GUIA PRÁTICO

Como fazer sua análise de risco

MarketTrends... | GlobalSuite SOLUTIONS

GUIA PRÁTICO

Como fazer sua análise de risco

MarketTrends... | GlobalSuite SOLUTIONS

MarketTrends... | GlobalSuite SOLUTIONS

Índice

Introdução

Hoje em dia, todo gestor de Risco de uma organização precisa trabalhar com uma plataforma que permita centralizar e padronizar suas análises e, desta forma, identificar possíveis adversidades e executar efetivamente seus procedimentos de mitigação. Graças à experiência em ajudar muitas empresas na análise de risco, ao iniciar é sempre aconselhável fazer algumas perguntas:

01.

Sobre "elementos ou ativos": Como minha empresa está estruturada? O que vou analisar: aplicações, instalações, processos...?

02.

Sobre "análise de risco": Que riscos podem sofrer todos esses elementos que dão vida ao negócio? Posso agrupar esses riscos por categorias? Que abordagem eu dou para a análise?

03.

Sobre "controles": Como posso reduzir as consequências desses riscos se eles se materializarem? Posso evitar que esses riscos aconteçam?

04.

Sobre "resultados": Como posso tirar conclusões da análise que fiz? Existe uma maneira fácil e atraente de apresentar os resultados de uma análise de risco?

Como posso obter as informações acima se não estiver presente em todas as atividades da empresa?

Não há uma resposta única para cada uma delas, mas considerar possíveis soluções ajudará você a canalizar esse projeto que **garantirá tranquilidade e segurança em sua organização.**

Além disso, neste guia apresentaremos um **extrato de uma metodologia desenvolvida pela GlobalSuite Solutions e que vários clientes implementaram com sucesso.**

Se você conseguiu responder às perguntas que vimos anteriormente, agora você deve estar se perguntando como organizar todas as informações e realizar sua análise de risco.

Para isso, **recomendamos a utilização do GlobalSUITE®**, uma **ferramenta GRC que lhe permitirá centralizar, automatizar e acompanhar** o seu trabalho para que tenha todos os riscos sob controle.

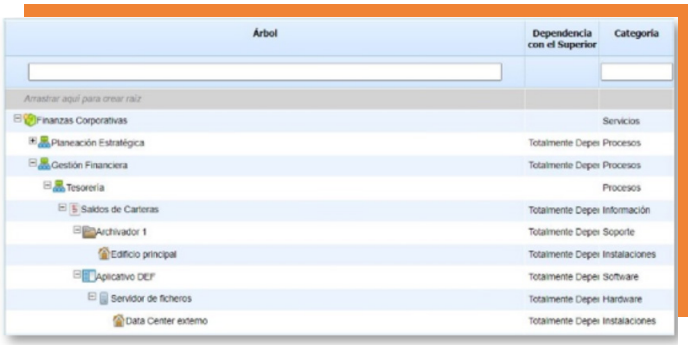
02. Elementos

Nesse ponto, é provável que você já saiba ou, pelo menos, tenha uma intuição sobre **quais elementos de sua empresa estão suscetíveis a algum risco**, seja ele operacional, de segurança da informação ou o cometimento de um delito ou infração. Você os tem agrupados por categorias? Você estabeleceu alguma hierarquia entre seus elementos? Existem elementos cujos riscos afetarão outros acima deles?

Propomos um desafio: tome como ponto de partida o esquema organizacional da sua empresa. Quais áreas e departamentos você vê? Agora pense em quais serviços essas unidades oferecem, talvez seja apenas um ou talvez sejam vários. O primeiro passo é selecionar uma área familiar e escrever o nome em uma planilha, arquivo de processamento de texto ou apenas em um pedaço de papel.

O segundo passo envolverá a listagem dos serviços prestados por esta área; aponte-os horizontalmente logo abaixo e una-os com setas com a área, criando assim uma árvore de dependências, uma hierarquia. Neste ponto, você sabe se esses serviços são suportados por processos? Em caso afirmativo, anote seus nomes no serviço correspondente. Considere se, para a análise que deseja realizar, você precisa continuar aprofundando essa estrutura. No caso de analisar possíveis delitos ou infrações você provavelmente vai parar no mapa organizacional, mas e se o seu objetivo for fazer uma análise com outra abordagem? Pense em quais elementos tornam possível prestar um serviço e como eles dependem uns dos outros para funcionar: ferramentas, software, hardware, instalações...

No GlobalSUITE® foi desenvolvida uma opção chamada Inventário, para que você possa reunir em um só lugar todos aqueles elementos que você vai analisar e que você também pode classificar por meio de uma Árvore de Dependência.



No topo da sua árvore deve localizar os elementos da categoria Serviços, ou se preferir, Linhas de Negócio ou mesmo Sociedades caso pretenda analisar um grupo empresarial por entidades. O próximo passo será identificar as subdivisões de seus Serviços e detalhar cada uma delas até atingir o nível de detalhamento necessário para sua análise de risco.

03. Análise de riscos

Você se lembra das perguntas no início? Com a estrutura da nossa Árvore de Dependência, prevemos que dois tipos de análise possam ser realizados: uma Operacional e outra de Segurança da Informação. E você, qual abordagem tem em mente?

Propomos um segundo desafio: escolha um elemento da árvore que você começou a desenhar no ponto anterior. É um serviço ou um processo? O que pode acontecer para que ele não possa mais ser prestado regularmente? E se for um software? Quais ameaças podem nos impedir de acessar os dados que ele contém? **Faça uma lista de riscos ou ameaças que podem afetar o elemento que você vai analisar.** Em seguida, em uma escala de 1 a 5, avalie a probabilidade para que se concretizem e o impacto que eles teriam sobre os objetivos de seu serviço ou a operação de seu software, por exemplo. Agora vamos contar como analisamos nosso processo de **Gestão Financeira em 4 passos:**

Primeiro passo

Enquadramos o processo numa **Análise de Risco Operacional,** uma vez que a intenção é realizar um estudo dos riscos que podem afetar o bom funcionamento dele.

Segundo passo

O próximo passo foi identificar os riscos potenciais que poderiam afetar a Gestão Financeira da nossa organização. A faixa do Risco Inerente foi estabelecida em 5 níveis: desde um risco muito baixo até um nível extremo. Mas com base em quê classificamos um risco como moderado ou extremo? Muito fácil, baseado em dois pilares: a probabilidade desse risco se materializar e o impacto que teria no nosso processo.

Riesgo Operativo	Causas	Impacto Inherente	Probabilidad Inherente	Nivel Riesgo Inherente
[OP.10] Empleados no familiarizados con las medi	Incorrecto procesos de selección. No realizar form	Alto	Muy alta	Extremo
[Leg.12] Incumplimiento requisitos legales de prod	Incumplimientos respecto a la propiedad intelectua	Alto	Moderada	Alto
[Leg.3] Imposibilidad de ejecución de una operació	Cambios legales o en las normas de un país. Caml	Muy alto	Muy alta	Extremo
[OP.17] Empleados con habilidades inadecuadas c	Mala selección del personal. Personal no correctan	Moderado	Alta	Alto
[OP.32] Interrupción de telecomunicaciones	No disponer de una línea de contingencia	Alto	Moderada	Alto
[OP.52] Competencia desleal (Dumping)	Empleados descontentos, falta de clausulas de cor	Moderado	Alta	Alto
[OP.9] Degradación estructura organizacional	Cambios en la estructura, cambios de dirigentes.	Alto	Moderada	Alto
[Leg.2] Incidencias negativas sobre actividades de	Incumplimientos respecto a la propiedad intelectua	Moderado	Alta	Alto
[OP.12] Accidentes de trabajo que involucren a em	Falta de medidas de seguridad.	Bajo	Alta	Alto

03. Análise de riscos

Terceiro passo

O terceiro passo da nossa análise consistiu em **descobrir até que ponto os controles que associamos a cada risco reduziram sua gravidade.** Para isso, fizemos uma média do nível de eficácia dos controles ao nível de cada risco específico. Você pode estar se perguntando, **em que nos baseamos para definir o nível de eficácia de um controle?** Vamos te explicar no próximo ponto onde falaremos sobre controles ou ações mitigadoras.

Quarto passo

O objetivo do quarto passo da nossa análise de risco foi **determinar o nível de Risco Residual.** O que isso significa? Trata-se de descobrir em quantos níveis reduzimos o Risco Inerente graças aos controles, aplicando-os à **probabilidade** e/ou ao **impacto**.

04. Controles

Eles são a última peça deste quebra-cabeça e também uma peça crucial.

Sem eles seria impossível mitigar os riscos que ameaçam a organização. Mas **são todos igualmente eficazes? A resposta é não, alguns são mais bem desenhados do que outros: têm um responsável, são automatizados e são aplicados regularmente,** outros não. E é precisamente com base nesses critérios, e mais alguns, que **calculamos a eficácia dos nossos controles.**

Nombre	Tipo Control	¿Está documentado?	¿Responsable asignado?	Tipo de ejecución	Percepción de efectividad	Aplicación	EFECTIVIDAD CONTROL
Asignación de Perfiles	Correctivo	SI, y se encuentra actualiz	SI	Automática	Poca efectividad	Eventualmente	Excelente
Bloqueo de Intermediarios Financieros que In	Preventivo	SI, y se encuentra actualiz	NO	Automática	Confirmada su efectividad	Siempre	Excelente
Cerrar líneas por agotamiento de recursos	Preventivo	SI, y se encuentra actualiz	SI	Automática	Confirmada su efectividad	Eventualmente	Excelente
Seguimiento a las carteras por parte del Com	Correctivo	SI, pero no se encuentra a	NO	Manual	Efectividad media	Siempre	Moderada

Propomos um terceiro desafio: Você se atreve a identificar os controles que realiza em sua organização para reduzir algum dos riscos ou ameaças que identificou anteriormente?

Vamos começar com um. Quando tiver, indique ao lado, em uma escala de 1 a 5, quão eficaz ou maduro é esse controle em relação ao risco que deseja reduzir. Pense também em quantos níveis a probabilidade ou o impacto seriam reduzidos se seu controle classificasse como 5. E se você colocar um 1? Isso significa que o controle é ineficaz e não mitiga?

> **Os controles são a última peça do quebra-cabeça e são cruciais para mitigar os riscos**

05. Resultados

Se sua empresa já possui metodologias estabelecidas de gestão e controles de riscos e você já realizou análises, os três últimos desafios permitirão que você reflita sobre o desenho do que já construiu.

Talvez você tenha pensado em alguma melhoria ou reestruturação com o objetivo de obter um certificado ISO, corrigir não conformidades decorrentes de uma auditoria ou simplesmente levar sua análise para o próximo nível. Se, por outro lado, você ainda está ingressando neste setor ou acabou de iniciar sua experiência, esses desafios vão incentivá-lo a traçar metas, considerar alternativas e avançar para um modelo de análise que se adapte às necessidades de sua empresa. É importante deixar tudo isso pronto para que a fase de reporte dê uma imagem verdadeira e consolidada da situação em que nos encontramos. A seguir, contaremos como termina nossa experiência.

Após estabelecer nossas metodologias e realizar nossa análise de risco, elaboramos um relatório e apresentamos aos nossos superiores. Para isso, elaboramos um documento descrevendo os achados mais relevantes: os Riscos Residuais que ultrapassaram o limite estabelecido como aceitável na nossa empresa, o nível moderado.

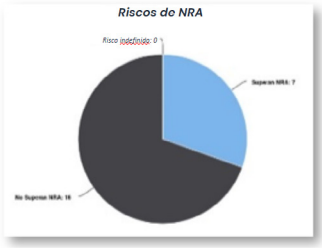
Esta tabela interativa oferecida pela GlobalSUITE® nos permitiu filtrar para saber em quais processos se encontram os riscos que ultrapassam o nível moderado e quais riscos associados a eles ultrapassam esse nível.

Probabilidade Inerente/Impacto Inerente	Muito Baixo	Baixo	Moderado	Alto	Muito Alto
Muito alta	0	0	0	0	0
Alta	0	1	3	2	0
Moderada	0	5	2	3	0
Baixa	0	1	2	1	0
Muito Baixa	0	0	1	0	0

Se você quiser ir mais longe, sugerimos adicionar uma comparação entre Risco Inerente e Risco Residual ao seu relatório. É uma maneira ideal de representar graficamente e, além disso, de forma muito visual e intuitiva como os resultados melhoraram.

Além disso, recomendamos que você apresente seus resultados **tanto por análise como por elementos**, principalmente mostrando aqueles que são mais relevantes dentro da organização. Como exemplo, mostro dois gráficos que usamos em nossa apresentação, ambos fornecidos pela GlobalSUITE® e se referem ao processo de Gestão Financeira.

O gráfico "Riscos de Elementos" mostra quantos Riscos Residuais de cada nível temos em nosso processo e o gráfico "Riscos de NRA" informa quantos riscos excedem o nível de risco aceitável, definido como moderado.



06. Conclusões

Não é difícil identificar que apesar de ter vários tipos de riscos, bem como as diferenças intrínsecas entre cada um deles, é fundamental para a boa governança e o futuro da organização poder monitorar todos eles de forma integrada e centralizada, contando com um mapa de riscos completo da organização.

Esse monitoramento, aliado a uma boa definição dos indicadores-chave de KRI, fornece sinais de alerta antecipados para prever possíveis desvios ou impactos e aproveitá-los novamente para transformar um eventual risco em uma oportunidade que faz a diferença.

Por todas estas razões, de forma a gerir o mapa de risco de forma centralizada e eficiente, com uma visão 360º, aproveitando as dependências e sinergias existentes entre os diferentes tipos de risco e podendo assim identificar rapidamente os possíveis efeitos que um sinal de risco precoce teria no mapa de objetivos estratégicos e processos críticos da empresa, é fundamental ter um GRC+ como o GlobalSUITE®, fator-chave tanto nesta gestão como na tomada de decisão e boa governança.

Analise, preveja e proteja para obter uma visão completa do que está acontecendo em sua organização!

MarketTrends... | GlobalSuite SOLUTIONS

A **MarketTrends** é uma distribuidora de alto valor agregado que reúne em seu portfólio uma ampla gama de produtos e serviços de marcas líderes globais e locais, baseada nos pilares tecnologia, processos e pessoas, desempenhando um importante papel na estratégia de empresas que buscam conformidade em seus processos para alavancar resultados.

Entre as soluções que oferece está a **GlobalSuite ®,** uma plataforma GRC **para otimizar os processos de risco, segurança, continuidade, auditoria, privacidade e conformidade** em seu negócio.

A plataforma foi concebida pela empresa de mesmo nome, a GlobalSuite Solutions, que há mais de 15 anos se dedica a **fornecer e implementar soluções em questões de Risco, Segurança, Continuidade, Conformidade Legal, Auditoria,** entre outras, em empresas de diversos setores como financeiro, seguro, industrial, transporte, telecomunicações, energia, público, etc.

Sobre o autor

Bartlomiej Palka

Consultor Funcional da GlobalSUITE® e certificado como GlobalSUITE® Certified Expert GSE. Possui 7 anos de experiência em configuração e parametrização de softwares do tipo ERP e GRC. Desenvolveu a sua carreira profissional em vários países europeus, o que lhe permitiu alargar a sua perspectiva e dar diferentes abordagens aos seus projetos. Dentro do GlobalSUITE®, ele ajudou vários clientes a implementar e melhorar os módulos relacionados a Conformidade, Continuidade de Negócios, Gestão de Riscos, RGPD e Segurança da Informação.

MarketTrends... | GlobalSuite SOLUTIONS

Para mais informações ou um teste grátis de como sua organização pode automatizar seus processos de GRC

- contato@mtrends.com.br
- 11 5643 1320
- www.mtrends.com.br