REVISTA
GESTÃO DE RISCOS
EDIÇÃO 110 | JUNHO 2017

b&a BRASILIANO & ASSOCIADOS

INTERISK Inteligência em Riscos

11

A importância estratégica da Classificação dos Dados PARA A SEGURANÇA CIBERNÉTICA

Gerir riscos no mundo com ameaças e oportunidades exponenciais: conseguimos?

O futuro é a execução imperfeita do desconhecido, no presente. Nos negócios, o futuro é sempre uma questão de vida ou morte. Quem consegue dar o salto entre o aqui e agora e o lá e então... sobrevive. Todos os outros irão cair com o tempo, haja visto o grande volume de CNPJ's que existem no cemitério empresarial.

Prof. Dr. Antonio Celso Ribeiro Brasiliano, CRMA, CES, DEA, DSE, MBS

Doutor em Science et Ingénierie de L'Information et de L'Intelligence Stratégique, pela Université East Paris - Marne La Vallée – Paris – França, é presidente da Brasiliano INTERISK.

abrasiliano@brasiliano.com.br

Hoje com a Quarta Revolução Industrial, puramente tecnológica e digital, a inovação passa a ser um componente estratégico para todo e qualquer tipo de negócio, indo desde a modelagem de como fazer o negócio em si, até os produtos e serviços oferecidos ao mercado.

Para que a empresa possa dar o salto para o futuro, a inovação tem que começar a ser feita no presente, aqui e agora! Ou no passado para poder entender as origens. O grande desafio dos executivos de hoje é a de resolver a luta entre passado, presente e futuro, no momento atual, ou seja, no presente. O passado teima em ir para o futuro, através do presente; o futuro não encontra um caminho para vir para o presente de lá; e, no presente, não há tempo suficiente para tratar nem de um nem de outro. O presente consome possíveis futuros, pois a volatidade, incerteza, complexidade e ambiguidade é tamanha que os executivos acabam ficando míopes, enxergando apenas o retrovisor.

O mundo dos negócios e os dos riscos, vivem em paralelo, com uma velocidade e expansão exponencial. Conforme escrevi, apenas citando os 6D's, no meu último Ponto de Vista (Revista 109): digitalizado, dissimulado, disruptivo, desmaterializador, desmonetizador e democratinizador. Neste resolvi detalhar cada um para que possamos entender e identificar seus sintomas das mudanças radicais do mercado que estamos inseridos, antecipando desta forma ameaças e oportunidades denominadas de exponenciais.

Digitalização: essa ideia começa com o fato de que a cultura torna o progresso cumulativo. A inovação ocorre à medida que há compartilhamento e troca de ideias. Qualquer coisa pode ser digitalizada, ou seja, representada por uns zeros, podendo ser disseminada à velocidade da luz ou ao menos da internet. A disseminação segue o padrão de uma curva exponencial;

Decepção: Logo em seguida a digitalização, vem a decepção, onde o crescimento é disfarçado, passa quase despercebido. Isso ocorre porque a duplicação dos números pequenos produz, logicamente, resultados pequenos, o que leva a uma interpretação míope, como lento crescimento. Ponto importante é que neste estágio é onde os executivos de negócios e de riscos devem colocar a lupa, pois o crescimento exponencial começa a tornar-se disruptivo. Caso os executivos não enxerguem esta disrupção, perdem a janela de oportunidade;

Disrupção: é uma inovação tecnológica que cria um mercado e abala outro já existente, de tal forma que pode jogá-lo para fora da arena de competidores. A pergunta sempre é a mesma: por que não enxergamos esta disrupção? Simples a resposta, a disrupção sempre vem após a decepção,

então a ameaça original sempre vai aparecer pequena e insignificante. Então se o gestor de risco não consegue enxergar o tsunami vindo, quando este chega, vem arrasando com uma série de produtos e serviços e, geralmente as empresas são pegas de surpresa.

Desmonetização: significa retirar o dinheiro da equação. Os produtos e serviços acabam ficando praticamente "free". Exemplo: O Skype desmonetizou a telefonia de longa distância; O Napster a indústria da música. Mas como a desmonetização é também dissimulada, as empresas, com seus executivos e gestores de riscos, nunca estão preparadas para as mudanças radicais;

Desmaterialização: Se a desmonetização desaparece com o dinheiro, antes pago com serviços e ou produtos, a desmaterialização consiste no desaparecimento dos próprios produtos e serviços. Citamos o caso da Kodak, com a Câmera Digital, que fez o desaparecimento dos filmes fotográficos e em seguida com a vinda dos Smartphones, que logo passou a ter como componente uma câmera de alta qualidade, as câmeras digitais se desmaterializaram. As câmeras passaram a virem grátis nos telefones. Em 1976 a Kodak possuía 85% do negócio de câmeras fotográficas. Em 2008, um ano após o lançamento do iPhone (primeiro smartphone com câmera digital de alta qualidade), o mercado dos filmes e câmeras fotográficas não mais existia!

Democratização: É o que ocorre quando os custos tangíveis ficam tão baixos que se tornam acessíveis a quase todo mundo. A democratização é o resultado lógico da desmonetização e da desmaterialização. Para que tenhamos uma ideia deste tsunami, o Professor Richard Foster, da Yale University, realizou uma pesquisa onde concluiu que o tempo médio das 500 maiores empresas, na década de 1920 era em torno de 67 anos. Hoje não é mais realidade. Os últimos 3 D's, em cadeia produzem uma reação exponencial, desmontando organizações e setores quase que da noite para o dia, reduzindo o tempo médio de vida no século XXI para 15 anos. O Professor Foster comenta ainda que em 2020 mais de três quartos das 500 maiores empresas serão organizações que ainda não ouvimos falar!

Pergunta estratégica para nós, gestores de riscos: conseguiremos acompanhar os riscos emergentes e disruptivos que impactarão massivamente os serviços e produtos da empresa? Identificaremos as incertezas críticas a tempo de reduzir seus impactos?

São perguntas sem respostas ainda. Estamos tentando acompanhar, mas nosso desafio é também muito grande. Um ponto para mim é claro, temos que continuar "pisando em terreno minado", mergulhando de cabeça na incerteza, com o objetivo de entender as causas e origens. Quanto mais formos amantes da incerteza, mais conheceremos as suas características intrínsecas e poderemos melhor enfrenta-la. Só desta maneira é que a gestão de riscos agregará valor para a empresa neste mundo VICA: Volátil, Incerto, Complexo e Ambíguo!

Boa leitura e sorte!

Antonio Celso Ribeiro Brasiliano
Publisher

acerte seu FUTURO!

ÚLTIMOS DIAS DE INSCRIÇÃO!!

MBA em Gestão de Riscos Corporativos

turmas de agosto

CURITIBA e SÃO PAULO

INFORMAÇÕES

FESP FACULDADE DE ENGENHARIA SÃO PAULO

Rua dos Ingleses, 569 -
Bela Vista - SP

b&a BRASILIANO&ASSOCIADOS GESTÃO DE RISCOS

INTERISK Inteligência em Riscos

Raphael de Melo Alves

Ex-militar do Exército Brasileiro, formado em Gestão de Segurança Privada, MBA em Gestão de Projetos e extensão universitária Master Business Security - MBS da Brasilinao INTERISK

Segurança patrimonial: análise para solução de problemas

A segurança patrimonial (empresarial/corporativa) vem gradativamente tomando seu definitivo espaço dentro das organizações, com isso, a cada dia esta área (departamento) ganha notória visibilidade sendo constantemente acionada para participar dos fóruns internos de discussões sobre os mais variados e diferentes temas do dia a dia, ligados tanto diretamente quanto indiretamente a suas atividades.

Os cenários encontrados pelo gestor de segurança são sempre desafiadores, exigindo dinamismo e autocontrole para a solução de problemas, problemas dos quais em sua grande maioria não se tem a devida tratativa para solucioná-los e acabam por receber ações “imediatistas“ para estancar e tirar foco do problema, ou seja, o famoso “apaga incêndio”. Por não ter uma base de dados (indicadores) para mapeamento e tratamento de ocorrências acaba-se por não encontrar a causa raiz e não se fazendo as devidas análises para ações efetivas, fazendo com que os mesmos problemas ressurjam constantemente forçando o gestor a desperdiçar esforços e investimentos desnecessários em ações ineficazes.

Partindo da definição, considerando-se que – Problema é um resultado indesejável de um trabalho, podemos elencar alguns exemplos de sintomas de problemas dos quais requerem a atenção do gestor de segurança, sendo eles:

- Número elevado de ocorrências;
- Alto índice de absenteísmo;
- Baixa qualidade dos serviços entregues por prestadores de serviços;
- Pessoal desmotivado;
- Rotatividade de efetivo;
- Desperdícios em geral e etc.

Os problemas costumam gerar perdas e podem afetar a sobrevivência da empresa.

Partindo do fato em que – Não há culpados para os problemas da empresa, pois existem causas, podemos citar algumas das mais conhecidas ferramentas da qualidade (vide abaixo) que podem auxiliar o gestor em uma análise e mapeamento de seus indicadores e possíveis problemas para a tomada de decisão, tendo consigo uma visão por completa de onde atuar com esforços e investimentos para mitigar suas principais causas/fatores e após, aplicar um plano de monitoramento efetivo para acompanhamento e tratamentos pontuais caso haja a necessidade.

- Brainstorming: Usada para gerar ideias rápidas e em grande quantidade;
- Diagrama de dispersão: Permite a identificação do grau de relacionamento entre duas variáveis consideradas em uma análise;
- Matriz G.U.T.: Utilizada para priorização das diversas ações a serem tomadas em plano de ação;
- Diagrama de Pareto 80:20: Onde exemplificando fala-se que 20% dos problemas representam 80% dos custos de desperdícios;
- Causa e efeito (diagrama de Ishikawa): Ferramenta destinada ao mapeamento de causas/fatores das quais consiste o problema;
- 5w 2h: Utilizada para planejar, organizar e administrar ações a serem tomadas;
- Método DMAIC: Utilizada em sua grande maioria com a finalidade de melhorar processos já existentes.

Tendo essas e muitas outras ferramentas à disposição para análise, mapeamento e identificação de problemas, podemos visualizar de forma um pouco mais ampla algumas aplicações conforme exemplo abaixo:

Exemplo ilustrativo – análise e mapeamento de indicadores.

Obs.: Importante na análise prévia dos indicadores, considerar e analisar os períodos sazonais, férias, épocas relevantes à atividade fim da empresa e etc., pois podem impactar no mapeamento de problemas.

Faltas e atrasos

SEGURANÇA PATRIMONIAL

Título do Documento: Alto índice de faltas e atrasos — **Líder:** Gestor de segurança

Integrantes do Time: Segurança Patrimonial (empresarial/corporativa). — **Dono do Processo:** Segurança Patrimonial — **Data:** 27/06/2017

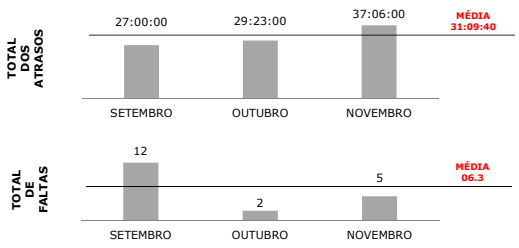
DEFINIR

DESCRIÇÃO DA OPORTUNIDADE

Reduzir os índices de absenteísmos existente na equipe de segurança.

MEDIR

MÉTRICAS



DEFINIR

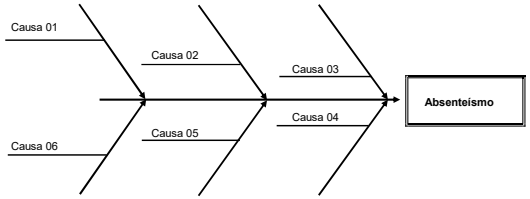
OBJETIVO PÓS ANÁLISE DAS MÉTRICAS

Reduzir os índies de faltas e atrasos em **70%** sobre a média apresentada.

ANALISAR

CAUSA RAIZ

Elencar as principais causas (fatores internos e externos)



PLANEJAR

MATRIZ G.U.T

Ordenar as causas de acordo com priorizações para tomada de ações.

Causas	Gravidade	Urgência	Tendência	GxUxT	Prioridades
Causa 01	5	5	5	125	**1º**
Causa 02	5	4	5	100	**3º**
Causa 03	4	4	4	64	**5º**
Causa 04	5	5	4	100	**2º**
Causa 05	5	4	4	80	**4º**
Causa 06	4	3	3	36	**6º**

IMPLEMENTAR

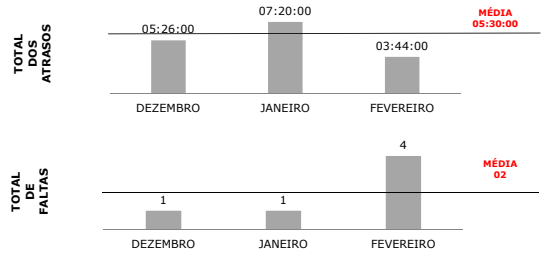
PLANO DE AÇÃO 5W 2H

Elencar ações e responsáveis de acordo com a priorização anterior.

What? O que?	Why? Por que?	Where? Onde?	Who? Quem?	When? Quando?	How? Como?	How Much? Quanto?	Status
xxxxxxxxx	xxxx	xxxx	xxxx	xxxx	xxxxxxx	xxxx	xxxx
xxxxxxxxx	xxxx	xxxx	xxxx	xxxx	xxxxxxx	xxxx	xxxx
xxxxxxxxx	xxxx	xxxx	xxxx	xxxx	xxxxxxx	xxxx	xxxx
xxxxxxxxx	xxxx	xxxx	xxxx	xxxx	xxxxxxx	xxxx	xxxx
xxxxxxxxx	xxxx	xxxx	xxxx	xxxx	xxxxxxx	xxxx	xxxx

CONTROLAR

MEDIÇÃO E AVALIAÇÃO DAS CONTRAMEDIDAS



RESULTADO DO PROCESSO

Após as ações adotas e acompanhamento dos processos, foi superado o objetivo de redução pré estabelecido de **70%**, alcançando a redução de **83%** sobre a média dos atrasos e alcançando o objetivo de redução de **70%** sobre as faltas.

Com o conhecimento dos sintomas e das causas primárias, é importante também conhecer as diferenças entre os tipos de ações que podem ser tomadas como:

- *Ação reativa: Trata o efeito, não assegura que ele não possa recorrer, apenas dispõe sobre o que fazer com o efeito indesejado, decisão tipicamente operacional, não requerendo análise.*
- *Ação corretiva: Elimina a causa/fator real ou minimiza a influência de uma causa isolada sobre o efeito indesejado, atuação no processo com o objetivo de impedir a recorrência do problema ou melhorar os índices de desempenho planejados.*
- *Ação preventiva: Levam-se em consideração todas as causas potenciais que possam influenciar direta ou indiretamente o efeito (problema) em maior ou menor intensidade, atuação no sistema como um todo para bloqueio das causas potenciais, não apenas em um processo do sistema.*

Levando em consideração o modelo ilustrativo e suas aplicações, podemos aplicar a diversas áreas de negócios, a área de "Prevenção de Perdas", por exemplo, podemos aplicar aos indicadores de ocorrências dos P.A.R. (Produto de Alto Risco) ou até mesmo nos P.A.Q. (Produto de Alta Quebra) podendo mapear e redesenhar os processos através de fluxogramas.

Importante destacar que toda implementação de uma solução requer um planejamento, e para cada solução a ser implementada requer que se tenha validação para que após sua implementação se tenha comprovação da eficácia das ações.

"Se você quer algo novo, você precisa parar de fazer algo velho" – Peter Drucker.

NOVA PARCERIA DE SOLUÇÃO EM INTELIGÊNCIA!

A **Brasiliano INTERISK** em parceria com a **Boldon James** fornecedora global de soluções de Segurança e Classificação de Dados, agrega maior valor para nossos clientes.

Agora em nossas soluções de inteligência em riscos também oferecemos a classificação e gerenciamento de informações digitais para empresas de todos os portes e segmentos com o classificador da Boldon James.

CONHEÇA MELHOR A NOSSA SOLUÇÃO!!

b&a
BRASILIANO & ASSOCIADOS
GESTÃO DE RISCOS

INTERISK
Inteligência em Riscos

boldonjames
A QinetiQ Company

método

Prof. Dr. Antonio Celso Ribeiro Brasiliano, CRMA, CES, DEA, DSE, MBS
Doutor em Science et Ingénierie de L'Information et de L'Intelligence Stratégique, pela Université East Paris - Marne La Vallée – Paris – França, é presidente da Brasiliano INTERISK
abrasiliano@brasiliano.com.br

A importância estratégica da classificação dos dados: primeira barreira contra fuga de informações e ataques cibernéticos

Conhecer suas informações e ou dados que a empresa possui deve ser uma preocupação constante do Chief Information Security Officer – CISO, ou no Brasil o responsável pela segurança das informações e cibernética nas instituições.

método

Quando falamos em conhecer os dados que circulam pela empresa, de dentro para fora, de fora para dentro e entre os colaboradores, estamos falando em colocar em prática a Política de Segurança da Informação, que em sua grande maioria, prevê a classificação dos dados e informações sobre o sigilo e o nível de resguardo que ela deveria possuir, mas que na prática isso não acontece.

1.Introdução

A importância da classificação dos dados/informações da empresa passa a ser estratégica por uma simples razão: se for executada de forma clara e consciente pelos colaboradores, a classificação fica sendo sua primeira barreira de defesa contra possíveis riscos de fuga, roubo, sequestro e ataques cibernéticos. Por que? Pelo simples fato do usuário saber que aquela informação que ele está lidando é de importância estratégica para a empresa, tanto o texto como também anexos de e-mails. As empresas devem possuir uma ferramenta, um software denominado de Classificador de Dados/Informações, que obriga o usuário a praticar as regras da sua política de segurança da informação.

Os mercados norte-americano e europeu estão muito mais maduros que o do Brasil, além de terem a questão regulatória, que as empresas têm o dever de proteger os dados/informações de seus clientes. Ou seja, neste rol entram os bancos, indústria farmacêutica, hospitais, laboratórios, cartões de crédito, entre outros. O percentual de empresas que utilizam software de classificação é de 44% e mais 18% que pretendem implantar nos próximos 12 meses. Esta pesquisa foi realizada com 436 organizações, com mais de 1000 funcionários, segundo o Forrester's Global Business Technographics Security Survey, 2015.

A segurança dos dados/informações passa por um processo, que deve ser estruturado em cinco fases:

1. Identificação dos dados/informações estratégicas e sensíveis na empresa;
2. Entender os dados/informações sensíveis: dissecar causa e origem dos dados e informações;
3. Diagnóstico: Ambiente regulatório – o que a legislação obriga? E o ambiente interno em termos de sensibilização dos usuários dos dados/informações sensíveis;
4. Realizar uma análise de riscos para saber o nível de criticidade em função da fragilidade: controles x riscos existentes;
5. Proteção dos dados/informações: classificação do nível do dado/informação e medidas de segurança.

Pelos processos acima estruturados, vemos claramente que a primeira medida é a empresa saber quais dados/informações são sensíveis e estratégicas. Ou seja, a empresa deve saber o que é importante proteger, o que é sensível para seus negócios e se esses dados forem roubados / violados a instituição sofrerá consequências massivas em seus resultados.

...as organizações devem identificar, gerenciar e controlar os dados que são cruciais para o seu funcionamento sem que os sistemas sejam sufocados por dados que não sejam relevantes.

2. Por que classificar?

Para controlar o acesso aos dados de forma consistente e eficaz, os usuários devem entender o valor desses dados e quem deve ser autorizado a compartilhar esses dados. Temos seis grandes motivos, ou direcionadores para que as organizações classifiquem dados e informações, com softwares classificadores. São eles:

2.1 Crescimento de dados não estruturados

Uma busca rápida no Google fornece uma indicação do tamanho e forma atual do problema de dados não estruturados. O Gartner prevê que os dados das empresas crescerão 800% nos próximos cinco anos, sendo que 80% serão não estruturados.

O material não estruturado abrange todas as formas de conteúdo, incluindo e-mail, documentos, imagens, vídeos e texto, dificultando a gestão com sistemas comerciais e soluções de segurança tradicionais.

Independentemente do volume, as organizações devem identificar, gerenciar e controlar os dados que são cruciais para o seu funcionamento sem que os sistemas sejam sufocados por dados que não sejam relevantes. Eles também devem garantir que as tecnologias de apoio, como arquivamento e armazenamento, continuem a ser econômicas e gerenciáveis. A classificação de dados permite que as organizações gerenciem melhor seus dados, introduzindo uma estrutura em seus dados não estruturados e focando tempo e recursos em dados críticos.

2.2 Ambientes colaborativos

O aumento nos ambientes de trabalho colaborativo pressiona as organizações para que compartilhem dados de forma mais ampla dentro e fora de seus perímetros, por exemplo, com organizações fornecedoras ou parceiros. Além disso, a adoção rápida de ferramentas de colaboração, como o Microsoft SharePoint, superou as habilidades das organizações para impor políticas consistentes para segurança de dados, governança e controle de acesso. A facilidade com que os sites do SharePoint podem ser criados significa que eles geralmente se sentem fora da visão de departamentos de TI, pessoal de segurança e até mesmo administradores dedicados do SharePoint. Isso apresenta um enorme

Quando os dados são classificados, as políticas podem ser aplicadas sobre onde as informações confidenciais são acessadas e quais dispositivos podem acessá-lo

risco de segurança para o negócio, pois aqueles que manipulam dados podem não ter conhecimento suficiente para tomar decisões informadas e as ferramentas para protegê-lo.

Ambientes colaborativos podem resultar em proteção excessiva (onde não é compartilhada informações suficientes para fazer o trabalho) ou proteção insuficiente dos dados (o que pode resultar em perda ou vazamento).

A classificação de dados significa que a avaliação do usuário sobre a importância dos dados pode viajar com ele, de modo que todos que manipulem esses dados sejam claros quanto à sua sensibilidade e requisitos de salvaguarda.

2.3 Mobile

Uma força de trabalho mais móvel e ágil quer ser capaz de acessar os dados de uma organização em seus próprios dispositivos, o que apresenta um risco grande para a organização.

A empresa não tem visibilidade para determinar o que acontece com os dados sensíveis no dispositivo. Quando os dados são classificados, as políticas podem ser aplicadas sobre onde as informações confidenciais são acessadas e quais dispositivos podem acessá-lo, e os usuários podem ser educados sobre o impacto potencial da combinação de dados pessoais e organizacionais no mesmo dispositivo.

2.4 Governança, Risco e Conformidade (GRC)

Muitas organizações têm uma forte governança ou requisito regulamentar para adicionar classificação de dados aos seus processos de negócios, a fim de reduzir o risco comercial ou financeiro. Os regulamentos variam de acordo com o setor em que a empresa opera. No Brasil, conforme já comentado neste artigo não há, ainda, obrigatoriedade das empresas em gerenciar com segurança os dados de seus clientes.

> *Uma grande novidade é a nova regra de proteção de dados implementada pela União Europeia, que poderá causar perdas milionárias às empresas, ainda que elas estejam baseadas no Brasil e não tenham presença física em solo europeu. Esta é uma nova visão e passa a causar obrigatoriedade!*

O Regulamento Geral sobre a Proteção de Dados, conhecido como GDPR por sua sigla em inglês, vai entrar em vigor em 28 de maio de 2018 e deve afetar as atividades de empresas de todo o

mundo, desde que elas coletem ou processem dados de indivíduos, empresas ou organizações presentes na Europa.

De acordo com essa regulamentação, as empresas que preenchem os requisitos definidos pela UE terão de adotar medidas como a implementação de sistemas de proteção de dados, estruturas para reportar eventuais violações de forma imediata às autoridades e até mesmo a indicação de um profissional ou parceiro comercial para **desempenhar a função de Data Protection Officer, ou DPO. Mais uma nova função de riscos em segurança de dados. OPORTUNIDADE!**

A não-conformidade com tais exigências pode render à empresa multas que podem chegar a até €20 milhões ou 4% do seu faturamento anual em todo o mundo. Vale o que for maior.

A expectativa é que as autoridades europeias vão fazer farto uso destes novos poderes. De acordo com relatório sobre o tema publicado pela corretora Marsh, apenas as empresas que compõem o índice FTSE 100 da Bolsa de Londres devem receber um total de US$ 6 bilhões em multas ligadas ao GDPR apenas no primeiro ano de vigência da nova regra.

Para se tornar um alvo em potencial dos reguladores, basta que a empresa colete dados de sujeitos europeus e que haja motivo para acreditar que ela pretende fazer uso dos dados em questão.

Já a consultoria Hyperion calculou que os bancos europeus estão expostos a levar multas de €4,7 bilhões nos três primeiros anos do GDPR, com uma média de €260 milhões por violação.

As multas podem ser tão elevadas que, mesmo que estejam cobertas por apólices de seguros contra riscos cibernéticos, é bem possível que as capacidades não sejam suficientes.

Uma pesquisa global divulgada em abril pela Veritas, outra consultoria, constatou que uma em cada cinco empresas consultadas temem que multas derivadas de violações do GDPR possam levá-las à bancarrota.

Ainda que a norma esteja mais diretamente relacionada com empresas baseadas ou com subsidiárias na União Europeia, mesmo companhias que só estão presentes no Brasil podem ter que se adaptar ao GDPR.

Para se tornar um alvo em potencial dos reguladores, basta que a empresa colete dados de sujeitos europeus e que haja motivo para acreditar que ela pretende fazer uso dos dados em questão.

Por exemplo, uma empresa baseada no Brasil pode acabar debaixo de fiscalização se tiver um website que pode ser acessa-

do na Europa e que ofereça a opção de fazer compras e pagar em euros ou libras esterlinas.

As informações concernidas pelo GDPR incluem desde dados biométricos e financeiros de indivíduos, seus endereços e dados sanitários, até informações de fornecedores e clientes, entre várias outros tidos de dados privados.

Umair Javed, um advogado associado no escritório Wiley Rein, em Washington (EUA), observa que o GDPR introduz conceitos de jurisdição mais relacionados com o local onde os dados são coletados do que com o país onde a empresa possui sua sede legal.

Isso passa a inverter o jogo das regulações no Brasil!

Sua aplicação fora da Europa, porém, dependerá de acordos legais internacionais e da habilidade dos governos europeus de conseguir convencer seus pares de outras partes do mundo de que eles têm o dever de processar os culpados.

2.5 Melhorando as Tecnologias de Segurança Complementares

Muitas organizações investiram em tecnologias de segurança das quais ainda não conseguiram obter os benefícios que esperavam.

Muitas organizações investiram em tecnologias de segurança das quais ainda não conseguiram obter os benefícios que esperavam.

Um bom exemplo é uma solução de prevenção de perda de dados (DLP). As organizações que usam soluções de DLP geralmente experimentam frustração com a sobrecarga de gerenciamento de eventos pelo usuário final, e uma necessidade constante de refinar políticas e regras.

Quando os dados são classificados pelos usuários que entendem seu contexto, através da aplicação de metadados na mensagem ou arquivo, as ferramentas DLP podem atuar sobre esta informação contextual adicional para fornecer resultados mais efetivos, com menos erros falso-positivos, melhor experiência do usuário e maior redução global do risco.

2.6 Uma abordagem de segurança em camadas

As soluções de classificação de dados superam a distância entre as soluções de segurança de TI de perímetro mais tradicionais (como proteção de firewall) e soluções de gerenciamento de informações. Cada vez mais, a classificação de dados está se tornando uma parte da melhor prática de uma abordagem de segurança em camadas, que pode incluir DLP, criptografia e gerenciamento de direitos.

3. Conclusão

Os funcionários das empresas, os denominados Primeira Linha de Defesa, passam a entender, com a classificação das informações, que eles agora têm uma responsabilidade e, em alguns casos, um requisito legal a cumprir, visando proteger os dados de seus clientes, bem como da própria propriedade intelectual. Com isso passam a ser coniventes com a segurança, assumindo uma responsabilidade proativa, que vem agregar valor para a empresa, diante do Mercado.

As organizações que usam soluções de classificação de dados, deixando bem claro, software classificador, colocam os usuários no centro de sua abordagem de segurança, o que ajuda a aumentar sua consciência do valor da informação que eles manipulam e determina como ela deve ser protegida.

O volume cada vez maior de dados, a necessidade de proteger os dados confidenciais enquanto o compartilhamento é outra exigência do mercado, para que a empresa seja ágil, flexível e rápida em suas respostas exige que a organização possua uma ferramenta para saber lidar com os níveis de criticidade dos respectivos dados e informações.

Há muitas maneiras de implementar política de segurança de TI, mas a maioria dos métodos requer algum conhecimento sobre o conteúdo que está sendo processado para ser efetivo. Este é o principal motivo das referidas políticas ficarem na gaveta.

As técnicas de classificação automatizada podem ser utilizadas para complementar uma solução de classificação orientada pelo usuário, que fornece contexto para a detecção automatizada de conteúdo, que atua como um portão com cadeado, para verificação se nenhuma outra informação confidencial foi negligenciada.

No nosso entendimento e experiência, a única maneira de classificar os dados, satisfazendo hoje o mundo volátil, incerto, complexo e ambíguo, que exige agilidade, flexibilidade e rapidez de reação é que a classificação dos dados seja conduzida pelos usuários e informado, por eles, o valor estratégico da informação.

Com isso, as empresas terão uma grande chance de aumentar sua abrangência de proteção de seus dados, simultaneamente de seus funcionários e agregando valor para seus negócios.

A Auditoria Baseada em Riscos - ABR valida o Processo de Gestão de Riscos da empresa

INTERISK é o software que possibilita o acesso à essas informações!

b&a
BRASILIANO & ASSOCIADOS
GESTÃO DE RISCOS

Informações:
www.brasiliano.com.br
11 5531 6171

Instituto dos Auditores Internos do Brasil

Rio será a capital da Auditoria Interna em 2017

Cidade maravilhosa foi escolhida para receber o Congresso Brasileiro de Auditoria Interna deste ano. O principal evento da carreira no país, deverá ter recorde em participações e debates calorosos em torno de temas como corrupção corporativa

Os holofotes da Auditoria, Governança e Ética terão o Rio de Janeiro em foco entre os dias 26 e 29 de novembro. São esperados cerca de 800 profissionais na 38a edição do Conbrai – Congresso Brasileiro de Auditoria Interna, conferência que deverá se transformar na maior já realizada na América Latina. Em 2017, o encontro apresenta o tema 'Auditoria Interna e a Expectativa dos Stakeholders'.

O crescimento contínuo do evento nos últimos cincos anos é um dos termômetros que comprova o excelente momento da carreira no país, com valorização bem acima da curva, mesmo em tempos de recessão. "As organizações privadas e públicas compreenderam que para que haja um ambiente corporativo transparente e ético é preciso criar e fortalecer áreas de auditoria. Investir nesse setor passou a ser quase compulsório", comenta Braselino Assunção, diretor geral do IIA Brasil – Instituto dos Auditores Internos do Brasil, entidade que promove o Conbrai.

Este ano serão mais de 30 painéis, que destacarão temas como: Lava Jato, Lei Anticorrupção, compliance, auditoria governamental, prevenção a fraudes e auditoria de TI. O evento promoverá também dois importantes debates envolvendo ética corporativa.

Entre as novidades da edição, serão realizados quatro workshops simultâneos e os congressistas contarão com um aplicativo para o celular, que disponibilizará todos os destaques e informações da conferência.

Nos próximos meses, o IIA Brasil divulgará a confirmação dos diversos keynotes speakers que virão em novembro, para o Conbrai.

Instituto dos Auditores Internos do Brasil

São aguardados alguns dos principais nomes da auditoria mundial, além de executivos que comandam as áreas de governança e compliance de órgãos públicos e de diversas gigantes nacionais.

Serviço

Conbrai – 38º Congresso Brasileiro de Auditoria Interna

Quando: 26 a 29 de novembro

Local: Centro de Convenções Riocentro - Av. Salvador Allende, 6555 – Barra da Tijuca, Rio de Janeiro/RJ

Inscrições e informações: eventos@iiabrasil.org.br – Tel.: (11) 5523-1919 – iiabrasil.org.br/conbrai

Sobre o IIA Brasil

O Instituto dos Auditores Internos do Brasil completou 56 anos de fundação sendo uma das cinco maiores entidades da carreira do planeta, entre os 190 países afiliados ao The Institute of Internal Auditors – IIA Global, a mais importante associação do setor no mundo. Referência na América Latina, o IIA Brasil auxilia na formação de outros Institutos como o IIA de Angola. No Brasil, a entidade coordena todo o processo de obtenção de certificações internacionais, como o CIA (Certified Internal Auditor), além de promover debates, cursos técnicos, seminários e o Conbrai – Congresso Brasileiro de Auditoria Interna.

Mais informações sobre o IIA Brasil

Tel. (11) 5523-1919 - www.iiabrasil.org.br

Amanajé Comunicação - Assessoria de Imprensa

Telefax: (11) 2674-4472 - www.amanaje.com.br - Carlos Marcondes - (11) 98160-7110 - marcondes@amanaje.com.br

Instituto dos Auditores Internos do Brasil

CGU oficializa integração com as normas do instituto global de auditoria interna

Órgão federal acaba de definir novas diretrizes de atividades de auditores internos do governo, tendo como referência as melhores práticas publicadas pelo The IIA

Órgão federal acaba de definir novas diretrizes de atividades de auditores internos do governo, tendo como referência as melhores práticas publicadas pelo The IIA

O Ministério da Transparência e Controladoria-Geral da União (CGU) acaba de anunciar a publicação do novo Referencial Técnico da Atividade de Auditoria Interna Governamental do Poder Executivo Federal, aprovado por meio da Instrução Normativa CGU nº 03/2017. O novo padrão, atualizado após 16 anos, fornece as diretrizes e os requisitos fundamentais para a prática da profissão no país no âmbito do poder público federal.

A nova norma de conduta técnica e ética foi elaborada pela CGU tendo como base as disposições do IPPF – sigla em inglês para Estrutura Internacional de Práticas Profissionais – considerado como a 'Bíblia' da profissão, instituído pelo The IIA – The Institute of Internal Auditors, a principal instituição de auditoria no mundo.

Segundo Gustavo de Queiroz Chaves, diretor deplanejamento e coordenação das ações de controle da CGU, os motivos que levaram a criação da nova norma foram as grandes alterações de contexto no ambiente corporativo em empresas públicas e privadas, decorrentes das diversas ondas de inovações tecnológicas e culturais nas últimas décadas. "O novo referencial de auditoria traz fatos novos à legislação. As respostas são significativas para o avanço da atividade de auditoria interna, ao

incluir a possibilidade de prestação de serviços de consultoria e reforçar o papel do auditor interno no aprimoramento e fortalecimento, pela Administração, dos processos de gestão de riscos, controles internos e governança", ressalta.

Entre as principais exigências da nova norma,destaca-se a necessidade de que a auditoria interna esteja alinhada ao propósito de agregar valor à gestão e melhorar a eficácia dos processos de governança, gerenciamento de riscos e de controles internos. Também reforça os valores éticos a serem seguidos pelos auditores e os requisitos de independência das unidades de auditoria interna do Poder Executivo Federal.

Para Fabio Pimpão, diretor de certificações do IIA Brasil – Instituto dos Auditores Internos do Brasil, entidade filiada ao The IIA e responsável pela promoção do IPPF no país, a escolha da CGU gerará resultados práticos extremamente positivos. "O IPPF é uma ferramenta de gestão que foi desenvolvida pelas mentes mais excepcionais do mundo da auditoria, com a ajuda de mais de 180.000 associados de quase 190 países. Ao utilizar o IPPF o departamento de auditoria garante maior independência e objetividade, agregando mais valor para o setor público", alerta.

O novo Referencial Técnico foi publicado no Diário Oficial da União no último dia 12 de junho e entra em vigor 180 dias após sua publicação. A norma abrange a Secretaria Federal de Controle Interno da CGU; as Secretarias de Controle Interno da Presidência da República, do Ministério das Relações Exteriores, do Ministério da Defesa e suas unidades setoriais; e as unidades de auditoria interna singulares, incluindo as de empresas estatais e de autarquias federais.

Sobre o IIA Brasil

O Instituto dos Auditores Internos do Brasil completou 56 anos de fundação sendo uma das cinco maiores entidades da carreira do planeta, entre os 190 países afiliados ao The Institute of Internal Auditors – IIA Global, a mais importante associação do setor no mundo. Referência na América Latina, o IIA Brasil auxilia na formação de outros Institutos como o IIA de Angola. No Brasil, a entidade coordena todo o processo de obtenção de certificações internacionais, como o CIA (Certified Internal Auditor), além de promover debates, cursos técnicos, seminários e o Conbrai – Congresso Brasileiro de Auditoria Interna.

Mais informações sobre o IIA Brasil

Tel. (11) 5523-1919 - www.iiabrasil.org.br

Amanajé Comunicação - Assessoria de Imprensa

Telefax: (11) 2674-4472 - www.amanaje.com.br - Carlos Marcondes - (11) 98160-7110 - marcondes@amanaje.com.br

Após sucesso em São Paulo, Rio de Janeiro e Curitiba, foi a vez de Belo Horizonte receber a palestra de Inteligência em Riscos!

Abordando os principais pontos da Inteligência em Riscos Corporativos (IRC), a Diretora de Relacionamento da Brasiliano INTERISK, Sandra Alves, explicou os conceitos e aplicabilidade da Interconectividade entre riscos e a importância da integração de disciplinas, com diferentes métricas e ferramentas, em um único framework.

A palestra que ocorreu dia 18 de Julho de 2017 no Ramada Encore Minascasa - BH também contou com a apresentação do novo software INTERISK, nossa solução de INTELIGÊNCIA EM RISCOS que possui ferramentas e métricas para integrar qualquer disciplina de riscos (operacional, estratégico, legal, fraudes, crédito, mercado, liquidez, projeto, segurança, entre outras) realizando a interconectividade, garantindo velocidade, usabilidade com interface simples, eficiência no processo, linguagem padrão, qualidade na gestão de riscos e priorização de recursos, sempre atendendo as melhores práticas nacionais e internacionais.

você já conhece o SOFTWARE
que facilita a Gestão de Riscos?

que **integra** todos os RISCOS de DIFERENTES
DISCIPLINAS em um único framework?

que PERMITE a gestão
completa com mais AGILIDADE?

SOFTWARE
INTERISK
Inteligência em Riscos

a SOLUÇÃO para
sua **empresa!**

Prof. Dr. Antonio Celso Ribeiro Brasiliano, CRMA, CES, DEA, DSE, MBS
Doutor em Science et Ingénierie de L'Information et de L'Intelligence Stratégique, pela Université East Paris - Marne La Vallée – Paris – França, é presidente da Brasiliano INTERISK
abrasiliano@brasiliano.com.br

O perfil do gestor de riscos para o século XXI: generalista ou especialista?

Estamos entrando em um território marcado por turbulências imprevisíveis e mudanças exponenciais para as quais as empresas e seus líderes não estão preparados. É uma era em que tudo está sendo reinventado, rediscutido e reprogramado

O mundo está se transformando na velocidade da luz, na qual os processos organizacionais, as culturas empresariais e os sistemas de tecnologia da informação do século XX, já não suportam as novas demandas deste novo século XXI. As empresas, através da liderança de seus executivos, necessitam romper estrategicamente alguns dogmas da administração, impondo um ritmo de muita rapidez, agilidade e criatividade – RAC, suficientes para identificarem e se beneficiarem das janelas de oportunidades e, ao mesmo tempo gerenciarem seus riscos com consequências negativas. Estas janelas de oportunidades, riscos com consequências positivas, com aberturas pequenas, abrem e fecham com muito mais velocidade nos dias de hoje.

O gestor de riscos entra neste contexto para lidar com o ambiente de negócios agressivo e incerto, cheio de disrupções e descontinuidades tecnológicas, e, ao mesmo tempo ajudar a empresa a se manter no rumo estabelecido. É um mundo extremamente turbulento.

A empresa moderna, dinâmica, para sobreviver a esta avalanche, tem que se reinventar constantemente, em todas as suas áreas de negócios. A área de gestão de riscos entra com uma posição estratégica porque tem que acompanhar esta velocidade e ritmo frenético, tendo há a necessidade de quebrar os dogmas existentes, as regras praticadas, sair da zona de conforto, pensar fora da caixa e principalmente ser ousado para correr riscos em apostar em novas tecnologias e conceitos.

O importante é o gestor de riscos da corporação enxergar que as incertezas estruturais surgem sempre do lado de fora das empresas. É um elemento fora de controle, uma variável externa incontrolável que se não for detectada a tempo e não houver na empresa uma grande agilidade e flexibilidade em se adaptar no novo ambiente que se forma, a empresa e seu negócio morrem. Temos como exemplo atual o declínio da Dell Computers que derrubou os grandes players do mercado de computadores ao "inventarem" o "modelo de negócio sob encomenda", que lhes permitia saber exatamente quando e quais componentes eram necessários. A agilidade da sua cadeia logística na entrega ao cliente decolou, pois, o nível de estoque passou a ser quase zero. Giro rápido, margens baixas com preços baixos, a Dell conquistou o mercado. A Gestão de Riscos da Dell não conseguiu enxergar que a Lenovo, com preços baixos e inovação constante, poderia ser uma grande ameaça. A Lenovo passou a ser líder de mercado, deixando a Dell e HP na poeira. Simultaneamente ocorreu outra grande mudança estrutural: A Apple, comandada

A empresa moderna, dinâmica, para sobreviver a esta avalanche, tem que se reinventar constantemente, em todas as suas áreas de negócios.

O gestor de riscos não deve ser nem especialista ou nem generalista. O gestor de riscos do século XXI deve ser Nexialista

pelo ousado Steve Jobs, lançou os Tablets e Smartphones. Toda a indústria de computadores foi pega de surpresa, representou o declínio do mercado de desktops e laptops. Para a Dell era o seu fim, pois suas principais competências essenciais deixaram de ser vantagem competitiva. Faltou visão de futuro para a área de riscos/estratégia da Dell na época.

Outro exemplo atual de disrupção no modelo de negócios foi o dos taxis. O modelo econômico não mudou em décadas de tarifas reguladas e um alto preço de associação às cooperativas, o que limitava a entrada de novos concorrentes. Até que a UBER passou a oferecer "caronas" pagas, através de aplicativos e os motoristas com carro próprio. A UBER surgiu em 2012 em São Francisco – Estados Unidos. Em 2014 já estava presente nas principais cidades dos Estados Unidos e do mundo inteiro. Houve tentativa, por parte dos reguladores de impedir, mas a força do mercado foi maior e hoje é uma realidade.

O que que isto significa? Significa que o gestor de riscos tem que estar com seus radares ligados, acompanhando as estratégias da empresa, neste mundo turbulento. Em 2016 ficou marcado como o ano da Quarta Revolução Industrial, a revolução das máquinas, baseada no uso de sistemas físicos cibernéticos onde fenômenos como a internet das coisas, impressão 3D, big data, inteligência artificial, só para citar algumas, deixaram de ser ficção científica e passaram a incorporar na nossa realidade.

O gestor de riscos não deve ser nem especialista ou nem generalista. O gestor de riscos do século XXI deve ser Nexialista. O que? Nexi o que? Isso mesmo temos que ser Nexialista! São pessoas que movem tudo e todos ao seu redor para atingir seus objetivos. O Nexialista é um eterno insatisfeito, eterno curioso, tem o "por quê" no cotidiano e busca sempre formas melhores e mais eficientes de fazer tudo ao redor para fazer acontecer.

O Nexialista, gestor de riscos do século XXI, deve ter habilidade para integrar diferentes matérias ou disciplinas nas empresas, tais como psicologia, química, administração, engenharia, física, entre outras, na busca da solução. Único generalista e integrador processual entre vários especialistas focados em suas respectivas disciplinas, acaba sendo responsável pela solução holística e visão de interconectividade.

O Nexialismo significa neste século XXI, uma espécie de supra - ciência que integra de maneira sinérgica, complementar e sequencial as várias disciplinas que compõem o conhecimento

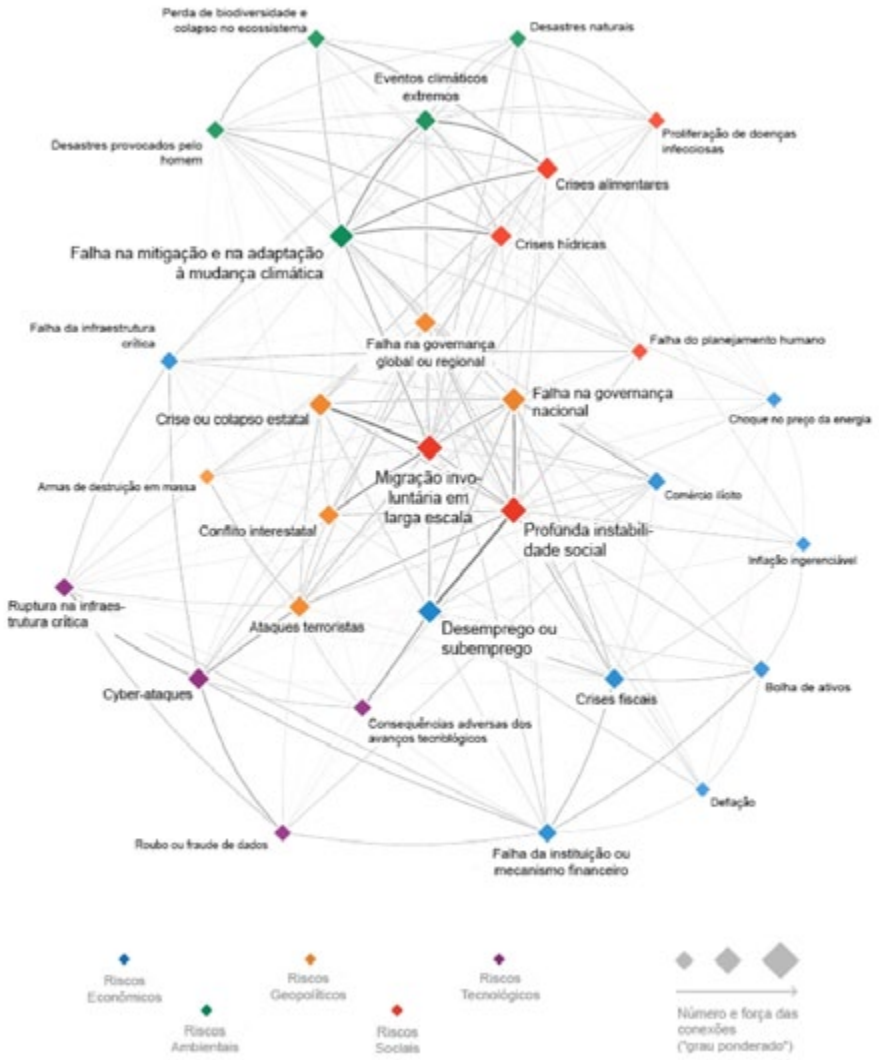


Figura 1 – Mapa de Interconexões de Riscos Globais 2017 – Função do Gestor de Riscos entender a motricidade dos riscos estratégicos da empresa - Fonte: Global Risk Report 2017 – Forum Mundial

humano, de modo que as atividades façam nexo entre si. Trabalhando com os paradoxos da consistência e do determinismo, sendo uma abordagem que aproveita os insights gerados por diferentes disciplinas e integra esses insights de maneira que produza resultados exponenciais (Figura 1).

Em um universo de especialização cada vez maior, nada mais importante de ter à visão do todo, poder enxergar a floresta além das árvores. Ser capaz de desenvolver princípios e critérios comuns para o julgamento de nossas ações.

Neste mundo cada vez mais Volátil, Incerto, Complexo e Ambíguo – Mundo VICA, é cada vez mais importante o gestor de riscos possuir, não necessariamente a resposta para todas as perguntas, mas a habilidade de saber onde olhar para buscá-las (Figura 2).

Esta é a chave deste século XXI, entendendo que nenhumas das soluções que estamos buscando para os riscos interconectados virão de uma ferramenta específica ou de um só especialista.

Faltam, em nosso mercado, ainda gestores de riscos com a visão sinérgica e isenta que permita ter ideias e buscar soluções que integrem múltiplas ferramentas e múltiplas abordagens sem peso específico ou ênfase pré-concebida a nenhuma delas. E isso porque faltam mais Nexialistas, com capacidade de integrar de maneira sinérgica, equilibrada e isenta, ousadia com pertinência (coragem com responsabilidade), criatividade com tecnologia (adequação com conhecimento), tática com estratégia (resultado imediato com posicionamento perene) (Figura 3).

Não é apenas uma questão de conhecimento ou experiência. É uma questão de ótica e de ética. Ótica de enxergar o todo e não apenas as partes, e ética de ter a coragem de recomendar a solução ideal, e não apenas aquela que interessa e melhor remunera. Nexialismo é a totalidade concebida e aplicada. Isenta e soberana. Só através dela podemos assegurar os resultados esperados.

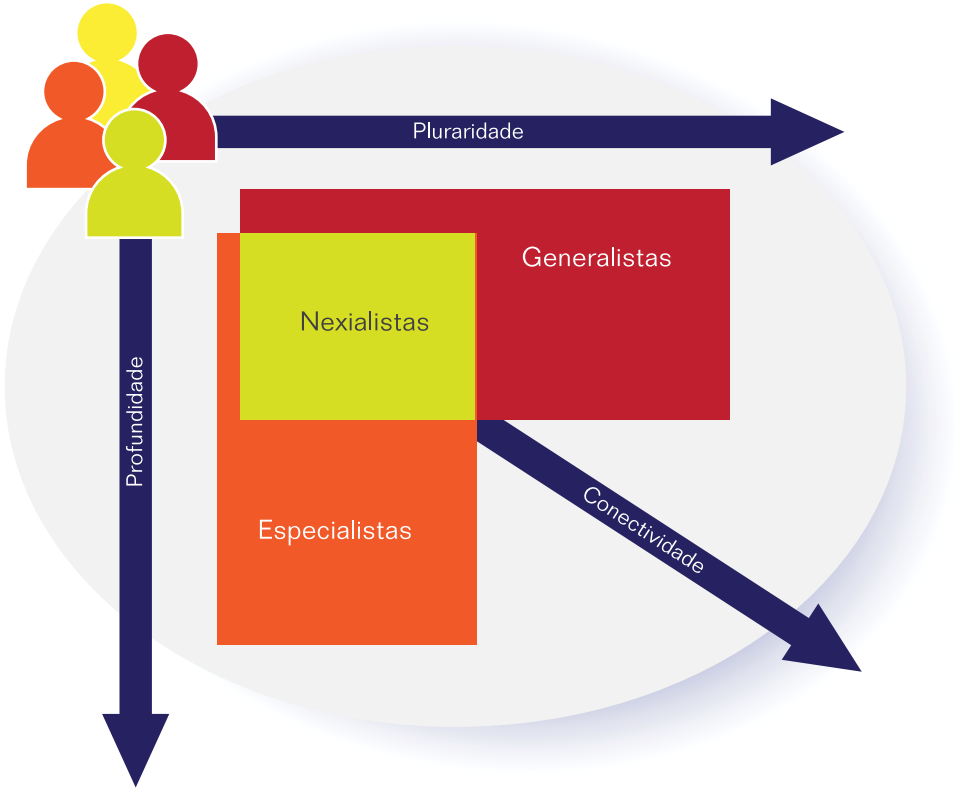


Figura 2 – Característica do Nexialista, onde a habilidade principal é a conectividade - Fonte: O marketing na Era do Nexo. Longo, Walter e Tavares, Zé Luis. Rio de Janeiro: BestSeller, 2009

	GENERALISTA	ESPECIALISTA	NEXIALISTA
CONHECIMENTO	multidisciplinar estanque	monodisciplinar profundo	multidisciplinar sinérgico
OBSERVAÇÃO	multifocal	focada	organizacional
DIAGNÓSTICO	genérico	pontual	sistêmico
RECOMENDAÇÃO	superficial	tendensiosa	isenta
SOLUÇÃO	paliativa	parcial	integrada

Figura 3 – Quadro Comparativo entre as habilidades do Generalista, Especialista e Nexialista - Fonte: O marketing na Era do Nexo. Longo, Walter e Tavares, Zé Luis. Rio de Janeiro: BestSeller, 2009

ler e saber

conheça a NOVA PUBLICAÇÃO INTERNACIONAL, disponível na BIBLIOTECA DIGITAL da BRASILIANO INTERISK

Direto de Luxemburgo, a portuguesa Maria João Ribeiro disponibiliza sua publicação sobre Impostos Diferidos, em parceria com a Brasiliano INTERISK.

clique aqui para DOWNLOAD GRATUITO

REVISTA
GESTÃO DE RISCOS
EDIÇÃO 110 | JUNHO 2017

b&a BRASILIANO&ASSOCIADOS
INTERISK Inteligência em Riscos

Críticas e sugestões de pauta:
comunicacao@brasiliano.com.br

www.brasiliano.com.br

Publisher: Antonio Celso Ribeiro Brasiliano

Edição: Enza Cirelli

Coedição: Matheus Fridori

Edição de arte: Marina Brasiliano

Edição 110 - Junho 2017 | ISSN 1678-2496N

A revista Gestão de Riscos é uma **publicação gratuita** eletrônica da Brasiliano INTERISK

Rua Barão de Jaceguai, 1768. Campo Belo - São Paulo - SP, 04606-004, BRASIL