Compliance Urgente

Fundamentos e Guia de Referências

João Roberto Peres

Não esqueça a regra básica dos negócios...

"Preço é o que você paga; valor é o que você recebe."

Warren Buffett

Aqui, todos só recebem VALOR!!!

JOÃO ROBERTO PERES

COMPLIANCE URGENTE

Fundamentos e Guia de Referências

1ª edição

São Paulo
Edição do Autor
2018

COMPLIANCE URGENTE
Fundamentos e Guia de Referências

O autor e cocriadores afirmam que mesmo havendo processo de depósito legal de COPYRIGHT ©, e proteção garantida pela constituição federal, amparada na lei 9.610 de 1998, os leitores podem utilizar os textos aqui publicados, desde que citem explicitamente os autores e a fonte.

1ª Edição - outubro de 2018

Dados Internacionais de Publicação (CIP)
Catalogação na Fonte pelo Autor
Consulta ISBN - http://www.isbn.bn.br/website/consulta/cadastro/

VERSÃO DO EDITOR
- Não Comercial -

P512c
Peres, João Roberto, 1949 – Compliance Urgente: fundamentos e Guia de Referências / João Roberto Peres – São Paulo – Ed. do Autor, 2018
Recurso Digital - Formato PDF - Requisitos do Sistema: Adobe Acrobat Reader ou similar.
Modo de Acesso: World Wide Web

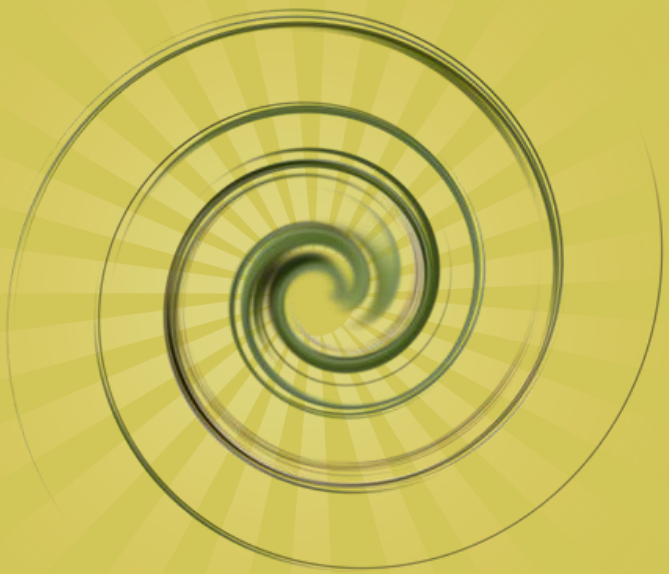
Bibliografia.
ISBN: 978-85-923158-2-5 (Recursos Digital)

1.Corrupção e Compliance no nosso DNA, 2.Corrupção e Fraudes no mundo, 3.Riscos Cibernéticos, 4.Como Reduzir Riscos, 5.Ações de Diagnóstico, 6.Implementação de sistema Compliance, 7.Programa de Integridade, 8. Melhores Práticas. 9. Bibliografia.

CDD 347.09:003
CDU 304:001.8

Autor: João Roberto Peres e cocriadores:
Daniel Péres, Manuel Deus.

"É preciso 20 anos para construir uma reputação e cinco minutos para destruí-la. Se você pensar nisso, fará as coisas de forma diferente." Warren Buffett



"Nas empresas, "Controles Internos" é a base para os "Sistemas de Compliance". As organizações quando promovem um "Programa de Integridade Empresarial" apoiado por estruturas de Compliance com alinhamento mundial, garantem uma repercussão positiva com benéfico impacto social, cujo alcance irradia no âmbito nacional e global. Com um bom Programa de Integridade fundamentado em Compliance, as empresas contribuem efetivamente para a evolução prática da ética e da moralidade humana."

João Roberto Peres

Declaração

Sobre a publicação – Série UPGRADE – COMPLIANCE URGENTE

Este é um e-book gratuito nesta fase, de uso livre e irrestrito, podendo o conteúdo ser copiado, modificado e ampliado, desde de que seja divulgada a fonte, seus autores e endereço WEB de origem, suas partes mínimas copiadas e as modificações realizadas. O autor e cocriadores possuem o direito de reivindicar judicialmente a autoria dos textos e imagens copiados sem a devida referência.

A publicação se destina a reforçar os conhecimentos prévios dos leitores interessados nos temas correlatos a Conformidade Regulatória ou COMPLIANCE, bem como, no atendimento das necessidades pessoais e empresariais, principalmente com proposta de passos para implementar um "Programa de Integridade". Não é uma publicação comercial, nem abrangente, e não esgota o assunto. Não concorremos com a grandes empresas de Consultoria na divulgação de temas. Da mesma forma, usamos linguagem coloquial não técnica ou jornalística, que não deve ser considerada como aconselhamento profissional, pois este, deve ser buscado por leitores para atender suas necessidades específicas. O autor e cocriadores não assumem responsabilidades sobre o uso das informações disponibilizadas.

As definições, afirmações e conceitos, abrangem unicamente a convicção do autor e apoio dos cocriadores, não representando a opinião integra dos apoiadores, patrocinadores e divulgadores.

Toda a produção gráfica e textual do conteúdo é artesanal e foram fundamentadas em informações universais de fontes abertas, URLs web, banco de imagens e figuras de domínio público, sendo tratadas especificamente, onde as referências autorais e direitos de terceiros, sempre foram respeitados. Da mesma forma, a validação textual de plágio por coincidência, foi legitimada e aprovada por sistema automático de alta reputação e aceitação internacional.

Estamos abertos a qualquer colaboração, seja crítica ou construtiva – faça contato: kontato@komp.com.br

Fontes de Imagens e figuras: < https://pixabay.com/pt/ > ou através do site de figuras livres < http://br.freepik.com/ > .

Validação: "Full Grammarly's Grammer and Plagiarism Checker": disponível no endereço URL < https://www.grammarly.com/plagiarism-checker >." acessos em 20/07/2018.

Publicação ofertada por NewKOMP, apoiada por: NTSC-BR, KOMP SECURITY BRAZIL, Komp Tecnologia, JDPERES, ...

Autor - João Roberto Peres

Consultor, Professor, Empresário, Palestrante, Autor-Editor.

Pesquisador, entusiasta sobre inovações nos temas ligados à Conformidade Regulatória, Gestão Empresarial, Segurança Cibernética e Tecnologias Avançadas. Atua nos últimos 35 anos como professor, palestrante, consultor e empresário. Possui formação superior em Engenharia Elétrica e Ciência da Computação, entre outras, com diversas certificações internacionais ligadas à área de Segurança Empresarial.

É multiespecialista em GRC (Governança, Riscos e Compliance), Planejamento Estratégico, Prevenção de Fraudes e Corrupção, Perícia Computacional, Gestão de Riscos, Direito Digital, Investigação e Defesa de Cibercrimes, GCN (Gestão da Continuidade de Negócios), IoT/IoE (internet das Coisas e de Tudo), DS(Data Science), Big Data & Analytics, Segurança de Redes e Datacenters,...

Também é coautor do Guia de Referências "Segurança Corporativa", da Comissão Direito Eletrônico e Crimes de Alta Tecnologia – OAB/SP (Ordem dos Advogados do Brasil – São Paulo). Possui como autor-editor ISBN diversas publicações, além de artigos e citações na WWW.

Faz parte do Grupo de Estudos "Digital" - Temático em Direito Digital e Compliance, na FIESP e OAB-SP. Nos últimos 13 anos atua com Professor Associado e Consultor de Projetos na FGV (Fundação Getulio Vargas).

Contato: jperes@komp.com.br - joao.peres@fgv.br

Prefixo Editorial - Autor-Editor ISBN nº 923158

https://www.linkedin.com/in/joão-peres-a0521017/

COMPLIANCE URGENTE

Fundamentos e Guia de Referências

Contribuíram de forma decisiva na produção desta publicação os seguintes COCRIADORES:

- **Daniel Péres** – Especialista em Controles Internos, Avaliações de Riscos, Códigos de Conduta, Investigação de fraudes, Segurança Empresarial, Segurança Cibernética, Ethical Hacker, Planejamento Estratégico, PDTI, IoT-M2M, Tecnologia da Informação e Internet.

linkedin.com/in/daniel-péres-newkomp

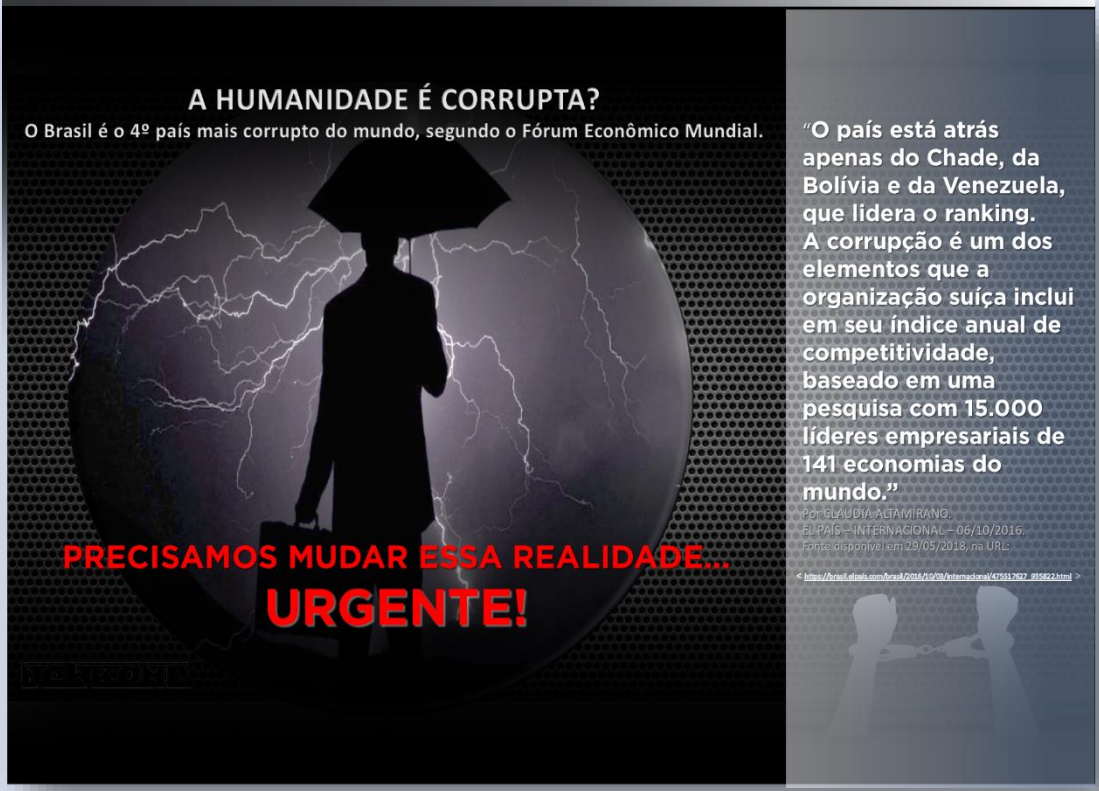
- **Manuel Deus** – Especialista em GRC (Governança, Riscos e Compliance), Planejamento Estratégico, Gestão de Projetos, Segurança Empresarial, Telecomunicações, Engenharia Eletrônica e de Telecomunicações, IoT&M2M, Automação Industrial, Canais de Denúncia, Medidas Disciplinares.

linkedin.com/in/manueldeus

Obs.: Os conteúdos apresentados nesta obra são de inteira responsabilidade do autor. Os cocriadores apoiaram, contribuíram com propostas de conteúdos e ajustes, o que não significa que todos concordem plenamente com as colocações, conclusões e observações do autor.

Este e-Book explicita o conteúdo apresentado no evento de 09 de agosto de 2018 no "Instituto de Engenharia de São Paulo" primeira palestra, sobre o tema "**COMPLIANCE – Instrumento de defesa contra a Corrupção e Fraudes nas Empresas**"

por **João Roberto Peres** – **NewKomp**



Artigo escrito por CLAUDIA ALTAMIRANO - EL PAÍS – INTERNACIONAL – 06/10/2016.
Fonte disponível em 29/05/2018, na URL:
< https://brasil.elpais.com/brasil/2016/10/03/internacional/1475517627_935822.html >

COMPLIANCE URGENTE
Fundamentos e Guia de Referências

SUMÁRIO DINÂMICO COM HIPERLINKS

TEMAS ABORDADOS NESTA PUBLICAÇÃO

- Introdução
- Programas de Compliance e Programas de Integridade
- Corrupção & Compliance integrantes do nosso DNA
- Corrupção no mundo hoje
- Mapa global de fraudes
- Riscos Cibernéticos
- Fraudes Ocupacionais
- IPCL – Índice de Percepção de Cumprimento de Leis – Brasil
- Impacto do hábito coletivo brasileiro do "furto" leve
- Como reduzir os Riscos de Corrupção e Fraudes nas Empresas
  - Diagnóstico Estratégico
  - Gestão e Governança
  - Potencialização do uso de tecnologias
  - Políticas Empresariais integradas
  - Programa de Integridade – Pequenas e Médias organizações
- Gestão de Compliance Norma "ISO 19.600:2014"
- Gestão Antisuborno Norma "ABNT NBR ISO 37.001:2017"
- Regulamento de Proteção de Dados GDPR e LGPD
- Da necessidade à ação efetiva para a Conformidade
- Certificações e Validações de Conformidade Anticorrupção
- Benefícios do Programa de Integridade
- ROI-PI Retorno de Investimentos em Programas de Integridade
- Glossário – termos usuais
- Agradecimento e Homenagem
- Bibliografia e Webgrafia
- Lançamento do e-book edição Preliminar

Conteúdo Objetivo entre as páginas 10 a 76 – 120 páginas .
Edição de avaliação do Autor - ainda sujeita a revisão ortográfica de textos.

Introdução

Combater a CORRUPÇÃO deixou de ser um ideal e se tomou uma necessidade imprescindível. Buscar e acessar informações sobre conceitos, padrões e melhores práticas confiáveis, sobre como promover a integridade ética e moral, das pessoas e das organizações, sejam elas privadas ou públicas é no momento um desafio que necessita ser enfrentado.

A internet é sem duvida uma grande biblioteca virtual que dispõe de informações de alta relevância e seriedade, assim como, apresenta também lamentáveis e inconsistentes dados, "verdadeiro lixo digital", informações incoerentes, sem fundamentos, que hoje podem ser genericamente denominadas de falsas, deturpadas ou até "Fake News".

Nesse mar de dados, que a internet disponibiliza, precisamos analisar atentamente "Que" informação buscar, "Quem" publicou o conteúdo, "Onde" a informação foi publicada (que site), "Quando" ela foi publicada (atualidade), "Por que" ela foi publicada (qual interesse), "Como" ela foi publicada (parcial, completa, com fontes de referências...), e somente quando estes questionamentos forem satisfatórios e a conclusão irrefutável, é que devemos utilizá-las.

Nesse contexto, esta publicação eletrônica, busca sintetizar em poucas páginas, não só informações objetivas e de fácil interpretação, como também indicar URLs (Uniform Resource Locator ou Links) confiáveis para que as informações fornecidas sejam validadas e complementadas.

No conteúdo deste e-book se apresenta incialmente, definições sobre Compliance, Integridade e sobre a origem da CORRUPÇÃO, de forma muito particular na visão do autor, bem como, um conjunto de "referências" impactantes sobre diversos aspectos e dados estatísticos dos riscos e casos de CORRUPÇÃO e FRAUDES, que objetivam mostrar aos leitores os principais problemas que se espera enfrentar.

Já na segunda parte, se busca direcionar os leitores em "como reduzir os Riscos de Corrupção e Fraudes nas Empresas", através da proposição de ações objetivas, de "COMPLIANCE" e "INTEGRIDADE", indicando os 20 passos para se alcançar a "integridade humana" nas organizações.

Na conclusão, se aborda a "necessidade de ações efetivas para a busca da Conformidade" e a indicação dos passos subsequentes para garantir as "Certificações e Validações da Conformidade de Processos de Compliance e Integridade", caso a empresa os tenha adotado.

Esperamos que a leitura seja agradável e aceitamos comentários e considerações sobre os temas e textos expostos.

Programas de Compliance e Programas de Integridade

Iniciamos nossa abordagem sobre "Compliance e Integridade" para que o leitor tenha uma visão objetiva da linha de pensamento empregada nesta publicação. Todas as colocações a seguir apresentadas, foram baseadas em pesquisas e estudos durante os últimos doze anos.

Acreditamos que a origem do termo "**Compliance**" seja do conhecimento de todos, pois tem sido continuamente divulgado, no entanto, vale relembrar, pois, sua origem na língua inglesa pode deixar dúvidas. O termo tem tradução direta e indiscutível para o português do Brasil, como "**Conformidade**", tendo sinônimos como "obediência", "concordância", "submissão", "capitulação", entre outros. Mas considerando a origem no verbo "(to) comply" ele nos mostra sinônimos como: "aceitar", "concordar", "assentir", "adequar-se", ou "aquiescer" (que significa agir de acordo com... ou considerar com transigência; condescender, anuir, consentir), entre outros. De forma clássica "Compliance" é definido no mercado como: "O termo Compliance origina-se do verbo inglês, "to comply" que significa cumprir, conformar-se, atender aos pré-requisitos que lhe foram impostos".

Considerando a abordagem "filosófica" do Termo Compliance, um "Programa de Compliance" convencional, compreende um conjunto de regras, controles e ações tomadas por uma organização em busca da Conformidade no cumprimento de Leis, normas e regulamentos que lhe foram impostos. Portanto, "[1]*uma organização baseada em "conformidade" é aquela que estabelece regras e condutas com penalidades por desobediência. O medo parece ser o motivador na adesão à ética baseada na conformidade. O incentivo para não ir para a prisão por menor tempo que seja, é um forte motivador para se ter adesão a um programa de conformidade. As repercussões da não conformidade mantêm os funcionários na linha*" (baseado no artigo de Bruce H. Geddes[1]).

Programas de Compliance aplicados de forma convencional, tem trazido resultados positivos para as organizações, no entanto, por serem impositivos e restritivos operacionalmente, não produzem um bom clima organizacional. O que se percebe é que as organizações fazem verdadeiros malabarismos para contornar situações impactantes com seus colaboradores ou mesmo para convencê-los à cooperar. Entendendo essa situação que perdura até hoje, em algumas organizações, vamos a seguir, refletir um pouco sobre a origem dos Programas de Compliance.

Programas de Compliance e Programas de Integridade

Programas de Compliance não são novos, possuem mais de um século, mas no Brasil veio no barco dos grandes Bancos, vinculado como "conceito idealista" aos Controles Internos, exigidos pelo "Comitê da Basiléia", para a rígida supervisão bancária. Programas de Compliance, internacionalmente, se aplicam efetivamente de forma intensiva desde a década de 1970.

O "Compliance" evoluiu e passou a ser um dos pilares dos códigos de Governança Corporativa, no mundo. Com o advento da Lei norte americana SOX, compliance ganhou força e importância por fazer intrinsicamente parte do COSO (padrão internacional de Controles Internos), evoluindo como estratégia, se tornou um conjunto de atividades imprescindíveis, ganhando status e uma posição de destaque no "organograma" dos bancos. Denominado de "Departamento de Compliance", exigindo profissionais treinados cognominados de "Compliance Officers". Nesse ponto, as atividades de compliance ganharam mais realce, amplitude e rigidez, buscando controles mais ligados à área de RH (Recursos Humanos), através de indicadores dos desvios de Conduta, postulados pelos Códigos de Ética, na época.

Compliance só ganhou notoriedade pública no Brasil após a promulgação da Lei federal n. 12.846/2013 "Anticorrupção", que passou a ter sua regulamentação através do Decreto n. 8.420, de 18 de março de 2015. Definitivamente a Lei passou a atuar como instrumento legislativo determinante, imputando as pessoas jurídicas (empresas) a responsabilização objetiva por práticas ilegais, contundentes ou lesivas a Administração Pública, independentemente da comprovação, do conhecimento ou ainda da conivência de seus diretores e colaboradores. A Lei foi impactante quanto a responsabilização objetiva dos administradores, sanções severas, pesadas multas, previsão de acordo de leniência, entre outros diversos aspectos preocupantes, causando muito medo para os infratores.

A Lei 12.846, em seu artigo 7, define que serão levados em consideração "**atenuantes**" na aplicação de "**sanções**", diversos fatores, sendo o principal explicitando em seu no inciso VIII do caput – "*a existência de mecanismos e* ***procedimentos internos de integridade****, auditoria e incentivo à denúncia de irregularidades e a aplicação efetiva de códigos de ética e de conduta no âmbito da pessoa jurídic*a;".

No caso citado, o documento da Lei 12.846 de 02 de agosto de 2013 já indicava "procedimentos de integridade" que foi interpretado pelo mercado como "Compliance". As palavras "Compliance" e ou "Conformidade" não fazem parte do texto da Lei.

Programas de Compliance e Programas de Integridade

A LEI brasileira Nº 12.846,"Anticorrupção", regulamentada através do Decreto n. 8.420/2015, que em seu capítulo IV trata especificamente "DO PROGRAMA DE INTEGRIDADE", possui o seguinte teor, que julgamos conveniente transcrever:

"Art. 41. Para fins do disposto neste Decreto, programa de integridade consiste, no âmbito de uma pessoa jurídica, no conjunto de mecanismos e procedimentos internos de integridade, auditoria e incentivo à denúncia de irregularidades e na aplicação efetiva de códigos de ética e de conduta, políticas e diretrizes com objetivo de detectar e sanar desvios, fraudes, irregularidades e atos ilícitos praticados contra a administração pública, nacional ou estrangeira.

Parágrafo Único. O programa de integridade deve ser estruturado, aplicado e atualizado de acordo com as características e riscos atuais das atividades de cada pessoa jurídica, a qual por sua vez deve garantir o constante aprimoramento e adaptação do referido programa, visando garantir sua efetividade."

Como pode ser observado, a norma legal esclarece o que o governo brasileiro considera "programa de Integridade", onde no texto integral do Decreto n. 8.420/2015, em nenhum momento, se escreve os termos "Compliance" ou "Conformidade". Para maior clareza a seguir apresentamos os principais paramentos requeridos na regulamentação do Decreto sobre a Lei "Anticorrupção" para um Programa de Integridade:

"Art. 42. Para fins do disposto no § 4o do art. 5o, o programa de integridade será avaliado, quanto a sua existência e aplicação, de acordo com os seguintes parâmetros:

I - comprometimento da alta direção da pessoa jurídica, incluídos os conselhos, evidenciado pelo apoio visível e inequívoco ao programa;

II - padrões de conduta, código de ética, políticas e procedimentos de integridade, aplicáveis a todos os empregados e administradores, independentemente de cargo ou função exercidos;

III - padrões de conduta, código de ética e políticas de integridade estendidas, quando necessário, a terceiros, tais como, fornecedores, prestadores de serviço, agentes intermediários e associados;

IV - treinamentos periódicos sobre o programa de integridade;

V - análise periódica de riscos para realizar adaptações necessárias ao programa de integridade;

VI - registros contábeis que reflitam de forma completa e precisa as transações da pessoa jurídica;

VII - controles internos que assegurem a pronta elaboração e confiabilidade de relatórios e demonstrações financeiros da pessoa jurídica;

Programas de Compliance e Programas de Integridade

VIII - procedimentos específicos para prevenir fraudes e ilícitos no âmbito de processos licitatórios, na execução de contratos administrativos ou em qualquer interação com o setor público, ainda que intermediada por terceiros, tal como pagamento de tributos, sujeição a fiscalizações, ou obtenção de autorizações, licenças, permissões e certidões;

IX - independência, estrutura e autoridade da instância interna responsável pela aplicação do programa de integridade e fiscalização de seu cumprimento;

X - canais de denúncia de irregularidades, abertos e amplamente divulgados a funcionários e terceiros, e de mecanismos destinados à proteção de denunciantes de boa-fé;

XI - medidas disciplinares em caso de violação do programa de integridade;

XII - procedimentos que assegurem a pronta interrupção de irregularidades ou infrações detectadas e a tempestiva remediação dos danos gerados;

XIII - diligências apropriadas para contratação e, conforme o caso, supervisão, de terceiros, tais como, fornecedores, prestadores de serviço, agentes intermediários e associados;

XIV - verificação, durante os processos de fusões, aquisições e reestruturações societárias, do cometimento de irregularidades ou ilícitos ou da existência de vulnerabilidades nas pessoas jurídicas envolvidas;

XV - monitoramento contínuo do programa de integridade visando seu aperfeiçoamento na prevenção, detecção e combate à ocorrência dos atos lesivos previstos no art. 5o da Lei no 12.846, de 2013; e

XVI - transparência da pessoa jurídica quanto a doações para candidatos e partidos políticos.

§ 1° Na avaliação dos parâmetros de que trata este artigo, serão considerados o porte e especificidades da pessoa jurídica, tais como:

I - a quantidade de funcionários, empregados e colaboradores;

II - a complexidade da hierarquia interna e a quantidade de departamentos, diretorias ou setores;

III - a utilização de agentes intermediários como consultores ou representantes comerciais;

IV - o setor do mercado em que atua;

V - os países em que atua, direta ou indiretamente;

VI - o grau de interação com o setor público e a importância de autorizações, licenças e permissões governamentais em suas operações;

Programas de Compliance e Programas de Integridade

VII - a quantidade e a localização das pessoas jurídicas que integram o grupo econômico; e

VIII - o fato de ser qualificada como microempresa ou empresa de pequeno porte.

Acreditamos que o artigo 42° e seus parâmetros, são demasiadamente claros e explícitos, quanto ao que se espera das organizações de todos os portes, mesmo que haja uma maior condescendência com empresas menores, porém não as excluí.

Considerando o exposto, agora se faz necessário refletir sobre os "Programas de Integridade", portanto, passaremos a explorar alguns conceitos filosóficos que compactuamos com o professor "Bruce H. Geddes", da School of Business, Western Governors University, Salt Lake City, USA, sobre o tema. – Seguem trechos com tradução e adaptação livre:

"*[1]Programas de Integridade consideram que a organização deva já ter a "missão" baseada na integridade declarada, o que implica compromissos e valores morais. Além disso, uma organização que reconhece sua missão como um modo de vida e continuamente se esforça para aderir à referida missão em todos os aspectos é indiscutivelmente uma organização que possui integridade. A ética organizacional é enquadrada por "Tomada de Decisão Baseada em Valores" (VBDM[2] Values Based Decision Making).*

Usando sua declaração de missão como sua principal orientação na tomada de decisões, o VBDM fornece uma base sobre a qual se pode construir uma plataforma (ou programa) e, se implementada com sucesso, uma organização com integridade será o resultado. Para uma organização construir integridade, há três condições que devem ser observadas; São elas: 1) estabelecer uma declaração de missão; 2) O VBDM deve ser usado para tomar todas as decisões e mudanças de políticas; 3) desenvolver um processo para navegar por decisões difíceis que a organização invariavelmente enfrentará.

A ética organizacional não pode ser determinada pela "conformidade" considerando que a "integridade" constitui a base para a compreensão da ética organizacional. Para aderir a seus valores de integridade de forma consistente e conduzir-se de forma a espelhar seu compromisso com os fundamentos, as empresas podem usar a abordagem VBDM para a ética APLICADA.

Programas de Compliance e Programas de Integridade

"[1]Outros pesquisadores concordam em estabelecer valores como base fundamental para a construção de ética baseada na integridade. Há quatro etapas na construção de um programa de integridade: 1) garantir que os líderes da empresa estejam comprometidos com os ideais; 2) identificar o que a empresa estabelecerá como seus valores centrais; 3) treinar seus funcionários; 4) delinear um plano para obter a ética gravada no próprio tecido da empresa. Empresas de sucesso são aquelas que podem colocar a maior ênfase no fato de que o comportamento ético é garantido e o comportamento antiético é desencorajado. Programas de incentivo e avaliações concluídas anualmente são duas maneiras de atingir a meta do comportamento ético continuado no alcance da integridade.

Programas de integridade podem ser usados como uma comparação com programas de conformidade. As organizações que têm programas de integridade estabeleceram princípios fundamentais que pedem a todos que sigam os princípios e se governem de acordo. Nesse caso, os funcionários entendem a importância dos princípios para a missão e o sucesso contínuo da organização. Este entendimento vem de uma abordagem de gerenciamento de cima para baixo de instalar uma declaração de missão clara e precisa que os funcionários vão comprar sempre.

Os programas de integridade produzem colaboradores que são mais propensos a se comprometer com suas organizações, mais conscientes em um sentido ético e mais dispostos a relatar problemas de natureza ética. Os programas de integridade permitem que as empresas monitorem: má conduta do funcionário, níveis de conforto do funcionário com relatos de má conduta se os funcionários acreditarem que estão sendo tratados de forma justa e se os funcionários se sentirem pressionados a negligenciar determinados assuntos. A partir dos resultados desse sistema de monitoramento, as organizações podem identificar contramedidas relacionadas à integridade baseadas na ética que produzirão resultados positivos.

Outra faceta dos programas de integridade são os princípios de incentivo entrelaçados na fundação. Recompensar o comportamento ético por reconhecimento e prêmios financeiros envia uma mensagem de que o comportamento ético é o modo de vida de uma organização. Em uma pesquisa conduzida por "Weber e Wasieleski", incentivos financeiros para programas éticos para proteger a empresa de funcionários de natureza antiética classificaram 4.1 de 7 em uma escala de Likert para importância. Isso quer dizer que, embora o dinheiro não seja a força motriz por trás dos programas de integridade, é um incentivo muito procurado."

Programas de Compliance e Programas de Integridade

"[1]*Programas de integridade não são isentos de seus detratores. Hartman argumenta que um sistema baseado na integridade pode ser neutro e permitir muito debate sem fornecer uma direção clara para os funcionários. Outro caso em questão é que os programas baseados em integridade exigem treinamento, em vez de apenas aplicar um conjunto específico de regras a uma situação como no programa de conformidade. É verdade que os funcionários têm dificuldade em fazer escolhas éticas se não conseguirem identificar prontamente a escolha ética. Consequentemente, é mais difícil para os colaboradores pensar e considerar cenários concorrentes, em vez de apenas aplicar as regras à situação."*

Como se pode observar as diferenças entre Programas de "Compliance ou Conformidade" e Programas de Integridade, descrito por "Geddes", está principalmente na forma de compreensão estratégica dos dirigentes empresariais, sendo que alguns optam por truculência e maior rigidez nos controles e outros aspiram ideais mais democráticos e flexíveis, na aplicação dos requerimentos de Normas, Códigos Éticos, de Conduta e legais.

O melhor dos dois mundos – sistema adotado no Brasil

Geddes ainda complementa, concluindo: ***"[1]****Hoje, uma empresa que deseja ser bem-sucedida por qualquer período de tempo deve ter uma vantagem competitiva. A vantagem competitiva de uma organização está em seus recursos estratégicos. Uma organização que pode "integrar e implementar programas de ética baseada em conformidade e integridade" terá uma vantagem estratégica sobre outros negócios no mesmo setor.* ***"A conformidade exige integridade e integridade precisa de conformidade".***

Uma integração da filosofia de conformidade (compliance) e de integridade traz uma infinidade de recompensas. Sem dúvida, o lucro é uma daquelas recompensas aprimoradas recebidas quando um negócio segue algum padrão ético. Milton Friedman disse que a única responsabilidade dos negócios é aumentar os lucros, desde que operem dentro das regras. As regras da economia global atual são que as organizações devem adotar padrões éticos que as tornem cidadãos responsáveis. Existe um argumento esmagador para incluir a tomada de decisão ética nas empresas como uma responsabilidade. Esta ideia começa no topo, com os líderes das organizações.

Os líderes de negócios devem encontrar uma maneira de instilar a ética em sua organização e, ao mesmo tempo, manter o objetivo de aumentar os lucros continuamente. Os líderes de negócios podem estabelecer uma linha de base para a ética em uma organização que ajuda o líder a identificar áreas que podem gerar resultados éticos da natureza positiva. Os líderes podem ter o maior impacto na cultura organizacional por causa de suas posições e isso, por sua vez, tem o impacto mais significativo sobre a ética corporativa."

Programas de Compliance e Programas de Integridade

"[1]*Para que a cultura ética seja eficaz e se espalhe por toda a organização, o compromisso com a ética não deve permanecer exclusivamente nas mãos do líder no topo. Esta responsabilidade deve fluir para todos os executivos e membros da administração para mostrar um alinhamento da mensagem de boa ética, eliminando assim a ambiguidade.*

Um líder eficaz encontra uma maneira de fazer com que seus subordinados desejem fazer as coisas necessárias para alcançar a meta estabelecida pelo líder. Se o objetivo é ter uma organização que tenha uma base na boa ética para alcançar a Integridade, então o líder deve encontrar uma maneira de fazer com que aqueles que seguem, queiram atingir esse objetivo. Quanto mais o líder lidera pelo exemplo de trazer valores éticos internos como uma força orientadora, mais confiança ele irá gerar de seus seguidores. Essa ideia não se transformará em uma confiança cega, mas quanto mais o líder fizer sacrifícios pessoais em prol de seus valores, mais os funcionários estarão dispostos a fazer o mesmo.

Apenas escrever um código ético não é suficiente; a Integridade deve estar entrincheirada na própria fibra da organização e comunicada pelo líder continuamente. Os líderes são a principal força por trás da conduta ética de uma organização e são responsáveis por orientar seus colaboradores na direção certa.

Ética e rentabilidade não são mutuamente exclusivas e isso é importante para todos em todas as esferas da vida em suas vidas pessoais e profissionais. No entanto, os dois não estão competindo entre si e que em muitas ocasiões a escolha lucrativa é de fato a escolha ética. A ética que conduz a Integridade é uma ferramenta de gerenciamento usada para aumentar a produtividade e, consequentemente, os lucros nos negócios. A adesão estrita aos padrões éticos aumenta os lucros, assim como a expansão dos negócios."

Na visão do autor deste e-book e seus cocriadores, as indicações claras do Decreto n. 8.420/2015, sobre a necessidade de Integridade nas organizações, mostram que o "Programa de Integridade" deve iniciar com as "práticas de Compliance" como sistema rígido de controle sobre os requerimentos, e este ser devidamente conexo no amago do padrão indicado para Programas de Integridade. Dessa forma o legislador brasileiro, se manteve atualizado com as tendências mundiais, de forma que os sistemas de Compliance flexíveis e evolutivos sejam parte indissociável dos Programas de Integridade.

Programas de Compliance e Programas de Integridade

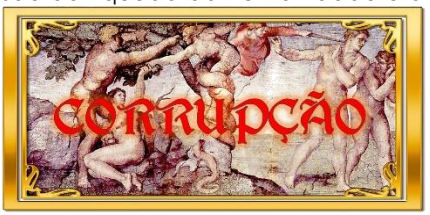
O **IBGC –** Instituto Brasileiro de Governança Corporativa, lançou um livro "Governança corporativa e integridade empresarial: dilemas e desafios", indicando como título de um dos capítulos -"**Um Programa de Integridade não é um Programa de Conformidade**" – e sobre o conteúdo esclarece: "*O capítulo convida conselheiros a refletirem sobre a importância da criação de um programa de integridade corporativa, cujo propósito seja a criação de ambientes de tomada de decisão que realmente favoreçam a prática da integridade pessoal. Para tanto, é necessário que o programa de integridade corporativa se desvincule dos modelos dos programas de compliance/conformidade atuais. O capítulo também aborda as relações entre integridade pessoal e programa de integridade corporativa, e evidencia as diferenças entre programas de integridade corporativa e programas de monitoramento (auditoria, controles, gerenciamento de riscos, compliance etc.)*". Informação disponível na URL - < http://www.ibgc.org.br/userfiles/files/Publica%C3%A7%C3%B5es/IBGC_livreto.pdf > texto explicitado na página 7 do pdf. Acesso 10/07/2018

Fundamentação sobre o exposto:

- [1] – **Trechos traduzidos e adaptados de:** "Geddes, B. (2017) Integrity or Compliance Based Ethics: Which Is Better for Today's Business?. Open Journal of Business and Management, 5, 420-429. doi: 10.4236/ojbm.2017.53036. - http://file.scirp.org/Html/2-1530470_77411.htm" - Work is licensed under the Creative Commons Attribution International License (CC BY 4.0).
- [2] – (VBDM - Values Based Decision Making) - OS CINCO TIPOS DE TOMADA DE DECISÃO – disponível na URL abaixo – acesso 10/07/2018. https://www.evolucaohumana.com.br/2011/11/16/os-cinco-tipos-de-tomada-de-decisao-como-e-que-voce-decide-na-vida-pessoal-ou-na-organizacao/
- Tullberg, J. (2012) Integrity-Clarifying and Upgrading an Important Concept for Business Ethics. Business & Society Review, 117, 89-121.https://doi.org/10.1111/j.1467-8594.2011.00401.x
- Ana, S.I. (2005) Values Based Decision Making: Organizational Mission and Integrity. HEC Forum, 17, 6-17. https://doi.org/10.1007/s10730-005-4947-3
- Hartman, L. (2000) Compliance versus Integrity: The Process of Ethics Integration. Journal of Employment Discrimination Law, 2, 157-159.
- Roberts, R. (2009) The Rise of Compliance-Based Ethics Management. Public Integrity, 11, 261-277.
- Eliason, M.J. (1999) Compliance plus Integrity. The Internal Auditor, 56, 30-33.
- Maesschalck, J. (2004) Approaches to Ethics Management in the Public Sector. Public Integrity, 7, 21-41.
- Arjoon, S. (2006) Striking a Balance between Rules and Principles-Based Approaches for Effective Governance: A Risks-Based Approach. Journal of Business Ethics, 68, 53-82.
- Thielemann, U. (2005) Compliance und Integrity-Zwei Seiten Ethisch Integrierter Unternehmenssteuerung. Zeitschrift Fuer Wirtschafts-Und Unternehmensethik, 6, 31-45 [Citation Time(s):1]

Corrupção & Compliance integrantes do nosso DNA

A história da humanidade contada através da Bíblia Sagrada, cita no livro de "Gênesis" que Deus criou Adão e Eva como base para a formação da raça humana. Eva foi corrompida pela serpente (primeira corruptoras da História) quando pecou por aceitar o fruto proibido. Da mesma forma, Eva corrompeu Adão, que aceitou comer do fruto proibido, esperando obter a "vantagem" de adquirir o conhecimento do bem e do mal. Dessa doutrina cristã nasceu o "Pecado Original", com a visão da "queda da humanidade e a expulsão do Paraiso".



(Parte do Afresco da "Queda da humanidade e a expulsão do paraíso". Por Michelangelo no teto da Capela Sistina - Vaticano.)

O "Pecado Original" indica que Deus imputou a Adão e a todos os seus descentes ao longo dos séculos, o pecado de "Corrupção Moral". Esse pecado de "Corrupção", logo, passou a fazer parte do DNA humano desde então, sendo hoje facilmente percebido, mas pouco aceito por todos, pois corrupto é sempre o outro, nunca nós mesmos.

Para superar essa parte "errada" do DNA a "Corrupção", a humanidade ao longo dos milênios da civilização, vem buscando meios para intensificar a percepção dos homens, da necessidade de corrigir os seus desvios éticos e morais, e para tanto, no século XX (vinte) consolidam-se os primeiros conceitos de "Compliance" moderno, que endereçam o "Estar e Ser Compliance", portanto, fazer tudo "Certo", em conformidade com os princípios sociais e legais, aceitos por todos.

(Desafios – Corrupção X Compliance – Certo e Errado fazem parte do DNA da humanidade)
(Corrupção = Compliance – opostos filosóficos)

É fundamental entender que "Corrupção" e "Compliance" são lado opostos que se complementam (Yin Yang: o princípio da Dualidade), deste modo, cremos que todos possuímos no DNA esses cromossomos.

Precisamos ***URGENTE*** potencializar a COMPLIANCE - pessoal, social, empresarial, governamental...

"É muito mais fácil corromper do que persuadir."

Sócrates

Corrupção no mundo hoje

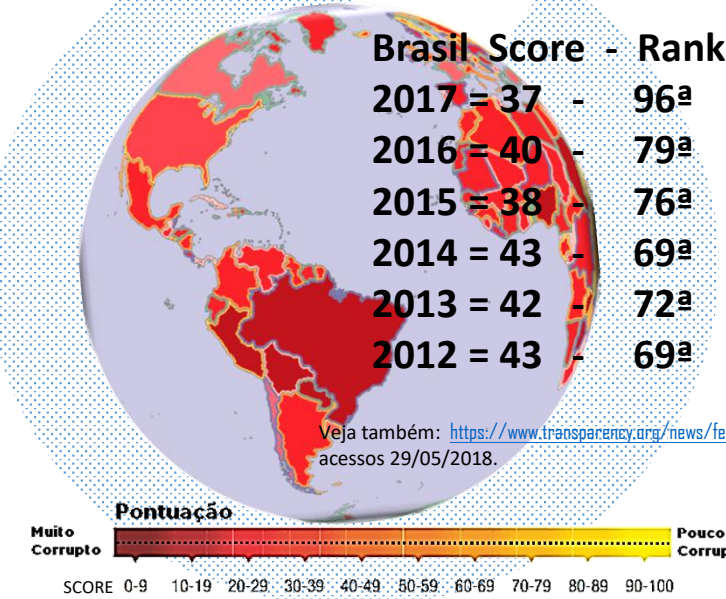
A Corrupção sempre foi endêmica no mundo e continua assim hoje. Não há país onde não haja a percepção de corrupção, mesmo que pequena.

Muitas organizações no mundo buscam compreender e promover a quantificação da corrupção com base na percepção de ações e instrumentos (Leis, Regulamentos, Normas, Padrões, estatísticas, etc.) desenvolvidos e aplicados especificamente. Nos últimos 20 anos a organização que mais se destacou e ganhou credibilidade na análise da corrupção foi a ONG "Transparency International - TI", que desde 1995 divulga anualmente um balanço da pesquisa de percepção de corrupção nos países, trabalho denominado "Corruption Perceptions Index – CPI".

O Brasil faz parte do estudo da "CPI" e tem se colocado com variabilidade preocupante nos últimos 3 (três) anos, onde em 2017 a percepção de corrupção cresceu e perdemos 17 posições no ranking dos países, considerando nossa posição em 2016, mesmo com o ingresso de só 4 (quatro) novos países na pesquisa. Isso significa que precisamos URGENTE melhorar nossos instrumentos de combate a corrupção, para que a COMPLIANCE da nação seja melhor avaliada.

Recomendamos impreterivelmente o acesso ao site web da ONG "Transparency International", para a leitura atenta dos diversos relatórios ofertados, em especial a página do "Global Corruption Barometer".

Dados da "TI", disponível em < https://www.transparency.org/ >



Veja também: https://www.transparency.org/news/feature/corruption_perceptions_index_2017 acessos 29/05/2018.

Mapa global de fraudes

Acreditamos que haja uma nítida percepção coletiva de que a "corrupção" ética e ou moral, sejam elementos de base para o impulso de diversos desvios de conduta, levando indivíduos a praticar diversos crimes, como os de Fraude.

O estudo dos diversos riscos ligados ao acometimento de fraudes, nos leva a buscar entender o "fenótipo*" dos homens que as realizam, pois só assim compreenderemos as motivações. Da mesma forma, as fraudes podem ser classificadas em vários tipos, no entanto, no estudo anual da Kroll "Global Fraud & Risk Report" de 2017/2018, ela integra incidentes de Fraudes, incidentes Cibernéticos e de Segurança, informados por respondentes de cada país, que os vivenciaram nos últimos 12 meses, em suas empresas.

A Kroll aponta que no Brasil as Fraudes foram indicadas por **84%** dos respondentes, enquanto os incidentes Cibernéticos por **89%** e de Segurança por **63%**. É fundamental entender que esses três tipos de Risco, podem e devem ser atribuídos aos desvios de conduta humana, portanto, fruto da corrupção.

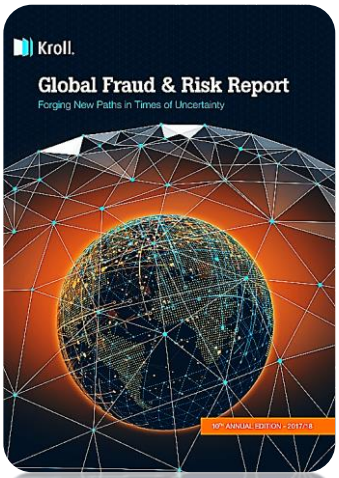
É importante baixar o relatório da Kroll Inc. (uma das maiores do mundo no ramo da investigação corporativa) e examinar em detalhes como ela entende a questão da Fraude e outros riscos correlatos no mundo.

É fato que as Fraudes e seus derivados, como os incidentes de Segurança e Cibernéticos, necessitam ***URGENTE*** tratamento, para serem reduzidos. Precisamos agir!

Mapa Global de Fraudes

Recomendamos a leitura atenta do relatório - Global Fraud & Risk Report – Kroll – 10 TH ANNUAL EDITION 2017/18.

Disponível em < https://www.kroll.com/en-us/global-fraud-and-risk-report-2018 >



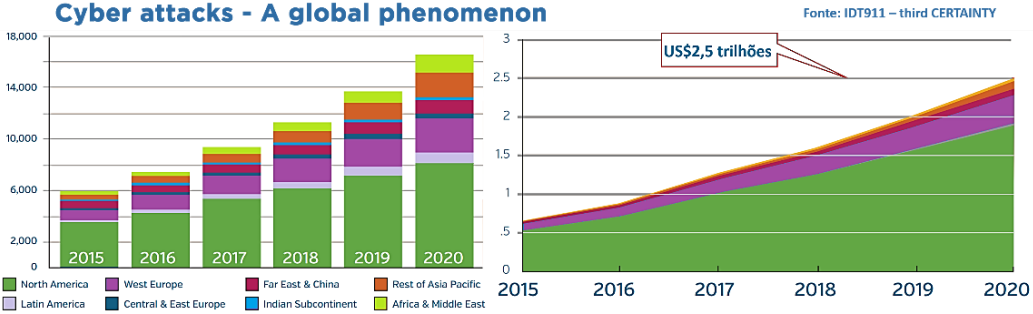
*"fenótipo"- Tema tratado no e-Book "COMPLIANCE - Corrupção e Fraudes no Mundo Empresarial", do mesmo autor, que pode ser baixado gratuitamente em:
< http://www.ntsc-br.com/data/documents/CCFME-vl-eBook2a.pdf > acessos 30/05/2018.

Riscos Cibernéticos

Segundo uma das maiores empresas de segurança do mundo, a McAfee, em seu relatório "Economic Impact of Cybercrime[1]" de fevereiro de 2018 desenvolvido em parceria como o "Centro de Estudos Estratégicos e Internacionais (CSIS)", o Brasil é o alvo número um dos ataques cibernéticos na América Latina e a principal fonte de ataques online, e que em todo o mundo, é a segunda nação de onde partem a principal fonte de ataques, (*o Brasil tem uma grande comunidade de "Hackers black-hat" altamente ativos*) sendo também o terceiro alvo mais afetado atualmente. Os impactos econômicos dos crimes pela Internet chegam próximo de US $ 600 bilhões perdidos a cada ano, ou seja, quase um por cento do PIB global.

Dados mais alarmantes são preconizados no estudos da Juniper Research, "The Future o Cybercrime and Security[2]" atualizado em 2017, que indica o custo das violações de dados por cyber ataques de US $ 1,1 trilhões globalmente em 2019, chegando a US $ 2,5 trilhões em 2022. (*veja gráfico abaixo e acesse o infográfico da projeção original[3] 2015*)

Outras fontes indicam que boa parte dos ataques Hacker que alcançam os alvo, são cometidos com a ajuda de colaboradores (empregados) das organizações afetadas. Temos de reforçar ***URGENTE*** a COMPLIANCE DIGITAL pessoal ou individual. (baseado em: *Temenos - NetGuardians*).



URGENTE – estamos em época de Cyber Ataques "Fake News". Cuidado!

1< https://www.mcafee.com/enterprise/en-us/assets/reports/restricted/economic-impact-cybercrime.pdf >

2< https://www-cdn.webroot.com/5415/0396/2242/The-Future-of-Cybercrime-and-Security-Juniper.pdf >

3 < http://thirdcertainty.com/wp-content/uploads/2015/05/Cybercrime.pdf > acessos 29/05/2018.

Riscos Cibernéticos

Inevitavelmente, todas as pessoas e organizações já utilizam em larga escala dispositivos diversos conectados em redes (WiFi, LAN, 3G/4G,...), desde impressoras, notebooks, smartphones, televisores, rastreadores de veículos, maquininhas de pagamentos (POS - Point of Sale), câmeras de vídeo IP, etc. que podem ser considerados como dispositivo da classe "Internet das Coisas – IoT". Todos são dispositivos "IoT" vulneráveis, com nível de proteção contra ataques "hacker" muito baixo.

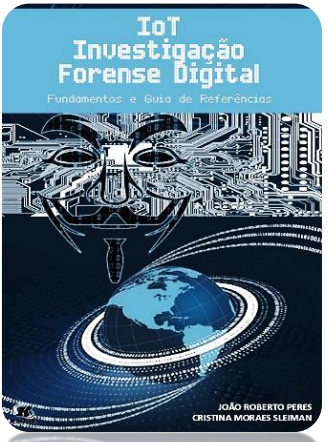
Hoje vivenciamos eventos marcantes no uso integrado das tecnologias, onde a "Internet das Coisas" IoT, deve alcançar próximo de 100 bilhões de dispositivos conectados na Internet internacional até 2025. Esse fato é extremamente preocupante, pois, os hackers já vêm causando estragos com prejuízos milionário ao se infiltrarem em dispositivos IoT e propagarem ataques de paralização de serviços "DDoS" (Distributed Denial of Service) de grande abrangência mundial.

Em pesquisas recentes sobre segurança em redes, as perdas por ataques de negação de serviços DoS/DDoS utilizando dispositivos vulneráveis IoT, custam em média US $ 127.000 cada, no entanto, o maior impacto está ligado aos casos do uso de dispositivos "IoT" por "Insiders" (dentro de casa – por empregados) descuidados ou maliciosos, de forma acidental ou proposital, chegando ao prejuízo médio de US $ 145.000.

A paralização de serviços, o furto de dados (pessoais e empresariais), e outros ataques através de dispositivos conectados em redes/nuvens, tendem a crescer exponencialmente, e sem duvida já representam um grande desafio a ser enfrentado de forma ***URGENTE***, na busca do COMPLIANCE de Segurança para todo tipo e porte de empresa.

Riscos Cibernéticos

Recomendamos a leitura das seguintes publicações e artigos:



e-Books gratuitos com participação do mesmo autor – disponíveis em:
< http://www.uberconsult.com.br/artigos-e-conteudos/e-books-disponibilizados/ >

Artigos: Valor Econômico - < http://www.valor.com.br/patrocinado/embratel/tendencias-ti-e-telecom/hackers-aproveitam-novas-tecnologias-para-intensificar-ataques-ddos >
JOTA < https://www.jota.info/opiniao-e-analise/artigos/seguranca-da-informacao-e-iot-no-brasil-prioridades-modelos-e-alternativas-06032018 >

IBM < https://www.ibm.com/developerworks/br/library/iot-anatomy-iot-malware-attack/index.html >
COMPUTERWORD < http://computerworld.com.br/rede-mirai-ataques-virtuais-dispositivos-de-iot-se-tornam-mais-comuns > acessos 04/06/2018.

Diversas fontes de pesquisa com elevada reputação, apresentam ao mundo suas análises que indicam que os crimes cometidos através das redes empresariais, principalmente através da Internet (Cyber Crimes), possuem altíssima probabilidade de ocorrer a qualquer instante, em qualquer dispositivo ou computador. Isso de forma simples significa que os computadores de sua empresa podem ser "vítima" ou produzir ataques cibernéticos.

O fato é que empregados, de muitas organizações que não possuem processos ativos de COMPLIANCE de segurança, utilizam as "redes" de suas empresas para produzir ataques a pessoas e a outras empresas, cometendo crimes através delas.

No caso, os gestores responsáveis das organizações através das quais os ataques são produzidos, por estarem não conformes em segurança, sempre serão responsabilizados e penalizados.

Riscos Cibernéticos

Uma da fontes respeitáveis de informação sobre a probabilidade de riscos e impactos globais é a organização do "World Economic Forum", com sede em Genebra, Suíça – que produz um relatório de análise denominado "The Global Risk Landscape".

O relatório "The Global Risk Landscape 2018 - 13th Edition", publicado em janeiro deste ano, aponta "Ataques Cibernéticos e Fraudes de dados ou Roubo" com alta probabilidade de ocorrência estando alinhados em terceiro e quarto lugar, com impacto médio, onde as tecnologias possuem relevância significativa. Vale conferir, com leitura atenta.

O relatório The Global Risks... Pode ser baixado – Disponível em < http://www3.weforum.org/docs/WEF_GRR18_Report.pdf > acesso 30/05/2018.

Leitura Recomendada: Artigo LEC disponível em:< http://www.lecnews.com.br/blog/revista-lec-especialistas-apontam-como-empresas-devem-se-proteger-contra-ataques-ciberneticos/>
Artigo: Global Risks in 2018: What Lies Ahead? (O que está a frente?)
<https://www.internationalinsurance.org/sites/default/files/2018-03/Global%20Risks%20Watch%202018.pdf>
acessos 30/05/2018.

CityRisk Index – Maiores Riscos Urbanos

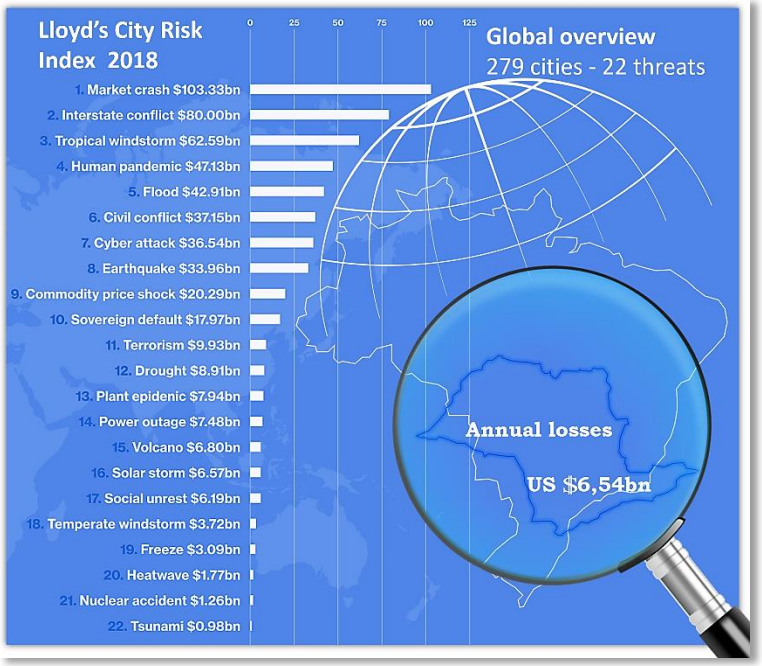
Hoje diferentes centros de estudos pesquisam os múltiplos riscos mundiais e seus possíveis impactos econômicos, de infraestrutura e sociais, caso ocorram. Aqui, citamos as informações divulgadas pelo Centro de Estudos de Risco da "Universidade de Cambridge" que desenvolveu o "ÍNDICE DE RISCO URBANO LLOYD'S" previsto para o período de 2015-2025.

A análise de riscos urbanos LLOYD'S 2018 verificou a exposição econômica de 279 das maiores cidades do mundo, face a 22 ameaças específicas, incluindo catástrofes naturais e eventos provocados pelos homens.

A cidade de São Paulo se coloca em segundo lugar entre as cidades latino-americanas mais ameaçadas, perdendo só para a cidade do México que possui alto risco de terremotos.

O impacto financeiro anual previsto para a cidade de São Paulo, chega a US $6,54 Bilhões em média.

É importante observar que a pesquisa aponta "Cyber Attacks" entre os 10 maiores riscos, com impacto de US $36.54 Bilhões.



Informações: disponíveis em: <https://cityriskindex.lloyds.com/wp-content/uploads/2018/06/Lloyds_CRI2018_executive%20summary.pdf
Site dinâmico: <https://cityriskindex.lloyds.com/>
Noticias em < https://www.revistaapolice.com.br/2018/06/sao-paulo-perder-ameacas-geradas-homem/ > acessos 08/06/2018

Se faz ***URGENTE*** considerar as ameaças e buscar alternativas de Controle, Transferência de Riscos, Contingência e Continuidade Operacional, para que nossas organizações fiquem em COMPLIANCE.

Fraudes Ocupacionais

Um dos maiores desafios nas organizações é compreender a causa raiz de determinadas situações, pois os gestores não percebem que a maioria dos colaboradores não estão em COMPLIANCE, preocupados com a empresa, mas sim como são vistos, suas avaliações, a remuneração, o reajuste salarial, etc. Isso ocorre, pois pouco investimento normalmente é feito para a valorização da marca, da conformidade regulatória e do "patriotismo empresarial" que fomente o orgulho de pertencer à organização.

No contexto mundial, a "Association of Certified Fraud Examiners (ACFE)" vêm há muitos anos desenvolvendo estudos e pesquisas, sobre as Fraudes cometidas nas organizações, por colaboradores empregados ou com a ajuda destes. Anualmente a entidade ACFE produz um relatório consolidado, denominado "REPORT TO THE NATIONS - GLOBAL STUDY ON OCCUPATIONAL FRAUD AND ABUSE", que objetiva: 1) Identificar os principais casos de fraudes ocupacionais em áreas críticas; 2) Identificar os métodos pelos quais os profissionais cometem fraudes; 3) Entender como as fraudes cometidas são descobertas; 4) Identificar quais as características das organizações que são vítimas de fraude ocupacionais; 5) Entender quais as características das pessoas que cometem fraudes ocupacionais; 6) Verificar quais as consequências e resultados dos casos após as fraudes serem detectadas e os autores identificados.

Os dados do relatório anual da ACFE de 2018, sobre pesquisas em 125 países são impactantes, e advertem que 82% das "Fraudes" identificadas, são cometidas por empregados do sexo masculino, sendo que 70% dos casos de corrupção são atribuídos as pessoas com poder de decisão nas empresas, sendo 38% por Gestores e 32% por executivos de maior nível, até por sócios.

Aponta ainda, que a perda financeira nos 2690 casos de Fraudes avaliados ultrapassam US $ 7 bilhões, com um prejuízo médio de US $ 130.000 mil por evento.

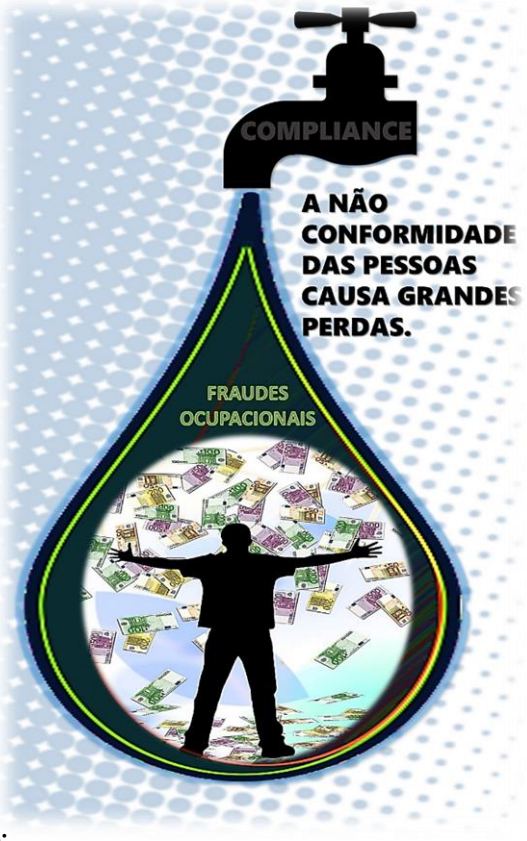
Precisamos ***URGENTE***, ficar atentos em nossas organizações.

COMPLIANCE *URGENTE*!!!

Leitura Recomendada: – Livro aberto.pt-pdf: < https://obegef.pt/wordpress/wp-content/uploads/2010/12/e001.pdf >
Livro "FORENSIC ACCOUNTING" - OBEGEF – em português. Página resumo ACFE "REPORT TO THE NATIONS – 2018" < ttp://www.acfe.com/report-to-the-nations/2018/ > acesos 30/05/2018.

Fraudes Ocupacionais

Ainda no que tange aos prejuízos financeiros, o relatório da ACFE indica que a perda média produzida por fraude, cometidas por executivos ou sócios, chegam a US $ 850.000 mil cada. As fraudes nas pequenas e médias empresas, são muito significativas; empresas com mais de 100 empregados a média de perdas é de US $ 104.000 mil, enquanto nas organizações com menos de 100 empregados ela alcança US $ 200.000 mil.



No referido estudo a ACFE caracteriza e informa as perdas financeiras por setor empresarial (segmentos da indústria), e indica que os "Esquemas de FRAUDE" levam de 12 até 30 meses para serem descobertos, dependendo do tipo de fraude realizada.

O conteúdo do relatório "REPORT TO THE NATIONS 2018 - GLOBAL STUDY ON OCCUPATIONAL FRAUD AND ABUSE" é muito abrangente e merece ser lido atentamente, e devidamente compreendido, podendo ser baixado sem ônus, a partir do endereço URL: <https://s3-us-west-2.amazonaws.com/acfepublic/2018-report-to-the-nations.pdf > acesso 30/05/2018.

Outras leituras recomendadas com ênfase:

►Livroaberto.pt-pdf, baixar URGENTE em: <https://www.gestaodefraude.eu/wordpress/wp-content/uploads/2014/10/e007.pdf > Título -"As Facetas da Fraude" Crónicas – Organização: Nuno Gonçalves e Carlos Pimenta – OBEGEF - Observatório de Economia e Gestão de Fraude (Portugal).

►Artigo Técnico disponível em <https://periodicos.ufsc.br/index.php/contabilidade/article/view/2175-8069.2017v14n32p108/34989 > Título - "Triângulo de fraudes de Cressey (1953) e teoria da agência: estudo aplicado a instituições bancárias brasileiras" - autores: Michele Rílany Rodrigues Machado e Ivan Ricardo Gartner. O artigo pode ser lido ou baixado em PDF.

►Recomendamos a aquisição e leitura do Livro "Manual das Fraudes" (2a. edição) do nosso famoso amigo Consultor "Lorenzo Parodi" <http://www.brasport.com.br/informatica-e-tecnologia/seguranca/manual-das-fraudes-2a-edicao/> veja também < http://www.fraudes.org/showpage1.asp?pg=10 > acessos 08/06/2018.

IPCL – Índice de Percepção do Cumprimento de Leis – Brasil

(compliance with the law)

A Escola de Direito da Fundação Getulio Vargas de São Paulo, desenvolveu uma pesquisa para a criação do Índice "IPCL", durante seis semestres (3 anos), medindo a partir de rígidos critérios, a percepção do comportamento social dos cidadãos brasileiros, quanto ao "respeito" as Leis e as autoridades, com uma amostragem muito significativa, nos Estados de "São Paulo, Rio de Janeiro, Minas Gerais, Rio Grande do Sul, Bahia, Pernambuco, Amazonas e Distrito Federal".

Segundo a FGV Direito:

"o IPCLBrasil é composto por 2 subíndices. O primeiro, o Subíndice de Percepção, é composto por 4 indicadores: legitimidade, instrumentalidade, controle social e moralidade. O outro componente do ICPLBrasil é o Subíndice de Comportamento, formado por questões que buscam avaliar a frequência com que os entrevistados disseram ter realizado condutas que violam regras de convivência social e a lei."

No gráfico 06 do relatório (exposto abaixo) é possível observar o Subíndice de Comportamento, onde se apresentam o percentual de respondentes que já realizaram as condutas questionadas, onde é plausível se surpreender com a informação de que 3% da população "levou itens baratos de uma loja **sem pagar por eles**".

Na conclusão, entendemos que podemos ter no país um grande número de "larápios" ou "furtadores" (crime Art. 155 – CP) em plena atividade.

Precisamos ***URGENTE*** ficar atentos e buscar melhorar a conformidade (COMPLIANCE) pessoal com as Leis e os bons costumes!

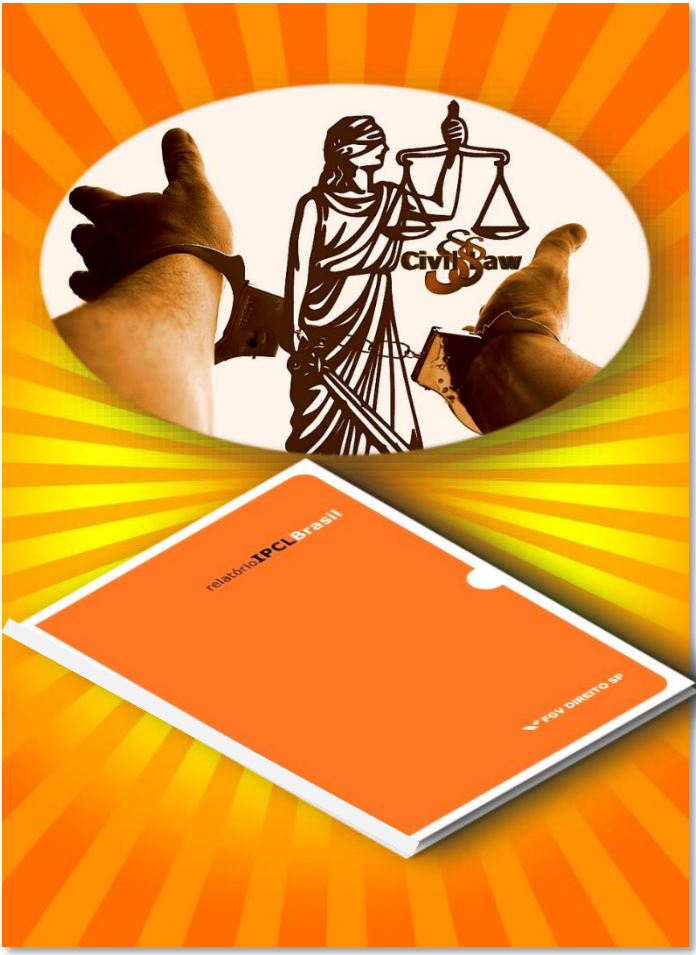
IPCL – Índice de Percepção do Cumprimento de Leis – Brasil

Maiores informações sobre o IPCL BRASIL FGV podem ser obtidas nos endereços URLs:

Composição Técnica: < http://direitosp.fgv.br/noticia/direito-gv-lanca-indicador-avalia-percepcao-brasileiro-sobre-cumprimento-leis >

Todos os relatórios: < http://bibliotecadigital.fgv.br/dspace/handle/10438/10777 >

Acessos 30/05/2018.

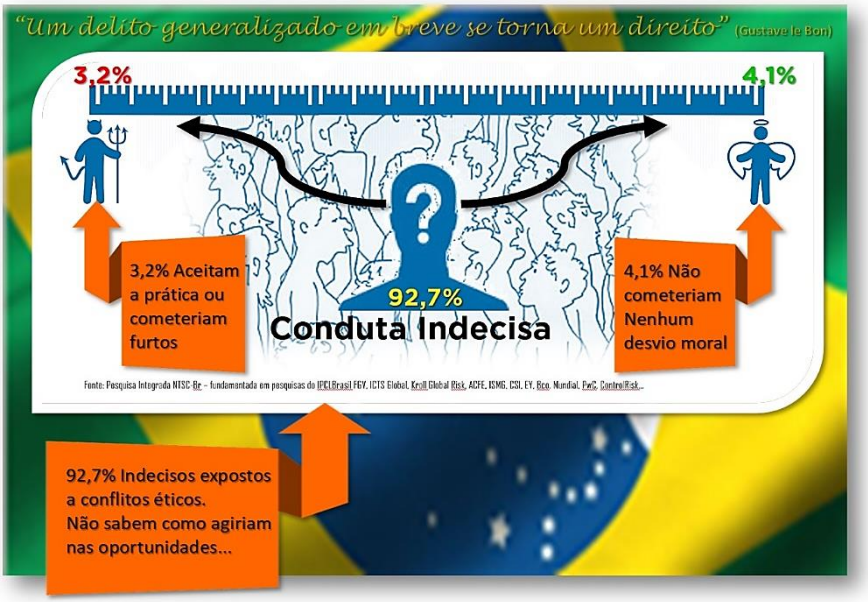


Impactos do hábito coletivo brasileiro do "furto" leve

Diversas fontes de pesquisa buscam entender o comportamento básico dos cidadãos brasileiros. A nossa situação é crítica quando observamos que as pesquisas integradas do NTSC-BR (Núcleo Técnico de Segurança Corporativa) apontam que 92,7% da amostra média da população, são de indecisos ou inseguros quanto a "qual conduta" teriam na ocorrência de oportunidades reais, de auferirem vantagens significativas, de qualquer espécie. Para a ICTS os números são ainda maiores.

Quanto a conduta média da população brasileira, ela não se difere muito dos dados de pesquisas de outras partes do mundo, e a questão da "criminalidade coletiva de uma população" não é tema novo. No entanto, sempre é bom lembrar o PERIGO que essas pessoas indecisas representam ao trabalharem nas organizações do país.

Precisamos ***URGENTE*** aplicar ações efetivas de COMPLIANCE pessoal pc



Leitura recomendada:

Livro – "A multidão Criminosa" – Spicio Sighele (1868-1913) Ed. 1954 Digitalização eBooksBrasil < http://www.ebooksbrasil.org/adobeebook/multicrim.pdf>

Apresentação ICTS – Pesquisa - IMPORTANTE:

< https://www.icts.com.br/app/webroot/files/uploads/ckfinder/files/perfil_etico_bienal_2703_FINAL(2).pdf > acessos 30/05/2018.

COMPLIANCE URGENTE
Fundamentos e Guia de Referências

Pressão Internacional

Muitas nações no mundo buscam criar Leis, Regulamentos, Normas, e promover ações contra a Corrupção. Vamos citar algumas:

- 1977 • FCPA - Foreing Corrupt Practices Act - USA
- 1996 • OEA – Convenção Interamericana Contra a Corrupção – USA-Americas
- 1997 • OCDE – Convenção sobre o Combate a corrupção – Internacional
- 1998 • Alteração FCPA > ênfase contra a Corrupção - USA
- 2000/2004 • Pacto Global ONU (décimo princípio contra a corrupção) - Internacional
- 2002 • Sarbanes–Oxley Act (SOX) – USA
- 2003 • Loi de sécurité financière (LSF) na mesma linha da SOX - França
- 2009 • Brasil - Publicação "Responsabilidade das Empresas" CGU/ETHOS[1]
- 2010 • UK Bribery Act (Lei do Suborno) – Inglaterra
- 2011 • Lei 12527 – (Lei Complementar 131/2009) Lei da Transparência - Brasil
- 2013 • Lei Federal 44/273-FZ Contramedidas contra a Corrupção - Rússia
- 2013 • Lei 12.846/13 (Lei Anticorrupção) - Brasil
- 2016 • Lei 13.303/16 (Lei das Estatais) - Brasil
- 2016/18 • GDPR - General Data Protection Regulation (EU- Europa) – 25/05/2018
- 2017 • Lei Estadual nº 7753 (Programa de Integridade)- Brasil – RJ
  Temos no Brasil, diversas outras Leis e Normas alinhadas a anticorrupção...

O mundo espera ***URGENTE*** que todos busquem estar em COMPLIANCE com as leis, normas, e melhores práticas anticorrupção.

Leitura recomendada:
Artigo: https://www.terra.com.br/noticias/dino/rio-passa-a-exigir-compliance-de-fornecedores,34181691527fb0c10cd8ecc06da024bc4te552d2.html
Artigo FCPA:
http://www.direitodoestado.com.br/colunistas/cristiana-fortini/uma-rapida-comparacao-entre-a-lei-1284613-e-norte-americano-foreign-corrupt-practices-act-fcpa
Artigo Técnico USP:
https://www.revistas.usp.br/rdda/article/viewFile/120090/122698
1>:https://www.cgu.gov.br/Publicacoes/etica-e-integridade/arquivos/manualrespsocialempresas_baixa.pdf
> acessos 30/05/2018.

Conclusões

Neste momento, esperamos que os leitores tenham absorvido uma visão mínima, porém consistente, dos grandes problemas relacionados a CORRUPÇÃO e FRAUDES, principalmente com a identificação da responsabilidade humana sobre esses eventos, com base nos dados que fornecemos.

Acreditamos que foi possível indicar diversas referências de alta relevância como a ONG "Transparência Internacional", a Kroll Inc., a McAfee, a Juniper Research, o "The World Economic Forum", a Universidade de Cambridge / LLOYD'S, a "Association of Certified Fraud Examiners (ACFE)", a "Escola de Direito da Fundação Getulio Vargas de São Paulo", o NTSC-Br, entre diversas outras indicações de Livros, artigos e informações complementares, que devem concretizar o entendimento dos problemas a serem superados.

Na consolidação das questões "endêmicas" sobre a CORRUPÇÃO e consequentes FRAUDES, as sociedades humanas mais avançadas do mundo, entendem hoje, que o remédio, mas eficaz, são os "Sistemas de Controles Internos" aplicados nas organizações, que por meio da validação permitem conduzir, ou porque não dizer "moldar" o comportamento humano dos seus colaboradores, colocando-os em conformidade ou em COMPLIANCE, com o que é ético e moral, aceitando o CERTO e combatendo o ERRADO. Dessa forma as empresas, como células de replicação de COMPLIANCE, cumprem o seu importante papel social.

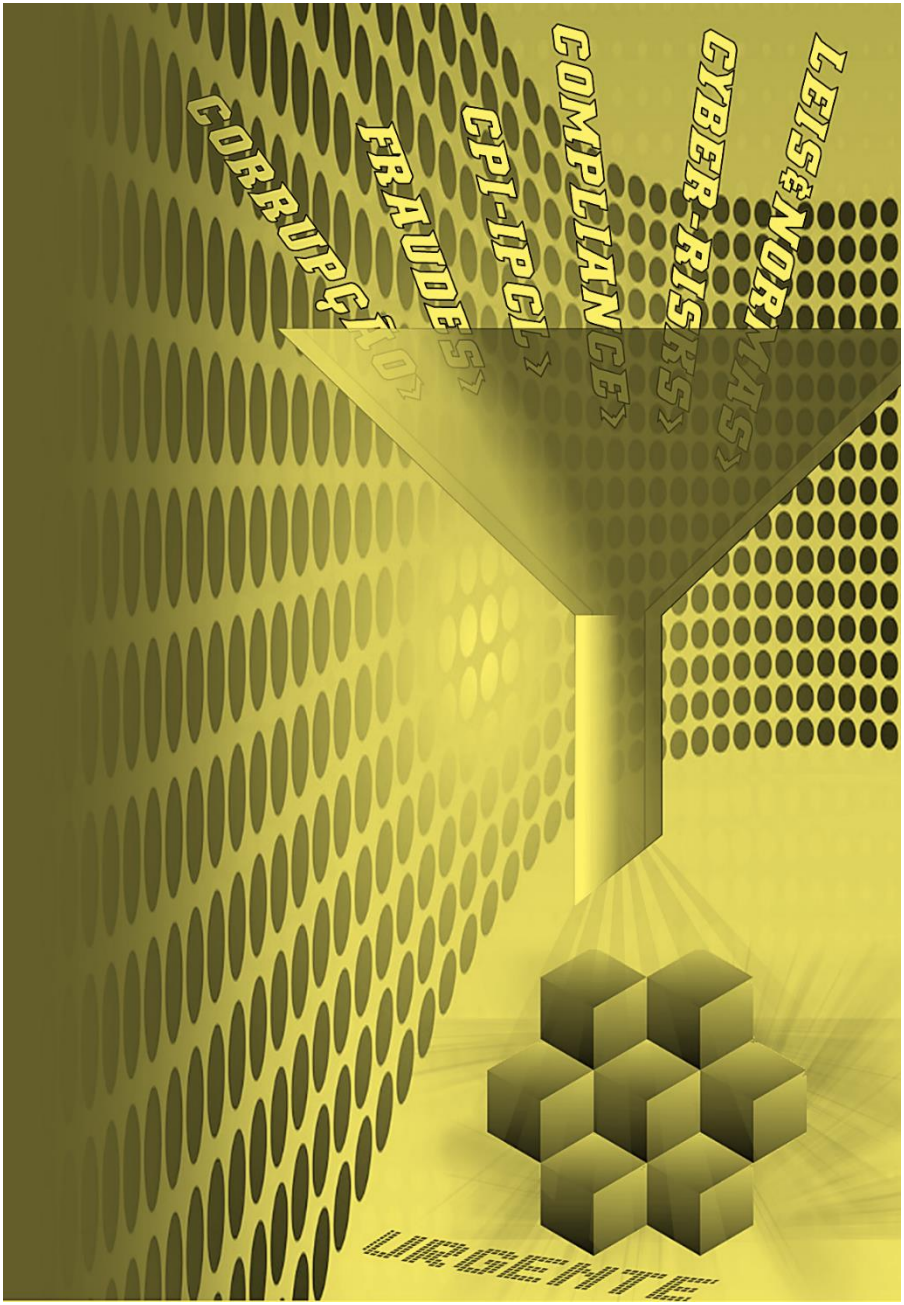
Aqui buscamos destacar a urgência de se adotar sistemas confiáveis de "Controles Internos", que possam conduzir o comportamento humano em agir em conformidade com Leis, Regulamentos, padrões e regras aceitáveis no mundo todo.

Precisamos ***URGENTE*** potencializar a COMPLIANCE - pessoal, social, empresarial, governamental...

COMPLIANCE URGENTE

COMPLIANCE URGENTE

Fundamentos e Guia de Referências



COMPLIANCE URGENTE

Fundamentos e Guia de Referências

Como reduzir os Riscos de Corrupção e Fraudes

É importante compreender que nossa visão é clara quanto a necessidade ***URGENTE*** de se implementar processos consistentes de COMPLIANCE. Entendemos que COMPLIANCE para a organização é um "EPE", ou seja, um Equipamento de Proteção Empresarial, e da mesma forma para as pessoas COMPLIANCE é um "EPI" – Equipamento de Proteção Individual, fazendo uma analogia com a indústria de Construção Civil.

O objetivo desta publicação, abordando "Como reduzir Riscos de Corrupção e Fraudes", é indicar pontos de atenção que possam colaborar com os leitores, como dicas práticas, que permitam levar ao entendimento de quais ações poderão ser tomadas, quando se busca prevenir, reduzir ou mesmo controlar as ocorrências de desvios éticos, que conduzem a corrupção e as fraudes, nas organizações de todos os portes e ramos de atividades.

BOA LEITURA

Compliance como instrumento para combater a Corrupção e Fraudes

Diversos autores vêm ao longo do tempo escrevendo sobre como COMPLIANCE pode contribuir para a redução da corrupção e das fraudes nas organizações. Nossa abordagem nesta publicação se fundamenta e cita a monografia "Categoria Profissional" do famoso colega Consultor Especialista "Renato Almeida dos Santos", denominada "Compliance como ferramenta de mitigação e prevenção da fraude organizacional", publicada como trabalho premiado durante o 6º Concurso do CGU (Controladoria Geral da União) em 2011, nominado coletânea "Prevenção e combate à corrupção no Brasil"[1], artigo apresentado a partir da página 161 da publicação.

Na prática, todos os preceitos para a redução da corrupção e das fraudes nas organizações, estão ligados à aplicação de algumas disciplinas integradas à "Administração de Empresas", como "Governança", gestão de "Riscos" e "Compliance" – ou o célebre acrônimo GRC, tão divulgado pelas mídias durante os últimos dez anos.

Hoje, mesmo que não se perceba GRC é essencial para qualquer organização independente dos ramos de atividade ou porte. Indiretamente GRC, quando trata Corrupção e Fraudes, em seu amago, aborda principalmente as pessoas, pois em Governança, se governam pessoas, em Riscos se avaliam os riscos que as pessoas podem produzir e em Compliance, se avaliam se as pessoas responsáveis cumprem suas obrigações.

Em particular, como já dito, GRC se aplica em qualquer organização, principalmente considerando a responsabilidade e o poder disciplinar dos empregadores, que está intimamente relacionado ao cumprimento do "contrato de trabalho" com os empregados, sendo este "sinalagmático" ou bilateral, pois gera obrigações e deveres para ambas as partes.

Exatamente "o poder disciplinador dos empregadores" é que habilita e facilita a implementação das Políticas de Gestão de RISCO, de COMPLIANCE e ANTICORRUPÇÃO, entre outras necessárias, e permite que se faça um amplo diagnóstico da organização, se avalie os processos de gestão e ou se implemente os processos de GOVERNANÇA básica, não corporativa.

Para se alcançar resultados adequados é fundamental e URGENTE potencializar o uso das tecnologias da Informação e de Telecomunicações no suporte aos controles internos essenciais, na busca da conformidade.

É importante lembrar que não existem padrões para a adoção de um sistema de COMPLIANCE, muito menos para implementação de Programas de INTEGRIDADE empresarial, no entanto, milhares de empresas nacionais e internacionais em conjunto com instituições públicas e privadas no mundo, já estabeleceram um "conjunto de melhores práticas" que servem de balizador aceito naturalmente, como procedimentos adequados na implementação de sistemas de COMPLIANCE, mínimo necessário.

Compliance como instrumento para combater a Corrupção e Fraudes

Nosso objetivo é oferecer total transparência e informar de forma segura os interessados na adoção de COMPLIANCE em suas organizações. Para isso seguem algumas recomendações URLs para se baixar guias e publicações relevantes:

- Programa de Integridade: Diretrizes para Empresas Privadas
- Cartilha - Integridade Para Pequenos Negócios
- Cartilha - Proteja a sua Empresa contra a Corrupção

Disponíveis em: < http://www.cgu.gov.br/Publicacoes/etica-e-integridade/colecao-programa-de-integridade >

1Monografia< http://www.cgu.gov.br/Publicacoes/controle-social/arquivos/6-concurso-monografias-2011.pdf >

Guia "Alliance for Integrity"
< https://www.allianceforintegrity.org/wAssets/docs/publications/Own-Publications/20161215_Compliance-Handbook-Brazil.pdf > em português

Artigo FIESP < http://www.fiesp.com.br/noticias/seminario-na-fiesp-debate-fraudes-na-industria/ >

Artigo Thomson < http://fgvprojetos.fgv.br/eventos/2nd-thomson-reuters-regulatory-summit >

Artigo Jornal do Comércio
< http://www.jornaldocomercio.com/site/noticia.php?codn=106644 >

Todos os acessos nos sites URLs disponíveis em: 08/06/2018.

COMPLIANCE *URGENTE*: *"A primeira e pior de todas as fraudes é enganar-se a si mesmo. Depois disto, todo o pecado é fácil".*

Philip J. Bailey

Iniciando

- **Diagnóstico Estratégico**

O primeiro passo para qualquer ação efetiva na busca de implementação de programas de COMPLIANCE que possa garantir a INTEGRIDADE empresarial é promover ***URGENTE*** uma análise profunda e isenta da organização (Assessment e Diagnóstico), buscando seus pontos fortes, suas fraquezas, as ameaças e imprevistos que podem impactá-la, bem como, identificar as oportunidades que possam advir após um processo reorganizacional.

O trabalho de Diagnóstico Estratégico sempre que possível deverá ser realizado por Consultores isentos, não pertencentes ao quadro funcional da organização, exatamente para que haja total transparência nos resultados obtidos.

Conhecer o âmago da empresa é fundamental para que se possa planejar ações efetivas no combate a Corrupção e suas consequências. Mesmo que se saiba que mais de 90% do que é necessário em termos de Controles Operacionais para COMPLIANCE são similares para qualquer organização, próximo de 10% desses controles devem ser ajustados e personalizados as reais necessidades de da cultura empresarial.

O Diagnóstico Estratégico, bem conduzido, é alicerce para o desenvolvimento de Políticas Empresarias consistentes, pois são exatamente essas Políticas, discutidas, ajustadas e escritas por empresários, sócios, executivos, gestores, etc. que permitirão a implementação de Programas efetivos de Integridade Empresarial.

O resultado isento do Diagnóstico Estratégico é fundamental para que a empresa possa planejar e materializar às mudanças necessárias, bem como, preparar-se adequadamente para agir positivamente em ambientes hostis internos e externos, sob seu controle.

Gestão e Governança

Didaticamente, as empresas, por menor que sejam, sempre adotam processos administrativos para controlar e dirigir aspectos operacionais relativos as questões contábeis, fiscais, trabalhistas, financeiras, jurídicas, e em especial controlar os ativos, a produção/operação e os clientes. De forma geral, com base nos processos administrativos, as Chefias, Gerencias e Diretorias, dessas empresas, atuam tomando decisões politico-administrativas, na maioria das vezes hierarquizadas, buscando a sinergia dos seus liderados e o aproveitamento racional dos recursos disponíveis. Esse fato que se denomina "fazer GESTÃO", ou seja, aplicar a capacidade individual de cada profissional empoderado de cargo Administrativo, na condução "ativa" da organização.

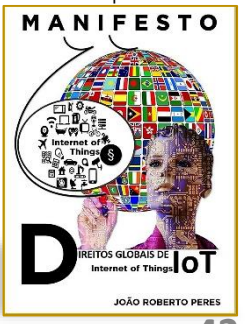
Constatamos que ao longo dos anos, os Consultores mais experientes vivenciaram grandes mudanças no mercado empresarial, onde por questões práticas, se fez necessário aplicar novos termos para identificar e distinguir claramente as visões e ações administrativas, onde a aplicação do termo "Governança" se mostrou adequado e passou a ser aplicado no mundo empresarial. A pesquisa e a história da adoção do termo Governança é polemica, mas temos convicção de que "Governança", classicamente, se aplica única e exclusivamente para "governar pessoas", que executam processos Administrativos para fazer Gestão efetivamente.

Em particular eu (autor) defendo a tese de que é possível claramente diferenciar Processos Administrativos, de Processos de Gestão e principalmente de Processos de Governança, portanto, esses Processos Operacionais "Documentados e Validados", podem e devem ser ajustados e aplicados à todo tipo e porte de organização. Ressalto aqui, que "falo" de Processos de Governança Operacional, não de "Governança Corporativa".

A Governança Corporativa, com suas práticas e diretrizes ainda não padronizadas no mundo, atua em um patamar mais avançado, mesmo se valendo de conceitos puristas de "Governança", que teve origem ideologicamente há muitos séculos atrás. A Governança Operacional, que aqui incentivo, está fundamentada em conceitos e "melhores práticas" mundiais, onde através da "Governança Simples", em qualquer empresa as decisões possam ser colegiadas, e os gestores dessa forma, serão dirigidos estrategicamente e agirão de forma uniforme, em termos de conduta e ética organizacional, buscando resultados positivos e a perenidade da empresa.

Leitura Recomendada:

Ler impreterivelmente, o "Apêndice" – Governança conceitos Fundamentais - inicia na página 53 do e-book do mesmo autor, disponível em:
< http://www.komp.com.br/gallery/e-book-iot-manifesto-edicao1qp.pdf > acesso 05/06/2018.



Gestão e Governança

Observe as diferenças sutis, mas determinantes, entre Gestão e Governança e o que elas significam na prática, pois são complementares.

Potencialização do uso de tecnologias para "Controles Internos"

É fundamental compreender que as tecnologias integradas, principalmente, da "Informação e Telecomunicações", são fundamentais, pois atuam como ferramentas de suporte operacional, e contribuem de forma decisiva para a implementação de "**controles internos**", essenciais para se alcançar a conformidade, com padrões operacionais, normas internas, procedimentos operacionais, regulamentos setoriais, normas nacionais e internacionais, Leis e requerimentos específicos sobre o setor onde a organização atua.

A adoção efetiva de sistemas de "controles internos" informatizado e seguro é basilar para assegurar a fidedignidade e integridade dos dados e registros operacionais, bem como para a produção de relatórios contábeis, financeiros e gerenciais eficientes para a apropriada tomada de decisões.

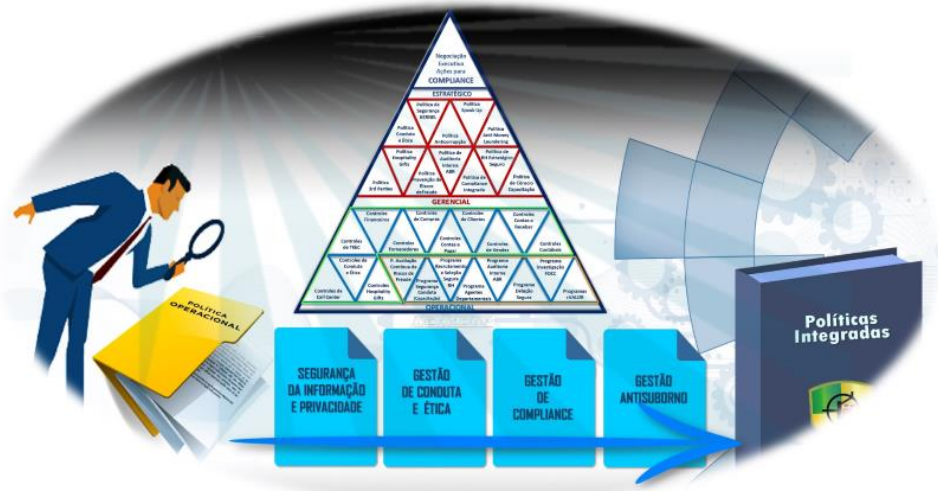
Temos de avaliar ***URGENTE*** se os recursos tecnológicos que utilizamos em nossas empresas estão aderentes, atualizados e preparados para nos apoiar no processo de implementação de COMPLIANCE.

Leitura Recomendada: Estudo < https://www.tjdft.jus.br/institucional/controle-interno/informativos/tcu-estudo-de-controle-interno-um-estudo-dos-modelos-e-das-normas-disciplinadoras-em-diversos-paises/at_download/file >
Artigo Técnico "Uso Efetivo de Controles Internos em uma Microempresa" – UFRGS : <https://www.ufrgs.br/ppgcont/arquivos/Contabilidade%20para%20Usu%C3%A1rios%20Internos/03%20Elionai_de_Moraes_Postiglione.pdf >
Manual de Gestão de Integridade, Riscos e Controles Internos da Gestão – Guia - Ministério do Planejamento: < http://www.planejamento.gov.br/publicacoes/controle-interno/manual_de_girc___versao_2_0.pdf >
Artigo Técnico "A Tecnologia da Informação como suporte à Gestão Estratégica da Informação na Pequena Empresa" < http://www.scielo.br/pdf/jistm/vInI/03.pdf >
Artigo mercado TI: < https://gaea.com.br/compliance-e-tecnologia-da-informacao-entenda-essa-relacao/ >
acessos em 30/05/2018.

Políticas Empresariais integradas

É obrigatório às empresas antes de iniciar suas atividades, estabelecer o "objetivo social", ou seja, quais atividades a organização pretende realizar. Assim, é provável que os sócios tenham discutido e definido "que tipo de empresa se quer ser" e formado uma visão de atuação para a organização, cujo documento escrito costuma ser chamado de "Política Empresarial" ou "Política Operacional". Na prática, essas "Políticas" são criadas gradativamente ao longo do tempo de vida da empresa, atendendo demandas organizacionais e situacionais.

Ocorre que na maioria das vezes, os sócios ou executivos, ao estabelecerem novos direcionamentos estratégicos, em novas Políticas, não observam o alinhamento com as definições anteriores que já foram publicadas e divulgadas, criando muitas vezes incoerências e abrindo brechas para interpretações diversas dos seus colaboradores. O fato, potencializa os riscos de CORRUPÇÃO e FRAUDES.



O tema "Política Empresarial" é amplo e polemico, mas entendemos, que para o nosso objetivo algumas definições possam contribuir:

"**Política:** Definição escrita que indica a "direção" ampla para a organização como um todo: "que tipo de empresa queremos ser"?

Objetivo: Medida "quantitativa" ou "qualitativa" que complementa ou apoia a política.

Estratégia: Alternativas consistentes que otimizem ou através das quais se permita cumprir as políticas da empresa.

Plano: programa e passo-a-passo para se atingir as estratégias identificadas e consolidadas nas políticas."[1]

Políticas Empresariais integradas

Considerando as práticas de mercado é fundamental para a implementação de um "Programa de Integridade" apoiado por COMPLIANCE, que ao se estabelecer novas "Políticas Internas", estas sejam devidamente integradas e alinhadas as políticas internas anteriores, bem como, com a Missão, Visão e Valores da organização.

É fundamental buscar "ser e estar" em ***COMPLIANCE URGENTE***.

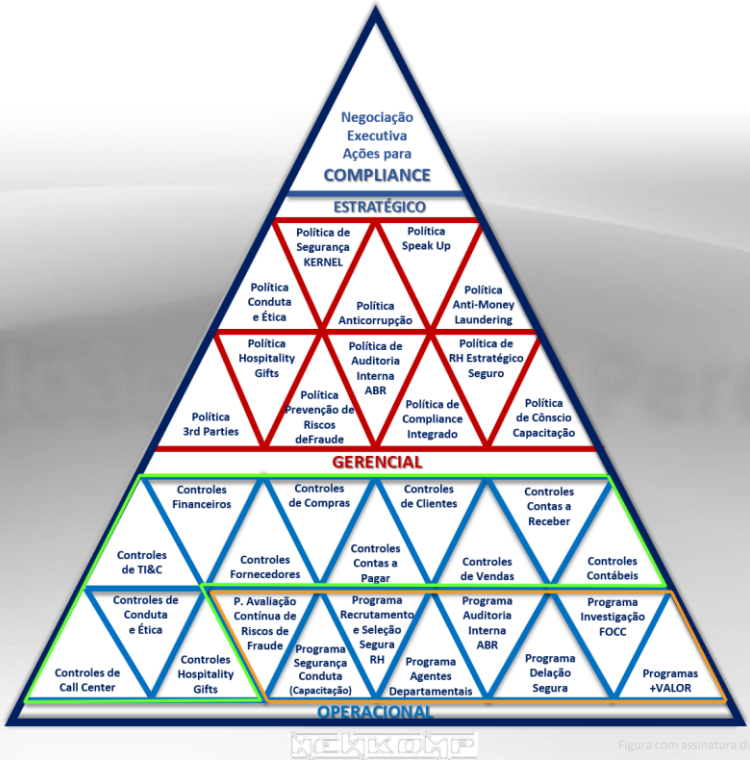


Figura com assinatura digital

Leitura Recomendada:

Artigo Técnico "Possíveis Definições para as Políticas Empresariais":
< http://sistema.semead.com.br/7semead/paginas/artigos%20recebidos/Pnee/PNEE14_-_Poss%EDveis_defini%E7%F5es_pol%EDticas_empres.PDF >

Políticas exemplos - Documento Público - Modelo Amplo – disponível em:
<http://ri.fleury.com.br/fleury/web/download_arquivos.asp?id_arquivo=E2BE1967-95D1-4ECA-A399-67EA7F3C3A9C > acessos 30/05/2018.

"Procurando pessoas para contratar, você busca três qualidades: integridade, inteligência, e energia. E se elas não têm a primeira, as outras duas matarão você." Warren Buffett

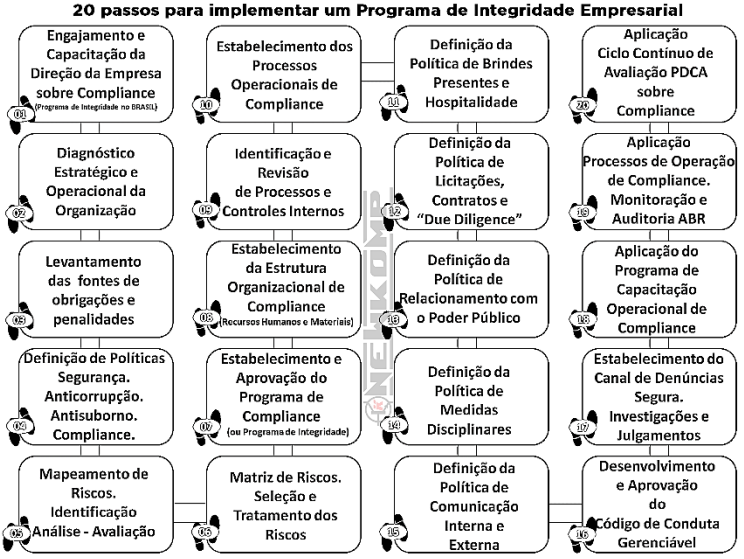
Prepare-se URGENTE para enfrentar o futuro.
Implemente programas de Integridade!

Programa de Integridade
Pequenas e Médias organizações - *URGENTE*

Implementar um "Programa de Integridade" incluindo efetivamente a COMPLIANCE empresarial, não deve ser considerada uma missão inalcançável, pois, se devidamente identificada a necessidade e os benefícios do "Programa" pelo sócios, mesmo na pequena empresa, a iniciativa de colocá-lo e prática é só uma questão de atitude, pois o investimento financeiro para isso pode ser muito baixo, principalmente se houver a devida compreensão de que muito do que é necessário, provavelmente já esteja sendo realizado pela organização.

Em pequenas organizações, cada integrante da sociedade (sócio) e todos os colaboradores deverão inicialmente serem sensibilizados, capacitados e treinados continuamente, para absorverem gradativamente a cultura de COMPLIANCE, ou seja, "serem e estarem em COMPLIANCE". Dessa forma, antes de se pôr em prática um "Programa de Integridade", é fundamental desenvolver um processo de conscientização organizacional sobre o tema COMPLIANCE e suas vantagens para os colaboradores, para a organização e para a sociedade.

O que se observa na prática, é que mesmo nas pequenas organizações se promovem reuniões, encontros e dinâmicas motivacionais, onde se discutem metas, estratégias, se incentivam a produtividade, entre outros temas, de forma que, tratar sobre as vantagens do COMPLIANCE, poderia ser mais um objetivo e principalmente em "empoderar" cada colaborador para se tornar um "AGENTE de COMPLIANCE", sobre as atividades que realizam cotidianamente.

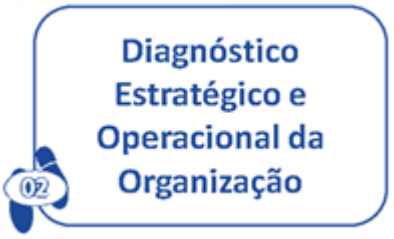


Leitura Recomendada:
Fundamentação Código de COMPLIANCE - Guia de Melhores Práticas de Compliance no Âmbito Empresarial 2017.
<http://ibdee.org.br/wp-content/uploads/2017/05/IBDEE-2017-Guia-Compliance-digital.pdf>
IBDEE - Instituto Brasileiro de Direito e Ética Empresarial.
acesso 30/05/2018.

Programa de Integridade
Pequenas e Médias organizações - *URGENTE*

- **Proposta de Passos sequenciais para implementação:**

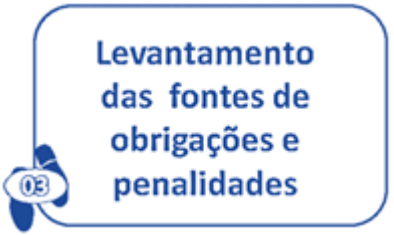
A implementação de um Programa de Integridade exige o irrestrito apoio da alta administração da empresa. Para isso se determina o estabelecimento de um "Termo Declaratório de Comprometimento", com cláusulas específicas sobre o apoio dos signatários ao fomento a uma cultura de integridade ética e moral, com total aderência as Leis, regulamentos e normas (internas e externas) aplicáveis ao perfil de negócios da organização. Neste mesmo documento de "start" mandatório de promoção do Programa de Integridade, também é importante estabelecer parâmetros de comprometimento dos gestores quanto ao prazo e alcance, bem como, definir a responsabilidade e a independência irrestrita da instância operacional de COMPLIANCE.



Para conhecer a organização e facilitar a implantação de um sistema eficaz de "Controles Internos", que fornecerá dados para os processos de COMPLIANCE, é importante contratar um serviço de "terceira parte" isenta, para realizar um "Assessment Organizacional" que permita estabelecer o "Diagnóstico Estratégico" da empresa, sendo este subsidio para um ciclo de "Planejamento Estratégico Situacional[1]" flexível. O diagnóstico permitirá conhecer o potencial da organização e direcionar forças para ampliar segurança e assertividade nas tomadas de decisão. Recomenda-se que o processo de "Diagnóstico Estratégico" seja realizado de forma cíclica, com periodicidade bienal, sempre validando resultados dos 2 anos anteriores.

Leitura Recomendada: [1]Artigo Técnico: "Planejamento Estratégico Situacional" < http://www.scielo.br/pdf/prod/v3n2/v3n2a04.pdf > acesso 30/05/2018.

Programa de Integridade
Pequenas e Médias organizações - *URGENTE*



Este requerimento normalmente é realizado inicialmente no passo 02 durante o Diagnóstico, no entanto, conhecer em profundidade as obrigações Legais, Regulatórias, de Mercado, Contratuais, entre outras, que incidem sobre a área de atuação e o tipo de negócio da empresa é fundamental.
É importante conhecer os riscos e as penalidades e multas as quais a organização estará sujeita, no caso do não cumprimento de obrigações, legais ou regulatórias, entre outras, portanto, os responsáveis por atividades contábeis, fiscais, trabalhistas, tecnológicas e principalmente jurídicas, deverão estar atentos continuamente em alinhar os novos requerimentos de conformidade, com os controles internos, e o devido atendimento as obrigações.

Com base no "Diagnóstico" e "Planejamento Estratégico" para um próximo horizonte de tempo, as Políticas Operacionais ou Empresariais existentes devem servir de base para alinhamento na definição e inclusão gradativa de novas políticas "prioritárias" de "Segurança Empresarial"; "Anticorrupção"; "Antisuborno" e "Compliance". Outras como: Controles Internos; Conduta Ética; Gestão de Riscos; Auditoria Interna; Privacidade; Gestão Humana; Capacitação e Cônscio; Saúde e Segurança Ocupacional; Gestão de Ativos; Gestão Ambiental; Integridade; etc. também devem ser consideradas. Recomenda-se a criação de novas Políticas sempre integradas coerentemente com as publicações anteriores, colocadas em prática.

Leitura Recomendada:
Mapeamento dos Riscos de Corrupção:
< http://www.pm.al.gov.br/intra/downloads/bc_corrupcao/cor_04.pdf >
Grisk-TRT6< http://www.trt6.jus.br/portal/sites/default/files/documents/metodologiagestaoriscostrt6_0_3.pdf >
acessos 30/05/2018.

Programa de Integridade
Pequenas e Médias organizações - *URGENTE*

Como quinto passo na implementação de um "Programa de Integridade", o objetivo é adotar na prática uma Metodologia de Identificação, Mapeamento, Análise a Avaliação de Riscos que se ajuste ao perfil da empresa. Recomenda-se a aplicação de metodologias consagradas, conforme o perfil da empresa, como: métodos Qualitativos> (APR; Método de Mosler; Método William T. Fine;...) ; ou Quantitativos> (Monte Carlo, FMEA,...) entre outros mais avançados como COSO-ERM, e sempre que possível "informatizar os processos" e manter documentada a identificação e o mapeamento básico dos riscos, para atender ao sexto passo do "Programa de Integridade".

Neste passo é fundamental construir uma "Matriz do Impacto dos Riscos" e avaliar os riscos mapeados com base na sua escala de relevância, classificando-os e selecionando os Riscos Críticos para uma ponderação mais detalhada, que possa indicar qual o melhor tratamento a ser dado, na hipótese de se Evitar o Risco, Mitigar o Risco ou seja, buscar reduzi-los, Transferir o Risco, ou seja exemplo: adquirir Apólice de Seguro para garantir a redução de perdas, ou ainda Aceitar os Riscos Mitigados e residuais, de forma que possam ser tratados através da monitoração e gerenciamento. Os Controles Internos sobre os Riscos devem considerar os Riscos da Não Conformidade ou Riscos de COMPLIANCE.

Leitura Recomendada: Metodologia de Gestão de Riscos
< https://www.cgu.gov.br/Publicacoes/institucionais/arquivos/cgu-metodologia-gestao-riscos-2018.pdf >
Gerenciamento de Riscos IBGC < http://www.ibgc.org.br/userfiles/3.pdf >
Manual Documentação de Procedimentos
< https://supad.ufba.br/sites/supad.ufba.br/files/manualsupaditspos.pdf > acessos 30/05/2018.

Programa de Integridade
Pequenas e Médias organizações - *URGENTE*

Com base no Diagnóstico, no Planejamento, na identificação das fontes de obrigações e penalidades, nas definições de novas Políticas Empresariais Integradas, na Matriz de Riscos e na seleção dos riscos a serem tratados, se faz possível estabelecer/planejar adequadamente um "Programa de Compliance", ajustado a realidade da empresa. O estabelecimento das "Ações Chaves Estratégicas" do Programa de Compliance é fundamental para que após sua implementação, em conjunto com outras ações, se possa garantir que a organização disponha de um "Programa de Integridade" efetivo. Alguns Consultores atribuem ao Programa de Compliance o atributo de "Programa de Integridade", mas este é maior e mais abrangente.

O Programa de Compliance estabelecido no passo 07 deve determinar que haja um responsável nominado na estrutura organizacional formal, para exercer o cargo de líder ou chefe de conformidade ou mais tecnicamente (CCO) "Chief Compliance Officer". Em empresas pequenas esse título é dispensável, mas a necessidade de nomear um responsável é imprescindível. Da mesma forma, a equipe que trabalha com "COMPLIANCE" deverá ser estabelecida com pessoal treinado, ou seja, os "Compliance Officers", onde em empresas pequenas, a equipe poderá ser diminuta, sem treinamento profundo, contando com a colaboração de todas as chefias operacionais com atribuição adicional, não remunerada, de "Agente de Conformidade".

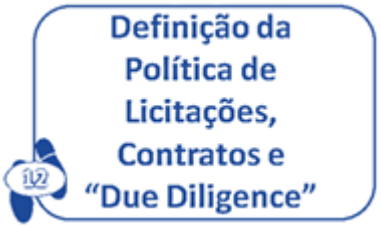
Programa de Integridade
Pequenas e Médias organizações - *URGENTE*

De forma similar, o Programa de Compliance do passo 07, deve indicar a rápida execução de um trabalho de revisão dos Controles Internos, com a identificação e ou estabelecimento de "pontos de verificação da Conformidade" nos "processos / procedimentos operacionais" já existentes. É imprescindível que os processos operacionais e os controles internos estejam minimamente documentados, sendo que da mesma forma, devem ser incluídos na documentação os "pontos de verificação da Conformidade" estabelecidos. A inclusão dos "pontos de verificação da Conformidade" deverá ocorrer sempre que um novo processo / procedimento operacional de qualquer espécie seja implementado na organização.

Com base na Revisão dos Processos Operacionais, seus Controles Internos, e da inclusão dos "pontos de verificação da Conformidade", se faz possível alinhar todas as "fontes de obrigações e penalidades", em calendário de compromissos e estabelecer Processos / Procedimentos Operacionais de Validação da Conformidade e Ações de identificação de "Não Conformidade". Os processos / procedimentos Operacionais de Compliance devem ser aderentes as determinações da Política de Compliance e demais Políticas Empresariais. A execução dos Processos Operacionais de Compliance será realizada por "Compliance Officers" ou "Agentes de Conformidade", gerenciados pelo CCO ou Chefe, com responsabilidade atribuída formalmente.

Programa de Integridade
Pequenas e Médias organizações - *URGENTE*

Como requerimento mandatório para um "Programa de Integridade", o desenvolvimento interno de uma políticas que trate da oferta de brindes, do recebimento de presentes de terceiros e das ações de hospitalidade da organização quanto a clientes e fornecedores, se faz necessária. O mercado denomina essa política de "Policy for Gifts & Hospitality", sendo internacionalmente reconhecida como necessária na regulação ética e moral entre a empresa, seus parceiros, fornecedores e principalmente clientes. Este decimo primeiro passo é importante, no entanto, cada organização deverá estabelecer em seu documento da Política sobre o tema, os limites de valores e de entendimento do que considera ético com base na sua cultura.



Neste decimo segundo passo, a recomendação e desenvolver após a devida análise, uma política interna que estabeleça o comportamento organizacional quanto a participação de concorrências e licitações comerciais. Da mesma forma, acreditamos que possa ser incluída na mesma política o relacionamento da organização com fornecedores, quanto as práticas de aquisição através de todos os mecanismos do mercado. Quanto a "aquisições empresariais" é fundamental que a política interna estabeleça os cuidados na análise das credenciais reputacionais dos fornecedores, dos documentos fiscais, entre outros cuidados, executando a "Due Diligence", para mitigar riscos envolvidos em operações de aquisição de toda a espécie.

Leitura Recomendada: Artigos sobre Políticas, Normas e Procedimentos:
1< https://www.gestaodesegurancaprivada.com.br/politica-norma-e-procedimento-o-que-e/>
2 < https://advisera.com/27001academy/pt-br/knowledgebase/sete-passos-para-a-implementacao-de-politicas-e-procedimentos/ > acessos 30/05/2018.

Programa de Integridade
Pequenas e Médias organizações - *URGENTE*

Este decimo terceiro passo é fundamental, pois, o desenvolvimento de uma política empresarial que trate do Relacionamento da Empresa com organismos públicos governamentais e seus servidores, para quaisquer atividades da empresa, sejam fiscal tributária, trabalhista, e até como prestadora de serviços ou fornecedora de ativos é muito importante. A Política deve estabelecer rígidas diretrizes que possam nortear a conduta de seus colaboradores, terceiros a seus serviços, parceiros e fornecedores, no relacionamento com o setor público, em quaisquer circunstância. Objetiva prevenir a ocorrência de condutas e situações que possam ser interpretadas como e atos ilícitos ou de corrupção contra a Administração Pública.

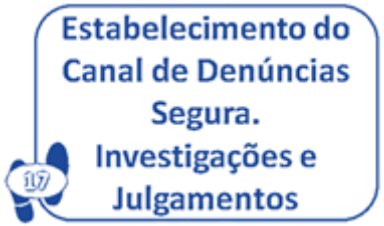
Desenvolver previamente uma política empresarial que trate sobre medidas disciplinares e suas consequências após a apuração de fatos, que comprovadamente caracterizem desvios comportamentais éticos e de conduta moral, dos integrantes da organização, sejam sócios, executivos de alto escalão, chefias, colaboradores, terceiros, parceiros, fornecedores e até clientes, possui um elevado peso no alcance de um bom "Programa de Integridade". É estratégico nesse momento de desenvolvimento, antever a maioria das diretrizes de conduta ética e moral que deverão ser requeridas quando do desenvolvimento futuro do "Código de Conduta Empresarial" necessário.

Programa de Integridade
Pequenas e Médias organizações - *URGENTE*

No decimo quinto passo, se propõe o desenvolvimento de uma politica empresarial para estabelecer previamente processos formais de comunicação interna, com os colaboradores, prestadores de serviços, terceiros contratados e parceiros, onde o devido emprego dos conceitos de "endomarketing" sejam aplicados, considerando minimizar impactos de "comunicação" que possam ser considerados assédio; intelectual, moral, de comunicação perversa, impositiva, entre outros. A politica também deve regular a comunicação e pré-estabelecer padrões de mensagens adequadas e éticas com fornecedores, clientes e autoridades, principalmente nos temas ligados a possíveis desvios de conformidade, ou acidentes operacionais imprevistos.

O decimo sexto passo, para a implementação do Programa de Integridade é fundamentado em conceito estratégico, onde a exigência da organização dispor de um "Código de Conduta Gerenciável" é imprescindível. De forma oposta aos antigos Códigos de Ética, que explicitavam ideologicamente os preceitos éticos entendidos pela organização, os modernos "Códigos de Conduta" especificam de forma endereçável e mais detalhada na prática, os "procedimentos" esperado dos colaboradores, em cada situação prevista. O atendimento as diretrizes do Código de Conduta, deverá operar através da validação de "Controles Internos", passando dessa forma, ser gerenciada a aderência ou desvios da conduta esperada.

Programa de Integridade
Pequenas e Médias organizações - *URGENTE*



Em especial é exigência que os "Programas de Integridade" empresarial, disponham de "mecanismos isentos" que permitam aos colaboradores se manifestarem sobre seus sentimentos, interpretações, identificações de ocorrências, de desvios comportamentais e éticos, em especial desvios de conduta quanto a corrupção e fraudes, sem medo de penalidades. As ouvidorias ou "Canais Ativos de Denúncias e Investigações" objetivam o recebimento de manifestações, elogios, críticas e denúncias, que devem ser investigadas em profundidade, através de processos adequados. Sempre que possível, os "Canais Ativos" deverão ser terceirizados para garantir a equidade e permitir "julgamentos imparciais" de ocorrências.

No passo dezoito, se considera que a estrutura do "Programa de Integridade" esteja quase que completa, sob a ótica de diretrizes e procedimentos operacionais estabelecidos. Neste momento se faz necessário promover um programa (planejamento e execução) de Capacitação e Treinamentos em "COMPLIANCE e INTEGRIDADE específicos da Empresa" aplicando-os integralmente aos "Compliance Officers" e ou "Agente de Conformidade", bem como, a todos os demais colaboradores e terceiros ligados a organização. A Capacitação considera ensinar o que não se sabe, enquanto os Treinamentos fortalecem e aperfeiçoam conhecimentos pré-existentes, assim como, a Conscientização informa e promove reações comportamentais.

Programa de Integridade
Pequenas e Médias organizações - *URGENTE*

Neste ponto o "Programa de Integridade", já se encontra apto a entrar em operação, com a ativação operacional do sistema de Controles Internos ajustados, com os processos operacionais de COMPLIANCE ativos, momento a partir do qual se inicia o ciclo operacional e de "Monitoração Contínua" da conformidade, que busca garantir que a organização opere de forma ética e integra, cumprindo e justificando seu papel social. Para que ocorra a validação da Monitoração de COMPLIANCE, é fundamental estabelecer processos de Auditoria Interna Baseada em Riscos (ABR), que utilizando devidamente a metodologia "ABR" possa auditar operações e situações de maior risco, conforme receba alertas do sistema de Gestão de Riscos.

Para concluir, o vigésimo passo recomenda o desenvolvimento de um "ciclo contínuo" PDCA, de revisão e aperfeiçoamento dos processos de Controles Internos, dos processos operacionais de COMPLIANCE, de Monitoração e de Auditoria Interna, para promover a avaliação, ajustes e inclusões no Código de Conduta, no aprimoramento dos processos de "investigação interna", nos mecanismos dos "Canais Ativos de Denúncias", entre outros. O planejamento e execução de ciclos contínuos PDCA promove a garantia de que o "Programa de Integridade" adotado sempre se mantenha em COMPLIANCE com os anseios da organização e sociedade humana em geral.

Leitura Recomendada: Guia – Auditoria Baseada em Riscos
< https://www.qsp.org.br/pdf/implemente_abr.pdf >
Artigo Treinamento Compliance
< https://epocanegocios.globo.com/Publicidade/Petrobras/noticia/2017/12/treinamento-em-compliance-e-estrategia-essencial.html > acessos 30/05/2018.

Gestão de Compliance Norma "ISO 19.600:2014"

A norma internacional "ISO 19.600:2014" (ISO significa: International Organization for Standardization), foi lançada para ser um guia básico, indicando o que deve ser feito para a "gestão da conformidade" (COMPLIANCE), mas não aconselha como proceder ou implantar os processos operacionais de controle de COMPLIANCE.

A versão inicial da norma, por nascer "Guideline", não se dedica a propiciar as empresas, processos de CERITIFICAÇÃO de sua adoção. A Norma é simples e possui apenas 31 páginas (Brasil 34) abordando objetivamente; o "Contexto da Organização", a "Liderança" necessária para a realização das fases de "Planejamento", "Suporte", "Operação", e as de "Avaliação do Desempenho" e "Melhoria Contínua", necessárias.

O fundamento da norma ISO 19.600, tem raiz a norma Australiana, de fevereiro de 2013, designada como ONR 192050:2013 02 01. Como parte essencial a norma ISO 19.600 emprega os padrões de "Gestão de Riscos" da Norma ISO 31.000, que no Brasil é a atual ABNT NBR ISO 31000:2018 (diretrizes). No caso, a recomendação é iniciar os processos de COMPLIANCE com a definição de Políticas (Anticorrupção/Antisuborno, entre outras) com um amplo inventário de Riscos, com sua devida avaliação, e que esse processo seja integrado de forma contínua, por gestão de riscos, conforme recomenda a norma ISO 31.000, para servir de "input" para os controles internos, sendo base para as entradas 4.1 (problemas), conforme gráfico na próxima página ao lado esquerdo.

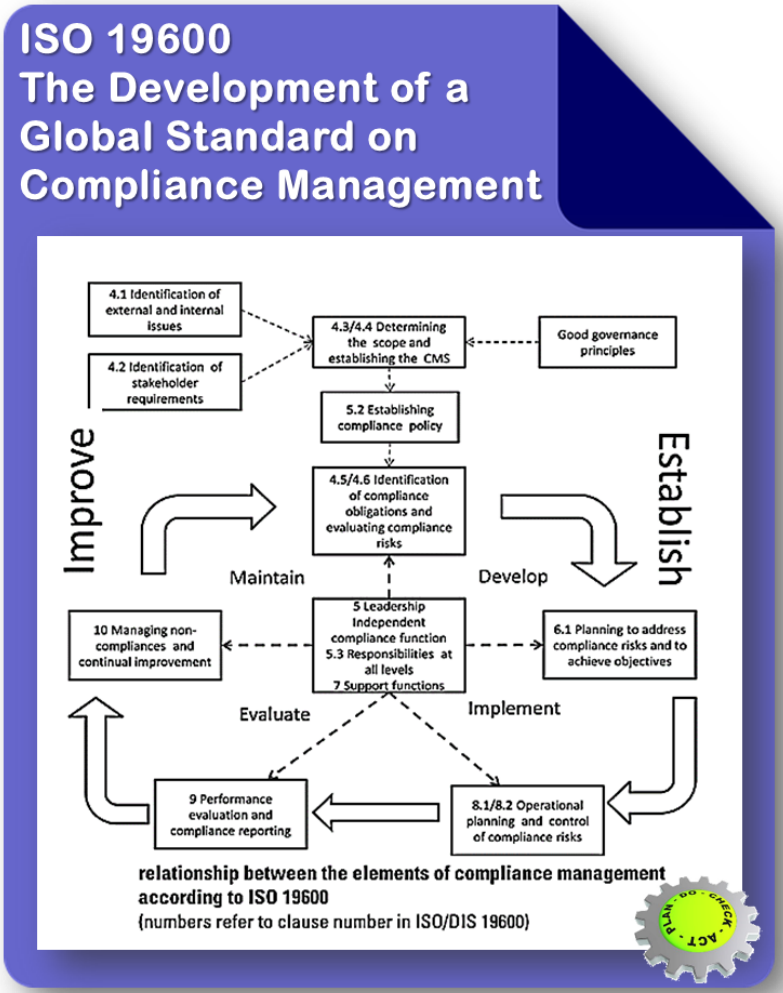
O modelo de gestão de COMPLIANCE se inicia efetivamente no capitulo 4.1 e 4.2, da norma, com a devida identificação dos usuários internos e externos que atuam sobre os processo de conformidade, dos "stakeholders" (público estratégico ou influenciadores diretos ou indiretos), seguindo no estabelecimento do escopo do CMS (Compliance Management Systems) nos capítulos 4.3 e 4.4. Na sequência se estabelecem as Políticas de Compliance (5.2) e se identificam as obrigações de avaliação dos riscos de conformidade (4.5 e 4.6), concluindo-se na fase de estabelecimento do modelo (Establish). No conjunto de processos seguinte identifica-se o ciclo de melhoria contínua (PDCA), com a indicação clara nos capítulos da Norma, em cada fase.

Aquisição da Norma 19.600 ABNT: <http://www.abntcatalogo.com.br/norma.aspx?ID=359340> acesso 30/05/2018.

COMPLIANCE URGENTE

Fundamentos e Guia de Referências

Gestão de Compliance Norma "ISO 19.600:2014"



Leitura recomendada: e-book do mesmo autor "Guia Introdutório sobre COMPLIANCE, abrangendo as principais áreas de alcance." < http://www.uberconsult.com.br/artigos-e-conteudos/e-books-disponibilizados/ > acesso 30/05/2018.

Gestão Antisuborno - Norma "ABNT NBR ISO 37.001:2017"

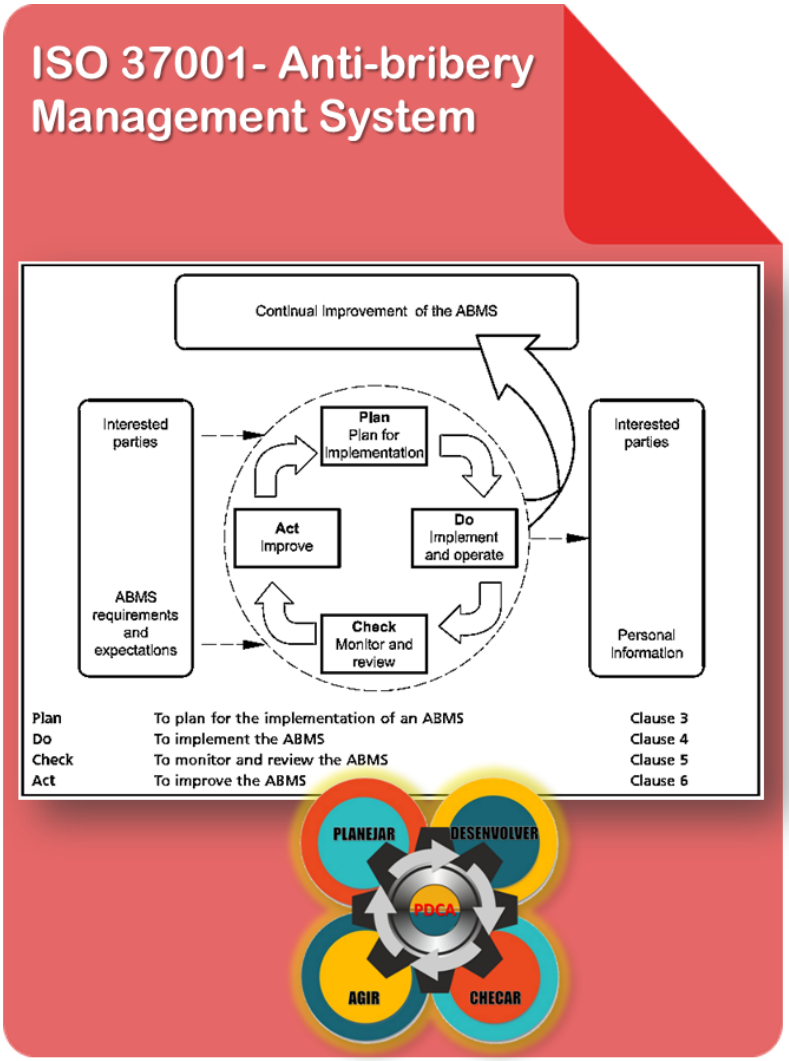
A Norma ABNT NBR ISO 37.001:2017, publicada originalmente em outubro de 2016 – em Genebra, Suíça, veio efetivamente se tornar um complemento para a Norma ISO 19.600, pois as organizações que já utilizam a "Gestão de Compliance" terão bastante facilidade em atender os requisitos da Norma 37.001.

O objetivo da Norma 37.001 não é diretamente combater a CORRUPÇÃO em todas as suas formas, mas combater uma das principais causas, ou seja, o SUBORNO. Portanto, a 37.001 possui foco em estabelece medidas nas empresas, para prevenir e detectar os casos de suborno considerando:

- Mapear e avaliar os riscos de suborno
- Desenvolver Política Antisuborno
- Desenvolver Política de Presentes, Entretenimento e Hospitalidade
- Desenvolver e Implementar Processos de Controle Antisuborno
- Estabelecer Processos de "due dligences" (investigação prévia de oportunidades de negócios)
- Atribuir a função de compliance a responsabilidade de monitorar a operação do sistema de Gestão Antisuborno
- Capacitar, treinar e conscientizar colaboradores e terceiros envolvidos em ações Antisuborno
- Divulgar a política e ações Antisuborno aos stakeholders (subcontratados, terceiros, parceiros de negócios, fornecedores, etc.)
- Validar o cumprimento das condutas e ações Antisuborno praticadas
- Implementar e validar operações e procedimentos dos canais de denúncia
- ...

De forma geral o sistema de Gestão Antisuborno da Norma 37.001 é simples e baseado no padrão PDCA, como indica figura a seguir:

Gestão Antisuborno - Norma "ABNT NBR ISO 37.001:2017"



Leitura recomendada: Artigo de fundamentação < https://mauricioflankejchel.jusbrasil.com.br/artigos/387448721/iso-37001-sistema-de-gestao-antisuborno-a-hora-e-agora > Artigo de Referência do IBDEE < http://www.ibdee.org.br/os-programas-de-compliance-e-a-certificacao-iso-37001/ > Aquisição da Norma ABNT NBR ISO 37.001 < http://www.abntcatalogo.com.br/norma.aspx?ID=368323 > acessos 08/06/2018.

Regulamento de Proteção de Dados GDPR

Considerando a seriedade do tema, devemos dar a importância necessária, pois a "Privacidade de Dados" e consequente privacidade de informações pessoais e empresariais passam a ser de alta relevância no momento atual da humanidade, motivo pelo qual a Comunidade Europeia desde 25/05/2018 passa a exigir a aplicação do Regulamento GDPR. No contexto é bom observar que as tecnologias de Comunicação e Processamento de Dado, em larga escala "BIG DATA", bem como as tecnologias de "Analytics", entre inúmeras outas, estão disponibilizando dados e consolidando informações privadas a quem não dispõe do direito a cessá-las. Muitas organizações no mundo e governos estão comercializando dados pessoais e empresarias em troca de remuneração - veja: "CHUPA DADOS" - ISSO NECESSITA SER INIBIDO**1.**

A regulamentação GDPR é fundamental para todas as pessoas e organizações, pois, endereça medidas preventivas e atribui responsabilidades no tratamento, preservação e armazenamento de informações pessoais de cidadãos Europeus, mas indiretamente também pode ser aplicada ao mundo todo.

Estar em COMPLIANCE com a GDPR é uma questão Ética que necessita **URGENTE** ser considerada por todas as organizações, independente do ramo de atividade e porte.

Para adoção básica do GDPR, faça a leitura e interpretação do INFOGRAFICO indicado. No entanto, para adoção adequada e completa, recomendamos a contratação de Consultoria Especializada, devido à complexidade legal e requerimentos internacionais.

INFOGRAFICO – INTERATIVO EM PDF
ACESSO < https://www.kaspersky.pt/other/custom-html/local-pages/gdpr/img/diagram.pdf > acesso 30/05/18

Regulamento de Proteção de Dados GDPR

[1]site da CODINGRIGHTS projeto CHUPADADOS < https://chupadados.codingrights.org/ >

Fonte Oficial de dados GDPR < https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_pt > acessos 30/05/2018 (em português)

Lei Geral de Proteção de Dados – LGPD Brasil

A lei nº 12.965, de 23 de abril de 2014, que estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil, teve proposta de alteração aprovada pelo Senado em 10/07/2018, com fundamento no PLC 53/2018 do deputado Milton Monti (PR-SP), que regulamenta o tratamento de dados pessoais no Brasil, tanto pelo poder público quanto pela iniciativa privada.

O estudo e discussão das questões de "Privacidade de Dados no Brasil", já ocorre há mais de 8 (oito) anos, mas a sociedade brasileira através de entidades como a Brasscom (Associação Brasileira das Empresas de Tecnologia da Informação e Comunicação), a OAB-SP, a FIESP, entre diversas outras representantes da sociedade civil e institutos de defesa do consumidor, fomentaram a urgência de aprovação do PLC 53/2018, para permitir ao país a adequação e competitividade no cenário de inovação tecnológica, com respeito a direitos, em alinhamento a recente atualização da regulamentação europeia GDPR.

Considerando que o Senado aprovou a PLC, agora o projeto de Lei segue para apreciação e aprovação do Presidente da República, podendo ***URGENTE*** levar o Brasil ao rol dos diversos países do mundo que já possuem legislação sobre Privacidade de Dados.

Segundo a Agência Senado "*A proposta disciplina a forma como as informações são coletadas e tratadas, especialmente em meios digitais, como dados pessoais de cadastro – incluindo nome, endereço, e-mail, idade, estado civil, entre outros – ou até mesmo textos e fotos publicadas em redes sociais.*

Assim, os cidadãos terão um maior controle sobre suas informações pessoais, uma vez que o texto exige o consentimento explícito do usuário para que seus dados sejam coletados e usados, e obriga que sejam oferecidas opções para o cidadão visualizar, corrigir e excluir esses dados.

Essa autorização deve ser solicitada de forma clara, em cláusula específica, e não de maneira genérica. Caso uma empresa colete um dado para um determinado fim e mude essa finalidade, deve obter um novo consentimento. A permissão dada pelo usuário, contudo, deve ser revogada se o titular assim desejar."

"Mais de 100 países já colocaram de pé leis e diretrizes de proteção de dados no ambiente da internet. A internet não pode ser ambiente sem regras. A privacidade é um valor civilizatório"

Senador "Ricardo Ferraço" (PSDB-ES)

Lei Geral de Proteção de Dados – LGPD Brasil

O "Portal da Privacidade"* publicado na internet pelo escritório do amigo "RENATO MULLER DA SILVA OPICE BLUM", divulga o "Infográfico: Conheça os 12 principais pontos sobre a LGPD", acrescentado abaixo, sendo muito esclarecedor sobre as propostas do PLC 53/2018.

Com a aprovação do senado a nova lei, segue para a sanção do Presidente Temer, e cria um marco legal para proteção, tratamento e uso de informações pessoais no país.

O "Vacatio Legis" ou prazo de regulamentação e entrada em vigor da Lei é de um ano e meio após aprovada, com multas para o descumprimento que pode chegar a R$ 50.000.000,00 (cinquenta milhões de reais).

Disponível em < http://portaldaprivacidade.com.br/2018/07/10/infografico-conheca-os-12-principais-pontos-sobre-lgpd/ > *< http://portaldaprivacidade.com.br/ > na próxima página - Agência Senado - < https://www12.senado.leg.br/noticias/materias/2018/07/03/regras-para-protecao-de-dados-pessoais-sao-aprovadas-e-vao-a-plenario > acessos em 11/07/2018.

Entenda o marco legal de proteção de dados (Agência Senado)	
Estrutura	* O PLC 53/2018 tem 65 artigos, distribuídos em 10 Capítulos. O texto foi inspirado fortemente em linhas específicas da regulação europeia que entrou em vigor no dia 25 de maio deste ano, o Regulamento Geral de Proteção de Dados (GDPR, em sua sigla em inglês)
Hipóteses para o tratamento de dados	* Com o consentimento do titular; * Para o cumprimento de obrigação legal ou regulatória pelo responsável pelo tratamento; * Pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas; * Para a realização de estudos por órgão de pesquisa, sem a individualização da pessoa; * Para a proteção da vida ou da incolumidade física do titular ou de terceiro; * Para a tutela da saúde, com procedimento realizado por profissionais da área da saúde ou por entidades sanitárias; * Para a execução de um contrato ou de procedimentos preliminares relacionados a um contrato do qual é parte o titular quando a seu pedido; * Para pleitos em processos judicial, administrativo ou arbitral; * Para a proteção do crédito, nos termos do Código de Defesa do Consumidor.
Abrangência	* Quaisquer dados, como nome, endereço, e-mail, idade, estado civil e situação patrimonial, obtido em qualquer tipo de suporte (papel, eletrônico, informático, som e imagem, etc).
Contratos de adesão	* Nos casos de contratos de adesão, quando o tratamento de dados pessoais for condição para o fornecimento de produto ou de serviço, o titular deverá ser informado com destaque sobre isso.
Dados sensíveis	* O texto traz o conceito de dados sensíveis, que recebem tratamento diferenciado: sobre origem racial ou étnica; convicções religiosas; opiniões políticas; filiação a sindicatos ou a organizações de caráter religioso, filosófico ou político; dados referentes à saúde ou à vida sexual; e dados genéticos ou biométricos quando vinculados a uma pessoa natural.
Vacatio legis	* As novas regras só passarão a viger depois de um ano e meio da publicação da lei para que órgãos, empresas e entidades se adaptem.
Autoridade Nacional de Proteção de Dados (ANPD)	* O projeto prevê a criação de uma autarquia especial vinculada ao Ministério da Justiça com a missão de zelar pela proteção dos dados, fiscalizar e aplicar sanções, entre outras atribuições.
Sanções administrativas	* Quem infringir a nova lei fica sujeito a advertência, multa simples, multa diária, suspensão parcial ou total de funcionamento, além de outras sanções.
Responsabilidade civil	* O responsável que, em razão do exercício de atividade de tratamento de dados, causar a dano patrimonial, moral, individual ou coletivo, é obrigado a reparar. O juiz, no processo civil, poderá inverter o ônus da prova a favor do titular dos dados quando, a seu juízo, for verossímil a alegação, houver hipossuficiência para fins de produção de prova ou quando a produção de prova pelo titular resultar-lhe excessivamente onerosa

- **Da necessidade à ação efetiva para a Conformidade**

É muito provável que os executivos de pequenas e medias organizações, já tenham identificado a necessidade de conduzir suas empresas na adoção de novos processos operacionais que as tornem, mas eficaz, mais competitivas e lucrativas, no entanto, existe a percepção de que permanecem entraves legais e operacionais, no âmbito trabalhista, tributário (impostos e taxas), fiscal (Sped Fiscal (EFD, ECD, EFD-Contribuições, ECF e eventos EFD-Reinf.), Dime, GIAM, etc), entre outros, que as colocariam em risco. Esse receio tem impedido que muitas organizações evoluam e cresçam como seria possível, no mercado altamente competitivo em que vivemos.

Hoje observamos muitos empresários atentos e focados exclusivamente na operação do negócio ou no "Core business", deixando em segundo plano a retaguarda necessária da empresa o "Back office", que intrinsicamente sustenta o próprio negócio. A consequência do fato pode não ser percebida claramente em curto prazo, mas inevitavelmente conduz a empresa enfrentar ao longo do tempo, situações arriscadas e desagradáveis, comprometendo inclusive a própria subsistência da organização.

Um dos objetivos desta publicação é incentivar a reflexão da necessidade de se repensar os processos de "Back office" através dos quais, recomendasse URGENTE implementação dos processos de COMPLIANCE, que possam proporcionar as empresas o incremento da eficiência, da eficácia e da efetividade do "Core business", no alcance da maior competitividade, diferenciação estratégica no mercado e consequentemente, na obtenção de maiores lucros.

Entendemos ser fundamental investir ***URGENTE*** na implementação de COMPLIANCE na organização, mesmo que pareça que hoje não é o momento oportuno.

"É oportuno fazer-se temeroso enquanto o perigo estiver distante, mas, ao vê-lo aproximar-se, é preciso combatê-lo sem medo."

Veda Vyasa – do "Mahabharata" – cultura hinduístas.

Após implementar:
Certificações e Validações da Conformidade de Processos Anticorrupção

As organizações no mundo todo estão adotando ações estruturadas para o combate a corrupção e ao suborno, mas é importante lembrar que não existem padrões rígidos e uniformes ou determinados por Normas de larga aceitação internacional. Da mesma forma, as questões de conformidade regulatória ou COMPLIANCE, variam em requerimentos para cada perfil empresarial (tipo de organização e mercado) inclusive, quanto ao país de origem ou onde atua a empresa.

No Brasil as empresas podem ser "certificadas" por organizações credenciadas pelo INMETRO, quanto a adoção de algumas Normas Internacionais, no caso em especial da Norma ABNT NBR ISO 37.001:2017 que estabelece um Sistema de Gestão Antisuborno. As certificações são exigentes e onerosas, sendo indicadas para empresas que possuem relacionamentos internacionais.

No contexto nacional cresce a adoção voluntária de melhores práticas de integridade, por empresas de todos os portes e ramos de atuação, podendo seus processos operacionais voltados para a prevenção Anticorrupção, Antisuborno e Antifraudes serem aceitos e validados por inciativa governamental, como é o caso do programa "Empresa Pró-Ética1" do MT/CGU.

Diversas organizações privadas também estão ofertando métodos cíclicos de Validação de Processos, atestando, como terceira parte, que a organização avaliada segue regularmente os padrões estabelecidos de conformidade, obviamente com custos menores que as certificações.

[1]Informações disponível em <http://www.cgu.gov.br/assuntos/etica-e-integridade/empresa-pro-etica > acesso 30/05/2018.

Benefícios do Programa de Integridade

Em uma análise preliminar, implementar um sistema de Compliance para apoio concreto à um "Programa de Integridade Empresarial" pode apenas significar aos leigos, que se atribui a organização um "selo" de boas práticas, capaz de conferir a ela uma imagem de conformidade e ética, na condução responsável dos negócios e na monitoração do comportamento moral de seus funcionários.

Visto por outro ângulo, se uma empresa dispuser de um "sistema de Compliance" e tenha implementado um Programa de Integridade", portanto, estando em conformidade com leis e regulamentos internos e externos, investindo esforços através de controles adequados, para prevenir, detectar e responder a possíveis problemas de desvios, bem como, tendo adotado boas práticas e padrões de mercado, isto é, preservando a sua reputação, a empresa se fortalece e recebe naturalmente o devido reconhecimento do público, como ética e integra.

Programas de Integridade Empresarial, garantem a vantagem competitiva das empresas, e elas recebem seguramente outros benefícios diretos como: facilidades em obter financiamentos e descontos especiais em linhas de crédito; maior valorização mercadológica do negócio; redução de erros; redução de perdas; ganhos de desempenho; melhor retorno dos investimentos, entre muitos outros ganhos.

Observando a realidade dos negócios, cada vez mais será exigido o "selo" do Compliance / Integridade para que as empresas tenham acesso a mercados de exportação, na interação com autoridades nacionais e estrangeiras, que já exigem tais controles das organizações.

E, por fim, a administração pública nacional, vem exigindo em seus editais, por força das Leis, a comprovação da implementação dos "Programas de Integridade", dos quais Compliance é parte essencial, para que as empresas se qualifiquem em Licitações. Da mesma forma, há uma tendência de que as contratações privadas entre empresas, passarão exigir eticamente a comprovação de que o fornecedor ou parceiro possua práticas de Compliance / Integridade. Compliance já é requerimento necessário e é essencial para garantir a perenidade das empresas.

"Compliance is a great deal for all.."

"A conformidade é um ótimo negócio para todos."

ROI-PI (fundamentação)
Retorno do Investimentos em Programas de Integridade

O estudo sobre o "Retorno do Investimento-ROI" em implementação de "Programas de Integridade - PI" se baseia em experiências empíricas na observação metódica dos resultados obtidos em milhares de empresas pelo mundo, nos últimos 20 anos. Com fundamentação a partir da prática em projetos, da observação sistemática comprovada, (fonte: *Jacqueline Leoni – KPMG - 2018*)se afirma que para cada US$ 1.00 investido em PI se obtém em prazo de um ano um retorno de US$ 5.00 diretamente contabilizado.

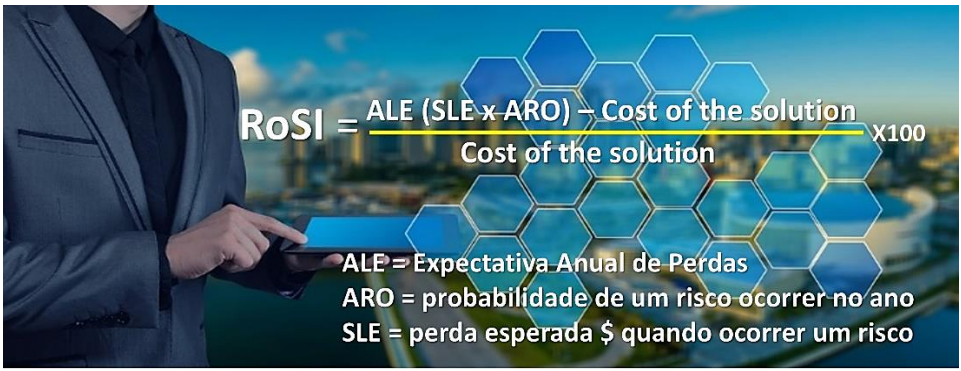
Essa afirmação da relação de ganho de US$ 5 para cada US$1 investido é polemica e pode ser questionada, no entanto, o estudo sobre o ROI-PI considerando diversas variáveis organizacionais, inclusive do porte, ramo de atividade e mercado em que as empresas atuam, nos mostram efetivamente que as variações não são tão impactantes, mostrando a plausibilidade da conclusão da relação 5/1.

Para a devida compreensão vamos rever o conceito básico do indicador ROI (Return On Investiments – taxa percentual) que é apenas uma equação simples que quantifica o retorno financeiro produzido pelas decisões assertivas ou não de investimento, de forma a mensurar os resultados econômico de um empreendimento. O indicador ROI pode ser usado nas avaliações de um simples projeto na validação do seu custo-benefício, bem como, para a avaliação do desempenho de resultados de uma empresa em relação aos concorrentes ou ao mercado.

O ROI é obtido pela razão entre o lucro líquido ou ganho alcançado ou projetado e o valor investimento efetuado ou previsto, dentro de um período de tempo.

Estimar os ganhos obtidos através do investimento em Projetos de construção de Programas de Integridade, exige a capacidade de enxergar além das fronteiras convencionais, para poder mensurar ganhos de produtividade / desempenho, ganhos na redução de perdas, ganhos com a melhora da qualidade e da imagem empresarial, entre outros. De maneira análoga o **ROI-PI** ou seja, o Retorno do Investimentos em Programas de Integridade, pode ser comparado ao **ROSI**[1] (**R**eturn **o**n **S**ecurity **I**nvestment) pois o seu cálculo é influenciado por variáveis internas (endógenas) dependendo do sucesso ou qualidade das soluções técnicas de segurança adotadas, no entanto, estas varáveis também são influenciadas por outras externas (exógenas) ocasionadas por circunstâncias diversas, mas que impactam os resultados e o equilíbrio das variáveis endógenas.

Tipicamente o ROSI se calcula pela seguinte equação, simples, mas eficaz:



O RoSI se fundamenta nas perdas financeiras prováveis, com problemas de segurança, que uma organização poderá ter ao logo do ano, mesmo que não se dê conta ou as perceba na prática.

A natureza específica dos incidentes de segurança física ou cibernética, implica na maior complexidade de identificação e apuração financeira dos prejuízos, pois, se deve levar em conta os impactos de todos os recursos em que os incidentes incidirão.

Vamos a seguir discorrer sobre uma breve visão do problema:

Por exemplo, um laptop furtado não só custará a substituição do equipamento em si, mas também implicará na perda de produtividade, no dano à reputação, no tempo de suporte e, possivelmente, impactará no custo da propriedade intelectual dos dados nele armazenados. Dessa forma, o custo total de um incidente deve incluir todas as perdas diretas (tempo de inatividade, substituição de hardware, substituição de perda de dados, etc.) e o custo de perdas indiretas (tempo de investigação, perda de reputação, impacto na imagem, etc.).

Quando se pensa no retorno do Investimento em Programas de Integridade, da mesma forma que no ROSI, temos de buscar entender todas as variáveis que podem produzir valor e as que podem produzir perdas. Mesmo que objetivamente o ROI seja um indicador de resultado, o mesmo conceito ajustado, pode ser utilizado para projeção de cenários, que podem estimular o alcance esperado. No caso do ROI-PI, entendendo que PI (Programa de Integridade) seja um projeto, como em qualquer outro, devemos estimar o "GEP" ou ganho Esperado com o projeto, considerando os ganhos objetivos - melhor desempenho operacional, redução de erros operacionais, entre outros, e os ganhos subjetivos – melhor clima organizacional, colaboração entre os empregados, Redução do Risco de Fraudes, etc.

A seguir apresentamos uma proposta de formula para o cálculo do ROI-PI, que costumamos aplicar:

É importante observar que o ROI-PI se fundamenta no investimento inteligente prévio e devidamente estabelecido, através de um planejamento para a implementação de ações de um Programa de Integridade, onde a projeção de ganhos é baseada no custo evitado em um incidente de não conformidade ou de fraude ocupacional, entre outros. Como um dos parâmetros de perdas, por fraudes ocupacionais que podem ser revertidas em ganhos por sua prevenção, sugerimos usar a informação atualizada anualmente pela ACFE[2], como segue:

[2]Disponível na pagina 24 do relatório < https://s3-us-west-2.amazonaws.com/acfepublic/2018-report-to-the-nations.pdf > acesso 20/07/2018.

A menor perda média observada pela pesquisa de 2018 da ACFE foi no setor de varejo, chegando ao valor de US$50,000 cuja representatividade em R$ é muito significativa. Essa informação pode ser utilizada para ajudar a calcular o RoSI do projeto PI.

Nosso objetivo aqui não é ensinar a calcular o ROI-PI, mas mostrar que é possível prever e justificar, com fundamentação técnica, resultados positivos do retorno de investimentos em projetos de PI.

Acreditamos que um "Programa de Integridade Empresarial" devidamente implementado, possa reduzir em 99,9% a probabilidade das perdas operacionais, das perdas por fraudes ocupacionais, das perdas por acidentes cibernéticos, bem como, com as multas por não conformidade, entre outras perdas de alto impacto que podem afetar as organizações.

Fundamentação do RoSI

Existem diversas referências na Internet, mas optamos por indicar as mais significativas:

[1]Disponível em:

a)<https://www.enisa.europa.eu/publications/introduction-to-return-on-security-investment/at_download/fullReport>
b)<https://www.enisa.europa.eu/act/rm/files/EoS%20Final%20report>

c)<http://infosecwriters.com/text_resources/pdf/ROSI-Practical_Model.pdf>

acessos 20/07/2018.

Considerações Finais

COMPLIANCE URGENTE é uma publicação da série de temas ◤**UPGRADE**◥ que se propõe a divulgar a opinião e conhecimentos do autor e cocriadores, em diversos assuntos ligados ao "management" empresarial.

O tema COMPLIANCE que aqui se conclui, possui uma importância estratégica, sendo base para que se garanta que tudo que possa ser importante para a evolução e sobrevivência das organizações, venha a ser identificado, tratado e controlado.

Os riscos de corrupção e fraudes que foram enfaticamente citados nesta publicação indicam que o ser humano é o maior responsável por eles. No entanto, a grande massa humana também pode ser conduzida através de processos de conformidade, na superação das "Condutas Indecisas", de forma que busquem não cometer nenhum desvio moral.

Buscou-se também indicar a URGENTE necessidade de implementar COMPLIANCE nas organizações, para que estas alcancem melhores RESULTADOS comprovando o ROI, e contribuam de forma decisiva para melhoria das sociedades onde atuam, para o país e para a humanidade.

Até breve!

Glossário - Termos Usuais

Os dados a seguir apresentados foram adaptados através da interpretação e tradução livre de entidades acadêmicas como a Universidade da Califórnia, a ONG Norte Americana "ECI"- The Ethics & Compliance Initiative, entre outras, onde se buscou respeitar os conceitos e efetuar a indicação das respectivas URLs (Links).

Este glossário foi integrado, contendo termos de mercado normalmente utilizados em diálogos ou textos publicados em diversas mídias de larga circulação e divulgação. Abrange aspectos sobre Ética, Compliance, Auditoria, Gestão de Riscos, Governança Corporativa, e assuntos correlatos. **Boa Leitura**.

- **Accountability** (GRC) - É um termo da língua inglesa que expressa a obrigação de executivos e membros de conselhos de administração em utilizar à "responsabilidade com ética" para alcançar à "transparência" requerida nos processos de Governança Corporativa. Os processos e indicadores de Accountability já começam a ser considerados e validados por controles de compliance.
- **Accountability** (GRPD) - Expressão técnica que exige que seja implementado um programa de conformidade capaz de monitorar a conformidade em toda a organização e demonstrar às autoridades de proteção de dados e aos titulares dos dados que toda essa informação pessoal está em segurança – termo aplicado em GRC e GDPR.
- **Amostra** - Compreende uma pequena seleção destinada a ser representativa do todo. Por exemplo, a pesquisa de opinião é frequentemente conduzida em uma porção da população selecionada aleatoriamente, em vez de um censo de todo o grupo. A seleção da amostra pode ser estratificada para permitir que o resultado seja representativo de subgrupos identificados, bem como da população como um todo.
- **Áreas Cinzentas** - Ocorrem em situações em que não é claro para um indivíduo como responder a um dilema ético. Às vezes, o indivíduo pode não estar familiarizado com uma diretriz, ou as diretrizes podem ser vagas e sujeitas a interpretação. As diretrizes geralmente são escritas para fornecer aos gerentes o máximo de latitude apropriada, e isso pode criar áreas cinzas ou de indecisão.

Glossário - Termos Usuais

- **Aspiracional** - Representa um forte desejo de alcançar algo alto ou grande. Implica em estabelecer um código de aspiração destinado a alcançar um padrão mais elevado de "fazer o que é certo", substituindo ou superando a mera conformidade com o que a lei determina.

- **Ações corretivas em controles** - Processo de organizar desvios causados pela ocorrência de condições ou eventos indesejáveis; ação capaz de reduz a probabilidade, impacto e velocidade contínuos de condições, eventos e efeitos indesejáveis adicionais em controles internos.

- **Ações de Detecção** - Ações para detectar a ocorrência real ou potencial de condições e eventos desejáveis e indesejáveis.

- **Ações de gestão** - São decisões administrativas tomadas por pessoas, com o uso de processos e de recursos associados que aumentam a probabilidade de que os objetivos sejam alcançados.

- **Ações proativas de controles** - São ações deliberadas pelos gestores que proativamente promovem incentivos desejáveis aos colaboradores; objetiva "evitar" condições ou eventos indesejáveis.

- **Ações Responsivas de Controles** - São ações promovidas por gestores ofertando recompensas desejáveis aos colaboradores; objetiva "corrigir" condições ou eventos indesejáveis.

- **Alvo** - É um valor mensurável que uma entidade se esforça para alcançar.

- **Ameaça** - É um evento que tem, no balanço, um efeito indesejável no alcance dos objetivos.

- **Apetite ao Risco** - Corresponde ao nível de risco que a organização está disposta a aceitar (positivo ou negativo) para atingir os objetivos.

Glossário - Termos Usuais

- **Armazenamento Seguro -** Os dados pessoais ou empresariais devem ser inseridos e armazenados de forma segura nos sistemas, utilizados para seu processamento e de acordo com as permissões de acesso necessárias para os objetivos para os quais foram coletados. O gerenciamento de informações, dados pessoais, propósito de processamento de dados, remoção de dados e anonimização e consentimento devem ser controlados.
- **Atestado -** Compreende o reconhecimento de terceira parte, com a compreensão sobre o cumprimento de políticas, procedimentos e treinamentos, estabelecidos na empresa validada, para um ou mais objetivos.
- **Ato HITECH -** A Lei de Tecnologia da Informação em Saúde para a Saúde Econômica e Clínica (Lei HITECH) é a legislação criada para incentivar a adoção de registros eletrônicos de saúde (EHR) nos Estados Unidos. A HITECH faz parte da Lei Americana de Recuperação e Reinvestimento de 2009 (ARRA).
- **Avaliar -** Compreende realizar processos formais para identificar a situação de uma organização ou processo operacional, verificar as ameaças, as oportunidades e ou requisitos; compreender o nível de risco, recompensa e conformidade; e alinhar uma abordagem para alcançar objetivos com segurança, considerando a incerteza e compromissos com a integridade.
- **Avaliação de Risco -** A avaliação de risco é o processo de identificação de variáveis que têm o potencial de impactar negativamente a capacidade de uma organização de conduzir negócios.
- **Auditoria Externa -** Compreende um exame realizado por um terceiro independente que verifica as diretrizes descritas por um órgão regulador, seja interno ou externo a organização
- **Auditoria Interna -** Compreende um exame realizado por um colaborador dedicado, que verifica as diretrizes descritas por um órgão regulador, seja interno ou externo a organização.

Glossário - Termos Usuais

- **Auditoria de Conformidade -** Uma auditoria de conformidade é uma revisão abrangente da adesão de uma organização às diretrizes regulamentares (interna e externas). Consultores independentes de Contabilidade, Segurança e ou TI avaliam a força e o rigor da preparação para conformidade. Auditores revisam Políticas de segurança, controles de acesso de usuários e procedimentos de gerenciamento de riscos ao longo de uma auditoria de conformidade.
- **Auditoria de TI -** Uma auditoria de TI é uma avaliação da tecnologia da informação e das políticas de TI de uma organização. A auditoria revisará todos os aspectos da tecnologia da informação, incluindo hardware, software de sistema operacional, software de aplicativo, armazenamento, backup, preparação para recuperação de desastre e segurança.
- **Benchmarking -** O processo de comparação com as "melhores práticas" estabelecidas, organizações de pares ou mesmo resultados anteriores, a fim de entender melhor os pontos fortes, os desafios e o progresso alcançado.
- **BIA** – Business Impact Analysis – ou análise de impacto nos negócios usada em avaliações de riscos, indicando impactos, quantitativos financeiramente e qualitativos estrategicamente. É base para decisões, considerando o MTPOD (Most Tolerable Period of Disruption) e o RTO (Recovery Time Objective) em processos de Continuidade Operacional de Negócios.
- **Blockchain -** Um blockchain é um registro público digitalizado, descentralizado, de todas as transações que envolvem criptomoedas e outros processos seguros. Crescendo como blocos concluídos, as transações mais recentes são registradas e adicionadas à cadeia em ordem cronológica, permitindo que os participantes do mercado acompanhem as transações sem manutenção central de registros. Cada nó (um computador conectado à rede) obtém uma cópia do "blockchain" que é baixado automaticamente. Originalmente desenvolvido como método contábil, foi aplicado na segurança das moedas virtuais como o Bitcoin. Blockchains usam o que hoje é conhecido como tecnologia de contabilidade distribuída (DLT). Essa tecnologia cria registros indeléveis que não podem ser alterados, pois a autenticidade pode ser verificada por toda a comunidade usando o "blockchain" em vez de uma única autoridade centralizada.

Glossário - Termos Usuais

- **Boa fé -** Impressão que uma pessoa transmite a outras, com base na crença na exatidão da informação ou preocupação relatada.
- **Canais Éticos -** Correspondem aos meios tecnológicos de comunicação (telefone-internet), próprios ou terceirizados, que se destinam em apurar e investigar fatos relacionados à condutas inadequadas ou a eventuais irregularidades na condução dos negócios e/ou das atividades sociais, em nível empresarial e ou profissional. Os meios disponibilizados permitem que se façam reclamações referentes ao cometimento de infrações, descumprimento de normas internas ou públicas, acusações de natureza criminal, denúncias de corrupção ou fraudes, facilitação de irregularidades, exigência indevida de vantagens ou comunicação de quaisquer situações suspeitas, nas empresas.
- **Capacidade de Risco -** Compreende o nível máximo de risco que a organização é capaz de resolver (mitigar/controlar) ou assumir.
- **Capacitação -** Compreende o desenvolvimento das principais habilidades e capacidades de uma organização, como liderança, gestão, finanças e captação de recursos, programas e avaliação, a fim de construir a eficácia e a sustentabilidade da organização. Compreende a transmissão de conhecimentos não existentes anteriormente. É o processo de ajudar um indivíduo ou grupo a identificar e abordar questões e obter informações, conhecimento e experiência necessários para resolver problemas e implementar mudanças. A capacitação é facilitada por meio do fornecimento de atividades de apoio técnico, incluindo Transferência de Conhecimentos inexistentes, treinamento cíclico e de aperfeiçoamento sobre conhecimentos existentes, assistência técnica específica e rede de recursos adicionais.
- **Capacidade de GRC -** Corresponde a "intensidade" dos processos e recursos que permitem que uma organização alcance seus objetivos com segurança, abordando as incertezas e agindo com integridade; incluindo a governança, a garantia e gerenciamento de desempenho, o controle dos riscos e a validação da conformidade. Existem organizações com baixa, média e alta capacidade de GRC.

Glossário - Termos Usuais

- **Carga de conformidade -** A carga de conformidade, também chamada de carga regulatória, é o custo administrativo de um regulamento em termos de dólares ou Reais, também compreende o tempo e complexidade para implementação.

- **Cibersegurança -** A segurança cibernética é o conjunto de tecnologias, processos e práticas projetados para proteger redes ligadas a Internet, seus computadores, programas e dados contra ataques, danos ou acessos não autorizados.

- **Código de Conduta ou Código de Ética -** Em linhas gerais podem ser vistos como um guia central e referência para auxiliar na tomada de decisões do dia-a-dia. Destinam-se a esclarecer a missão de uma organização, valores e princípios, ligando-os com padrões de conduta profissional. Como referência, pode ser usado para esclarecer padrões, valores e políticas organizacionais; promover a tomada efetiva de decisões; e direcionar os usuários para identificar recursos relevantes relacionados à ética dentro da organização.

- **Código de Conduta -** Refere-se a uma lista de comportamentos exigidos, cuja violação resultaria em ação disciplinar. Na prática, usado de forma intercambiável com o Código de Ética.

- **Código de Ética -** Muitas vezes transmite valores organizacionais, um compromisso com padrões e comunica um conjunto de ideais. Na prática, usado de forma intercambiável com o Código de Conduta. Na Seção 406 (c), a Lei Sarbanes-Oxley define "código de ética" como padrões razoavelmente necessários para promover: (1) conduta ética e honesta, incluindo o tratamento ético de conflitos de interesse reais ou aparentes entre e relações profissionais; (2) divulgação completa, justa, precisa, oportuna e compreensível nos relatórios periódicos que devem ser arquivados pelo emissor; e (3) em conformidade com as regras e regulamentos governamentais aplicáveis.

Glossário - Termos Usuais

- **Código de Conduta Centrado nas Regras -** Frequentemente assume a forma de uma lista de requisitos comportamentais, cuja violação pode resultar em ação disciplinar. Normalmente possui estrutura que permite pontuar o seu cumprimento e gerenciar os desvios dos colaboradores. Especifica claramente as penalidades do não atendimento.

- **Coleta legal -** De acordo com o GDPR, os dados pessoais devem ser coletados somente para fins específicos, definidos e apenas armazenados durante o tempo necessário para tais fins. As funcionalidades dos sistemas informatizados devem facilitar isso, permitindo que cada assunto relacionado aos dados seja identificado e tenha um ou mais objetivos definidos para processamento de informações pessoais, incluindo durações, onde cada um pode ser associado a uma ou mais bases legais para o processamento.

- **Compliance -** O termo compliance (do inglês to comply) significa "agir de acordo com regras ou instruções". Na área jurídica, por exemplo, é comum falar em "estar em compliance" com as regras de governança corporativa da empresa ou exigências da SOX, entre outros regulamentos.

- **Comunicação -** Meios de fornecer informações relevantes, confiáveis e oportunas para as audiências corretas, conforme exigido pelos mandatos ou conforme necessário para desempenhar responsabilidades e moldar atitudes de maneira eficaz.

- **Competência -** É a combinação de conhecimentos, habilidades e comportamentos que permite que um indivíduo faça seu trabalho. É o estado de ser capaz de provar o cumprimento de um requisito estabelecido.

Glossário - Termos Usuais

- **Conciliação de Depósitos Judiciais -** A Conciliação de Depósitos Judiciais consiste em realizar a vinculação e conferência dos valores depositados nas contas judiciais determinadas para os processos e seus valores de condenação. Com esse controle é possível recuperar valores que, muitas vezes, não são utilizados na sua totalidade. Para isso, é necessário associar a conta e o valor depositado com o código processual de cada ação, conciliando o extrato bancário com os valores de depósito registrados na empresa.
- **Conflito de Compromisso -** Corresponde a uma situação na qual os interesses externos de um colaborador interferem em seus deveres para com a organização.
- **Conflito de Interesses -** Ocorre quando uma pessoa está em uma posição de confiança que exige que ela exerça julgamento em nome de outras pessoas (pessoas, instituições etc.) e também tem interesses ou obrigações do tipo que podem interferir o exercício de seu julgamento, no caso a pessoa é obrigada a evitar ou reconhecer abertamente esse conflito.
- **Conflito de Tempo -** Uma situação em que um funcionário / colaborador não dedica a quantidade de tempo ao seu trabalho conforme exigido pelas obrigações do se contrato empregatício.
- **Conformidade -** Significa a capacidade de consonância ou adaptação das ações de uma pessoa aos desejos de outra pessoa, a uma regra ou a uma necessidade explicita governamental ou legal. Um código de conformidade seria destinado aos colaboradores orientando-os em atender a todos os requisitos de uma Política Interna ou normas legais, as quais a organização se subordina.
- **Conformidade com PCI** (conformidade com o setor de cartões de pagamento) **-** A conformidade com a indústria de cartões de pagamento (PCI) é um conjunto de diretrizes estabelecidas pelas principais operadoras de cartão de crédito. Todas as empresas que aceitam cartões de crédito, armazenam ou transmitem dados de cartão de crédito devem seguir as diretrizes para evitar o roubo de dados, ou adulteração em transações com cartões de crédito ou similares.

Glossário - Termos Usuais

- **Congruência Ética -** Corresponde a uma situação em que a decisão de uma pessoa é consistente com o (s) conjunto (s) aplicável (is) de valores. Nestas circunstâncias, a escolha de tomar alguma ação será harmonizada com os valores do decisor. Compreende o estado organizacional em que valores, comportamentos e percepções estão alinhados aos melhores padrões éticos.
- **Consentimento do titular dos dados pessoais -** Corresponde formalmente a qualquer manifestação de vontade, livre, específica, informada e explícita, nos termos da qual os titulares dos dados aceitam, mediante declaração ou ato positivo inequívoco, que os seus dados pessoais sejam objeto de tratamento.
- **Contencioso de Massa -** O grande desafio dos departamentos jurídicos, o Contencioso de Massa acontece quando há ou pode haver contestação ou discussão em grande volume. Administrar uma carteira volumosa de processos de forma eficiente, para garantir à empresa êxito quanto às condenações e fortalecimento da marca, se torna fundamental para o sucesso do departamento jurídico. Empresas de prestação de serviços, como as de telefonia, por exemplo, costumam lidar com um Contencioso de Massa bastante expressivo.
- **Controle interno -** Um controle interno é uma prática de negócio, política ou procedimento que é estabelecido dentro de uma organização para criar valor ou minimizar riscos. Os controles internos buscam também aferir o desempenho e promover ajustes necessários na dinâmica das operações da organização.
- **Considerações Idealistas -** Compreende a manifestação sobre "Qual é a coisa certa a fazer - conforme definido pelos valores e princípios que se aplicam a essa situação - sendo considerada prática usual na sociedade onde se vive?"
- **Considerações Individualistas -** Compreende a manifestação sobre "O que acontecerá comigo como consequência dessa ação ou decisão?"
- **Considerações Pragmáticas -** Compreende a manifestação sobre "Quais são as consequências comerciais dessa ação ou decisão? "

Glossário - Termos Usuais

- **Coragem -** Corresponde escolher fazer o que se acredita está certo, mesmo que o resultado não seja do agrado de todos ou possa levar a perdas pessoal.
- **Corrupção -** Compreende o abuso do "poder" para benefício privado ou público. Corresponde a perversão ou destruição de integridade pessoal no cumprimento de obrigações públicas/privadas por suborno ou favor ou o uso ou a existência de práticas corruptas, especialmente em uma empresa estatal ou pública, no relacionamento com o mercado privado. A corrupção também pode ser pessoal, através de desvios morais nas práticas cotidianas.
- **Credo -** São as crenças fundamentais (ou um conjunto de crenças) ou princípios orientadores que uma pessoa adota ou se submete.
- **Critério -** São "Padrões" em relação aos quais a avaliação ou as decisões podem ser baseadas.
- **Critérios de Análise de Risco -** São valores quantitativos ou qualitativos metodológicos em relação aos quais o "nível" de risco é avaliado.
- **Cultura de Conformidade -** Significa os preceitos assumidos e Inclui os valores, crenças e comportamentos sobre governança, garantia e gerenciamento de conformidade, incluindo: identificação de requisitos de conformidade. Opiniões sobre o impacto da conformidade na conduta e nas decisões; e modelagem de comportamento adequado e compatível.
- **Cultura da Ética -** Significa a adoção de medida para que os funcionários, em todos os níveis, estejam comprometidos em fazer o que é certo e manter com sucesso valores e padrões. A cultura de ética inclui liderança ética (tom no topo); reforço do supervisor do comportamento ético; e o comprometimento dos colegas para apoiar uns aos outros em fazer o que é certo.
- **Cultura de Performance -** Abrange os valores, crenças e comportamentos sobre a governança, a garantia e gerenciamento de desempenho, incluindo: definição de objetivos e indicadores de desempenho; habilitar e avaliar o desempenho; e como o desempenho individual e da equipe é reconhecido e recompensado.

Glossário - Termos Usuais

- **Cultura de Risco -** Envolve os valores, crenças e comportamentos sobre a governança, garantia e gerenciamento de risco, incluindo: definição de apetite e tolerância ao risco; visões sobre o impacto do risco na conduta e nas decisões; e modelagem de comportamento de risco apropriado.
- **Custas Judiciais -** Compreendem as taxas cobradas pela Justiça para determinados procedimentos, como citação dos réus, alocação de peritos e outras diligências, são chamadas de Custas Judiciais. Elas representam o preço da prestação do serviço público de Justiça nos tribunais.
- **Dados Pessoais -** Corresponde a qualquer informação, de qualquer natureza e independentemente do respectivo suporte, incluindo som e imagem, relativa a uma pessoa singular identificada ou identificável ("titular dos dados"); é considerada identificável a pessoa que possa ser identificada direta ou indiretamente, designadamente por referência a um identificador como o nome, número de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, mental, econômica, cultural ou social.
- **Dados Qualitativos -** Correspondem aos dados que são descritivos e não numéricos. Eles podem ser coletados de várias maneiras: grupos focais, entrevistas e perguntas de pesquisa abertas. Os dados qualitativos são geralmente mais subjetivos que os dados quantitativos.
- **Dados Quantitativos -** São essencialmente numéricos e, como tal, se prestam mais facilmente a comparações. Dados quantitativos são frequentemente coletados por meio de pesquisa de pesquisa.
- **Denunciante** (Whistleblower) **-** Compreende uma pessoa ou entidade que faz uma divulgação ou delação protegida. O delator (pessoa física ou jurídica) é comumente referido como "denunciante". Os denunciantes podem ser funcionários, candidatos a emprego, estudantes, pacientes, fornecedores, contratados, terceiros e ou o público em geral. O papel do denunciante é como um relator de fatos observados ou interpretados, portanto, não pode sofrer nenhum tipo de impedimento ou constrangimento, devendo ser garantido o seu anonimato. Eles não são investigadores ou descobridores de fatos, nem determinam as ações investigativas, corretivas ou protetivas apropriadas que poderão ser realizadas com base em sua denúncia.

Glossário - Termos Usuais

- **Depósito Judicial -** Corresponde em depositar um valor em juízo, isso significa que o dinheiro é colocado em uma conta bancária vinculada a um processo judicial. Essa conta só pode ser movimentada com ordem judicial.
- **Desempenho Planejado -** Corresponde ao nível de recompensa ou ganhos que a organização espera obter uma vez que as ações planejadas e os controles estejam operando corretamente de forma interativa.
- **Desempenho com Princípios -** Corresponde ao ato de alcançar objetivos de maneira confiável, abordando a incerteza e agindo com integridade. O desempenho pode ser pessoal ou empresarial.
- **Destinatário -** É a pessoa singular ou coletiva, a autoridade pública, a agência ou qualquer outro organismo a quem sejam comunicados dados pessoais ou empresariais, independentemente de se tratar ou não de um terceiro.
- **Detectar -** Corresponde avaliar e identificar continuamente o progresso das ações operacionais em direção a objetivos, bem como condições e eventos indesejáveis reais e potenciais, usando ações e controles de gerenciamento.
- **Diferenças Éticas -** São situações em que duas pessoas concordam com um determinado valor e discordam quanto à ação a ser tomada ou a decisão a ser tomada por questões de princípios morais ou éticos.
- **Dilemas Éticos -** São situações que exigem um julgamento ético. Muitas vezes, há mais de uma resposta certa e nenhuma solução ganha-ganha na qual se possa obter tudo o que se quer. Há uma clara dificuldade da pessoa ou organização identificar o que é certo e o que é errado.
- **Diretor de Privacidade -** É um executivo chefe de privacidade (CPO). É um executivo corporativo encarregado de desenvolver e implementar políticas projetadas para proteger dados de funcionários e clientes contra acessos não autorizados.
- **DPIA** – (GDPR) – "Data protection impact assessments" ou avaliações de impacto de proteção de dados, para riscos de privacidade.

Glossário - Termos Usuais

- **DPO -** (DATA PROTECTION OFFICER - GDPR) – E um profissional de proteção de dados pessoais e seu papel é de liderança e execução dos processos exigidos pela regulamentação GDPR.
- **Diretor de Riscos -** O diretor de risco (CRO) é o executivo corporativo encarregado de avaliar e mitigar ameaças competitivas, regulatórias e tecnológicas significativas ao capital e lucros de uma empresa. A posição é às vezes chamada de diretor de gerenciamento de risco ou simplesmente diretor de Riscos.
- **Efeito -** Corresponde a uma medida de resultado expressa em função da probabilidade de um evento ocorrer produzindo impacto negativo ou positivo.
- **Efeito negativo -** (ao lidar com um evento futuro ou passado)**-** É uma medida de resultado, expressa em função da probabilidade de um evento ocorrer; da rapidez com que o evento pode afetar os objetivos e do impacto negativo estimado que um evento pode ter sobre os objetivos.
- **Empatia -** Efeito de se preocupar com as consequências das escolhas de alguém ao afetarem os outros. Corresponde estar preocupado com o efeito que as decisões têm sobre aqueles que não têm voz na decisão em si.
- **Encarregado de Proteção de Dados (DPO – *Data Protection Officer*) -** Pessoa designada pela organização que estará envolvida em todas as questões relacionadas com a proteção de dados pessoais. Esta função deve ser atribuída sempre que o processamento for levado a cabo por uma entidade pública; se verifique a monitorização constante de indivíduos em larga escala; ou exista processamento de dados sensíveis em larga escala. As principais funções do encarregado de proteção de dados envolvem informar e aconselhar a empresa sobre a "conformidade da proteção de dados"; aconselhar sobre a avaliação do impacto da proteção de dados; monitorar a conformidade da proteção de dados, que inclui, por exemplo, formar a equipe e realizar auditorias relacionadas com essa área; e cooperar e atuar como ponto de contato com as autoridades de proteção de dados.

Glossário - Termos Usuais

- **Ética -** Corresponde ao estudo filosófico que é centrado no comportamento humano social. As reflexões sobre esse tema foram formuladas por filósofos famosos, como Aristóteles, Sócrates, entre outros. Pressupõe-se que o pensamento ético busca ponderar o comportamento humano, dizendo o que é certo e errado, justo e injusto, leal ou desleal, entre outros atributos.
- **Escala Nominal -** É uma escala na qual as informações são exibidas em categorias sem nenhuma ordem específica.
- **Escala Ordinal -** É uma escala na qual a informação é exibida em ordem de magnitude porque não há um padrão de medição de diferenças.
- **Estrutura de avaliação de Risco (RAF) -** Uma estrutura de avaliação de risco (RAF) é uma estratégia para priorizar e compartilhar informações sobre os riscos de segurança em uma infraestrutura de tecnologia da informação (TI).
- **Estrutura de Conformidade -** Uma estrutura de conformidade é um conjunto estruturado de diretrizes que detalha os processos de uma organização para manter a conformidade com os regulamentos, especificações ou legislação perfeitamente estabelecidos.
- **Exposição ao Risco -** A exposição ao risco é um potencial de perda quantificado nos negócios. A exposição ao risco é geralmente calculada multiplicando-se a probabilidade de um incidente ocorrer por suas perdas potenciais
- **Fake News -** como conceito pode abranger qualquer processo de comunicação espúria, desde uma informação falsa criminosa até um erro involuntário, ou voluntário como uma paródia, informações obtidas de fontes não fidedignas ou ainda fruto de uma má interpretação.
- **FCPA -** A Lei de Práticas de Corrupção no Exterior é uma lei federal Norte Americana, promulgada em 1977 para proibir as empresas de pagar propinas a autoridades governamentais estrangeiras e figuras políticas com a finalidade de obter negócios.
- **Financiamento de Risco -** Objetiva fornecer fundos para ações coordenadas em reduzir o impacto financeiro dos efeitos indesejáveis dos Riscos experimentados por uma organização.

Glossário - Termos Usuais

- **Fraude -** Corresponde Intencionalmente produzir ações de má-fé, com atos ardilosos como mentir, enganar ou trapacear para conseguir algo ao qual não se tem direito. Existem inúmeros tipos de fraudes envolvendo atividades empresariais. As fraudes direta ou indiretamente sempre são cometidas por pessoas.
- **Gerenciamento de Desempenho -** É o ato de gerenciar processos e recursos para buscar recompensa ao mesmo tempo em que aborda riscos. O gerenciamento pode ser pessoal ou empresarial.
- **Gerenciamento de Riscos -** É o ato de gerenciar processos e recursos para lidar com riscos enquanto busca identificar os impactos positivos e negativos.
- **Gestão -** O ato de dirigir, controlar e avaliar internamente uma empresa, organização, processos ou recursos.
- **Gestão de Informação -** O ato de dirigir, controlar e avaliar processos e recursos, de modo que as informações capturadas, tratadas e armazenadas, sejam relevantes, confiáveis, oportunas, seguras e disponíveis.
- **GRC (Governança, Riscos e Compliance) -** Corresponde a coleção integrada de "disciplinas" do conhecimento humano, e dos recursos que permitem que uma organização alcance objetivos de maneira confiável, abordando a incerteza e agindo com integridade. Abrange a governança, garantia e gerenciamento de desempenho, o gerenciamento de riscos e de conformidade regulatória.
- **Grupo Focal -** É um pequeno grupo de pessoas que se reuni para compartilhar suas opiniões e experiências, servindo, assim, como uma amostra representativa de uma população maior. As informações obtidas dos grupos focais não são analisadas estatisticamente, mas usadas para fins informativos e de projeção (isto é, para avaliar a cultura de uma organização).
- **Governança -** Compreende o ato, processos ou cadeia de poder em exercer autoridade, comando e controle em um ambiente organizacional, focado em coordenar pessoas que realizam as atividades designadas de gestão.

Glossário - Termos Usuais

- **Governança Corporativa -** Governança corporativa é um termo que se refere amplamente às regras, processos ou leis pelos quais os negócios são operados, regulados e controlados. O termo pode se referir a fatores internos definidos pelos diretores, acionistas ou constituição de uma corporação, bem como as forças externas, como as de grupos de consumidores, clientes e regulamentações governamentais e de mercado.

- **Governança de TI -** Governança de TI é um conjunto de práticas, padrões e relacionamentos estruturados, assumidos por executivos, gestores, técnicos e usuários de TI de uma organização, com a finalidade de garantir controles efetivos, ampliar os processos de segurança, minimizar os riscos, ampliar o desempenho, aperfeiçoar a aplicação de recursos, reduzir custos, suportar as melhores decisões e consequentemente alinhar estrategicamente TI aos negócios. (Prof. João Peres – 1998)

- **Honorários Advocatícios -** Corresponde a remuneração destinada aos advogados, que pelo seu trabalho que visam proteger um direito de uma das partes de um processo, violado ou ameaçado de violação.

- **Hotline-ethics -** É também o termo usado para o sistema comum de denúncias que dá acesso telefônico anônimo aos funcionários que desejam denunciar possíveis ocorrências de irregularidades.

- **Impacto -** Compreende uma medida quantitativa e qualitativa de como uma empresa ou seus objetivos são afetados positiva ou negativamente.

- **Impacto Qualitativo -** É um impacto frequentemente expresso usando uma escala ordinal ou escala nominal.

- **Impacto Quantitativo** - É um efeito positivo / negativo em ativos financeiros, ativos tangíveis, ativos intangíveis, continuidade de negócios e saúde e segurança.

Glossário - Termos Usuais

- **Implantação -** Compreende o ato ou efeito de fixar, enraizar, introduzir, estabelecer, elevar, etc, mas não significa necessariamente colocar em prática alguma coisa. Pode ficar só no âmbito das ideias introduzidas ou implantadas em uma organização.

- **Implementação -** Compreende ações objetivas de pôr em prática, executar ou assegurar a realização de alguma coisa.

- **Incerteza -** Corresponde ao estado de ser incapaz de prever completamente; determinar; ou definir algo.

- **Independência -** No uso mais geral, é a liberdade de agir sem controle ou influência dos outros, estar livre para tomar decisões e agir sem restrição externa. No mundo dos negócios, a independência passou a ter um significado especializado. É mais comumente entendida como "liberdade de interesses conflitantes" - o caso especializado de ter a capacidade de tomar uma decisão ou agir de maneira livre de conflitos entre os interesses pessoais e os interesses da parte em cujo nome se está tomando a decisão.

- **Indicador -** É uma métrica (padrão de medição) que pode ser usada para aferição e poder julgar a atividade, desempenho ou comportamento organizacional, pessoal, etc.

- **Indicadores Jurídicos -** Indicadores Jurídicos são ferramentas de gestão utilizadas para medir o desempenho da área. Com a competitividade do mercado e a cobrança por resultados, também o departamento jurídico, como outros, precisa estar envolvido nas estratégias estabelecidas pela empresa na busca de melhores resultados com menores custos, assim como no trabalho para prevenção de novos processos. O crescimento do volume de ações, o valor médio de honorários por processo e a redução entre previsto e realizado nos valores dos processos são exemplos de indicadores de performance de um departamento jurídico. O exemplo pode ser replicado para todos os departamentos ou atividades empresariais ou pessoais.

Glossário - Termos Usuais

- **Informações Pessoais Identificáveis (PII) -** É qualquer informação, como; nome, endereço, dados de documentos triviais (RG, CPF, CNH,...), data de nascimento ou outras informações que possam ser usadas sozinhas para identificar alguém.
- **Informações de Saúde Protegidas (PHI) -** PHI (Protected Health Information) é a combinação de informações sobre a saúde de uma pessoa com outras informações que possam identificar quem ela é. Exemplos de PHI incluem nomes de pacientes, números de telefone, números de previdência social e até fotos do pacientes e exames. Esse tipo de informação pode aparecer de diversas maneiras, incluindo contas médicas, e-mails, agendamento de consultas, resultados de diagnósticos médicos e correio de voz. É importante lembrar que o PHI inclui todas as informações que entram ou saem de uma entidade de saúde. O PHI não abrange apenas os registros eletrônicos, inclui informações verbais, escritas, visíveis nas telas dos computadores e até mesmo conversas que podem ser ouvidas por acaso.
- **Inquérito -** Compreende periodicamente buscar e investigar informações para entender percepções sobre a governança, garantia e gerenciamento de desempenho, risco e conformidade; bem como a ocorrência de eventos e atividades indesejáveis.
- **Integrar -** Organizar partes separadas (dados, sistemas, processos operacionais, controles, Políticas...) para fornecer um todo harmonioso coordenado.
- **Integridade (Integrity) -** Compreende a consistência de valores e ações que geram confiança nas partes interessadas (todos ligados a empresa). A Integridade é percebida quando os valores declarados e praticados operacionalmente estão em congruência.
- **Lei Dodd-Frank -** A Lei Dodd-Frank (totalmente conhecida como Reforma de Dodd-Frank Wall Street e Lei de Proteção ao Consumidor) é uma lei federal dos Estados Unidos que coloca a regulamentação do setor financeiro nas mãos do governo. A legislação, promulgada em julho de 2010, visa impedir outra crise financeira significativa, criando novos processos regulatórios financeiros que reforcem a transparência e a prestação de contas, ao mesmo tempo em que implementam regras para a proteção do consumidor.

Glossário - Termos Usuais

- **Lei Sarbanes-Oxley (SOX) -** A Lei Sarbanes-Oxley de 2002 (muitas vezes abreviada para SOX) é uma legislação aprovada pelo Congresso dos EUA para proteger os acionistas e o público em geral contra erros contábeis e práticas fraudulentas nas empresas, além de melhorar a precisão das divulgações corporativas. A Securities and Exchange Commission (SEC) dos EUA administra a lei, que estabelece prazos para o cumprimento e publica regras continuamente sobre os requisitos.

- **Limitação do Tratamento -** Requisito de inserção de um "marcador" nos dados pessoais conservados (armazenados na empresa) com o objetivo de identificar registros e limitar o seu tratamento ou divulgação inadequada no futuro.

- **Linha de Ajuda -** É um canal tipo HotLine ao vivo ou sob demanda para as pessoas fazerem perguntas antes ou enquanto estiverem participando de uma tarefa.

- **Maxim -** São instruções curtas e concisas que são usadas para instruir e guiar o comportamento humano.

- **Métrica -** É um padrão único de valor obtido por medição direta, ou calculado usando vários outros valores constituintes.

- **Minimização dos Dados (*Data Minimisation*) -** Significa que os dados pessoais recolhidos devem ser limitados ao que é necessário relativamente às finalidades para as quais serão tratados.

- **Minutas -** As minutas são como prévias de um documento, submetidas às partes para avaliação e aprovação antes de serem utilizadas oficialmente. É como se fosse um rascunho, que após aprovado por todos os interessados se torna oficial para selar o acordo ou divulgação.

- **Missão -** Texto que afirma o que a organização objetiva alcançar.

Glossário - Termos Usuais

- **NIST** (Instituto Nacional de Padrões e Tecnologia) - É uma unidade do Departamento de Comércio dos EUA que promove e mantém padrões de medição e comportamento tecnológico.
- **Notificação -** Processo formal que fornece múltiplos caminhos para relatar a ocorrência real ou potencial de condições, eventos e condutas indesejáveis; bem como a ocorrência de eventos desejáveis.
- **Objetivo -** É algo que uma empresa ou pessoa pretende atingir ou realizar.
- **Ombudsman -** É um profissional designado para resolução de disputas neutro ou imparcial cuja principal função é fornecer assistência confidencial e informal a gerentes e funcionários e / ou clientes do empregador: pacientes, estudantes, fornecedores ou clientes.
- **Oportunidade -** É um evento que tem, no balanço, um efeito desejável no alcance dos objetivos.
- **Oposição ao *PROFILING* -** Os titulares dos dados têm direito a opor-se ao uso de *profiling*, ou seja, qualquer forma automatizada de processamento de informação pessoal, com o objetivo de avaliar e tipificar indivíduos com base nos seus dados pessoais.
- **Orquestrar -** Compreende as formas e meios de governança, desempenho, risco, controle e capacidade de alcançar a conformidade.
- **Papéis GRC -** No organograma da empresa, dever incluir qualquer função (pessoa designada) que seja principalmente responsável pela governança, garantia ou gerenciamento de desempenho, risco e conformidade.
- **Pedidos -** O pedido em um processo que representa a reclamação do autor, o objetivo almejado por ele com determinada ação judicial. Em uma causa trabalhista, a equiparação salarial e depósitos do Fundo de Garantia por Tempo de Serviço (FGTS) podem ser exemplos de pedido. Vale lembrar que uma ação pode ter mais de um pedido, como pedir indenização por danos materiais e indenização por danos morais, entre outros. Os controles dos pedidos devem fazer parte dos controles de conformidade, para registro e acompanhamento dos processos.

Glossário - Termos Usuais

- **Pesquisa -** É um conjunto de perguntas usadas para examinar uma condição, situação ou valor, cujas respostas registradas possam permitir a tabulação e obtenção de resultados.
- **Política -** É um documento que especifica e fornece o "porquê" formalmente; é de alto nível e estratégico; define o tom, contexto ou intenção da alta direção da empresa, no que quer estabelecer; e muda com pouca frequência.
- **Privacidade desde a Concepção (*Privacy by Design*) -** Significa levar o risco de privacidade em conta em todo o processo de concepção de um novo produto ou serviço em vez de considerar as questões de privacidade apenas posteriormente. Portanto "PbD" significa avaliar cuidadosamente e implementar medidas e procedimentos técnicos e organizacionais adequados desde o início para garantir que o tratamento de privacidade está em conformidade com a GDPR e protege os direitos dos titulares dos dados.
- **Privacidade por defeito (*Privacy by Default*) -** Significa assegurar que são colocados em prática, dentro de uma organização, mecanismos para garantir que, por defeito, apenas será recolhida/coletada, utilizada e conservada para cada tarefa a quantidade necessária de dados pessoais. Esta obrigação do GDPR aplica-se à extensão do seu tratamento, ao prazo de conservação e à sua acessibilidade de forma a assegurar que os dados pessoais não sejam disponibilizados sem intervenção humana a um número indeterminado de pessoas singulares.
- **Privacy Impact Assessments -** É um inventário que possibilita que a organização encontre problemas de privacidade nas fases iniciais de qualquer projeto, reduzindo os custos associados e danos à reputação que poderiam acompanhar uma violação das leis e regulamentos de proteção de dados (GDPR).
- **Proact -** Indica que proativamente se incentive condições e eventos desejáveis; implica em prevenir condições e eventos indesejáveis com ações e controles de gestão.

Glossário - Termos Usuais

- **Probabilidade** (matemática) - É a probabilidade hipotética de que um evento que já ocorreu anteriormente produziria um resultado específico se ocorresse agora.
- **Probabilidade -** É uma medida da chance de que um evento (ou conjunto de eventos) ocorrerá expresso em uma escala linear de 0 (impossibilidade) a 1 (certeza).
- **Procedimento -** Especificação formal que fornece por escrito "como" aplicar as "políticas" empresariais e orienta na prática sua implementação; é específico do público; fornece instruções exatas que garantirão a conformidade com uma determinada política.
- **Processo -** É uma sequência de procedimentos interdependentes e vinculados, que consomem um ou mais recursos, para converter entradas em saídas e produzir os efeitos estabelecidos, nos procedimentos.
- **Programa Compreensivo de Ética e Conformidade** (PCEC conforme definido pela ECI) - Um programa de ética e conformidade deve incluir seis elementos-chave: 1) padrões escritos de conduta ética no local de trabalho; 2) treinamento sobre os padrões; 3) recursos da empresa que fornecem conselhos sobre questões éticas; 4) um meio de denunciar possíveis violações de forma confidencial ou anônima; 5) avaliações de desempenho de conduta ética; e 6) sistemas para disciplinar infratores. Um sétimo elemento, recém introduzido, é um conjunto estabelecido de valores ou princípios orientadores. Podemos afirmar que o PCEC é parte chave de um Programa de Integridade Empresarial.
- **Programa de Ética e Conformidade Efetivo** (ou Bem Implementado) (conforme definido pela ECI) - Uma parte vital de uma empresa e a sua maneira de fazer negócios, que garante que a conduta ética seja recompensada e que os funcionários saibam como se sentir apoiados em seus esforços para manter os padrões de ética em seu trabalho. A ECI mede seis indicadores de uma empresa para um programa eficaz de ética e conformidade: 1) liberdade de questionar a gestão sem medo; 2) recompensas por seguir padrões de ética; 3) não recompensar práticas questionáveis, mesmo que produzam bons resultados para a empresa; 4) feedback positivo para conduta ética; 5) prontidão dos funcionários para lidar com condutas impróprias; e 6) a disposição dos funcionários em buscar aconselhamento sobre ética.

Glossário - Termos Usuais

- **Providências -** Providências são iniciativas ou tarefas que o departamento jurídico ou outros devem tomar ou fazer. Existem as chamadas providências preliminares, que são determinações do juiz, feitas após a resposta do réu, para a regularização de qualquer falha no processo, se necessário (artigo 323 do Código de Processo Civil).
- **Provisões de Código -** Compreende os padrões específicos de comportamento e expectativas de desempenho que sua organização escolhe destacar e abordar em seu código operacional ou Políticas Integradas.
- **Provisão de Valores -** As causas nas quais sua empresa é envolvida terão um valor atribuído a elas. As provisões são cálculos feitos, na maioria das vezes, com base em históricos de outros processos similares que servem de base para a Contabilidade, gerando prováveis valores que a empresa deverá dispor para processos jurídicos.
- **Pseudonimização -** Compreende o recurso tecnológico de suporte à pseudonimização (substituição de material pessoalmente identificável por identificadores artificiais) e à cifragem (codificação de mensagens para que apenas as pessoas autorizadas as possam ler). É o tratamento de dados pessoais de forma a que deixem de poder ser atribuídos a um titular de dados específico sem recorrer a informações suplementares, desde que essas informações suplementares sejam mantidas separadamente e sujeitas a medidas técnicas e organizacionais para assegurar que os dados pessoais não possam ser atribuídos a uma pessoa singular identificada ou identificável.
- **Ransomware -** Ransomware é um tipo de VIRUS, mais precisamente um malware (software malicioso) distinto de outros tipos de malware; sua característica definidora é que ele tenta negar o acesso aos dados de usuários, geralmente criptografando os dados com uma chave conhecida apenas pelo hacker que implantou o malware, até que um resgate seja pago.

Glossário - Termos Usuais

- **Recompensação de Ações e Controles -** Ações e recursos motivadores para reconhecer conduta desejável; e encorajar conduta semelhante no futuro.
- **Registro de Educação em Compliance -** Compreende o Registros Escrito que contêm informações do alunos / treinandos em Programas de Conformidade, que são mantidos ou armazenados por uma instituição educacional, internamente em uma empresa ou por um terceiro, agindo em nome da empresa.
- **Regra de Privacidade (GDPR) -** A regra de privacidade dá aos indivíduos certos direitos com respeito a suas informações de saúde entre outras. Seus direitos incluem, mas não se limitam ao direito de inspecionar qualquer um de seus registros e solicitar correções ou alterações em seus registros, inclusive médicos. A Regra de Privacidade exige que as entidades cobertas notifiquem os indivíduos sobre seu direito à privacidade e expliquem como suas PHI serão usadas e se serão compartilhadas com qualquer pessoa.
- **Regulamento Geral de Proteção de Dados (GDPR) -** O Regulamento Geral de Proteção de Dados (GDPR) é uma estrutura legal que estabelece novas diretrizes para a coleta e o processamento de informações pessoais de indivíduos da União Europeia (UE). O GDPR estabelece os princípios para o gerenciamento de dados e os direitos do indivíduo, além de impor multas que podem ser baseadas em receita. O Regulamento Geral de Proteção de Dados aplica-se a todas as organizações que lidam com dados de cidadãos da UE, tornando-se um regulamento crítico para os responsáveis pela conformidade corporativa em bancos, seguradoras e outras organizações financeiras. Em 25 de maio de 2018, o GDPR entrou em vigor em toda a EU e no mundo.
- **Recurso -** Um ativo útil que pode ser usado para atingir objetivos. Ativos como capital, pessoas, tecnologia, instalações e informações, etc.
- **Responsável pelo Tratamento dos Dados Pessoais -** Designa a pessoa singular ou coletiva, a autoridade pública, a agência ou qualquer outro organismo que, individualmente ou em conjunto com outrem, determine as finalidades e os meios para o tratamento dos dados pessoais.

Glossário - Termos Usuais

- **Resultados -** Resultados das ações realizadas. Os resultados esperados de um programa de ética e conformidade são avaliados continuamente para não comprometer os padrões; menos observações de má conduta; taxa aumentada de observações de relatórios que ocorrem; e um declínio na retaliação contra os denunciantes.
- **Risco -** Uma medida do efeito negativo da incerteza no alcance dos objetivos. Uma medida da probabilidade de ocorrência de um evento, a rapidez com que o evento pode afetar a empresa e o impacto negativo estimado que um evento pode ter sobre os objetivos.
- **Riscos de Conformidade ou de Compliance -** Risco de conformidade é a exposição a penalidades legais, confisco financeiro e perda de material que uma organização enfrenta quando não age de acordo com as leis e regulamentos do setor, políticas internas ou melhores práticas prescritas.
- **Risco de Ética –** É o potencial para danos a uma organização causados por má conduta que não é detectada e persiste devido à falta de conscientização e ação da gerência.
- **Risco Inerente -** É o nível de risco na ausência de ações e controles.
- **Risco Jurídico -** O Risco Jurídico de uma empresa está associado à exposição dela a questões jurídicas. A análise dos riscos ganha cada vez mais atenção por parte das empresas, e os departamentos jurídicos vêm buscando atuar de forma preventiva quanto às demandas litigiosas, trabalhando na mitigação das suas causas e não somente na sua resolução. Uma empresa que precisa, por exemplo, fazer a demissão de um grande número de funcionários, deve avaliar junto à área jurídica os riscos envolvidos nessa operação, para tomar as ações preventivas cabíveis quanto à regularização de todo o processo.
- **Risco Residual -** É o nível de risco após as ações de mitigação e controles estarem em vigor
- **Risco de Reputação –** É o potencial para danos resultantes da perda da confiança das partes interessadas.

Glossário - Termos Usuais

- **Repórter –** Processo de comunicação de qualquer funcionário que observe má conduta no local de trabalho e informe uma autoridade apropriada (externa ou interna à organização).
- **Retenção -** É o uso de fundos internos para financiar a cobertura dos riscos.
- **RPA for COMPLIANCE** – RPA (**R**obotic **P**rocess **A**utomation) para COMPLIANCE, compreende a aplicação das mais avançadas ferramentas de software de automação, para realizar a validação de processos de conformidade, com o uso de "IoT" nos escritórios, via BPM (Business Process Management (Gerenciamento de processos de Negócios), visando automatizar as atividades repetitivas de verificação, reduzindo erros e ampliando o desempenho e a confiabilidade nos controles internos de COMPLIANCE - (*Advanced Compliance* – João R. Peres).
- **Segurança –** É a percepção metrificada ou a crença na garantia das pessoas em se sentir seguras. A segurança é um fator determinante nos relatórios de conformidade.
- **Segurança da manutenção/remoção -** Três dos principais requisitos do GDPR são: a manutenção dos registros atualizados, o direito de um dado assunto de ser esquecido, e a necessidade do controlador de dados em reter os registros para propósitos legais além do consentimento.
- **Sistema de Denúncias -** Qualquer mecanismo (por exemplo, linha de apoio, linha direta ou site) estabelecido por uma organização para fornecer aos funcionários e outros agentes meios para denunciar condutas indevidas à organização sem medo de represálias. É um componente essencial de um programa de Integridade Empresarial. Os sistemas de relatórios podem ser confidenciais e / ou anônimos de forma a permitir que a organização "exerça a devida diligência para prevenir e detectar conduta criminosa".
- **Stakeholder -** É uma pessoa, grupo ou organização que tem participação ou influência direta ou indireta em uma organização. Dessa forma ela pode afetar ou ser afetada pelas ações, objetivos e políticas da organização.
- **Subcontratante (*Data Processor*) -** É a pessoa singular ou coletiva, a autoridade pública, a agência ou qualquer outro organismo que trate os dados pessoais por conta do responsável pelo tratamento destes.

Glossário - Termos Usuais

- **Suborno (Bribe) -** Algo que é dado ou oferecido a uma pessoa ou organização para incentivar essa pessoa / organização a tomar uma ação de benefício para o doador.
- **Subsídios -** Um subsídio pode ser uma referência de apoio monetário concedido por uma parte a outra, individual ou coletiva. Além disso, subsídios podem representar também informações ou dados importantes para a preparação de uma defesa jurídica, um estudo ou relatório da área. Em um processo tributário, por exemplo, os históricos e recibos de pagamento de determinado imposto são subsídios importantíssimos para a elaboração da defesa e pasta do processo.
- **Suporte Integrado –** Sistema que fornece aconselhamento e educação "just-in-time" a indivíduos enquanto estão executando uma tarefa.
- **Tolerância -** O nível aceitável de variabilidade de alcance de um alvo.
- **Tolerância de Risco -** É o nível de risco que a organização não deseja exceder para atingir os objetivos.
- **Tomada de decisão ética –** São decisões executivas que abrangem considerações altruístas: considerando "que impacto essa ação ou decisão terá sobre os outros ou sobre o decisor no relacionamento com eles?
- **Transparência -** A transparência, em um contexto de negócios ou governança, é honestidade e abertura. Transparência e prestação de contas são geralmente considerados os dois principais pilares da boa governança corporativa
- **Tratamento de dados pessoais -** qualquer operação ou conjunto de operações efetuados sobre dados pessoais, com ou sem meios automatizados, tais como a recolha, o registo, a organização, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, por difusão ou por qualquer outra forma de disponibilização, a comparação ou interconexão, bem como a limitação, apagamento ou destruição.

Glossário - Termos Usuais

- **Terceiro (GDPR) -** pessoa singular ou coletiva, autoridade pública, o serviço ou qualquer outro organismo que, não sendo o titular de dados, o responsável pelo tratamento, o subcontratante ou outra pessoa sob autoridade direta do responsável pelo tratamento ou do subcontratante, esteja autorizado a tratar os dados.
- **Uso Legal (GDPR) –** Compreende a manutenção de dados pessoais no sistema e a possibilidade de recuperar, relatar e remover dados quando necessário é essencial, e tudo depende da configuração correta, manutenção e uso de informações pessoais que, por sua vez, dependem da facilidade de acesso, visualização de dados e capacidade de ser informado.
- **Valores Morais –** são valores que atribuímos a um sistema de crenças que ajudam o indivíduo a definir o certo versus o errado, bom versus ruim. Estes geralmente obtêm sua autoridade de algo fora do indivíduo - um ser superior ou uma autoridade superior (ou seja, governo, sociedade). Conceitos morais, julgamentos e práticas podem variar de uma sociedade para outra.
- **Velocidade –** É uma medida da rapidez com que uma empresa é afetada quando ocorre um evento positivo ou negativo.
- **Violação de Dados (GDPR) -** É um incidente no qual dados confidenciais, informações regulamentadas, segredos comerciais ou propriedade intelectual foram expostos a pessoas que não estão autorizadas a visualizá-las. Isso pode ser devido a atividades ilegais ou à liberação acidental ou inadvertida de dados confidenciais fora do controle da organização.
- **Violação de Dados pessoais (GDPR) -** violação da segurança que provoque, de modo acidental ou ilícito, a destruição, a perda, a alteração, a divulgação ou o acesso não autorizado, a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento.
- **Violação de segurança (incidentes de segurança) -** evento com um efeito adverso real na segurança das redes e dos sistemas de informação, tal como um acesso não autorizado ao sistema de informação.

Glossário - Termos Usuais

- **Visão -** Declara o que a organização objetiva ser.
- **Workflows -** Workflows são fluxos de trabalho que determinam a sequência de passos necessários para automatizar os processos de negócio da área jurídica. Com eles, e de acordo com um conjunto de regras definidas e alçadas de aprovação, podem ser distribuídos os processos, aprovados os contratos, entre outras atividades jurídicas. É mais produtividade e controle no departamento, assim como garantia de compliance com a governança corporativa da empresa. O envolvimento da TI como parte da gestão estratégica da companhia é de extrema importância. Para isso, conhecer essas expressões é especialmente relevante, a fim de estreitar os laços com o departamento jurídico da empresa.
- Poderíamos inserir muito mais ...
- **Links de algumas pesquisas Integradas:**

  - https://www.ucop.edu/ethics-compliance-audit-services/compliance/glossary.html
  - http://www.ethics.org/resources/free-toolkit/toolkit-glossary
  - https://www.navexglobal.com/compliancenext/understanding-the-basics/pocket-guide-to-compliance-terminology-2/
  - https://www.idology.com/resources/compliance-glossary-terms/
  - https://www.lombardrisk.com/regulatory-compliance-terminology/
  - https://www.lyonslive.com/resource-center/payment-glossary/
  - https://www.flexiblesystems.com/it-consulting-long-island/compliance/information-security-compliance-glossary/

Agradecemos a contribuição dos Leitores, com novos termos, ajustes nas definições, subsídios de todos os tipos.

Todas as URLs (links) para acesso aos conteúdos na Internet indicados foram testadas e estavam disponíveis em 20/07/2018.

Agradecimento Especial

Este e-book foi liberado em sua versão preliminar para os participantes do "seminário - **COMPLIANCE - como entender e por que aplicar essa nova cultura**", realizado pelo "Instituto de Engenharia de São Paulo", em 09 de agosto de 2018. Na oportunidade, solicitamos aos interessados a indicação de correções de texto e indicações extras para que este e-book fosse melhorado.

Recebemos diversas contribuições, mas em especial nos foi encaminhada uma planilha detalhada, indicando os ajustes necessários, produzida por "**Mauricio Martins Lopes**", que sem dúvida foi fundamental para o resultado do trabalho. Somos muito gratos ao empenho do Engenheiro Mauricio, e por isso o parabenizamos.

Agradecemos também por seus elogios em julgar riquíssimo o material apresentado.

Mauricio Martins Lopes

- Engenheiro civil formado pelo IEEP em 1985, com MBA em Administração de Projetos pela FIA e Bentley College – MA/EUA. Certificado como PMP® (Project Management Professional) pelo PMI® em 2000. Foi fundador, diretor por duas gestões, membro dos conselhos de orientação e fiscal do Capítulo São Paulo do PMI. Experiência de 20 anos em Gerenciamento de Empreendimentos, tendo atuado junto a empresas como Racional Engenharia, Setin Engenharia, Klabin Segall, CPLAN, OAS, Construtora Liderança, Construtora Zion, Construtora ICEC, Construtora Ribeiro Caram, FBS Construtora e Pavimentadora, ENGIURD, Racional Empreendimentos, Synergy Consulting, Planservice, Minerbo-Fuchs Engenharia S.A., Votorantim Metais, etc. É instrutor em cursos de gerenciamento de projetos na CPLAN, FATEC, INPG, IETEC e FIA (convidado) e palestrante em seminários nacionais e internacionais de gerenciamento de projetos.

  linkedin.com/in/mauricio-martins-lopes-pmp-8942451

Mauricio Martins Lopes é owner da **empresa M2L** – vide: http://www.m2l.com.br

Homenagem

"Eu não tenho ídolos. Tenho admiração por trabalho, dedicação e competência."

Ayrton Senna

Luiz Augusto de Angelo Musa – **Foi um Amigo**, companheiro de trabalho com competência admirável e irmão na luta cotidiana.

Homenagem

LUIZ AUGUSTO DE ANGELO MUSA

Atuou na área de ICT por mais de 40 anos, desenvolveu carreira profissional em empresas de grande porte como; Ford do Brasil, IBM BRASIL (23 anos), RCG / Gartner Group, Boucinhas & Campos, MIPS, MRO Software, CSC BRASIL / REMEDY e FGVSP-GVconsult, exercendo funções técnicas, gerenciais e executivas. Formação acadêmica em Física - Física do Estado Sólido, Química, Estatística, Eletrônica e Administração - pela USP e diversos cursos de especialização em ITIL, Segurança e Gestão empresarial.

Atuou como: Negociador da IBM junto a SEI, foi Gerente de Serviços Profissionais IBM, Coordenador de Pesquisas e Consultoria RCG/GartnerGroup (ABC Grupo Algar, Lexmark, Origin, IBM/GSI, Siemens, Comsat, Grupo Silvio Santos, Freios Varga, ...), Diretor Comercial MIPS/PSDI/MRO (Oxiteno, Muller, Ripasa, Alston, Grupo Votorantin, Alcan, Líder Táxi Aéreo, MBR, Belgo Mineira, Gerasul, Metro SP, Novartis, Carbocloro, Petrobrás, ...), Diretor de Professional Service CSC/REMEDY (Intelig, Telefônica, CPqD, gedas/Volkswagen,). Foi diretor do Grupo de Segurança Corporativa da SUCESU-SP e da VP de Telecom. Foi professor da FAAP e da UNISA e professor em cursos da GVPEC em Gestão de Serviços de ICT e Governança de ICT. Foi membro do itSMF Brasil. Articulista e colaborador em periódicos especializados como: Revista Banco Hoje, Jornal Telecom, Informática Hoje, Computeworld, Exame Informática,... Atuou em painéis Técnicos apresentado palestras em Entidades de Classe, Universidades e em eventos específicos sobre temas de interesse nas áreas de ICT, Segurança Corporativa, Gestão de Empresas e Projetos, Gestão de Serviços e Ativos em ICT, entre outros.

Foi um grande e excepcional profissional – contribuiu positivamente com muitas organizações, além das citadas...

- **Exemplo de um dos projetos que participamos em 2005: "Projeto Smart Security Saint-Gobain – Vidros Brasil"**

SAINT-GOBAIN
VIDROS BRASIL

ATESTADO

A SAINT GOBAIN VIDROS S.A com Sede na Av. Santa Marina nº 482, 3º andar, Água Branca, São Paulo – SP, CEP 05036-903, inscrita no CNPJ/MF sob nº 60.853.942/0001-44, ATESTA para os devidos fins, que a Fundação Getúlio Vargas ("FGV"), inscrita no CNPJ/MF sob n.º 33.641.663/0001-44, com endereço na Praia de Botafogo n.º 190, Rio de Janeiro, RJ, através do núcleo de consultoria da Fundação Getúlio Vargas – São Paulo ("FGV-SP"), GVconsult, executou serviços de consultoria para Implantação do Projeto Smart Security, tendo este trabalho sido realizado no período de 14 de Setembro de 2005 a 14 de Outubro de 2005, compreendendo as seguintes atividades:

Atividades Desenvolvidas:

Realização visando:

- Proporcionar o nivelamento teórico dos participantes sobre os temas e requerimentos, abordados na norma internacional ISO/IEC 17799:2005;
- Promover uma reflexão sobre o documento "Saint-Gobain IT Security Questionnaire 2005" considerando a interpretação adequada dos requerimentos da norma de boas práticas de segurança;
- Desenvolvimento de um trabalho grupal para concluir um plano de ação de curto e médio prazo e a produção de um Guidelines de Melhores Práticas de Segurança, para serem utilizadas imediatamente.

O projeto contou com a participação da seguinte Equipe de Trabalho da FGV/SP - GVconsult:

Paulo Roberto Vampré Hummel (Coordenador do Projeto)

Luiz Augusto de Ângelo Musa

João Roberto Peres

Os trabalhos realizados, não merecem qualquer restrição de nossa parte no que se refere à qualidade e prazos convencionados, cumprindo a FGV/SP-GVconsult satisfatoriamente todos os compromissos contratuais.

14º SUBDISTRITO LAPA

São Paulo, 31 de outubro de 2005

José Luiz Teixeira Machado
Gerente Geral Informática Corporativa
11 3874-7227
Jose-luiz.machado@saint-gobain.com

14º OFICIAL DE REG. CIVIL DAS P. NATURAIS DO 14º SUB. LAPA - SÃO PAULO - SP
Praça Professor José Arruda Penteado, 45/49 - Lapa - CEP: 05072-050 - Fone: (11) 3836-9395
Reconheço, por semelhança, a firma de: JOSE LUIZ TEIXEIRA MACHADO (46231).
São Paulo, 01 de novembro de 2005
Em testemunho da verdade.
Débora Regina da Silva Paula Souza, escrevente autorizada
Preço por firma R$ 4,05 ; Valor total R$ 4,05

SAINT-GOBAIN VIDROS S.A.
Av. Santa Marina, 482 - 05036-903 - São Paulo - SP
Tel.: 55 (11) 3874-7420 Fax: 55 (11) 3874-7511
www.saint-gobain-vidros.com.br

FIRMA VALOR ECONÔMICO
1022AA075934

Fotos de trabalho durante o desenvolvimento do:
"Projeto Smart Security Saint-Gobain – Vidros Brasil" em 2005.

Luiz Augusto e João Peres

Equipe da Consultoria FGV – Gvconsult-SP e colaboradores da área de Segurança Corporativa e de Tecnologia da Informação, da Saint-Gobain.

Bibliografia e Webgrafia

Bibliografia - (Principais livros e referência para consultas indicados)

- BARROSO LEITE, Celso. Sociologia da corrupção. Rio de Janeiro: Zahar Editor, 1987.
- BATISTA, Antenor. Corrupção - fator de progresso? São Paulo: Editora Simples, 1979.
- BEZERRA, Marcos Otávio. Corrupção: um estudo sobre o poder público e relações pessoais no Brasil. Rio de Janeiro: Relume-Dumara: ANPOCS, 1995.
- CAVALCANTI, Pedro Rodrigues de Albuquerque. A corrupção no Brasil. São Paulo: Siciliano, 1991, p. 17-19.
- ELLIOTT, Kimberly Arm (org.). A Corrupção e a Economia Global. Brasilia: Editora Universidade de Brasilia, 2002.
- FAORO, Raymundo. Os donos do poder: formação do patronato político brasileiro. 5ª. ed. Porto Alegre: Globo 1979.
- FRANCO SOBRINHO, Manoel de Oliveira. O Controle da Moralidade Administrativa. São Paulo, Saraiva, 1974.
- GIACOMUZZI, José Guilherme. A moralidade administrativa e a boa fé da administração pública. São Paulo, Malheiros, 2002.
- GOHN, Maria da Glória. Teorias dos Movimentos Sociais: paradigmas clássicos e contemporâneos. 5ª. Ed. São Paulo: Loyola, 2006.
- JESUS, Damásio E. de. Crimes de corrupção ativa e tráfico de influência nas transações comerciais internacionais. São Paulo: Saraiva, 2003.
- LIVIANU, Roberto. Corrupção e Direito Penal: um diagnóstico da corrupção no Brasil. Coimbra editora, 2007.
- MAURO, Paolo. Corruption and Growth. The Quarterly Journal of Economics. Cambridge, Volume 110, No. 3. p. 681-712. 1995.
- MOTTA, Sylvio. FREIRE, Elias. Ética na Administração Pública. São Paulo:Campus, 2007.
- OLIVEIRA, Edmundo. Crimes de Corrupção. Rio de Janeiro:Forense, 1991.
- RAMINA, Larissa L. O. Ação internacional contra a corrupção. Curitiba: Juruá, 2002.

- RIBEIRO, Antônio Silva Magalhães. Corrupção e controle na administração pública brasileira. Sao Paulo: Atlas, 2004.
- ROSE-ACKERMAN. The Political Economy of Corruption. In: ELLIOTT, Kimberly A. Corruption And The Global Economy. Washington, DC: Peterson Institute for International Economics. 1997. p. 31-70.
- SILVA, Marcos Fernandes Gonçalves. A Economia Política da Corrupção no Brasil. São Paulo: Editora SENAC São Paulo, 2001.
- TREVISAN, Antonino Marmo et al. Combate à Corrupção nas Prefeituras do Brasil. São Paulo: Ateliê Editorial, 2003.

Webgrafia (seleção de algumas referências entre as milhares)

- Ministério da Agricultura, Pecuária e Abastecimento exige que prestadores de serviços instituam programas de integridade:
http://www.agricultura.gov.br/noticias/mapa-exige-que-prestadores-de-servicos-instituam-programas-de-integridade

- Obrigatoriedade de compliance já é realidade
https://politica.estadao.com.br/blogs/fausto-macedo/obrigatoriedade-de-compliance-ja-e-realidade/

- Fórum de Compliance apresenta os desafios e benefícios para integridade corporativa
https://ecommercenews.com.br/noticias/lancamentos/forum-de-compliance-apresenta-os-desafios-e-beneficios-para-integridade-corporativa/

- Conduta ética na saúde é urgente e deve incluir pacientes, alertam consultores
https://oglobo.globo.com/sociedade/saude/conduta-etica-na-saude-urgente-deve-incluir-pacientes-alertam-consultores-21472723

- Urgente: Estado do Rio torna obrigatório Compliance para empresas que contratarem com a Administração Pública
https://www.teixeirafilho.com.br/noticia/862/urgente--estado-do-rio-torna-obrigatorio-compliance-para-empresas-que-contratarem-com-a-administracao-publica/

- PL722/2017 – Cria Selo Anticorrupção concedido a empresas que adotem Programas de Integridade – *www.sãopaulo.sp.leg.br*
http://www.saopaulo.sp.leg.br/blog/selo-anticorrupcao-e-sugerido-em-projeto-de-lei/

Webgrafia

- A corrupção como tema global: a busca por integridade planetária na OCDE em Paris, no ano de 2018 ""Integridade Planetária não é um sonho distante, é uma necessidade urgente".

http://www.migalhas.com.br/dePeso/16,MI279511,61044-A+corrupcao+como+tema+global+a+busca+por+integridade+planetaria+na

- PLANO NACIONAL DE INTEGRIDADE, TRANSPARÊNCIA E COMBATE À CORRUPÇÃO - TEXTO BASE - INSTITUTO ETHOS - Medidas de integridade e transparência ..... Avaliação do Sistema de Integridade da Administração Pública exige urgente revisão.

http://www.cnmp.mp.br/portal/images/Comissoes/fncc/TEXTO_BASE_PLANO_INTEGRIDADE_ETHOS_4a_VERS%C3%830_-_FORMATADO.pdf

- URGENTE - Coordenadoria de Auditoria Interna (CAIN), Coordenadoria de Promoção da Integridade, (COPI), Corregedoria Geral do Município (CORR) e Ouvidoria Geral do Município (OGM)- Divulga "Programa de Integridade e Boas Práticas da Secretaria Municipal do Verde e do Meio Ambiente (SVMA)-SP.

http://www.prefeitura.sp.gov.br/cidade/secretarias/upload/programa_svma.pdf

- URGENTE- POR MENOS CORRUPÇÃO NO BRASIL

https://mude.org.br/

- URGENTE - Relatório de Corrupção no Brasil

https://www.business-anti-corruption.com/country-profiles/brazil/

- Petrobras of Brazil to Pay $2.95 Billion Over Corruption Scandal

https://www.nytimes.com/2018/01/03/business/dealbook/brazil-petrobras-corruption-scandal.html

- Corruption in Brazil

https://en.wikipedia.org/wiki/Corruption_in_Brazil

- Conceitos – diferenças entre Ética e Moral
https://www.diferenca.com/etica-e-moral/

- Trecho do Livro "A LUTA CONTRA A CORRUPÇÃO" – jurista "Deltan Dallagnol"

http://www.esextante.com.br/media/upload/livros/Alutacontraacorrupcao_Trecho.pdf

Webgrafia

- Entrevista - TORQUATO JARDIM, MINISTRO DA TRANSPARÊNCIA, FISCALIZAÇÃO E CGU - "A corrupção é da natureza humana" Carlos Sambrana - Edição 19/05/2017 - nº 1019

https://www.istoedinheiro.com.br/corrupcao-e-da-natureza-humana/

- Corrupção: natureza humana ou condição social?

http://www.oestadoce.com.br/opiniao/corrupcao-natureza-humana-ou-condicao-social

- Corrupção no Brasil: uma visão da psicologia analítica – Artigo - Camila Souza Novaes

http://pepsic.bvsalud.org/scielo.php?script=sci_arttext&pid=S0103-08252016000200002

- Livro Disponível WEB – "As múltiplas faces da corrupção e seus efeitos na democracia contemporânea" - organizadores, Rogério Gesta Leal e Ianaiê Simonelli da Silva. – Santa Cruz do Sul : EDUNISC, 2014.

http://unisc.br/editora/as_multiplas_faces_red.pdf

- Livro Aberto – "A corrupção da inteligência" - Flávio Gordon. - 1. ed. - Rio de Janeiro: Record, 2017.

http://livrosgratisbibliotecaonline.com/wp-content/uploads/2018/01/A-Corrup%C3%A7%C3%A3o-da-Intelig%C3%AAncia-Intelectuais-e-poder-no-Brasil-Fl%C3%A1vio-Gordon.pdf

- TESIS DOCTORAL – "AS RAIZES DA CORRUPÇAO: ESTUDOS DE CAOS E LIÇOES PARA NO FUTURO" - ROCHA FURTADO, LUCAS 2012.

https://gredos.usal.es/jspui/bitstream/10366/121413/1/DDP_RochaFurtadoLucas_Tesis.pdf

- "Global Conference on Transparency Research" **será realizada no Rio, na FGV em 26 e 27 de junho de 2019**. A Conferência é o principal evento mundial sobre transparência e acolhe pesquisas sobre o tema a partir de pontos de vista multidisciplinares e multimetodológicos. O tema da edição 2019 será "Measuring Transparency: Impact, Compliance, and Implementation".

https://eventos.fgv.br/en/transparency2019

https://spaa.newark.rutgers.edu/gctr

- Diagnóstico institucional: primeiros passos para um plano nacional anticorrupção

http://bibliotecadigital.fgv.br/dspace/bitstream/handle/10438/18167/Diagn%c3%b3stico%20institucional%20-%20primeiros%20passos%20para%20um%20plano%20nacional%20anticorrup%c3%a7%c3%a3o.pdf?sequence=3&isAllowed=y

Webgrafia

vídeos

- Entenda a corrupção no Brasil - Vídeo TV FOLHA - Publicado em 4 de set de 2011 – (11 minutos)
  https://www.youtube.com/watch?v=PTDIhB09uWA
- Leandro Karnal fala sobre a corrupção na natureza humana – Vídeo - (3 Minutos)
  https://globoplay.globo.com/v/5962297/
- O que você tem a ver com a corrupção? Campanha conjunta promovida pelo Ministério Público - SC e Tribunal de Contas - SC.
  Vídeo (4 Minutos)
  https://www.youtube.com/watch?v=hblBLIKTTfw
- Jô entrevista Dr. Judivan, autor da coleção "Corrupção no Mundo" - Vídeo (22 Minutos)
  https://www.youtube.com/watch?v=klOK7hGBKAU
- CORRUPÇÃO E DESONESTIDADE (COM CORTELLA) Vídeo – (13 Minutos)
  https://www.youtube.com/watch?v=5ut6FT3Fu7o
- Leandro Karnal e Lázaro Ramos I Espelho - "A corrupção é um mal social", afirma Leandro Karnal. Na conversa com Lázaro Ramos, o professor fala sobre o conceito de ética e comenta os atuais movimentos sociais e políticos. Vídeo (26 Minutos)
  https://www.youtube.com/watch?v=vYmJEW7E05s
- Projeto sobre proteção de dados aguarda sanção de Temer – vídeo GloboNews (04:33 Minutos)
  http://gl.globo.com/globo-news/jornal-das-dez/videos/v/projeto-sobre-protecao-de-dados-aguarda-sancao-de-temer/6884539/

Webgrafia

Vídeos

- Especial – Unidos Contra a Corrupção – Manifesto – vídeo (1:14 minutos)

https://www.youtube.com/watch?time_continue=14&v=9Dj2qc8juHE

Site web - http://www.unidoscontraacorrupcao.org.br/

- Deltan Dallagnol - #UnidosContraACorrupcao - vídeo (1:44 minutos)

https://twitter.com/i/status/1020462612952375297

Webgrafia – entidades contra a corrupção Brasil

URLs de algumas entidades anticorrupção muito atuantes:

https://www3.ethos.org.br/

http://anticorrupcao.direitorio.fgv.br/projetos/plano-nacional-anticorrupcao

http://osbrasil.org.br/

http://www.contasabertas.com.br/

https://instituto.cidadedemocratica.org.br/

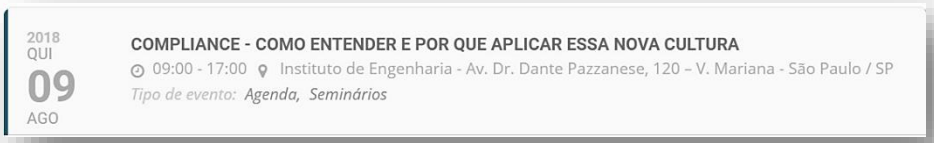
https://transparenciainternacional.org.br/home/destaques

Todas as URLs (links) para acesso aos conteúdos na Internet indicados foram testados e estavam disponíveis em 20/07/2018.

- Este e-book teve sua divulgação inicial durante o "seminário" amplamente divulgado pelo "**Instituto de Engenharia de São Paulo**":

URL de acesso < https://www.institutodeengenharia.org.br/site/events/seminario-compliance/ .> disponível em 05/07/2018.

INSCRIÇÕES GRATUITAS



- ***Programa**
- **9h – Abertura** – Eduardo Lafraia – Presidente Instituto de Engenharia
- **9h15 – 10h10 – 1ª Palestra** – **COMPLIANCE – Instrumento de defesa contra a Corrupção e Fraudes nas Empresas**
  Por João Roberto Peres – NewKomp

  Motivadores em busca de Soluções
  Corrupção no mundo;
  Mapa global de fraudes;
  Riscos Cibernéticos – previsão até 2020;
  Fraudes Ocupacionais no mundo empresarial;
  IPCL – Índice de Percepção de Cumprimento de Leis – Brasil;
  Impacto do hábito coletivo brasileiro do "furto" leve
  Como Reduzir os Riscos de Corrupção e Fraudes nas Empresas
  Diagnóstico Estratégico;
  Gestão e Governança – Da Governança Familiar à Corporativa;
  Potencialização no uso de tecnologias de TIC – Informação e Comunicações;
  Políticas de Segurança Empresarial, da Informação e de Compliance integradas;
  Programas de Compliance Empresarial – do Básico ao Avançado;
  Gestão de Compliance no padrão Internacional – uso da Norma "ISO 19.600:2014";
  Gestão Antisuborno no padrão Internacional – uso da Norma "ABNT NBR ISO 37.001:2016";
  Certificações de Conformidade Anticorrupção.
  Conclusões
- **10h10 – 11h05 – 2º Palestra – Governança Corporativa e responsabilidade social das organizações**
  Por Ailton Fernandes Barcelos

  Valores e princípios
  Governança Corporativa
  Responsabilidade Social das organizações.

- **11h05 – 11h35 – Intervalo**
- **11h35 – 12h30 – 3º Palestra -Compliance: conceitos e implementação nas organizações -**
  Por Orlando Carneiro de Ribeiro Arnaud – UBERCONSULT
  Compliance
  Conceito de compliance
  Fontes de Obrigações
  Riscos de não compliance (penalidades)
  Programa de integridade corporativa, governança corporativa e a responsabilidade social das empresas.
  Benefícios do compliance
  Implantação do compliance
  Alternativas para organização da área de compliance
  Metodologia para implementação do compliance
  Gerenciamento de projeto para implementação do compliance
  Aperfeiçoamento dos processos e sistemas de controle
  Mudança de cultura, endomarketing e comunicação externa
  Metodologia para implementação do "compliance"
  Redução de custos na implementação
  Alternativa para uso da consultoria compartilhada visando a redução de custos na implementação. Características da consultoria compartilhada
- **12h30 – 14h – Almoço**
- **14h – 14h55 – 4ª Palestra -Lei anticorrupção (Lei 12.846/13) e Lei de Improbidade Administrativa (Lei 8.429/92)**
  Por Márcio Pestana – Pestana e Villasbôas Arruda Advogados
  Contextualização e aspectos estruturais da Lei Anticorrupção (Lei 12.846/2013) e da Lei 8.429/1992. Sujeitos ativos e passivos;
  Os atos lesivos. Integração normativa;
  Lei Anticorrupção: processo administrativo e judicial, sanções, dosimetria e Acordo de Leniência,
  Lei de Improbidade Administrativa: sanções, processo administrativo e judicial.
- **14h55 – 15h50 – 5ª Palestra – Delação Premiada**
  Por Mário Luiz Sarrubbo – Subprocurador-Geral de Justiça
  Delação Premiada e o papel do Ministério Público
- **15h50 – 16h35 – 6ª Palestra – Resultados da implementação do compliance na Siemens**
  Por Reynaldo Goto – Diretor de Complice – Siemens
- A implementação do programa de compliance na Siemens, quais os impactos do programa na cultura da empresa e na relação com os fornecedores.
- **16h35 – 17h** – Encerramento

Autor e Cocriadores: João Roberto Peres, Daniel Péres, Manuel Deus.

ISBN: 978-85-923158-2-5

Direitos Reservados - Vide Detalhes em “Declaração” página 06.