COMPLIANCE URGENTE

INSTITUTO DE ENGENHARIA

1916

COMPLIANCE

Instrumento de defesa contra a Corrupção e Fraudes nas Empresas

NEWKOMP

João Roberto Peres

Professor, Palestrante, Consultor, Empresário, Autor-Editor

Consultor e Professor (FGV), formação: Engenharia Elétrica (EPUSP) e Ciência da Computação (UNICAMP), com cursos e certificações internacionais em Segurança Empresarial. Multiespecialista em GRC (Governança, Riscos e Compliance), Planejamento Estratégico, Perícia Computacional, Direito Digital, IoT/IoE, Big Data & Analytics... É autor de publicações e e-books; "COMPLIANCE-FUNDAMENTOS", "COMPLIANCE – Corrupção e Fraudes no Mundo Empresarial", "COMPLIANCE URGENTE", "Manifesto-Direitos Globais de IoT" , "IoT – Investigação Forense Digital", coautor do Guia de Referência "Segurança Corporativa – OAB-SP", membro do Grupo de Estudos "Direito Digital e Compliance" da FIESP, participou do estudo "Bytes de IoT - Internet das Coisas: um plano de ação para o Brasil" do BNDES / MCTIC, entre outros.

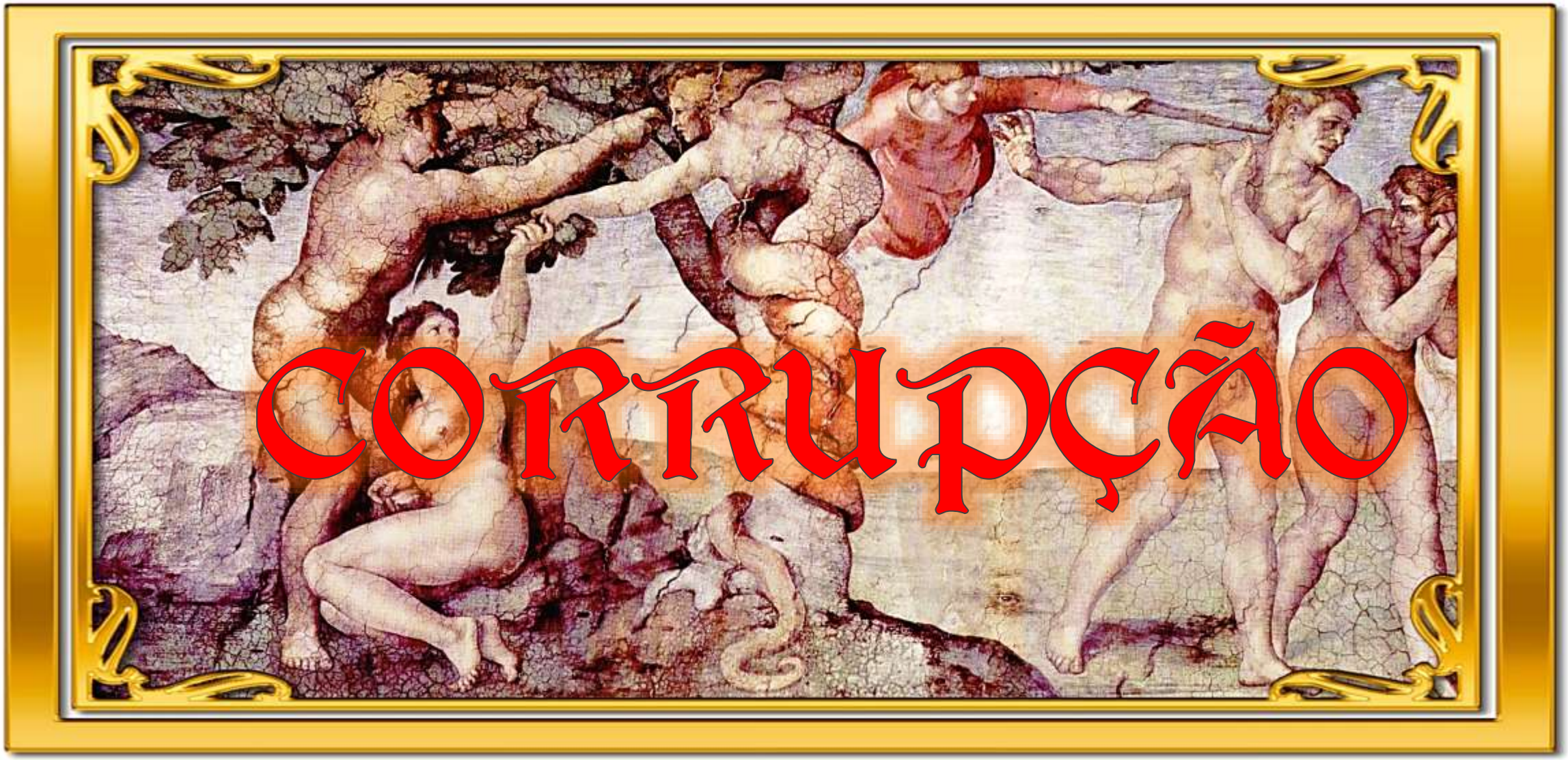
Agenda temática – COMPLIANCE & INTEGRIDADE

- Corrupção & Compliance
- 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”;
  - Lei Internacional de Proteção de Dados GDPR e a Lei Brasileira LGPD;
  - Certificações de Conformidade Anticorrupção.
- Conclusões

9h15 – 10h10 - Palestra 40 minutos – Questões 10 minutos -> 09/08/2018


DESAFIOS DO SÉCUULO XXI
CORRUPÇÃO
COMPLIANCE
ERRADO
CERTO

Corrupção – falha do DNA Humano



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


MLIZATION
COMPLIANCE

MOTIVADORES

Corrupção no mundo

21/02/2018

Brasil Score - Rank - Countries

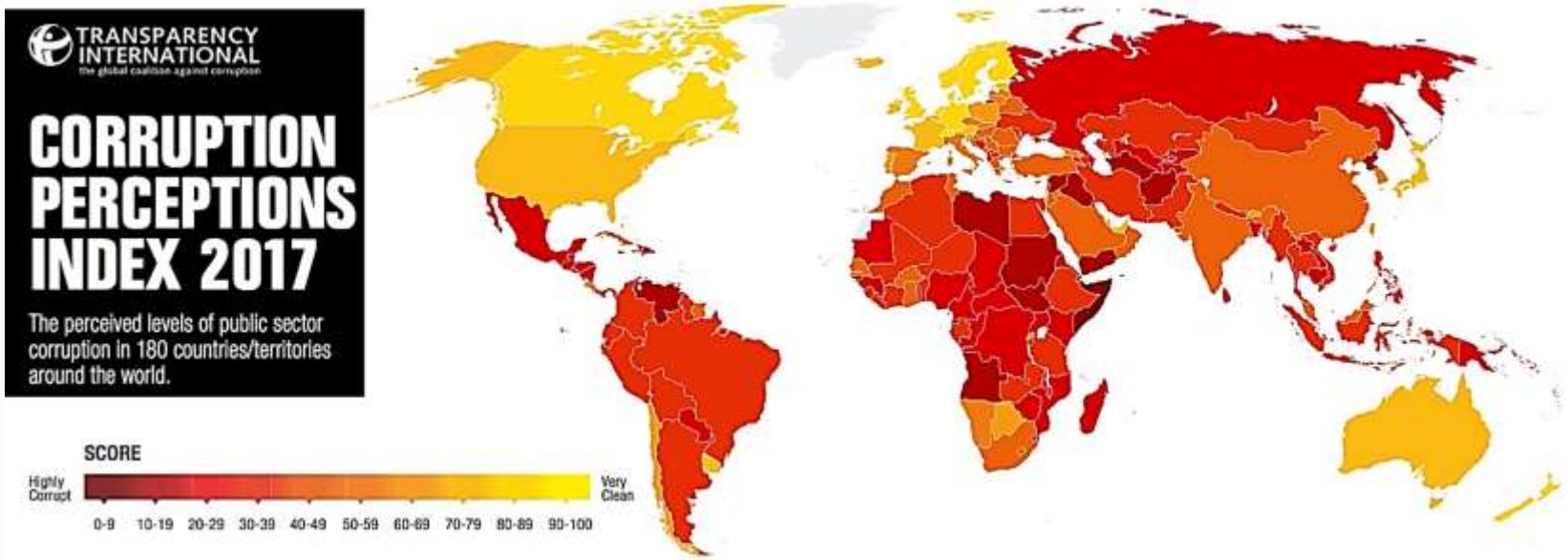
2017 = 37 - 96ª (180)
2016 = 40 - 79ª (176)
2015 = 38 - 76ª (168)
2014 = 43 - 69ª (175)
2013 = 42 - 72ª (177)
2012 = 43 - 69ª (174)

Índice de Percepção da Corrupção (Corruption Perceptions Index, ou CPI), produzido anualmente desde 1995 pela ONG Transparência Internacional.

TRANSPARENCY INTERNATIONAL
the global coalition against corruption

CORRUPTION PERCEPTIONS INDEX 2017

The perceived levels of public sector corruption in 180 countries/territories around the world.

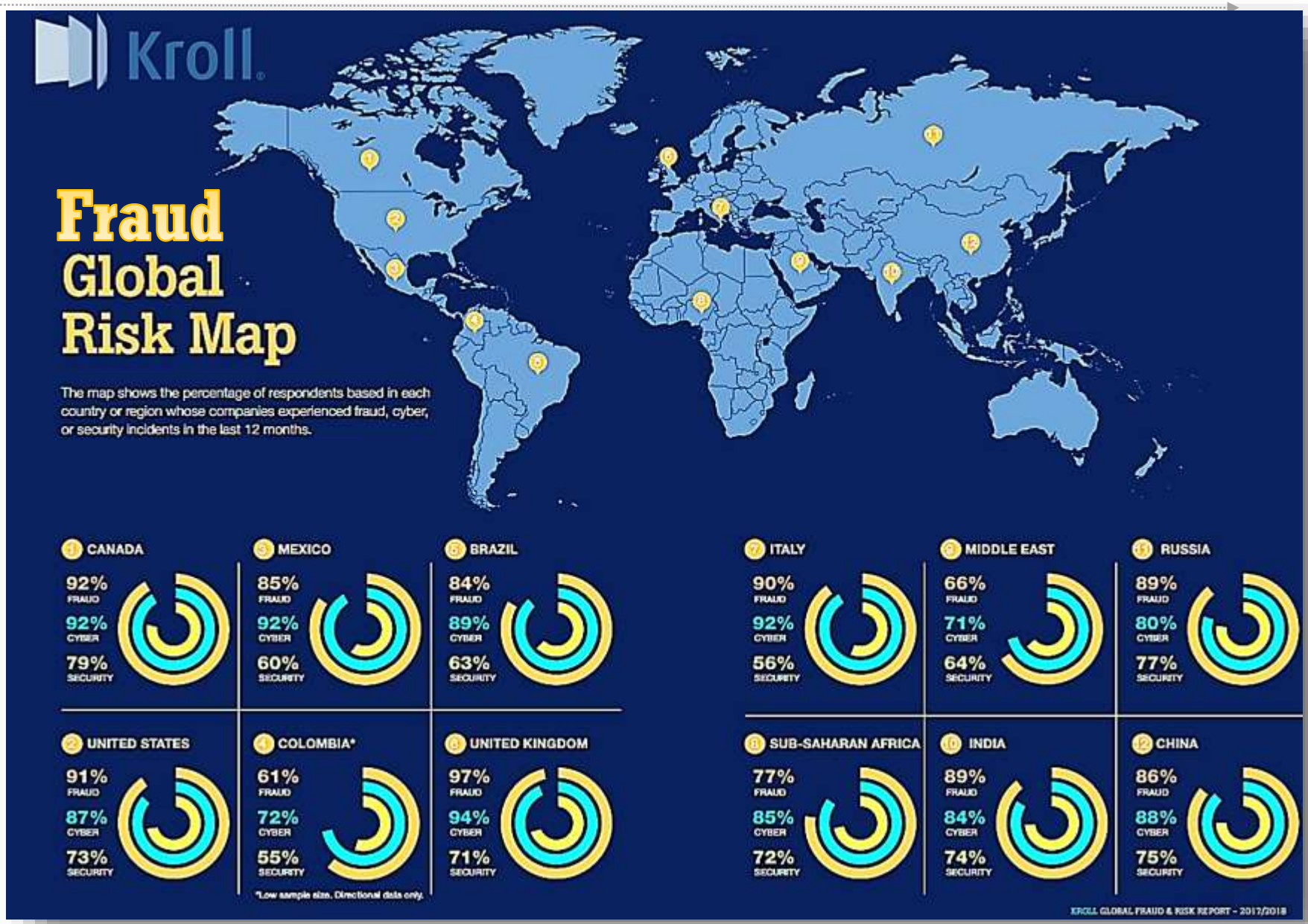


RANK	COUNTRY/TERRITORY	SCORE
1	New Zealand	89
2	Denmark	88
3	Finland	85
3	Norway	85
3	Switzerland	85
6	Singapore	84
6	Sweden	84
8	Canada	82
8	Luxembourg	82
8	Netherlands	82
8	United Kingdom	82
12	Germany	81
13	Australia	77
13	Hong Kong	77
13	Iceland	77
16	Austria	75
16	Belgium	75
16	United States	75
19	Ireland	74
20	Japan	73
21	Estonia	71
21	United Arab Emirates	71
23	France	70
23	Uruguay	70
25	Barbados	68
26	Bhutan	67
26	Chile	67
28	Bahamas	65
29	Portugal	63
29	Qatar	63
29	Taiwan	63
32	Brunei Darussalam	62
32	Israel	62
34	Botswana	61
34	Slovenia	61
36	Poland	60
36	Seychelles	60
38	Costa Rica	59
38	Lithuania	59
40	Latvia	58
40	Saint Vincent and the Grenadines	58
42	Cyprus	57
42	Czech Republic	57
42	Dominica	57
42	Spain	57
46	Georgia	56
46	Malta	56
48	Cabo Verde	55
48	Rwanda	55
48	Saint Lucia	55
51	Korea (South)	54
52	Grenada	52
53	Namibia	51
54	Italy	50
54	Mauritius	50
54	Slovakia	50
57	Croatia	49
57	Saudi Arabia	49
59	Greece	48
59	Jordan	48
59	Romania	48
62	Cuba	47
62	Malaysia	47
64	Montenegro	46
64	Sao Tome and Principe	46
66	Hungary	45
66	Senegal	45
68	Belarus	44
68	Jamaica	44
68	Oman	44
71	Bulgaria	43
71	South Africa	43
71	Vanuatu	43
74	Burkina Faso	42
74	Lesotho	42
74	Tunisia	42
77	China	41
77	Serbia	41
77	Suriname	41
77	Trinidad and Tobago	41
81	Ghana	40
81	India	40
81	Morocco	40
81	Turkey	40
85	Argentina	39
85	Benin	39
85	Kosovo	39
85	Kuwait	39
85	Solomon Islands	39
85	Swaziland	39
91	Albania	38
91	Bosnia and Herzegovina	38
91	Guyana	38
91	Sri Lanka	38
96	Brazil	37
96	Indonesia	37
96	Panama	37
96	Peru	37

Mapa global de fraudes e outros riscos

% indicado por executivos entrevistados, sobre a ocorrência de Fraudes Internas, Ataques Cibernéticos e incidentes de Segurança Física – tipo furto de ativos.

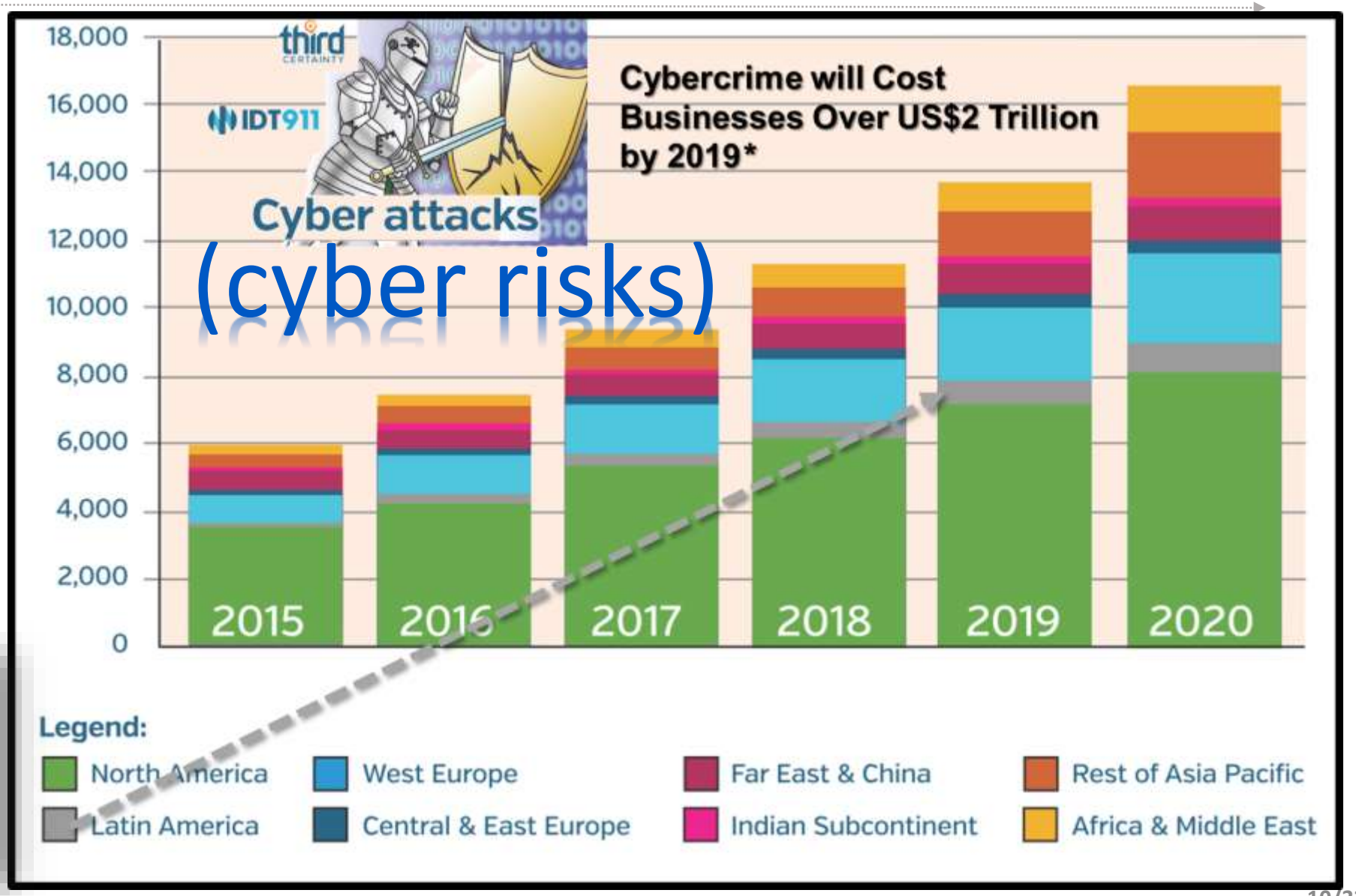
Employee and Insider Fraud



Riscos Cibernéticos

Se sua empresa nunca foi atacada por meios cibernéticos, tenha a absoluta certeza de que um dia ela será.

É só questão de Tempo!



http://thirdcertainty.com/infographics/

Top 10 Global Risks

The Global Risks Landscape 2018

Probabilidade

1. Eventos climáticos extremos
2. Desastres naturais
3. Ataques cibernéticos
4. Fraude de dados ou roubo
5. Falhas adaptação às mudanças climáticas
6. Migração involuntária em larga escala
7. Desastres ambientais provocados
8. Ataques terroristas
9. Comércio ilícito
10. Bolhas de ativos na economia

Impacto

1. Armas de destruição em massa
2. Eventos climáticos extremos
3. Desastres naturais
4. Falhas adaptação às mudanças climáticas
5. Crise de água
6. Ataques cibernéticos
7. Crises alimentares
8. Perda de biodiversidade e ecossistema
9. Migração involuntária em larga escala
10. Propagação de doenças infecciosas

Categorias

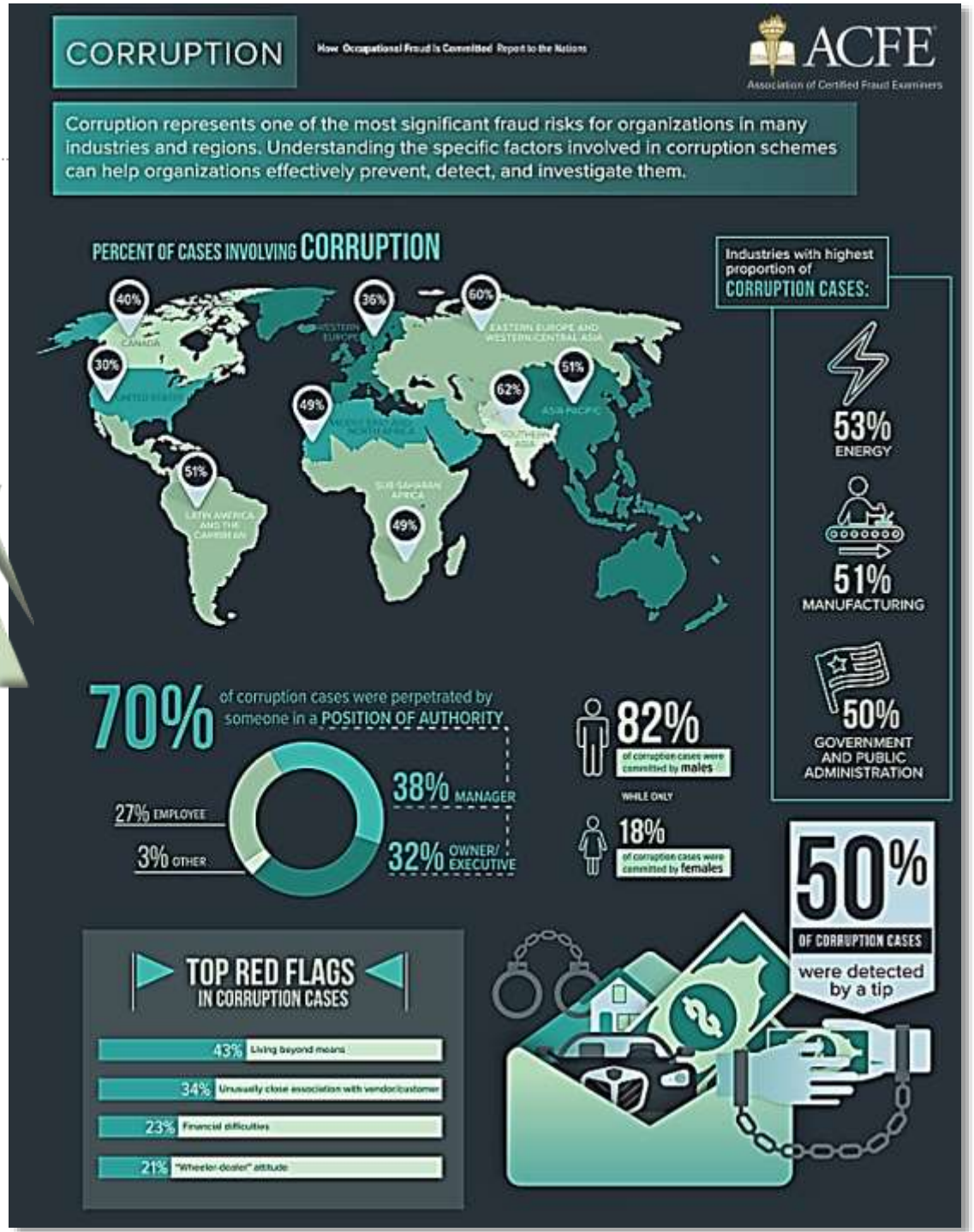
- Econômico
- Ambiental
- Geopolítico
- Sociedade
- Tecnologias

Os riscos da cibersegurança também estão aumentando, tanto em sua prevalência quanto em seu potencial disruptivo. Ataques contra empresas quase que dobraram em cinco anos, e incidentes que antes seriam considerados excepcionais estão se tornando cada vez mais comuns. O impacto financeiro de falhas na cibersegurança está crescendo e alguns dos maiores custos de 2017/2018 estão relacionados com ataques pedindo resgate, que representaram 64% de todos os e-mails mal-intencionados.

The Global Risks Report 2018, 13th Edition, is published by the World Economic Forum.

Fraudes Ocupacionais

Os esquemas Fraudulentos levam de 12 até 30 meses para serem descobertos, dependendo do tipo realizado.



IPCL – Índice de Percepção do Cumprimento de Leis

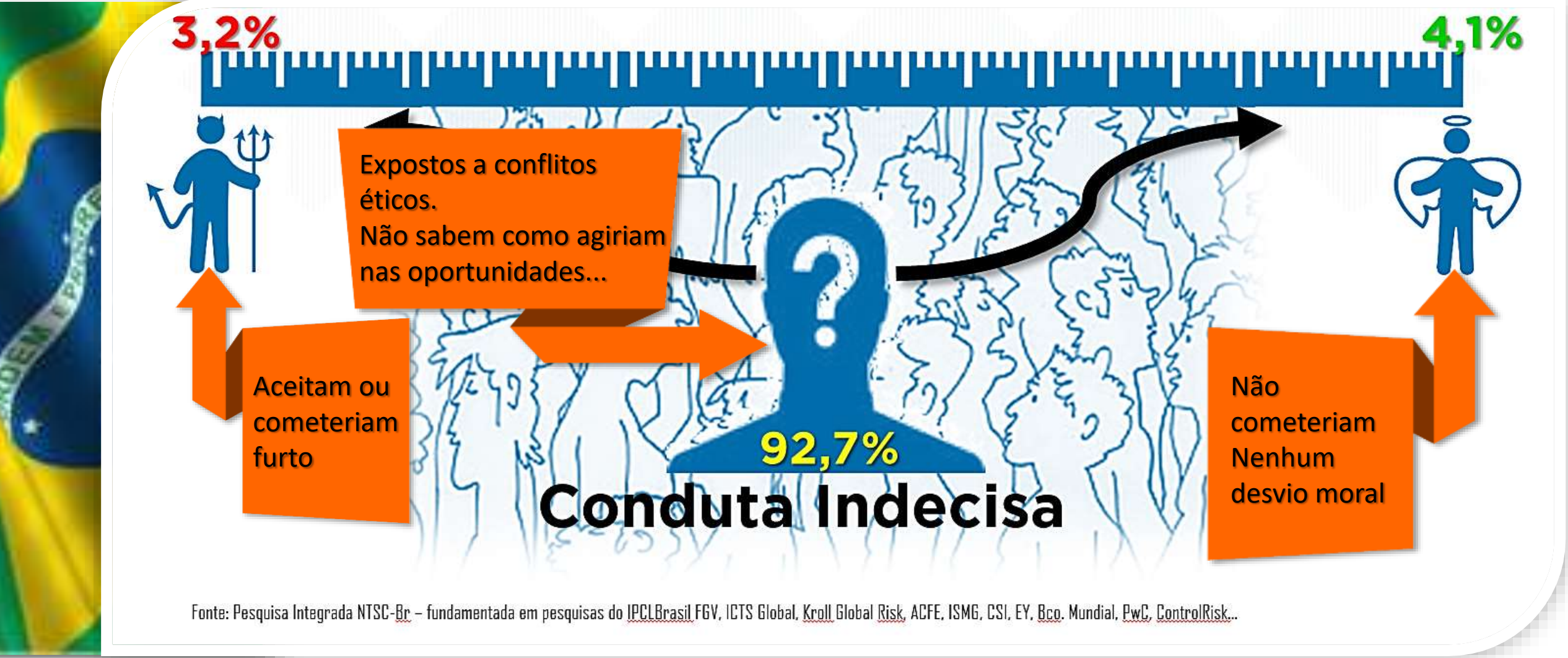
- IPCLBrasil (Índice de Percepção do Cumprimento da Lei – amostra em 3 anos), 82% da população acredita que é fácil desobedecer as leis no Brasil.

209.000.000 x 3% =

3%= 6.270.000 de larápios

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

Impacto do hábito coletivo brasileiro do “furto” leve



Fonte: Pesquisa Integrada NTSC-Br – fundamentada em pesquisas do IPCLBrasil FGV, ICTS Global, Kroll Global Risk, ACFE, ISMG, CSI, EY, Bco. Mundial, PwC, ControlRisk...

Pressão Internacional – Algumas Leis e Convenções

- 1977 • FCPA - Foreing Corrupt Practices Act .
- 1996 • OEA – Convenção Interamericana Contra a Corrupção
- 1997 • OCDE – Convenção sobre o Combate a corrupção
- 1998 • Alteração FCPA > ênfase contra a Corrupção
- 2000/2004 • Pacto Global ONU (décimo princípio contra a corrupção)
- 2002 • Código Penal Brasileiro
- 2002 • Sarbanes–Oxley Act
- 2009 • Publicação “Responsabilidade das Empresas” CGU/ETHOS
- 2010 • UK Bribery Act (Lei do Suborno)
- 2011 • Brasil – Lei 12527 – (Lei Complementar 131/2009) Lei da Transparência
- 2013 • Brasil - Lei 12.846/13 (Lei Anticorrupção)
- 2016/18 • GDPR - General Data Protection Regulation (EU) – 25/05/2018


Do desafio à ação >
Como reduzir os Riscos
de Corrupção e Fraudes?

REGRA DE OURO

Adotar e implementar gradativamente um "PROGRAMA DE INTEGRIDADE EMPRESARIAL" apoiado em processos de CONFORMIDADE ou COMPLIANCE

Sempre praticar a simplicidade, a economia e a eficácia.

Compliance x Programa de Integridade

Atividades de controle de atendimento à conformidade regulatória “Interna e Externa” as organizações, sugiram há muito tempo, ou seja, são as atividades que hoje denominamos de “COMPLIANCE”. Por outro lado, os modernos “Programas de Integridade Empresarial ou Corporativos”, buscam ser mais abrangentes e efetivos, uniformizando procedimentos operacionais e alinhando a ética e moralidade organizacional ao padrões de aceitação mundiais.

É possível voar só na busca do COMPLIANCE?

Como se inicia um sistema de COMPLIANCE?

- Política de Compliance
- Agentes de Compliance
- Normas Internas e Procedimentos
- Controles Operacionais
- ...

COMPLIANCE

Como avançar para um Programa de INTEGRIDADE?

Diagnóstico Estratégico

Quando um Consultor for iniciar o estudo para implementar um sistema de Compliance no apoio para um futuro Programa de Integridade Empresarial, ele deve:

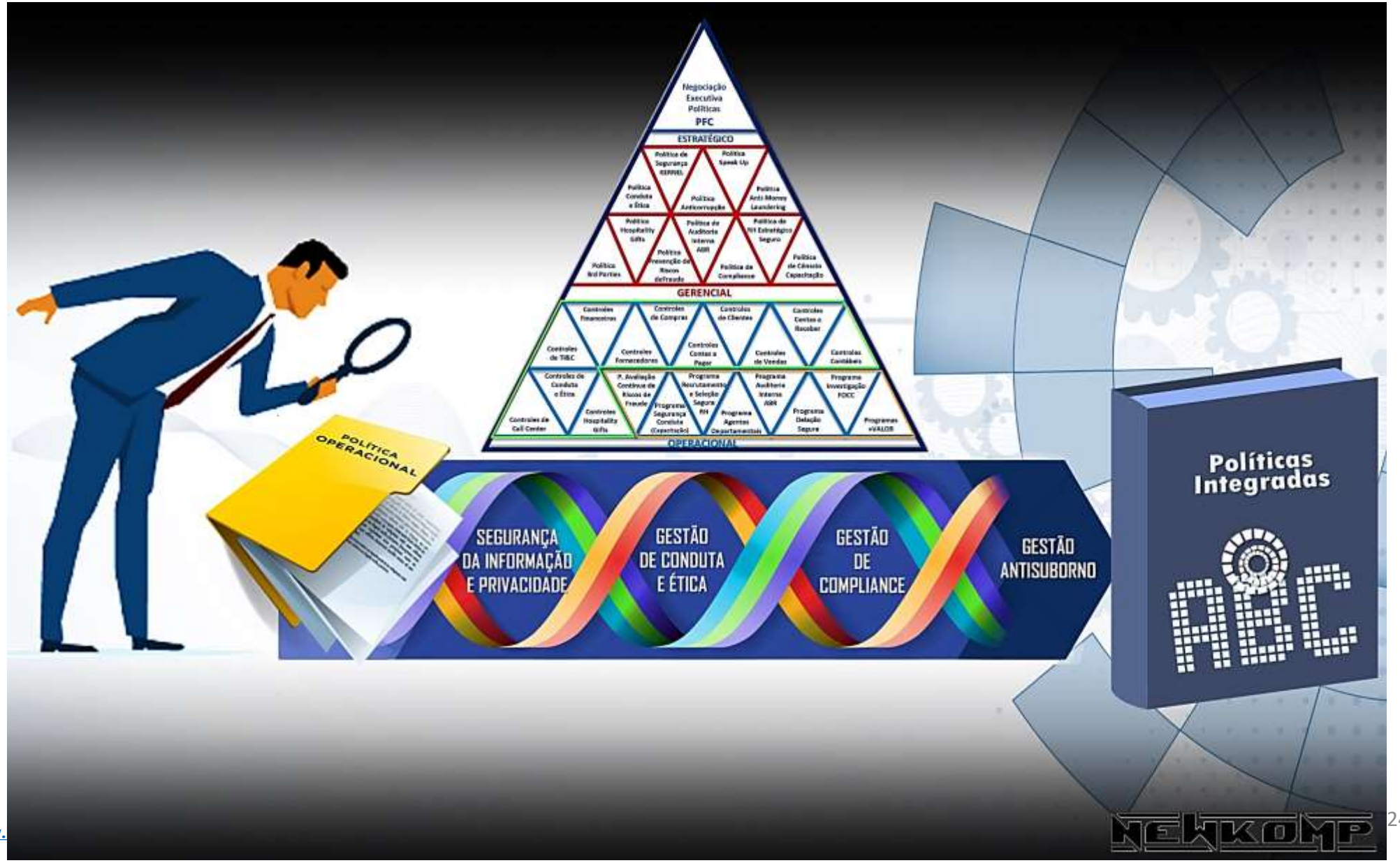
Gestão e Governança

- Todas as empresas praticam Gestão – algumas também Governança Operacional

Potencialização do uso de tecnologias da Informação

Políticas Integradas – Segurança, Compliance...

Para preparar um bom Programa de Integridade é fundamental unificar e alinhar as Políticas e Normas Internas.



Programas de Integridade Empresarial

VANÇADO

INTEGRIDADE BRASIL

20 passos para implementar um Programa de Integridade

01 Engajamento e Capacitação da Direção da Empresa sobre Compliance (Programa de Integridade no BRASIL)	10 Estabelecimento dos Processos Operacionais de Compliance	11 Definição da Política de Brindes Presentes e Hospitalidade	20 Aplicação Ciclo Contínuo de Avaliação PDCA sobre Compliance
02 Diagnóstico Estratégico e Operacional da Organização	09 Identificação e Revisão de Processos e Controles Internos	12 Definição da Política de Licitações, Contratos e "Due Diligence"	19 Aplicação Processos de Operação de Compliance. Monitoração e Auditoria ABR
03 Levantamento das fontes de obrigações e penalidades	08 Estabelecimento da Estrutura Organizacional de Compliance (Recursos Humanos e Materiais)	13 Definição da Política de Relacionamento com o Poder Público	18 Aplicação do Programa de Capacitação Operacional de Compliance
04 Definição de Políticas Segurança. Anticorrupção. Antisuborno. Compliance.	07 Estabelecimento e Aprovação do Programa de Compliance (ou Programa de Integridade)	14 Definição da Política de Medidas Disciplinares	17 Estabelecimento do Canal de Denúncias Segura. Investigações e Julgamentos
05 Mapeamento de Riscos. Identificação Análise - Avaliação	06 Matriz de Riscos. Seleção e Tratamento dos Riscos	15 Definição da Política de Comunicação Interna e Externa	16 Desenvolvimento e Aprovação do Código de Conduta Gerenciável

Gestão de Compliance no padrão Internacional

- ISO 19.600:2014”

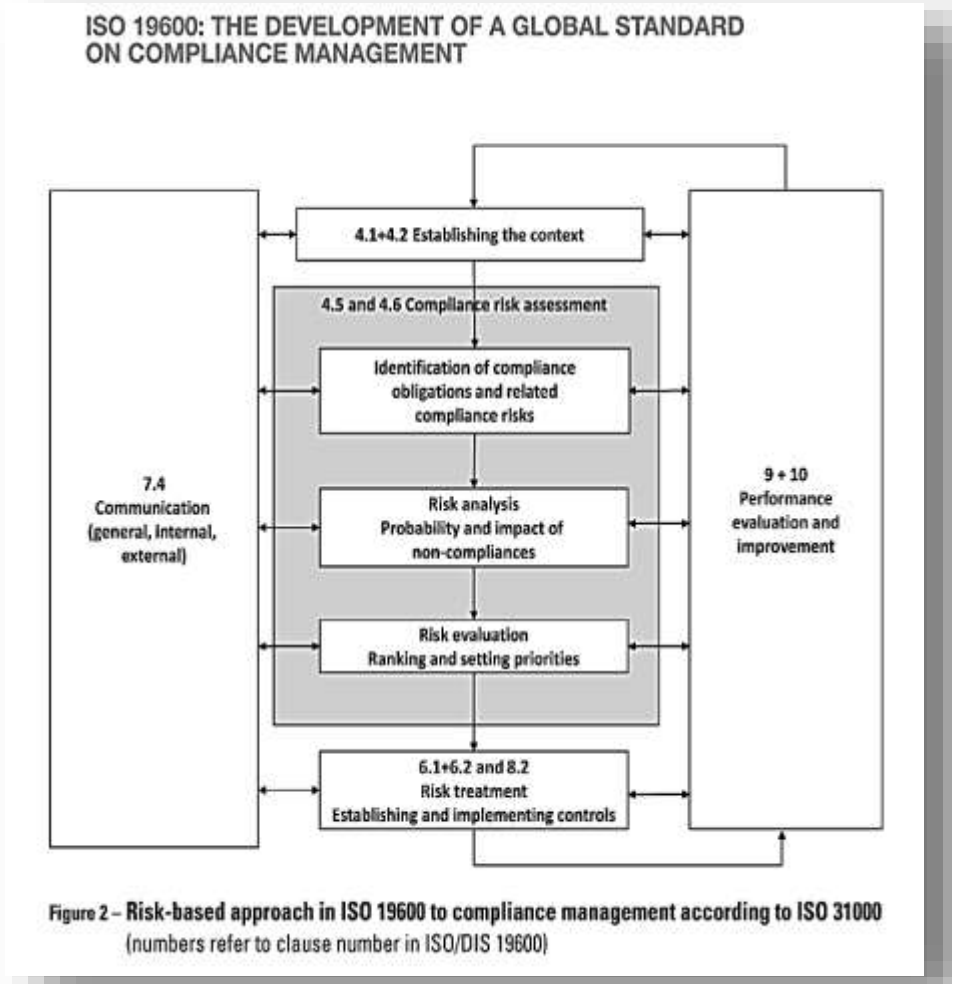
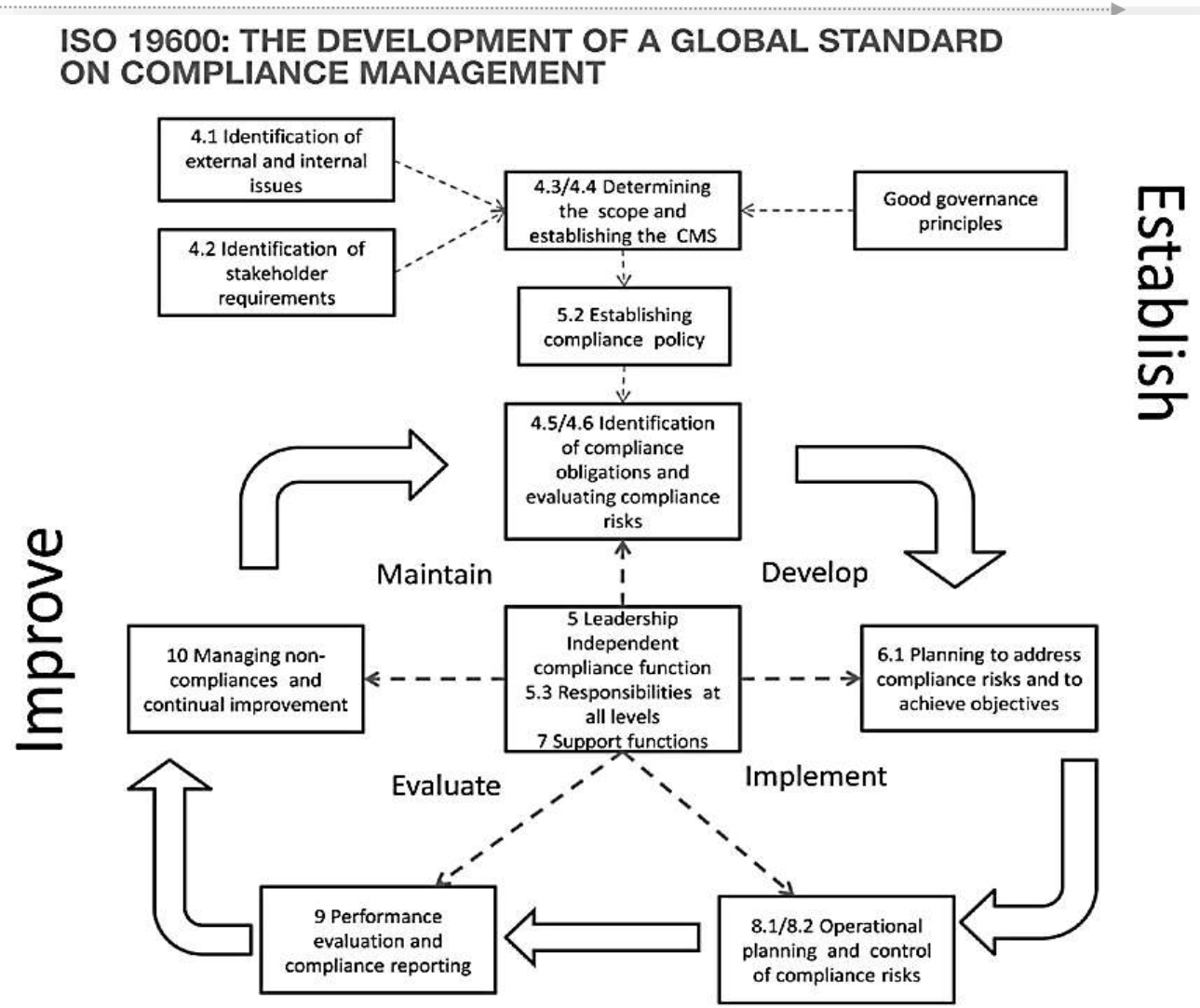


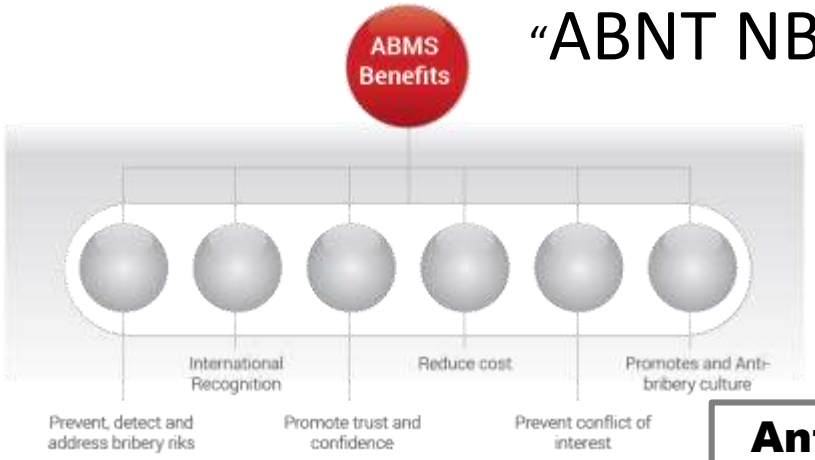
Figure 2 – Risk-based approach in ISO 19600 to compliance management according to ISO 31000 (numbers refer to clause number in ISO/DIS 19600)



relationship between the elements of compliance management according to ISO 19600
(numbers refer to clause number in ISO/DIS 19600)

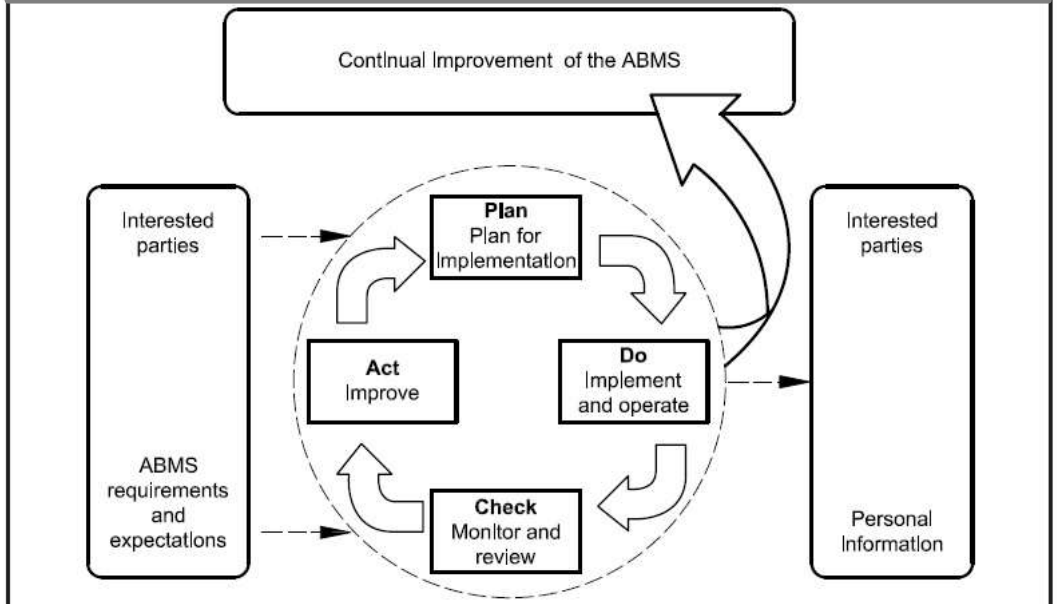
Gestão Antisuborno no padrão Internacional (UK)

"ABNT NBR ISO 37001:2016"



Padrão para Gestão Antisuborno, fundamentado na Lei Britânica Act 2010 (c.23 – UKBA) que abrange o direito penal relativo ao suborno.

Anti-bribery Management System (ABMS)



Plan	To plan for the implementation of an ABMS	Clause 3
Do	To implement the ABMS	Clause 4
Check	To monitor and review the ABMS	Clause 5
Act	To improve the ABMS	Clause 6

ISO/DIS 37001:

1. Context
2. Foreword
3. Terms and definitions
4. Context of the organization
4.1. Understanding the organization and its context
4.2. Understanding the needs and expectations of stakeholders
4.3. Determining the scope of the anti-bribery management system
4.4. Anti-bribery management system
4.5. Bribery risk assessment
5. Leadership
5.1. Leadership and commitment
5.1.1. Governing body
5.1.2. Top management
5.2. Anti-bribery policy
5.3. Organizational roles, responsibilities ad authorities
5.3.1. Roles and responsibilities
5.3.2. Anti-bribery compliance function
5.3.3. Delegated decision-making
6. Planning
6.1. Actions to address risk and opportunities
6.2. Anti-bribery objectives and planning to achieve them
7. Support
7.1. Resources
7.2. Competence
7.2.1. General
7.2.2 Employment procedures
7.3. Awareness and training
7.4. Communication
7.5. Documented information
7.5.1. General
7.5.2. Creating and updating
7.5.3. Control of documented information
8. Operation
8.1. Operational planning and control
8.2. Due diligence
8.3. Financial controls
8.4. Non-Financial controls
8.5. Implementation of anti-bribery controls by controlled organizations and by business associates
8.6. Anti-bribery contract terms
8.7. Gifts, hospitality, donations and similar benefits
8.8. Managing inadequacy of anti-bribery controls
8.9. Raising concerns
8.10. Investigating and dealing with bribery
9. Performance evaluation
9.1. Monitoring, measurement, analysis and evaluation
9.2. Review by anti-bribery compliance function
9.3. Internal audit
9.4. Top management review
9.5. Governing body review
10. Improvement
10.1. Nonconformity and corrective action
10.2. Continual improvement

Annex A (informative) - Guidance on the use of this International Standard

A.1. General
A.2. Scope of the anti-bribery management system
A.2.1. Standalone or integrated anti-bribery management system
A.2.2. Facilitation and extortion payments
A.3. Reasonable and proportionate
A.4. Bribery Risk Assessment
A.5. Roles and responsibilities of governing body and top management
A.6. Anti-bribery compliance function
A.7. Resources
A.8. Employment procedures
A.8.1. Due diligence on personnel
A.8.2. Performance bonuses
A.8.3. Conflicts of interest
A.8.4. Bribery of the organization's personnel
A.8.5. Temporary staff or workers
A.9. Awareness and training
A.10. Due diligence
A.11. Financial controls
A.12. Non-financial controls
A.13. Implementation of the anti-bribery management system by controlled organizations and business associates
A.13.1. General
A.13.2. Controlled organizations
A.13.3. Business associates
A.14. Anti-bribery commitments
A.15. Gifts, hospitality, donations and similar benefits
A.16. Internal audit
A.17. Documented information
A.18. Investigating and dealing with bribery
A.19. Monitoring
A.20. Public officials
A.21. Anti-bribery initiatives

Lei Internacional de Proteção de Dados GDPR

A Regulação Geral de Proteção de Dados (General Data Protection Regulation – GDPR) (Regulação EU 2016/679) é um Regulamento/Lei da União Europeia de abril de 2016 para substituir a Diretiva 95/46/EC ou Diretiva Europeia de Proteção de Dados Pessoais.
A Regulação recebeu uma "vacatio legis" (tempo decorrido da publicação de uma lei e o dia em que ela entra em vigor) de 24 meses, portanto passou a ser exigida somente a partir de **25 de maio de 2018**, efetivamente substituindo a antiga Diretiva.

A Regulação terá um efeito global, uma vez que ela se aplica a empresas que processam dados pessoais, mesmo quando o tratamento se dá fora da limitação geográfica da União Europeia.

Disponível < http://www.profissionaldeecommerce.com.br/lei-nacional-de-protecao-de-dados/ >
e < https://ico.org.uk/media/16824219/preparing-for-the-gdpr-12-steps.pdf > acessos em 10/07/2018.

LGPD Brasil – PLC 53/2018

A lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet), 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 ao cenário de inovação tecnológica, com respeito a direitos, em alinhamento a recente atualização da regulamentação europeia GDPR.

Disponível em < https://www12.senado.leg.br/noticias/materias/2018/07/03/regras-para-protecao-de-dados-pessoais-sao-aprovadas-e-vao-a-plenario > acesso 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

Lei Geral de Proteção de Dados – LGPD Brasil

O "Portal da Privacidade"* publicado na internet pelo escritório do amigo "Renato Opice Blum", divulga o "Infográfico: Conheça os 12 principais pontos sobre a LGPD", aposto ao lado, 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 sancionada, com multas para o descumprimento que podem 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/ > acessos em 11/07/2018.

Certificações de Conformidade Anticorrupção

Conformidade:

- Certificação (com Acreditação)
  - C[illegible]

IBC Instituto Brasileiro de Compliance

RINA 1861

BRA certificadora — PROGRAMA DE CERTIFICAÇÃO SISTEMA DE GESTÃO ANTICORRUPÇÃO

[illegible]ia

HIC Intelligence — ANTI-CORRUPTION COMPLIANCE PROGRAM

EBANC Empresa Brasileira Acreditadora de Norma de Compliance

EMPRESA PRÓ ÉTICA — CGU — INSTITUTO ETHOS

PROCESSOS VALIDADOS — NEWKOMP

PROCESSOS OPERACIONAIS = VALIDADOS = — 2 Überconsult

apcer ISO 9001 — IQNet MANAGEMENT SYSTEM

INMETRO

http://www.cgu.gov.br/assuntos/etica-e-integridade/empresa-pro-etica/arquivos/documentos-e-manuais/regulamento-2017.pdf

e-Book “COMPLIANCE URGENTE”

Pré-lançamento

INSTITUTO DE ENGENHARIA 1916

exclusivo para os participantes

Encaminhe e-mail contendo:
Assunto = “e-book IE”
Nome completo
Empresa onde trabalha

kontato@komp.com.br

Obrigado!!!

Esteja COMPLIANCE e ajude a combater a CORRUPÇÃO.

João Roberto Peres
jperes@komp.com.br

9 de dezembro - Dia Internacional contra a Corrupção