas por agentes internos e externos.

■ **Atores internos:** funcionários e contratados. Erros de procedimento, descumprimento de normas, negligência, vazamento de informações e até mesmo dolo propiciam a ação criminosa. Daí a necessidade de todos perceberem sua responsabilidade e se comprometerem com as questões de segurança.

■ **Atores externos**: de maneira geral são os criminosos especializados, responsáveis pelos mais variados tipos de ataques, tais como sequestros, assaltos, arrombamentos, furtos, fraudes, vandalismo, lavagem de dinheiro e crimes cibernéticos. Numa proporção menor, mas responsáveis por grandes transtornos, ocorrem os incidentes e desastres de natureza não criminosa (chuva, terremoto, etc.).

Estratégias

O terceiro fator considerado na gestão de segurança, e o mais relevante, são constituídos pelas estratégias que viabilizam esse macroprocesso:

■ **Prevenção ou inibição**: o objetivo principal é de identificar condições, situações ou pessoas que possam ser causadoras de ameaças, de maneira a se criar fatores que inibam ocorrências. Este conceito, de certa forma, abrange os demais, uma vez que o objetivo maior é evitar os incidentes de segurança. Estão entre as atividades de prevenção ou inibição: a disseminação de instruções e cultura de segurança, as aplicações de metodologias e políticas, a definição de especificações de ferramentas e equipamentos de segurança, análise de riscos etc.

■ **Correção:** a partir de análises internas e do cenário externo, procura-se manter dinâmico o processo preventivo, corrigindo e redefinindo mecanismos, ferramentas, práticas, instruções, estrutura

tecnológica e humana, já existentes e aplicados, de forma a manter a eficácia das medidas de segurança estabelecidas anteriormente. Estão entre essas atividades as atualizações de sistemas e equipamentos, monitoramento de tendências, cenários, acompanhamento da efetividade das medidas de inibição adotadas, avaliação e controle de situações e incidentes de crise, entre outras.

■ **Recuperação:** trata-se da elaboração de planos de continuidade de negócios.

Se o incidente ocorrer, a empresa deve ter previsto um plano de recuperação de suas atividades. Por outro lado, é fundamental que se utilize o conhecimento gerado por incidentes efetivados, para reavaliar e adaptar os módulos anteriores, com o intuito de se evitar novas ocorrências.

O plano busca também recuperar os ativos comprometidos pelos incidentes.

■ **Pesquisa estratégica**: tem por objetivo coletar informações consideradas úteis para a segurança preventiva em todas as suas dimensões.

A pesquisa estratégica envolve relacionamento com outras instituições financeiras, empresas e grupos especializados em segurança na internet, órgãos go governamentais, universidades, organismos policiais, órgãos de inteligência e outros. Por meio de pesquisa estratégica, por exemplo, podemos gerar subsídios para muitas decisões estratégicas, ações emergenciais para evitar delitos.

TEORIA DOS CÍRCULOS CONCÊNTRICOS APLICADOS A UMA EMPRESA.

Os ambientes apresentam diferentes níveis de criticidade devido às características intrínsecas de cada um e a gestão de segurança de ambientes precisa considerar o nível de criticidade de cada ambiente para desenvolver as ações voltadas para a segurança desses locais. Ambientes mais sensíveis (suscetíveis a ataques) recebem um maior nível de proteção.

Aplica-se neste caso, a teoria dos círculos concêntricos, que pode ser definida como a estratégia de partir do mais simples para o mais complexo, domais próximo para o mais afastado e do mais baixo para o mais alto nível de segurança. No esquema de círculos concêntricos pode-se ver os vários níveis de segurança, sendo que o círculo central representa a área ou instalação (unidade) com nível de segurança mais elevado (Figura 1).

Fonte: Mandarini (2006)

De acordo com Mandarini (2006), conforme a importância do local pode classificá-lo e ter as seguintes gradações de segurança para as áreas, instalações, unidades e ambientes:

SEGURANÇA EXCEPCIONAL: área de excepcional sensibilidade ou periculosidade, cujo acesso é restrito a pessoas estrita e institucionalmente envolvidas nas atividades aí desenvolvidas. Local estratégico para a unidade ou organização, para o qual o autor classifica o controle de acesso como **ULTRASSECRETO**;

São passíveis de classificação como **ultrassecretos**, dentre outros, dados ou informações referentes à soberania e à integridade territorial nacional, a planos e operações militares, às relações internacionais do País, a projetos de pesquisa e desenvolvimento científico e tecnológico de interesse da defesa nacional e a programas econômicos, cujo conhecimento não autorizado possa acarretar dano excepcionalmente grave à segurança da sociedade e do Estado.

SEGURANÇA ELEVADA: área de elevada sensibilidade ou periculosidade, cujo acesso é restrito a pessoas íntima e institucionalmente envolvidas nas atividades aí desenvolvidas. O Controle de acesso neste caso é classificado como **SECRETO**;

São passíveis de classificação como **secretos**, dentre outros, dados ou informações referentes a sistemas, instalações, programas, projetos, planos ou operações de interesse da defesa nacional, a assuntos diplomáticos e de inteligência e a planos ou detalhes, programas ou instalações estratégicos, cujo conhecimento não autorizado possa acarretar dano grave à segurança da sociedade e do Estado.

SEGURANÇA MEDIANA: área de mediana sensibilidade ou periculosidade, com acesso restrito a pessoas que tenham relações institucionais com as atividades aí desenvolvidas. Para este caso, o controle de acesso é classificado como **CONFIDENCIAL**;

São passíveis de classificação como **confidenciais** dados ou informações que, no interesse do Poder Executivo e das partes, devam ser de conhecimento restrito e cuja revelação não autorizada possa frustrar seus objetivos ou acarretar dano à segurança da sociedade e do Estado.

SEGURANÇA ROTINEIRA: área de baixa sensibilidade ou periculosidade, cujo acesso é restrito a pessoas que tenham necessidade de trato funcional ou de negócios com as atividades aí desenvolvidas. Normalmente o controle de acesso é classificado como **RESERVADO**;

São passíveis de classificação como **reservados** dados ou informações cuja revelação não autorizada possa comprometer planos, operações ou objetivos neles previstos ou referidos.

SEGURANÇA PERIFÉRICA: área isenta de sensibilidade ou periculosidade, que integra os limites do perímetro da unidade ou instalação.

Níveis de Segurança

Exemplos de ambiente bancário:

Segurança excepcional	Salas de servidores de centros tecnológicos; tesouraria, corredores de abastecimento de terminais, bateria de caixas, ambiente de processamento.
Segurança elevada	Elevada Centros de processamento de dados – CPD; salas dos comitês de Unidades Estratégicas
Segurança rotineira	Saguão das agências, destinado ao atendimento aos clientes.
Segurança periférica	Estacionamentos, áreas externas (corredores, fundos etc.) e, até mesmo, áreas públicas

COMPARTIMENTAÇÃO DE ÁREAS VIGILADAS.

A **compartimentação de áreas vigiladas** é muito utilizada em Indústrias/empresas que possuem edificações que precisam ser protegidas, porém, ***são construídas em áreas muito extensas***.

A condição de proteção ao patrimônio, quando disposto em locais muito extensos demanda um grande investimento em segurança, no que tange a construção de barreiras perimetrais, disposição de câmeras de segurança, rondas motorizadas, etc. Então, com a finalidade de reduzir o custo com a implantação de barreiras e outros dispositivos, muito Indústrias/empresas optam em investir na proteção de áreas menores

dispostas dentro desta área, que sejam importantes, porém, vulneráveis, efetivando a ***proteção de áreas menores*** dentro de **uma área maior**. **Exemplo**: Proteção de Instalações onde são **guardados, manuseados e produzidos** Materiais sigilosos, Áreas perigosas, dispostos em locais isolados tais como fazendas, etc.

Ainda no que se refere a **compartimentação de áreas**, é muito comum verificarmos nas indústrias/empresas, a existência de uma restrição de acesso a tais áreas que foram compartimentadas, com a utilização de **identidades funcionais personalizadas (crachás)**, onde a identificação das cores de restrição estão dispostas nos fundos das fotografias e/ou em tarjas, em caso de identidades de visitantes**.**

Classificação da criticidade de acesso a áreas compartimentadas (exemplo):

Uma empresa pode utilizar **cores** para **classificar suas áreas**, dinamizando o controle e melhorando o emprego dos meios disponíveis para a sua proteção da seguinte forma:

Cor que indica a restrição:	Grau de restrição do acesso:	Controle do acesso:
Branco	**Inexistente**	Áreas bem vigiadas, comumente onde transitam colaboradores, prestadores de serviço, visitantes, etc. Não necessitam de acompanhamento específico e qualquer atuação neste local não interfere na atividade principal da Indústria/Empresa.
Verde	**Baixo**	Nestes locais pode ser feito o acompanhamento visual ou pessoal.
Amarelo	**Médio**	Nestes locais os acessos devem ser controlados. **Necessita de acompanhamento constante**. Intervenções danosas nestes locais causam sérios danos.
Vermelho	**Alto**	Nestes locais o acesso é restrito, seja por motivo de assunto, material a ser tratado, guardado, manuseado produzido, etc, que não deva ser de domínio público e sim de domínio de pessoas devidamente autorizadas. (**O acompanhamento é sempre necessário).** Qualquer intervenção danosa nestes locais é desastrosa.

Entre os aspectos analisados para o monitoramento do nível de segurança estão:

■ **região geográfica:** existem diferenciações entre as ações criminosas (*modus operandi*) nas diversas regiões do país, bem como entre o interior e capital de Estado e até mesmo entre as diferentes regiões de uma cidade, tais como centro, bairro e regiões historicamente mais violentas;

■ **Localização:** a localização da dependência interfere no seu nível de risco.

Por exemplo, uma agência bancaria situada à margem de uma rodovia ou em local de pouca movimentação noturna possui um maior nível de risco.

Por outro lado, as dependências localizadas em shoppings ou próximas a organismos policiais apresentam um menor nível de risco;

■ **Outras características:** outras variáveis que também interferem no risco e que devem ser consideradas, tais como: quantidade de pavimentos da dependência, leiaute, estrutura dos ambientes, segmento negocial, perfil da clientela, histórico de ocorrências e limite de numerário entre outros.

Gestão da continuidade de negócios:

A gestão da continuidade de negócios - GCN é uma disciplina de gestão relativamente nova que se tornou muito importante dada o ambiente extremamente turbulento em que as organizações estão inseridas.

Atividades terroristas, mudanças climáticas drásticas, falhas ou danos nas instalações físicas, interrupção na cadeia de suprimento e ameaças de pandemias humanas e animais são alguns exemplos dos eventos mais relevantes que podem resultar em interrupções em larga escala, impactando a capacidade das organizações disponibilizarem seus produtos e serviços.

E não são apenas estes eventos que podem causar rupturas na continuidade das operações de negócio. Uma em cada cinco organizações do Reino Unido sofre paralisações em suas atividades a cada ano, causadas por incidentes de menor nível de relevância, tais como incêndios, doenças, paradas decorrentes de problemas em sua infraestrutura tecnológica, negação de acesso aos sistemas informatizados ou perda de um fornecedor chave. Estes eventos

podem não impactar toda a coletividade em que a organização está inserida, mas pode levá-la a perder clientes ou a ter problemas em seu fluxo de caixa.

Ao adotar a gestão da continuidade, as organizações estão mais bem preparadas para superar os desafios de uma interrupção qualquer que seja a sua causa.

O conceito de continuidade de negócios foi desenvolvido a partir da metade da década de 80, como uma nova maneira de gerenciar os riscos de negócio.

A base da GCN é o comprometimento do corpo diretivo da organização em garantir a continuidade das funções de negócio, a qualquer tempo e sob quaisquer circunstâncias.

Eventos inesperados não acontecem de repente; muito frequentemente têm sua causa-raiz na própria organização. Todas organizações possuem fragilidades e podem ficar sujeitas a possibilidades de exploração de suas vulnerabilidades. Exames mais apurados das causas dos principais desastres demonstram que são decorrentes da combinação dessas fragilidades.

A gestão da continuidade de negócios é focada na prevenção, não somente na reação à ocorrência de incidentes. Não diz respeito única e exclusivamente à capacidade de lidar com incidentes, quando e se eles ocorrerem, mas também em estabelecer uma cultura que busque construir maior resiliência, forma a garantir a entrega de produtos e serviços aos clientes.

Em resumo, a GCN age proativamente ao estabelecer os fundamentos estratégicos e operacionais para desenvolvimento da resiliência da organização a eventos causadores de ruptura, interrupção ou perda da capacidade de fornecer produtos e serviços. Não contempla medidas puramente reativas a se adotar depois que um incidente ocorre. Requer uma abordagem holística, com planejamento abrangendo todas as esferas, uma vez que a resiliência depende igualmente dos níveis gerenciais e operacionais e da tecnologia.

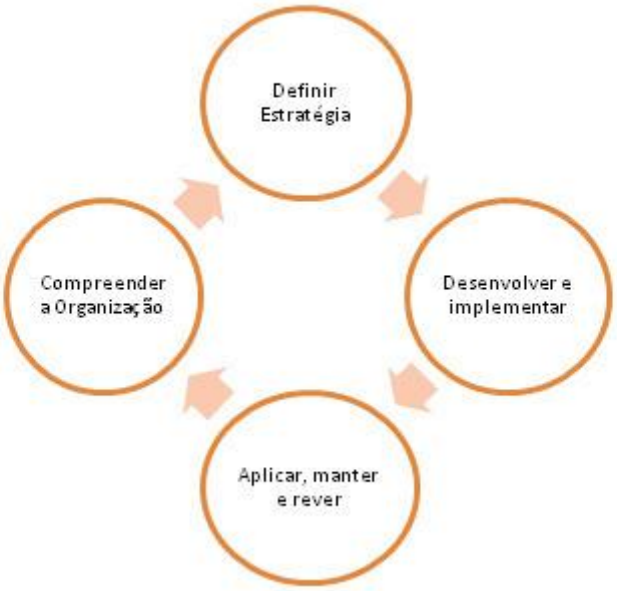
Pesquisas realizadas demonstram que o impacto de desastres no valor de mercado das ações das empresas pode ser significativo. A falta de confiança na capacidade dos gestores em agir rápida e profissionalmente em caso de desastre são as causas principais dessa desvalorização.

A GCN revela a capacidade estratégica e tática da organização para planejar.

A estrutura de GCN

A visão mais aceita do assunto percebe a GCN como um ciclo que permite compreender melhor a organização e prepará-la para o enfrentamento de crises, ao definir os processos críticos, fazer a avaliação de risco e impacto destes processos, definir as estratégias de continuidade de negócios, determinar responsabilidades, desenvolver e testar os planos de continuidade. Graficamente, podemos entender esse ciclo como demonstrado na figura

Ciclo de gestão da continuidade de negócios



A realização da análise de impacto é o ponto de partida. É um processo dinâmico que busca identificar operações e serviços críticos, dependências internas e externas e níveis de resiliência apropriados. Avalia os riscos e impactos potenciais dos vários cenários de interrupção

nos processos de uma organização e na sua imagem e reputação. Os processos e atividades críticas são sustentados por pessoas (funcionários, colaboradores etc.) e recursos (tecnologias, infraestrutura física e de logística, fornecedores etc). Torna-se necessário perceber as ameaças a que estão sujeitas as pessoas e os recursos, as vulnerabilidades e o impacto que a interrupção provocada por um incidente possa causar nos negócios da empresa. Esta percepção é conseguida por meio da análise de risco e impacto.

É fundamental a realização da análise de risco e impacto para perceber e mensurar a real criticidade dos processos. As análises de risco e impacto fornecem subsídios para tomada de decisão, permitindo um direcionamento nas ações contingenciais, com vistas a priorizar a retomada dos processos mais importantes para a organização.

A estratégia de continuidade parte dos objetivos de recuperação e das prioridades, baseando-se nos resultados da análise de impacto nos negócios. Entre outras coisas, estabelece objetivos para o nível de serviço que a organização busca entregar no caso de uma interrupção e a retomada das operações.

Os planos de continuidade proveem orientação detalhada para implementar a estratégia de recuperação. Eles estabelecem os papéis e alocam responsabilidades por administrar as situações emergenciais durante as interrupções e garantem orientações claras, relativas à alçada de decisão das equipes no caso de uma interrupção que incapacite as pessoas chave.

A segurança das pessoas não pode ser esquecida e deve ser a preocupação máxima dos planos de continuidade dos negócios de uma organização.

É importante lembrar que a confusão pode ser um grande obstáculo para uma resposta efetiva a uma interrupção significativa. Nesse sentido, papéis, responsabilidades e autoridade para agir, bem como o encadeamento dos planos, devem ser claramente descritos no programa de gestão da continuidade.

Análise de impacto nos negócios

A análise de impacto nos negócios é o pilar central da GCN. É responsável pela identificação, quantificação e qualificação do impacto nos negócios gerado pela perda, interrupção ou ruptura dos processos de negócio de uma organização e provê as informações que subsidiarão a determinação das estratégias de continuidade mais adequadas.

A análise de impacto, ao identificar, quantificar e qualificar o impacto nos negócios permite:

■ Obter uma maior compreensão dos processos mais críticos, a prioridade de cada um deles e os tempos máximos de retomada após uma interrupção não programada;

■ Identificar quais impactos nos negócios são mais relevantes para a organização, considerando-se aspectos como imagem, reputação, perda financeira etc;

■ Propiciar informações para as estratégias de recuperação se tornarem mais efetivas;

■ Identificar quais impactos podem resultar em danos à reputação, ativos e posição de mercado da organização;

■ Quantificar o tempo máximo tolerado de uma interrupção para cada processo de negócio.

Ao avaliar os impactos, convém que a organização considere aqueles que se relacionam ao atingimento de seus objetivos. Os impactos a serem avaliados incluem:

- Impacto ao bem-estar das pessoas;
- Dano ou perda de instalações, tecnologias ou informação;
- Não cumprimento de deveres ou regulamentações;
- Danos à reputação;
- Danos à viabilidade financeira;
- Deterioração da qualidade de produtos ou serviços;
- Danos ambientais.

Ocorre, então, uma análise dos recursos, das ameaças e vulnerabilidades, para que se possa classificar o grau de impacto que estas ameaças poderão provocar no caso de um incidente.

Para realizar a análise de impacto são utilizados *workshops*, aplicados questionários ou realizadas entrevistas com os gestores dos processos.

As boas práticas de GCN indicam a necessidade de revisão mínima anual dos resultados da análise de impacto.

Análise de riscos

A análise de risco, no âmbito da GCN, é realizada para os processos considerados críticos. O objetivo é determinar e identificar os modelos de avaliação de riscos e os níveis aceitáveis de risco aos qual a organização está disposta a enfrentar.

Para isso, os riscos dos processos são mensurados e classificados de acordo com seu grau de criticidade. A análise de riscos, ao estudar probabilidade de ocorrer o evento e seu impacto no processo, permite identificar uma série de ameaças de interrupção.

A análise de riscos deve ser focada nos processos mais urgentes identificados durante a análise de impacto. Tem como propósito identificar as ameaças internas e externas que podem provocar descontinuidade nos negócios e sua probabilidade e impacto; priorizar as ameaças de acordo com um método aceito pela organização; e prover informações para os planos de ações mitigadoras do risco.

Os principais tópicos a serem abordados na análise de riscos são:

■ Detalhamento dos impactos e das probabilidades de ocorrência em ordem de criticidade e relevância;

■ Identificação das ameaças aos processos de maior impacto identificados na fase de análise de impacto;

■ Estimativa do impacto das ameaças na organização usando um método único de avaliação;

■ Determinação dos valores estatísticos associados à probabilidade ou frequência de cada ameaça;

■ Cálculo do risco, combinando o impacto e a probabilidade de ocorrência de cada ameaça, utilizando método previamente definido;

■ Categorização dos resultados obtidos

Definição de estratégias

Para uma boa prática de GCN, todas as organizações devem perceber quais são seus processos mais críticos e desenvolver estratégias para minimizar o impacto nos negócios, imagem e marca, advindo de uma interrupção.

Para o desenvolvimento de boas estratégias de continuidade, vários fatores devem ser considerados, como por exemplo:

■ As pessoas envolvidas nos processos;

■ Os recursos tecnológicos disponíveis;

■ Os fornecedores;

■ A segurança da informação (atendendo aos requisitos de confidencialidade, integridade e disponibilidade)

■ O período aceitável de interrupção;

■ Os custos para implementação das estratégias;

■ Consequências das ações, grau de tempestividade e até da inação;

■ Atendimento às expectativas dos acionistas e clientes.

As estratégias de continuidade oferecem soluções alternativas para se manter operacionais os processos críticos de uma organização. São respostas de proteção às vulnerabilidades dos processos críticos apontadas na análise de risco. Estas soluções devem ser preparadas e testadas antes de uma interrupção nos negócios, de modo a garantir a eficácia da estratégia com ganhos para a empresa.

Existem várias estratégias possíveis de utilização em caso de interrupção nos negócios. A utilização ou não dessas estratégias

depende do grau de risco e impacto levantados e da decisão do gestor dos processos.

As estratégias de continuidade de negócios têm de estar alinhadas à estratégia corporativa e à direção fornecida pela alta administração da organização.

Entre outros aspectos relevantes dessa estratégia encontram-se a revisão regular das análises de risco e impacto dos processos críticos, a formação de equipe especializada em gestão da continuidade de negócios, a implantação de um programa corporativo de GCN e a providência dos recursos necessários para um rápido retorno à normalidade dos negócios.

ESTRATÉGIAS PARA GARANTIA DA CONTINUIDADE DE NEGÓCIOS

Definição:

As estratégias de continuidade de negócios são os mecanismos e soluções definidos com o objetivo de mitigar os riscos provenientes de uma indisponibilidade que afetem direta ou indiretamente os processos estratégicos da empresa.

As estratégias de continuidade devem ser detalhadas nos planos de continuidade de negócios, para serem ativadas quando ocorrerem os cenários de interrupção.

Como vimos, a avaliação de processos estratégicos identifica os processos críticos e classifica-os por grau de impacto e risco. O gestor deve perceber as vulnerabilidades de seus processos e confeccionar os planos de continuidade.

Após perceber quais processos possuem maior grau de impacto e risco, algumas decisões estratégicas têm de ser tomadas pelo gestor. Tais decisões envolvem identificar as estratégias de continuidade, verificar as estratégias alternativas possíveis, analisar a relação custo e benefício da adoção das estratégias e comunicar às instâncias decisórias da organização, para aprovação, as ações a serem tomadas.

Quanto à esfera decisória, as ações podem ser:

■ Não fazer nada: quando o risco é aceitável;

■ Mudar ou finalizar o processo: alinhar o processo a outros processos da organização;

■ Garantir um seguro: providenciar recursos suficientes mediante a contratação de apólices de seguro para garantir a possível perda;

■ Baixar a mitigação: providenciar ações para mitigar o risco;

■ Desenvolver um plano de continuidade de negócios: modo mais eficaz de prover resiliência à organização, em caso de interrupção nos negócios.

O gestor irá considerar opções estratégicas para os processos de maior grau de impacto e risco e para os recursos que cada processo consumirá durante sua restauração. A(s) estratégia(s) mais(s) apropriada(s) depende(m) de uma série de fatores, como:

■ O período máximo de interrupção tolerável;

■ Os custos de implementação de uma ou mais estratégias;

■ As consequências de não se agir.

Estratégias podem ser necessárias para os seguintes recursos:

■ Pessoas;

■ Instalações;

■ Tecnologia;

■ Informação;

■ Fornecedores de suprimentos ou serviços.

Em cada caso o gestor deve evitar implementar uma solução de continuidade que possa ser afetada pelo mesmo incidente que causou a interrupção no processo de negócio.

Formalização

Após a identificação dos processos críticos, a avaliação de impacto e risco e a definição das estratégias de continuidade, tornam-se necessários o detalhamento e a formalização dessas estratégias.

As estratégias de continuidade são formalizadas por meio da elaboração e documentação dos planos e procedimentos de continuidade de negócios. Os planos de continuidade são parte integrante do ciclo de vida dos processos de negócio, devendo, portanto, ter atenção especial do administrador.

Vários fatores influenciam a elaboração dos planos de continuidade de negócios: recursos, tempo de recuperação, prioridades, responsabilidades, estrutura organizacional, lista de acionamento etc.

Um plano de continuidade deve ser conciso, escrito de forma clara e objetiva, de fácil leitura e conter todas as informações relevantes para uma melhor tomada de decisão no momento inicial da interrupção.

Veja as principais informações que devem estar contidas nos planos:

■ Objetivo geral do plano;

■ Listagem dos processos atendidos pelo plano; cenários para os quais o plano se aplica;

■ Estratégias de continuidade adotadas;

■ Critérios de avaliação dos testes e exercícios;

■ Situação para a decretação ou ativação dos planos;

■ Premissas ou observações essenciais para funcionamento do plano;

■ Periodicidade de realização de testes ou exercícios.

Bibliografia:

ALVIM, Paulo César Rezende de Carvalho. **Inteligência competitiva nas empresas de pequeno porte**. In: I Workshop Brasileiro de Inteligência Competitiva.

FERREIRA, Fernando Nicolau Freitas. **Segurança da Informação**. Rio de Janeiro: Ciência Moderna, 2003.

FERREIRA, Fernando Nicolau Freitas; ARAÚJO, Márcio Tadeu de. **Política de Segurança da Informação**: guia prático para elaboração e implementação. Rio de Janeiro: Ciência Moderna, 2006.

MANDARINI, Marcos. **Segurança Corporativa Estratégica**. São Paulo: Manole, 2006.

MOREIRA, Nilton S. **Segurança mínima**: uma visão corporativa da segurança de informações. Rio de Janeiro: Axcel Books, 2001.

BRASILIANO, Antonio Celso Ribeiro. **Manual de Análise de Risco**. São Paulo: Sicurezza, 2003.

BRASILIANO, Antonio Celso Ribeiro. **Manual de Planejamento** - Gestão de Riscos Corporativos. São Paulo: Sicurezza, 2003.

BRASILIANO, Antonio Celso Ribeiro. **Manual de Planejamento Tático e Técnico em Segurança Empresarial**. São Paulo: Sicurezza, 2003.

BRASILIANO, Antonio Celso Ribeiro. **Planejamento da Segurança Empresarial**. São Paulo: Sicurezza, 1999.

Outras fontes de consulta

CURSOS do Banco do Brasil: Agente de Registro. Certificação Digital. Grafoscopia.

Universidade Corporativa Banco do Brasil – Curso Gestão de Segurança

DANTAS FILHO, Diógenes. **Segurança e Planejamento**. Rio de Janeiro: Ciência Moderna, 2004.

DANTAS FILHO, Diógenes. **Segurança Pessoal**. Rio de Janeiro: Ciência Moderna, 2002.

GIL, Antonio de Loureiro. **Segurança Empresarial e Patrimonial**. São Paulo: Atlas, 1995,

PARA SUAS ANOTAÇÕES:----------

