I ConGRC

Conferência Nacional de Governança, Riscos e Compliance.

Rumo a um novo Brasil.

CONGRC2018
I Conferência Nacional:
Governança, Riscos e Compliance

APOIO:

IBGRC

JML

Apresentação

Não é de hoje que muito se fala em governança, riscos, conformidade. As teorias estão por aí, basta abrir o google, digitar o tema desejado, selecionar um ou dois arquivos e estudá-los.

O acesso fácil às informações é sempre bom e deve ser estimulado. Contudo, a impressão que tenho é a de que se tem cada vez menos tempo para cada vez mais informação disponível. Para dificultar ainda mais, as respostas têm sido exigidas com cada vez mais urgência, fato que contribui para diminuir a já escassa disponibilidade de tempo.

Traga estes fatos para o ambiente organizacional e some-os às restrições de pessoas e orçamento e pronto: tem-se a realidade se tornando cada vez mais restritiva. Por outro lado, a Constituição Federal exige-nos eficiência e eficácia. Ainda mais importante, a sociedade carece que sejamos eficientes e eficazes!

Ao se considerar os problemas advindos da convergência dos termos expostos - governança, riscos, conformidade, informação, recursos humanos, tempo, orçamento, restrição, resposta, eficiência, eficácia, sociedade, carência - surge uma pergunta. Uma questão que passa pela cabeça de todos os servidores públicos cônscios de seu papel: como fazer mais e melhor com menos? Tenho a certeza de que, ainda que de forma inconsciente, todos queremos isto. E cada um de nós, ao seu próprio modo, encontra um conjunto de respostas.

A minha resposta começou em 2007, quando fui nomeado no Tribunal Superior do Trabalho. Nos trabalhos que fiz tentei otimizar tempo, seja criando procedimentos formais, seja automatizando atividades, seja disseminando conhecimentos.

Para resumir, em 2014 comecei a capacitar pessoas em governança, controles internos, contratação de soluções de TI, gestão de riscos, conformidade, governança de TI. Tudo fruto dos conhecimentos que adquiri e implementei no TST. Não tem jeito, Paulo Freire já havia avisado: "Quem ensina aprende ao ensinar". Mais cedo ou mais tarde você vê que está tudo interligado, e mais: passa a enxergar os pontos de conexão entre todos estes temas.

Entendi que um de meus propósitos seria disseminar conhecimento, conectar pessoas e, assim, trazer mais um pouco de eficiência para o serviço público. Afinal porque não criar atalhos aproveitando o conhecimento de quem já resolveu um problema?

Assim surgiu a ideia da ConGRC: Conferência Nacional de Governança, Riscos e Compliance, juntando pessoas com conhecimento prático, que já resolveu ou está resolvendo problemas em suas instituições. Acadêmicos, servidores públicos dos três poderes e dos três níveis de governo, pessoal da iniciativa privada, todos trocando ideias, compartilhando soluções.

Daí para a execução da Conferência foi relativamente simples, todas as pessoas consultadas, público, parceiros, palestrantes, foram solícitos e mesmo diante de imprevistos não se abalaram.

A JML foi o primeiro parceiro a acreditar no evento e o apoiou fortemente com conselhos, ideias, sugestão de palestrantes, impressão de bloco de notas e a cereja do bolo: a diagramação e distribuição gratuita deste e-book!

Algumas informações sobre a nossa I Conferência Nacional: Governança, Riscos e Compliance – ConGRC 2018:

- **Data de realização:** 4 e 5 de outubro de 2018.
- **Local:** Instituto Serzedello Corrêa, Escola Superior do Tribunal de Contas da União. Brasília – DF.
- **1.087** inscrições.
- Média de **570 pessoas** nos dois dias do evento.
- **42** palestras e workshops.
- **4** ambientes.
- Por fim, não posso deixar de agradecer a todos os envolvidos direta e indiretamente, palestrantes, pessoal do **TST** e do **ISC**, parceiros, amigos, família!

Sandro Tomazele

- Criador e organizador da ConGRC: Conferência Nacional: Governança, Riscos e Compliance. A primeira edição ocorreu em 4 e 5/10/2018 no Instituto Serzedello Corrêa em Brasília-DF. Contou com mais de 40 conferencistas, ocorreu em 4 ambientes simultâneos, teve mais de 1.000 inscritos e público médio presente de 570 pessoas nos dois dias.
- Membro do Comitê de Governança das Corporações da ABNT – Associação Brasileira de Normas Técnicas.
- Membro do Comitê de Gestão de Riscos da ABNT – Associação Brasileira de Normas Técnicas.
- Fundador do IBGRC – Instituto Brasileiro de Governança, Riscos e Compliance.
- Analista Judiciário – Especialidade Analista de Sistemas. Desde 1/3/2011. Supervisor da Seção de Gestão da Segurança da Informação do TST – Tribunal Superior do Trabalho. Foi Coordenador Substituto da Coordenadoria de Apoio à Governança e Gestão de TIC entre 2012 e 2018. Desenvolvi e implantei o modelo de gestão de riscos corporativos do TST. Coordena o Comitê Gestor de Riscos de TI e o Escritório de Riscos Corporativos e componho o Comitê Gestor de Riscos Corporativos.

Apresentações disponibilizadas:

01. Transform GRC to IRM

Hamilton Felix invested the last 25 years in IT Business as Client, Vendor and Entrepreneur. Now he wants to share how Gartner could inspire the CEOs and Executives of high-tech and telecom providers to take advantage of our insights and advice.

02. Gestão de Riscos para a Efetividade do Programa de Compliance

Naiara Augusto

Especialista em Direito Penal e Processual Penal, Propriedade Intelectual, Direito Cibernético, Direito Corporativo e Compliance, com certificação em ISO 37001:2017 e Sistema de Gestão Antissuborno, com qualificação em governança corporativa, gestão estratégica, gestão de processos e projetos, em técnicas de negociação, em combate à corrupção e lavagem de dinheiro via PNLD do Ministério da Justiça, em investigação forense científica, com cursos em Ciência de Dados, Introduction to American Law pela University of Pennsylvania, Strategic management pela Copenhagen Business School, Property and Liability: An Introduction to Law and Economics pela Wesleyan University, atualmente cursando MBA em Inovação Jurídica e em formação no Program on Corporate Compliance and Enforcement em NY/USA, e membro de grupos de estudo sobre Compliance no Brasil e América Latina.

Experiência na implantação de programas de Compliance em pequenas e grandes empresas. Responsável pro bono pelo programa de Integridade no Movimento Acredito, associação que conta mais de 12 mil colaboradores.

03. Governança e Compliance. Um Pensamento Integrado e Sistêmico

Celia Lima Negrão

Especialista em Direito e Processo do Trabalho, em Gestão Estratégica Empresarial pela Universidade de São Paulo- USP e cursando o MBA em Governança e Compliance pela Universidade de Brasília. Certificada em Gestão de Projetos pelo Project Management Institute – PM. Bacharel em Administração e Habilitação em Ciência e Tecnologia. Coautora do livro Compliance, Controles Internos e Riscos, 2ªEdição, Ed. Senac. Produz semanalmente vídeos no Canal do Professor Jacoby Fernandes, no youtube, sobre Governança, compliance, programa de integridade, riscos e controles internos.

Participou de diversos eventos sobre Compliance e Riscos e do Canadian Fraud Conference, considerado o maior evento de compliance e prevenção às fraudes, realizado no Canadá, pela ACFE. Experiência nas áreas de gestão de projetos corporativos, tecnologia, gestão de pessoas e auditoria interna. Atuação em projetos de auditoria na área de licitações e contratações. Coordenou os trabalhos de auditoria voltados à implementação de programa de prevenção às fraudes dos correios, de mecanismos de compliance e riscos na área de gestão de pessoas, tendo realizado estudos junto às

empresas Vale, Siemens, Banco do Brasil, Bradesco, Banco Central, CPFL, dentre outras. Participou do grupo de implementação do modelo de sistema de controle interno para os Correios e do Grupo de Governança para às adequações dos Correios à Lei 13.303/2016. Coordenou e participou de grupos para implementação e estruturação da Empresa de Participações dos Correios – CorreiosPar, com foco na estruturação dos mecanismos da governança corporativa, controles e riscos, desenvolvimento de processos de constituição e aquisições de empresas (M&A), secretariado aos órgãos de Governança, Conselho de Administração e Fiscal, planos e processos orçamentários e financeiros e coordenação dos assuntos referentes à atualização do estatuto da CorreiosPar à Lei 13.303/2016, bem como seus desdobramentos no âmbito da Empresa. Atuou como assessora da Vice-Presidência de Administração dos Correios, em ações estratégicas de implementação dos Centros de Serviços Compartilhados (CSC), Relatórios de Gestão e de Administração, Prestação de Contas, auditorias externas (CGU/TCU) e Coordenação da Implantação do Projeto E-social nos Correios. Atualmente, como assessora na área de Relacionamento Institucional, da Presidência dos Correios, que abrange atividades de relacionamento com o governo, com instituições e organismos internacionais, sustentabilidade empresarial, transparência e demandas de auditoria dos órgãos de controle externo (TCU/CGU).

04. Como mitigar riscos com a implantação de esteira de entrega contínua de software

Claudson Melo

Formado em sistemas de informação, com pós-graduação em engenharia de software e cursando pós-graduação em Inteligência Artificial.

Sou adepto da filosofia lean e de métodos ágeis.

Gosto de promover iniciativas com propósitos claros e que gerem engajamento nas equipes, com foco na simplificação e na automação de processos de desenvolvimento de software.

Desde 2009, tenho trabalhado com contratações de serviços de desenvolvimento e sustentação de sistemas, processo de desenvolvimento de software, métricas e qualidade de software. Com minha equipe, criamos a métrica de ponto de especificação por exemplo – PEEX, em uso com a atual fábrica de software.

Em 2017, começamos projeto de disseminação da cultura Devops no TST e já temos projeto piloto em pleno funcionamento.

No momento, sou responsável pela definição de modelo de contratação de soluções cognitivas (ciência de dados) com CRISP-DM e Scrum, no âmbito do TST.

Praticante de diversos esportes (corrida, ciclismo, natação, futvolei, vôlei...); adoro curtir e respeitar a natureza e de, também, tocar instrumentos musicais (violão, teclado e violino).

Casado há 20 anos com a Adriana, grande companheira que tem me apoiado em todas iniciativas que tenho me envolvido, graças a Deus!

05. Resultados e Lições aprendidas de uma equipe que já sabia contratar

Antônio Fernandes Soares Netto

Mestre em Engenharia Elétrica pela Universidade de Brasília, na temática de Gestão de Riscos nas Contratações Públicas (doutorado em andamento). Consultor, Palestrante, Parecerista e autor de artigos da temática de Contratações de bens e serviços e Contratos Administrativos. Criador do Jogo de Contratações e da plataforma de capacitação de gestores públicos JOGOGOV. Autor da obra: Contratações de Tecnologia da Informação: O Jogo. Atualmente é Coordenador de Planejamento e Gestão Estratégica da Advocacia-Geral da União, onde atua com os temas de Gestão de Riscos, Planejamento de Contratações de TIC, Projetos, Processos e Governança. Professor na ENAP. Coach pelo Neuroleadership Institute e formação em gamification pela Pennsylvania University (EUA). Certificações: COBIT 5 e ITILF. Antes de ingressar no serviço público, atuou no mercado privado pela Xerox e GVT.

06. Implementando a Gestão de Riscos no Setor Público

Rodrigo Fontenelle de Araújo Miranda

Graduado em Ciências Econômicas, pela UFMG. Especialista em Gestão de Negócios com ênfase em Finanças pelo IBEMEC. Mestre em Contabilidade pela UnB. Especialista em Auditoria Financeira pela UnB. Professor de várias instituições de ensino entre elas, Universidade do Estado de Minas Gerais, Faculdade Serrana de Ensino Superior, Universidade de Brasília, Escola de Administração Fazendária, Instituto de Gestão, Economia e Políticas Públicas. É professor da Fundação Getúlio Vargas – FGV, na cadeira de Controles Internos II. Foi membro do Conselho de Administração da Companhia Urbanizadora da Nova Capital do Brasil, Chefe de Divisão da Coordenação-Geral de Auditoria da Área Fazendária da CGU, Coordenador-Geral de Auditoria da Área Fazendária da CGU, Assessor Especial de Controle Interno do Ministro da Fazenda, Membro do Conselho de Administração da Indústrias Nucleares do Brasil – INB. É Membro do Conselho de Administração da Casa da Moeda do Brasil – CMB. Atualmente ocupa o cargo de Chefe da Assessoria Especial de Controle Interno do Ministério do Planejamento, Desenvolvimento e Gestão.

07. Governança nas compras públicas. Iniciativas do Ministério do Planejamento

Virgínia Bracarense Lopes

Experiência no setor público, especificamente na área de recursos logísticos e compras públicas; acompanhamento e assessoramento em contratações; coordenação e acompanhamento de projetos; auxílio nas funções de planejamento e gestão orçamentária/contratual.

Especializações: licitações e contratações públicas, compras públicas sustentáveis, logística do setor público, gerenciamento de projetos.

08. Programas de Complianc. Por onde começar?

Mariângela Mattia

Advogada formada pela Faculdade de Direito da Universidade Federal do Mato Grosso (UFMT); Pós-graduada em Marketing e Comunicação pela FIA/USP; Especialista em Compliance e Governança pela Universidade de Brasília (UNB); Assessora na Diretoria de Controles Internos e Compliance do Banco do Brasil; e Membra da Comissão de Legislação, Anticorrupção e Compliance da OAB/DF.

09. O Projeto Cesta de Materiais e a Retomada do Controle de Estoque no TRT 3ª Região

Paulo Sérgio Barbosa Carvalho

Mestre em Administração pela Faculdade de Ciências Empresariais da Universidade FUMEC – Fundação Mineira de Educação e Cultura (Área de Concentração em Gestão Estratégica de Organizações); Pós-Graduado em: Administração do Comércio Exterior pela Faculdade de Ciências Gerenciais da UNA/CEPEDERH/MG; Direito de Empresa pela Pontifícia Universidade Católica de Minas Gerais; Direito de Empresa pela Universidade Gama Filho/RJ e Centro de Atualização em Direito CAD/MG; Direito da Economia e da Empresa pela Fundação Getúlio Vargas/MG; Licitações e Contratos Administrativos pelo Centro Universitário UMA/MG; Administração Pública com ênfase em Gestão Pública pela Fundação João Pinheiro/MG; Graduado em Direito pela Faculdade de Direito Milton Campos/MG; Analista Judiciário do TRT da 3ª Região (out./2006); Assistente de Desembargador (dez./06- ago./12); Assessor Jurídico de Licitações e Contratos da Diretoria-Geral (set./12-mar./15); Assessor de Desembargador (abr.-dez./15); Diretor-Geral do Tribunal Regional do Trabalho de Minas Gerais (biênio 2018/2019); Professor de Pós-graduação do CEDIN desde 2016 (FA/MG).

10. Gestão de Riscos Corporativos

Wildenildo Oliveira dos Santos

Administrador, servidor do quadro efetivo da Agência Nacional de Vigilância Sanitária – Anvisa, Analista Administrativo, desde 2007. Bacharel em Administração pela Universidade Federal do Piauí (2004); Especialista em Administração Pública pela Universidade Federal do Piauí (2005); Especialista em Vigilância Sanitária pela Fundação Instituto Oswaldo Cruz (2011); Especialista em Gestão da Vigilância Sanitária pelo Instituto Sírio Libanês de Ensino e Pesquisa (2012). Tem experiência na área de Administração, com ênfase em Administração Pública, Gestão da Qualidade Regulatória, Gestão da Qualidade em Processos Organizacionais e Gestão de Riscos Corporativos na Anvisa.

Fabiano Ferreira de Araújo

Especialista em Gestão da Vigilância Sanitária, 2012, graduado em Administração pela Universidade de Brasília (2002). Servidor da ANVISA (desde 2007), Coordenador de Gestão da Qualidade em Processos Organizacionais na Assessoria de Planejamento da Anvisa, desde 2010. Tendo atuado como analista de meios eletrônicos sênior em empresa do ramo de Seguros e Professor Colaborador da Universidade de Brasília e tutor na Universidade Aberta do Brasil.

Mary Anne Fontenele Martins

Graduação em Enfermagem, Mestrado em Saúde Pública. Especialista em Regulação e Vigilância Sanitária da Agência Nacional de Vigilância Sanitária (Anvisa), desde 2005. Atuação na Gerencia Geral de Regulação Econômica, participação na equipe de elaboração do Plano Diretor de Vigilância Sanitária, e na organização da Secretaria Executiva do Conselho Consultivo da Anvisa. Ouvidora substituta da Agência (2007-2010) e Gerente Geral da área responsável pelo registro de Saneantes da Anvisa (2011-2012). Desde 2013, na Assessoria de Planejamento, responsável pela elaboração/monitoramento do Contrato de Gestão e do Relatório de Gestão da Anvisa. Coordenação e articulação dos projetos de cooperação técnica com os organismos internacionais (OPAS e PNUD). Coordenação do processo de elaboração da Política de Gestão de Riscos da Anvisa e sua implantação.

Patrícia Fernanda Toledo Barbosa

Médica, especialista em regulação e vigilância sanitária da Agência Nacional de Vigilância Sanitária. Coordenadora de Vigilância em Serviços Sentinela. Tem experiência na área de atenção à Saúde, como médica, com atuações na área de Clínica Médica e Medicina de Família e Comunidade; experiência de gestão em saúde - Programas de Saúde Pública, Gestão Hospitalar, Controle, Avaliação e Auditoria.

11. Gestão de Riscos Corporativos. O caso de uma agência reguladora de saúde

Fabiano Ferreira de Araújo

Especialista em Gestão da Vigilância Sanitária, 2012, graduado em Administração pela Universidade de Brasília (2002). Servidor da ANVISA (desde 2007), Coordenador de Gestão da Qualidade em Processos Organizacionais na Assessoria de Planejamento da Anvisa, desde 2010. Tendo atuado como analista de meios eletrônicos sênior em empresa do ramo de Seguros e Professor Colaborador da Universidade de Brasília e tutor na Universidade Aberta do Brasil.

12. Gestão de Riscos em Projetos

José Flávio Albernaz Mundim

Formado em Engenharia Civil e Filosofia pela Universidade de Brasília, MBA em Gerenciamento de Projetos pela FGV, mestrando em Governança e Desenvolvimento pela ENAP. Servidor do Tribunal Superior do Trabalho, atualmente, exercendo a função de Assessor Técnico na Secretaria Especial de Assuntos Estratégicos da Presidência da República. Atuou por cerca de 25 anos na área de TIC como desenvolvedor de sistemas, gerente de projetos, gestor de unidades de planejamento, escritório de projetos e governança, e como Secretário substituto da unidade de TIC do TST.

13. Data Protection for Vertical Markets

Edson Carlotti

Develop and implement innovative solutions to accelerate business growth by creating a disruptive, high-performance culture, focusing on efficient management, reducing time to market and improving shareholder outcomes.

Specialties:

- Information Security Expert (with focus on Data);
- Application Security and Secure Software Development Expert;
- EAI (Enterprise Application Integration) Expert;
- BPM (Business Process Modeling) Specialist;
- Network and Communications Expert;
- Software Architecture Engineer;
- Software Quality Assurance Specialist;
- Software Development Methodology Specialist;

14. Compliance na Esfera Trabalhista

Juliana Dato Ferreira Leal

Sócia no Escritório Petrarca Advogados; Especialista em Compliance do setor privado com ênfase em conformidades Trabalhistas; Controller Jurídico; Diretora Social do Instituto Brasileiro de Governança, Riscos e Compliance - IBGRC; Inscrita na Ordem dos Advogados do Brasil na Seção do Distrito Federal; Diretora Social do Clube dos Advogados do Distrito Federal triênio 2016/2018; Membro da Diretoria na Comissão de Legislação Anticorrupção e Compliance da OAB/DF; Graduada pelo Centro Universitário de Desenvolvimento do Centro Oeste - UNIDESC; Estagiou no Ministério Público do Estado de Goiás, na Promotoria da Infância e Juventude.

Listagem de todos os palestrantes:

- Ministro Augusto Nardes
- Dr. Medina Osório
- Alexandre Vargas
- Amanda Ramalho
- Ana Cláudia Mendonça
- Anna Dantas
- Antônio Netto
- Ary Lopes
- Asclepius Soares
- Carlos Athayde Valadares Viegas
- Carolina Marques
- Celia Lima Negrão
- Claudson Melo
- Dalmo Jorge Lima Palmeira
- Denise Evangelista
- Edson Carlotti
- Eduardo Nery
- Fabiano Ferreira de Araújo
- Flávia Xavier Araujo
- Frank Ned Santa Cruz
- Gustavo Nardelli
- Izabela Frota Melo
- João Leão
- João Paulo Mota
- José Flávio Albernaz Mundim
- Juliana Dato
- Ketlin Feitosa
- Luciana Melo
- Luciano Dantas
- Lúcio Carlos de Pinho Filho
- Marcelo Almeida
- Mariângela Mattia
- Marisa de Souza Alonso
- Mary Anne Martins
- Michel Neves
- Mônica Venâncio
- Naiara Augusto
- Patrícia Toledo Barbosa
- Paulo Sérgio Barbosa Carvalho
- Renato Ribeiro Fenili
- Robnaldo Alves
- Rodrigo Fontenelle
- Sara Possidônio
- Thiago Bueno
- Tiago Beckert Isfer
- Tiago Peixoto
- Vinicius Braga
- Virgínia Bracarense
- Wildenildo Santos
- Wilmar de Castro

Apresentação 1:

Transform GRC to IRM

HAMILTON FELIX

Transform GRC to IRM

Hamilton Felix
HighTech & Telecom Providers – Director
(61) 98119-6146
hamilton.felix@gartner.com

Gartner

Transform GRC to IRM

Transform Governance, Risk and Compliance to Integrated Risk Management

John A. Wheeler
Sr Director, Advisory

Refreshed 8 May 2018,Published 6 October 2016 - ID G00314880 - 9 min read

FOUNDATIONAL This research is reviewed periodically for accuracy.

Supporting Key Initiative is Risk Management Program

Gartner

“Integrated risk management enables simplification, automation and integration of strategic, operational and IT risk management processes and data. Risk and security leaders should use Gartner's definition for IRM to structure risk management processes, functions and technology requirements.”

John A. Wheeler
Senior Director Advisory | IRM

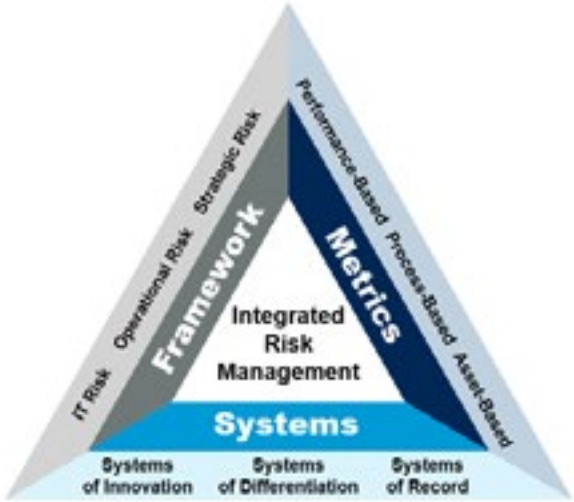
Gartner

IRM – Introduction

IRM is a set of practices and processes supported by a risk-aware culture and enabling technologies, that improves decision making and performance through an integrated view of how well an organization manages its unique set of risks.

- To understand the full scope of risk, organizations require a comprehensive view across all business units and risk and compliance functions, as well as key business partners, suppliers and outsourced entities. Developing this understanding requires risk and security leaders to address all six IRM attributes.
- Using Gartner's three dimensions of IRM — framework, metrics and you can increase the maturity of your risk management disciplines to mitigate the digital business risks of the future.

Three Dimensions of IRM



ID: 356175

Gartner

Risk Management Remains a High Priority for CEOs in 2018

In fact, 93% of CEOs and senior executives report that they plan to maintain or increase their legal, compliance and risk management investment

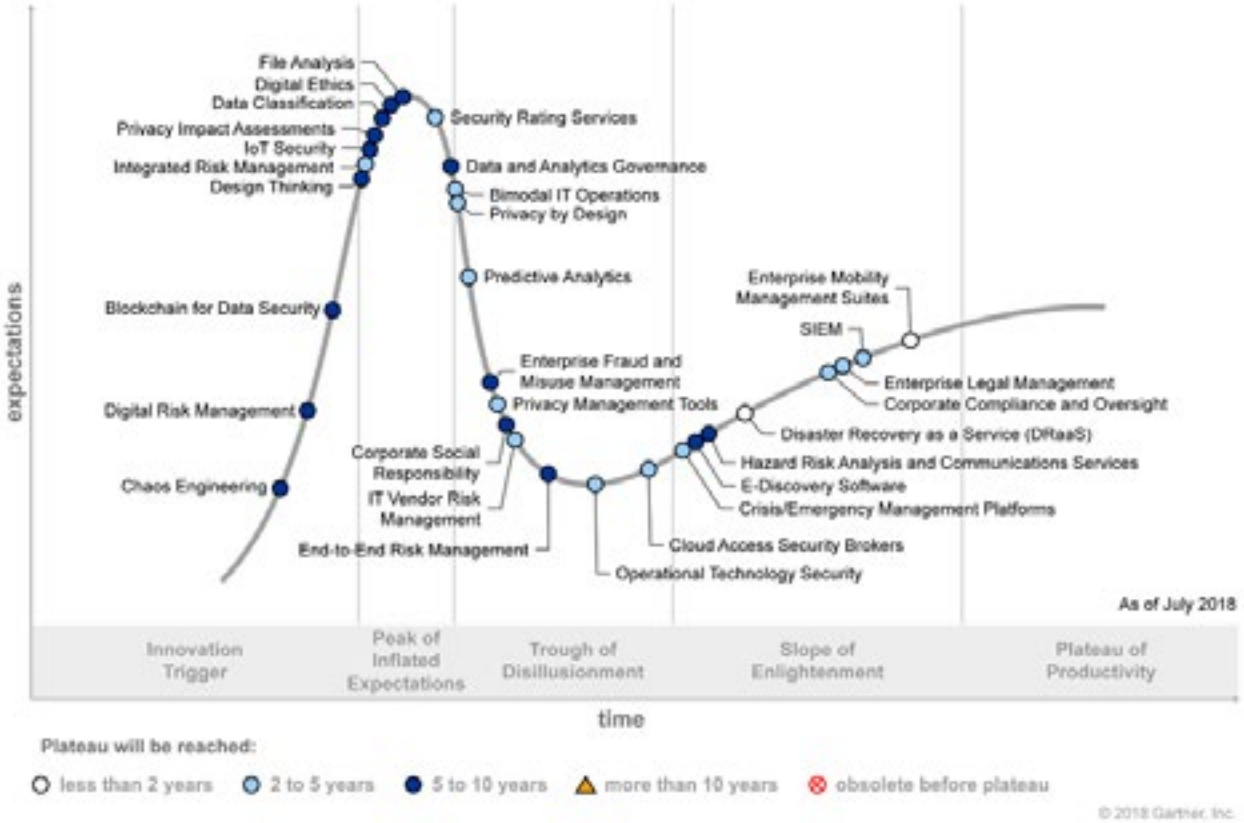
- Gartner end-user clients report via daily interactions that their governance, risk and compliance (GRC) solutions fail to meet the demands for cross-organization collaboration due to the fragmented use of GRC technology point solutions
- This fragmentation is a result of buying decisions made at a departmental rather than at an organizational level.
- As a result, the fragmented use requires a great deal of manual intervention to create an aggregated risk assessment to inform senior executive stakeholders for strategic decision-making purposes

Gartner

Gartner IRMS Research and Related Key Roles

Gartner

Hype Cycle for Risk Management, 2018



Gartner

IRM Solutions

By 2021, 50% of large enterprises will use an IRM solution set to provide better decision-making capabilities, up from 30% in 2017.

- Integrated risk management (IRM) solutions focus specifically on linking enterprise, operational and IT/cybersecurity management programs to enable better decision making.
- Mirroring program maturity, the technology required to manage risk has evolved over the past 15 years from single-mandate, compliance-driven software applications to more robust, risk-based solutions.
- IRM solutions can be very useful in managing the rapidly evolving set of cybersecurity and digital risks due to the related convergence of physical and technological risks.

Gartner

IRM Final Recommendations

Define and deploy leading risk indicators, and identify a limited set of risk indicators that serve as "early warnings," rather than measures of past risk events.

Integrate cybersecurity and technology risks with broader operational risk, focusing on areas that are tied to strategic objectives to ensure that risk oversight is "forward looking."

Organize for enterprise wide risk identification and accountability, and be explicit as to how the company communicates risk information and assigns risk ownership.

Use IRM solutions to inform better decision making, without allowing IRM to be viewed as a panacea for weak risk oversight and/or risk management practices

Gartner

Leadership Vision: Security and Risk Management

- Key components of an effective digital security vision and strategy
- Requirements for digital security programs
- Drivers that will shape security strategy in 2019

Is your organization truly safe? Digital business continues to challenge the conventions of risk and security management. IT leaders must develop a clear vision and strategy that enable a coherent digital security program. This webinar unlocks what constitutes an effective digital security vision and strategy, the elements you need for your digital security program, and the drivers that will shape security strategy in 2019.

Gartner

2018 Risk Management Leadership Vision

30 de Outubro às 12:00 (Horario de Brasilia)

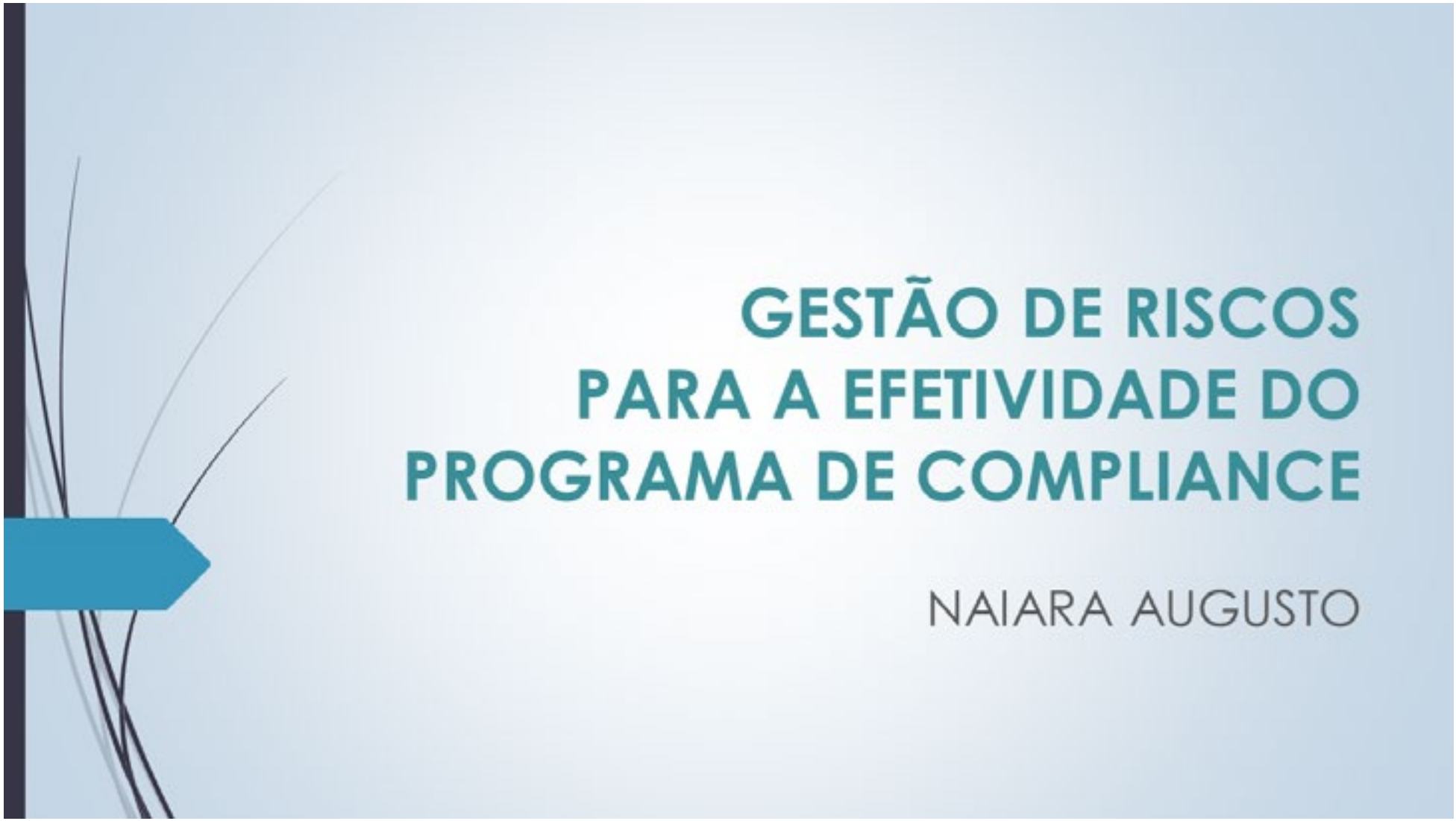
Jeffrey Wheatman
Research VP

Gartner

Apresentação 2:

Gestão de Riscos para a Efetividade do Programa de Compliance

NAIARA AUGUSTO


GESTÃO DE RISCOS
PARA A EFETIVIDADE DO
PROGRAMA DE COMPLIANCE
NAIARA AUGUSTO


IMPORTÂNCIA DO TEMA
GOVERNANÇA CORPORATIVA
GERENCIAMENTO DE RISCOS
PROGRAMA DE COMPLIANCE

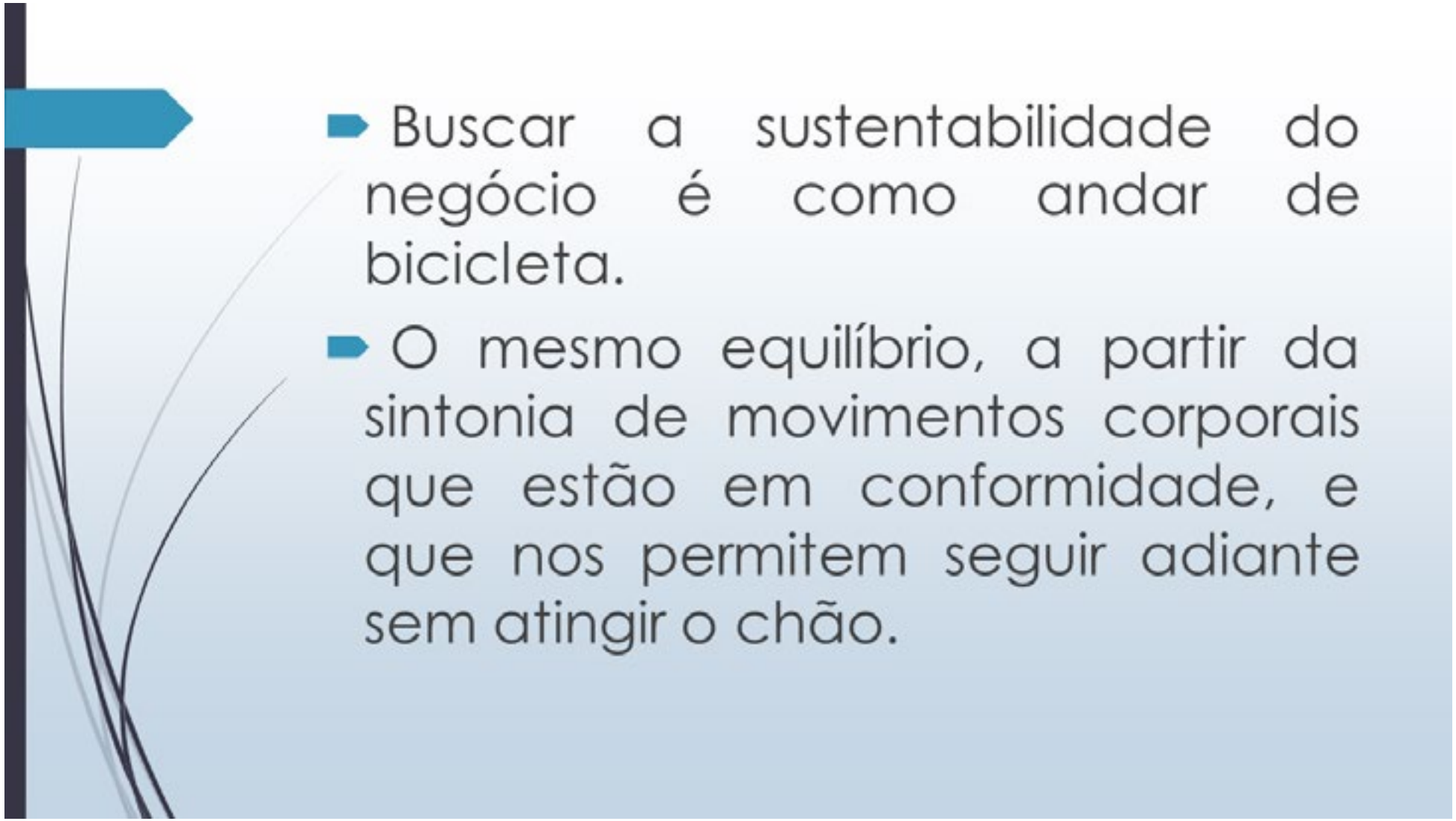

FALANDO SOBRE
GESTÃO DE
RISCOS...

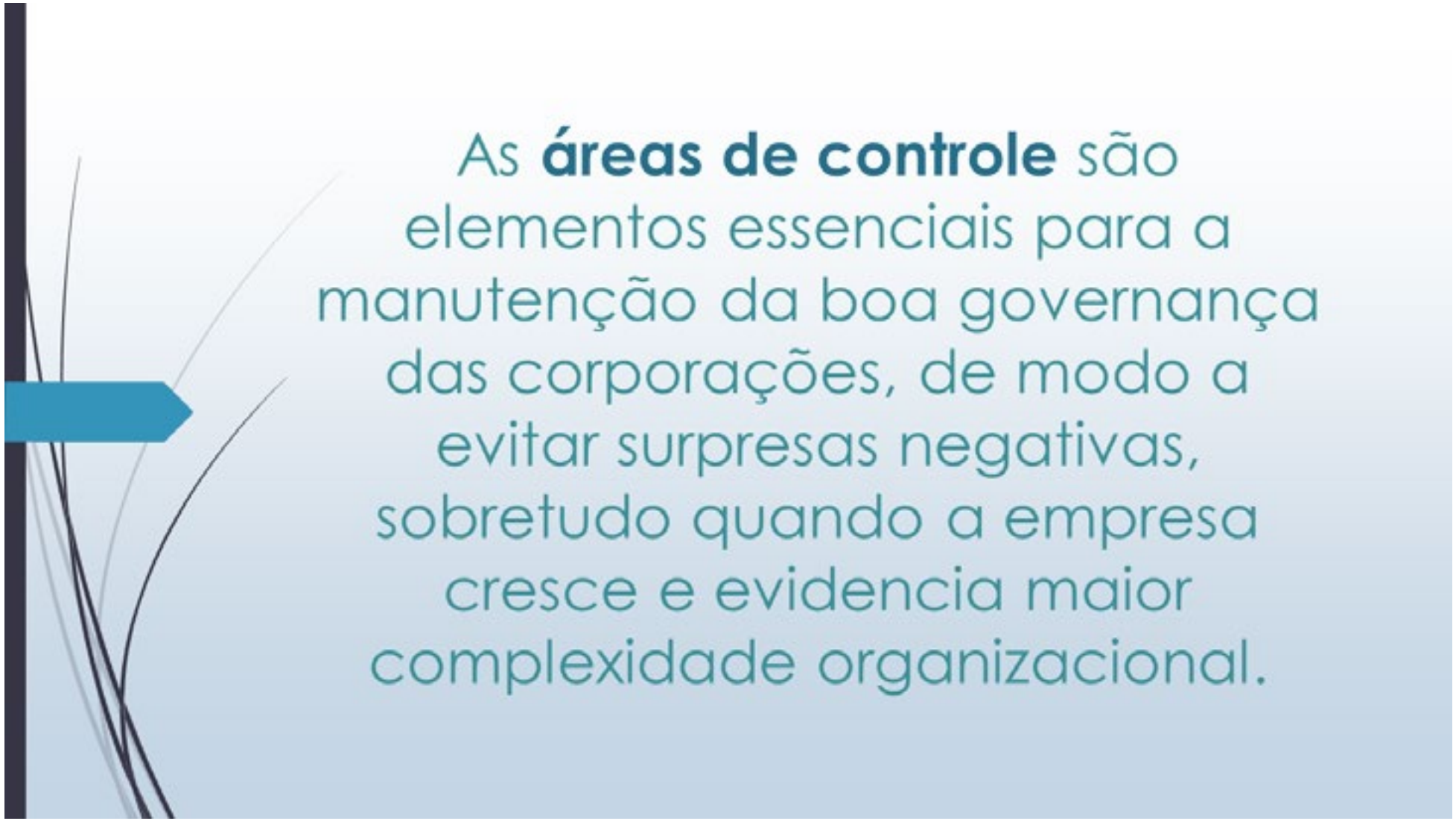

SOMOS GESTORES
DE RISCOS POR
NATUREZA


DESENVOLVIMENTO
PESSOA FÍSICA X
PESSOA JURÍDICA

SEGURANÇA

VELOCIDADE


Buscar a sustentabilidade do negócio é como andar de bicicleta.
O mesmo equilíbrio, a partir da sintonia de movimentos corporais que estão em conformidade, e que nos permitem seguir adiante sem atingir o chão.

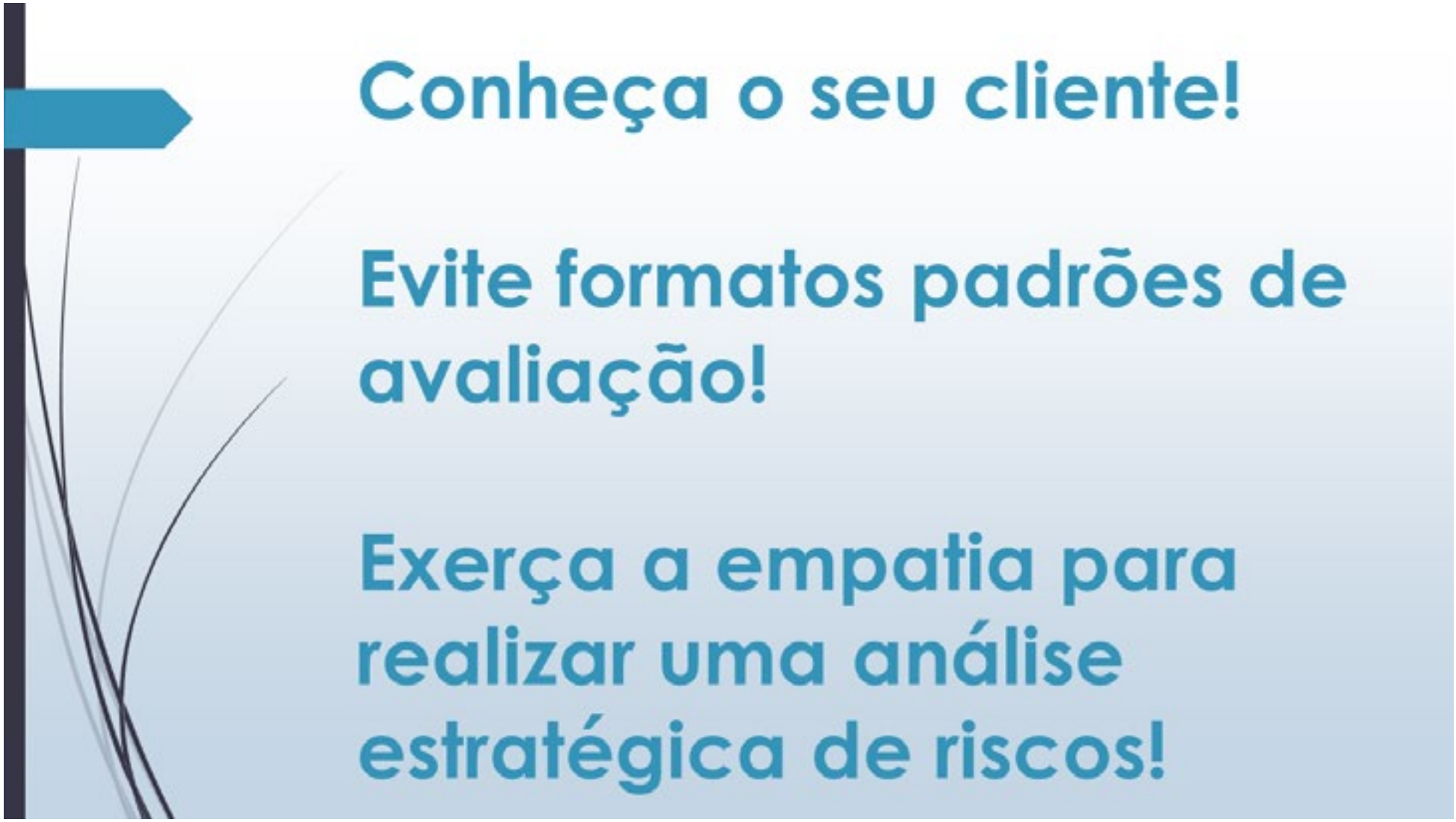

As **áreas de controle** são
elementos essenciais para a
manutenção da boa governança
das corporações, de modo a
evitar surpresas negativas,
sobretudo quando a empresa
cresce e evidencia maior
complexidade organizacional.


GESTÃO DE RISCOS EM TODAS AS ETAPAS, INCLUSIVE NO CRESCIMENTO....
ESPECIALMENTE NO RÁPIDO CRESCIMENTO!

CASO SADIA – R$ 3.8 bi prejuízos

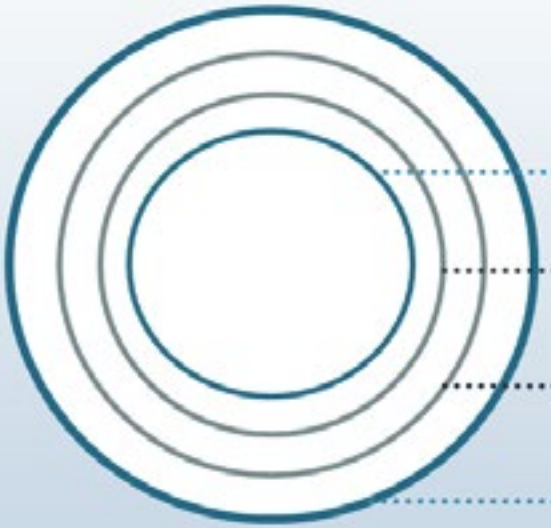
- CRESCIMENTO E RECEITA NOS ANOS IMEDIATAMENTE ANTERIORES AO COLAPSO
- 48% (2006 E 2008)
- FALHAS GRAVES NOS CONTROLES INTERNOS EM PERÍODO DE CRESCIMENTO


PONTOS DE REFERÊNCIA NA GESTÃO DE RISCOS
ORGANIZAÇÕES EM DIFERENTES ESTÁGIOS DE MATURIDADE
SINGULARIDADE DO PLANEJAMENTO ESTRATÉGICO
APETITE POR RISCOS


Conheça o seu cliente!
Evite formatos padrões de avaliação!
Exerça a empatia para realizar uma análise estratégica de riscos!


O começo...
Missão – Visão – Valores
(DNA da empresa)

ESTRUTURA ORGANIZACIONAL



Propósito (Por que fazemos)

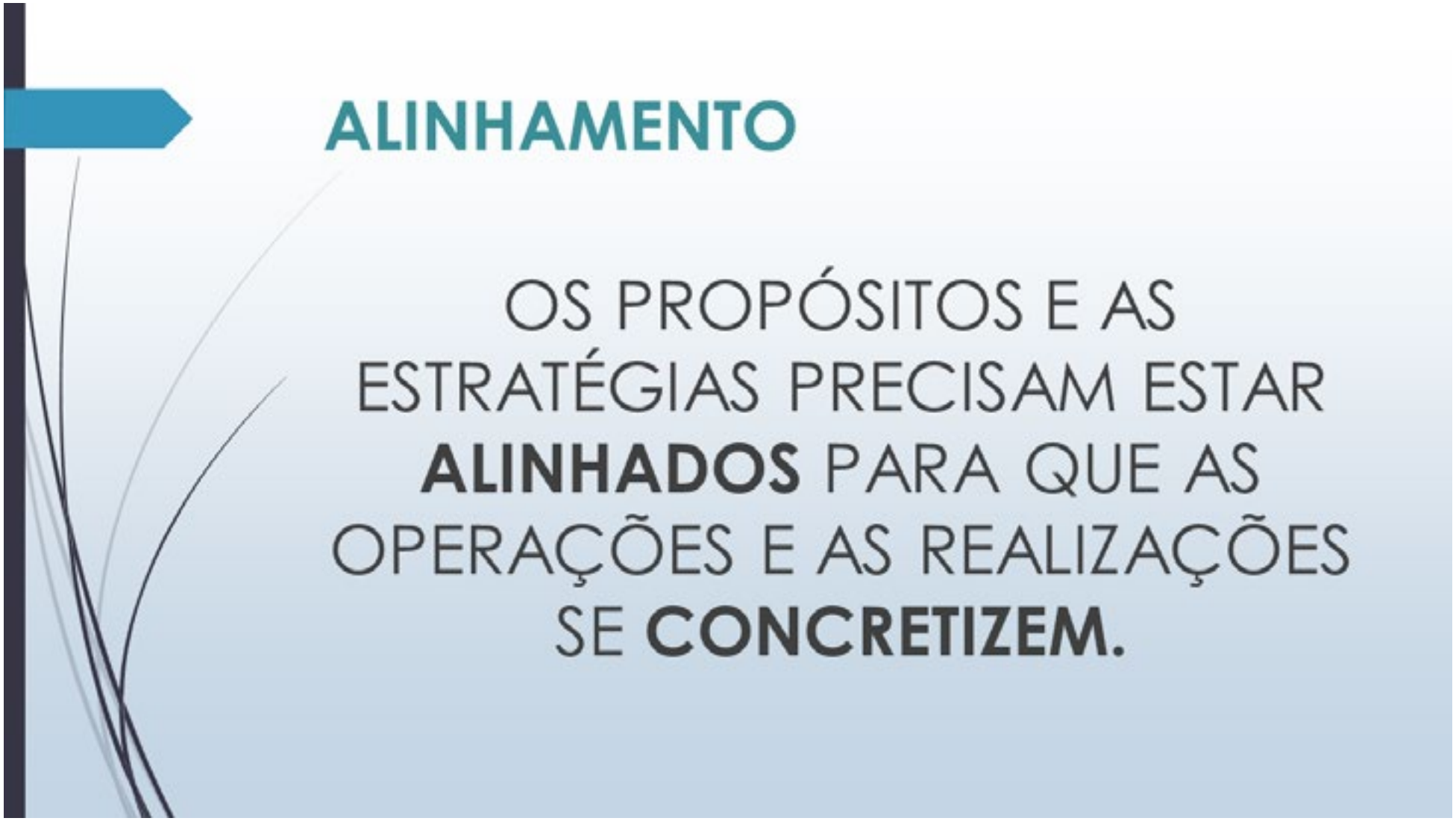
Estratégia (Como idealizamos fazer)

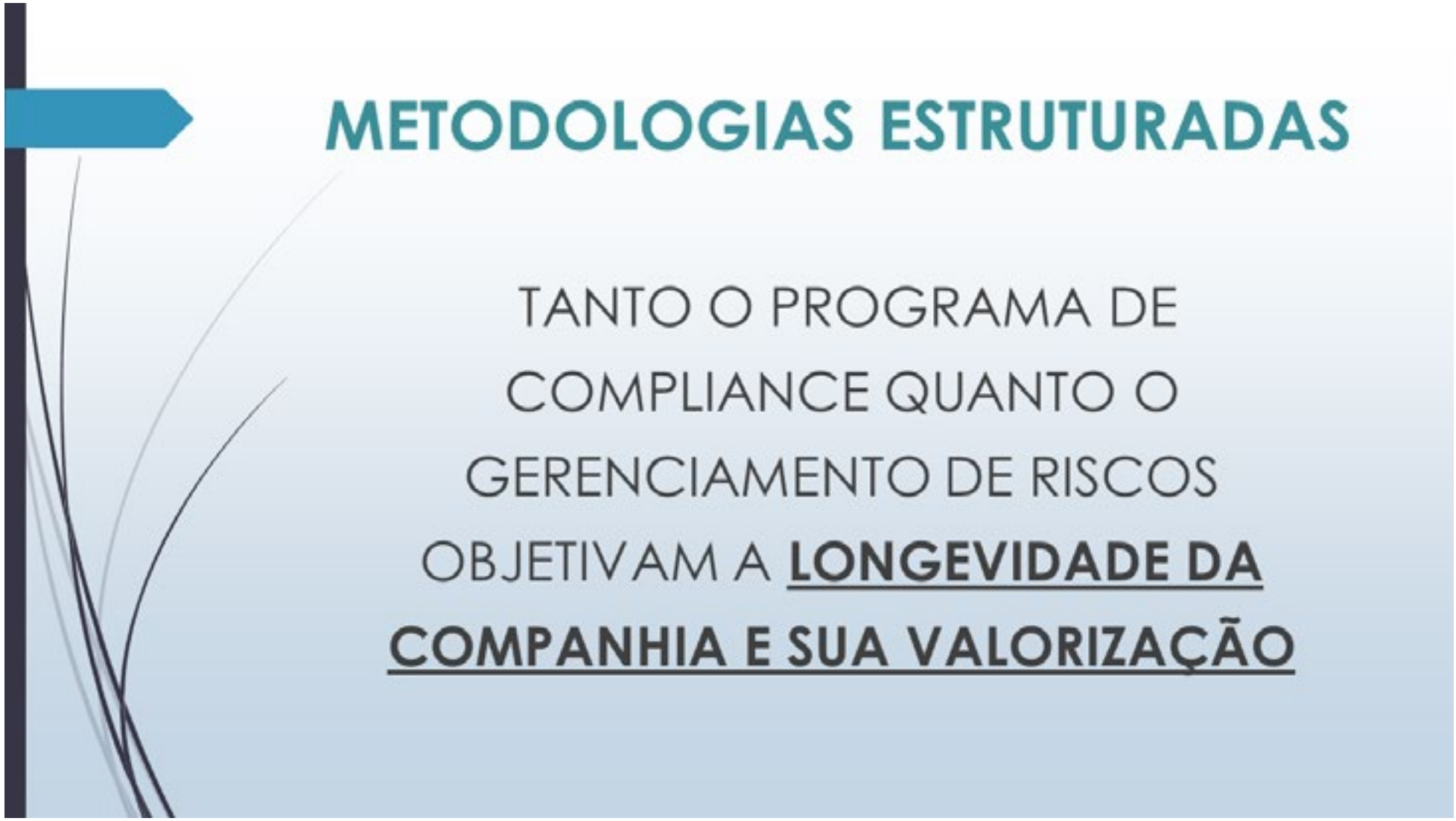
Operações (Como fazemos)

Realizações (O que fazemos)

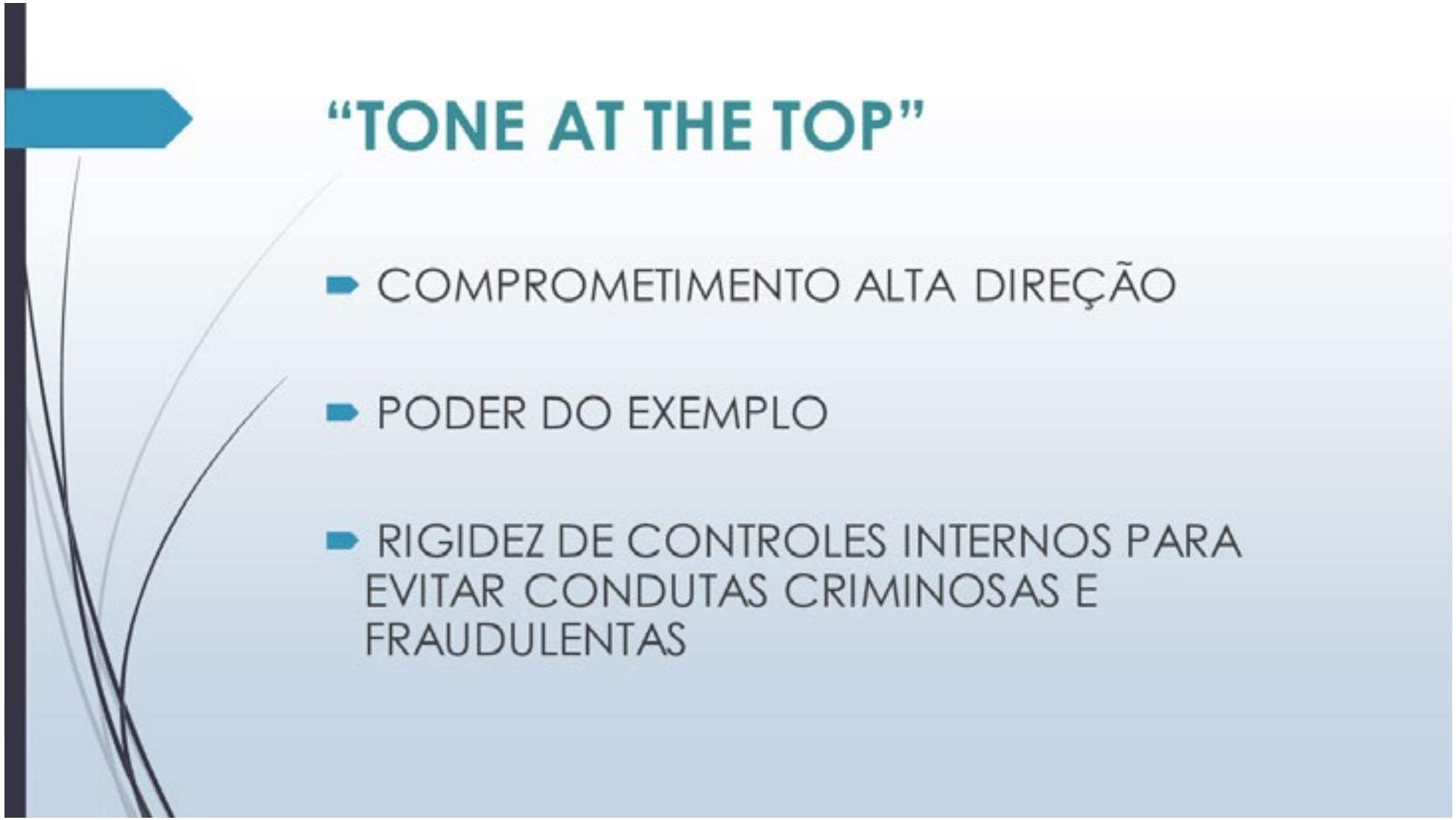

ESTRUTURA ORGANIZACIONAL
RISCOS
zemos)
lizamos fazer)
Operações (Como fazemos)
Realizações (O que fazemos)

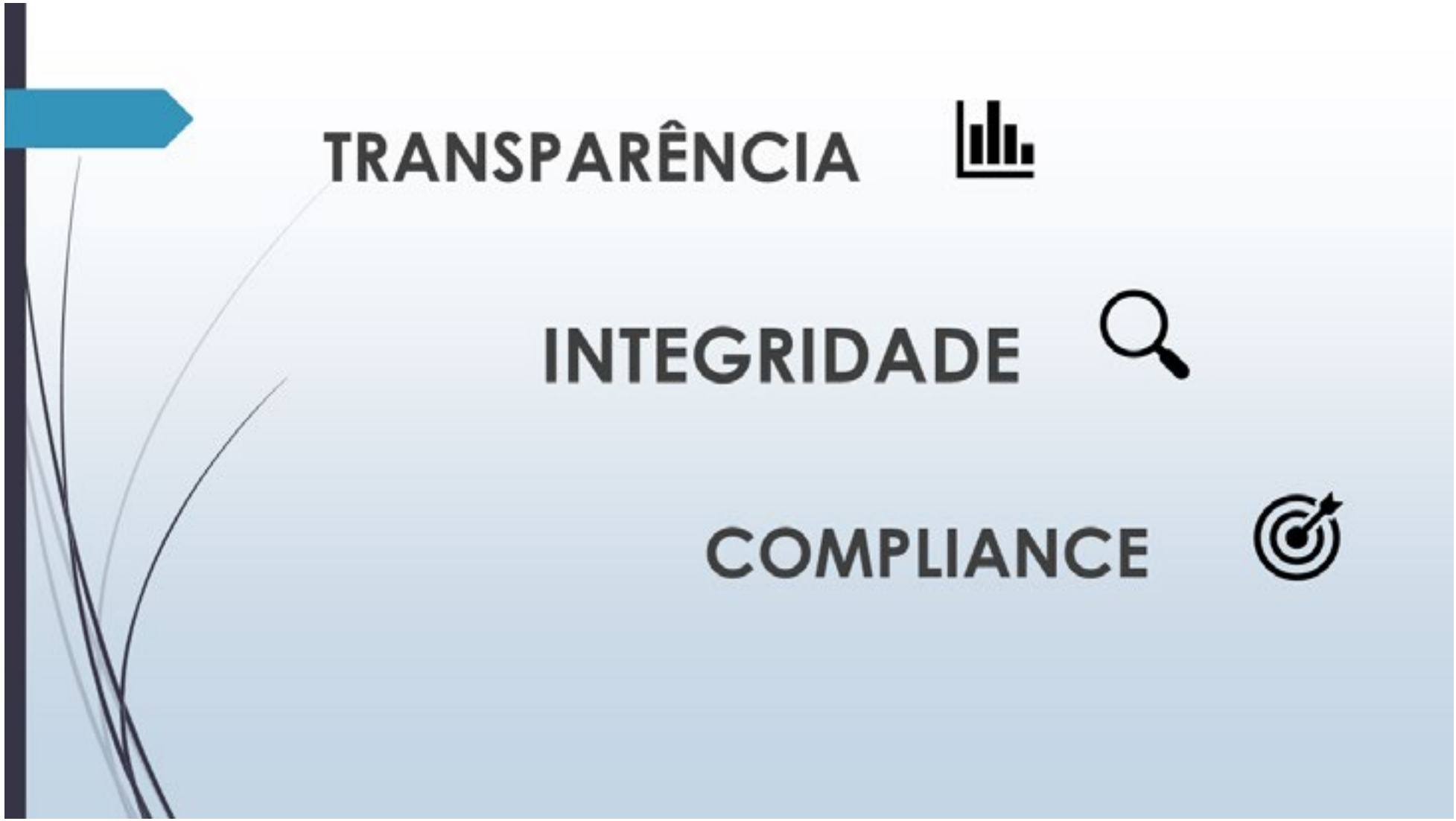

CONTROLES E COERÊNCIAS
VISÃO, MISSÃO E VALORES
PLANEJAMENTO ESTRATÉGICO
ADAPTAÇÃO PARA SUSTENTABILIDADE DO NEGÓCIO

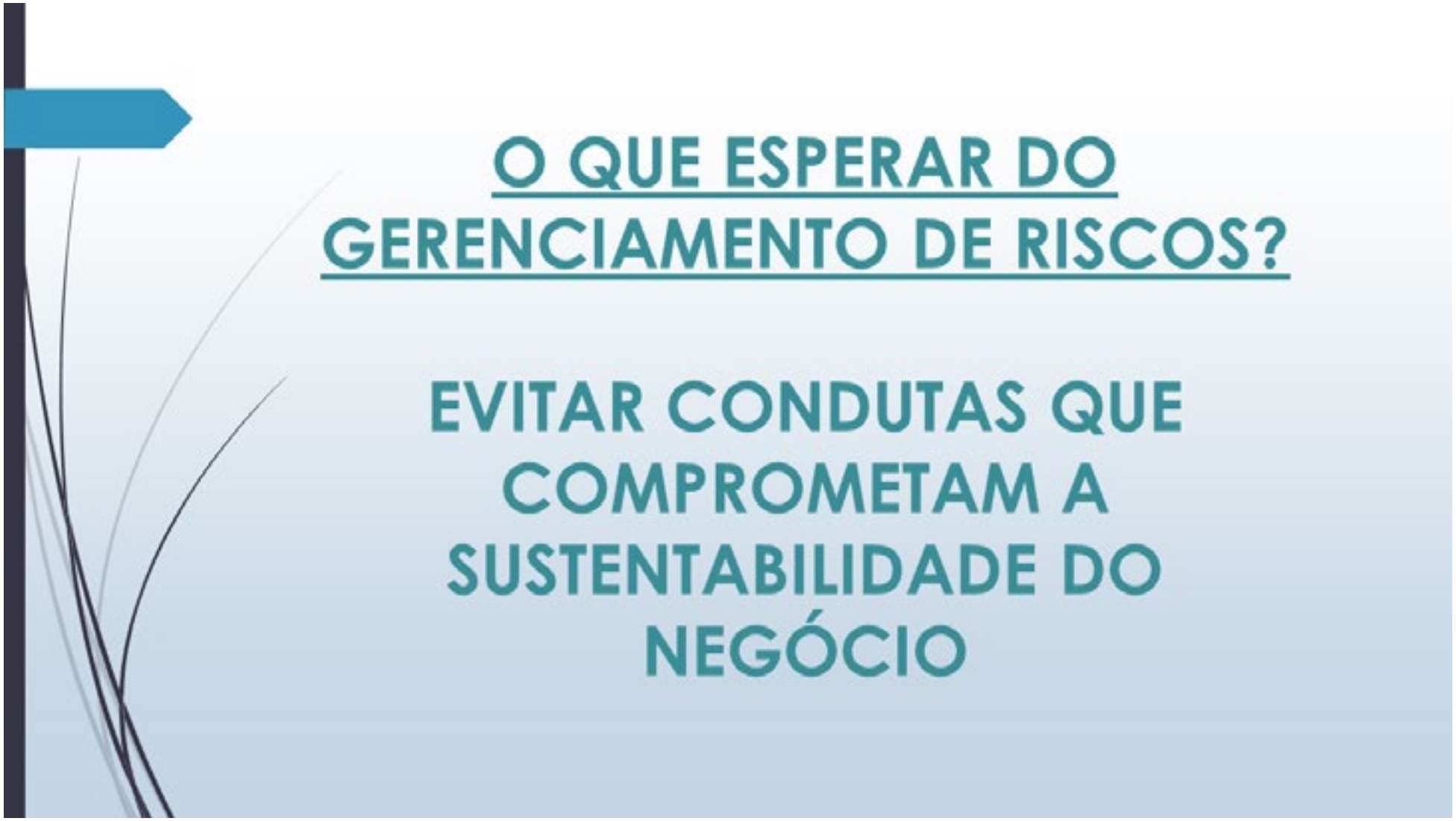

ALINHAMENTO
OS PROPÓSITOS E AS ESTRATÉGIAS PRECISAM ESTAR ALINHADOS PARA QUE AS OPERAÇÕES E AS REALIZAÇÕES SE CONCRETIZEM.


METODOLOGIAS ESTRUTURADAS
TANTO O PROGRAMA DE COMPLIANCE QUANTO O GERENCIAMENTO DE RISCOS OBJETIVAM A LONGEVIDADE DA COMPANHIA E SUA VALORIZAÇÃO

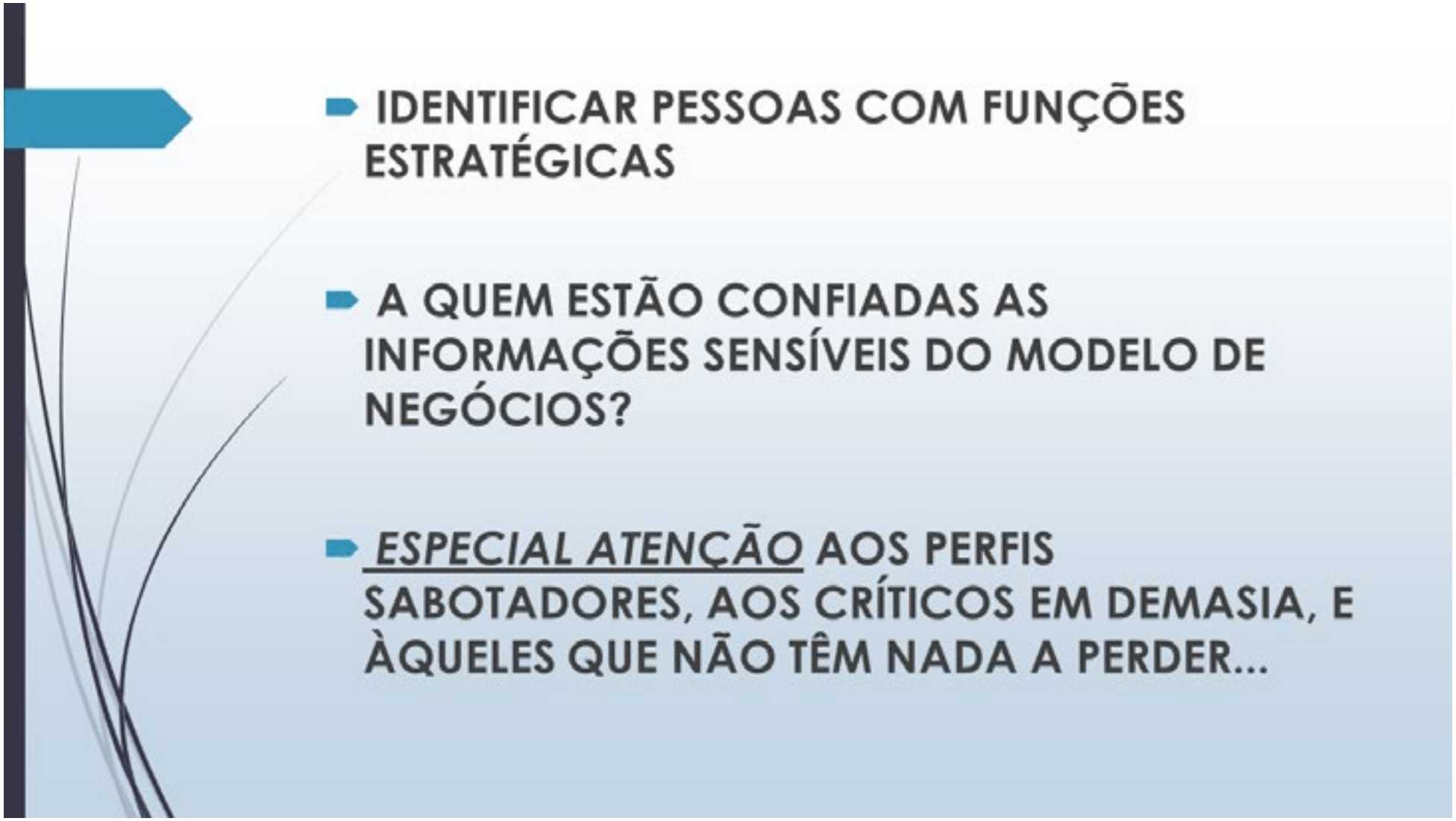

DIMENSIONAMENTO CONSTANTE
ECONÔMICO/FINANCEIRO
AMBIENTAL
SOCIAL
REPUTACIONAL
CONFORMIDADE E INTEGRIDADE

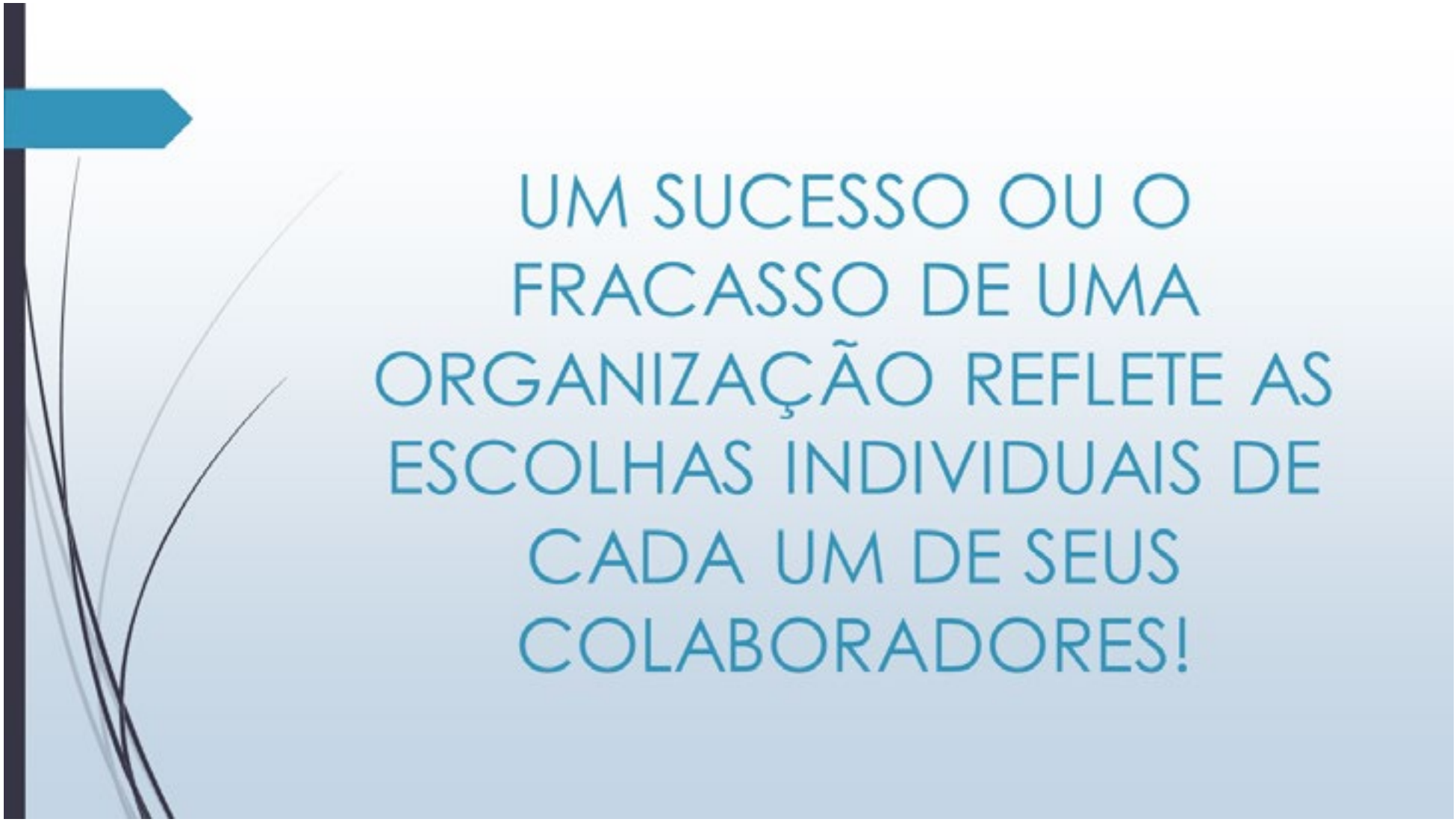

"TONE AT THE TOP"
COMPROMETIMENTO ALTA DIREÇÃO
PODER DO EXEMPLO
RIGIDEZ DE CONTROLES INTERNOS PARA EVITAR CONDUTAS CRIMINOSAS E FRAUDULENTAS

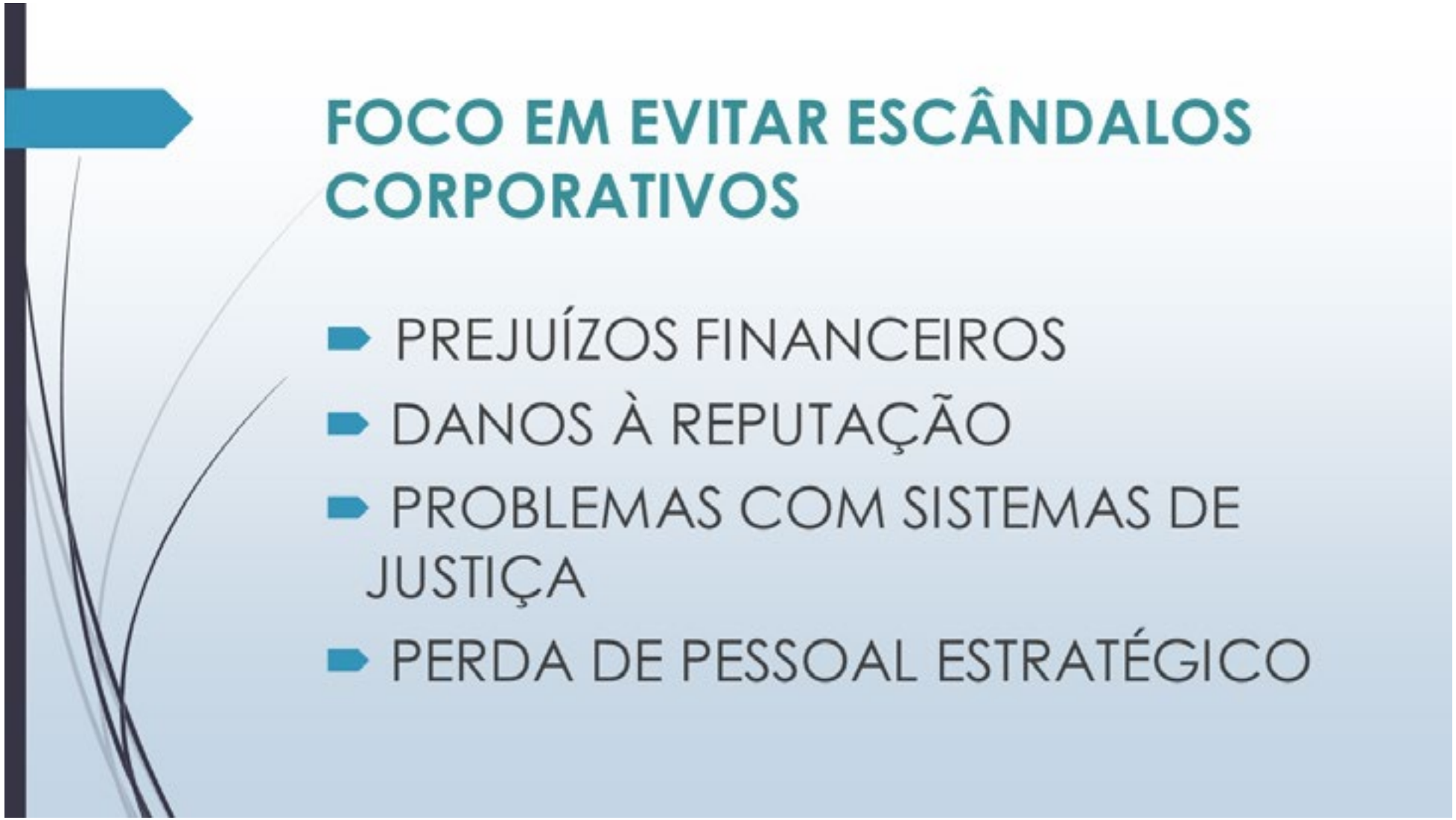

TRANSPARÊNCIA
INTEGRIDADE
COMPLIANCE


O QUE ESPERAR DO GERENCIAMENTO DE RISCOS?
EVITAR CONDUTAS QUE COMPROMETAM A SUSTENTABILIDADE DO NEGÓCIO

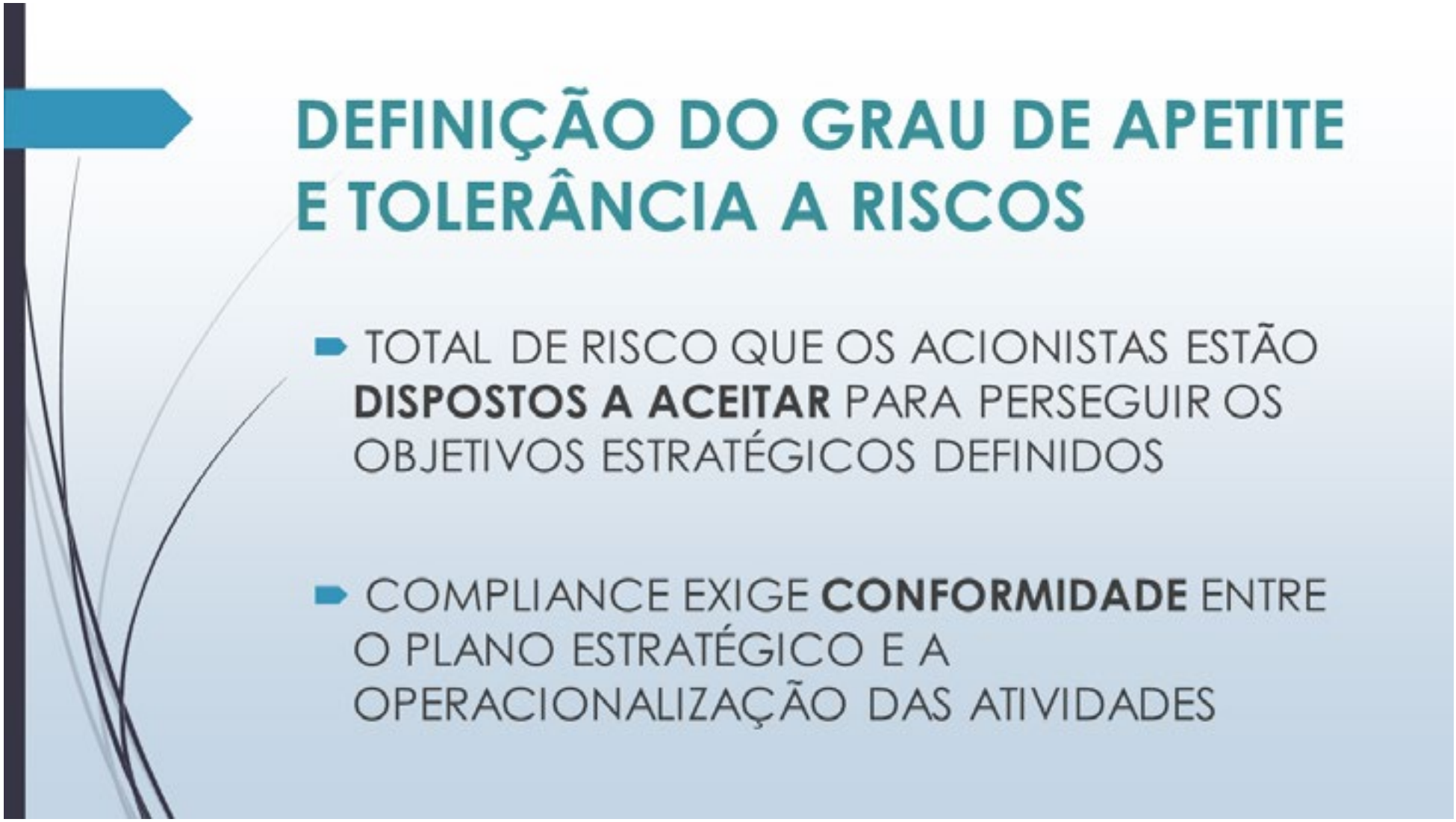
ENVOLVIMENTO DE TODAS AS ÁREAS

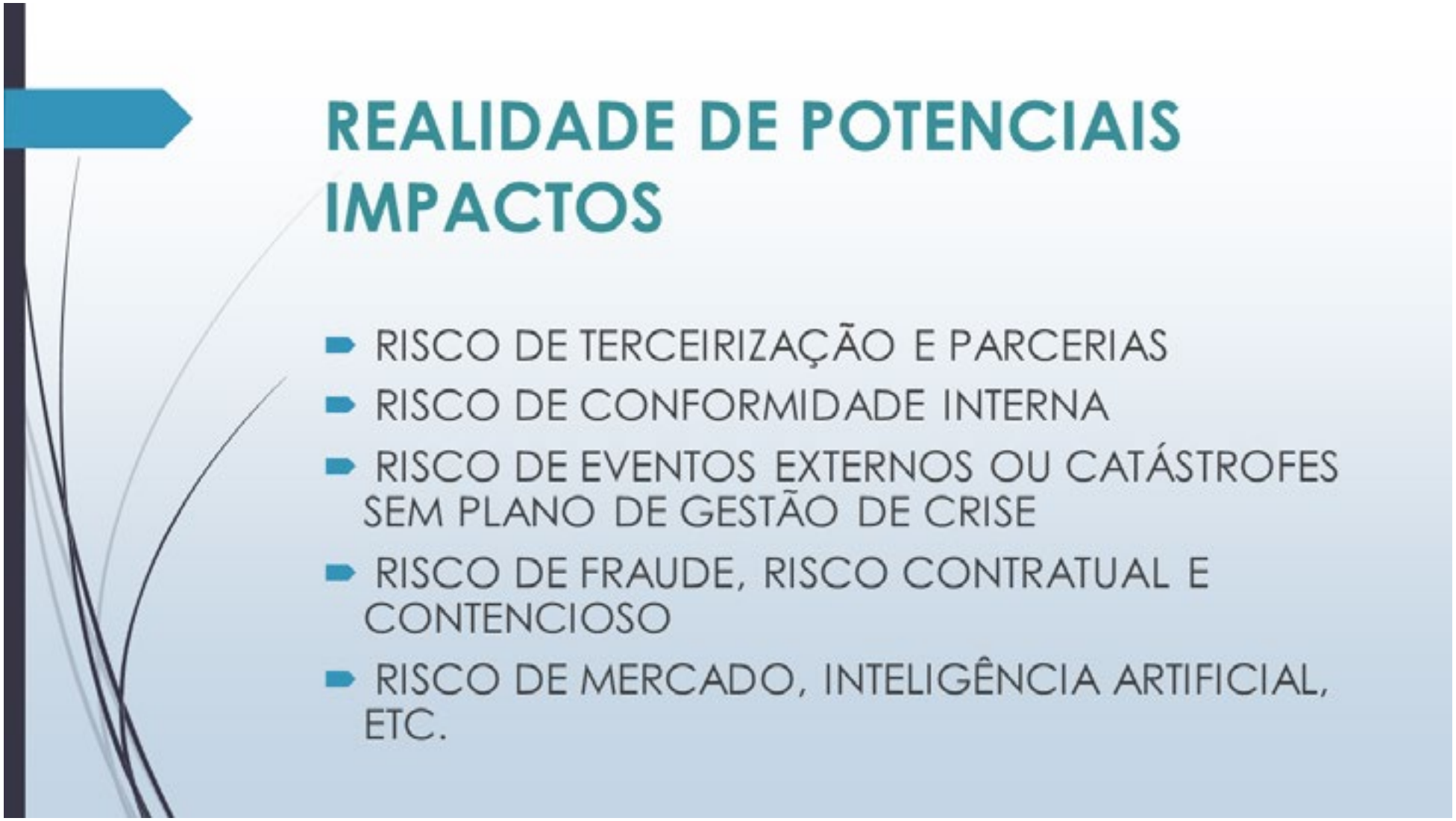

IDENTIFICAR PESSOAS COM FUNÇÕES ESTRATÉGICAS
A QUEM ESTÃO CONFIADAS AS INFORMAÇÕES SENSÍVEIS DO MODELO DE NEGÓCIOS?
ESPECIAL ATENÇÃO AOS PERFIS SABOTADORES, AOS CRÍTICOS EM DEMASIA, E ÀQUELES QUE NÃO TÊM NADA A PERDER...

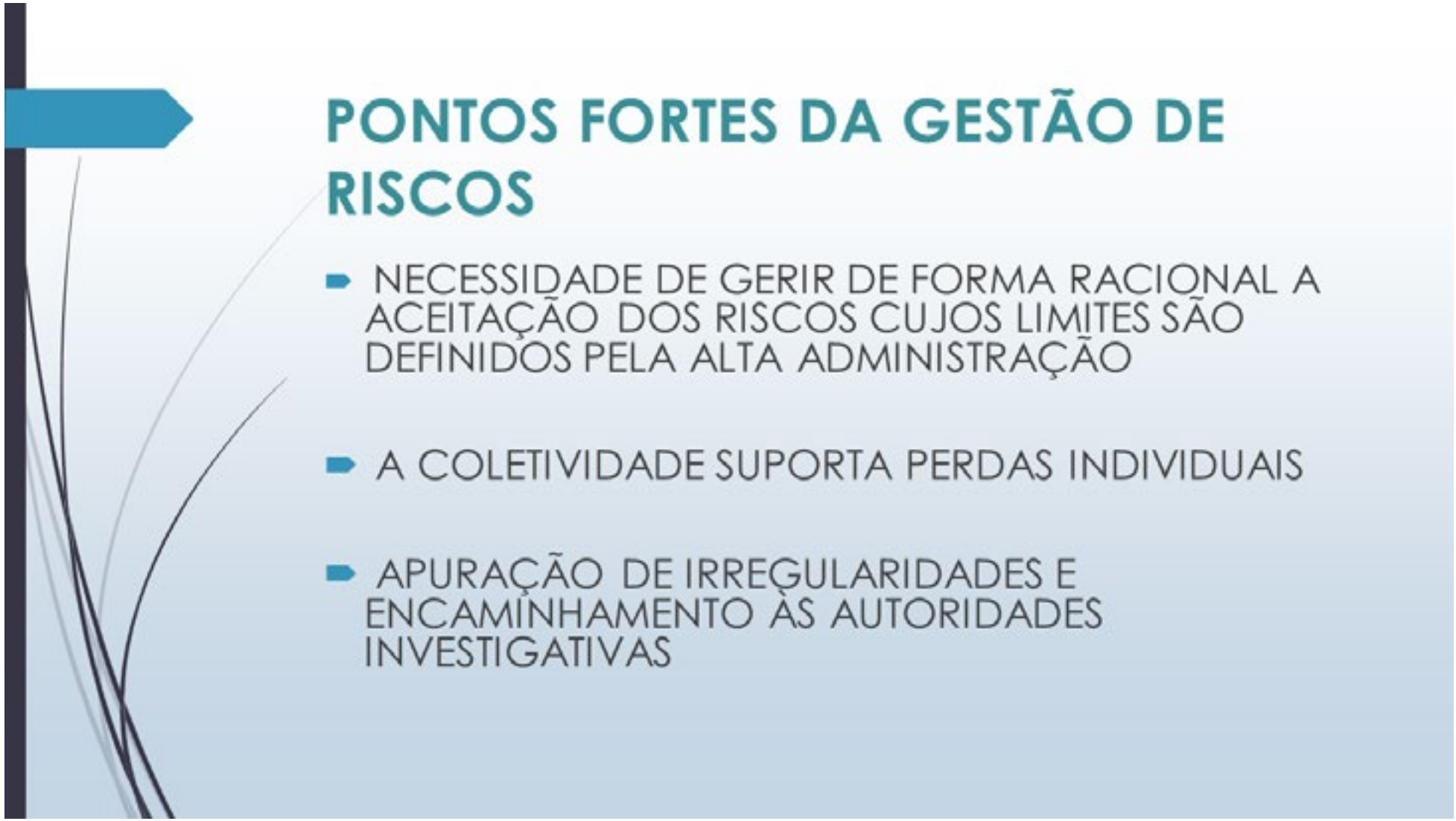

UM SUCESSO OU O
FRACASSO DE UMA
ORGANIZAÇÃO REFLETE AS
ESCOLHAS INDIVIDUAIS DE
CADA UM DE SEUS
COLABORADORES!


FOCO EM EVITAR ESCÂNDALOS CORPORATIVOS
PREJUÍZOS FINANCEIROS
DANOS À REPUTAÇÃO
PROBLEMAS COM SISTEMAS DE JUSTIÇA
PERDA DE PESSOAL ESTRATÉGICO


CONTROLES INTERNOS DEFICIENTES
SERVEM DE ALERTA PARA ANTEVER
ESCÂNDALOS CORPORATIVOS!


DEFINIÇÃO DO GRAU DE APETITE E TOLERÂNCIA A RISCOS
TOTAL DE RISCO QUE OS ACIONISTAS ESTÃO DISPOSTOS A ACEITAR PARA PERSEGUIR OS OBJETIVOS ESTRATÉGICOS DEFINIDOS
COMPLIANCE EXIGE CONFORMIDADE ENTRE O PLANO ESTRATÉGICO E A OPERACIONALIZAÇÃO DAS ATIVIDADES


REALIDADE DE POTENCIAIS IMPACTOS
RISCO DE TERCEIRIZAÇÃO E PARCERIAS
RISCO DE CONFORMIDADE INTERNA
RISCO DE EVENTOS EXTERNOS OU CATÁSTROFES SEM PLANO DE GESTÃO DE CRISE
RISCO DE FRAUDE, RISCO CONTRATUAL E CONTENCIOSO
RISCO DE MERCADO, INTELIGÊNCIA ARTIFICIAL, ETC.

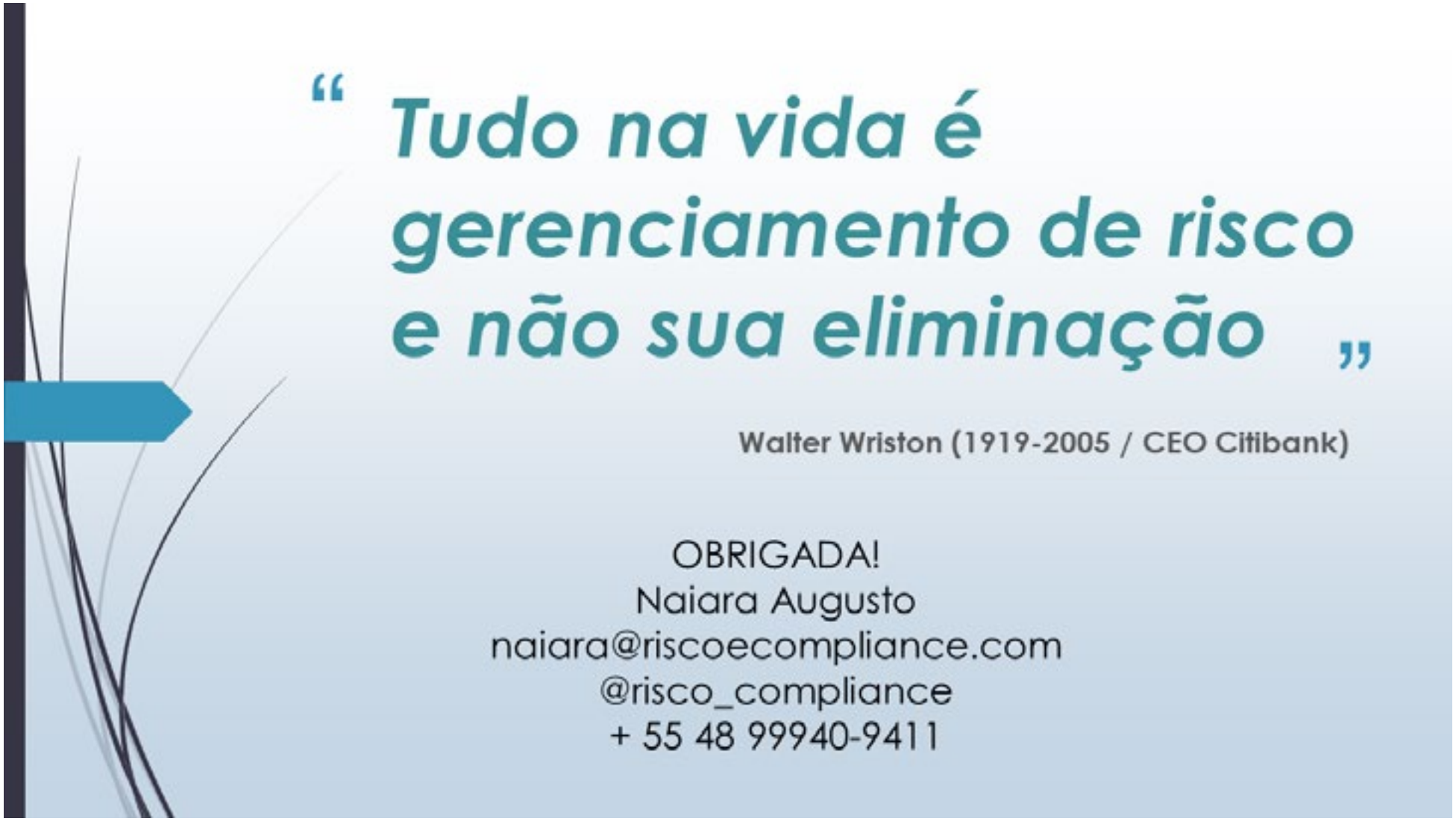

PONTOS FORTES DA GESTÃO DE RISCOS
NECESSIDADE DE GERIR DE FORMA RACIONAL A ACEITAÇÃO DOS RISCOS CUJOS LIMITES SÃO DEFINIDOS PELA ALTA ADMINISTRAÇÃO
A COLETIVIDADE SUPORTA PERDAS INDIVIDUAIS
APURAÇÃO DE IRREGULARIDADES E ENCAMINHAMENTO ÀS AUTORIDADES INVESTIGATIVAS


PROGRAMA DE COMPLIANCE EFETIVO
MITIGAÇÃO DE RISCOS
A APLICAÇÃO DO PROGRAMA DE COMPLIANCE PERMITIRÁ ENCONTRAR EQUILÍBRIO NOS NÍVEIS DE RETENÇÃO, REDUÇÃO, EXPLORAÇÃO E TRANSFERÊNCIA DE RISCOS.
ADEQUAÇÃO DAS OPERAÇÕES AO APETITE DE RISCOS DA ORGANIZAÇÃO.

EFETIVIDADE ESPERADA

REDUÇÃO DAS CHANCES DE FRACASSOS CORPORATIVOS POR FALHAS DE INTEGRIDADE E CONFORMIDADE

PREVALÊNCIA DA IMPORTÂNCIA ESTRATÉGICA


“Tudo na vida é gerenciamento de risco e não sua eliminação”
Walter Wriston (1919-2005 / CEO Citibank)
OBRIGADA!
Naiara Augusto
naiara@riscoecompliance.com
@risco_compliance
+ 55 48 99940-9411

Apresentação 3:

Governança e Compliance

Um Pensamento Integrado e Sistêmico

CÉLIA LIMA NEGRÃO

GOVERNANÇA E COMPLIANCE

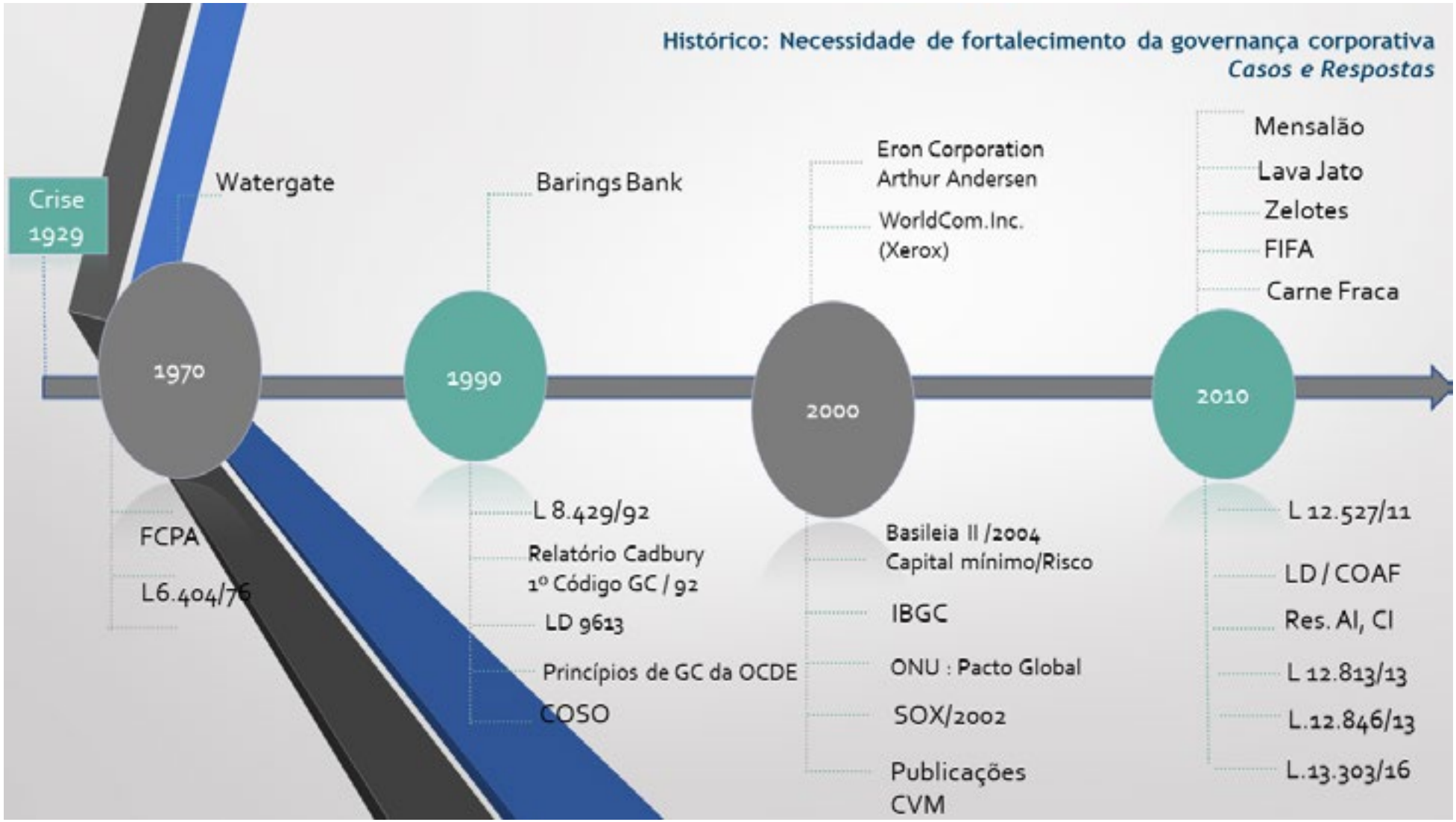
UM PENSAMENTO INTEGRADO E SISTÊMICO

I Conferência Nacional: Governança, Riscos e Compliance
4 e 5 de Outubro, Brasília.

Célia Lima Negrão


CASOS DE REPERCUSSÃO MUNDIAL
PESQUISAS
CENÁRIO ATUAL
GOVERNANÇA CORPORATIVA E GOVERNANÇA PÚBLICA
COMPLIANCE
MARCOS REGULATÓRIOS
PRÁTICAS – MONITORAMENTO, GESTÃO DE RISCOS E AÇÕES DE CONTROLE/CONFORMIDADE
COMUNICADO IMPORTANTE

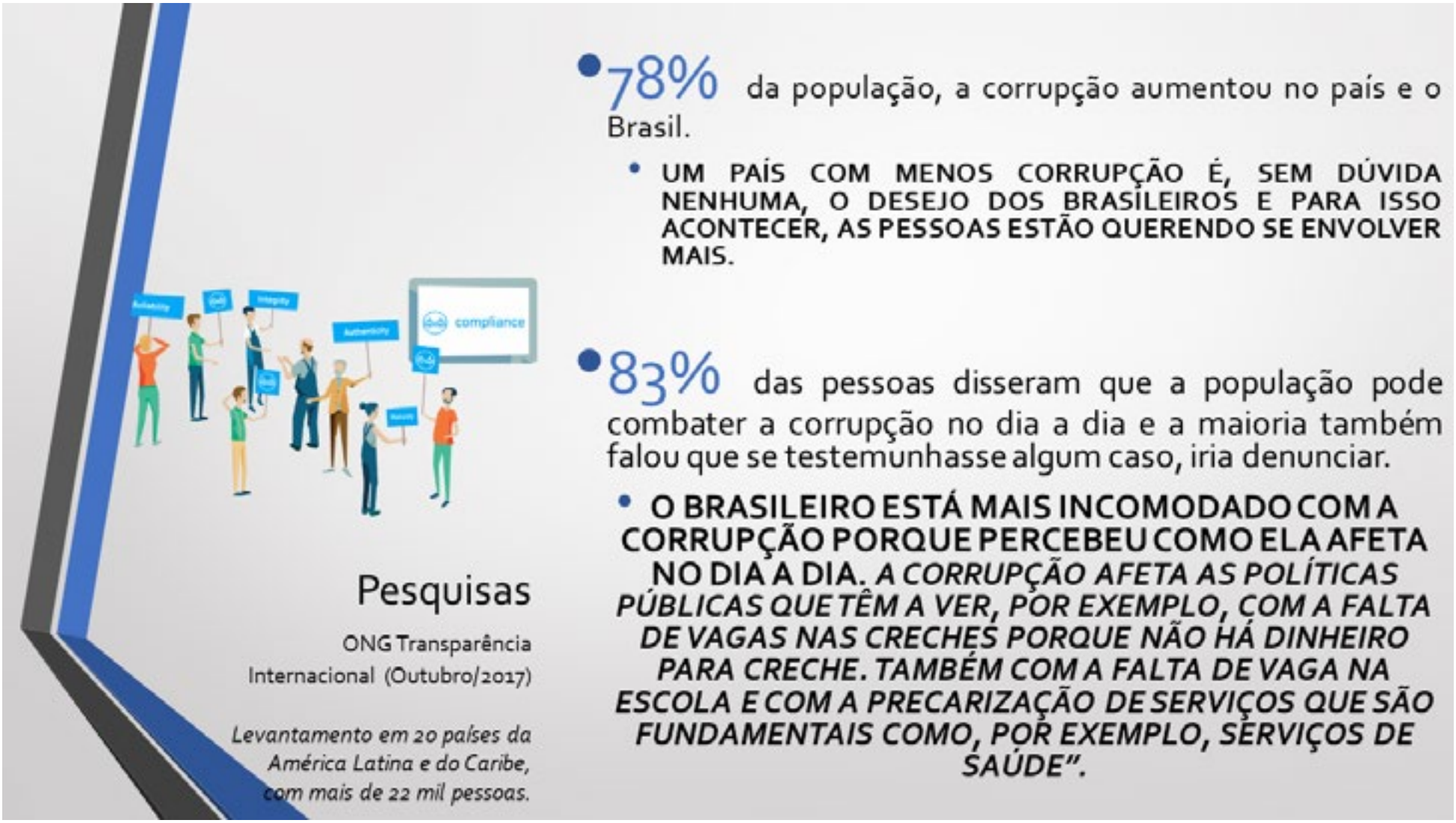

A CRISE DE
1929
Uma breve introdução
CASO ENRON
WORLDCOM
SIEMENS
MENSALÃO
PETROBRAS
JUDITH RAWNSLEY
GOING FOR BROKE
Barings Bank
NICK LEESON AND THE COLLAPSE OF BARINGS BANK
EXTRA! EXTRA!
READ ALL ABOUT IT!
PANIC!!
CRASH
OPERAÇÃO
ZELOTES
POLICIA FEDERAL
OPERAÇÃO
CARNE FRACA
FIFA
Pág. 86 - 93


Histórico: Necessidade de fortalecimento da governança corporativa
Casos e Respostas
Crise 1929
Watergate
Barings Bank
Eron Corporation
Arthur Andersen
WorldCom.Inc.
(Xerox)
Mensalão
Lava Jato
Zelotes
FIFA
Carne Fraca
1970
1990
2000
2010
FCPA
L6.404/76
L 8.429/92
Relatório Cadbury
1º Código GC / 92
LD 9613
Princípios de GC da OCDE
COSO
Basileia II /2004
Capital mínimo/Risco
IBGC
ONU : Pacto Global
SOX/2002
Publicações
CVM
L 12.527/11
LD / COAF
Res. AI, CI
L 12.813/13
L.12.846/13
L.13.303/16

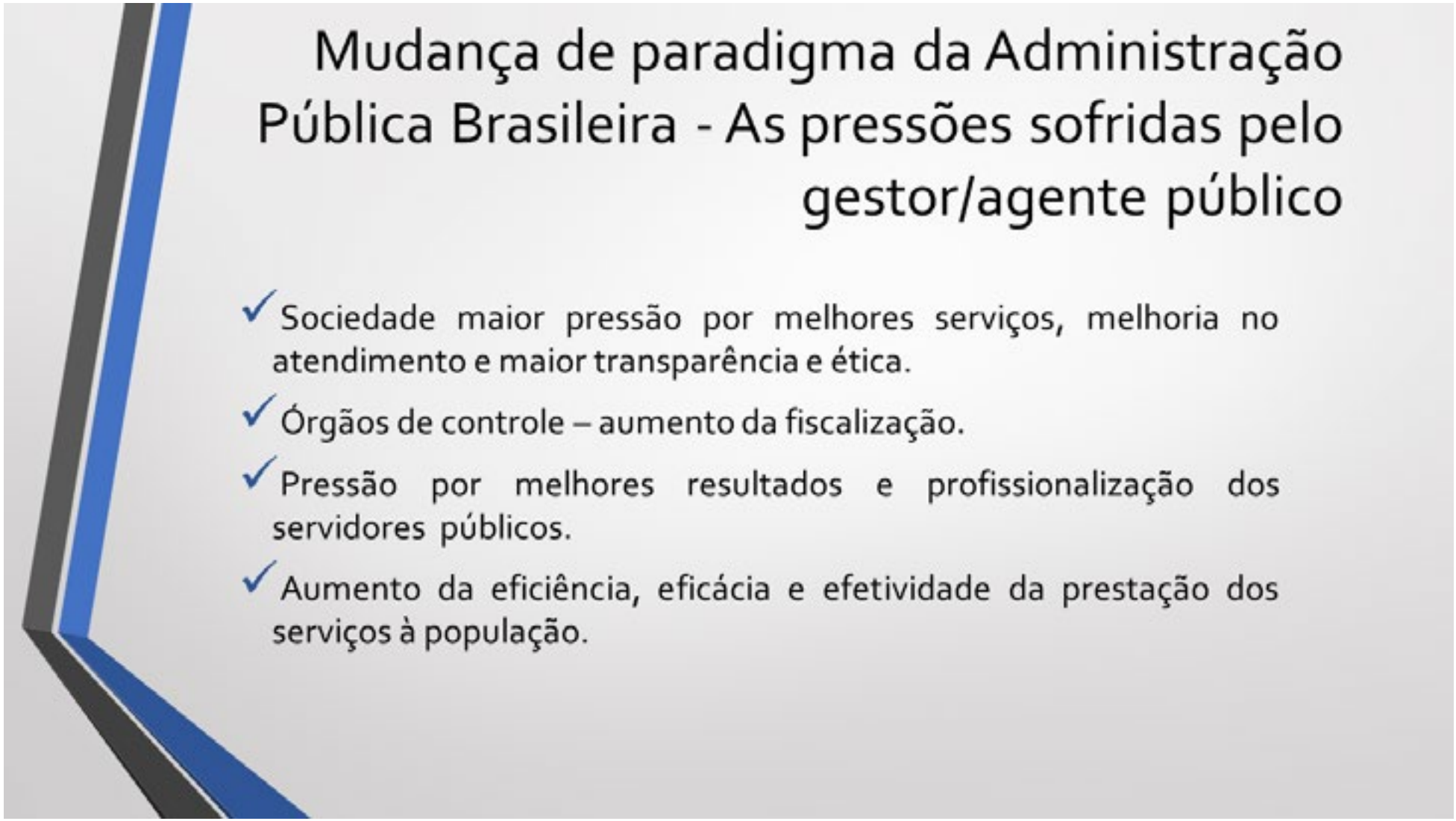
Pesquisas

Pela primeira vez a corrupção é vista como um dos maiores problemas do país.

- 34% dos eleitores colocam a corrupção como o principal **PROBLEMA DO BRASIL** na atualidade, na sequencia saúde, com 16%, desemprego, com 10%, educação e violência, ambos com 8%


compliance
Pesquisas
ONG Transparência Internacional (Outubro/2017)
Levantamento em 20 países da América Latina e do Caribe, com mais de 22 mil pessoas.
78% da população, a corrupção aumentou no país e o Brasil.
UM PAÍS COM MENOS CORRUPÇÃO É, SEM DÚVIDA NENHUMA, O DESEJO DOS BRASILEIROS E PARA ISSO ACONTECER, AS PESSOAS ESTÃO QUERENDO SE ENVOLVER MAIS.
83% das pessoas disseram que a população pode combater a corrupção no dia a dia e a maioria também falou que se testemunhasse algum caso, iria denunciar.
O BRASILEIRO ESTÁ MAIS INCOMODADO COM A CORRUPÇÃO PORQUE PERCEBEU COMO ELA AFETA NO DIA A DIA. A CORRUPÇÃO AFETA AS POLÍTICAS PÚBLICAS QUE TÊM A VER, POR EXEMPLO, COM A FALTA DE VAGAS NAS CRECHES PORQUE NÃO HÁ DINHEIRO PARA CRECHE. TAMBÉM COM A FALTA DE VAGA NA ESCOLA E COM A PRECARIZAÇÃO DE SERVIÇOS QUE SÃO FUNDAMENTAIS COMO, POR EXEMPLO, SERVIÇOS DE SAÚDE".


Transparency Internacional – 2017
O país ocupa o 96º lugar na lista de 2017. Na escala que vai de zero (mais corrupto) a 100 (menos corrupto), o Brasil aparece com 37 pontos, três a menos que em 2016.
O ranking leva em consideração a percepção que a população tem sobre a corrupção entre servidores públicos e políticos. Quanto melhor um país está situado no ranking, menor é a percepção da corrupção por seus cidadãos.

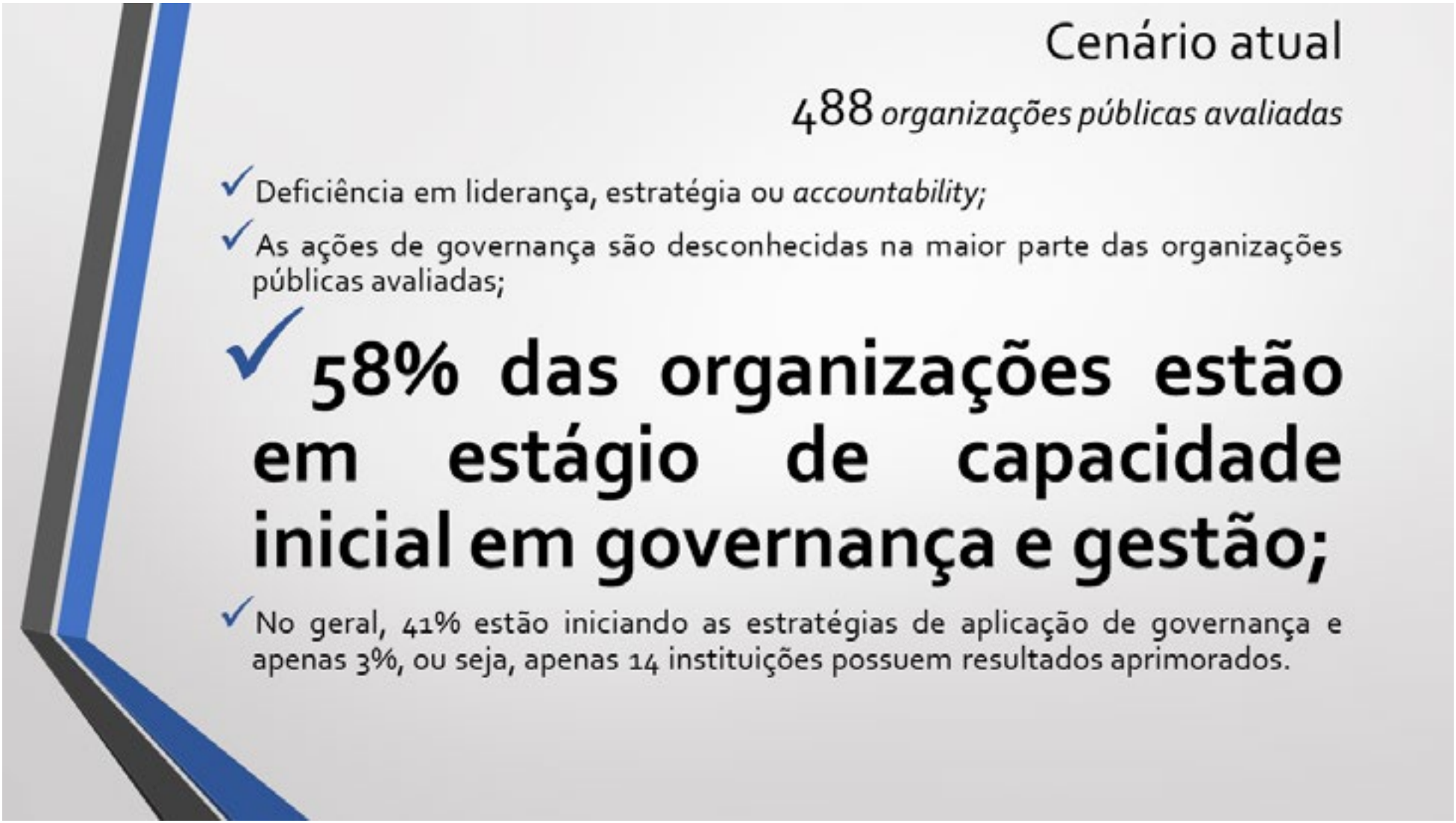

Mudança de paradigma da Administração Pública Brasileira - As pressões sofridas pelo gestor/agente público
Sociedade maior pressão por melhores serviços, melhoria no atendimento e maior transparência e ética.
Órgãos de controle – aumento da fiscalização.
Pressão por melhores resultados e profissionalização dos servidores públicos.
Aumento da eficiência, eficácia e efetividade da prestação dos serviços à população.

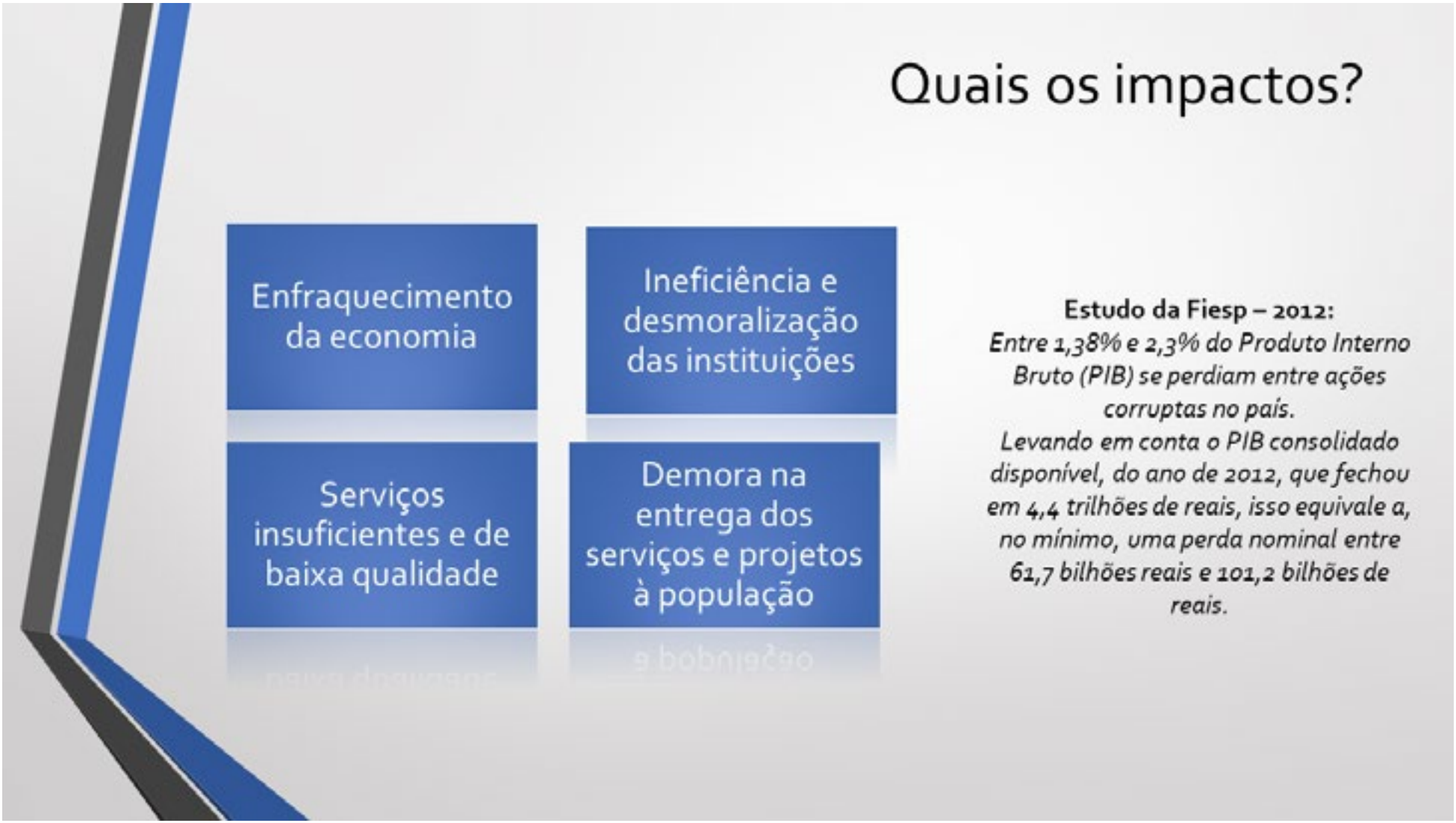
Cenário atual

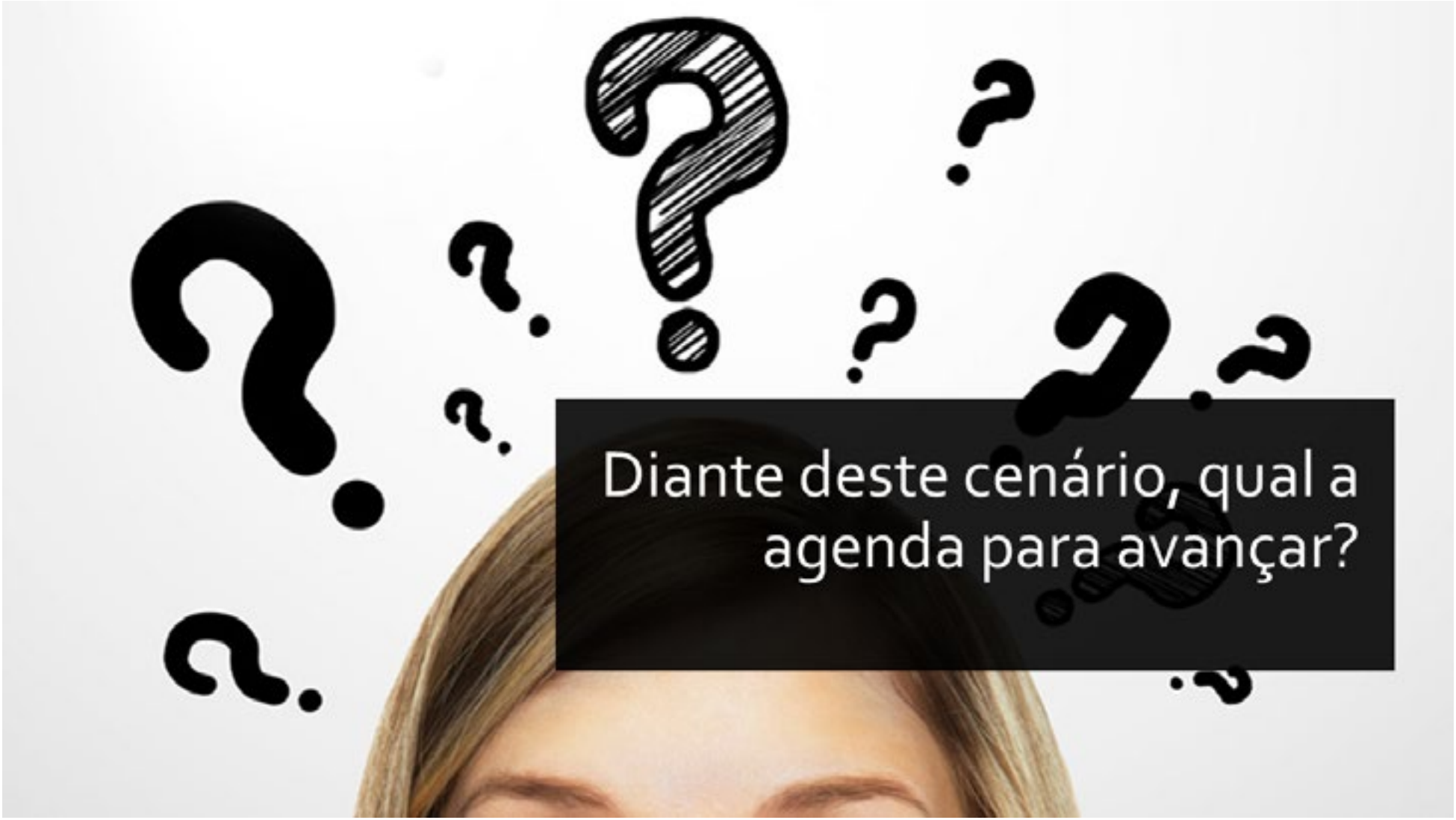
Acórdão 588/2018 – Plenário do Tribunal de Contas da União

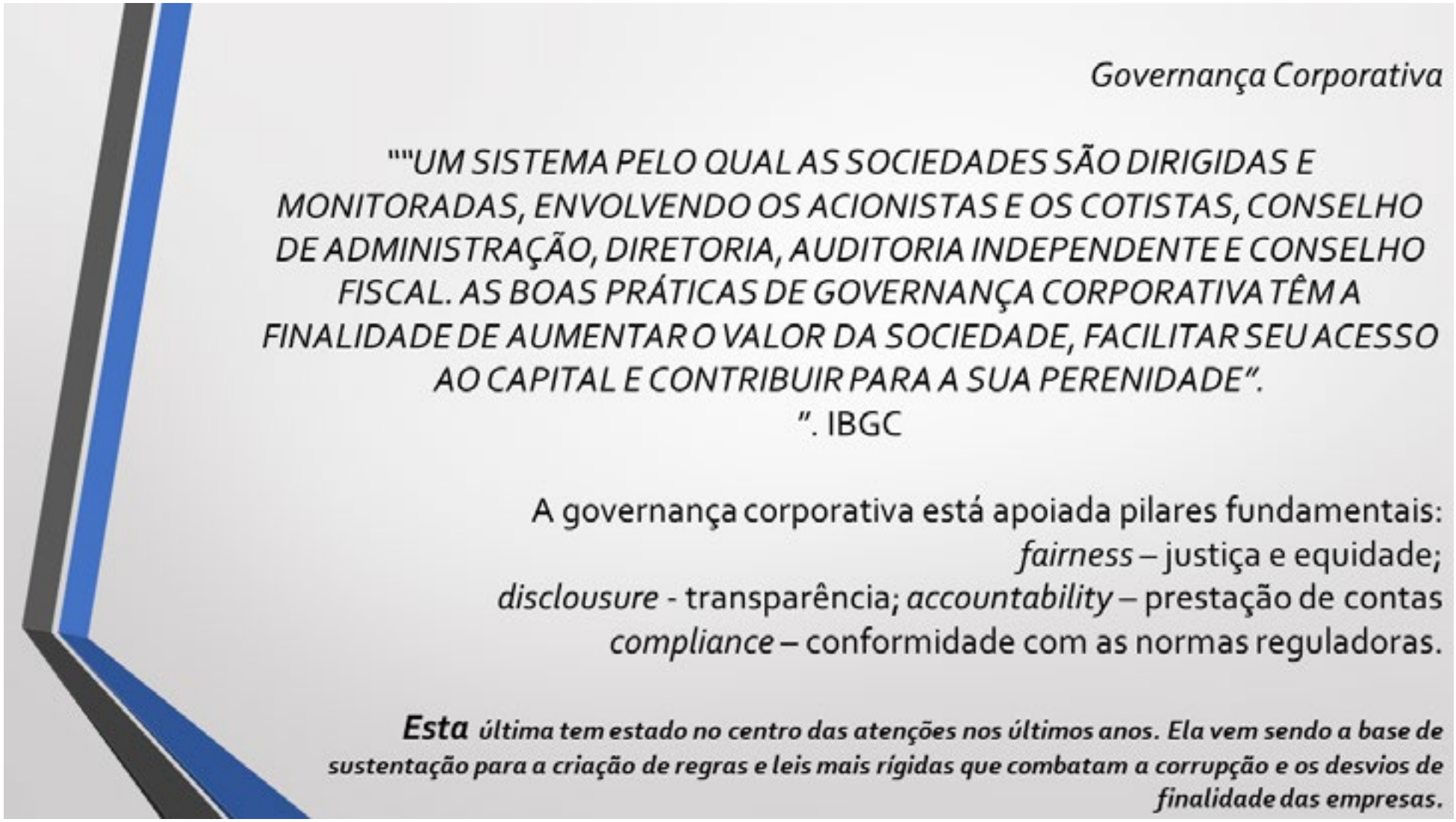
Administração Pública vulnerável quando o assunto é Governança

- A maior parte dos órgãos têm baixa maturidade na implantação de práticas de governança. *"organizações públicas federais (474) não possuem capacidade minimamente razoável de entregar o que se espera delas para o cidadão, gerindo bem o dinheiro público, cumprindo com suas competências e minimizando os riscos associados à sua atuação"*


Cenário atual
488 organizações públicas avaliadas
Deficiência em liderança, estratégia ou accountability;
As ações de governança são desconhecidas na maior parte das organizações públicas avaliadas;
58% das organizações estão em estágio de capacidade inicial em governança e gestão;
No geral, 41% estão iniciando as estratégias de aplicação de governança e apenas 3%, ou seja, apenas 14 instituições possuem resultados aprimorados.


Quais os impactos?
Enfraquecimento da economia
Ineficiência e desmoralização das instituições
Serviços insuficientes e de baixa qualidade
Demora na entrega dos serviços e projetos à população
Estudo da Fiesp – 2012:
Entre 1,38% e 2,3% do Produto Interno Bruto (PIB) se perdiam entre ações corruptas no país.
Levando em conta o PIB consolidado disponível, do ano de 2012, que fechou em 4,4 trilhões de reais, isso equivale a, no mínimo, uma perda nominal entre 61,7 bilhões reais e 101,2 bilhões de reais.


Diante deste cenário, qual a agenda para avançar?


Governança Corporativa
""UM SISTEMA PELO QUAL AS SOCIEDADES SÃO DIRIGIDAS E MONITORADAS, ENVOLVENDO OS ACIONISTAS E OS COTISTAS, CONSELHO DE ADMINISTRAÇÃO, DIRETORIA, AUDITORIA INDEPENDENTE E CONSELHO FISCAL. AS BOAS PRÁTICAS DE GOVERNANÇA CORPORATIVA TÊM A FINALIDADE DE AUMENTAR O VALOR DA SOCIEDADE, FACILITAR SEU ACESSO AO CAPITAL E CONTRIBUIR PARA A SUA PERENIDADE".
". IBGC
A governança corporativa está apoiada pilares fundamentais:
fairness – justiça e equidade;
disclousure - transparência; accountability – prestação de contas
compliance – conformidade com as normas reguladoras.
Esta última tem estado no centro das atenções nos últimos anos. Ela vem sendo a base de sustentação para a criação de regras e leis mais rígidas que combatam a corrupção e os desvios de finalidade das empresas.

Conflitos de agencia

- Separação entre a propriedade e a gestão - objetivos conflitantes no universo das empresas.
- **O Problema:**
  - Decisões ou objetivos do agente e do principal conflitantes; e
  - Difícil ou caro para o principal saber exatamente o que o agente está fazendo.
- **Alguns conflitos:**
  - Remuneração própria x maximização do lucro da empresa;
  - Conflitos entre majoritários e minoritários.

Fonte imagem: http://www.blbbrasil.com.br/artigos/teoria-da-agencia

Figura 1 – Contexto e estrutura do sistema de governança corporativa

* O profissional da secretaria de governança não é administrador, apesar de inserido junto aos demais órgãos do âmbito dos administradores.

Fonte: Código IBGC 5ª Edição

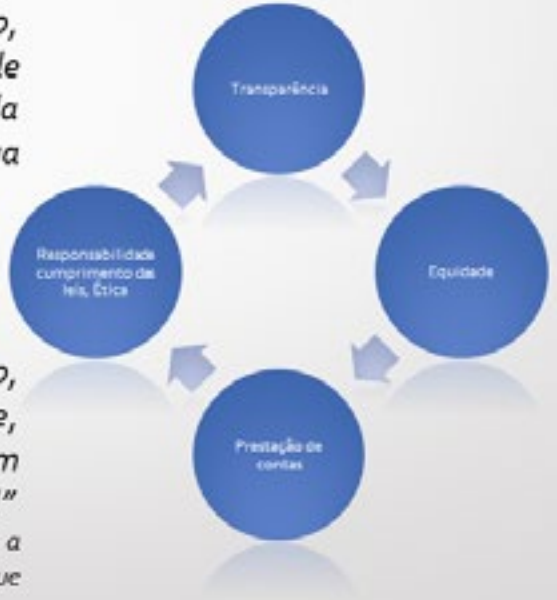
Governança - Convergência entre os princípios

Governança Corporativa

"um sistema pelo qual as sociedades são dirigidas e monitoradas, envolvendo os acionistas e os cotistas, conselho de administração, diretoria, auditoria independente e conselho fiscal. as boas práticas de governança corporativa têm a finalidade de aumentar o valor da sociedade, facilitar seu acesso ao capital e contribuir para a sua perenidade".
(IBGC)

Governança pública

"conjunto de ações sistêmicas e compartilhadas (entre governo, sociedade e mercado), executadas de maneira eficaz e transparente, visando soluções inovadoras para as demandas comunitárias num ambiente que resulte possibilidades para o desenvolvimento sustentável"
Em essência, a boa governança pública tem como propósitos conquistar e preservar a confiança da sociedade, por meio de conjunto eficiente de mecanismos, a fim de assegurar que as ações executadas estejam sempre alinhadas ao interesse público.
(TCU)



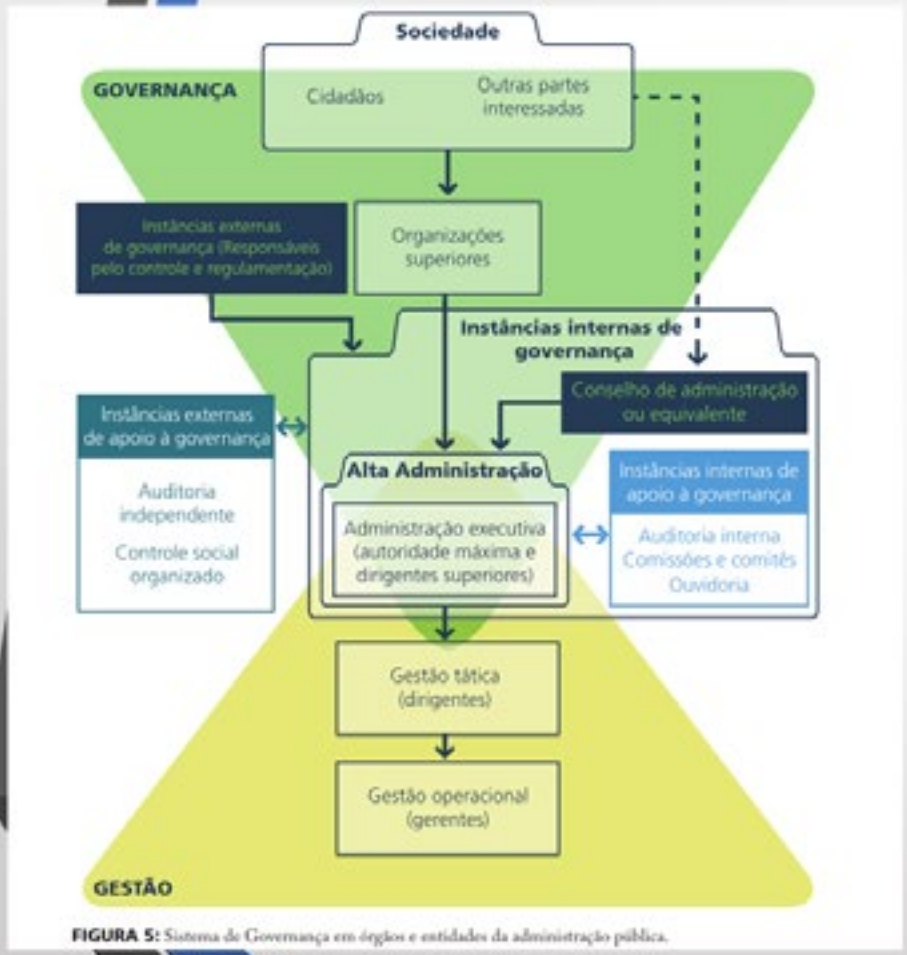


FIGURA 5: Sistema de Governança em órgãos e entidades da administração pública.

Fonte: Referencial de Governança TCU

Governança Pública

Diferença entre Governança e Gestão

FIGURA 6: Relação entre governança e gestão.

Fonte: Referencial de Governança TCU


Modelo de Três Linhas de Defesa
Órgão de Governança / Conselho / Comitê de Auditoria
Alta Administração
1a Linha de Defesa
Controles da Gerência
Medidas de Controle Interno
2a Linha de Defesa
Controle Financeiro
Segurança
Gerenciamento de Riscos
Qualidade
Inspeção
Conformidade
3a Linha de Defesa
Auditoria Interna
Auditoria Externa
Regulador
Adaptação da *Guidance on the 8th EU Company Law Directive* da ECIIA/FERMA, artigo 41

Governança Corporativa: alinhamento *Compliance*, Controles e Riscos
VISÃO INTEGRADA E SISTÊMICA

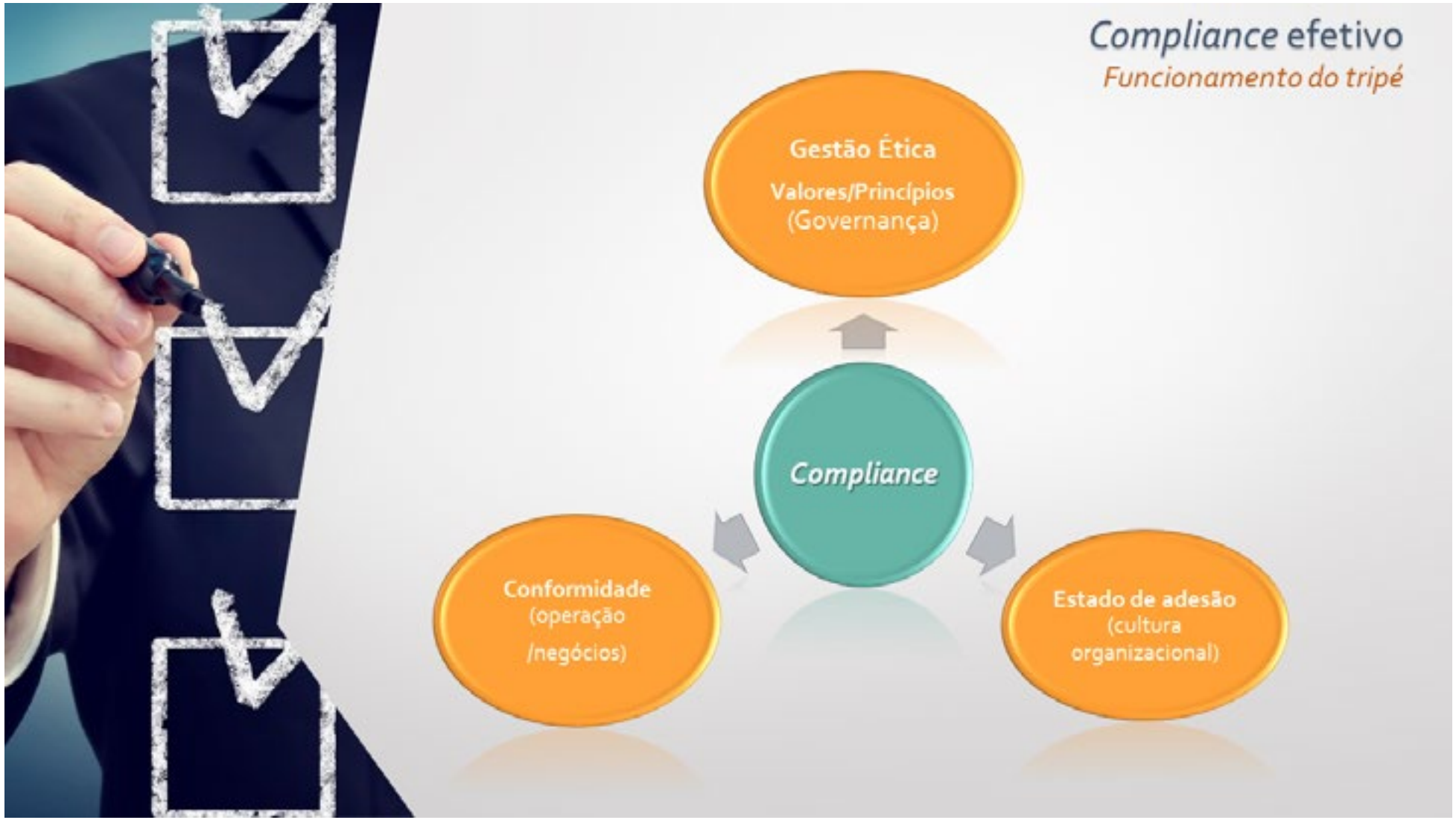
A condução dos assuntos, de forma conjunta, permite que a estratégia aconteça de forma unificada e transparente, com a devida avaliação de riscos e a garantia de conformidade com as políticas corporativas, leis e regulamentações.

Governança: É a forma que a organização é gerida.
Refere-se ao desenvolvimento de políticas e procedimentos, à definição de responsabilidades e também à criação de diretrizes para orientar as pessoas e os processos da organização.

Riscos: Por meio da gestão de risco, a empresa pode se antecipar aos eventos e imprevistos, analisar seus impactos e estudar o que fazer para evitá-los ou contorná-los.

Compliance, controles e auditorias: São as ações para garantir que a empresa esteja de acordo com as normas, legislações e boas práticas de seu segmento.


Compliance
Significa cumprir, executar, satisfazer.
É o cumprimento de leis, normas, códigos organizacionais e de conduta, inclusive dos padrões éticos e dos princípios de boa governança corporativa.
Compliance está além da verificação da conformidade e adequação com as leis, normas e políticas internas.
Possui como ponto principal inserir na cultura organizacional a consciência da responsabilidade individual de cada empregado da empresa, para realizar as atividades em conformidade com as normas.


Compliance efetivo
Funcionamento do tripé
Gestão Ética
Valores/Princípios
(Governança)
Compliance
Conformidade
(operação
/negócios)
Estado de adesão
(cultura
organizacional)

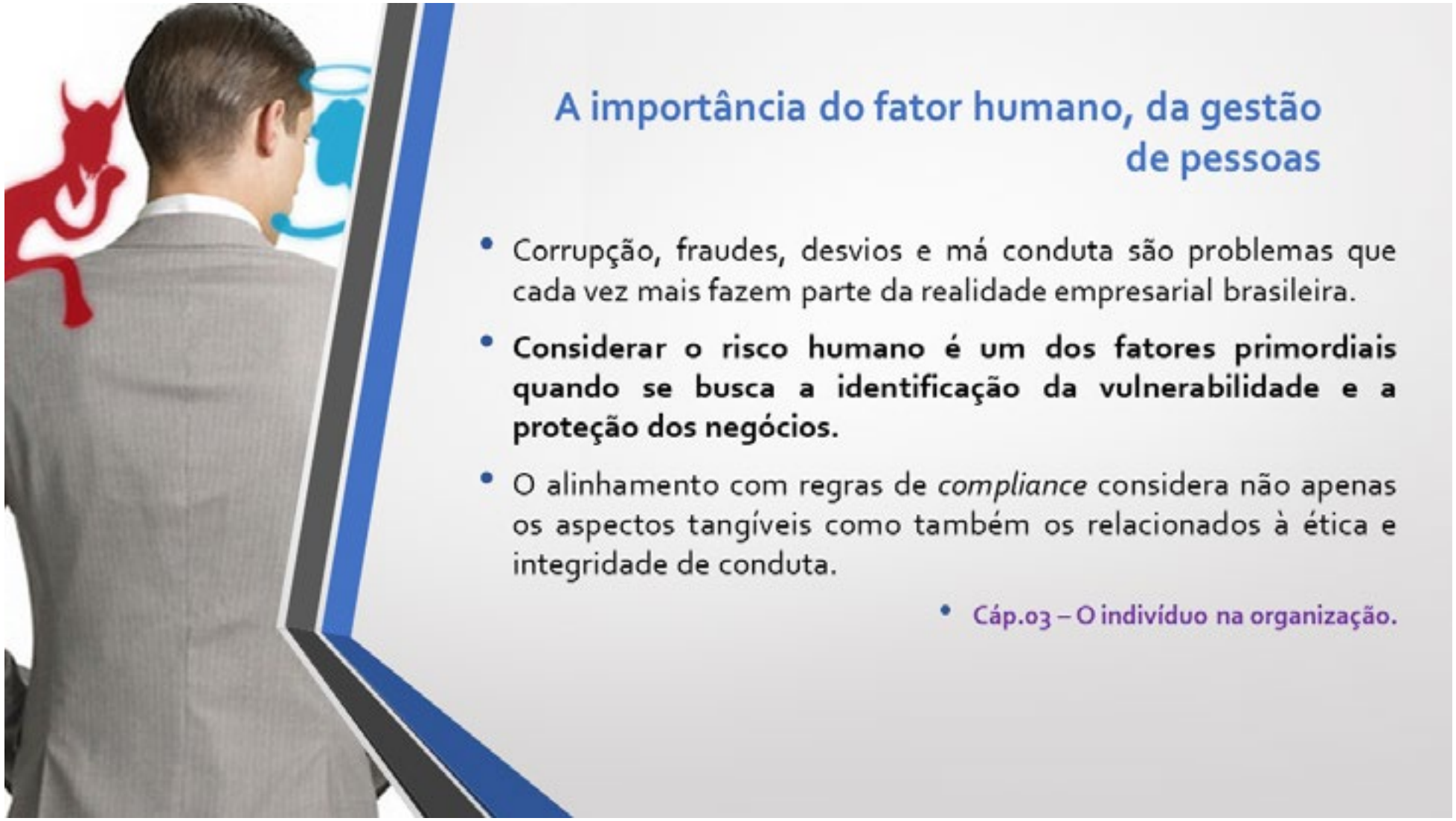
A Ética
(Código de Ética)

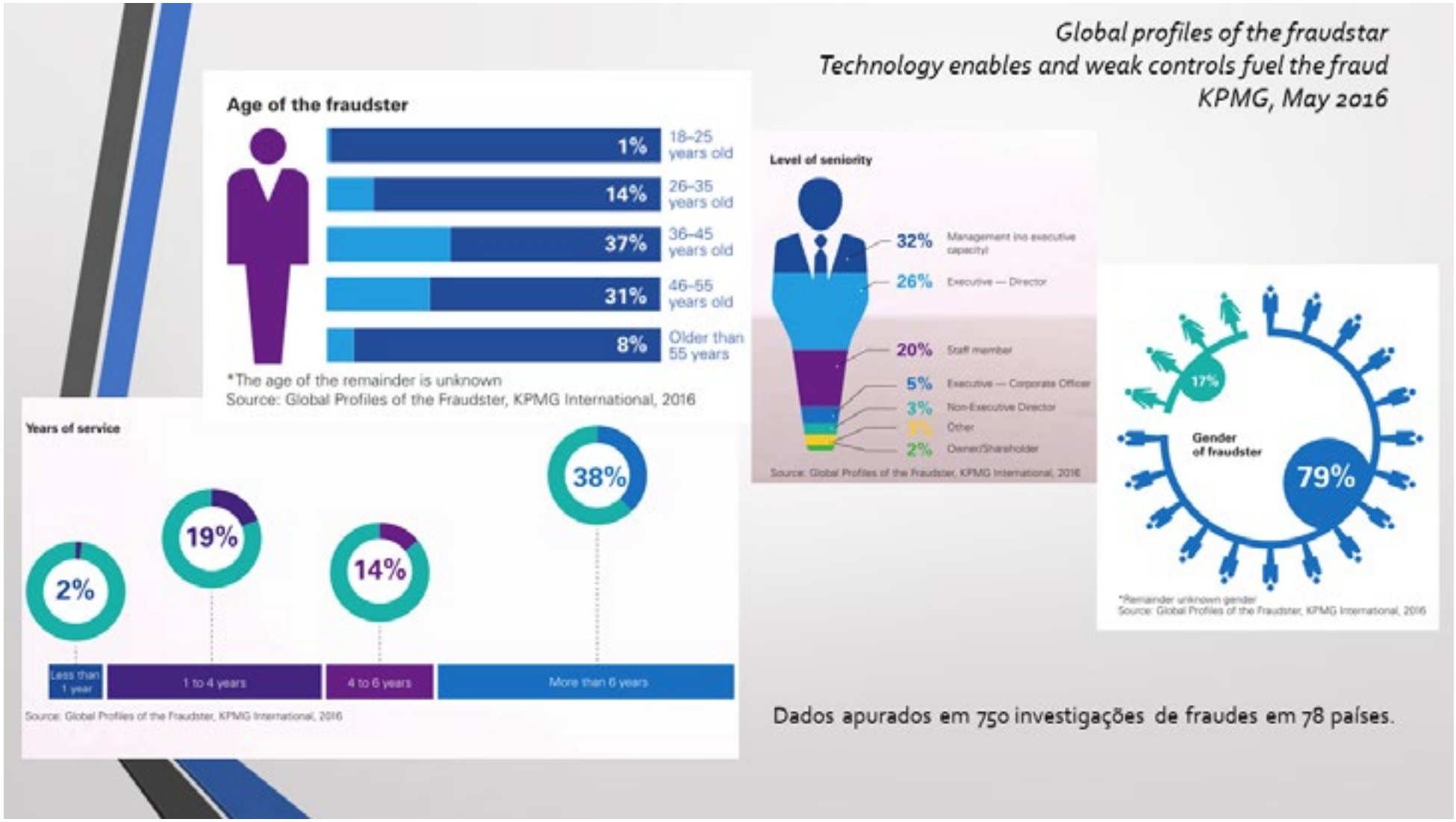
- Ética: valores que definem o que "quero" e "posso". Devo, porque nem tudo que eu quero eu posso, nem tudo que eu posso eu devo e nem tudo que eu devo eu quero.

Eça de Queiroz

- *Como implementar a Ética, veja exemplos.*

Pág 164 – 178
Pág 361 - legislação


A importância do fator humano, da gestão de pessoas
• Corrupção, fraudes, desvios e má conduta são problemas que cada vez mais fazem parte da realidade empresarial brasileira.
• **Considerar o risco humano é um dos fatores primordiais quando se busca a identificação da vulnerabilidade e a proteção dos negócios.**
• O alinhamento com regras de *compliance* considera não apenas os aspectos tangíveis como também os relacionados à ética e integridade de conduta.
• Cáp.03 – O indivíduo na organização.


Global profiles of the fraudstar
Technology enables and weak controls fuel the fraud
KPMG, May 2016
Age of the fraudster
1% 18–25 years old
14% 26–35 years old
37% 36–45 years old
31% 46–55 years old
8% Older than 55 years
*The age of the remainder is unknown
Source: Global Profiles of the Fraudster, KPMG International, 2016
Level of seniority
32% Management (no executive capacity)
26% Executive — Director
20% Staff member
5% Executive — Corporate Officer
3% Non-Executive Director
Other
2% Owner/Shareholder
Source: Global Profiles of the Fraudster, KPMG International, 2016
Years of service
2%
19%
14%
38%
Less than 1 year
1 to 4 years
4 to 6 years
More than 6 years
Source: Global Profiles of the Fraudster, KPMG International, 2016
17%
Gender of fraudster
79%
*Remainder unknown gender
Source: Global Profiles of the Fraudster, KPMG International, 2016
Dados apurados em 750 investigações de fraudes em 78 países.

Conclusões relevantes

A fraude tem mais chances de ser realizada em conluio **(62% em contraste com 38% do que a cometida por um indivíduo sozinho).**

"Mesmo que os controles sejam robustos, os fraudadores podem e irão esquivar-se deles ou infringi-los. Os fraudadores em conluio são capazes de driblar controles em 16% dos casos. Importante frisar que partes externas estão envolvidas em 61% das fraudes deste tipo".

"É importante que as empresas invistam em controle interno. O número de fraudadores capazes de praticar ações que visam tirar vantagem de controles deficientes aumentou para 27%, em comparação com os 18% do relatório de 2013.

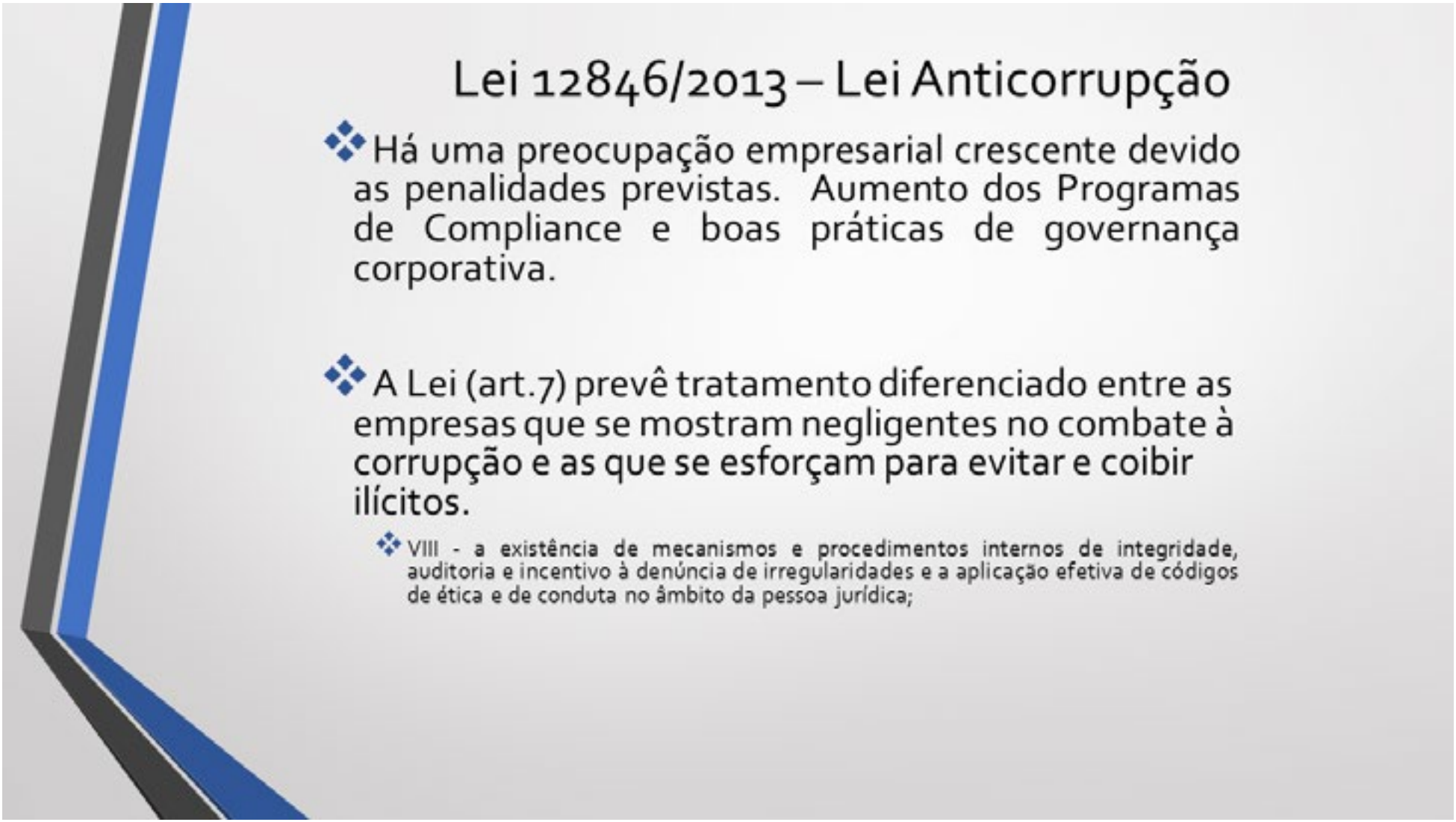
Sistemas de monitoramento de ameaças e ferramentas de análise de dados são imperativos para as organizações que estão na vigilância contra comportamentos estranhos ou suspeitos.

Legislação	Temas abrangidos	Aplicação
Lei nº 8.429/1995	Improbidade, sanções aplicáveis aos agentes públicos nos casos de enriquecimento ilícito no exercício de mandato, cargo, emprego ou função na administração pública direta, indireta ou fundacional e dá outras providências.	Agentes públicos
Lei nº 12.527/2011	Acesso à Informação, Transparência ativa	União, Estados, Distrito Federal e Municípios. Entidades privadas sem fins lucrativos.
Lei nº 12.813/2013	Conflito de interesses, impedimento ao exercício do cargo ou emprego.	Agentes no exercício de cargo ou emprego do Poder Executivo federal.
Lei nº12.846/2013 – Decreto 8.420/2015	Prevenção – programas de integridade, responsabilização, atos lesivos, acordos de leniência.	Sociedades empresárias e às sociedades simples, personificadas ou não, independentemente da forma de organização ou modelo societário adotado, bem como a quaisquer fundações, associações de entidades ou pessoas, ou sociedades estrangeiras.
Decreto nº 9.203/2017	Governança	Administração Direta, autárquica e fundacional.
Portaria nº 903/2018	Modelo de Governança (I - Organização Institucional; II - Assessoramento e Acompanhamento Legislativo; III - Assuntos Orçamentários e Financeiros; IV - Governança Pública; V - Programa de Integridade; VI - Contratações; e VII - Passagens e Afastamentos do País)	Para órgãos subordinados e entidades vinculadas da Casa Civil da Presidência da República (IN /SDA/ INCRA/ ITI)
IN / CGU nº 01/2016	Governança, riscos e controles	Poder Executivo Federal
Lei nº 13.303 /2016 e Decreto 8945/2016 - Lei das Estatais	Governança e Licitações	Estatais e Sociedades de Economia Mista
Portarias CGU – sobre PI INs CGU/MPOG	Avaliação dos programas de integridade; acordos de leniência. Governança, controles, riscos, prestação de contas, transparência.	Administraçao Pública

Marco Regulatório
Lei 12.846/2013

- ***"Altera a ordem tradicional do combate à corrupção, ao contrário dessa concepção tradicional, que correlaciona atos ilícitos a castigos contra pessoas físicas, a Lei Anticorrupção instalou um sistema de incentivos econômicos para que as pessoas jurídicas efetivamente incorporem mecanismos de compliance".***

- A lógica é PREVENTIVA, uma vez que a adoção do COMPLIANCE, senão impeçam, ao menos atenuem os atos de corrupção.


Lei 12846/2013 – Lei Anticorrupção
Há uma preocupação empresarial crescente devido as penalidades previstas. Aumento dos Programas de Compliance e boas práticas de governança corporativa.
A Lei (art.7) prevê tratamento diferenciado entre as empresas que se mostram negligentes no combate à corrupção e as que se esforçam para evitar e coibir ilícitos.
VIII - 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 jurídica;


Como atender a Lei Anticorrupção?
Programa de Integridade
PREVENÇAO
DETECÇAO
APURAÇAO
PROGRAMA DE INTEGRIDADE
INSTÂNCIA, AUTORIDADE E INDEPENDÊNCIA
ANÁLISE DE RISCOS
CONTROLES E PROCEDIMENTOS
Investigações internas
Responder rapidamente e investigar os fatos.
A realização de uma investigação interna robusta poderá resultar em benefícios concretos para a empresa.
Estabelecimento de canais de denúncias.
Due diligence de terceiros
Efetivo processo de due diligence anticorrupção específico em terceiros é fator extremante importante para reduzir riscos.
MONITORAMENTO

Principais aspectos da Lei que deverão ser implementados pelas empresas

DECRETO Nº 8.420, DE 18 DE MARÇO DE 2015

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.

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:

Incisos I a XVI

Pág. 51 – *Livro de Compliance*

Exigência de Programas de Integridade nas contratações

Lei 7753/17 | Lei nº 7753 de 17 de outubro de 2017. do Rio de janeiro
Dispõe sobre a instituição do programa de integridade nas empresas que contratarem com a administração pública do estado do rio de janeiro e dá outras providencias.

Lei nº 6.112, de 02 de fevereiro de 2018
Distrito Federal
Dispõe sobre a obrigatoriedade da implantação do programa de integridade nas empresas que contratarem com a administração pública do distrito federal, em todas esferas de poder, e dá outras providências.

MAPA

Portaria 877, Ministério da Agricultura, Pecuária e Abastecimento
Torna obrigatória a exigência nos seus editais de licitação e respectivos contratos a implantação de programas de integridade pelos contratados pelo órgão, a partir da data da publicação da portaria. A exigência será aplicada a todos os contratos firmados que possuam valor igual ou superior a R$ 5 milhões, e a efetividade do programa de integridade pelo contratado deverá ser comprovada ao Ministério no prazo de até nove meses, a contar da data da assinatura do contrato.

Projeto de lei 723/17, em tramitação na Câmara Municipal de São Paulo, em que se estipula como critério de desempate a existência de programa de integridade pelo licitante.

PL 1292/95 - 6.814/17, que trata da modernização da lei de Licitações e Contratos estabelece que o edital de licitação pode prever a obrigatoriedade de implantação de Programa de Integridade pelo licitante vencedor.

Decreto nº 9203/2017

- GOVERNANÇA PÚBLICA E O NOVO DECRETO Nº 9203/2017: MOTIVAÇÃO, COMPLIANCE, RESPONSIVIDADE E GESTÃO DE RISCOS
- O Decreto fixa conceitos de governança pública, valor público, alta administração e gestão de riscos (artigo 2º); estabelece os princípios e diretrizes da governança pública (artigos 3º e 4º), bem como os mecanismos para o seu exercício (artigo 5º); atribui à alta administração a incumbência de implementar e manter mecanismos de governança (artigo 6º); e dispõe sobre a composição, funcionamento e atribuições do Comitê Interministerial de Governança – CIG (artigo 7º e seguintes).
- Fator fundamental: **Liderança** do gestor público, definida como "*o conjunto de práticas de natureza humana*", dentre as quais merecem destaque a motivação e a responsabilidade.

Decreto nº 9203/2017

- Decreto estabelece que os órgãos e as entidades da administração direta deverão instituir **programa de integridade** (art. 19).
- **Política de gerenciamento de riscos**, visa garantir à instituição o atingimento de seus objetivos da forma mais eficaz, foco principal de uma boa governança. A gestão de riscos é estabelecida como um mecanismo de governança (art. 5º, III).

Portaria nº 903, 31/07/2018

- Estabelece medidas de governança para órgãos subordinados e entidades vinculadas da Casa Civil da Presidência da República.
- Os conceitos e os princípios constantes da política de governança da administração pública federal direta, autárquica e fundacional prevista no Decreto nº 9.203.

Art. 3º Os órgãos e as entidades previstos no caput do art. 1º deverão estabelecer medidas de estruturação de modelo de governança, no mínimo, para os seguintes temas de governança:

- I - Organização Institucional;
- II - Assessoramento e Acompanhamento Legislativo;
- III - Assuntos Orçamentários e Financeiros;
- IV - **Governança Pública;**
- V - Programa de Integridade;
- VI - **Contratações; e**
- VII - Passagens e Afastamentos do País.

Portaria nº 903, 31/07/2018

- **Art. 7º Para o tema de governança Governança Pública, as medidas a que se refere o art. 3º devem observar as seguintes diretrizes:**
  - I - instituir **comitê interno de governança, nos termos do art. 14 do Decreto nº 9.203**, de 22 de novembro de 2017, ou atribuir as competências correspondentes a colegiado já existente, por ato de seu dirigente máximo;
  - II - incentivar e promover iniciativas para implementar o acompanhamento de resultados no órgão ou entidade e promover soluções para melhoria do desempenho institucional;
  - III - incentivar e promover iniciativas que adotem instrumentos para o aprimoramento do processo decisório, como a segregação de funções para mitigação de riscos e a difusão do modelo de decisões colegiadas;
  - IV - **promover e acompanhar a implementação das medidas, dos mecanismos e das práticas organizacionais de governança definidos pelo Comitê Interministerial de Governança em seus manuais, resoluções e recomendações, e pelos referenciais de governança aplicáveis a órgãos e entidades da administração pública, dentre eles, o Índice Integrado de Governança e Gestão do Tribunal de Contas da União**; e
  - V - publicar as decisões do comitê interno de governança ou do órgão colegiado equivalente, em sítio eletrônico do órgão ou entidade, ressalvado o conteúdo sujeito a sigilo, conforme previsto no art. 16 do Decreto nº 9.203, de 22 de novembro de 2017.

Lei 13.303 /2016 e Decreto 8945/2016 Lei das Estatais

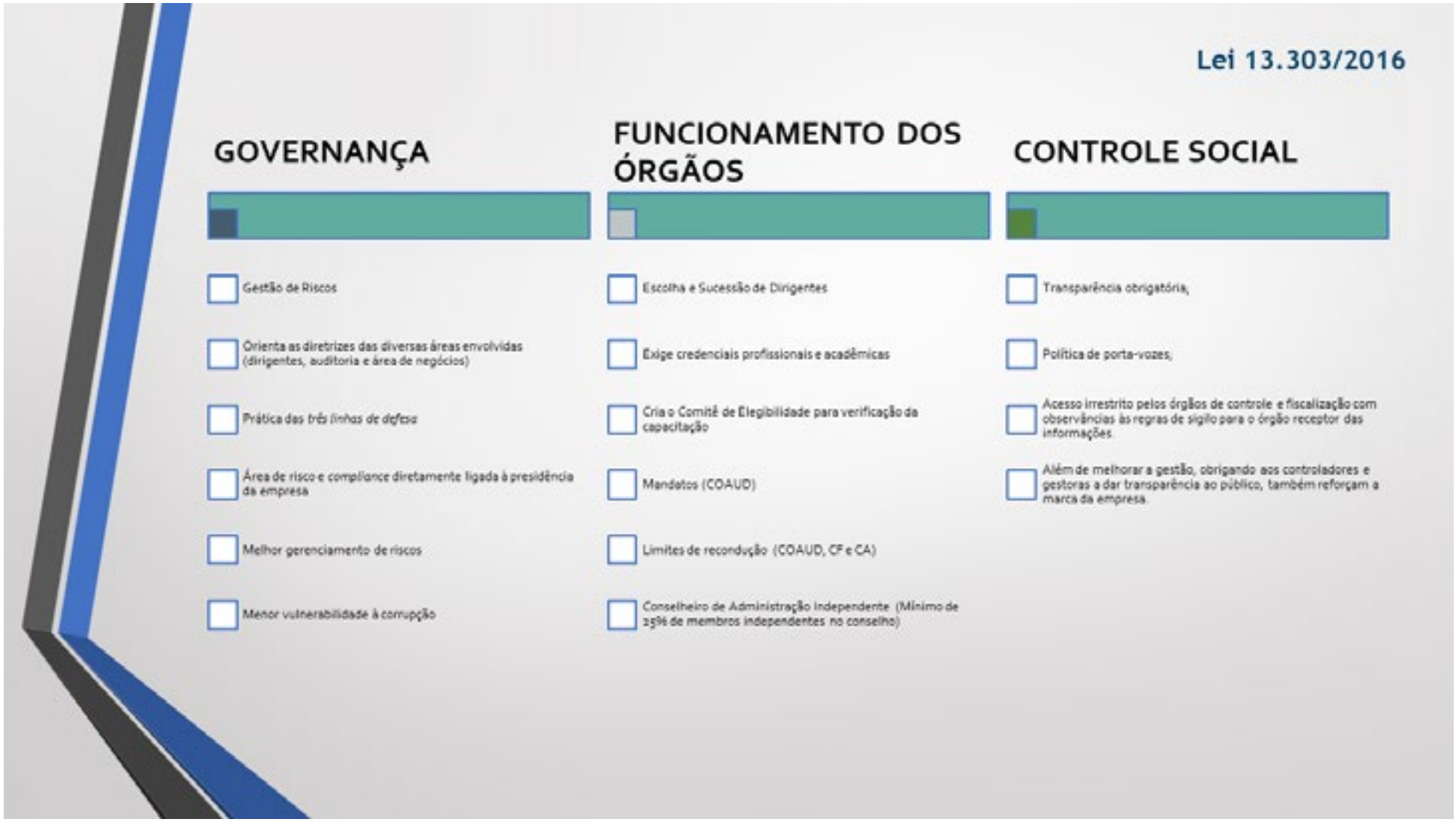
- Constituição Federal - Art. 173

O objetivo é buscar, para as empresas estatais que exploram atividade econômica, regras menos rígidas ou formalistas, de modo a conferir a elas maior flexibilidade gerencial, dado o regime de competição que lhes é imposto.

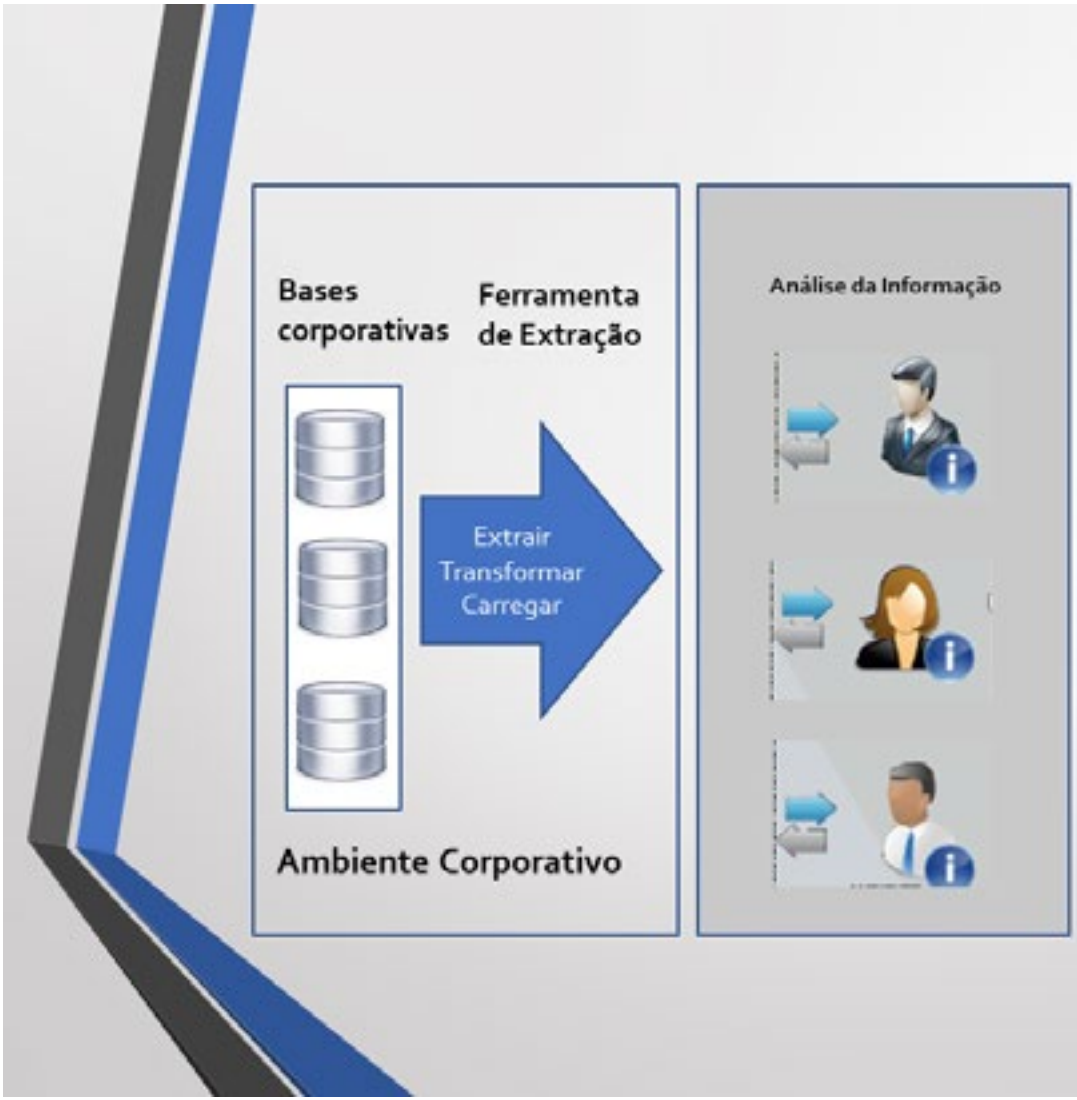
Lei 13.303 /2016 e Decreto 8945/2016
Lei das Estatais

- A Lei 13.303/2016 pode ser dividida em dois grandes temas:
  - **Regras de Governança e regime societário** (conjunto de normas sobre governança corporativa, transparência na gestão e mecanismos de controle da atividade empresarial);
  - **Licitações e Contratos** (normas sobre licitação e contratação a serem observadas pelas empresas estatais)
- **Apesar de estarem dispostos em capítulos diferentes os temas estão relacionados pois a "flexibilização" das regras de licitação depende da adoção de elementos de governança e gestão que evitem atos lesivos ou abusivos.**


Lei 13.303/2016
TRANSPARÊNCIA
Obrigatoriedade de elaboração e divulgação de diversos documentos
Carta anual: Recursos a serem empregados para consecução de políticas públicas, bem como dos impactos econômico-financeiros
Política de transações com partes relacionadas
Código de conduta e integridade: Prevenção de conflitos de interesses e corrupção; treinamento periódico; canal de denúncias.
Relatório de sustentabilidade; dentre outros
MONITORAMENTO
Instalação de estruturas internas
Comitês Estatutários: COAUD - Previsto expressamente como órgão auxiliar do conselho de administração. Composto de maioria de membros independentes e responsável por receber denúncias
Área responsável pela verificação de cumprimento de obrigações (compliance) e de gestão de riscos
Auditoria interna: Vinculada ao conselho de administração, diretamente ou por meio do comitê de auditoria estatutário
PRÁTICAS DE GESTÃO
Reforço de profissionalização e independência dos administradores
Associação a metas quantificáveis
Qualificação e experiência mínimas
Vedação a membros do governo (reguladores, ministros, secretários e alta administração) e políticos
Avaliação de desempenho, individual e coletiva, de periodicidade anual, dos administradores e dos membros de comitês

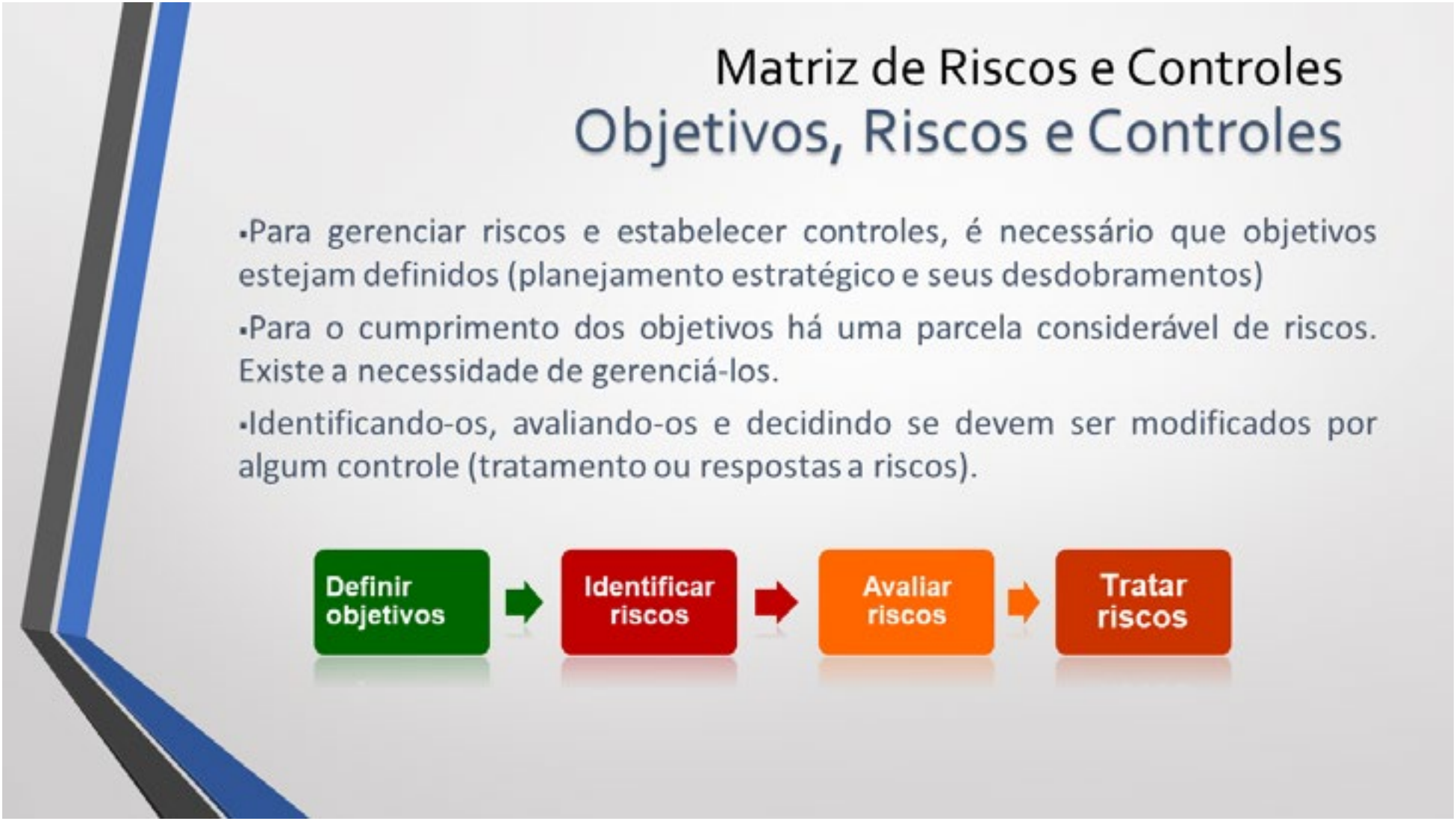

Lei 13.303/2016
GOVERNANÇA
Gestão de Riscos
Orienta as diretrizes das diversas áreas envolvidas (dirigentes, auditoria e área de negócios)
Prática das três linhas de defesa
Área de risco e compliance diretamente ligada à presidência da empresa
Melhor gerenciamento de riscos
Menor vulnerabilidade à corrupção
FUNCIONAMENTO DOS ÓRGÃOS
Escolha e Sucessão de Dirigentes
Exige credenciais profissionais e acadêmicas
Cria o Comitê de Elegibilidade para verificação da capacitação
Mandatos (COAUD)
Limites de recondução (COAUD, CF e CA)
Conselheiro de Administração Independente (Mínimo de 25% de membros independentes no conselho)
CONTROLE SOCIAL
Transparência obrigatória;
Política de porta-vozes;
Acesso irrestrito pelos órgãos de controle e fiscalização com observâncias às regras de sigilo para o órgão receptor das informações.
Além de melhorar a gestão, obrigando aos controladores e gestoras a dar transparência ao público, também reforçam a marca da empresa.

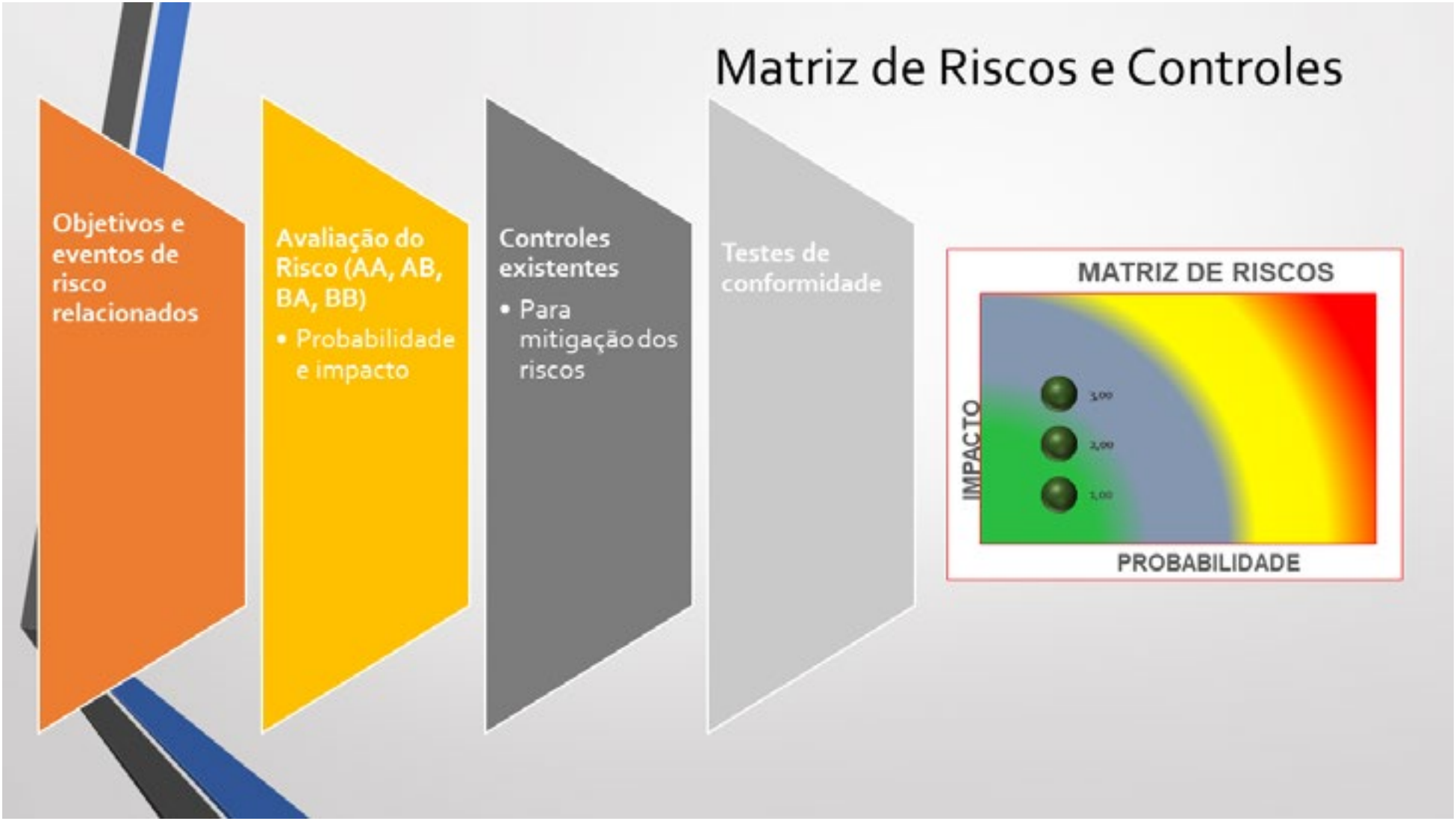

Boas práticas
Monitoramento e controle – uso da tecnologia como apoio para a tomada de decisão.
Matriz de riscos
Modelo integrado de riscos e controles
Ações de controles/conformidade



- Utilização de sistemas de extração de dados para análise e controle dos dados processados e necessidade de simulação com cruzamento.
- Pesquisa simulada cruzando informação de vários sistemas, com alarmes em cada pesquisa.

Case Licitações e Contratações
16 objetivos – redflags, entre eles:
- Existência de fracionamento de despesas ou fuga de modalidade;
- Contratação de fornecedor impedido de licitar;
- Empregados e dependentes nos quadros societários.


Matriz de Riscos e Controles
Objetivos, Riscos e Controles
•Para gerenciar riscos e estabelecer controles, é necessário que objetivos estejam definidos (planejamento estratégico e seus desdobramentos)
•Para o cumprimento dos objetivos há uma parcela considerável de riscos. Existe a necessidade de gerenciá-los.
•Identificando-os, avaliando-os e decidindo se devem ser modificados por algum controle (tratamento ou respostas a riscos).
Definir objetivos
Identificar riscos
Avaliar riscos
Tratar riscos


Matriz de Riscos e Controles
Objetivos e eventos de risco relacionados
Avaliação do Risco (AA, AB, BA, BB)
• Probabilidade e impacto
Controles existentes
• Para mitigação dos riscos
Testes de conformidade
MATRIZ DE RISCOS
IMPACTO
PROBABILIDADE


COMUNICADO
IMPORTANTE


SECURITY &
COMPLIANCE

Medo de sujar CPF paralisa a tomada de decisões no governo

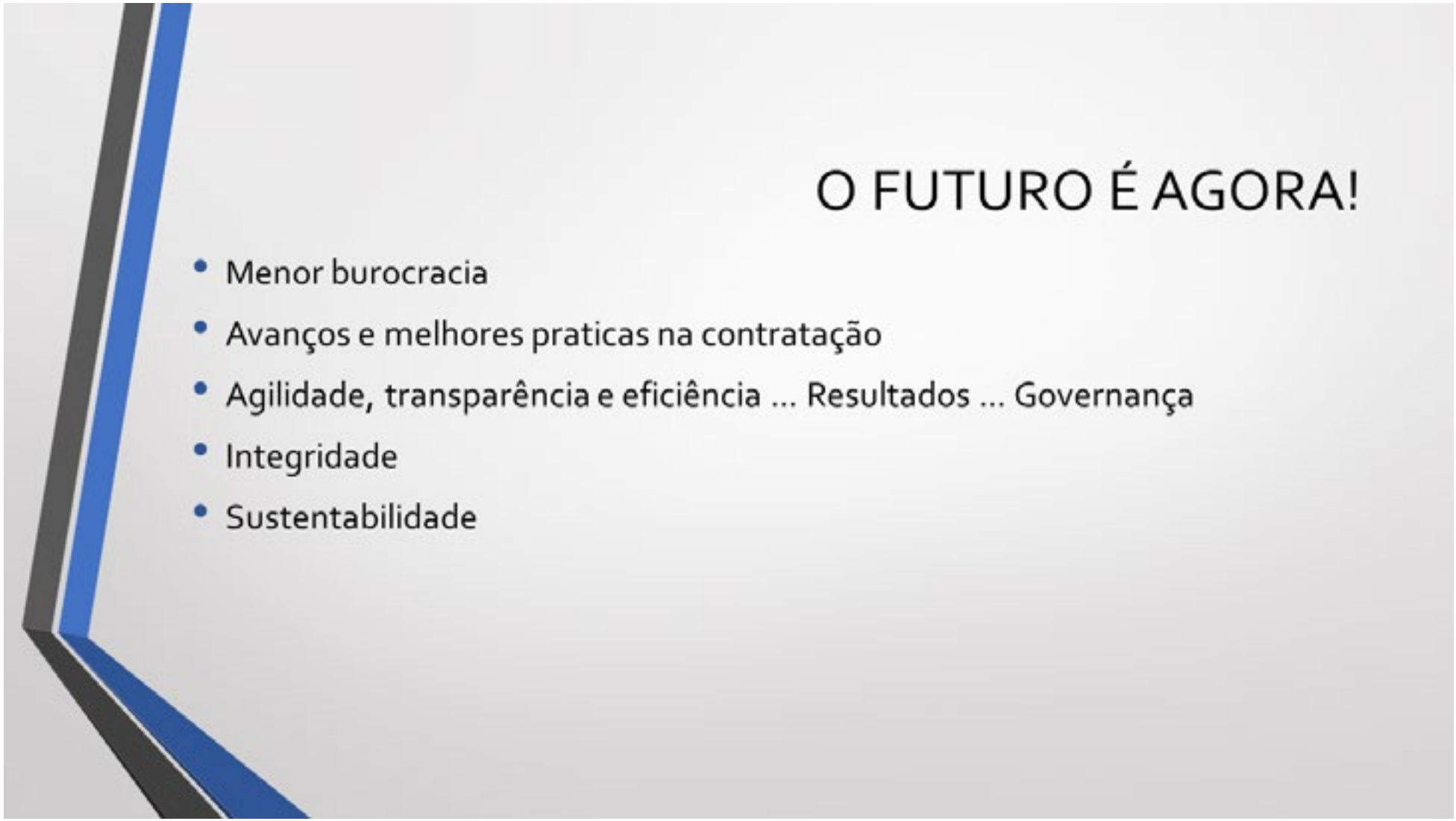
Um fato novo, porém, foi levantado espontaneamente como entrave para destravar projetos de infraestrutura. Novo porque, há cinco ou dez anos, praticamente não se falava disso. É o que César Borges, ex-ministro dos Transportes e hoje presidente da Associação Brasileira das Concessionárias de Rodovias, chama de "apagão de canetas" nas entranhas do Estado.

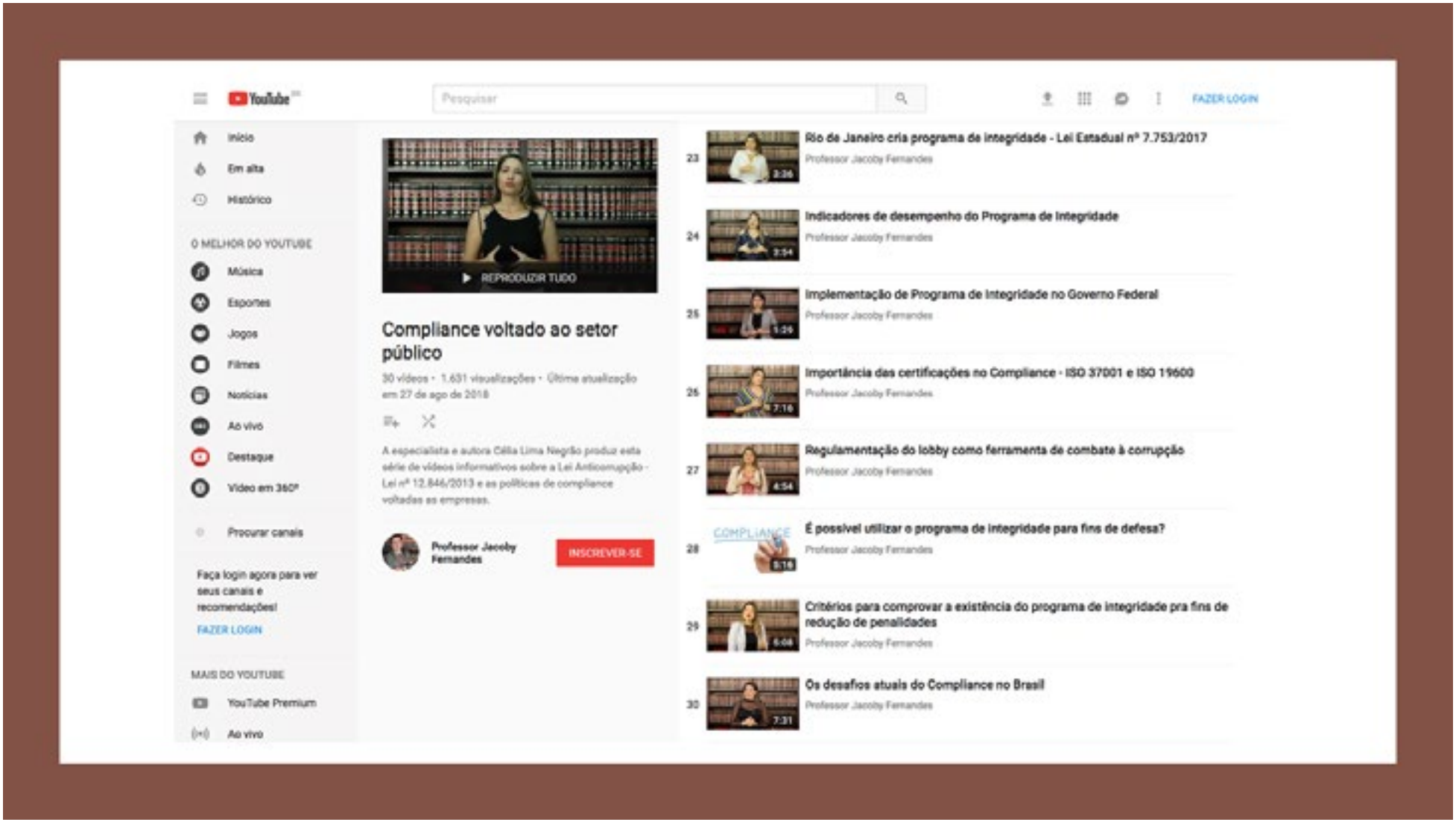
Trata-se do temor de gestores públicos de assinar qualquer documento que lhes possa comprometer — inclusive como pessoa física — mediante os órgãos de controle e a Justiça. A vigilância do Ministério Público e do Tribunal de Contas da União (TCU), com deveres constitucionais de fiscalizar, às vezes é tão forte que resulta em uma semiparalisia da máquina estatal. Em outras palavras, o receio de sujar o CPF faz com que agentes do Poder Executivo ajam com tal excesso de cautela que decisões de risco passam a ser evitadas ao máximo. Instala-se uma cultura do medo nos ministérios, autarquias, agências. Ninguém quer botar sua digital em nada.

O próprio César Borges, um dos participantes da mesa redonda de ontem, sentiu na pele o que isso significa. Como ministro, enviou à Agência Nacional de Transportes

"Temor dos gestores em assinar qualquer documento"

"Excesso de cautela"
"Cultura do medo"


O FUTURO É AGORA!
Menor burocracia
Avanços e melhores praticas na contratação
Agilidade, transparência e eficiência ... Resultados ... Governança
Integridade
Sustentabilidade


YouTube
Pesquisar
FAZER LOGIN
Início
Em alta
Histórico
O MELHOR DO YOUTUBE
Música
Esportes
Jogos
Filmes
Notícias
Ao vivo
Destaque
Vídeo em 360º
Procurar canais
Faça login agora para ver seus canais e recomendações!
FAZER LOGIN
MAIS DO YOUTUBE
YouTube Premium
Ao vivo
REPRODUZIR TUDO
Compliance voltado ao setor público
30 vídeos • 1.631 visualizações • Última atualização em 27 de ago de 2018
A especialista e autora Célia Lima Negrão produz esta série de vídeos informativos sobre a Lei Anticorrupção - Lei nº 12.846/2013 e as políticas de compliance voltadas as empresas.
Professor Jacoby Fernandes
INSCREVER-SE
23 Rio de Janeiro cria programa de integridade - Lei Estadual nº 7.753/2017
Professor Jacoby Fernandes
2:36
24 Indicadores de desempenho do Programa de Integridade
Professor Jacoby Fernandes
3:54
25 Implementação de Programa de Integridade no Governo Federal
Professor Jacoby Fernandes
1:39
26 Importância das certificações no Compliance - ISO 37001 e ISO 19600
Professor Jacoby Fernandes
2:16
27 Regulamentação do lobby como ferramenta de combate à corrupção
Professor Jacoby Fernandes
4:54
28 É possível utilizar o programa de integridade para fins de defesa?
Professor Jacoby Fernandes
5:16
29 Critérios para comprovar a existência do programa de integridade pra fins de redução de penalidades
Professor Jacoby Fernandes
6:08
30 Os desafios atuais do Compliance no Brasil
Professor Jacoby Fernandes
7:31

Obrigada

Célia Lima Negrão

celiar@correios.com.br

Play list* sobre *compliance

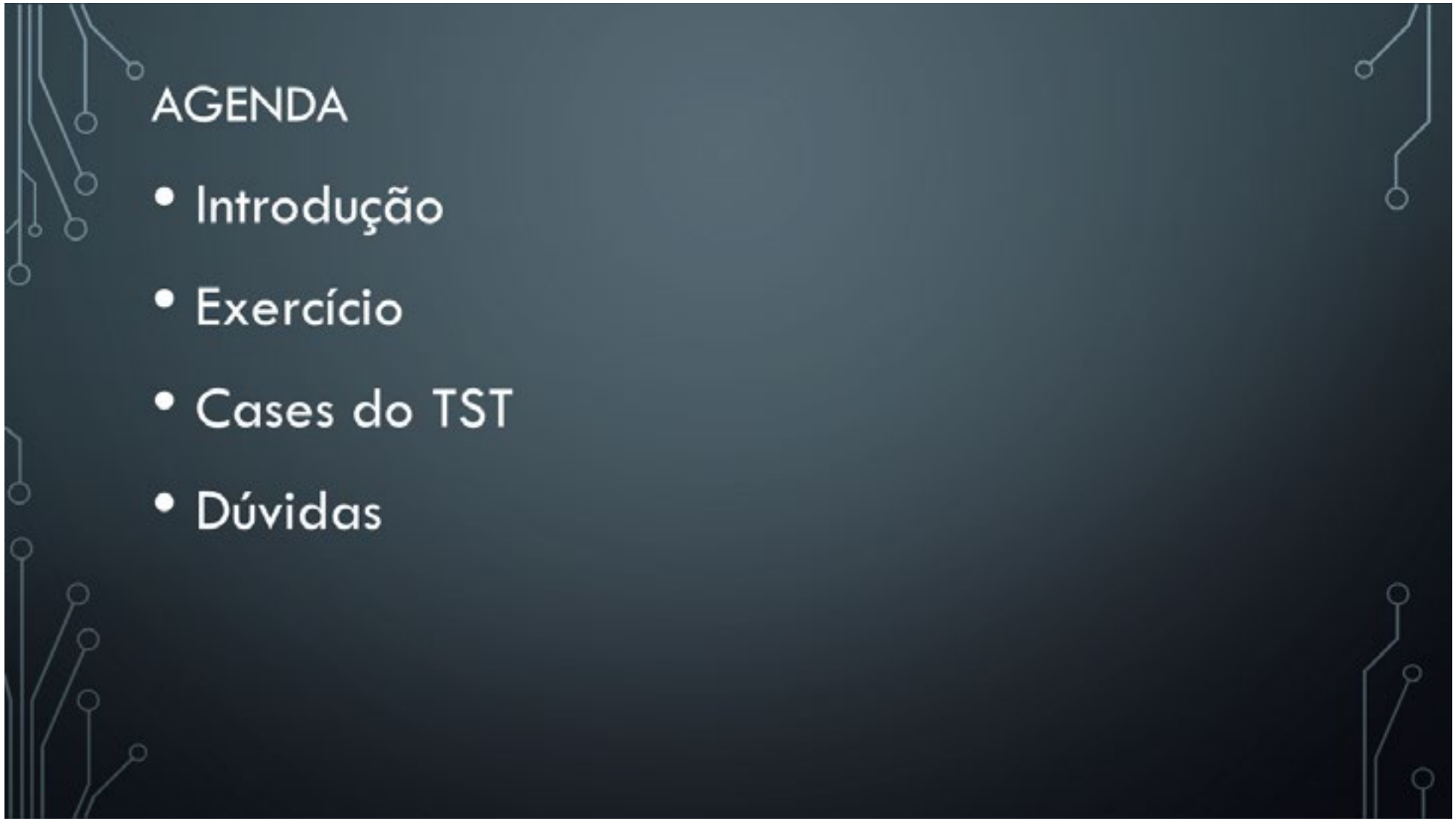
https://www.youtube.com/watch?v=52gE2rlR4bo&list=PLEeHNSDIsdOyhIos6PaNG4hJzpuqBvMBa

Apresentação 4:

Como mitigar riscos com a implantação de esteira de entrega contínua de software

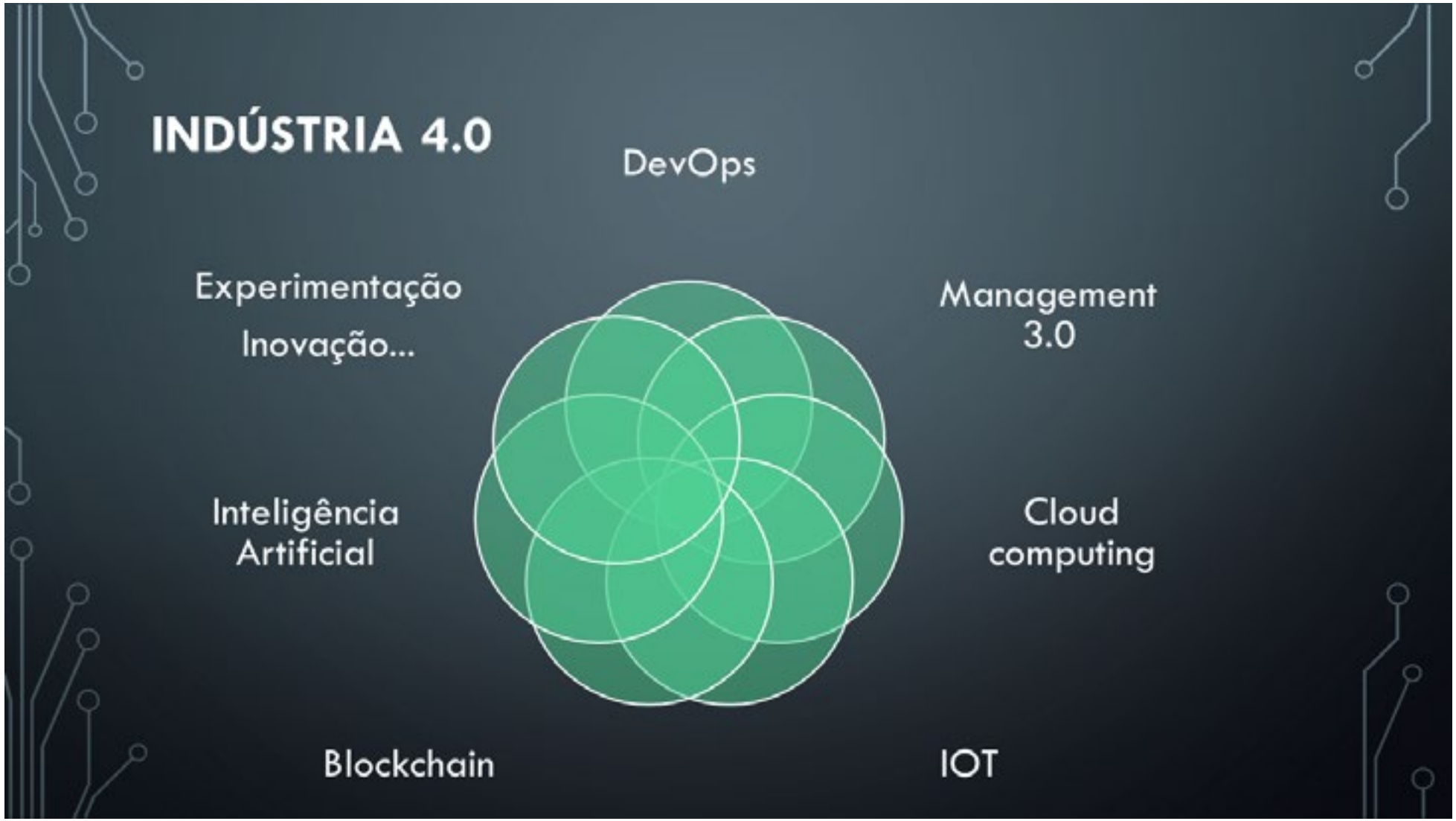
CLAUDSON MELO

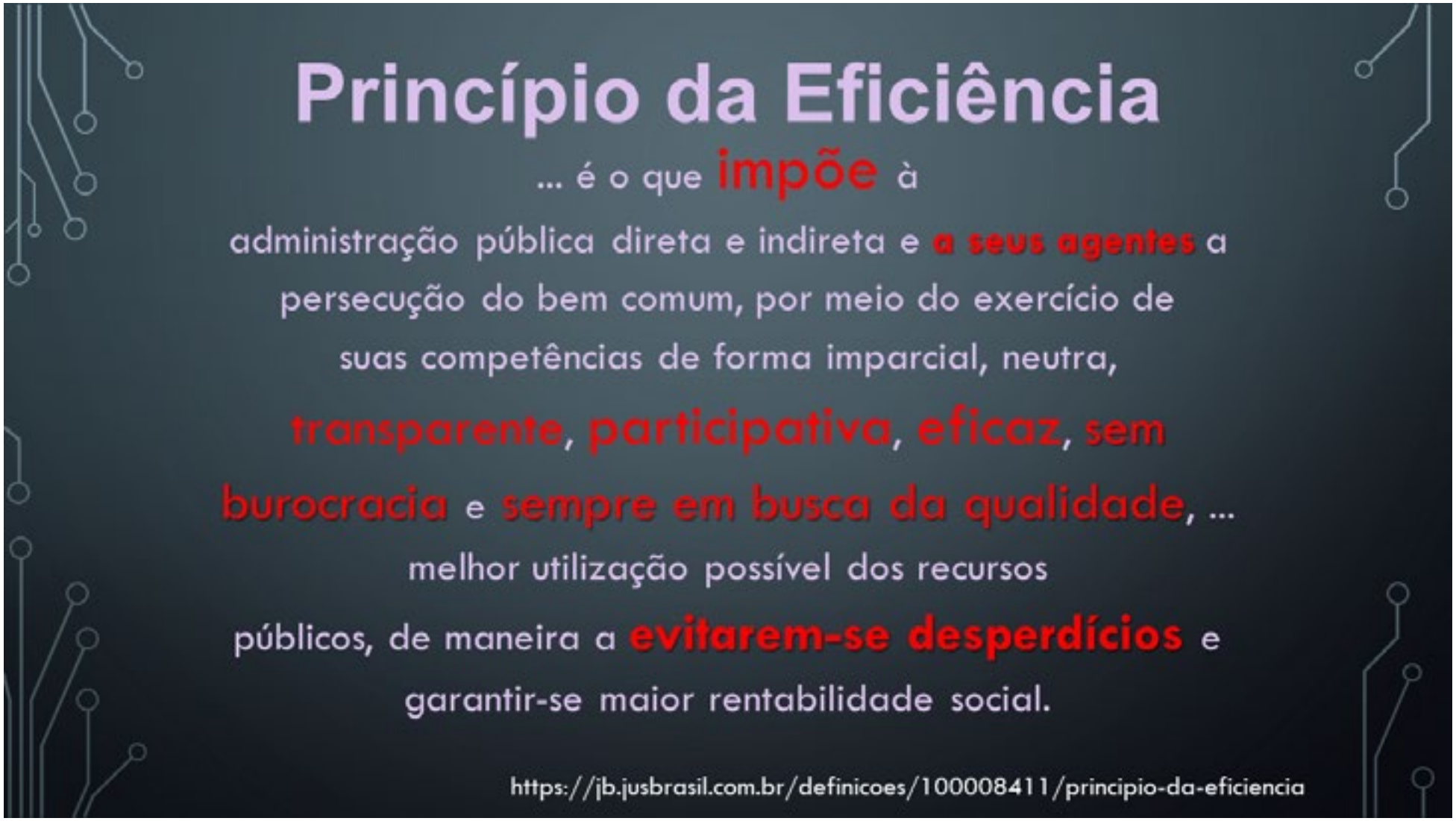

COMO MITIGAR RISCOS COM IMPLANTAÇÃO DE ESTEIRA DE ENTREGA CONTÍNUA DE SOFTWARE
TST
Tribunal Superior do Trabalho
CLAUDSON MELO

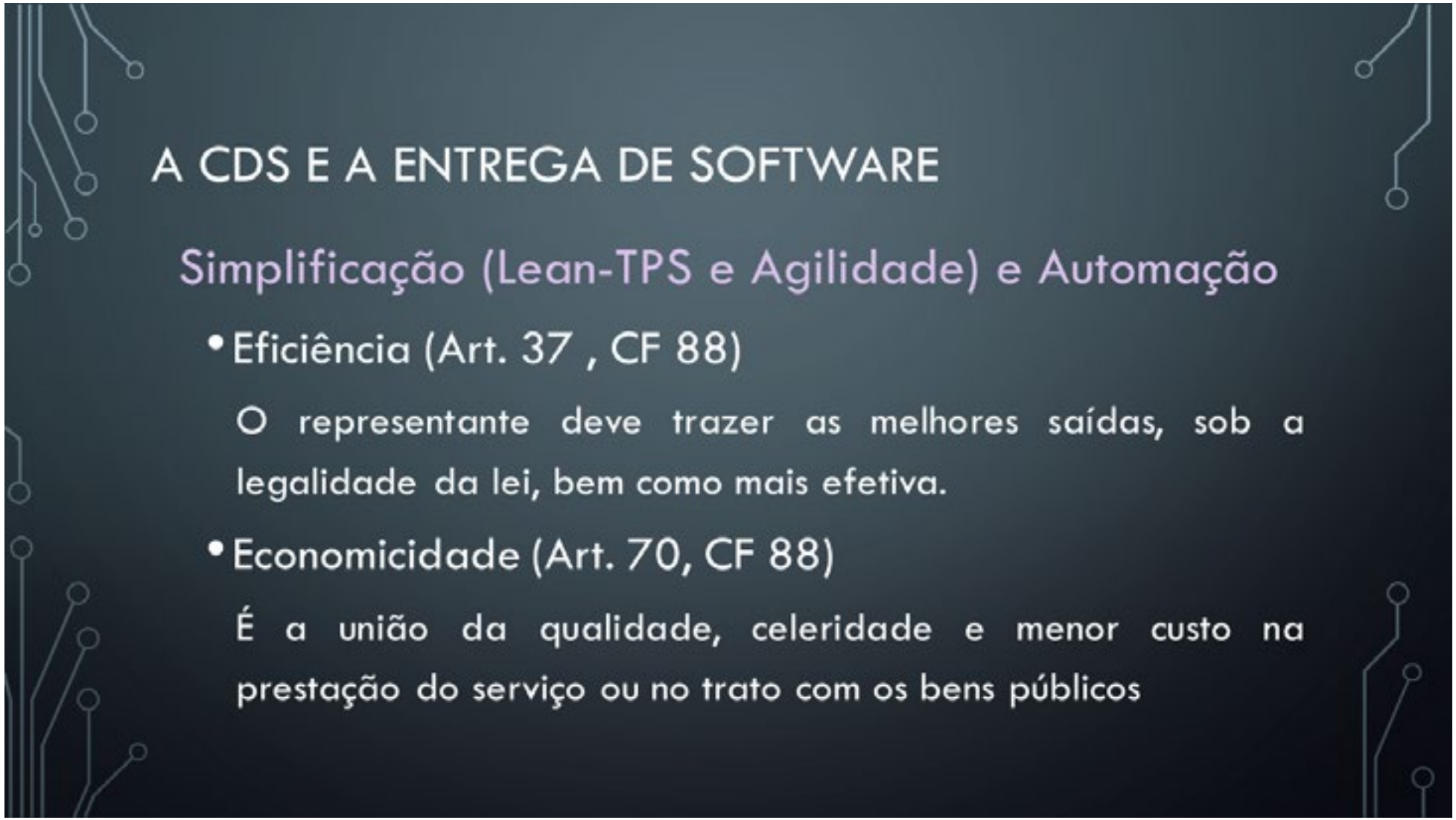

AGENDA
• Introdução
• Exercício
• Cases do TST
• Dúvidas

ASSUNTOS RECORRENTES EM EVENTOS RECENTES

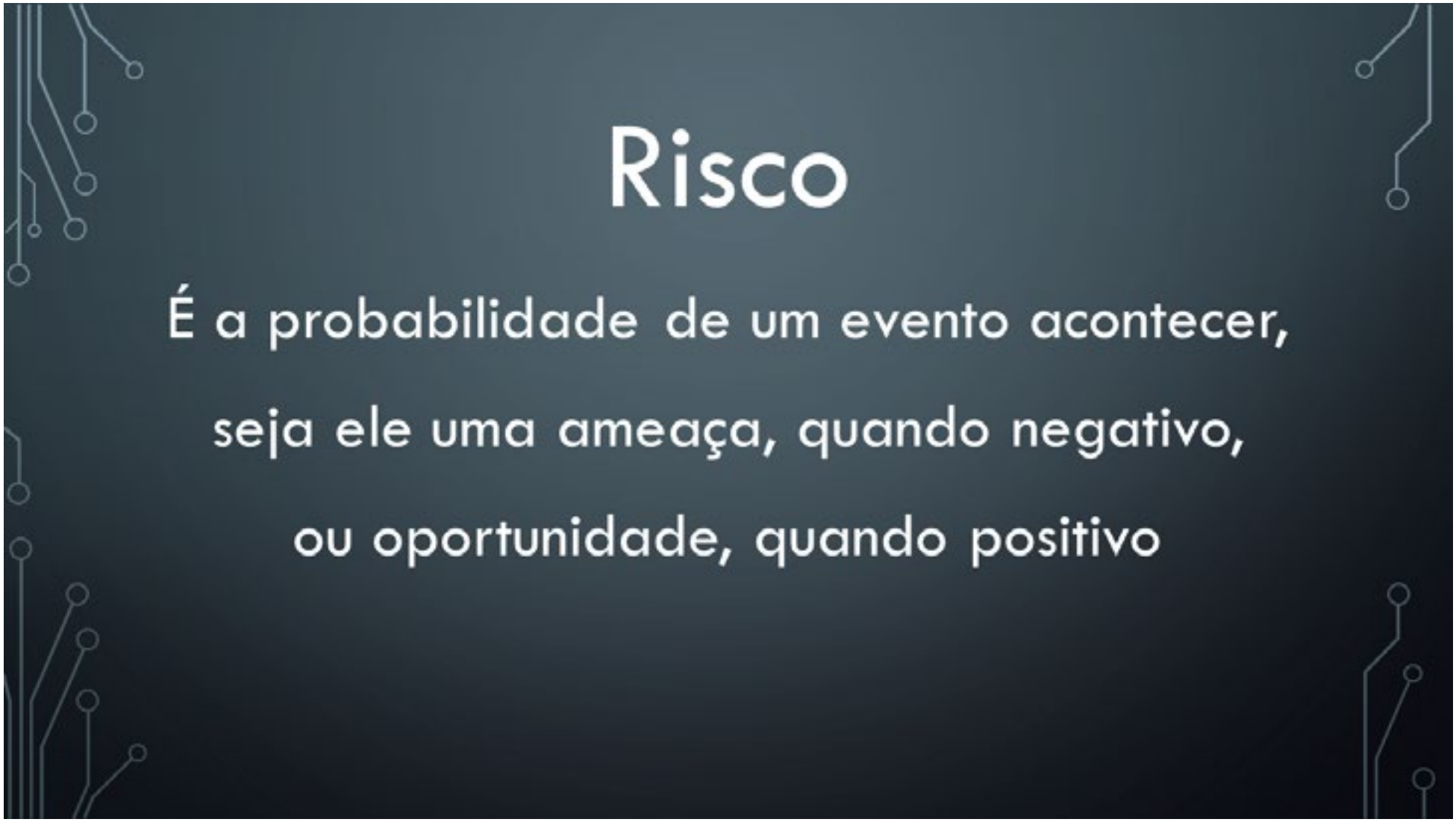
- Mudança cultural (maior desafio)
  - Respostas rápidas às mudanças (4ª Revolução Industrial; Ciclo de mudanças a cada 100 anos).
- Inovação:
  - "Democracia não se vence por nocaute. Se vence por acúmulo de pontos."; e "Quem tenta emplacar o novo tem os desafios de clarear e persistir; e de ser solitário". Ayres Brito (Ex-ministro do STF)


INDÚSTRIA 4.0
DevOps
Experimentação
Inovação...
Management
3.0
Inteligência
Artificial
Cloud
computing
Blockchain
IOT


Princípio da Eficiência
... é o que impõe à
administração pública direta e indireta e a seus agentes a
persecução do bem comum, por meio do exercício de
suas competências de forma imparcial, neutra,
transparente, participativa, eficaz, sem
burocracia e sempre em busca da qualidade, ...
melhor utilização possível dos recursos
públicos, de maneira a evitarem-se desperdícios e
garantir-se maior rentabilidade social.
https://jb.jusbrasil.com.br/definicoes/100008411/principio-da-eficiencia

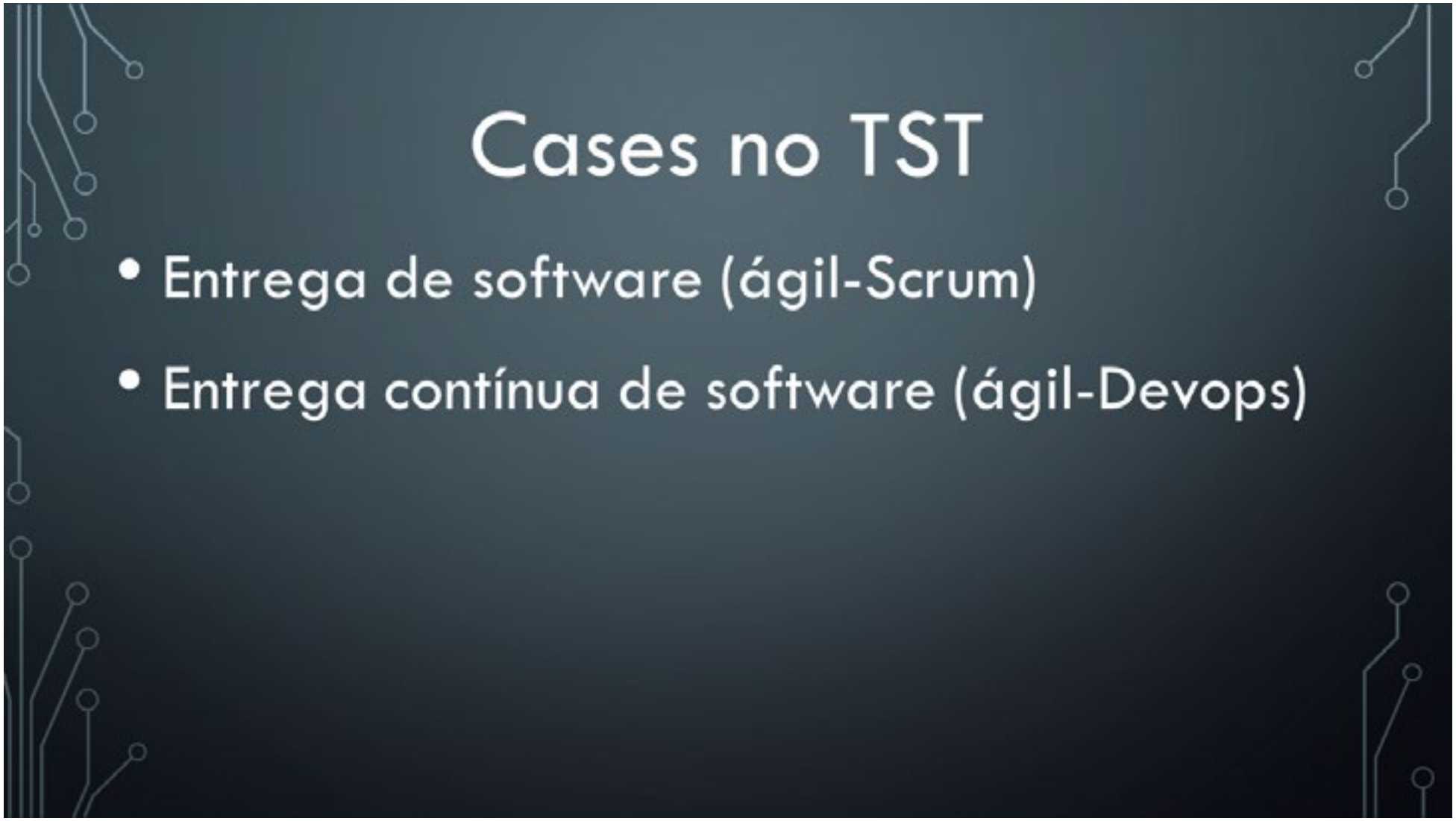

A CDS E A ENTREGA DE SOFTWARE
Simplificação (Lean-TPS e Agilidade) e Automação
• Eficiência (Art. 37 , CF 88)
O representante deve trazer as melhores saídas, sob a legalidade da lei, bem como mais efetiva.
• Economicidade (Art. 70, CF 88)
É a união da qualidade, celeridade e menor custo na prestação do serviço ou no trato com os bens públicos


Governança de TI
Deve entregar valor de forma consistente
Governança de Riscos
Garantir que os controles de GR sejam implementados e operem corretamente
ISACA


Risco
É a probabilidade de um evento acontecer,
seja ele uma ameaça, quando negativo,
ou oportunidade, quando positivo


Fases do gerenciamento de riscos
1. Identificar
2. Avaliar
3. Resposta e mitigação de riscos
4. Monitoramento e relatório de riscos e controle


Gestão
Build, Acquire and Implement - BAI
Construir, Adquirir e Implementar
BAI01 Gerenciar Programas e Projetos
BAI02 Gerenciar Definição de Requisitos
BAI03 Gerenciar Identificacao e Desenvolvimento de Solucoes
BAI04 Gerenciar Disponibilidade e Capacidade
BAI05 Gerenciar Capacidade de Mudanca Organizacional
BAI06 Gerenciar Mudancas
BAI07 Gerenciar Aceitacao e Transicao da Mudanca
BAI08 Gerenciar Conhecimento
BAI09 Gerenciar Ativos
BAI10 Gerenciar Configuracao
COBIT


Cases no TST
• Entrega de software (ágil-Scrum)
• Entrega contínua de software (ágil-Devops)


Exercício: Identificar eventos de risco
Cenário: Construção ágil de soft. baseado no Scrum.
Papéis: PO, Scrum Master e Time
Ritos: Refinamento; Sprint Planning; Diárias; Demo; Retrospectiva
Eventos esperados: Entregas rápidas (2 semanas); Ciclo de feedbacks contínuos; e Priorização (Eficácia)

Alguns possíveis riscos

Evento de Risco: Produto da Sprint não é validado por usuários finais.

Causa: 1. PO foca em requisitos gerenciais. 2. Administração quer cortar fita e não deseja antecipar o produto.

Consequência: sem feedback; sem pareto.

Evento de Risco: Produto da Sprint é um grande pacote de software.

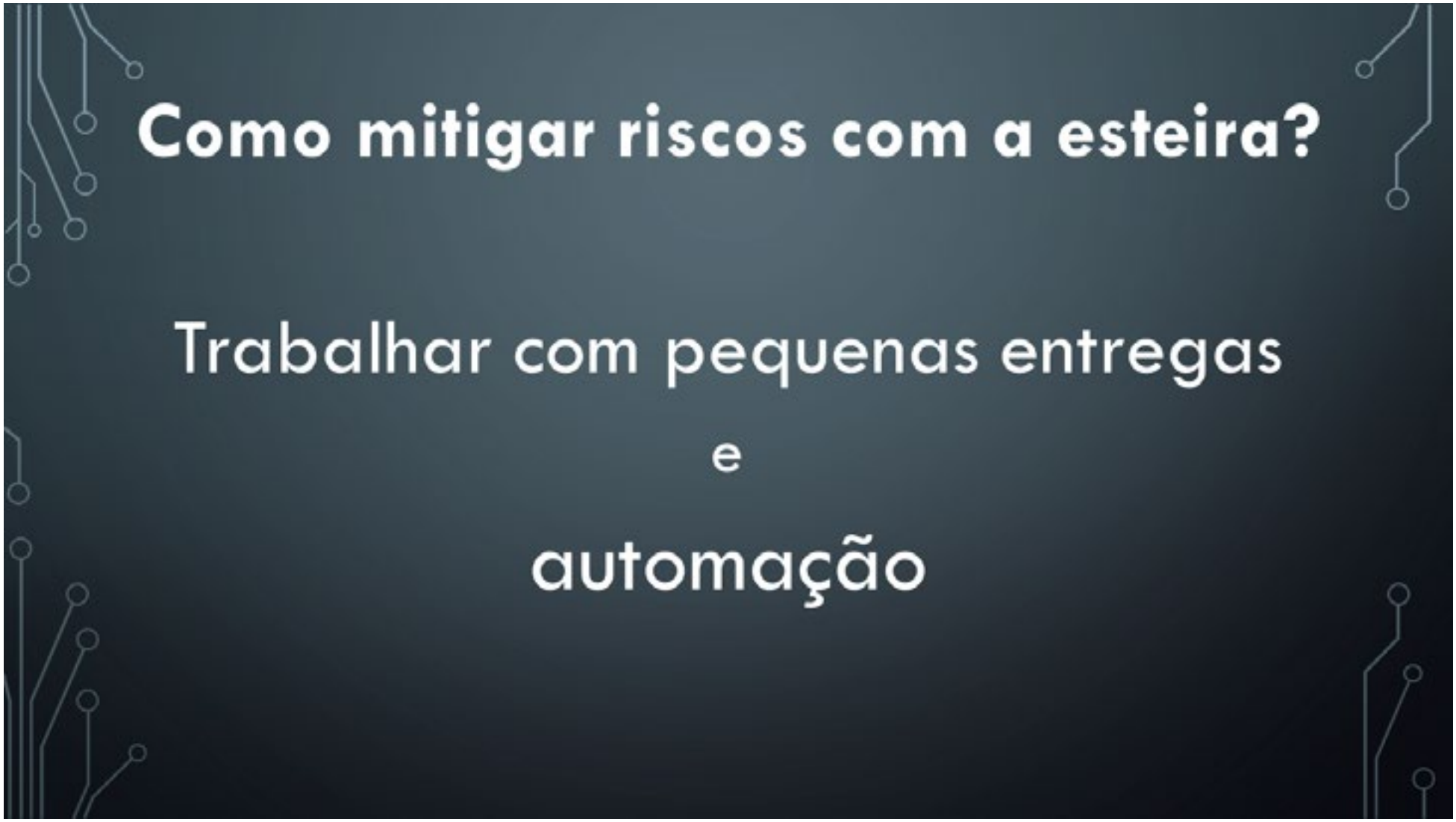
Causa: 1. PO tem medo que a pequena entrega resulte no fim do projeto. 2. SM não atuante.

Consequência: entrega-se mais que o necessário; Requisitos podem estar obsoletos na entrega; Retrabalho (desperdício).

Evento de Risco: Entrega da Sprint demora a ser disponibilizada (Janela GDM-liberação; comunicação, implantação).

Causa: 1. Necessidade por um ambiente estável. 2. Ineficiência nos gerenciamentos de liberação, implantação, gestão de mudança e comunicação.

Consequência: Usuário deixa de ser atendido de forma eficiente.

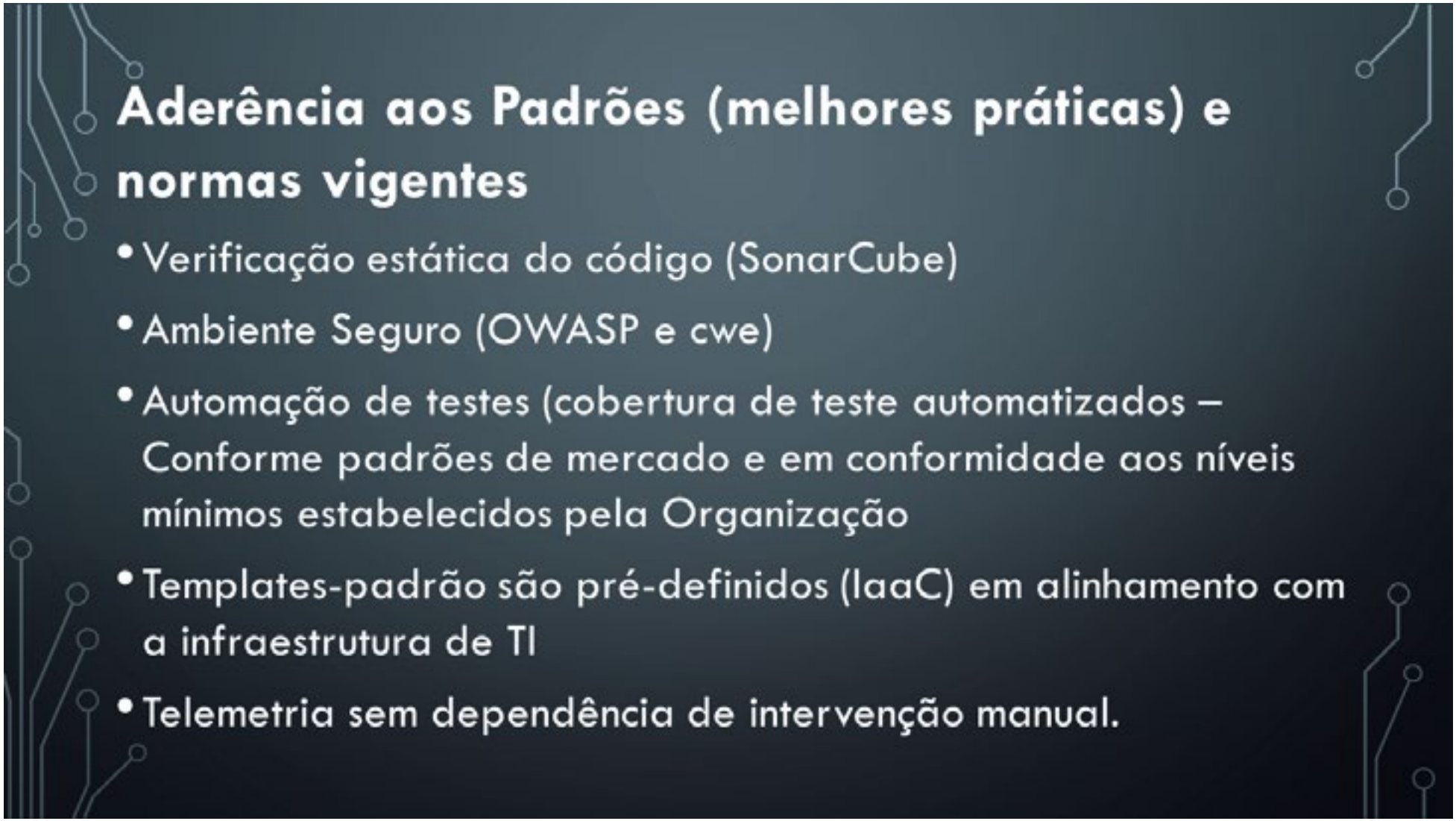

Como mitigar riscos com a esteira?
Trabalhar com pequenas entregas
e
automação

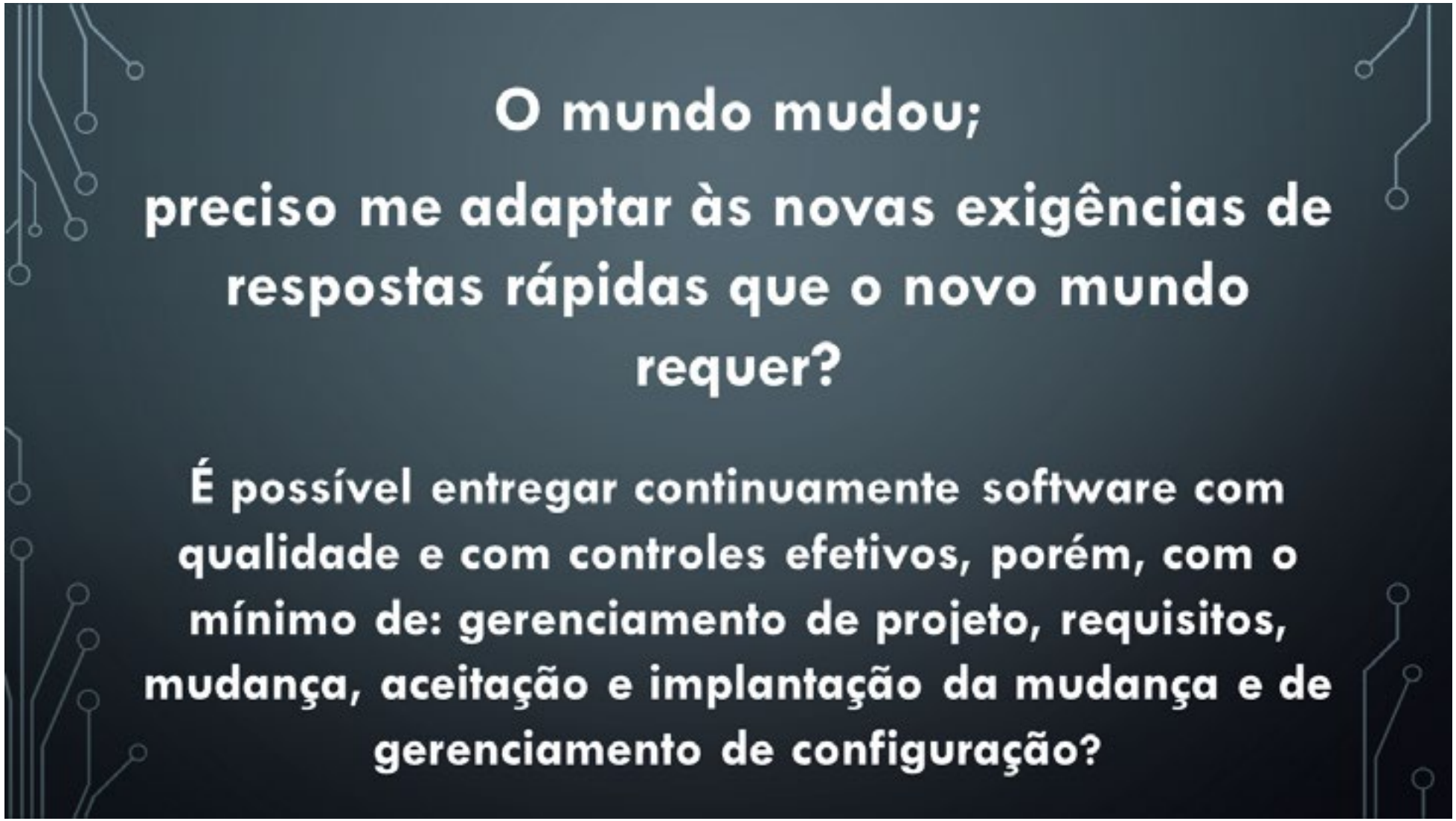
Benefícios advindos da esteira de entrega contínua de software

- Mudança de cultura organização (Dev+Segurança+Infra - DevSecOps)
- Pequenas entregas (2 a 3 dias) mitiga vários riscos
- Feedback rápido e contínuo (Fazer a coisa certa + pareto)
- Não paralisação da versão corrente do sistema em produção para disponibilização de versão mais nova.
- Possibilidade de retornar a versão anterior rapidamente.
- Possibilidade de ter melhor previsibilidade – Melhor gerenciamento

Aderência aos Padrões (melhores práticas) e normas vigentes

- Controle de versão (Gerenciamento de configuração – Git)
- O processo liberação e implantação estão automatizados na esteira.
- Integração contínua (Jenkins) – O fluxo de entrega segue padrão definido pelo Órgão.
- Gerenciamento das aplicações e alocação de recursos de forma dinâmica (garantia de maior disponibilidade do serviço por meio do OpenShift - Kurbenets)


Aderência aos Padrões (melhores práticas) e normas vigentes
• Verificação estática do código (SonarCube)
• Ambiente Seguro (OWASP e cwe)
• Automação de testes (cobertura de teste automatizados – Conforme padrões de mercado e em conformidade aos níveis mínimos estabelecidos pela Organização
• Templates-padrão são pré-definidos (IaaC) em alinhamento com a infraestrutura de TI
• Telemetria sem dependência de intervenção manual.


O mundo mudou;
preciso me adaptar às novas exigências de respostas rápidas que o novo mundo requer?
É possível entregar continuamente software com qualidade e com controles efetivos, porém, com o mínimo de: gerenciamento de projeto, requisitos, mudança, aceitação e implantação da mudança e de gerenciamento de configuração?

Muito obrigado!

claudson@tst.jus.br e claudson.melo@gmail.com

https://www.facebook.com/claudson.dossantosmelo

claudson-dos-santos-melo-0864a680

(61) 3043-4927 – (61) 99276-7725

Apresentação 5:

Resultados e Lições aprendidas de uma equipe que já sabia contratar

ANTÔNIO FERNANDES SOARES NETTO

APLICAÇÃO DA GESTÃO DE RISCOS EM UMA AQUISIÇÃO DE TECNOLOGIA DA INFORMAÇÃO: RESULTADOS E LIÇÕES APRENDIDAS DE UMA EQUIPE QUE JÁ SABIA CONTRATAR

LIVRO

www.jogodecontratacoes.com.br/livro

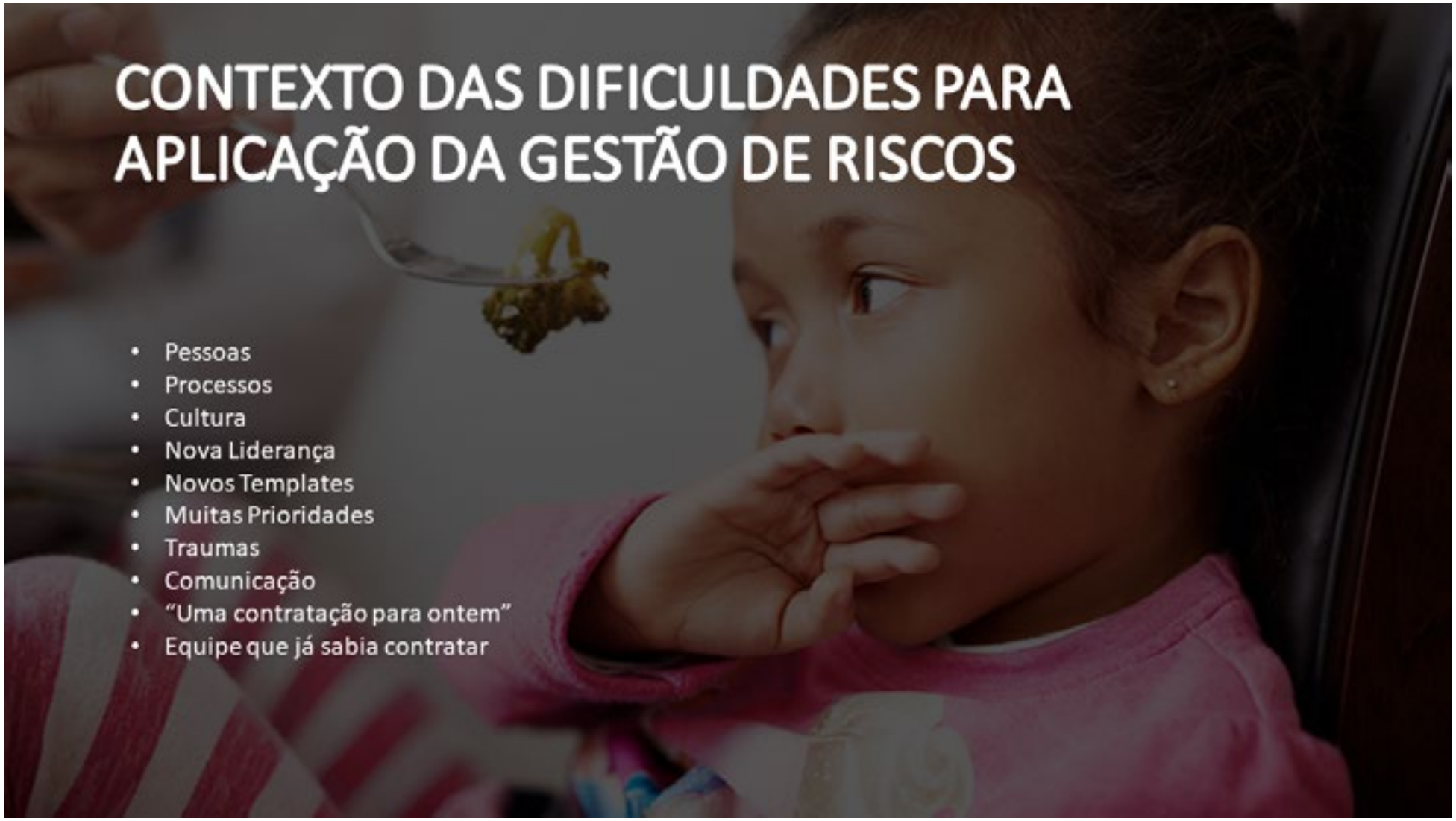
APRESENTAÇÃO

Antonio Fernandes Soares Netto

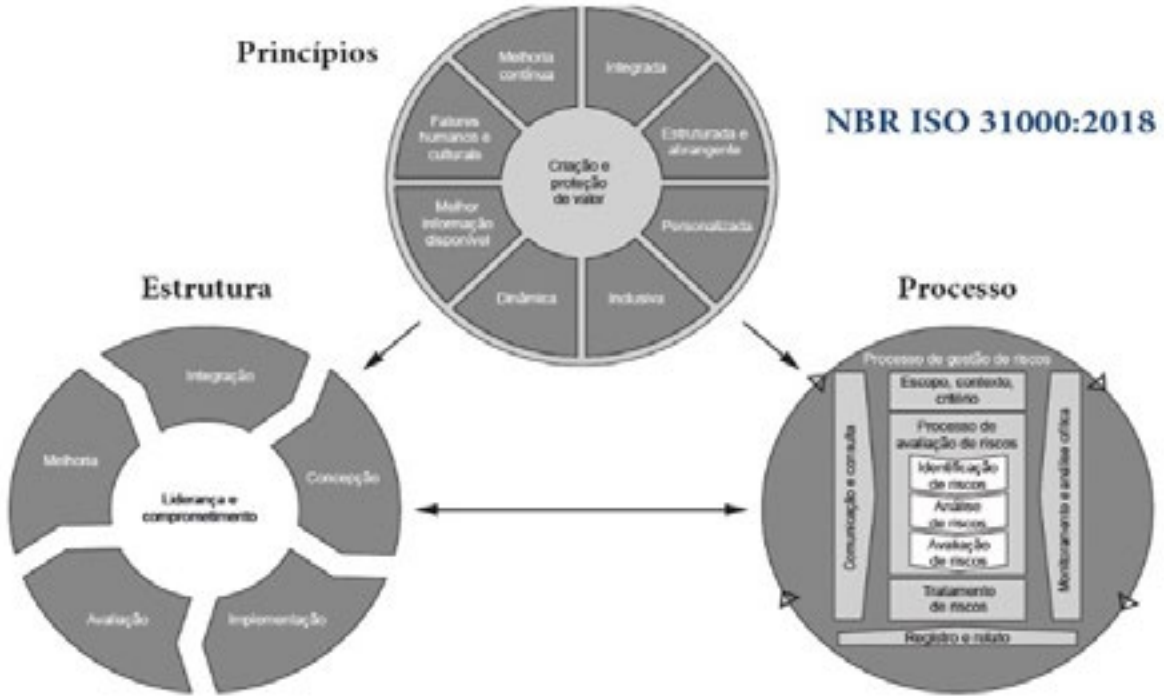
- Sobre TI (Estagiário e Técnico)
- Sobre Terceirização
- Sobre Mercado e Negócios
- Sobre Serviço Público (Técnico e Gestor***)
- Sobre Professor
- Sobre Pesquisador
- Sobre Tênis
- Sobre Game Designer
- Sobre o Autor do Livro e Projeto JC
- Sobre Liderança e Cargo
- Sobre Desafios, IN4 e Inovação
- Sobre o **Sistema Jogo de Contratações**
- Sobre o **Sistema de Gestão de Riscos**

ANTES DE COMEÇAR...

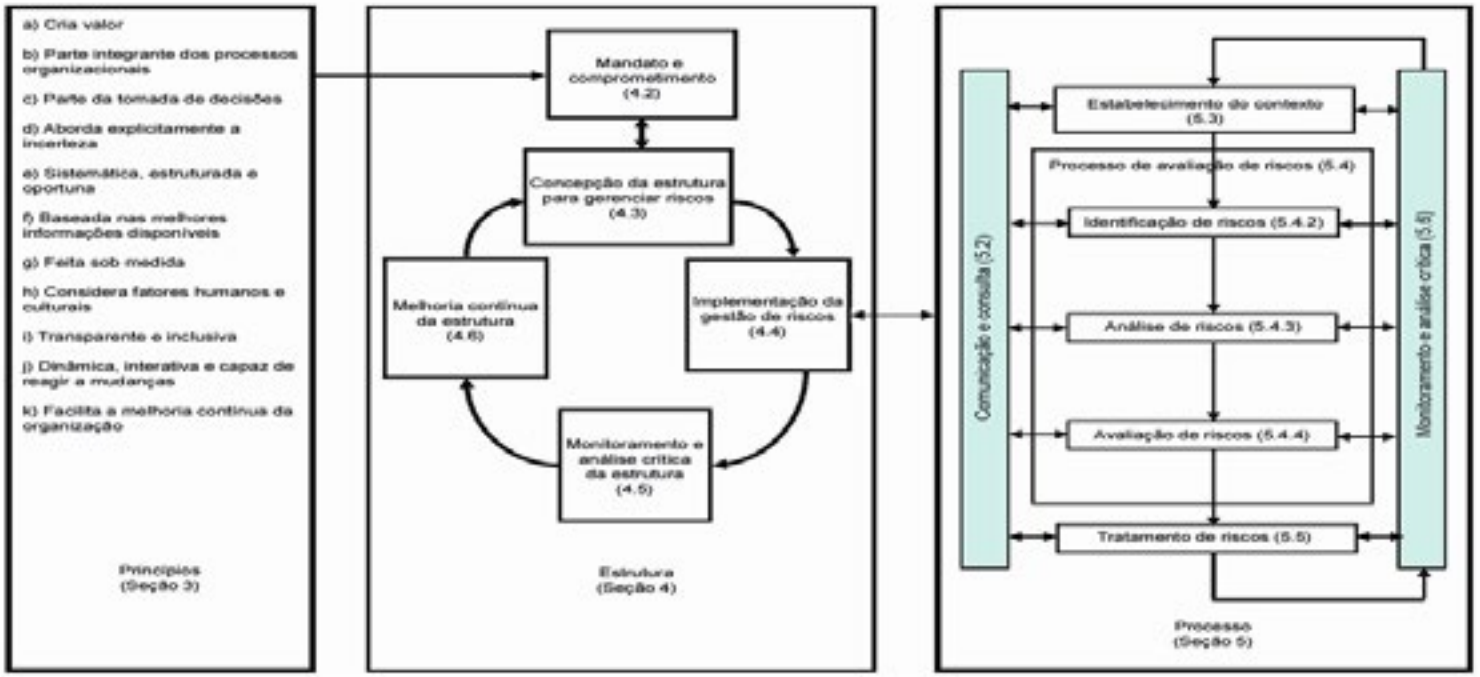
- Sobre o evento
- Objetivo principal
- Público alvo
- Metodologia
- Agenda


CONTEXTO DAS DIFICULDADES PARA APLICAÇÃO DA GESTÃO DE RISCOS
Pessoas
Processos
Cultura
Nova Liderança
Novos Templates
Muitas Prioridades
Traumas
Comunicação
“Uma contratação para ontem”
Equipe que já sabia contratar

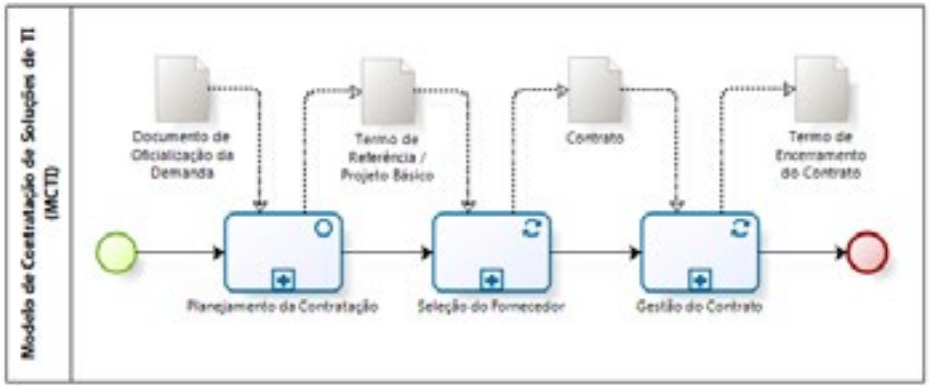
PRECISAMOS FALAR DE GESTÃO DE RISCOS



PRECISAMOS FALAR DE GESTÃO DE RISCOS



TEORIA x PRÁTICA




UM POUCO SOBRE
TECNOLOGIA,
RISCOS,
VERDADE...
• E TÊNIS...


Qual a “tecnologia” para se realizar uma aquisição de TIC?


Novos atores


Mais
comunicação


Stories
To Do
On Progress
Done :)
Métodos Ágeis para Contratações de TIC (Jogo de Contratações)

O CONTEXTO

- Priorização
- Seleção da contratação
- Definição dos papéis
- Definição do modo de trabalho (colaborativo, mas com um líder)
- Execução
- Monitoramento e análise crítica
- Comunicação e consulta
- Gestão de Riscos


AS ENTREGAS E
RESULTADOS

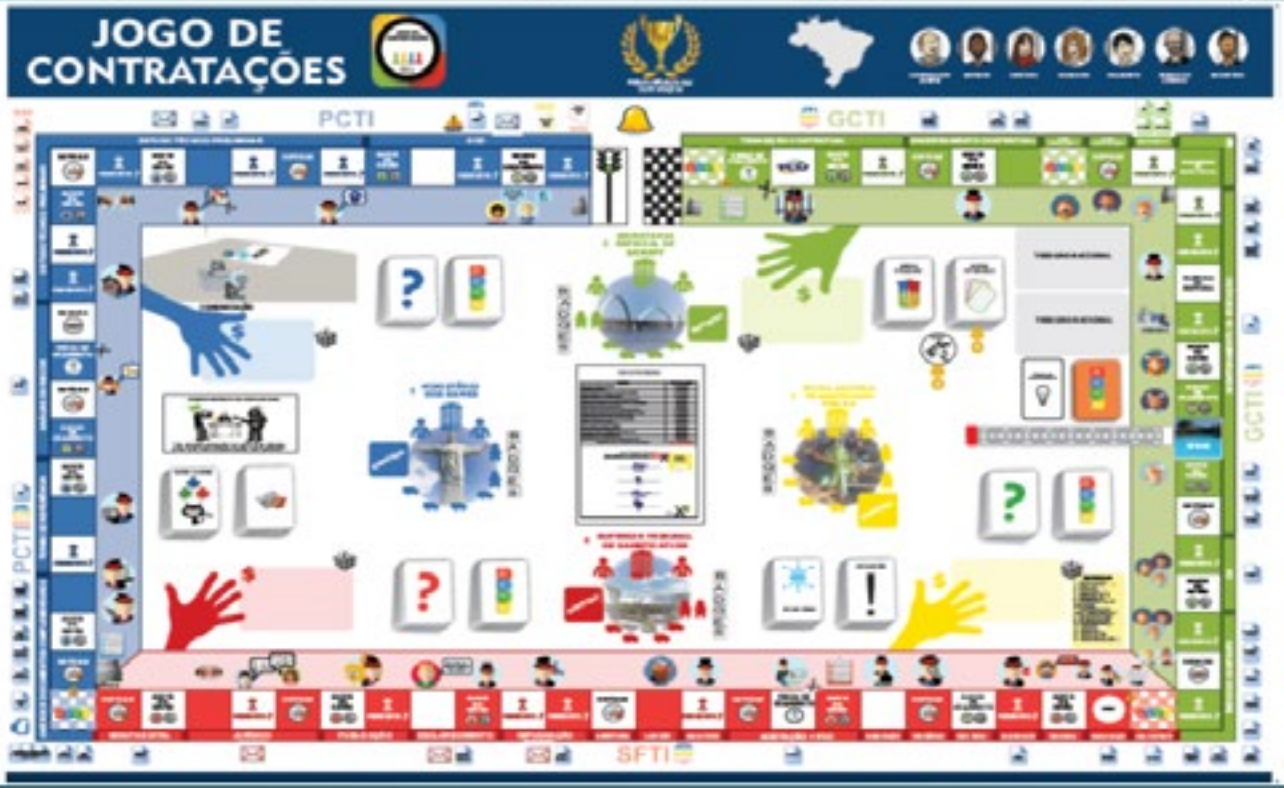
LIÇÕES APRENDIDAS

1. Liderança e feedbacks (SEG)
2. Comunicação (Clara, precisa e direta)
3. Confiança (isso é construído)
4. Revisão (double check)
5. Colaboração (com dedicação)
6. Hierarquia x estrutura projetizada (comparativo)
7. Silos não funcionam quando há muito trabalho
8. Identificação de riscos requer documentação
9. Análise dos riscos requer dedicação
10. Sem tempo para reorganizar o processo, a equipe se "canibaliza"

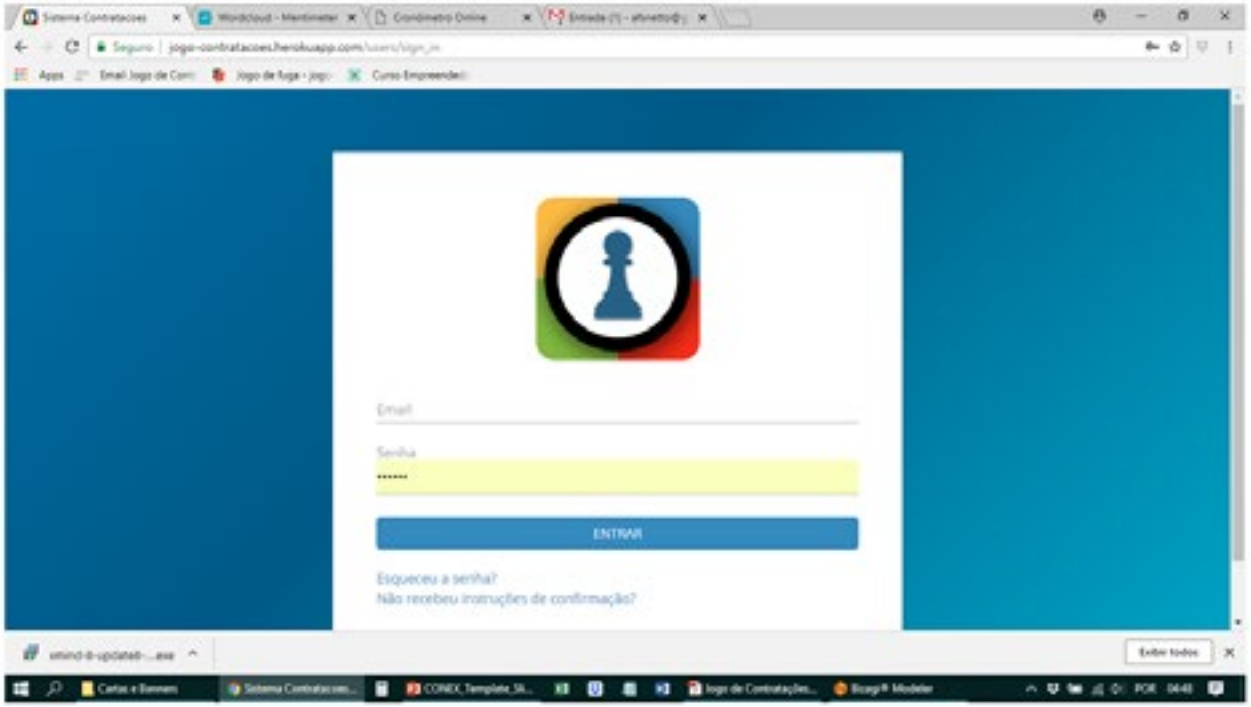
PRECISAMOS FALAR DE GESTÃO DE RISCOS

Lista de acidentes aéreos x lista de acidentes das contratações de TICs

JOGO DE CONTRATAÇÕES



SISTEMA JOGO DE CONTRATAÇÕES



ESTUDOS DE CASO

- Tamo Junto
- Métricas USI x UST
- Impressão de guerra
- Dispensa ou Inex da Infovia?
- Contando Bits
- TI Black List (barriga de aluguel)
- Fornecedor amigo do condomínio
- Micro o que?
- Compra sem licitação para atender a PR
- Atestado de incapacidade técnica
- Restos a pagar, mas pedindo orçamento
- *Comon Name*
- Gestão de Riscos? Ou de Crise?
- Decreto que te joga no preço mais caro.
- Jogo da Vergonha
- Baton na Cueca: Firewall
- Licenças na Nuvem, mesmo

CONCEPTU
CONSULTORES ASSOCIADOS

www.jogodecontratacoes.com.br

OBRIGADO!

contato@jogodecontratacoes.com.br
61 9 8423.3683

antonionetto

afsnetto

Material

Apresentação 6:

Implementando a Gestão de Riscos no Setor Público

RODRIGO FONTENELLE

Implementando a Gestão de Riscos no Setor Público

Rodrigo Fontenelle, CGAP, CRMA, CCSA

Por que estamos aqui hoje?

Estadão
7 h •

Bando tem setores jurídico, de transportes e de compliance, segundo MP; contribuição de 'associado' chega a R$ 950 mensais (via **Metrópole Estadão**) **#estadao**

BRASIL.ESTADAO.COM.BR
PCC vende 45 mil números de rifa e cobra mensalidade

631 79 comentários 158 compartilhamentos

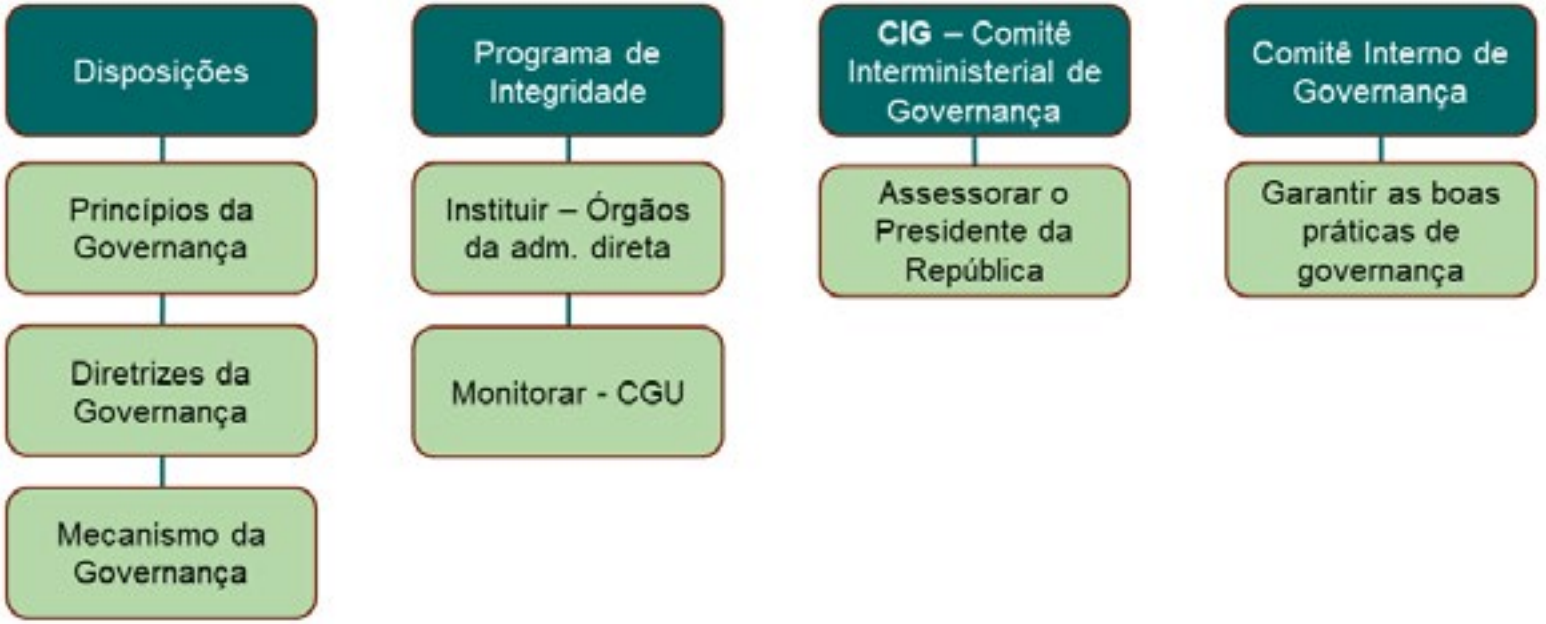
3

Decreto nº 9203, 22/11/2017

Política de Governança da Administração Pública

Decreto nº 9203, 22/11/2017

Ministério do **Planejamento**



Decreto nº 9203, 22/11/2017

Ministério do **Planejamento**

Sistema de Gestão de Riscos e Controles Internos

Art. 17. A **alta administração** das organizações da administração pública federal direta, autárquica e fundacional deverá **estabelecer, manter, monitorar e aprimorar sistema de gestão de riscos e controles internos** com vistas à identificação, à avaliação, ao tratamento, ao monitoramento e à análise crítica de riscos que possam impactar a implementação da estratégia e a consecução dos objetivos da organização no cumprimento da sua missão institucional, observados os seguintes princípios:

I - implementação e aplicação de forma sistemática, estruturada, oportuna e documentada, subordinada ao interesse público;

II - integração da gestão de riscos ao processo de planejamento estratégico e aos seus desdobramentos, às atividades, aos processos de trabalho e aos projetos em todos os níveis da organização, relevantes para a execução da estratégia e o alcance dos objetivos institucionais;

III - estabelecimento de controles internos proporcionais aos riscos, de maneira a considerar suas causas, fontes, consequências e impactos, observada a relação custo-benefício; e

IV - utilização dos resultados da gestão de riscos para apoio à melhoria contínua do desempenho e dos processos de gerenciamento de risco, controle e governança.

6

Conceitos

Esclarecendo...

Ministério do **Planejamento**

7

Gestão de Riscos

Ministério do **Planejamento**

Desafio no Brasil e no mundo

Quais os maiores desafios para sua empresa? (cf. Comitês de Auditoria) (global, até três opções; Brasil, múltiplas respostas permitidas)	**Global** (%)	**Brasil** (%)
Efetividade do processo de gerenciamento de riscos	**41 %**	**54 %**
Compliance legal/regulatório	**34 %**	**35 %**
Manter o ambiente de controle atuando por toda a organização	**28 %**	**43 %**
Gerenciamento dos riscos de segurança cibernética (*cyber security*)	**28 %**	**26 %**
Tone at the top e a cultura organizacional	**24 %**	**17 %**
Controles internos relacionados às demonstrações financeiras e demais relatórios financeiros	**22 %**	**33 %**
Assegurar a geração de valor pela Auditoria Interna	**21 %**	**20 %**
Pressões por resultados de curto prazo e alinhamento de das prioridades da companhia de longo prazo e de curto prazo	**19 %**	**22 %**
Risco de fraude	**13 %**	**15 %**
Implementação das novas normas de contabilidade (ex.: reconhecimento da receita, leasing, instrumentos financeiros)	**13 %**	**6 %**

Pesquisa mundial realizada junto a membros de Comitê de Auditoria, em 2017, pelo ACI Institute - KPMG

8

Gestão de Riscos

Ministério do **Planejamento**

Fatores-chave para o desenvolvimento

***Expectations of Risk Management Outpacing Capabilities*, KPMG, 2013 – estudo junto a + de mil empresas a nível internacional**

O que não é Gestão de Riscos

Ministério do **Planejamento**

10

Gestão de Riscos

Ministério do **Planejamento**

Percepção incorreta

Fonte: Miranda (2017)

11

Gestão de Riscos

Ministério do **Planejamento**

Percepção correta

Fonte: Miranda (2017)

Gestão de Riscos

Ministério do **Planejamento**

É necessário?

"Relatório do TCDF apontava necessidade de reparos em viaduto desde 2012"

Desabamento de viaduto no Eixo Sul – Brasília (DF)

"Outro fator que detectamos foi que não há um plano de alarme emergencial da empresa para a comunidade caso haja algum rompimento ou desastre".

Rompimento de barragem na região de Barcarena (PA)

13

Gestão de Riscos

Ministério do **Planejamento**

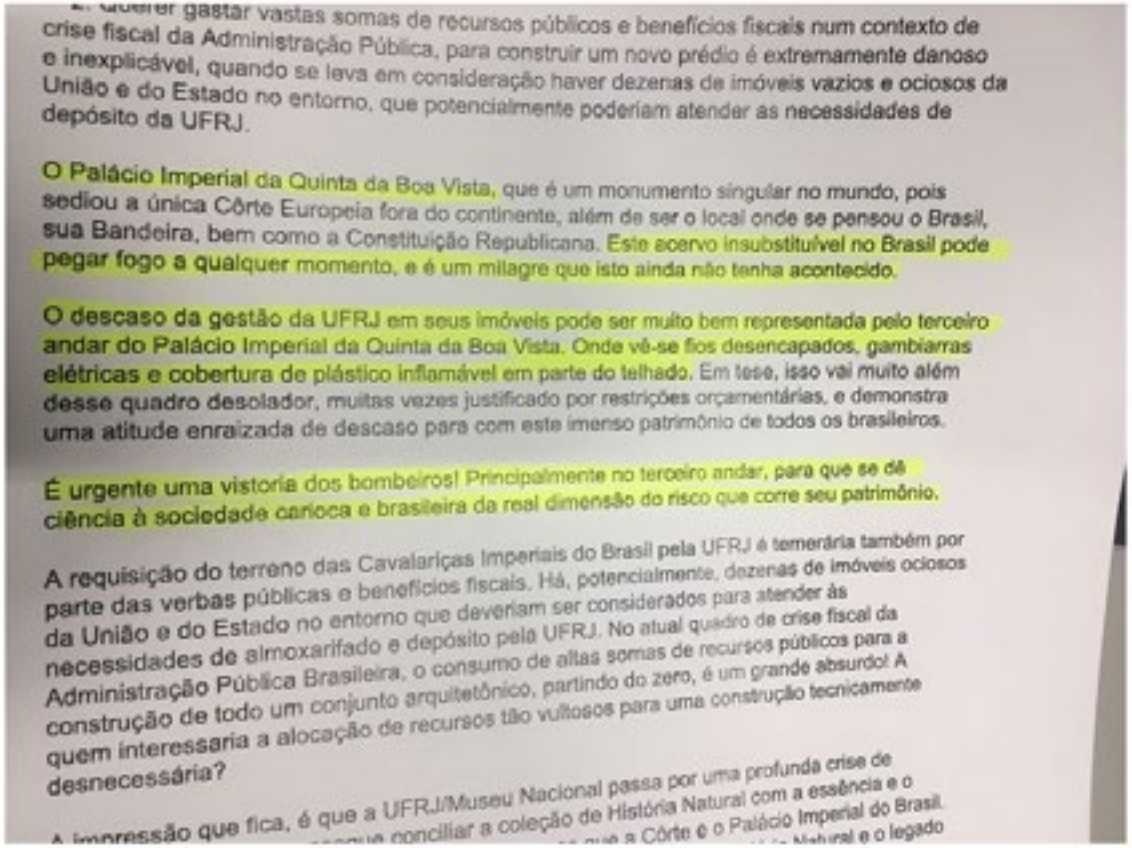
É necessário?

14

Gestão de Riscos

Ministério do **Planejamento**

É necessário?



...gastar vastas somas de recursos públicos e benefícios fiscais num contexto de crise fiscal da Administração Pública, para construir um novo prédio é extremamente danoso e inexplicável, quando se leva em consideração haver dezenas de imóveis vazios e ociosos da União e do Estado no entorno, que potencialmente poderiam atender às necessidades de depósito da UFRJ.

O Palácio Imperial da Quinta da Boa Vista, que é um monumento singular no mundo, pois sediou a única Côrte Européia fora do continente, além de ser o local onde se pensou o Brasil, sua Bandeira, bem como a Constituição Republicana. Este acervo insubstituível no Brasil pode pegar fogo a qualquer momento, e é um milagre que isto ainda não tenha acontecido.

O descaso da gestão da UFRJ em seus imóveis pode ser muito bem representada pelo terceiro andar do Palácio Imperial da Quinta da Boa Vista. Onde vê-se fios desencapados, gambiarras elétricas e cobertura de plástico inflamável em parte do telhado. Em tese, isso vai muito além desse quadro desolador, muitas vezes justificado por restrições orçamentárias, e demonstra uma atitude enraizada de descaso para com este imenso patrimônio de todos os brasileiros.

É urgente uma vistoria dos bombeiros! Principalmente no terceiro andar, para que se dê ciência à sociedade carioca e brasileira da real dimensão do risco que corre seu patrimônio.

A requisição do terreno das Cavalariças Imperiais do Brasil pela UFRJ é temerária também por parte das verbas públicas e benefícios fiscais. Há, potencialmente, dezenas de imóveis ociosos da União e do Estado no entorno que deveriam ser considerados para atender às necessidades de almoxarifado e depósito pela UFRJ. No atual quadro de crise fiscal da Administração Pública Brasileira, o consumo de altas somas de recursos públicos para a construção de todo um conjunto arquitetônico, partindo do zero, é um grande absurdo! A quem interessaria a alocação de recursos tão vultosos para uma construção tecnicamente desnecessária?

A impressão que fica, é que a UFRJ/Museu Nacional passa por uma profunda crise de ... conciliar a coleção de História Natural com a essência e o ... que a Côrte e o Palácio Imperial do Brasil ... Natural e o legado

15

CASE

MINISTÉRIO DO PLANEJAMENTO
GOVERNO FEDERAL

Histórico

Ministério do **Planejamento**

17

PGIRC/MP

Ministério do **Planejamento**

Instâncias de supervisão - Funções

Assessorar o Ministro na definição e implementação de diretrizes, políticas, normas e procedimentos para Gestão de Integridade, Riscos e Controles Internos da Gestão (Art. 11)

Estratégico

Comitê de Gestão Estratégica - CGE

Funções que aprovam, promovem e adotam as melhores práticas na gestão de riscos e controles internos

Tático

Subcomitê de Gestão de Integridade, Riscos e Controles - SIRC

Funções relacionadas a propor e promover as melhores práticas e avaliar a gestão de riscos e controles internos

Núcleo de Gestão de Integridade, Riscos e Controles Internos da Gestão - NIRC

Funções relacionadas a assessoramento ao ministro e demais áreas no ministérios quanto a gestão de riscos e controles

Operacional

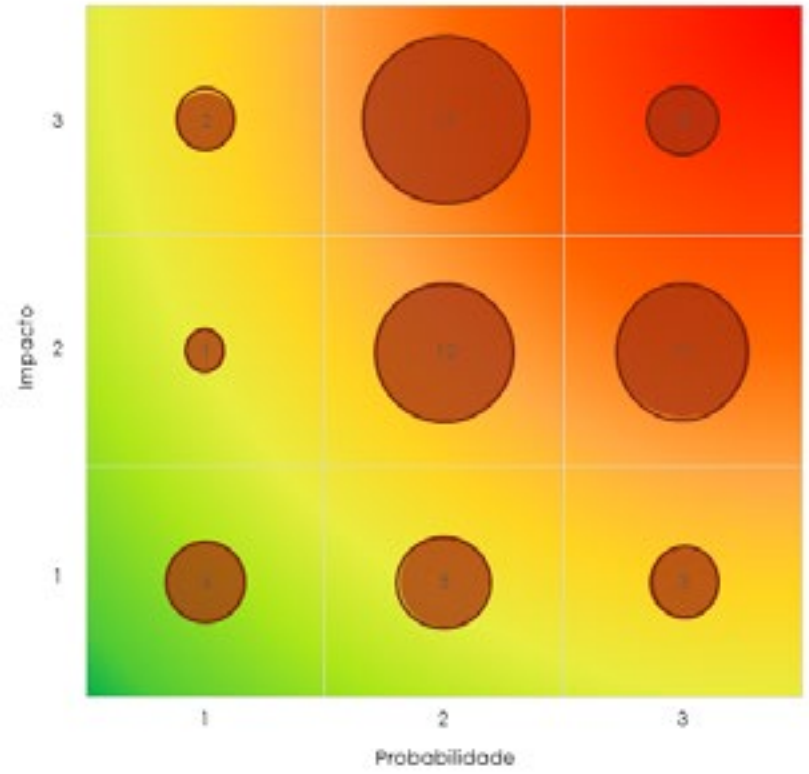
Unidade de Gestão de Integridade, Riscos e Controles Internos da Gestão - UIRC

Gestor

Funções que gerenciam e têm a propriedade sobre os riscos

18

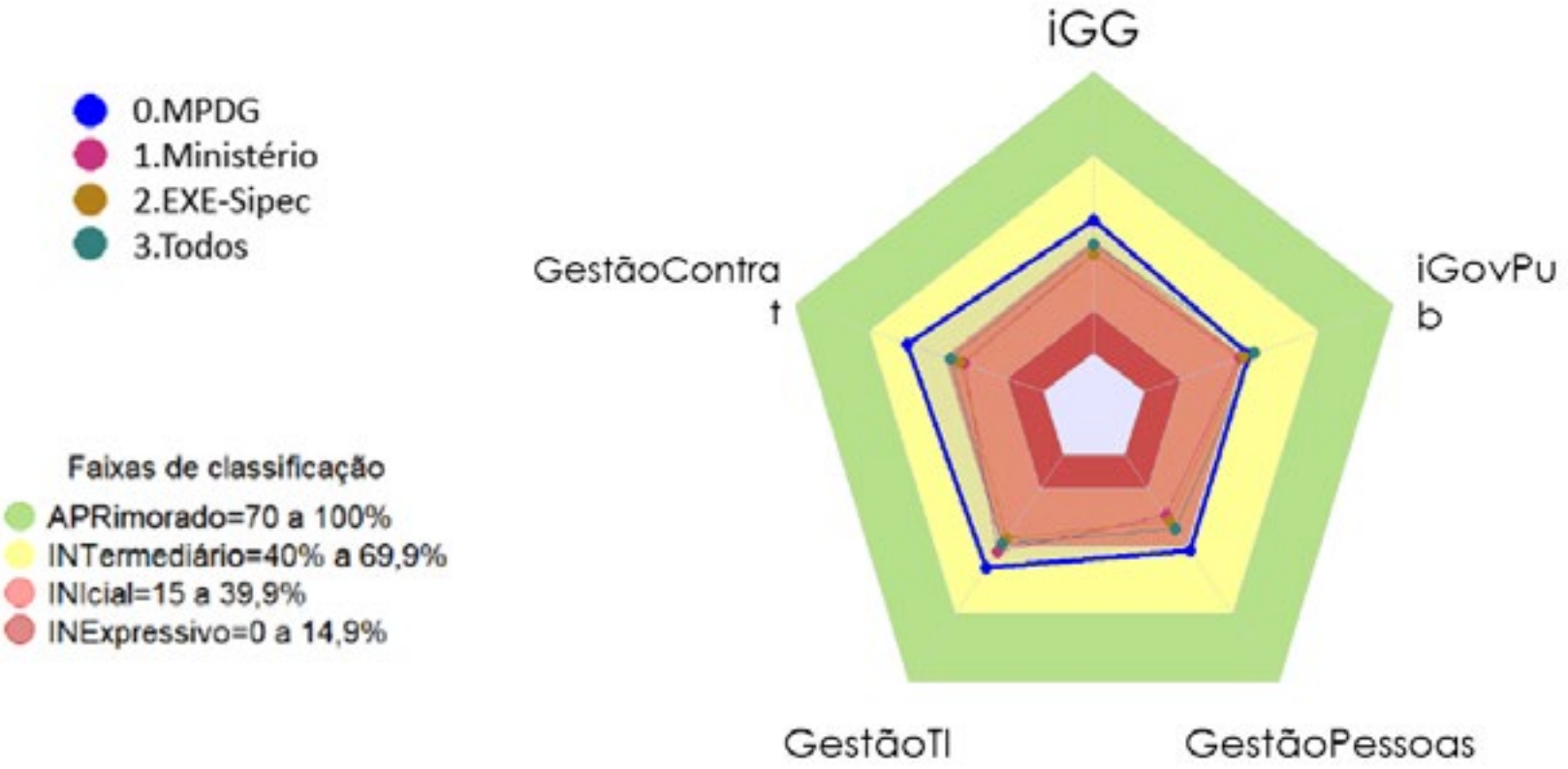
Mapa de Calor



Levantamento TCU - IGG - 2017

Ministério do **Planejamento**

Resultado MP



20

Atuação do MP – 2018

Ministério do **Planejamento**

Números

Atuação

- Palestras e eventos: 900* pessoas
- Cursos:
  - 08 horas – Agatha/MP: 85
  - 12 horas – outros órgãos: 240
  - 16 horas – outros órgãos: 113
  - 20 horas - ENAP: 60
- EAD:
  - 20 horas - Turma piloto: 6.649

Total: 8.047

* aproximadamente

21

Interação do MP

Ministério do **Planejamento**

Portal de Software de Público Brasileiro

https://www.softwarepublico.gov.br/social/agatha

Mais de 1000 downloads na primeira semana

Atuação do MP

Capacitação

Ministério do **Planejamento**

23

Interação do MP

Rede GIRC

Ministério do **Planejamento**

24

Atuação do MP

Ministério do **Planejamento**

Plano de Comunicação

Atuação do MP

Plano de Comunicação

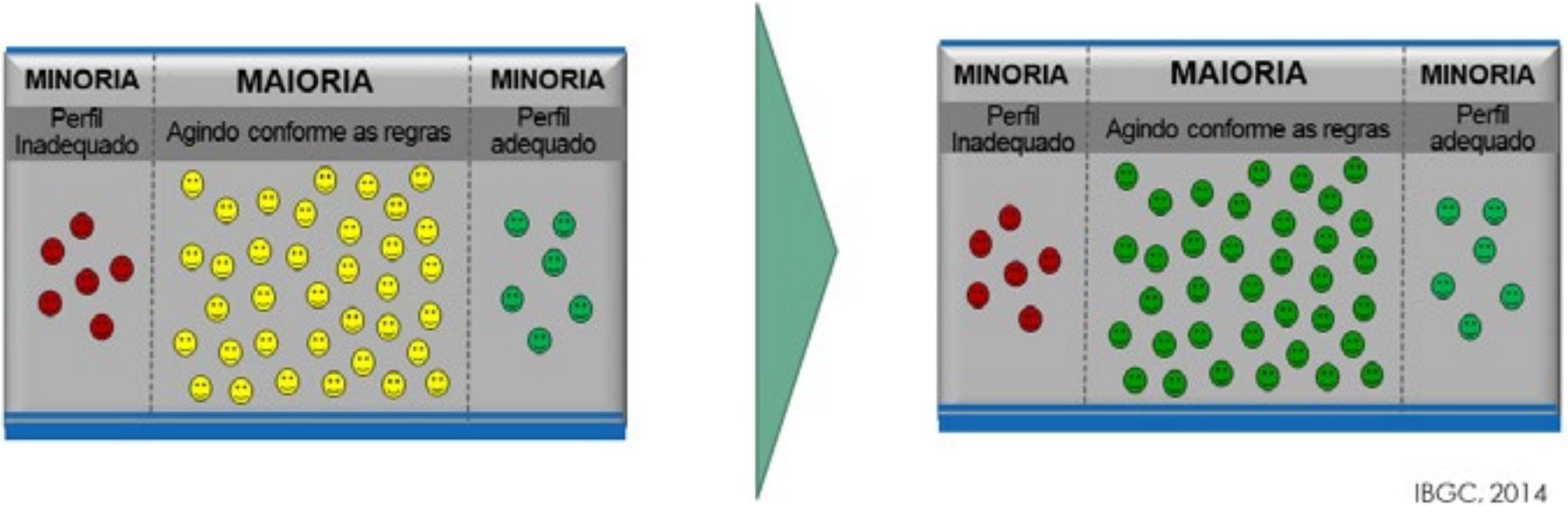
Ministério do **Planejamento**

ligado no controle

SÉRIE DE VÍDEOS


POR QUE TUDO ISSO?

Como o ambiente influencia na Conduta



IBGC, 2014

28

"Qualquer coisa que você faça será insignificante, mas é muito importante que você o faça." **Mahatma Gandhi**

OBRIGADO!

Rodrigo Fontenelle de Araújo Miranda, CGAP, CRMA, CCSA

Ministério do Planejamento, Desenvolvimento e Gestão – MPDG
Chefe da Assessoria Especial de Controle Interno
rodrigo.miranda@planejamento.gov.br
Fones: 2020.4020

29

Apresentação 7:

Governança nas compras públicas

Iniciativas do Ministério do Planejamento

VIRGÍNIA BRACARENSE LOPES


I Conferência Nacional: Governança, Riscos e Compliance
Governança nas compras públicas
Iniciativas do Ministério do Planejamento
Brasília, 05 de outubro de 2018

Governança é...

... como a sociedade, ou grupos dentro dela, se organizam para tomar decisões. Ao destrinchar essa simples afirmação, três grandes questões afloram:

- *Quem tem voz na tomada de decisões?*
- *Como as decisões são tomadas?*
- *Quem responde pelas decisões?*

Institute on Governance, Canadá

https://iog.ca

Governança no setor público...

... todos os conceitos pressupõem ***definições claras*** *de responsabilidade, grande importância dada às boas relações entre as* ***partes interessadas****, à* ***administração dos recursos*** *e à* ***entrega de resultados****.*

MIRANDA, Rodrigo Fontenelle

Transparência

Informações devem ser completas, precisas e claras

Integridade

Honestidade, objetividade, decência e probidade. Reflete na tomada de decisão e na qualidade dos resultados

Accountability

Obrigação de responder por uma responsabilidade conferida

Governança das aquisições...

*...compreende essencialmente o conjunto de mecanismos de **liderança, estratégia e controle** postos em prática para **avaliar, direcionar e monitorar** a atuação da **gestão das aquisições**, com objetivo de que as aquisições agreguem valor ao negócio da organização, com riscos aceitáveis.*

Relatório – Acórdão 2.622/15 – TCU-Plenário

Acórdão 2.622/15 – TCU-Plenário

01 Modelo de competências

02 Escolha das lideranças

03 Capacitação

04 Comitê de aquisições

05 Plano anual de aquisições

Acórdão 2.622/15 – TCU-Plenário

06 Gestão de riscos nas aquisições

07 Processo de contratação

08 Atuação da auditoria interna

09 Alocação de recursos com base em riscos

Iniciativas do MP

01 Consultas públicas
Normativos, processos, critérios

02 Padronizações
Processos, normativos, ferramentas

03 Planejamento de compras
Normativo (IN 01/2018), sistema

04 Capacitações
Normativos, sistemas, processos

05 Gestão de riscos
Normativo, processos

Iniciativas do MP

06 Ferramentas
Paineis, planilhas, checklist

07 Digitalização
PEN, SICAF

08 Rede Nacional de Compras
Boas práticas, integração, capacitação

09 Critérios
Gratificações, verificações, formação de preços

E na CENTRAL?

01 Estrutura de governança
Fluxo decisório

02 Modelagem de processos
Fluxos de trabalho e artefatos

03 Gerenciamento de riscos
Identificação e rotina de monitoramento

04 Planejamento de compras
Diretrizes e portfólio

E na CENTRAL?

05 Monitoramento e avaliação
Indicadores e paineis

06 Gestão de competências
Matriz elaborada em conjunto

07 Capacitação
Baseada em competências

08 Integridade, transparência e accountability
Publicização e acesso

Obrigada

Virgínia Bracarense Lopes
central.compras@planejamento.gov.br
(61) 2020-8667

Apresentação 8:

Programas de Compliance

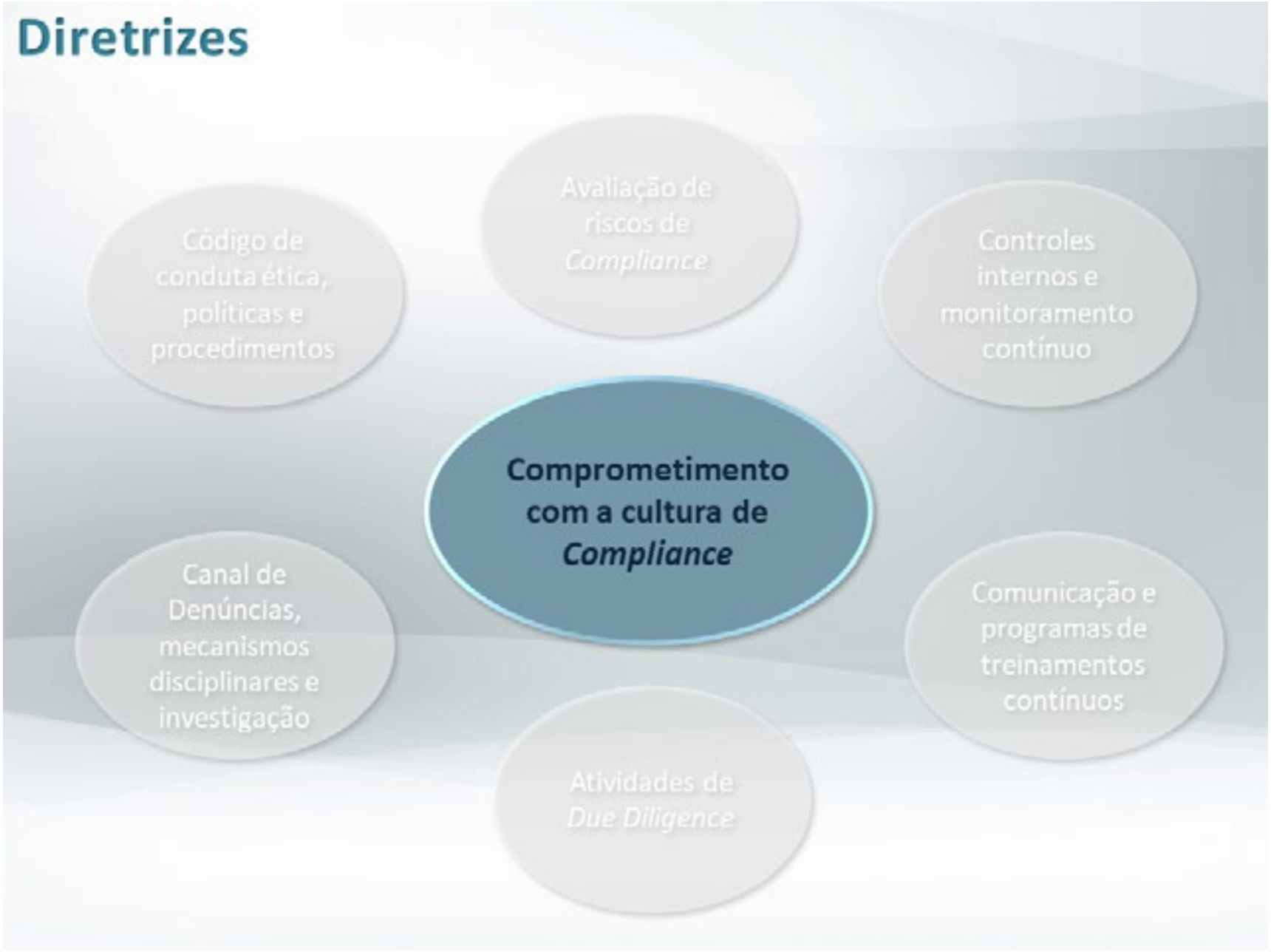
Por onde começar?

MARIÂNGELA MATTIA


Programas de Compliance
Por onde Começar?
Mariângela Mattia


Compliance
?


Diretrizes
Código de conduta, políticas e procedimentos
Avaliação de riscos
Controles internos e monitoramento contínuo
Comprometimento com a cultura de *Compliance*
Canal de Denúncias, investigação e gestão das consequências
Comunicação e treinamentos contínuos
Atividades de *Due Diligence*


Diretrizes
Código de conduta ética, políticas e procedimentos
Avaliação de riscos de *Compliance*
Controles internos e monitoramento contínuo
Comprometimento com a cultura de *Compliance*
Canal de Denúncias, mecanismos disciplinares e investigação
Comunicação e programas de treinamentos contínuos
Atividades de *Due Diligence*

Comprometimento com a Cultura de Compliance

- Liderança e o compromisso da alta gestão
- Nomeação de um profissional de compliance
- Adequação às normas deve ser *top-down*
- Compliance na cultura da empresa e na gestão das organizações

Dicas

Declarações escritas para os funcionários	Interação constante com os colaboradores	Exemplos de cumprimentos de regras

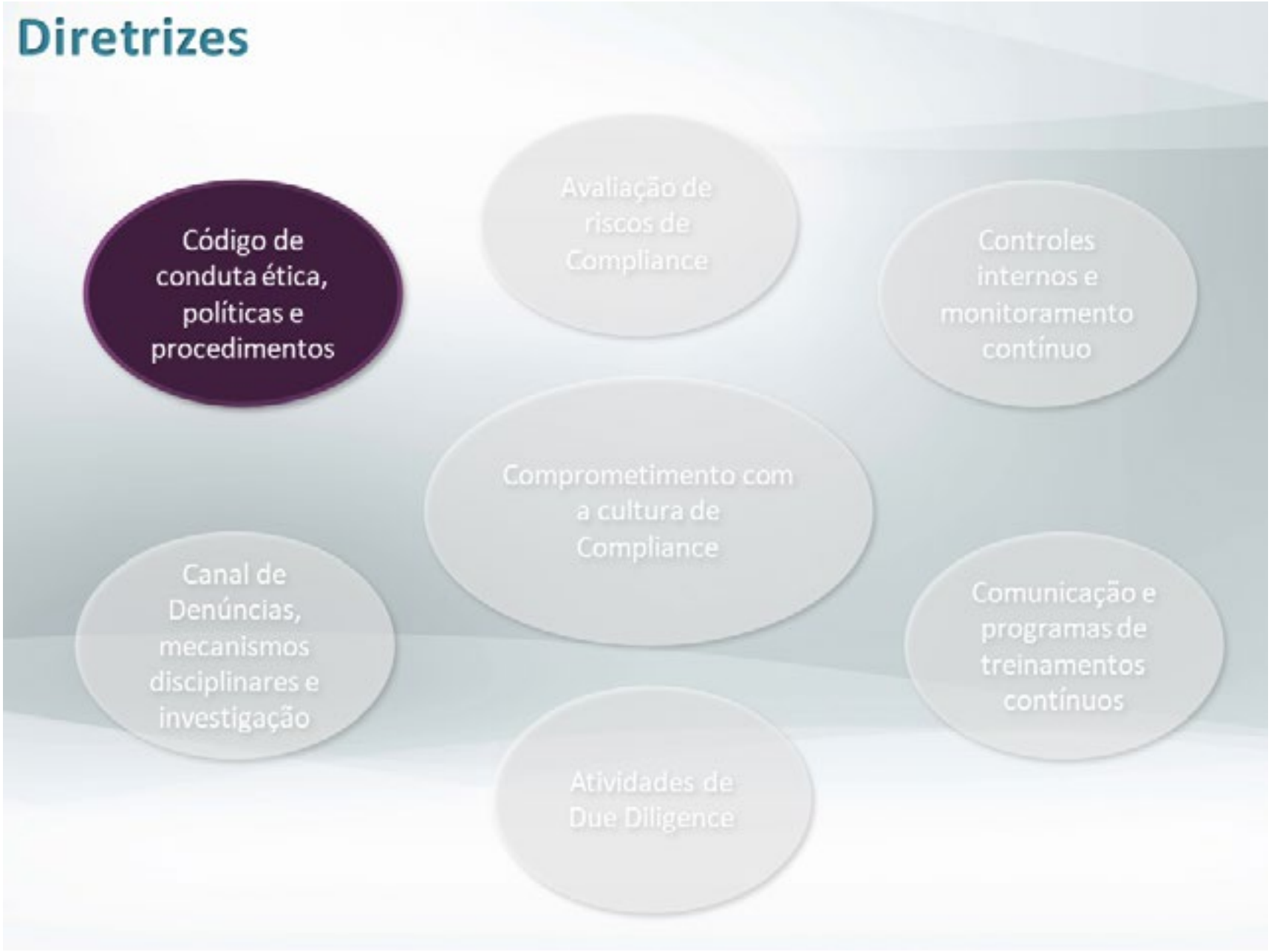

Diretrizes
Avaliação de riscos de Compliance
Código de conduta ética, políticas e procedimentos
Controles internos e monitoramento contínuo
Comprometimento com a cultura de Compliance
Canal de Denúncias, mecanismos disciplinares e investigação
Comunicação e programas de treinamentos contínuos
Atividades de Due Diligence

Avaliação de Riscos

- Conhecer a empresa é o ponto de partida
- Avaliar os riscos
- Monitorar e gerenciar os riscos identificados

Dicas

Identificar as leis e regulamentações	Diagnósticos de riscos	Matriz de riscos	Soluções para mitigação de riscos


Diretrizes
Código de conduta ética, políticas e procedimentos
Avaliação de riscos de Compliance
Controles internos e monitoramento contínuo
Comprometimento com a cultura de Compliance
Canal de Denúncias, mecanismos disciplinares e investigação
Comunicação e programas de treinamentos contínuos
Atividades de Due Diligence

Código de Conduta, Políticas e Procedimentos

- Criação de políticas e procedimentos
- Código de Conduta devem ter regras claras
- Meios para esclarecimentos de dúvidas

Dicas

Elaboração e revisão de códigos de conduta

Elaboração de Políticas

Ouvidoria Interna


Diretrizes
Código de conduta ética, políticas e procedimentos
Avaliação de riscos de Compliance
Controles internos e monitoramento contínuo
Comprometimento com a cultura de Compliance
Canal de Denúncias, mecanismos disciplinares e investigação
Comunicação e programas de treinamentos contínuos
Atividades de Due Diligence

Controles Internos e Monitoramento Contínuo

- Minimizar os riscos dos negócios
- Controles dinâmicos e adaptados à natureza do negócio
- Ferramentas para gestão e controle de *Compliance*

Dicas

Indicadores de riscos	Auditorias Internas	Avaliação do controle de ambientes internos	Análise de relatórios, reclamações de clientes


Diretrizes
Código de conduta ética, políticas e procedimentos
Avaliação de riscos de Compliance
Controles internos e monitoramento contínuo
Comprometimento com a cultura de Compliance
Canal de Denúncias, mecanismos disciplinares e investigação
Comunicação e programas de treinamentos contínuos
Atividades de Due Diligence

Comunicação e Programas de Treinamento Contínuos

- Comunicar o programa
- Treinamentos Periódicos
- Conscientizar aos prestadores de serviços, consultores e parceiros

Dicas

Campanhas de lançamento, plano anual de comunicação	Disseminação da cultura por meio de treinamentos, cursos, palestras	Ouvidoria Interna


Diretrizes
Código de conduta ética, políticas e procedimentos
Avaliação de riscos de Compliance
Controles internos e monitoramento contínuo
Comprometimento com a cultura de Compliance
Canal de Denúncias, mecanismos disciplinares e investigação
Comunicação e programas de treinamentos contínuos
Atividades de Due Diligence

Atividades de *Due Diligence*

- Avaliar riscos de terceiros
- Conhecer o perfil ético do profissional em contato direto com fornecedores

Dicas

Estruturação do processo de *Due Diligence*	Supervisionar contratos de terceirizados	Monitorar profissional que mantém contato direto com fornecedores


Diretrizes
Código de conduta ética, políticas e procedimentos
Avaliação de riscos de Compliance
Controles internos e monitoramento contínuo
Comprometimento com a cultura de Compliance
Canal de Denúncias, mecanismos disciplinares e investigação
Comunicação e programas de treinamentos contínuos
Atividades de Due Diligence

Canal de denúncias, mecanismos disciplinares e de investigação

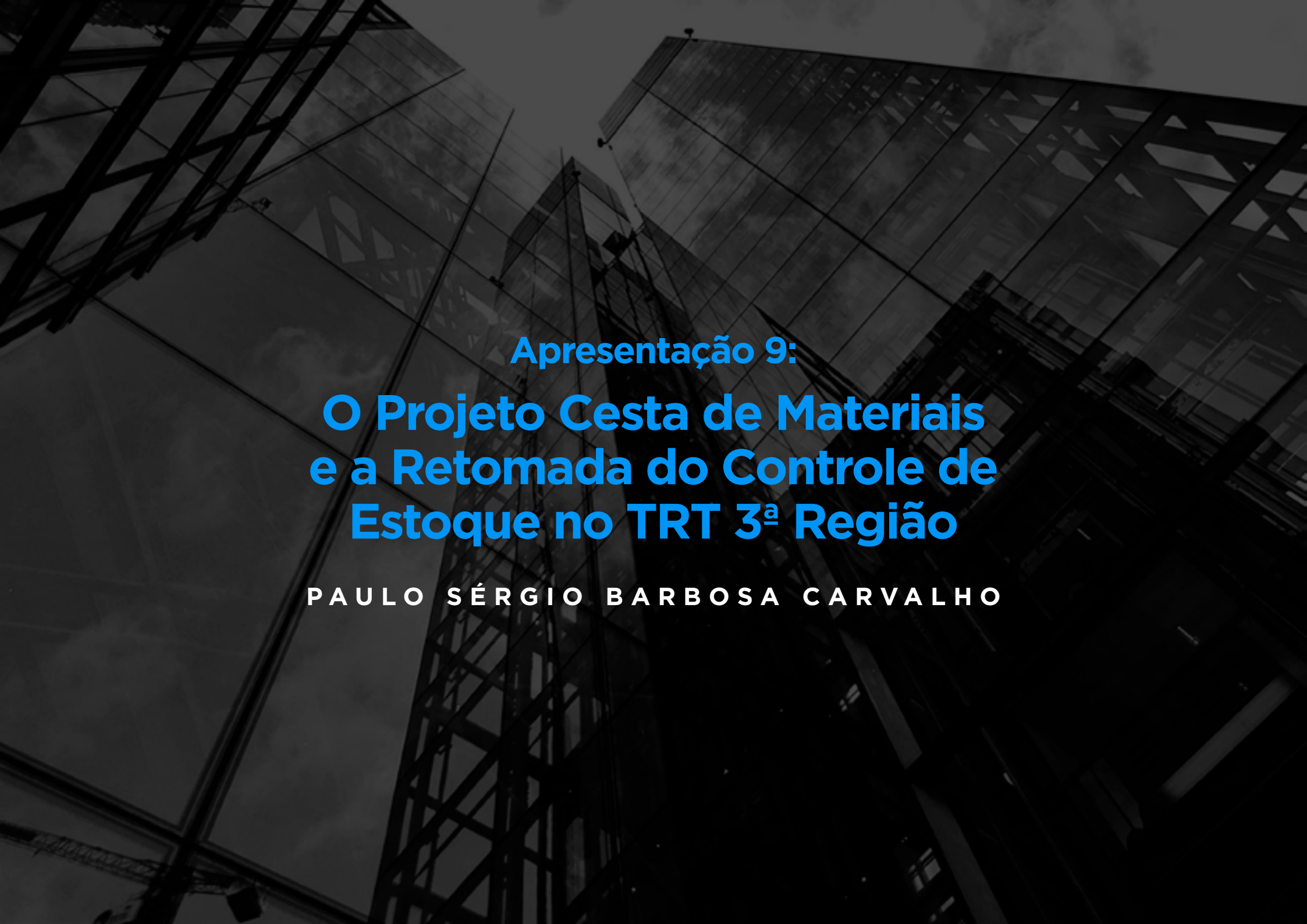
- Canal de Denúncias anônimo
- Política de proteção ao Denunciante
- Tratamento da denúncia
- Gestão das consequências

Dicas

Urna, telefone, internet	Definir processo de apuração de denúncias.	Incentivar o uso do canal de denúncias.


O que se espera do Programa...
Prevenir
Detectar
Corrigir
Políticas e procedimentos claros
Testes e canal de denúncia
Investigação e Gestão da Consequência


Como você faz para que seu filho leia livros?
Mariângela Mattia
msmattia@yahoo.com
@sercompliance



Apresentação 9:

O Projeto Cesta de Materiais e a Retomada do Controle de Estoque no TRT 3ª Região

PAULO SÉRGIO BARBOSA CARVALHO

O PROJETO CESTA DE MATERIAIS E A RETOMADA DO CONTROLE DE ESTOQUE NO TRT 3ª REGIÃO

Paulo Sérgio Barbosa Carvalho

TRTMG
TRIBUNAL REGIONAL DO TRABALHO DA 3ª REGIÃO

Apresentação do palestrante

Paulo Sérgio Barbosa Carvalho

Mestre em Administração (FACE-FUMEC/MG)

Especialista Adm.Comércio Exterior (FCG-UNA-CEPEDERH/MG);

Especialista em Direito de Empresa (PUC/MG);

Especialista em Direito de Empresa (UGF/RJ – CAD/MG);

Especialista em Direito da Economia e da Empresa (FGV/MG);

Especialista em Licitações e Contr. Administrativos (UNA/MG);

Especialista em Admin. Pública - Gestão Pública (FJP/MG);

Bacharel em Direito (FMC/MG);

Analista Judiciário do TRT da 3ª Região;

Assistente de Desembargador – dez./06-ago/12;

Assessor Jurídico de Licitações e Contratos – set./12-mar./15;

Assessor de Desembargador – abr./15-dez./15;

Assessor da Secretaria de Material e Logística – 2016-2017;

Diretor-Geral do TRT da 3ª Região (2018-atual);

Professor de pós-graduação do Centro de Estudos em Direito e Negócios (FA/MG).

COMPETÊNCIA REGULAMENTAR - SML

A Secretaria de Material e Logística é responsável por gerir e executar ações referentes a:

- aquisição,
- guarda,
- registro,
- distribuição,
- restauração,
- movimentação e desfazimento de materiais de consumo, materiais e bens permanentes;
- emissão e postagem de correspondências ;
- serviços gráficos no TRT-3ª ;

CESTA DE MATERIAIS - *Precedentes*

1- No TRT-3ª a questão do suprimento de materiais historicamente foi tratada como algo de menor importância

2- Entendia-se, à época, que, desde que não faltassem os materiais necessários, os meios desprendidos para tanto não eram importantes

3- Havia bastante disponibilidade orçamentária e pouca preocupação com a eficiência do setor

4- O modelo adotado - a criação de estoques locais, cada unidade possuía uma reserva de materiais que era gerida com total independência em relação ao setor de materiais do TRT3

5- À Secretaria competia, apenas, repassar os materiais solicitados por cada unidade sem qualquer tipo de intervenção (qualidade, finalidade e quantidade)

CESTA DE MATERIAIS - *Precedentes*

6- Paralelamente a isso, incidia também sobre o setor de materiais a incumbência de realizar aquisições com as sobras orçamentárias do Tribunal

7- Essa metodologia causava um grave impacto no sistema de armazenamento, pois com o passar do tempo gerou o pagamento de taxas extras contratuais, o que onerava os recursos do TRT3.

CESTA DE MATERIAIS

Constatada a DISCREPÂNCIA NO CONSUMO DE MATERIAIS entre unidades que possuem:

1- idêntica movimentação processual;
2- idêntico sistema informatizado (limitador de procedimentos);
3- encontram-se numa mesma jurisdição;
4- possuem o mesmo público alvo;
5- julgam o mesmo tipo de causas trabalhistas;

CESTA DE MATERIAIS

CRITÉRIOS OBJETIVOS DE DEFINIÇÃO DAS CESTAS DE MATERIAIS:

- ✓ apurou-se a média de consumo de materiais de cada unidade nos últimos 24 meses;
- ✓ agruparam-se as unidades conforme a movimentação processual igual ou aproximada;
- ✓ apurou-se a média de consumo destes grupos de Varas;

CESTA DE MATERIAIS

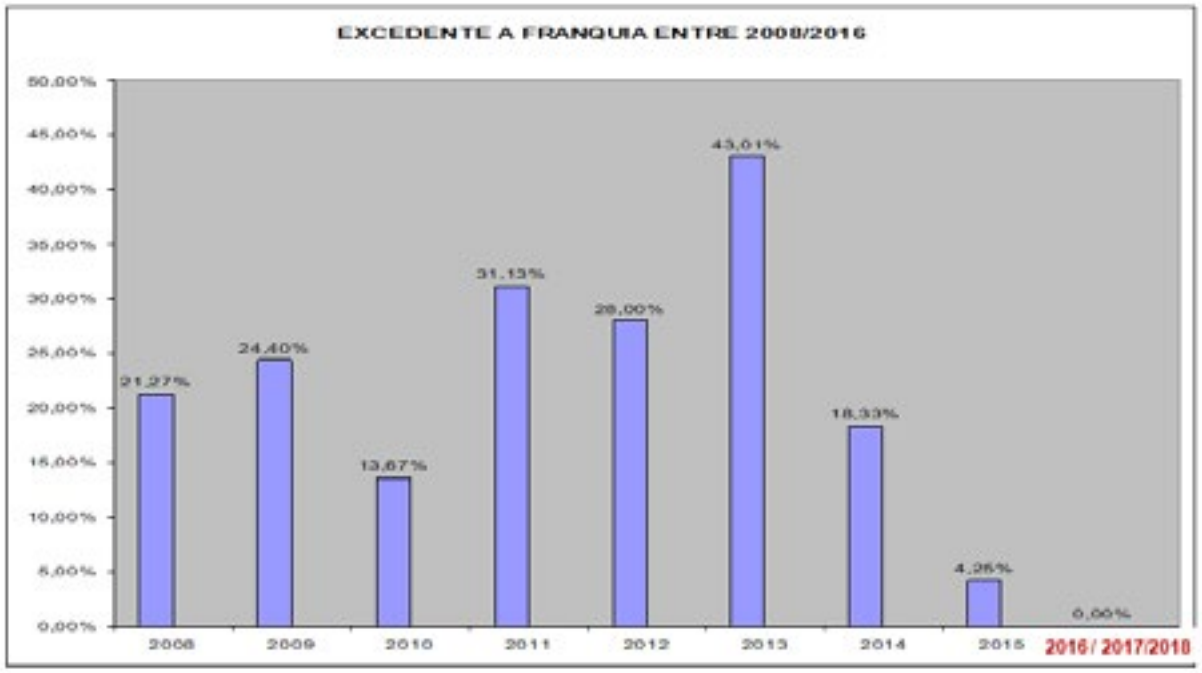
COMPOSIÇÃO DAS CESTAS DE MATERIAIS

CONSIDERA A MÉDIA DO GRUPO OU O MENOR GASTO DA UNIDADE

Forma de envio: mensal (Varas) ou trimestral (Gabinetes, Apoio Jud., Apoio Adm.)

CESTA DE MATERIAIS - *Resultados*

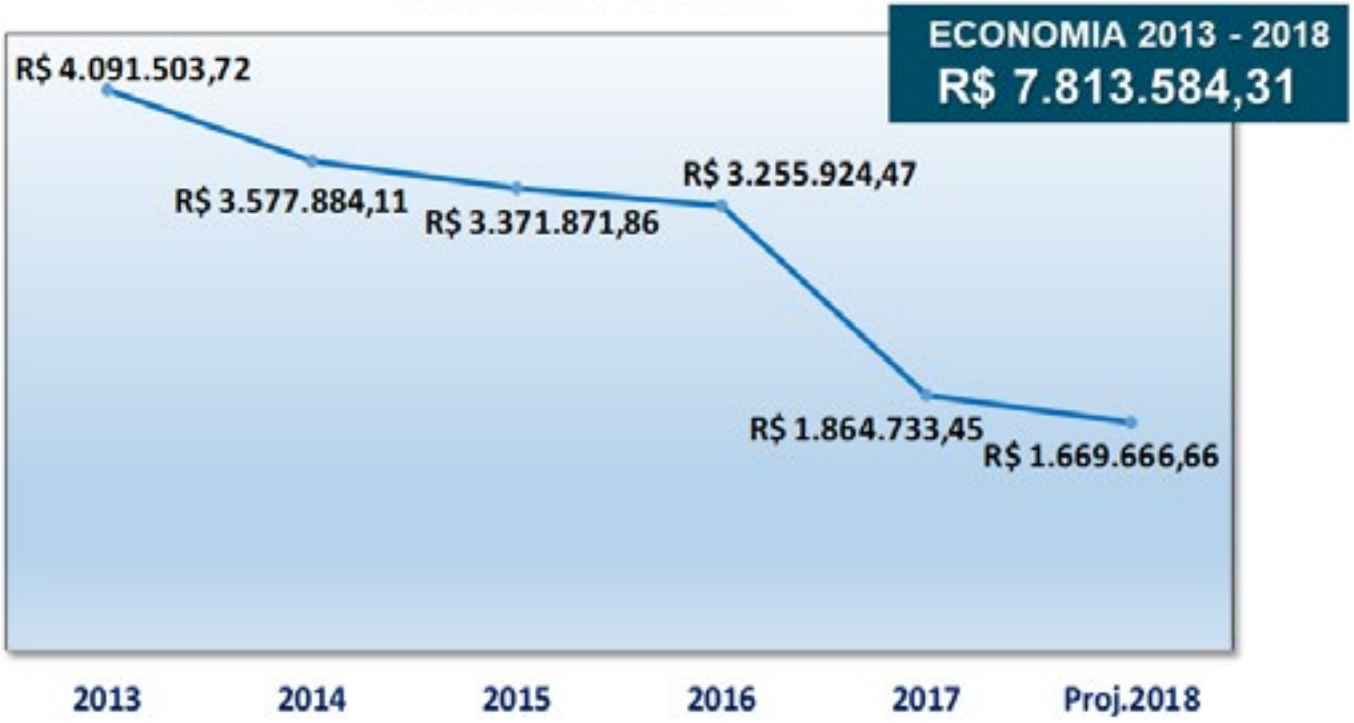
Redução do espaço de armazenagem no CLI



CESTA DE MATERIAIS - *Resultados*

Redução de custos de armazenagem e de distribuição

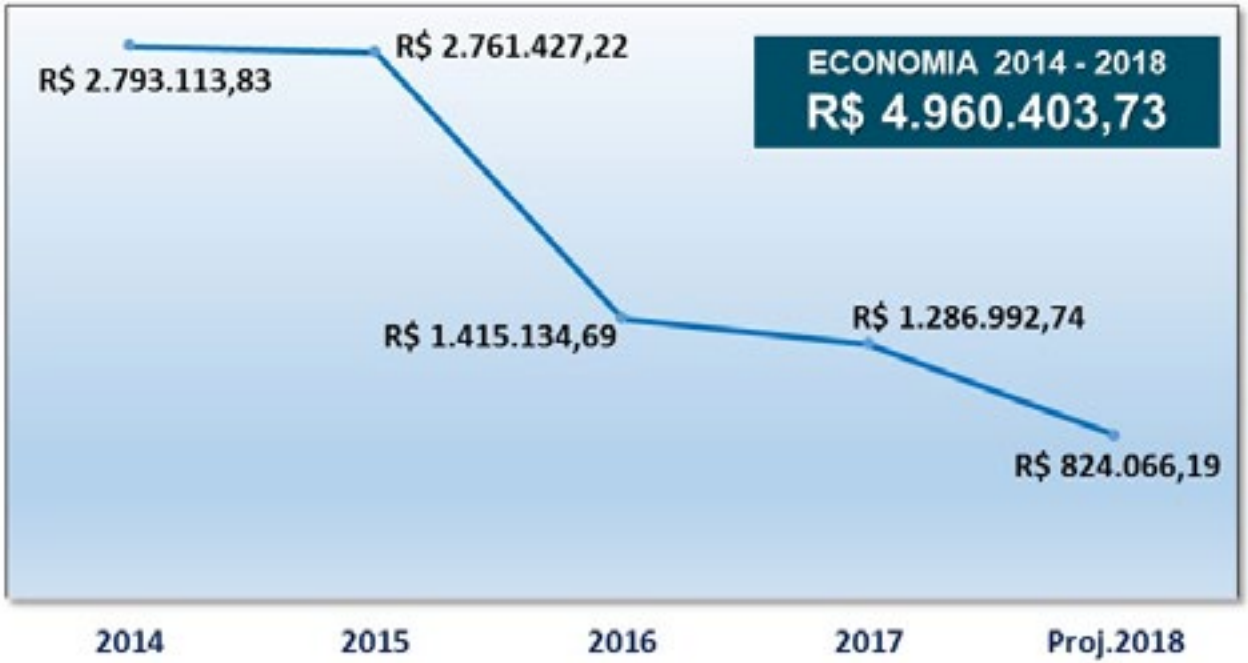
GASTOS COM LOGÍSTICA



CESTA DE MATERIAIS - *Resultados*

Redução do consumo de materiais

GASTO TOTAL COM MATERIAL DE CONSUMO



CESTA DE MATERIAIS *Continuação do Projeto*

Implementação da Cesta de Tonner (A4 x Toner)

	2013	2014	2015	2016	2017	PROJEÇÃO 2018
TOTAL DE RESMAS (A4)	44.804	51.168	55.444	39.197	29.299	23.036
TOTAL DE CARTUCHOS	4.303	2.997	2.855	1.217	1.261	1.084

Papel A4: consumo em 2018 será 49% menor do que em 2013

Cartucho: consumo em 2018 será 75% menor do que em 2013

(1)2013: Criação de 23 Varas e 19 Gabinetes de Desembargador

(2) 2014: Aumento do papel devido a implantação do Pje – impressão de todos os arquivos

(3) 2014: Redução do cartucho devido ao não atendimento de pedidos exorbitantes – limitação de qtdes

(4) 2015: Aumento do papel devido a erro no início da implantação da cesta de materiais, que passou a entregar para algumas unidades um quantitativo maior do que recebido anteriormente

(5) 2016: Redução devido ao controle temporal do envio de cartuchos e cesta de materiais

CESTA DE MATERIAIS *Continuação do Projeto*

- Análise crítica entre a qtde de papel fornecido *versus* capacidade de impressão (cópias potenciais) dos cartuchos

Cartuchos fornecidos em 2017 — 1.261 — *Equivale a* → **26.827.000** cópias potenciais *(capacidade/tinta do cartucho)*

X

Papel A4 (resmas) fornecido em 2017 — 29.299 — *Equivale a* → **21.974.250** páginas impressas possíveis *(metade em frente e verso)*

CÓPIAS POTENCIAIS EXCEDENTES EM RELAÇÃO AO TOTAL DE FOLHAS DE PAPEL CONSUMIDAS → **4.852.750**

CESTA DE MATERIAIS

Continuação do Projeto

PADRONIZAÇÃO DAS AQUISIÇÕES:

Redução da variedade dos materiais disponíveis, otimizando as aquisições

Como era	Como ficou
Caneta azul, vermelha e preta	Caneta azul e vermelha
Caneta hidrográfica, pincel atômico ponta grossa	Pincel atômico ponta média
Cola branca 90g e cola em bastão	Cola branca 90g
Colchetes nº 7, 11 e 14	Colchete nº 11
Envelope memorandum, circulação interna e de processo	Envelope circulação interna e de processo
Materiais gráficos	Tipo de papel, Espiral etc

TRTMG

CESTA DE MATERIAIS

Continuação do Projeto

Pesquisa de Satisfação de Materiais

Realizada trimestralmente com todos as unidades, de modo a obter informações sobre os produtos fornecidos na cesta de materiais, visando melhorar a qualidade desses.

Melhoria na execução dos contratos pela fiscalização dos usuários

TRIBUNAL REGIONAL DO TRABALHO DA 3ª REGIÃO
Secretaria de Material e Logística

PESQUISA DE AVALIAÇÃO DE PRODUTO PÓS-CONTRATAÇÃO

A Secretaria de Material e Logística (SML), unidade gestora e fiscalizadora das aquisições de materiais de expediente deste Tribunal, elaborou esta "Pesquisa de Avaliação de Produto Pós-Contratação" a ser preenchida pelas Unidades, de modo a obter informações sobre os produtos, visando melhorar a qualidade desses.

Ressalta que a partir do resultado obtido das avaliações dos produtos por V. Sa., a marca que não for satisfatória aos interesses deste Regional será substituída por outra, às expensas do fornecedor, pena das sanções cabíveis, bem assim poderá ser desqualificada em futuro procedimento licitatório, daí a importância do preenchimento e envio da Pesquisa a essa SML.

Assim, roga a V. Sa. se digne preencher os dados solicitados, de acordo com as orientações abaixo:

1) Informe a Unidade:

Nome da Unidade:	1a. VT de Ituiutaba

2) Marque com um "X" a resposta referente a cada produto (item), conforme a opção desejada.

2.1) Se todos os produtos atendem satisfatoriamente, marcar com um "X" somente a opção abaixo:

( ) Todos os produtos (itens) da cesta de materiais atendem satisfatoriamente.

2.2) Caso a opção para determinado produto seja "Atende" e outro seja "Não Atende" satisfatoriamente, assinalar cada opção com um "X". Favor JUSTIFICAR e informar a MARCA do produto que não atende satisfatoriamente.

Item	Produto	Atende	Não Atende	Marca	Justificativa
01	Apontador de lápis	x			
02	Almofada p/ carimbo	x			
03	Borracha branca	x			
04	Elástico	x			
05	Caneta esferográfica		x	Compactor Economic	Muitas não escrevem
06	Caneta hidrográfica				
07	Caneta para CD/DVD				
08	Caixa arquivo morto polionda				
09	Caixa arquivo morto papelão	x			

TRTMG

CESTA DE MATERIAIS

Continuação do Projeto

Pesquisa de Satisfação de Materiais

- Negociação com os fornecedores a troca de materiais em desconformidade com os padrões contratados e aquelas marcas apontadas nas pesquisas que não atendem as necessidades dos usuários.
  Ex: Troca do estoque da marca de colas e canetas consideradas insatisfatórias

- Criação de banco de dados das marcas de materiais adquiridos, classificando conforme a manifestação das unidades na pesquisa

CONTATOS

Tribunal Regional do Trabalho 3ª Região

Diretoria-Geral

dg@trt3.jus.br

paulobc@trt3.jus.br

(31) 3228-7011 / 3228-7002

Apresentação 10:

Gestão de Riscos Corporativos

WILDENILDO OLIVEIRA DOS SANTOS

FABIANO FERREIRA DE ARAÚJO

MARY ANNE FONTENELE MARTINS

PATRÍCIA FERNANDA TOLEDO BARBOSA


Gestão de Riscos
Corporativos
Aplicando a Metodologia Anvisa
Canvas Ágil de Riscos
ANVISA
Agência Nacional de Vigilância Sanitária


AGENDA
Alinhamento conceitual
O processo de GRC – metodologia Anvisa
Aplicação do método
Contexto do risco
Oficina
Considerações finais
ANVISA
Agência Nacional de Vigilância Sanitária

Alinhamento Conceitual

ANVISA
Agência Nacional de Vigilância Sanitária


Alinhamento
Risco é...
O efeito da incerteza sobre os objetivos.
(ISO 31000:2009)
Quando um objetivo é definido ...
devemos estar preparados para isso.
ANVISA
Agência Nacional de Vigilância Sanitária

Alinhamento

Por que gerir riscos?

ANVISA
Agência Nacional de Vigilância Sanitária

Alinhamento

Portaria nº 854, de 30 de maio de 2017

GRC: Processo contínuo, que consiste no desenvolvimento de um conjunto de ações destinadas a identificar, analisar, avaliar, priorizar, tratar e monitorar riscos corporativos positivos ou negativos capazes de afetar os objetivos, programas, projetos ou processos de trabalho da Anvisa nos níveis estratégico, tático e operacional.

ANVISA
Agência Nacional de Vigilância Sanitária

Alinhamento

Onde Aplicar

Gestão de riscos na Anvisa

MAPA ESTRATÉGICO

METAS ESTRATÉGICAS

PROJETOS ESTRATÉGICOS

CADEIA DE VALOR

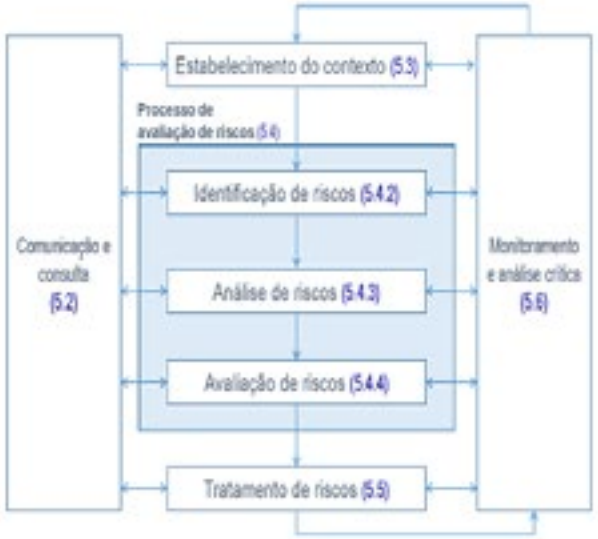
ANVISA
Agência Nacional de Vigilância Sanitária

Metodologia

Metodologia

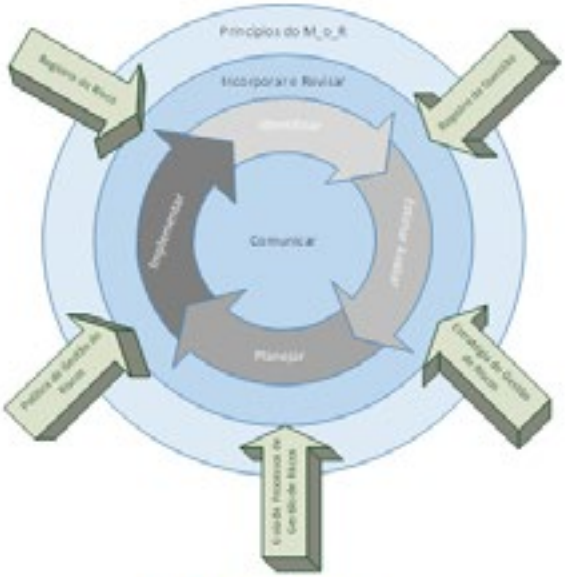
Fontes de inspiração

ISO 31000



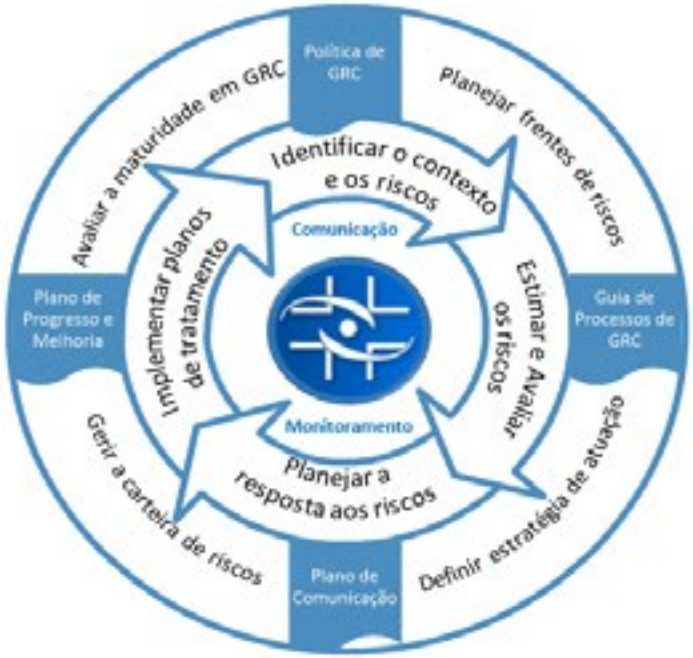
COSO ERM

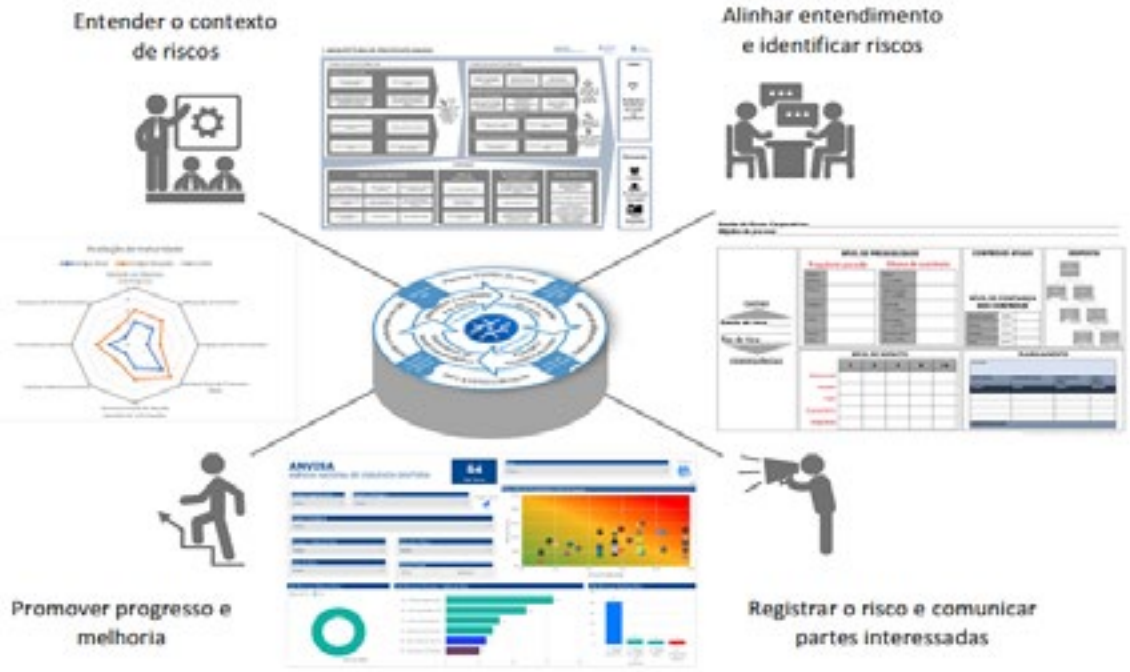
M_o_R

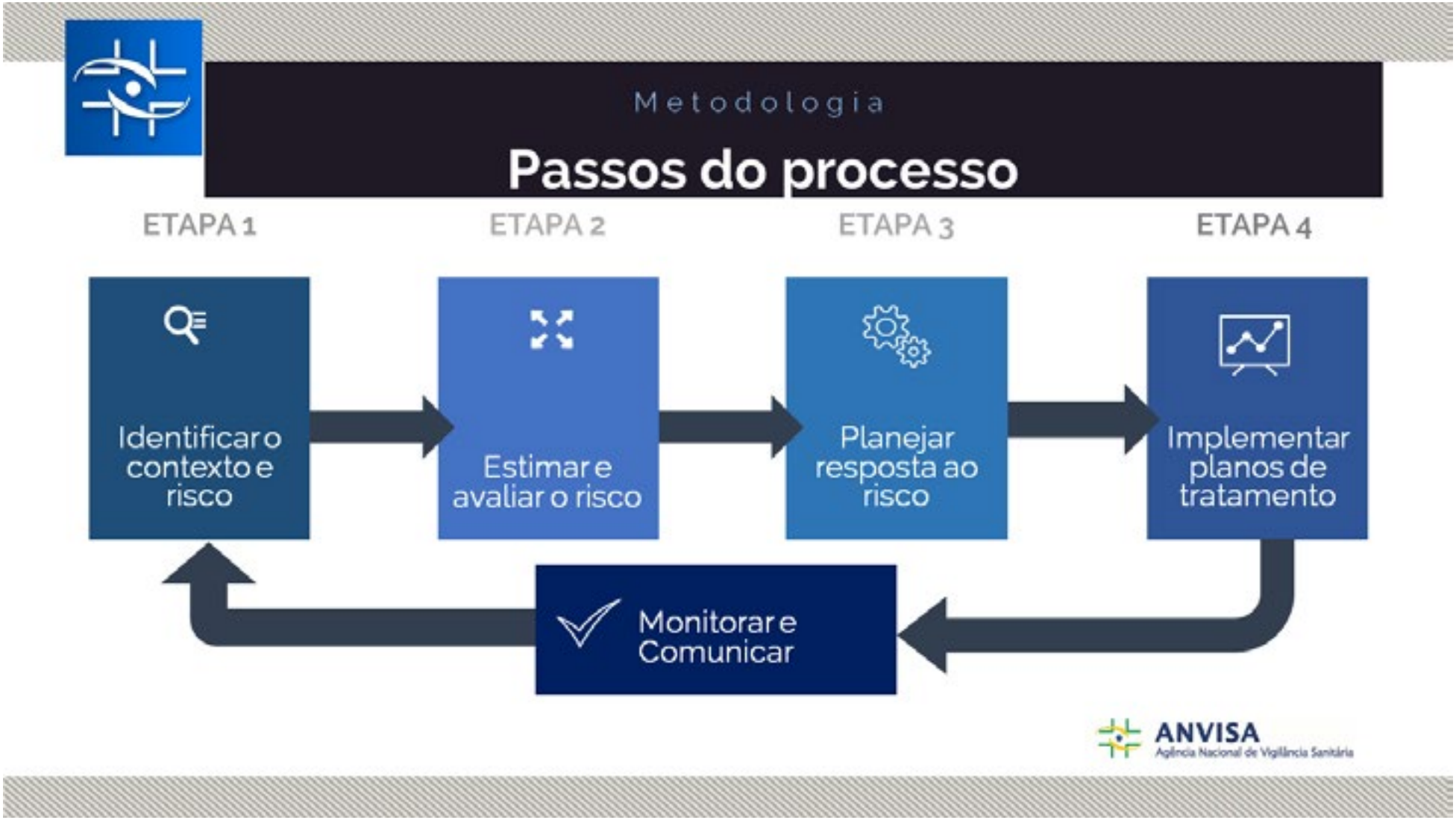


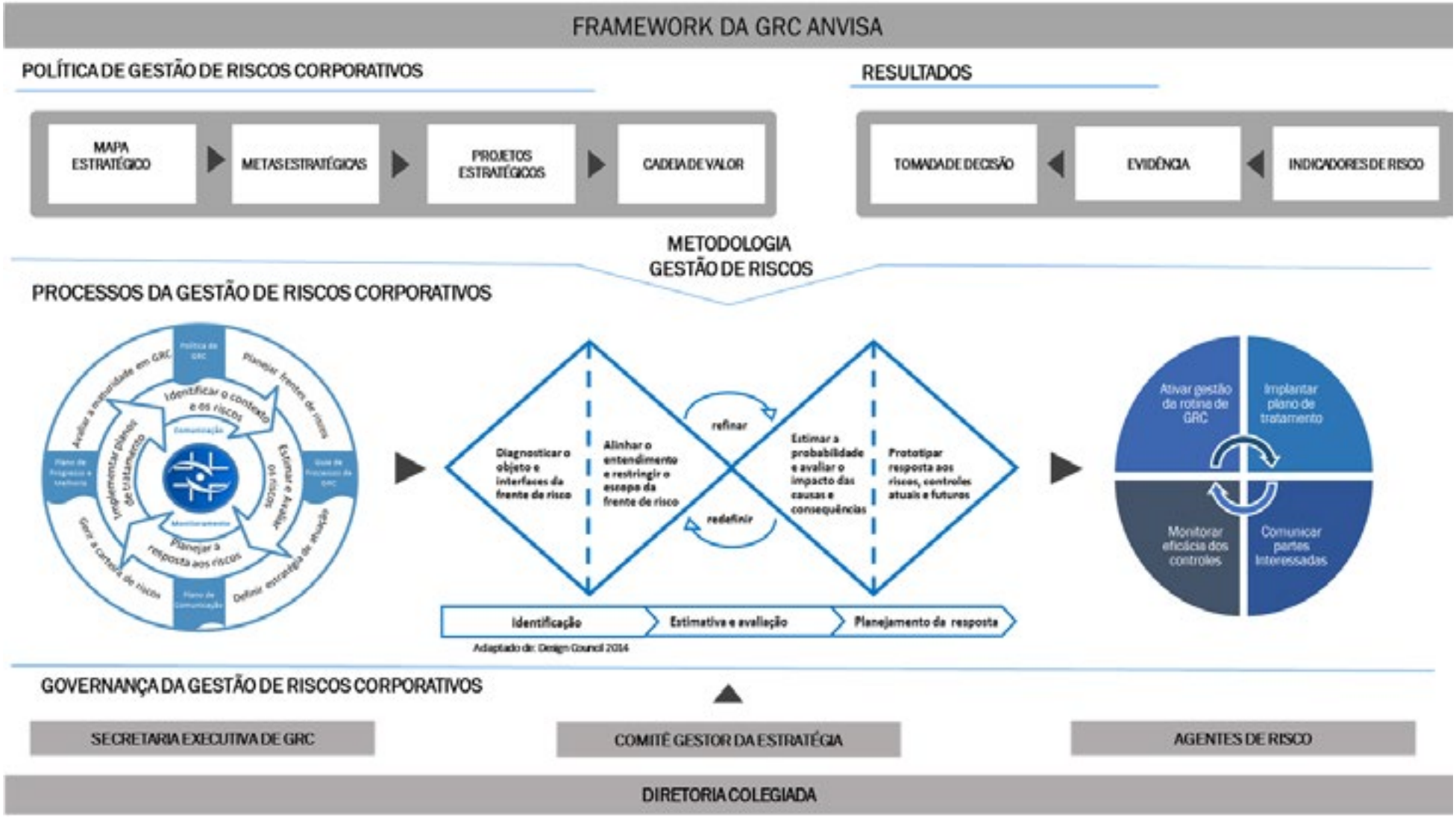
ANVISA
Agência Nacional de Vigilância Sanitária

Metodologia

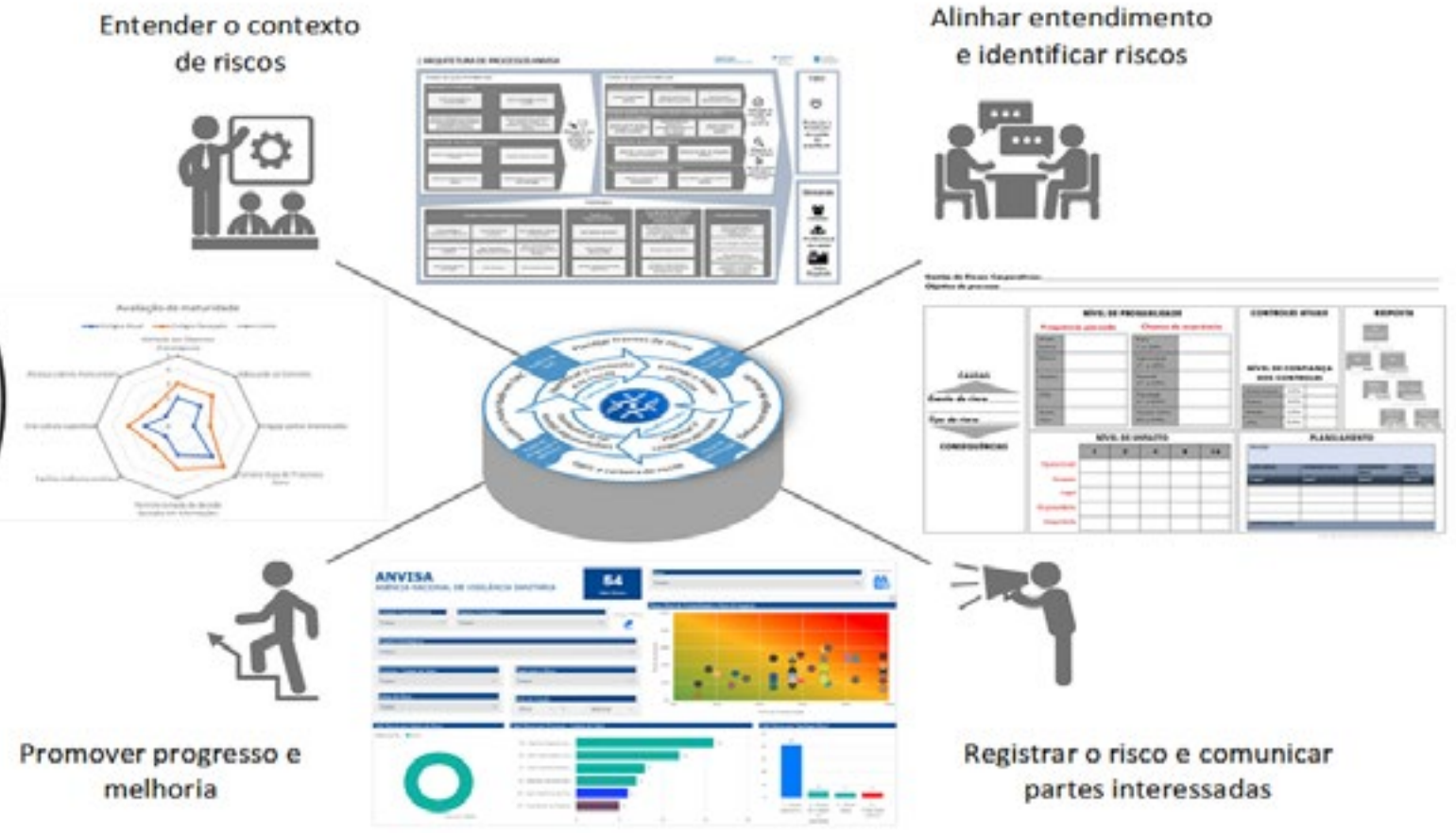





Metodologia
Passos do processo
ETAPA 1
ETAPA 2
ETAPA 3
ETAPA 4
Identificar o contexto e risco
Estimar e avaliar o risco
Planejar resposta ao risco
Implementar planos de tratamento
Monitorar e Comunicar
ANVISA
Agência Nacional de Vigilância Sanitária


FRAMEWORK DA GRC ANVISA
POLÍTICA DE GESTÃO DE RISCOS CORPORATIVOS
MAPA ESTRATÉGICO
METAS ESTRATÉGICAS
PROJETOS ESTRATÉGICOS
CADEIA DE VALOR
RESULTADOS
TOMADA DE DECISÃO
EVIDÊNCIA
INDICADORES DE RISCO
METODOLOGIA GESTÃO DE RISCOS
PROCESSOS DA GESTÃO DE RISCOS CORPORATIVOS
Política de GRC
Identificar o contexto e os riscos
Estimar e Avaliar os riscos
Definir estratégia de atuação
Planejar a resposta aos riscos
Gerir a carteira de riscos
Plano de comunicação
Implementar planos de tratamento
Avaliar a maturidade em GRC
Plano de Progresso e melhoria
Guia de Processos de GRC
Planejar frentes de riscos
Comunicação
Monitoramento
Diagnosticar o objeto e interfaces da frente de risco
Alinhar o entendimento e restringir o escopo da frente de risco
refinar
redefinir
Estimar a probabilidade e avaliar o impacto das causas e consequências
Prototipar resposta aos riscos, controles atuais e futuros
Identificação
Estimativa e avaliação
Planejamento da resposta
Adaptado de: Design Council 2014
Ativar gestão da rotina de GRC
Implantar plano de tratamento
Monitorar eficácia dos controles
Comunicar partes interessadas
GOVERNANÇA DA GESTÃO DE RISCOS CORPORATIVOS
SECRETARIA EXECUTIVA DE GRC
COMITÊ GESTOR DA ESTRATÉGIA
AGENTES DE RISCO
DIRETORIA COLEGIADA

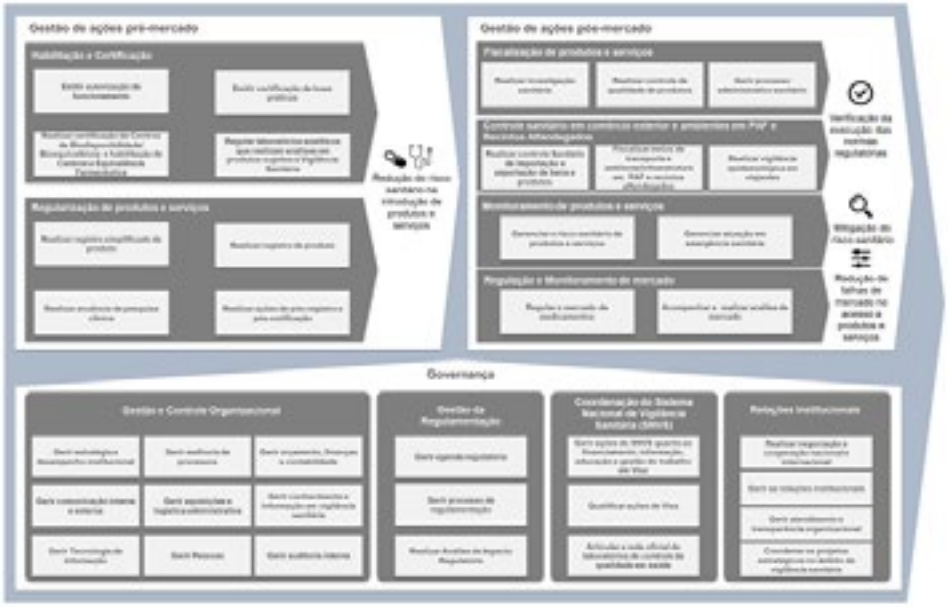
Ciclo de GRC


Entender o contexto de riscos
Alinhar entendimento e identificar riscos
Promover progresso e melhoria
Registrar o risco e comunicar partes interessadas
ANVISA

Metodologia

Contexto de risco

CADEIA DE VALOR



MAPA ESTRATÉGICO 2016-2019

Missão: "Proteger e promover a saúde da população, mediante a intervenção nos riscos decorrentes da produção e do uso de produtos e serviços sujeitos à vigilância sanitária, em ação coordenada e integrada no âmbito do Sistema Único de Saúde"

Visão: "Ser uma instituição promotora de saúde, cidadania e desenvolvimento, que atua de forma ágil, eficiente e transparente, consolidando-se como protagonista no campo da regulação e do controle sanitário, nacional e internacionalmente"

OBJETIVOS DE RESULTADO

1. Ampliar o acesso seguro da população a produtos e serviços sujeitos à vigilância sanitária
2. Aprimorar o marco regulatório em vigilância sanitária

OBJETIVOS HABILITADORES

3. Otimizar as ações de pré-mercado com base na avaliação do risco sanitário
4. Aprimorar as ações de vigilância em pós-uso, com foco no controle e monitoramento
5. Fortalecer as ações de coordenação do Sistema Nacional de Vigilância Sanitária
6. Elevar a eficiência das operações em portos, aeroportos e fronteiras
7. Aprimorar as ações de cooperação e convergência regulatória no âmbito internacional
8. Implantar modelo de governança que favoreça a integração, a inovação e o desenvolvimento institucional*
9. Fortalecer as ações de educação e comunicação em vigilância sanitária e o modelo de relacionamento institucional**

ANVISA
Agência Nacional de Vigilância Sanitária

Gestão de Riscos Corporativos - Anvisa

Participantes:_____ **Processo:**_____

Objetivo do processo: _____ **Vínculo com a Estratégia:**_____

IDENTIFICAÇÃO

CAUSAS

Evento de risco:_____

Tipo de risco:_____

CONSEQUÊNCIAS

ESTIMATIVA E AVALIAÇÃO

NÍVEL DE PROBABILIDADE

Frequência passada		Chance de ocorrência	
Muito baixa		Raro 1 a 20%	
Baixa		Improvável 21 a 40%	
Média		Possível 41 a 60%	
Alta		Provável 61 a 80%	
Muito Alta		Quase Certo 80 a 99%	

NÍVEL DE IMPACTO

	1	2	4	8	16
Operacional					
Imagem					
Legal					
Orçamentário					
Integridade					

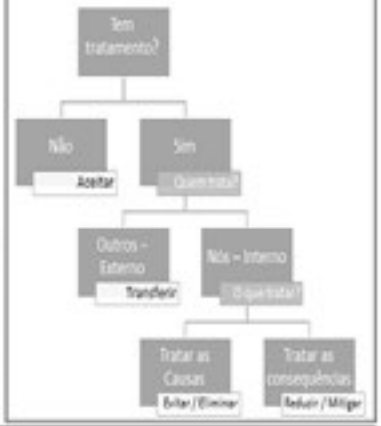
PLANEJAMENTO DA RESPOSTA

CONTROLES ATUAIS

NÍVEL DE CONFIANÇA DOS CONTROLES

Muito baixo	20%	
Baixo	40%	
Médio	60%	
Alto	80%	

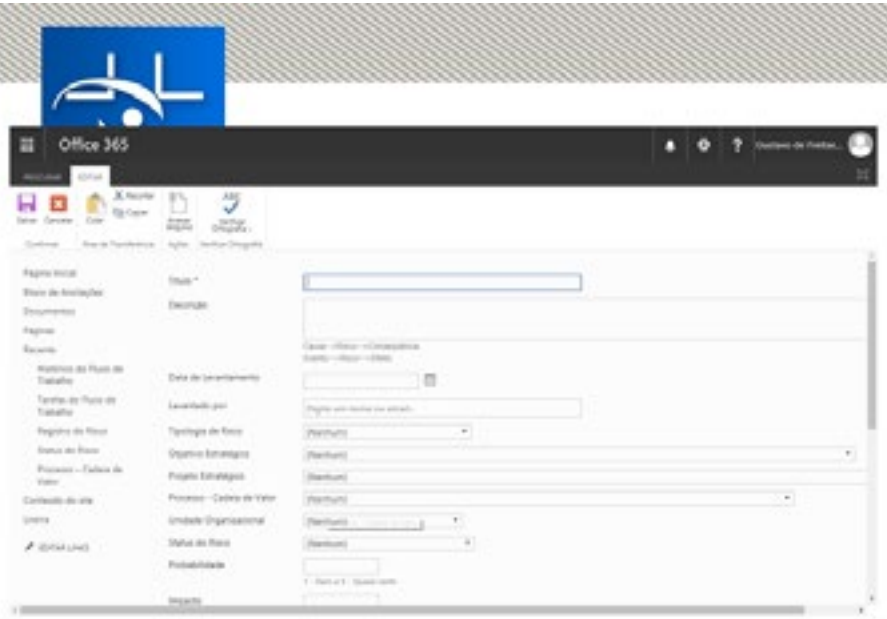
RESPOSTA



PLANEJAMENTO

Descrição			
AÇÃO (What)	ATIVIDADES (How)	RESPONSÁVEIS (Who)	PRAZO (When)
O que?	*Como?*	*Quem?*	*Quando?*
QUANTO (How much)?			

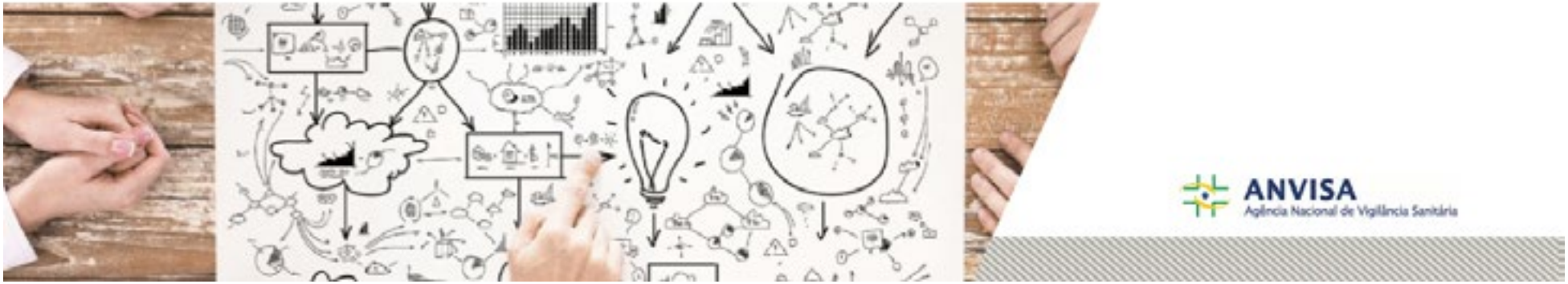
Canvas Ágil para Gestão de Riscos Corporativos_Anvisa | versão 3.0



Ferramenta para registro e gestão dos riscos

Painel de Gestão

Aplicando o método



Gestão de Riscos Corporativos - Anvisa

Participantes:_____ Processo:_____

Objetivo do processo: _____ Vinculo com a Estratégia:_____

IDENTIFICAÇÃO

1

CAUSAS

Evento de risco:_____

_____

Tipo de risco:_____

CONSEQUÊNCIAS

ESTIMATIVA E AVALIAÇÃO

2

NÍVEL DE PROBABILIDADE

Frequência passada		Chance de ocorrência	
Muito baixa		Raro 1 a 20%	
Baixa		Improvável 21 a 40%	
Média		Possível 41 a 60%	
Alta		Provável 61 a 80%	
Muito Alta		Quase Certo 80 a 99%	

NÍVEL DE IMPACTO

	1	2	4	8	16
Operacional					
Imagem					
Legal					
Orçamentário					
Integridade					

PLANEJAMENTO DA RESPOSTA

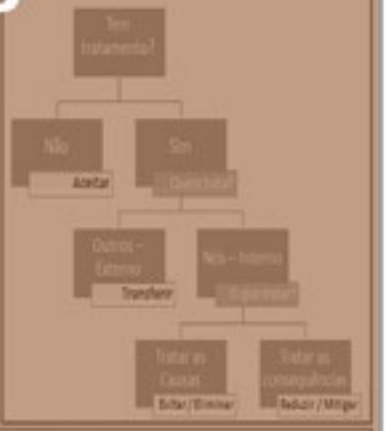
CONTROLES ATUAIS

NÍVEL DE CONFIANÇA DOS CONTROLES

Muito baixo	20%	
Baixo	40%	
Médio	60%	
Alto	80%	

3

RESPOSTA



PLANEJAMENTO

Descrição			
AÇÃO (What)	ATIVIDADES (How)	RESPONSÁVEIS (Who)	PRAZO (When)
O que?	*Como?*	*Quem?*	*Quando?*
QUANTO (How much)?			

Cartilha Agil para Gestão de Riscos Corporativos_Anvisa | versão 3.0

aplicação

Cases

01

•Gerir Tecnologia da Informação

02

•Gerir Contratações e Logística Administrativa

03

Gerir Pessoas

04

Gerir Atendimento e Transparência Organizacional

ANVISA
Agência Nacional de Vigilância Sanitária

aplicação

Eventos de riscos

•1.Falta de alinhamento entre o volume de demandas e projetos previstos no PDTI e a capacidade produtiva das demais áreas da instituição que atuam como corresponsáveis

2. Instabilidade nos sistemas operacionais, o que pode afetar a execução do processo

•3. Alterações inesperadas na legislação ou em marcos regulatórios pelos órgãos fiscalizadores e reguladores

4. Indisponibilidade de recursos, em virtude de concentração em um único fornecedor, o que pode impedir a execução do processo licitatório

5. Carência ou perda de conhecimento técnico especializado (implícito e explícito), o que pode afetar a qualidade dos serviços prestados

6.Resistência à mudança, o que pode dificultar a introdução de novas práticas gerenciais

7.Linguagem muito técnica nas respostas aos usuários

8. Rotatividade de colaboradores, comprometendo o bom atendimento aos usuários

VAMOS PRATICAR

ANVISA
Agência Nacional de Vigilância Sanitária

Prática

Regras

1. Cada time TEM UM MONITOR para ajudar no registro e sistematização das ideias.
2. Respeitar o **TEMPO É FUNDAMENTAL** para nossa oficina.
3. O monitor ajudará no entendimento da ferramenta, no controle do tempo e na mediação das discussões.
4. Pensamento visual, utilize post it para registrar as ideias (1 por ideia).
5. Uma ideia por vez, todos precisam compreender.
6. Estamos no momento de divergência, não existe certo ou errado.

ANVISA
Agência Nacional de Vigilância Sanitária

Gestão de Riscos Corporativos - Anvisa

Participantes:_____ **Processo:**_____

Objetivo do processo: _____ **Vínculo com a Estratégia:**_____

IDENTIFICAÇÃO

1

CAUSAS

Evento de risco:_____

Tipo de risco:_____

CONSEQUÊNCIAS

ESTIMATIVA E AVALIAÇÃO

NÍVEL DE PROBABILIDADE

Frequência passada		Chance de ocorrência	
Muito baixa		Raro 1 a 20%	
Baixa		Improvável 21 a 40%	
Média		Possivel 41 a 60%	
Alta		Provável 61 a 80%	
Muito Alta		Quase Certo 80 a 99%	

NÍVEL DE IMPACTO

	1	2	4	8	16
Operacional					
Imagem					
Legal					
Orçamentário					
Integridade					

PLANEJAMENTO DA RESPOSTA

CONTROLES ATUAIS

NÍVEL DE CONFIANÇA DOS CONTROLES

Muito baixo	20%	
Baixo	40%	
Médio	60%	
Alto	80%	

RESPOSTA

PLANEJAMENTO

Descrição			
AÇÃO (What)	ATIVIDADES (How)	RESPONSÁVEIS (Who)	PRAZO (When)
O que?	*Como?*	*Quem?*	*Quando?*
QUANTO (How much)?			

Canvas Ágil para Gestão de Riscos Corporativos, Anvisa | versão 3.0

Tipo (principal) de Risco:

Operacional

Comprometem as atividades da instituição: falhas, deficiência ou inadequação de processos internos, pessoas, infraestrutura e sistemas

Imagem

Comprometem a confiança da sociedade, parceiros, governo, setor regulado e/ou fornecedores em relação à capacidade da instituição em cumprir sua missão

Legal

Inovações ou alterações legislativas ou normativas que podem comprometer as atividades da instituição

Financeiro

Compromete a disposição dos recursos orçamentários e financeiros à realização de suas atividades; compromete execução orçamentária, ou acarretar prejuizo ao erário

Integridade

Refere-se ao alinhamento consistente e aderência a valores éticos compartilhados, princípios e normas para garantir e priorizar os interesses públicos sobre os privados.

ANVISA
Agência Nacional de Vigilância Sanitária

Causas e Consequências


O TEMPO ACABOU!
5
4
1
3
2
ANVISA
Agência Nacional de Vigilância Sanitária

Gestão de Riscos Corporativos - Anvisa

Participantes:_____ Processo:_____

Objetivo do processo: _____ Vínculo com a Estratégia:_____

IDENTIFICAÇÃO

1

CAUSAS

*Evento de risco:*_____

*Tipo de risco:*_____

CONSEQUÊNCIAS

ESTIMATIVA E AVALIAÇÃO

NÍVEL DE PROBABILIDADE

2

Frequência passada		Chance de ocorrência	
Muito baixa		Raro 1 a 20%	
Baixa		Improvável 21 a 40%	
Média		Possível 41 a 60%	
Alta		Provável 61 a 80%	
Muito Alta		Quase Certo 80 a 99%	

NÍVEL DE IMPACTO

	1	2	4	8	16
Operacional					
Imagem					
Legal					
Orçamentário					
Integridade					

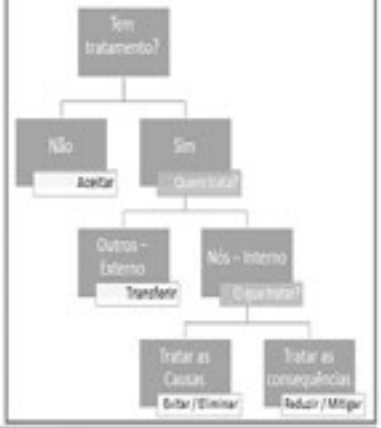
PLANEJAMENTO DA RESPOSTA

CONTROLES ATUAIS

NÍVEL DE CONFIANÇA DOS CONTROLES

Muito baixo	20%	
Baixo	40%	
Médio	60%	
Alto	80%	

RESPOSTA



PLANEJAMENTO

Descrição			
AÇÃO (What)	ATIVIDADES (How)	RESPONSÁVEIS (Who)	PRAZO (When)
O que?	*Como?*	*Quem?*	*Quando?*
QUANTO (How much)?			

Canvas Ágil para Gestão de Riscos Corporativos, Anvisa | versão 3.0

Probabilidade – 1 Voto/Pessoa:

Frequência - Passado

Grau	Categoria	Descrição	Ocorrência
1	Muito baixa	Eventos similares acontecem com uma frequência muito baixa	Quase não ocorreram no passado
2	Baixa	Outros eventos similares já aconteceram, mas são de baixa frequência	Existiram poucas ocorrências antes
3	Média	Eventos desse tipo ocorreram no passado com uma frequência regular	Ocorreram regularmente
4	Alta	Eventos similares acontecem na maioria das vezes ao no passado	Existiram bastante ocorrências antes
5	Muito alta	Outros eventos similares aconteceram com muita frequência no passado.	Ocorreram com muita frequência antes

ANVISA
Agência Nacional de Vigilância Sanitária

Probabilidade – 1 Voto/Pessoa:

Chance de Ocorrência - Futuro

Grau	Categoria	Descrição	Ocorrência
1	Raro - 1 a 20%	Este evento pode ter acontecido anteriormente na organização ou em organizações similares. Entretanto, na ausência de outras informações ou circunstâncias excepcionais, não seria esperado que ocorresse na organização no futuro próximo	O evento pode ocorrer apenas em circunstâncias muito excepcionais
2	Improvável - 21 a 40%	O evento não ocorre de maneira frequente na organização ou organizações similares. Os controles atuais e as circunstâncias sugerem que a ocorrência seria considerada altamente não usual	O evento pode ocorrer em algum momento, mas é improvável
3	Possível - 41 a 60%	O evento pode ter ocorrido ocasionalmente na organização ou em organizações similares. Os controles atuais ou as circunstâncias sugerem que há uma possibilidade plausível de ocorrência	O evento provavelmente ocorrerá em algumas circunstâncias
4	Provável - 61 a 80%	Este evento pode ocorrer regularmente na organização ou organizações similares. Com os controles atuais ou circunstâncias, pode-se esperar que ocorra ao longo de 1 ano	O evento provavelmente ocorrerá na maioria das circunstâncias
5	Quase certo - 81 a 90%	Este evento ocorre frequentemente na organização ou com os controles ou circunstâncias espera-se sua ocorrência	É esperado que o evento ocorra na maioria das circunstâncias

	Operacional	Imagem	Legal	Financeiro/ orçamentário	Integridade
16	Interrupção COMPLETA das operações ou de entrega de produtos ou serviços por período indeterminado de tempo OU A maioria dos programas ou projetos críticos não será concluído OU Intervenção externa para regularizar situação	Impacto adverso significativo OU Atenção extremamente negativa e consistente da mídia (meses) OU Perda de confiança irreconciliável na imagem da Anvisa	Resultará em litígios e multas significativos OU Pode envolver atividades sindicais OU Resultará em violações gravíssimas (não conformidade) de legislação / regulação	Impacto crítico de longo prazo no orçamento, não recuperável no exercício financeiro atual, nem no próximo	- Perturbações graves quanto à conduta e ética, resultando em grande corrupção ou fraudes OU - Grande priorização de interesses pessoais frente aos interesses públicos OU - Abuso de poder e uso das atribuições ou cargo para benefício próprio ou articulações indevidas
8	Interrupção SEVERA das operações ou de entrega de produtos ou serviços que impactem negativamente a imagem da Agência OU Um ou mais programas ou projetos críticos pode não ser concluído OU Intervenção de diretores para regularizar situação	Impacto adverso considerável OU Atenção negativa e consistente da mídia (semanas) OU Perda de confiança de ATORES específicos	Pode resultar em litígios que requeiram o envolvimento significativo da Procuradoria OU Resultará em violações graves (não conformidade) de legislação / regulação	Impacto muito alto no orçamento, não recuperável no exercício financeiro atual	- Utilizações incorretas de verbas e fundos para interesses próprios OU - Vazamento de informações privilegiadas ou restritas OU - Solicitação ou recebimento de propinas ou pagamentos indevidos
4	Interrupção em operações ou em entrega de produtos ou serviços que tenham algum impacto negativo OU Um ou mais programas ou projetos significativamente prejudicados OU Exige intervenção imediata do Gerente Geral	Impacto adverso localizado OU Atenção negativa da mídia (dias) OU Perda de confiança em processos de trabalhos atores específicos	Resultará em um incidente sério, com investigação e avaliação sobre responsabilidade legal OU Resultará em não conformidade de legislação / regulação	Impacto alto no orçamento, recuperável no exercício financeiro atual, mas requer priorização	- Descaso quanto à realização das atribuições causando desperdícios de recursos públicos ou má gestão OU - Nepotismo e uso das atribuições de forma antiética para influenciar agente públicos ou privados OU - Ceder a pressões internas ou externas que permitem corrupção, e não denunciar estes casos adversos
2	Alguma interrupção das operações ou na entrega de produtos ou serviços, mas que não causem tantos impactos OU Exige solução rápida (em até um mês), sendo gerente ou coordenador a tomar decisão.	Impacto e preocupação em atores locais OU Eventual atenção negativa da mídia	- Resultará em questões legais menos complexas ou não conformidades leves de legislação / regulação.	Impacto pequeno, mas perceptível, no orçamento, recuperável no exercício financeiro atual	- Imperícia e desleixo na condução das atribuições e tarefas OU - Repassar informações inverídicas ou fictícias para autopromoção OU - Tumultuar ambiente de trabalho e causar desinformação ou desserviço.
1	Impacto mínimo nas operações ou entrega de produtos ou serviços OU Exige solução rápida por meio da equipe.	Preocupação baseada em questões individuais OU Sem cobertura da mídia	- Surgem questões que podem ser resolvidas por procedimentos rotineiros, e não afetarão a conformidade com legislação ou regulação	Impacto mínimo no orçamento, recuperável no exercício financeiro atual	- Atitudes que quebram a confiança com superiores OU - Não desempenhar o trabalho com acurácia ou conformidade, desobedecendo regras superiores OU - Falta de companheirismo e altruísmo com os colegas de trabalho


O TEMPO
ACABOU!
5
4
1
3
2
ANVISA
Agência Nacional de Vigilância Sanitária

Gestão de Riscos Corporativos - Anvisa

Participantes:_____ Processo:_____

Objetivo do processo: _____ Vinculo com a Estratégia:_____

Resposta ao Risco

Ação ou resposta ao risco	Tipo de tratamento	Descrição
Aceitar	Não há o que fazer	Existem riscos em que nada pode ser feito.
Transferir	Passar a responsabilidade	Existem riscos em que devemos passar o ônus/responsabilidade para atores externos à Anvisa. (Ex.: Seguros, terceirizados, outros)
Eliminar ou Evitar	Tratar as causas	Existem riscos que devemos tratar suas causas, evitar que ocorram para que não impactem os objetivos.
Reduzir ou mitigar	Tratar as consequências	Existem riscos que não podemos evitar, mas que podemos tratar caso venham a acontecer.

ANVISA
Agência Nacional de Vigilância Sanitária

Controles Internos

Conjunto de regras, procedimentos, diretrizes, protocolos, rotinas de sistemas informatizados, conferências e trâmites de documentos e informações, entre outros, operacionalizados de forma integrada pela direção e pelos agentes públicos da instituição, destinados a enfrentar os riscos e fornecer segurança razoável na consecução da missão da Anvisa.

ANVISA
Agência Nacional de Vigilância Sanitária

Controles Internos x Nível de Confiança

Controles Atuais:

1. _____

2. _____

3. _____

4. _____

5. _____

... _____

Nível de confiança no controle	Escala	Descrição
Muito Baixo	20%	Os controles existentes são ineficazes, e dificilmente se poderá reduzir a probabilidade ou o impacto do risco.
Baixo	40%	Os controles são poucos e a confiança é baixa.
Médio	60%	Existe confiança nos controles atuais do risco.
Alto	80%	Os controles são satisfatórios e o risco tem grande possibilidade de ser controlado

ANVISA
Agência Nacional de Vigilância Sanitária

Planejamento

Descrição			
AÇÃO (What)	**ATIVIDADES (How)**	**RESPONSÁVEIS (Who)**	**PRAZO (When)**
O que?	***Como?***	***Quem?***	***Quando?***
QUANTO (How much)?			

ANVISA
Agência Nacional de Vigilância Sanitária


O TEMPO ACABOU!
5
4
1
3
2
ANVISA
Agência Nacional de Vigilância Sanitária

Wildenildo Santos

Cqual@anvisa.gov.br

Coordenação de Qualidade em Processos Organizacionais

Assessoria de Planejamento/Anvisa

ANVISA
Agência Nacional de Vigilância Sanitária

Apresentação 11:

Gestão de Riscos Corporativos

O caso de uma agência reguladora de saúde

FABIANO FERREIRA DE ARAÚJO


Gestão de Riscos Corporativos
O caso de uma agência reguladora da saúde
ANVISA
Agência Nacional de Vigilância Sanitária

AGENDA

- Contexto Anvisa
- A Política de GRC da Anvisa
  - Antecedentes
  - Processo de construção
- Metodologia sob medida
  - Prototipagem e capacitação
- Governança
- Perspectivas 2019-2020

ANVISA
Agência Nacional de Vigilância Sanitária

O QUE É

A ANVISA

MISSÃO

"Proteger e promover a saúde da população, mediante a **intervenção nos riscos decorrentes da produção e do uso de produtos e serviços** sujeitos à vigilância sanitária, em ação coordenada e integrada no âmbito do Sistema Único de Saúde"

VISÃO

"Ser uma instituição **promotora de saúde, cidadania e desenvolvimento**, que atua de forma ágil, eficiente e transparente, consolidando-se como protagonista no campo da regulação e do controle sanitário, nacional e internacionalmente"

ANVISA
Agência Nacional de Vigilância Sanitária


O QUE É
A ANVISA
SNVS
+
SUS
A ANVISA COORDENA O SISTEMA NACIONAL DE VIGILÂNCIA SANITÁRIA (SNVS), QUE É VINCULADO AO SISTEMA ÚNICO DE SAÚDE (SUS)
ANVISA
www.anvisa.gov.br
ANVISA
Agência Nacional de Vigilância Sanitária

O QUE É

A ANVISA

CRIADA HÁ 19 ANOS

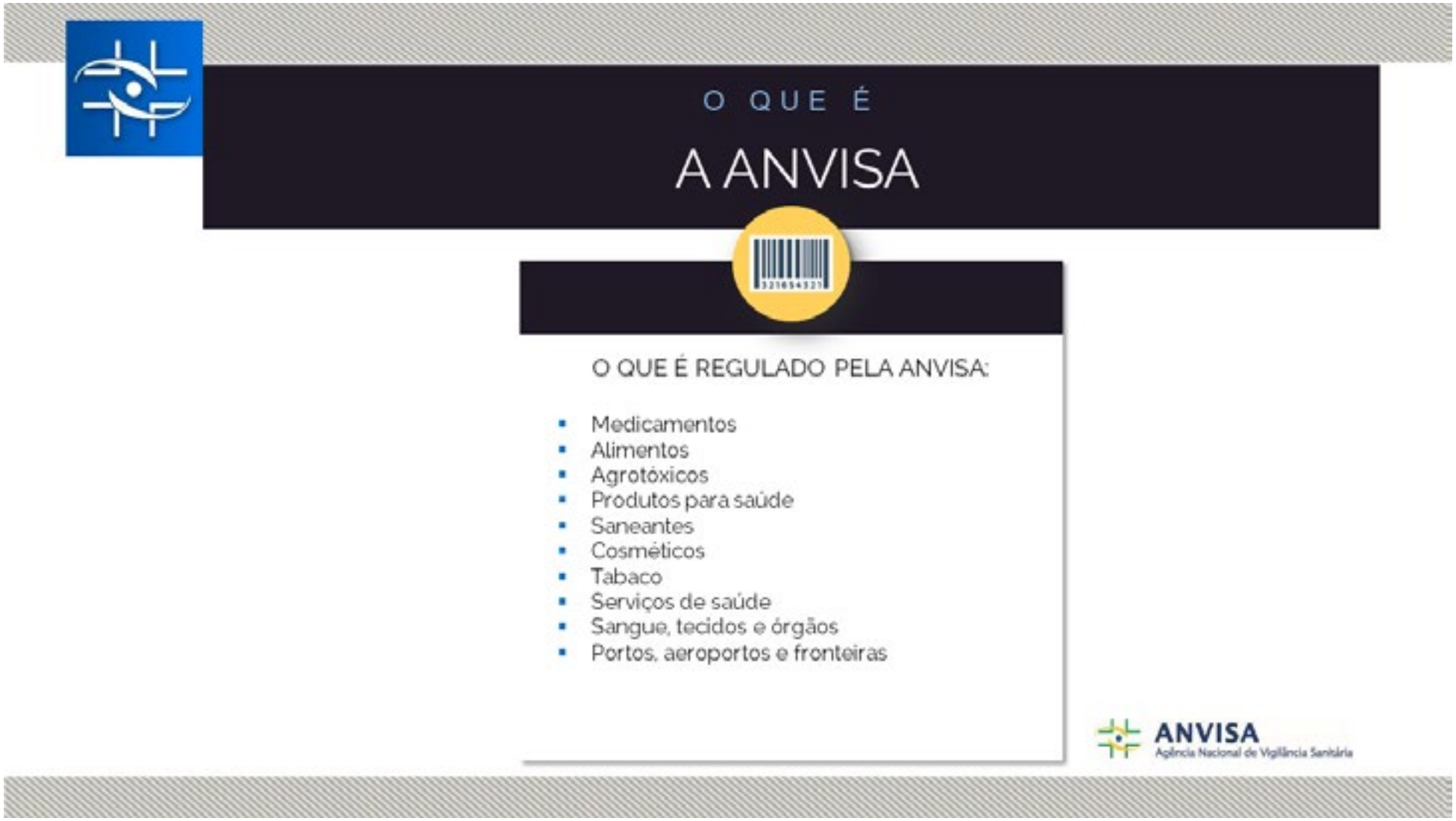
REGULA 22,7% do VAB*

IMPACTA EM 100% DAS VIDAS

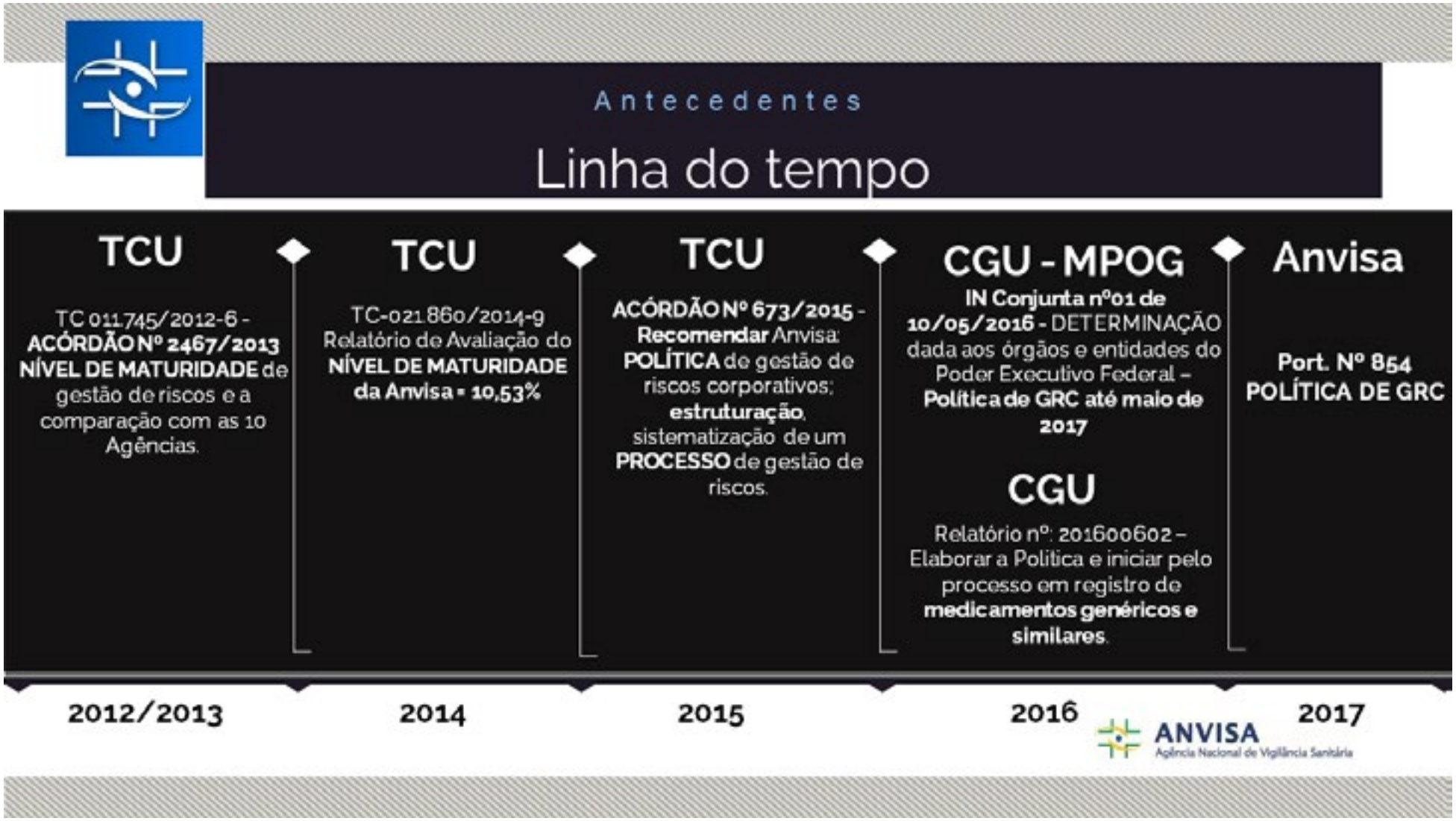
- **R$ 1,13 trilhão (22,7%) dos R$ 4,97 trilhões do valor adicionado bruto da economia brasileira (2014).**

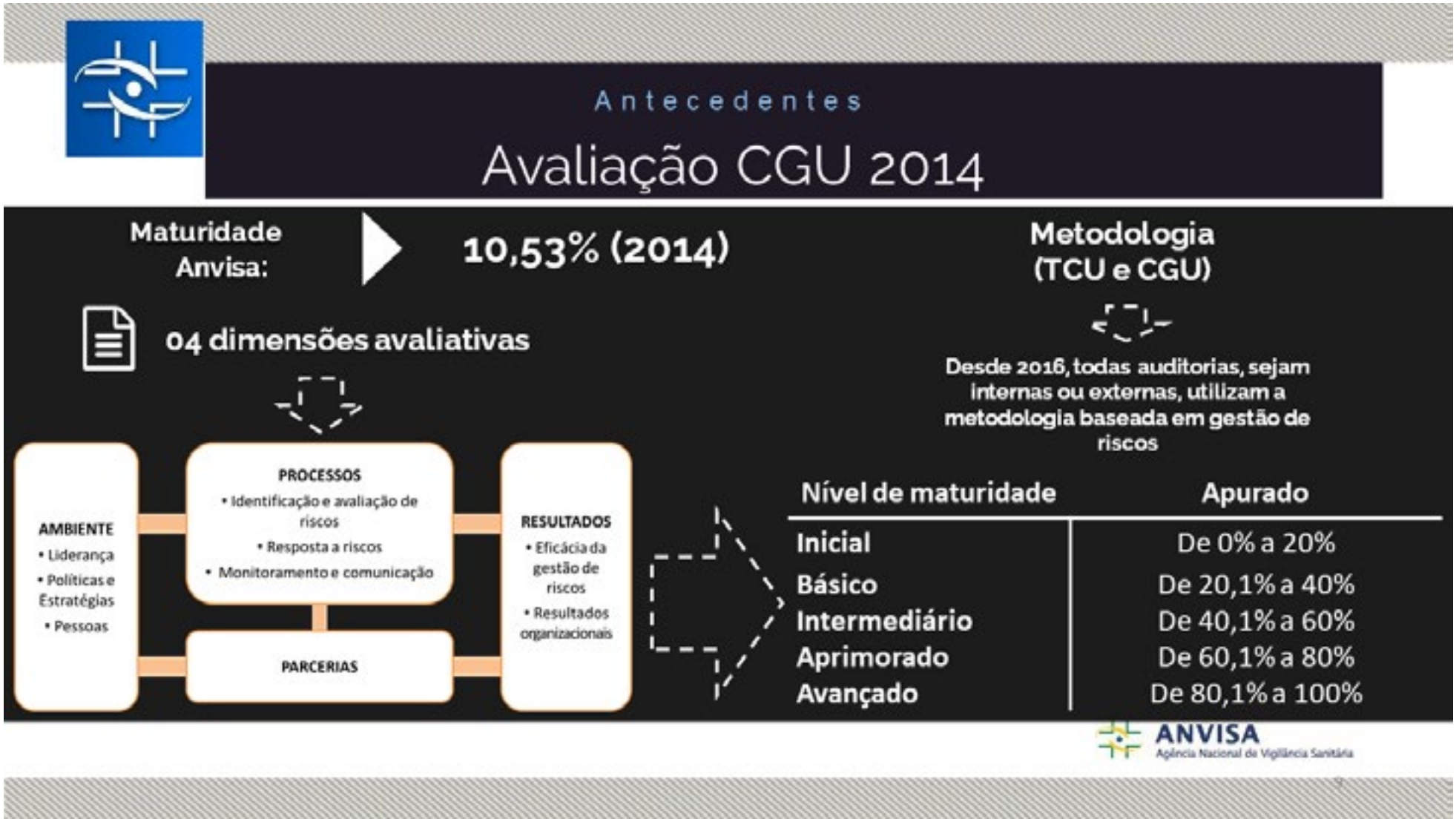
** Valor adicionado: Valor que a atividade agrega aos bens e serviços consumidos no seu processo produtivo. É a contribuição ao produto interno bruto pelas diversas atividades econômicas, obtida pela diferença entre o valor de produção e o consumo intermediário absorvido por essas atividades (IPEADATA).*

ANVISA
Agência Nacional de Vigilância Sanitária


O QUE É
A ANVISA
O QUE É REGULADO PELA ANVISA:
Medicamentos
Alimentos
Agrotóxicos
Produtos para saúde
Saneantes
Cosméticos
Tabaco
Serviços de saúde
Sangue, tecidos e órgãos
Portos, aeroportos e fronteiras
ANVISA
Agência Nacional de Vigilância Sanitária

Antecedentes


Antecedentes
Linha do tempo
TCU
TC 011.745/2012-6 - **ACÓRDÃO Nº 2467/2013** **NÍVEL DE MATURIDADE** de gestão de riscos e a comparação com as 10 Agências.
2012/2013
TCU
TC-021.860/2014-9 Relatório de Avaliação do **NÍVEL DE MATURIDADE da Anvisa = 10,53%**
2014
TCU
ACÓRDÃO Nº 673/2015 - Recomendar Anvisa: **POLÍTICA** de gestão de riscos corporativos; **estruturação**, sistematização de um **PROCESSO** de gestão de riscos.
2015
CGU - MPOG
IN Conjunta nº01 de 10/05/2016 - DETERMINAÇÃO dada aos órgãos e entidades do Poder Executivo Federal – **Política de GRC até maio de 2017**
CGU
Relatório nº: 201600602 – Elaborar a Política e iniciar pelo processo em registro de **medicamentos genéricos e similares**.
2016
Anvisa
Port. Nº 854 POLÍTICA DE GRC
2017
ANVISA
Agência Nacional de Vigilância Sanitária


Antecedentes
Avaliação CGU 2014
Maturidade Anvisa:
10,53% (2014)
Metodologia (TCU e CGU)
04 dimensões avaliativas
Desde 2016, todas auditorias, sejam internas ou externas, utilizam a metodologia baseada em gestão de riscos
AMBIENTE
• Liderança
• Políticas e Estratégias
• Pessoas
PROCESSOS
• Identificação e avaliação de riscos
• Resposta a riscos
• Monitoramento e comunicação
PARCERIAS
RESULTADOS
• Eficácia da gestão de riscos
• Resultados organizacionais
Nível de maturidade
Apurado
Inicial
De 0% a 20%
Básico
De 20,1% a 40%
Intermediário
De 40,1% a 60%
Aprimorado
De 60,1% a 80%
Avançado
De 80,1% a 100%
ANVISA
Agência Nacional de Vigilância Sanitária

Portaria Anvisa nº 854/2017

O processo de construção da Política de GRC Anvisa


Política
Processo de construção
Grupo de trabalho
5
DIRETORIAS ENVOLVIDAS
+ APLAN/GADIP + AUDITORIA
4 RODADAS
DE BENCHMARKING
2 PORTARIAS
PUBLICADAS
3
APRESENTAÇÕES DE SOFTWARE
7 NOTÍCIAS
PUBLICADAS
03 SUB-GRUPOS
ELABORAÇÃO DA POLÍTICA
1 CONSULTA INTERNA
LEITURA DE 20
POLÍTICAS
DE GRC
50 HORAS DE REUNIÃO
Pasta corporativa e e-mail institucional
ANVISA


Politica
Processo de construção
1.BENCHMARKING
2. AVALIAÇÃO DO DIAGNÓSTICO
3. FORMULAÇÃO DA POLÍTICA
4. CONSULTA INTERNA
ANS
ANATEL
BANCO CENTRAL DO BRASIL
EMBRAPA
OFICINAS DE ALINHAMENTO CONCEITUAL
LEITURA DOS RELATÓRIOS E ACÓRDÃOS DO TCU E CGU
ESTUDO DAS METODOLOGIAS
- ISO 31000
- COSO II
- M.o.R
Minuta de politica de GRC, a ser submetida à consulta interna e à aprovação da DICOL.
73 contribuições
71,2% nunca trabalharam com processo de gestão de risco corporativo
ANVISA

Politica

Portaria nº 854, de 30 de maio de 2017

ANVISA
Agência Nacional de Vigilância Sanitária

Politica

Publicações

https://revista.enap.gov.br/index.php/RSP/article/view/3159

Política de gestão de riscos corporativos: o caso de uma agência reguladora da saúde.
Revista do Serviço Público (Brasília). , v.69, p.7 - 32, 2018.

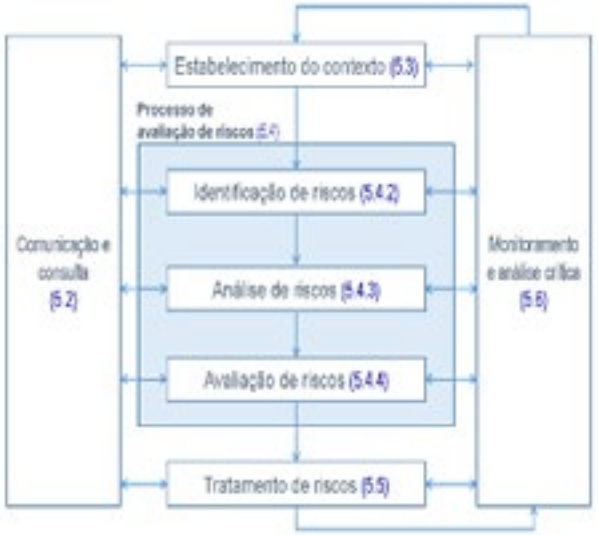
ANVISA
Agência Nacional de Vigilância Sanitária

Metodologia sob medida

Metodologia

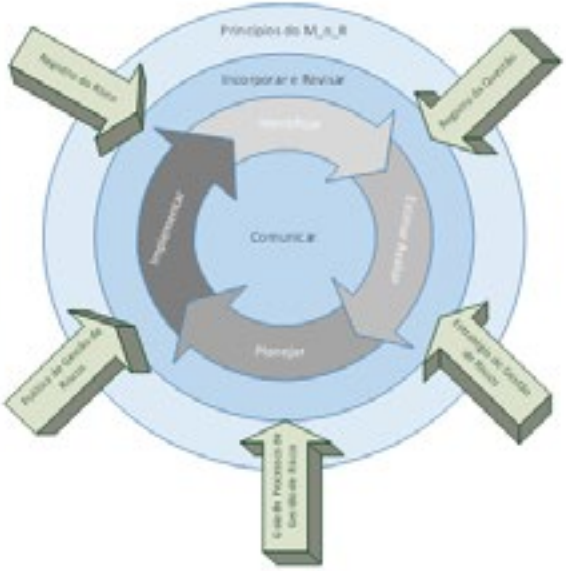
Fontes de inspiração

ISO 31000



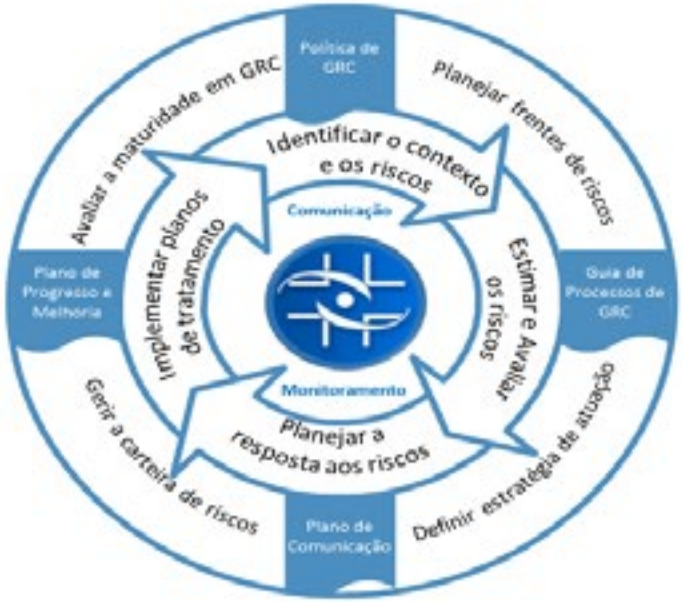
COSO ERM

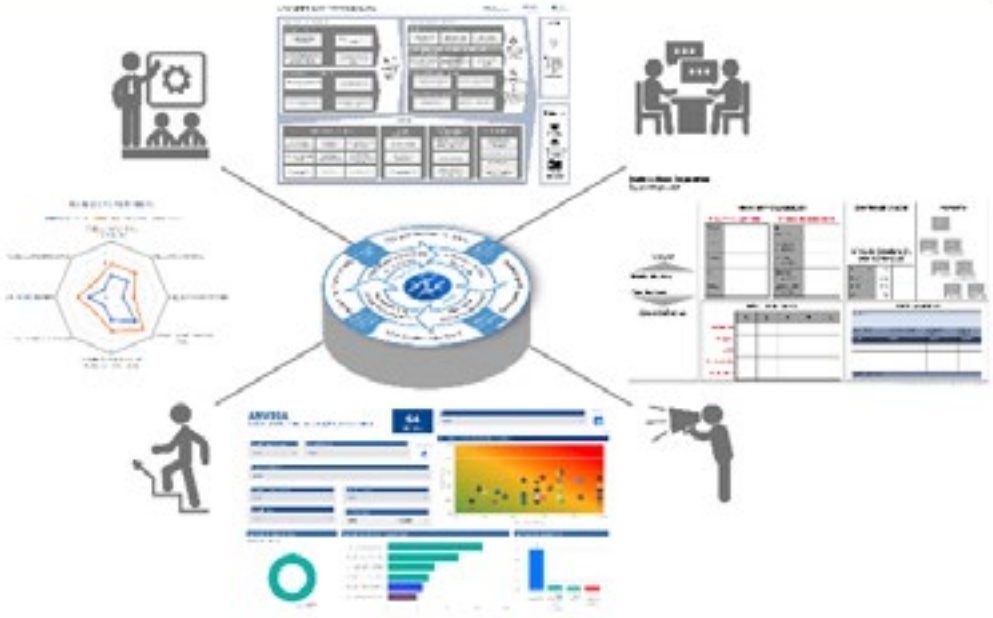
M.o.R.



ANVISA
Agência Nacional de Vigilância Sanitária

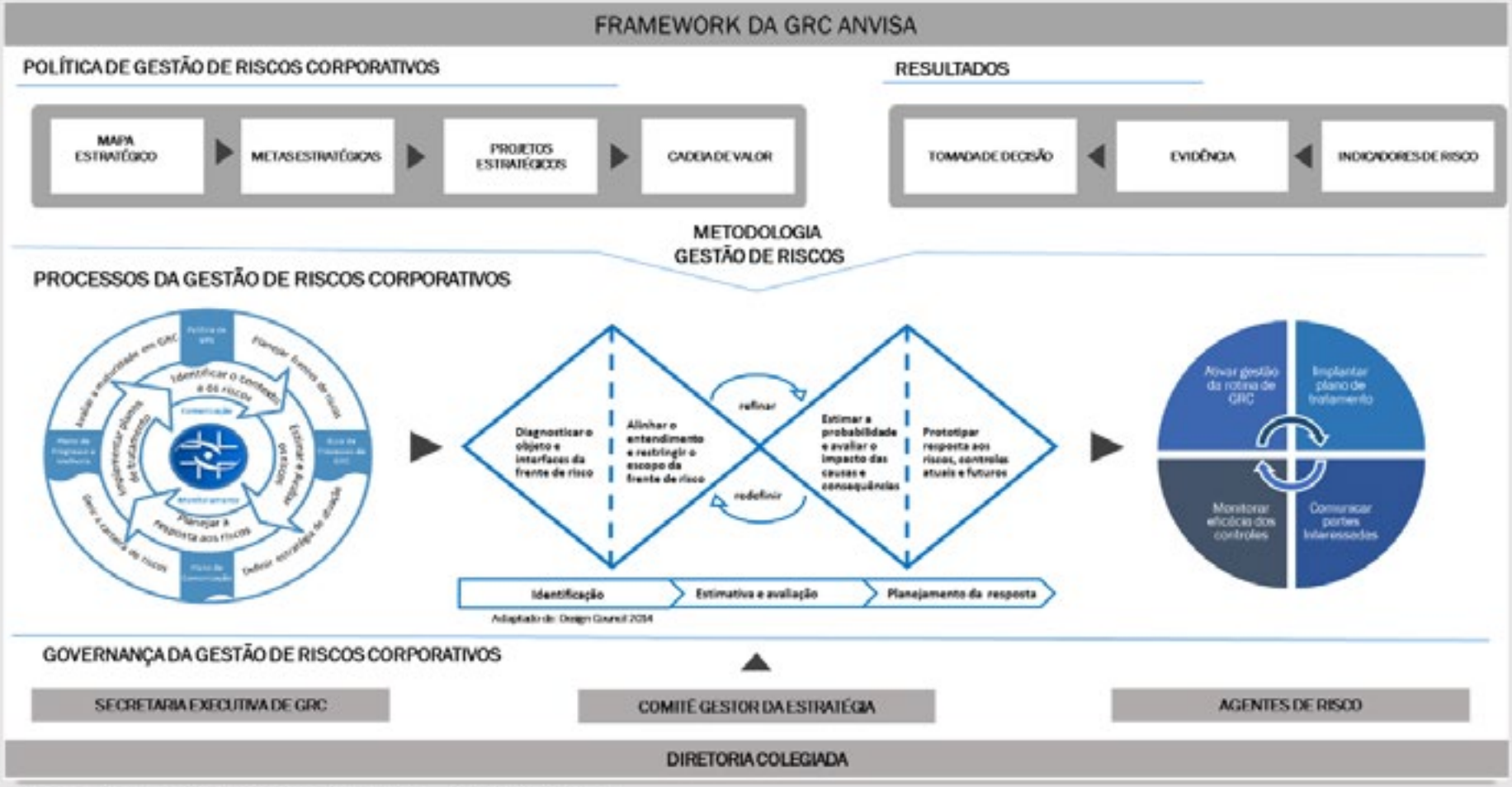
Metodologia



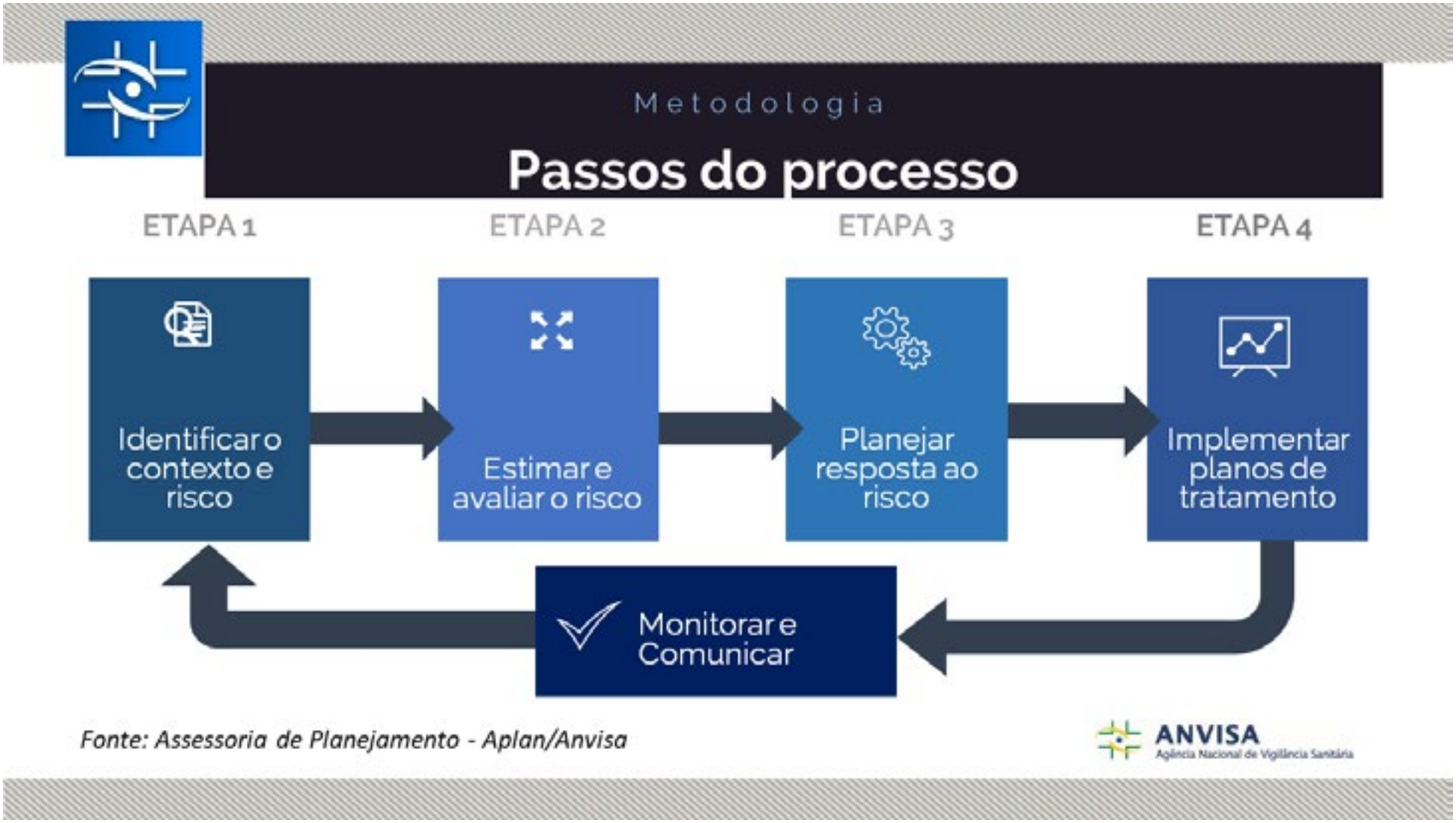


Fonte: Assessoria de Planejamento - Aplan/Anvisa

ANVISA
Agência Nacional de Vigilância Sanitária



Fonte: Assessoria de Planejamento - Aplan/Anvisa


Metodologia
Passos do processo
ETAPA 1
ETAPA 2
ETAPA 3
ETAPA 4
Identificar o contexto e risco
Estimar e avaliar o risco
Planejar resposta ao risco
Implementar planos de tratamento
Monitorar e Comunicar
Fonte: Assessoria de Planejamento - Aplan/Anvisa
ANVISA
Agência Nacional de Vigilância Sanitária

Metodologia

Princípios da GRC na Anvisa

1. Protege a missão e a visão institucionais
2. Subordina-se aos interesses públicos
3. Cria e protege valor institucional
4. Requer dinamismo, iteratividade, resiliência e inovação na Anvisa
5. Favorece a transparência e a inclusão

ANVISA
Agência Nacional de Vigilância Sanitária

Metodologia

Benefícios da GRC

ANVISA
Agência Nacional de Vigilância Sanitária

Metodologia

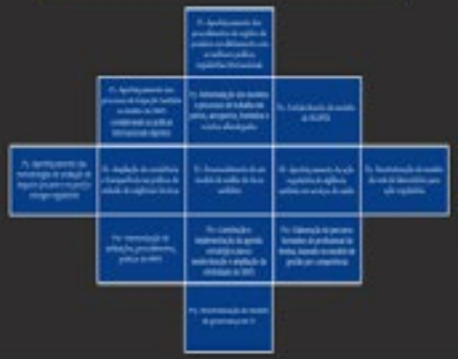
Onde aplicar

Gestão de riscos na Anvisa

MAPA ESTRATÉGICO

METAS ESTRATÉGICAS

PROJETOS ESTRATÉGICOS



CADEIA DE VALOR

ANVISA
Agência Nacional de Vigilância Sanitária

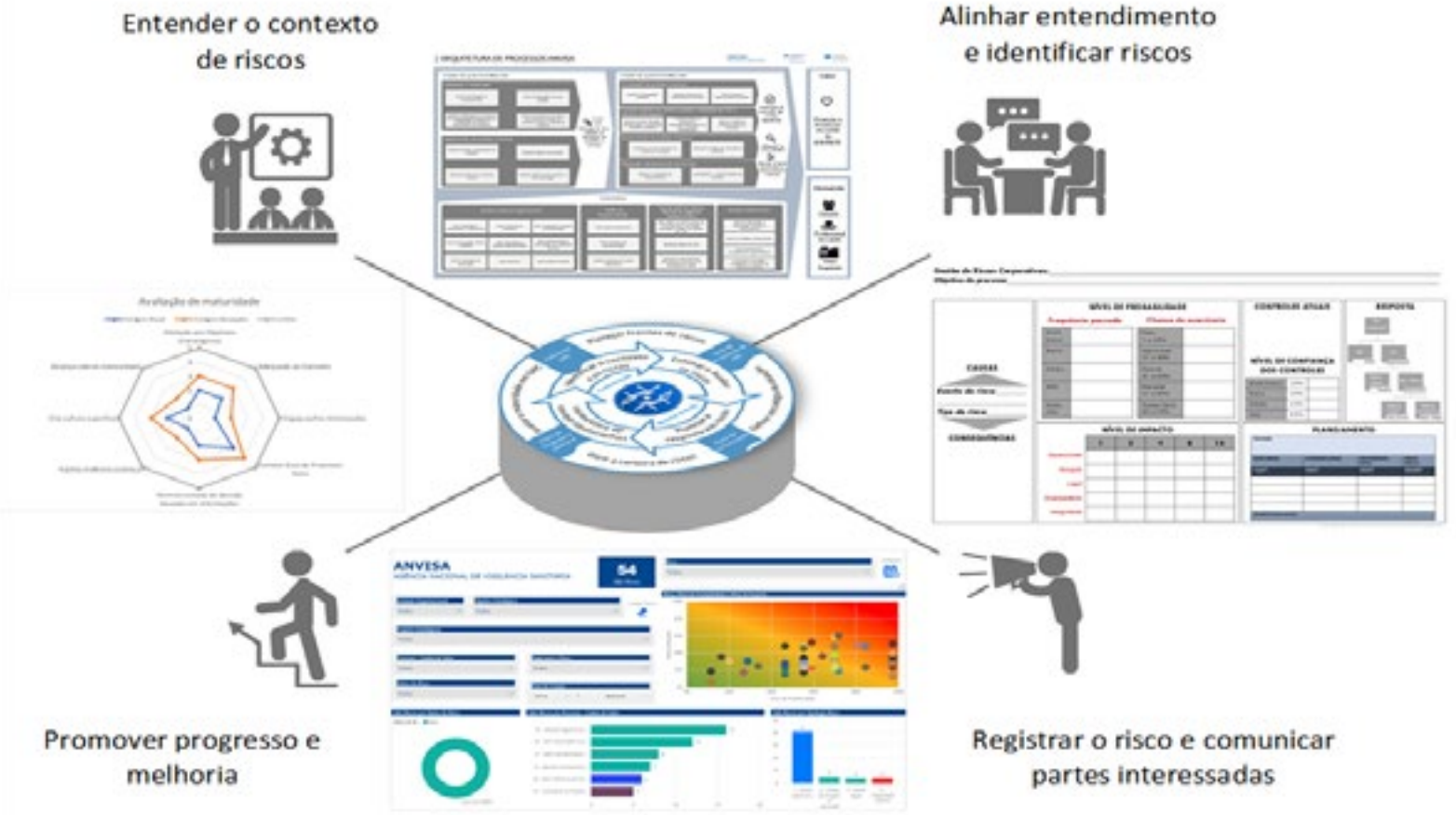
Prototipando a ferramenta e desenvolvendo competências


Prototipagem
Projetos-piloto
1. Gerir compras e aquisições;
2. Gerir melhoria de processos;
3. Coordenar as ações do plano nacional de resistência antimicrobiana;
4. Realizar registro e pós-registro de medicamentos;
5. Emitir anuência de importação (LI);
6. Gerir documentos;
7. Gerir estratégia e desempenho institucional; e
8. Projeto Estratégico nº 05 – Aperfeiçoamento da regulamentação.
ANVISA
Agência Nacional de Vigilância Sanitária


Formação de competências
Parceria CGU
Ministério da Transparência, Fiscalização e Controladoria-Geral da União
2017
2018 -1
2018 - 2

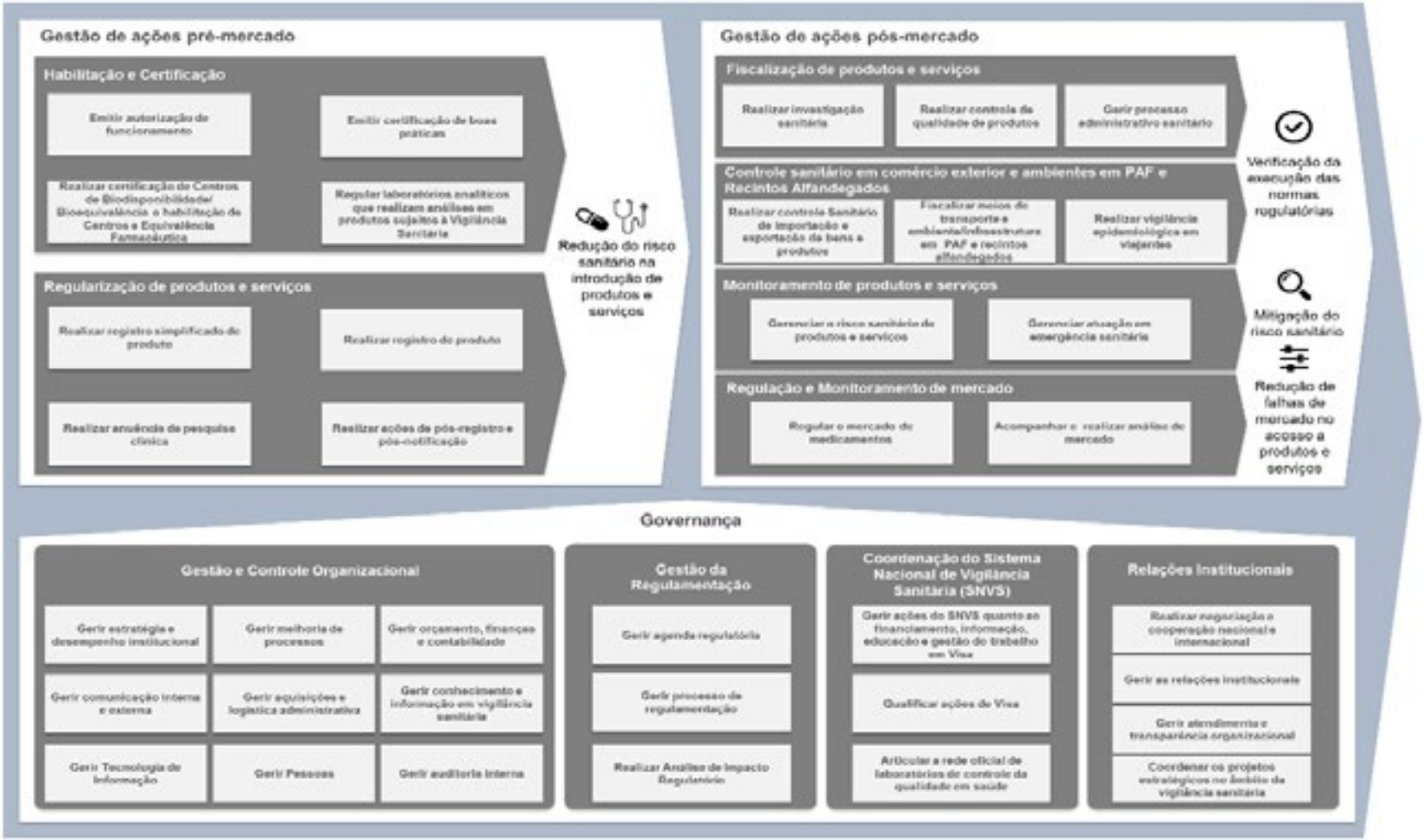
Ciclo de GRC

Desdobrando a metodologia



Fonte: Assessoria de Planejamento - Aplan/Anvisa

CADEIA DE VALOR



Gestão de Riscos Corporativos - Anvisa

Participantes:_____ **Processo:**_____

Objetivo do processo: _____ **Vínculo com a Estratégia:**_____

IDENTIFICAÇÃO

CAUSAS

Evento de risco:_____

Tipo de risco:_____

CONSEQUÊNCIAS

ESTIMATIVA E AVALIAÇÃO

NÍVEL DE PROBABILIDADE

Frequência passada		Chance de ocorrência	
Muito baixa		Raro 1 a 20%	
Baixa		Improvável 21 a 40%	
Média		Possível 41 a 60%	
Alta		Provável 61 a 80%	
Muito Alta		Quase Certo 80 a 99%	

NÍVEL DE IMPACTO

	1	2	4	8	16
Operacional					
Imagem					
Legal					
Orçamentário					
Integridade					

PLANEJAMENTO DA RESPOSTA

CONTROLES ATUAIS

NÍVEL DE CONFIANÇA DOS CONTROLES

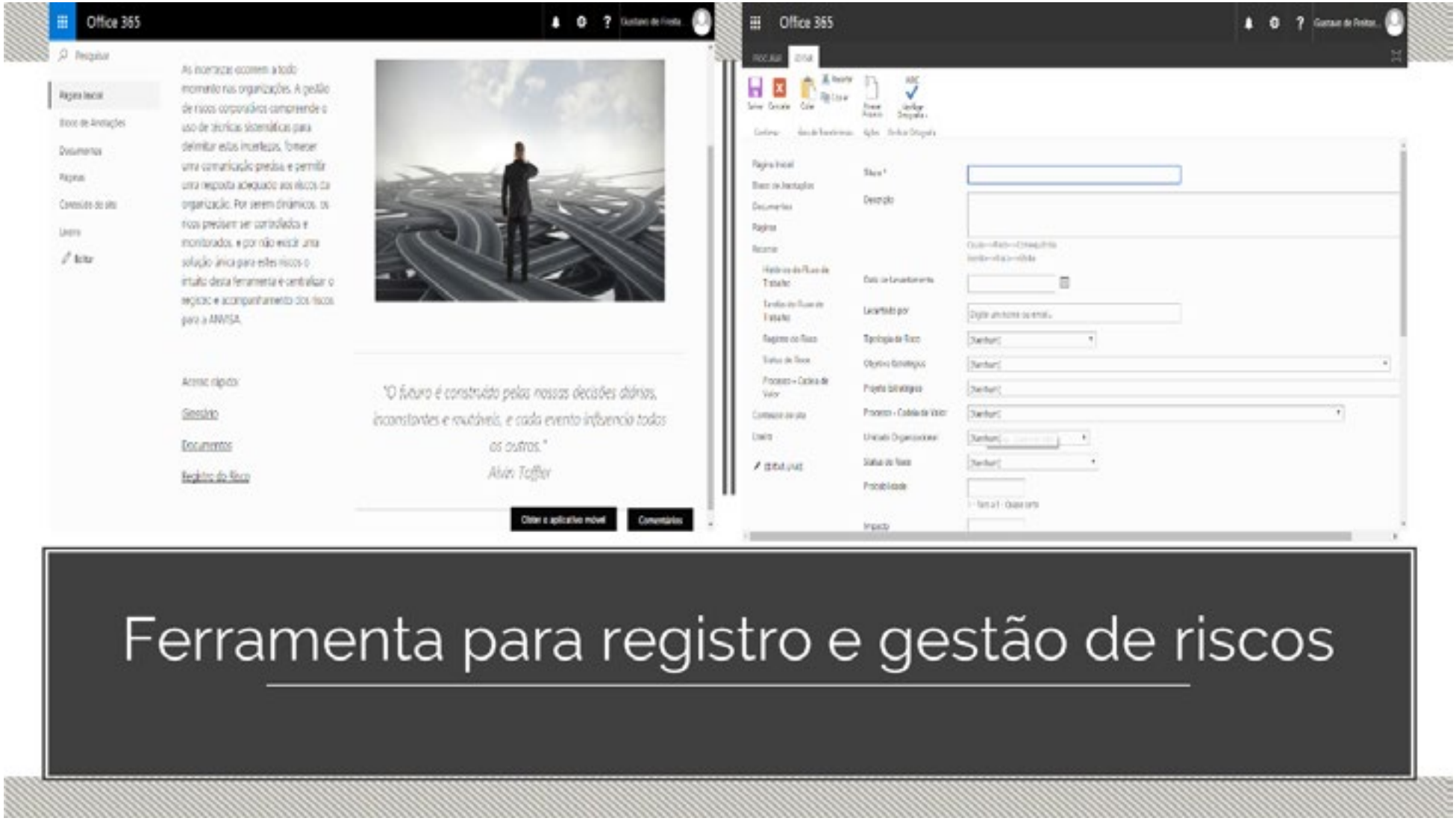
Muito baixo	20%	
Baixo	40%	
Médio	60%	
Alto	80%	

RESPOSTA

PLANEJAMENTO

Descrição			
AÇÃO (What)	ATIVIDADES (How)	RESPONSÁVEIS (Who)	PRAZO (When)
O que?	*Como?*	*Quem?*	*Quando?*
QUANTO (How much)?			

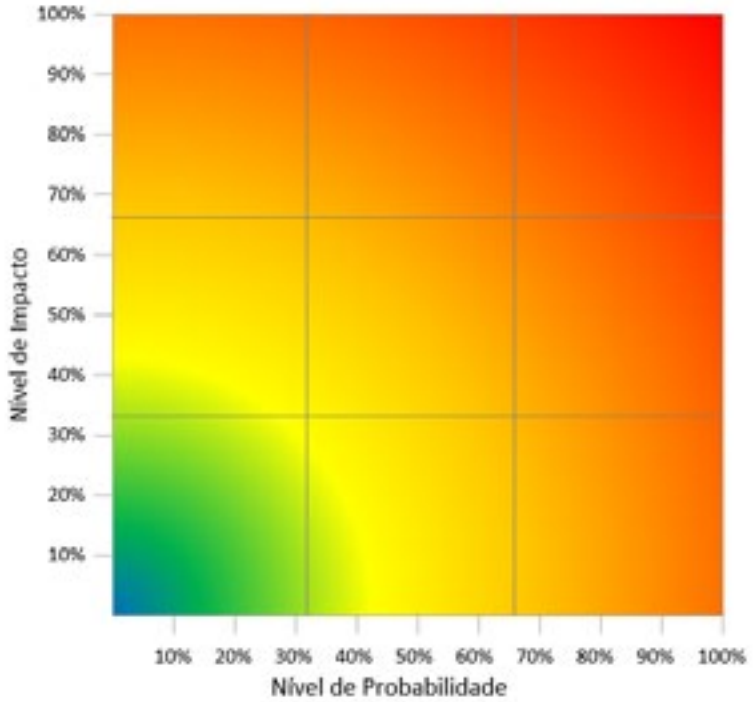
Canvas Ágil para Gestão de Riscos Corporativos, Anvisa | versão 3.0


Office 365
Office 365
Ferramenta para registro e gestão de riscos


ANVISA
AGÊNCIA NACIONAL DE VIGILÂNCIA SANITÁRIA
67
Qtd. Riscos
Risco
Todos
Histórico
Unidade Organizacional
Todos
Objetivo Estratégico
Todos
Limpar Filtros
Projetos Estratégicos
Todos
Processo - Cadeia de Valor
Todos
Etapa para o Risco
Todos
Status do Risco
Todos
Data de Criação
Último
1
Selecionar
Nível do Risco por Risco, Nível de Probabilidade e Nível de Impacto
100%
80%
60%
40%
20%
0%
Nível de Impacto
0%
20%
40%
60%
80%
100%
Nível de Probabilidade
Qtd. Riscos por Status do Risco
Status do Ri...
Ativo
Ativo 67 (100%)
Qtd. Riscos por Processo - Cadeia de Valor
05 - Realizar Registro...
16
24 - Gerir Aquisições ...
12
21 - Gerir Conhecime...
8
12 - Realizar Controle...
7
19 - Gerir Estratégia ...
7
(Em branco)
6
20 - Gerir Melhoria d...
6
37 - Coordenar os Pr...
5
Qtd. Riscos por Tipologia Risco
60
40
20
0
52
6
4
1
6
1 - Riscos operacionais
2 - Riscos de imagem ou
3 - Riscos legais
4 - Riscos orçamentár...
5 - Integridade

Mapa de Riscos

Avaliação do Risco: Nível de Risco



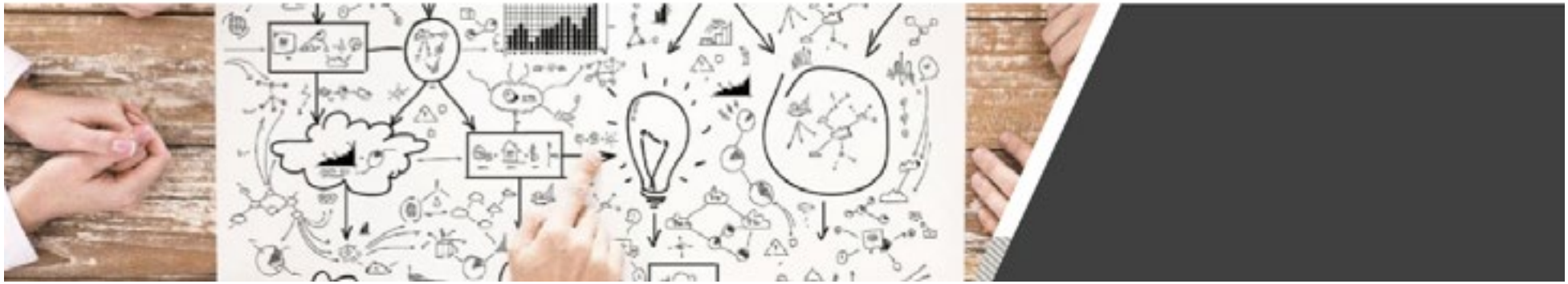
Níveis de tolerância			Detalhamento
	Acima de 65%	Ação imediata – Intolerável	Situações problema que possam impedir a organização de continuar funcionando.
	41 a 65%	Ação Média e Curto Prazo	Situações problema que possam impedir parte da organização de continuar funcionando.
	21 a 40%	Monitoramento e Gestão	Situações problema que possam afetar o funcionamento de unidades organizacionais com suas atividades.
	11 a 20%	Risco Controlável	Situações problema que possam afetar o andamento dos trabalhos.
	Abaixo de 10%	Risco Desprezível	Situações que não acarretam problemas

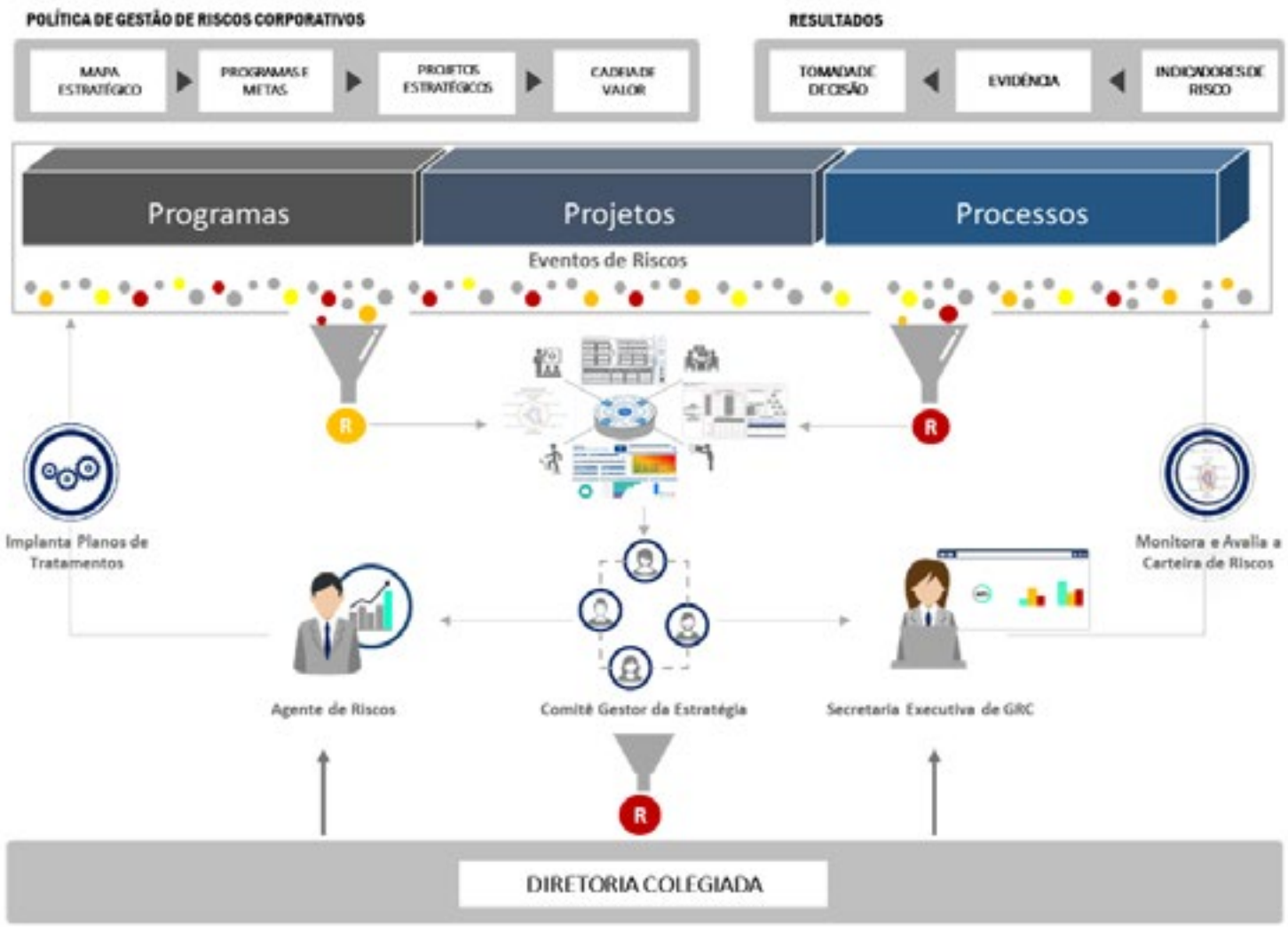
ANVISA
Agência Nacional de Vigilância Sanitária

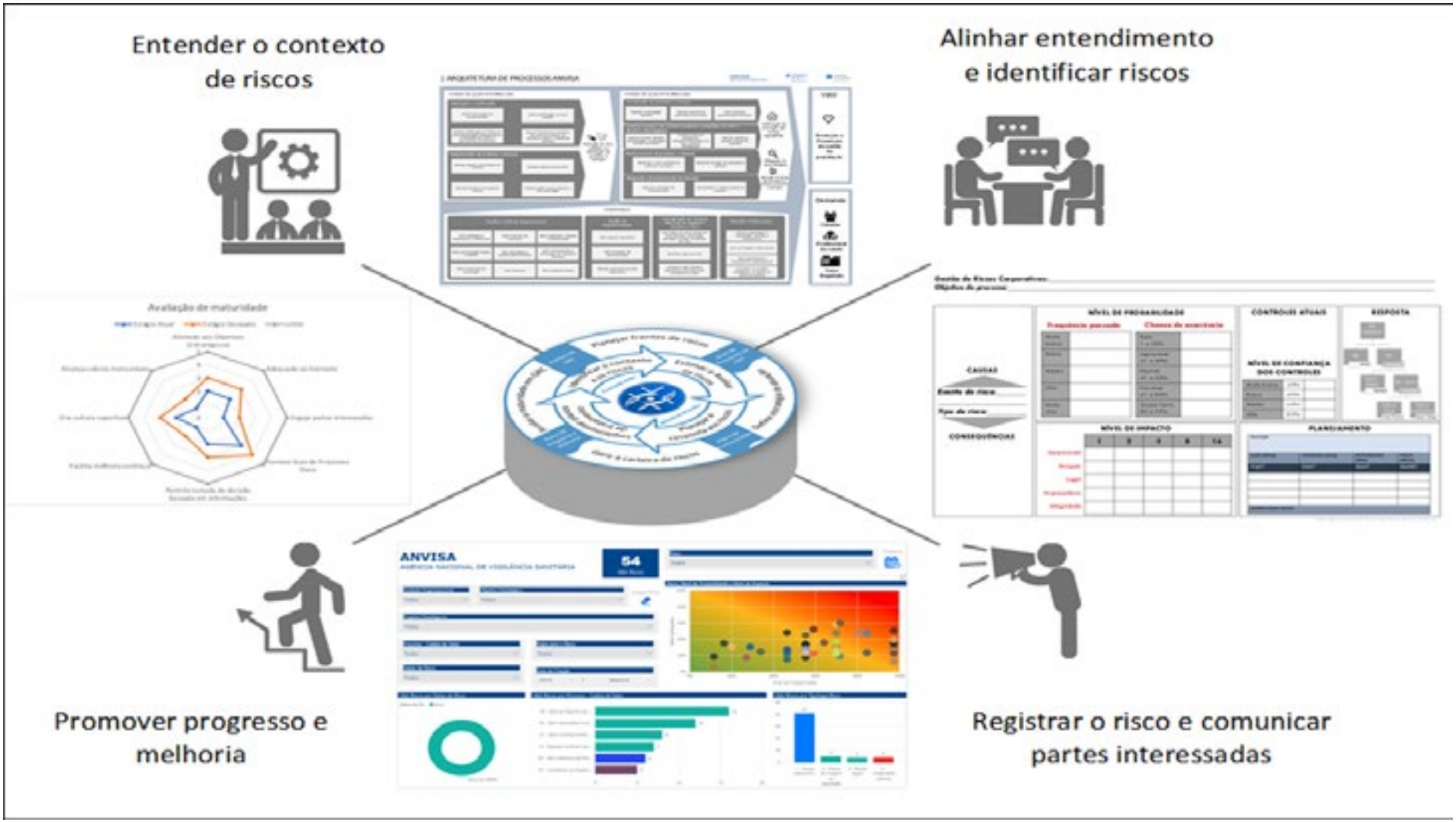
Princípios	Estágio Atual	Estágio Desejado	Limite
Alinhamento aos objetivos	2	3	5
Adequação ao contexto	2	3	5
Engajamento de partes interessadas	1	2	5
Fornecimento de um guia de processos claro	3	4	5
Apoio à tomada de decisão	2	3	5
Apoio à melhoria contínua	1	2	5
Criação de cultura suportiva	2	3	5
Alcance de valores mensuráveis	1	2	5

Progresso e melhoria

Governança em GRC na Anvisa

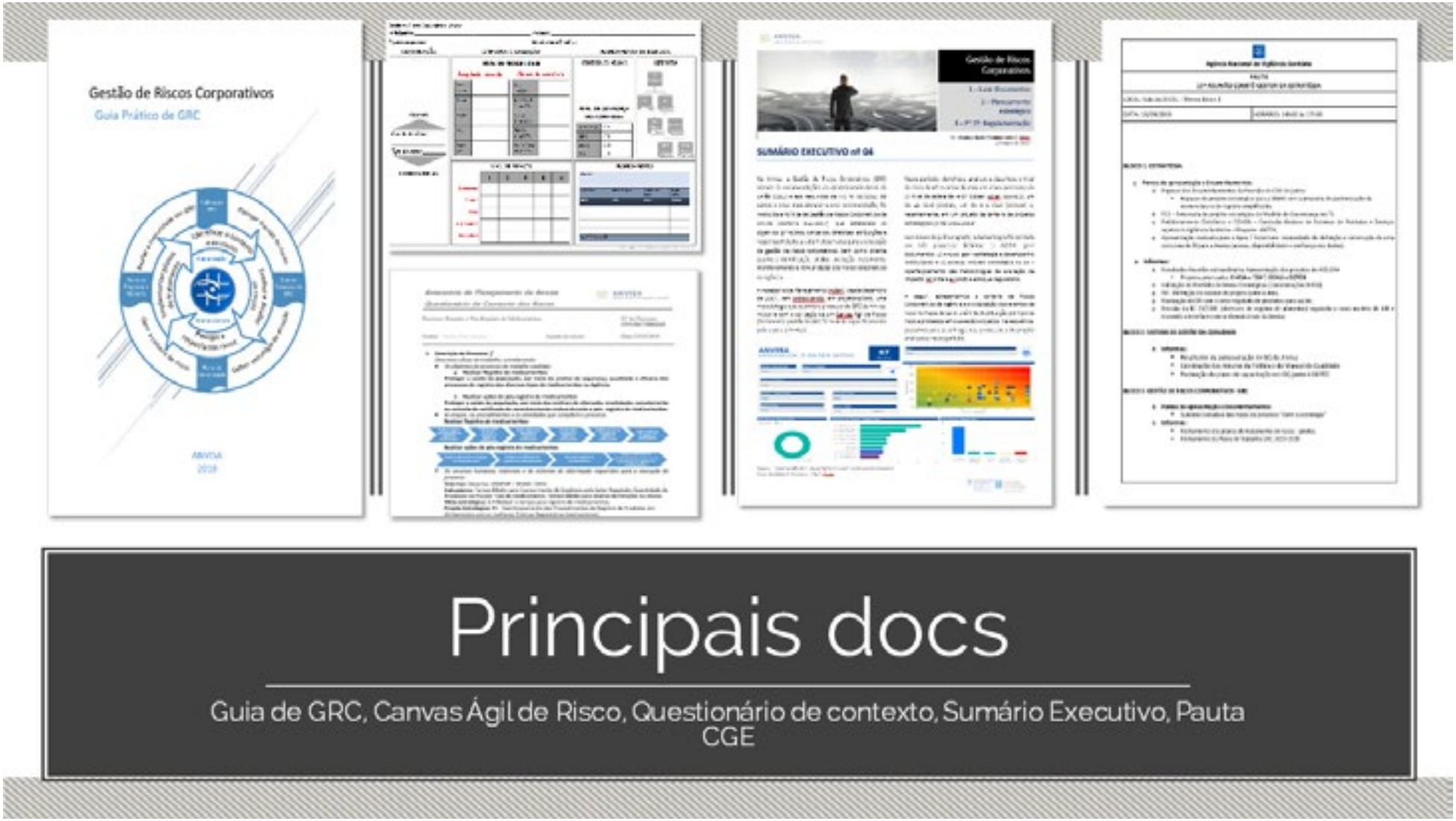



POLÍTICA DE GESTÃO DE RISCOS CORPORATIVOS
MAPA ESTRATÉGICO
PROGRAMAS E METAS
PROJETOS ESTRATÉGICOS
CADEIA DE VALOR
RESULTADOS
TOMADA DE DECISÃO
EVIDÊNCIA
INDICADORES DE RISCO
Programas
Projetos
Processos
Eventos de Riscos
R
R
Implanta Planos de Tratamentos
Monitora e Avalia a Carteira de Riscos
Agente de Riscos
Comitê Gestor da Estratégia
Secretaria Executiva de GRC
R
DIRETORIA COLEGIADA


Entender o contexto de riscos
Alinhar entendimento e identificar riscos
Promover progresso e melhoria
Registrar o risco e comunicar partes interessadas
ANVISA

Estrutura de governança


Papel do CGE
Escopo de atuação
Acompanhar o desenvolvimento e a implementação da estratégia
Promover as articulações necessárias para o adequado desenvolvimento da estratégia
Avaliar os resultados das ações realizadas na implementação da estratégia
Avaliar a adequação, suficiência e eficácia da estrutura e do Processo de GRC
Priorizar riscos e submeter recomendação e proposição à Diretoria Colegiada
Deliberar sobre a metodologia de GRC
Aprovar o apetite, a tolerância e definir os critérios de riscos
Estabelecer a estratégia de atuação da Anvisa, em cumprimento à sua finalidade institucional
ANVISA
Agência Nacional de Vigilância Sanitária



Principais docs

Guia de GRC, Canvas Ágil de Risco, Questionário de contexto, Sumário Executivo, Pauta CGE

Perspectivas 2019-2020


Gestão de Riscos Corporativos 2019-2020
ANVISA
Agência Nacional de Vigilância Sanitária
PLANEJAMENTO ESTRATÉGICO
ESCRITÓRIO DE PROCESSOS
PROCESSOS ENVOLVIDOS
GUIA DE GRC
PLANO DE COMUNICAÇÃO
AVALIAÇÃO DE MATURIDADE
ESCOPO DE PROJETO
IMPLANTAR METODOLOGIA DE GRC DA ANVISA
Consolidar metodologia de GRC da Anvisa aplicando o modelo nos 37 processos de terceiro nível da Cadeia de Valor até dezembro de 2020 (ciclo contínuo de GRC)
Planejamento do Projeto
* Templates e ferramentas
PLANEJAR FRENTES DE RISCOS E GERIR CARTEIRA DE RISCOS
a) Retomar planos de tratamento de projetos-piloto
b) Aplicar matriz de priorização de em processos críticos projetos estratégicos
c) Definir cronograma por frente de risco priorizada
d) Definir responsáveis pela implementação de cada frente de risco e suas respectivas atribuições
e) Delimitar prazos para cada etapa da frente de risco
PRODUTOS GERADOS
• Cronograma de aplicação das frentes de riscos
• Planner de cada frente de riscos no Sharepoint de GRC
Planejamento das frentes de GRC
CONSOLIDAR PLANO DE COMUNICAÇÃO
a) Formatar plano, definir estratégia, instrumentos e canais de comunicação
b) Avaliar riscos da comunicação (sigilo, restrição, insegurança jurídica, etc)
c) Definir público-alvo e instrumentos de comunicação
d) Definir o processo e os instrumentos de comunicação e consulta
e) Submeter o processo, instrumentos e canais ao CGE
f) Divulgar plano de comunicação
PRODUTOS GERADOS
• Plano de comunicação
• Instrumentos de comunicação e consulta*
Consolidar Plano de Comunicação
AVALIAR MATURIDADE EM GRC
a) Formatar plano de avaliação da maturidade: estratégia, escopo, objetivos, critérios, etc.
b) Definir instrumento e canal de consulta
c) Aplicar avaliação com servidores usuários e gestores da Agência
d) Elaborar relatório de maturidade em GRC e comparar ganhos
e) Divulgar resultados e propor plano de progresso
PRODUTOS GERADOS
• Plano de avaliação de maturidade
• Instrumento de avaliação
• Relatório de avaliação realizado
Avaliação da maturidade e lições aprendidas
PLANO DE PROGRESSO EM GRC
a) Implantar melhorias prospectadas ao fluxo do processo
b) Avaliar possibilidade de implementação do modelo simplificado de GRC
c) Atualizar guia de GRC
d) Definir plano de capacitação anual
e) Prospectar plataforma e sistema de GRC (TI)
PRODUTOS GERADOS
• Resultado da avaliação incorporando lições aprendidas
• Guia de GRC atualizado
Método atualizado
(01 Set)
4 semanas
(30 Set)
8 semanas
(30 Out)
12 semanas
(30 Nov)
16 semanas
(Dez 2019)
Definir planos de tratamentos de Projetos-piloto
Aplicar metodologia nos processos priorizados
(01 Set)
18 semanas
(Dez 2018)
96 semanas
(Dez 2020)

futuro

Meta de maturidade

Nível de maturidade CGU (2014)	Apurado
Inicial	De 0% a 20%
Básico	De 20,1% a 40%
Intermediário	De 40,1% a 60%
Aprimorado	De 60,1% a 80%
Avançado	De 80,1% a 100%

Adaptado de M.o.R - 2010

Fabiano Araújo

Cqual@anvisa.gov.br

Coordenação de Qualidade em Processos Organizacionais

Assessoria de Planejamento/Anvisa

ANVISA
Agência Nacional de Vigilância Sanitária

Apresentação 12:

Gestão de Riscos em Projetos

JOSÉ FLÁVIO ALBERNAZ MUNDIM

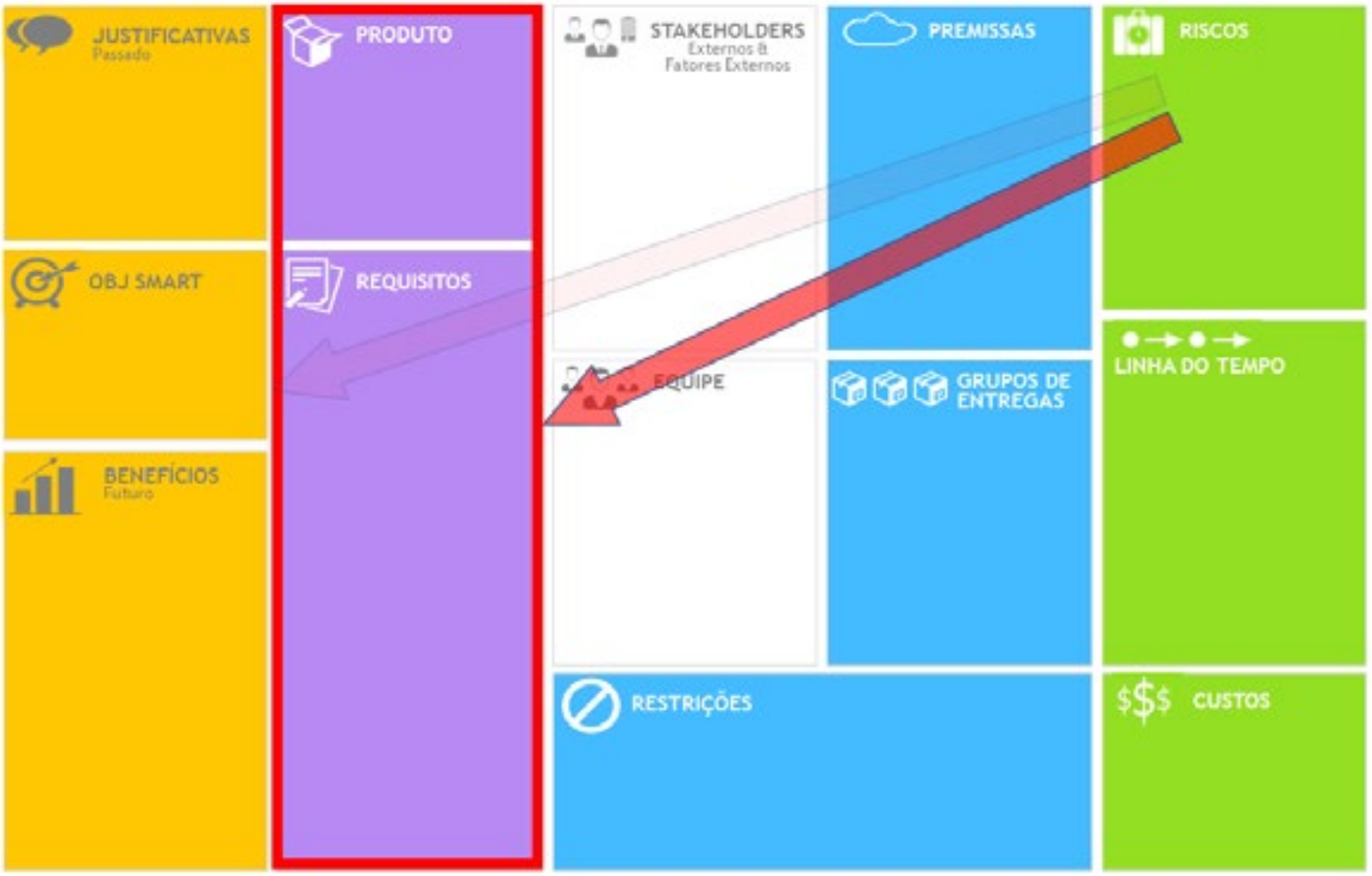

Gestão de Riscos
em
Projetos
Out/2018

Riscos:
tudo o que pode impactar os objetivos do projeto
(e repercutir para a organização)

Onde estão os riscos nos projetos?

Fonte: FINOCCHIO (2013)


JUSTIFICATIVAS
Passado
PRODUTO
STAKEHOLDERS
Externos & Fatores Externos
PREMISSAS
RISCOS
OBJ SMART
REQUISITOS
LINHA DO TEMPO
EQUIPE
GRUPOS DE ENTREGAS
BENEFÍCIOS
Futuro
RESTRIÇÕES
$$$ CUSTOS


JUSTIFICATIVAS
Passado
PRODUTO
STAKEHOLDERS
Externos & Fatores Externos
PREMISSAS
RISCOS
OBJ SMART
REQUISITOS
EQUIPE
GRUPOS DE ENTREGAS
LINHA DO TEMPO
BENEFÍCIOS
Futuro
RESTRIÇÕES
$$$ CUSTOS


JUSTIFICATIVAS
Passado
PRODUTO
STAKEHOLDERS
Externos & Fatores Externos
PREMISSAS
RISCOS
OBJ SMART
REQUISITOS
EQUIPE
GRUPOS DE ENTREGAS
LINHA DO TEMPO
BENEFÍCIOS
Futuro
RESTRIÇÕES
$$$ CUSTOS


JUSTIFICATIVAS
Passado
PRODUTO
STAKEHOLDERS
Externos & Fatores Externos
PREMISSAS
RISCOS
OBJ SMART
REQUISITOS
EQUIPE
GRUPOS DE ENTREGAS
LINHA DO TEMPO
BENEFÍCIOS
Futuro
RESTRIÇÕES
$$$ CUSTOS


JUSTIFICATIVAS
Passado
PRODUTO
STAKEHOLDERS
Externos &
Fatores Externos
PREMISSAS
RISCOS
OBJ SMART
REQUISITOS
EQUIPE
GRUPOS DE
ENTREGAS
A DO TEMPO
BENEFÍCIOS
Futuro
RESTRIÇÕES
$$$ CUSTOS


JUSTIFICATIVAS
Passado
PRODUTO
STAKEHOLDERS
Externos & Fatores Externos
PREMISSAS
RISCOS
OBJ SMART
REQUISITOS
EQUIPE
GRUPOS DE ENTREGAS
LINHA DO TEMPO
BENEFÍCIOS
Futuro
RESTRIÇÕES
$$$ CUSTOS


JUSTIFICATIVAS
Passado
PRODUTO
STAKEHOLDERS
Externos & Fatores Externos
PREMISSAS
RISCOS
OBJ SMART
REQUISITOS
EQUIPE
GRUPOS DE ENTREGAS
LINHA DO TEMPO
BENEFÍCIOS
Futuro
RESTRIÇÕES
$$$ CUSTOS

Há risco em gerenciar riscos??

Política de Gestão de Riscos

TRIBUNAL SUPERIOR DO TRABALHO
PRESIDÊNCIA

ATO Nº 131/ASGE.SEGP.GP, DE 13 DE MARÇO DE 2015.

Dispõe sobre a Política de Gestão de Riscos da Secretaria do Tribunal Superior do Trabalho e dá outras providências.

O **PRESIDENTE DO TRIBUNAL SUPERIOR DO TRABALHO**, no uso de suas atribuições legais e regimentais,

Considerando o Ato ASGE.SEGP.GP.Nº 93, de 25 de fevereiro de 2015, que instituiu o Comitê de Gestão de Riscos da Secretaria do Tribunal Superior do Trabalho;

Considerando que cabe ao Comitê de Gestão de Riscos da Secretaria do Tribunal Superior do Trabalho propor à Presidência do TST a Política de Gestão de Riscos;

Etapas do gerenciamento de riscos

- ✓ Identificar riscos
- ✓ Analisar riscos
- ✓ Planejar as respostas aos riscos
- ✓ Implementar as respostas aos riscos

Etapas do gerenciamento de riscos

- ✓ Identificar riscos
- ✓ Analisar riscos
- ✓ Planejar as respostas aos riscos
- ✓ Implementar as respostas aos riscos

Como vamos trabalhar

- ✓ Conceitos básicos
- ✓ Estudo de caso em grupo
  - ○ Identificar riscos
  - ○ Analisar riscos (análise qualitativa)
  - ○ Planejar as respostas aos riscos
  - ○ Apresentar para o grupão

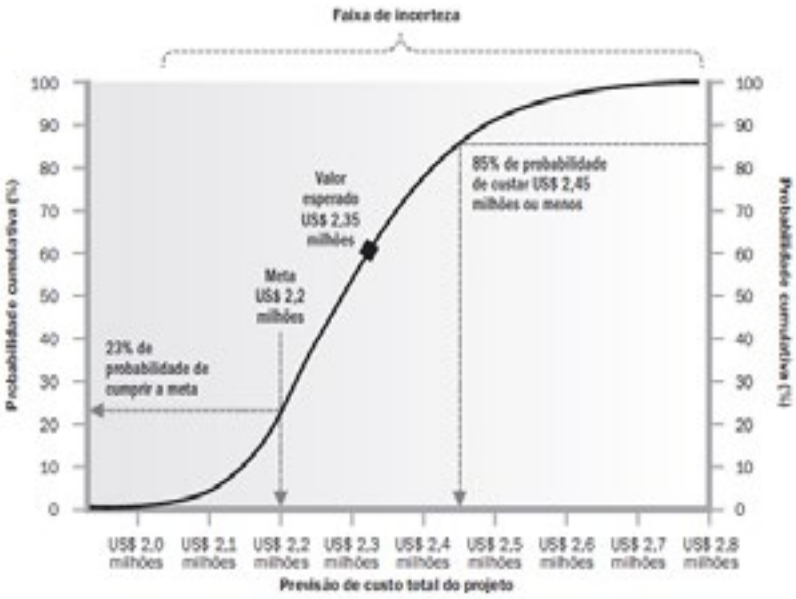
O trabalho em grupo

- ✓ Todos têm conhecimento e experiência
- ✓ É um trabalho de inteligência coletiva
- ✓ A imaginação é muito importante
- ✓ Haverá o momento da produção individual intensa
- ✓ Haverá o momento da organização

Análise Qualitativa

Legenda Nível de Risco Extremo Alto Médio Baixo		Probabilidade				
		1 Muito Baixa	2 Baixa	3 Média	4 Alta	5 Muito Alta
Impacto	5 Muito Alto	5	10	15	20	25
	4 Alto	4	8	12	16	20
	3 Médio	3	6	9	12	15
	2 Baixo	2	4	6	8	10
	1 Muito Baixo	1	2	3	4	5

Análise Quantitativa



MÃO NA MASSA

- ✓ Distribuir os casos de estudo
- ✓ Explicar brevemente cada caso
- ✓ 2’ para rearranjo dos grupos
- ✓ 30” de apresentação individual dentro do grupo
- ✓ Escolher o facilitador

Gr 1: Inovação. Inteligência artificial. Mudança de processos de trabalho.

Gr 2: Reestruturação organizacional. Remanejamento de pessoas. Eficiência.

Gr 3: Uma pousada na praia. Conjuntura do País. Mercado de turismo.

Gr 4: “ENEM”. Logística, prazos fixados, muitas etapas.

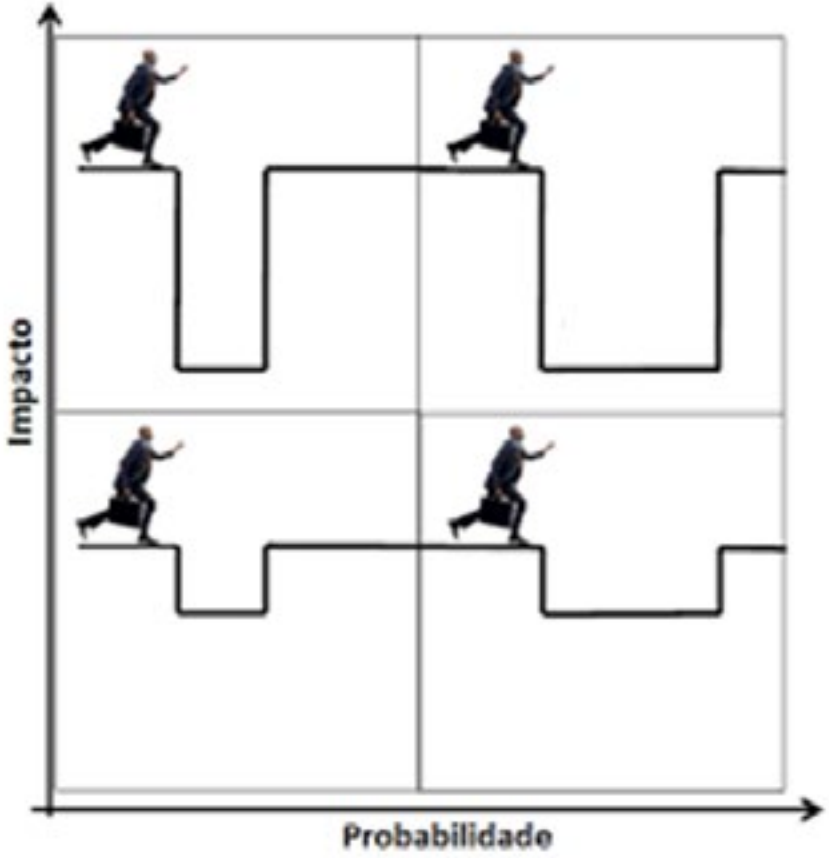
Gr 5: Escritório de projetos. Cultura organizacional. Mudança de processos.

Conceitos básicos

1. Probalidade

2. Impacto

- No escopo
- No prazo
- No custo
- Na qualidade




CONTEXTO (EAR)
EXTERNO
Ambiente Regulatório
Contratos
Desastre
Imagem da Organização
Mercado
Relacionamento com Fornecedores
Relações Institucionais
Ambiente macroeconômico
Infraestrutura Pública
Meio Ambiente
GERENCIAMENTO
Planejamento
Engajamento de Stakeholders
Gerenciamento de Operações
Equipe e Recursos
Comunicação
Mudança
Integração
Gerenciamento de Portfólio e Programas
ORGANIZACIONAL
Patrocínio
Priorização
Alinhamento Estratégico
Resultados Esperados
Cultura Organizacional
Clima Organizacional
Comunicação Institucional
Processos de Trabalho
Conformidade
Interdependências
Orçamento
Segurança Jurídica
Segurança Física
TÉCNICO
Escopo
Domínio da Solução
Integração da Solução
Complexidade
Requisitos
Estimativas, Premissas e Restrições
Obsolescência Tecnológica
Qualidade da Solução
Desempenho da Solução
Documentação
Segurança da Informação

Estudo de caso

- **Identificar riscos**
  - ***Slip de Crawford***
- **Analisar riscos (análise qualitativa)**
- **Planejar as respostas aos riscos**
- **Apresentar para o grupão**

Estudo de caso

- **Identificar riscos**
  - ***Slip de Crawford***
    - Grande volume de riscos em pouco tempo
    - Utiliza um "slip" ou pedaços de papel tipo Post-It®
    - Brainstorming individual e consolidação em grupo

NÃO SE CENSURE!! ESCREVA O QUE VIER À CABEÇA!

✓ **Frases curtas:**

"Ficar sem cliente"
"Roubo das provas"
"Inexperiência da universidade"
"Boicote dos desenvolvedores"
"Resistência dos funcionários"

MÃO NA MASSA

- ✓ Ler e discutir brevemente o caso de estudo
- ✓ Identificar riscos individualmente (1 por post-it)
  (utilize a EAR só se "travar")

Estudo de caso

- **Identificar riscos**
  - *Slip de Crawford*
  - **Categorizar os riscos (EAR)**

MÃO NA MASSA

- ✓ Escrever nível 1 da EAR na folha do flip
- ✓ Categorizar os riscos, eliminando os redundantes
- ✓ Ordenar pela importância (percepção do grupo)

Conceitos básicos: sintaxe do risco

No slip: "Inexperiência da universidade"

SINTAXE:

CAUSA: Inexperiência da universidade

EVENTO: Recisão contratual

EFEITO: Interrupção do projeto

Conceitos básicos: sintaxe do risco

No slip: "Roubo de provas"

SINTAXE:

CAUSA: Falha de segurança física

EVENTO: Roubo de provas

EFEITO: Cancelamento do concurso

Conceitos básicos: sintaxe do risco

No slip: “Boicote dos desenvolvedores”

SINTAXE:

CAUSA: Deficiência de engajamento

EVENTO: Boicote dos desenvolvedores

EFEITO: Atraso no projeto

Conceitos básicos: sintaxe do risco

No slip: "Ficar sem cliente"

SINTAXE:

CAUSA: Crise econômica

EVENTO: Baixa taxa de ocupação da pousada

EFEITO: Aumento do prazo de retorno do projeto

MÃO NA MASSA

- ✓ Reescrever os riscos usando a sintaxe correta (para o primeiro risco de cada categoria nível 1)
- ✓ Escrever 1 risco por folha A3

Estudo de caso

- Identificar riscos
- **Analisar riscos (análise qualitativa)**
- Planejar as respostas aos riscos
- Apresentar para o grupão

Estudo de caso

- Identificar riscos
- **Analisar riscos (análise qualitativa)**
  - **Atribuir probabilidade e impacto ao risco**
  - **Calcular o nível do risco (prob. X imp.)**
  - Posicionar o risco na matriz de Imp. e Prob.
- Planejar as respostas aos riscos
- Apresentar para o grupão

Nível do Risco = Probabilidade x Impacto

Prob. => CAUSA: Deficiência de engajamento
EVENTO: Boicote dos desenvolvedores

Imp. => EFEITO: Atraso no projeto

Probabilidade = **Alta => 4** **Impacto** = **Alto => 4**

Nível do Risco = **4 x 4 = 16** (Matriz => **Risco Extremo**)

MÃO NA MASSA

- ✓ Atribuir grau de probabilidade e grau de impacto para cada um dos 4 riscos
- ✓ Calcular o nível de risco = probabilidade X impacto

Estudo de caso

- Identificar riscos
- **Analisar riscos (análise qualitativa)**
  - Atribuir probabilidade e impacto ao risco
  - Calcular o nível do risco (prob. X imp.)
  - **Posicionar o risco na matriz de Imp. e Prob.**
- Planejar as respostas aos riscos
- Apresentar para o grupão

Conceitos básicos:

Matriz Impacto e Probabilidade

Legenda Nível de Risco Extremo Alto Médio Baixo		Probabilidade				
		1 Muito Baixa	2 Baixa	3 Média	4 Alta	5 Muito Alta
Impacto	5 Muito Alto	5	10	15	20	25
	4 Alto	4	8	12	16	20
	3 Médio	3	6	9	12	15
	2 Baixo	2	4	6	8	10
	1 Muito Baixo	1	2	3	4	5

MÃO NA MASSA

- ✓ Numerar os riscos e posicionar cada um na Matriz de Impacto e Probabilidade

Estudo de caso

- Identificar riscos
- Analisar riscos (análise qualitativa)
- **Planejar as respostas aos riscos**
- Apresentar para o grupão

Política de Gestão de Riscos

Tabela 9 – Diretrizes para Priorização do Tratamento de Riscos

Nível de Risco	Descrição	Diretriz para Resposta
Extremo	Indica um nível de risco absolutamente inaceitável, muito além do apetite a risco da organização.	Qualquer risco encontrado nessa área deve ter uma resposta imediata. Admite-se postergar o tratamento somente mediante parecer do Secretário da Unidade, ou cargo equivalente.
Alto	Indica um nível de risco inaceitável, além do apetite a risco da organização.	Qualquer risco encontrado nessa área deve ter uma resposta em um intervalo de tempo definido pelo Secretário da Unidade, ou cargo equivalente. Admite-se postergar o tratamento somente mediante parecer do Secretário da Unidade, ou cargo equivalente.
Médio	Indica um nível de risco aceitável, dentro do apetite a risco da organização.	Não se faz necessário adotar medidas especiais de tratamento, exceto manter os controles já existentes.
Baixo	Indica um nível de risco muito baixo, onde há possíveis oportunidades de maior retorno que podem ser exploradas.	Explorar as oportunidades, se determinado pelo Secretário da Unidade, ou cargo equivalente.

Conceitos básicos: estratégias de resposta

1. Escalar: p/ níveis mais altos
2. Prevenir: eliminar o risco (prob. = 0)
3. Transferir: seguros, garantias, cauções
4. Mitigar: reduzir probab. e/ou impacto
5. Aceitar: p/ risco baixo (reserva de contingência)

Estratégia de resposta ao risco: mitigar

CAUSA: Deficiência de engajamento

EVENTO: Boicote dos desenvolvedores

EFEITO: Atraso no projeto

Probabilidade = **Alta => 4** **Impacto** = **Muito Alto => 4**

Nível do Risco = **4 x 4 = 16** (Matriz => **Risco Extremo**)

Resposta: Incorporar métodos ágeis na metodologia do EGP

MÃO NA MASSA

- ✓ Indicar a estratégia de resposta para cada risco das faixas Extremo e Alto
- ✓ Desenvolver 1 resposta para cada um desses riscos

MÃO NA MASSA

APRESENTAÇÕES!!!!

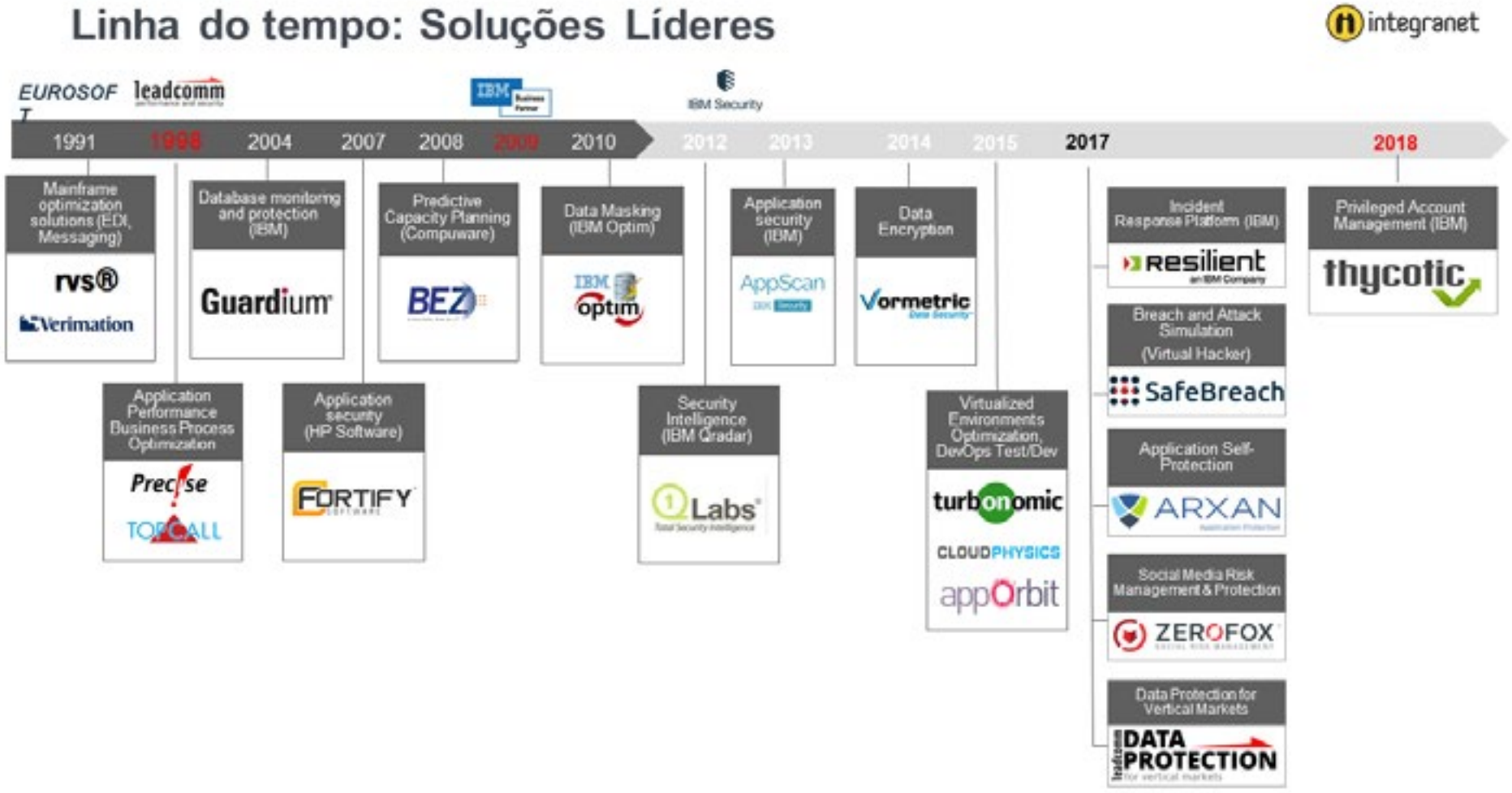
Apresentação 13:

Data Protection for Vertical Markets

EDSON CARLOTTI


integranet
leadcomm
performance and security
Data Protection for Vertical Markets
THE MANAGED AS-A-SERVICE SOLUTION FOR SENSITIVE DATA PROTECTION DESIGNED BY LEADCOMM
Edson Carlotti
CTO - LEADCOMM
Q4/2018

Linha do tempo: Soluções Líderes



O que é o DPVM?

LEADCOMM Data Protection for Vertical Markets

integranet

É uma solução de segurança gerenciada para detectar, proteger e auditar a má utilização e o abuso de dados sensíveis, especialmente desenhada para mercados verticais.

Powered by IBM Security Guardium

leadcomm DATA PROTECTION for vertical markets


integranet
leadcomm
performance and security
DPVM - LGPD
Lei Geral de Proteção de Dados (Lei 13.709/2018)
LEADCOMM DATA PROTECTION FOR VERTICAL MARKETS
Edson Carlotti
CTO - LEADCOMM
Q4/2018

integranet

Sobre a LGPD (Lei 13.709/2018)

- **Sancionada em 14/08/2018**
- **Conteúdo:**
  - Estabelecimento regras claras sobre coleta, armazenamento, tratamento e compartilhamento de dados pessoais
  - Impõe penalidades significativas para o não cumprimento da norma

Conheça os 12 principais pontos sobre a LGPD (Lei 13.709/2018)

integranet

1 – Escopo de Aplicação – Art. 1º
Afeta qualquer atividade que envolva utilização de dados pessoais, incluindo o tratamento pela internet, de consumidores, empregados, entre outros

2 – Aplicação Extraterritorial – Art. 3º
Aplica-se também a empresas que não possuem estabelecimento no Brasil

3 – Princípios de Proteção de Dados – Art. 6º
Introduzidos 10 princípios de proteção dos dados, incluindo-se o de demonstrar medidas adotadas para o cumprimento da lei (prestação de contas)

4 – Autorização para o Tratamento de Dados – Art. 7º
O consentimento será uma das 10 possibilidades que legitimarão o tratamento de dados pessoais

5 – Autoridade – VETADO
Previsão da Autoridade Nacional de Proteção de Dados, responsável por garantir o cumprimento da Lei – (Aguardando PL ou MP)

6 – DADOS: Sensíveis, de Menores e Transf. Internacional – Art. 11, 14 e 33
Regras específicas para tratar dados sensíveis, transferência internacional de dados e utilizar dados de crianças e adolescentes

7 – Direitos dos Titulares de Dados – Art. 17 a 22
Titulares de dados terão amplos direitos: informação, acesso, retificação, cancelamento, oposição e portabilidade, entre outros

8 – Mapeamento do Tratamento de Dados – Art. 37
Atividades de tratamento de dados devem ser registradas em relatório

9 – Assessment Sobre o Tratamento de Dados – Art. 38
Necessidade de realizer assessment de impacto à proteção de dados (semelhante ao DPIA)

10 – Data Protection Officer (DPO) – Art. 41
Toda empresa responsável por tratamento de dados deverá nomear Encarregado da Proteção de Dados Pessoais

11 – Notificações Obrigatórias – Art. 48
Em caso de incidents de segurança envolvendo os dados, nas situações aplicáveis

12 – SANÇÕES
Multa de até 50 milhões de Reais por infração, entre outras sanções

Fonte: Opice Blum Advogados

leadcomm

integranet

Como o DPVM atende aos requisitos da LGPD

DPVM | LGPD

integranet

Reduzir a vulnerabilidade a incidentes de segurança

- Mais de mil testes específicos para SGBD baseados em padrões da indústria (CVE, CIS, STIG)
  - Detecta situações de risco como uso de senhas padrão, patches não instalados, privilégios excessivos e uso de práticas não recomendadas de configuração do SGBD
  - Permite rastrear e opcionalmente bloquear alterações de configuração do SGBD

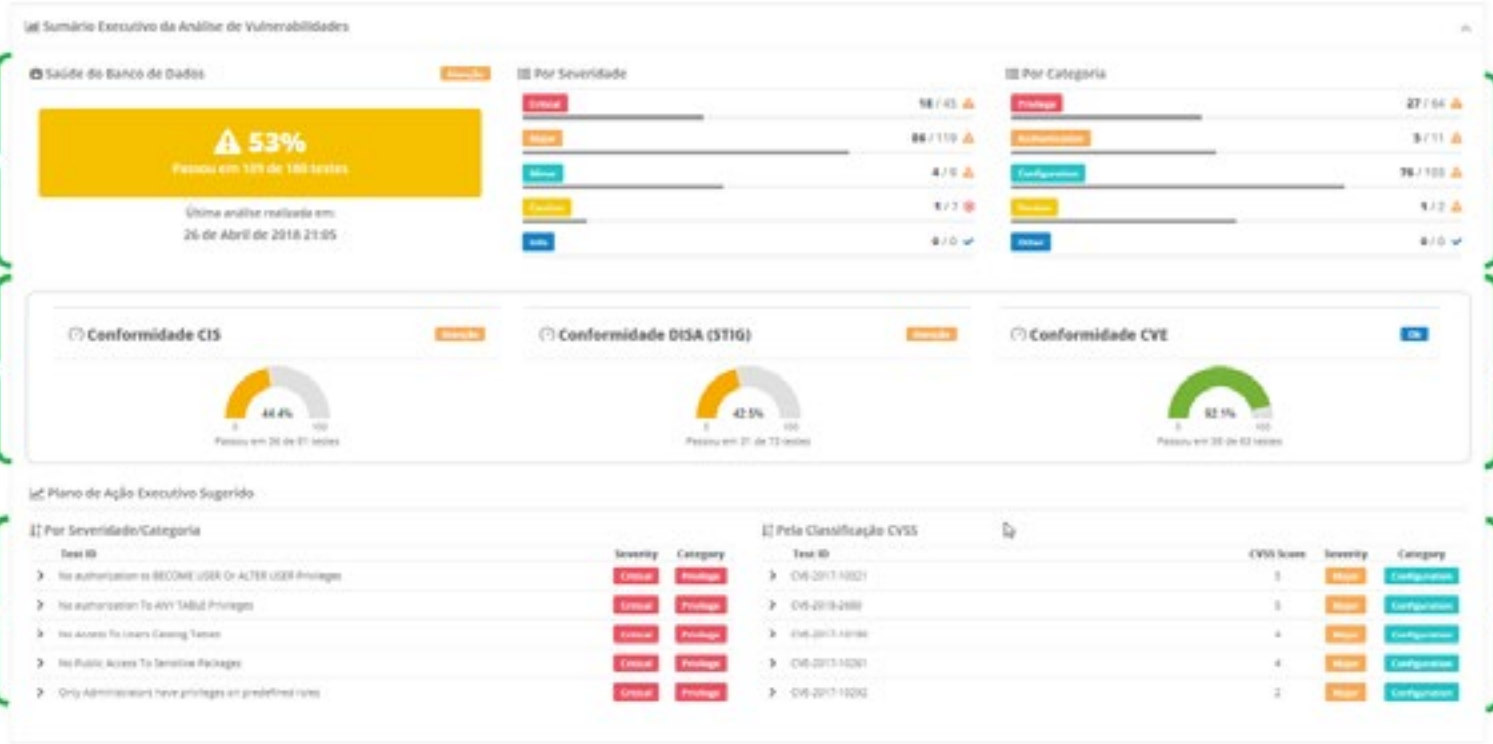
Reduzir a vulnerabilidade a incidentes de segurança

integranet

Resumo de Resultados

Análise de Conformidade

Principais problemas por severidade ou categoria



Resumo por Severidade e Categoria

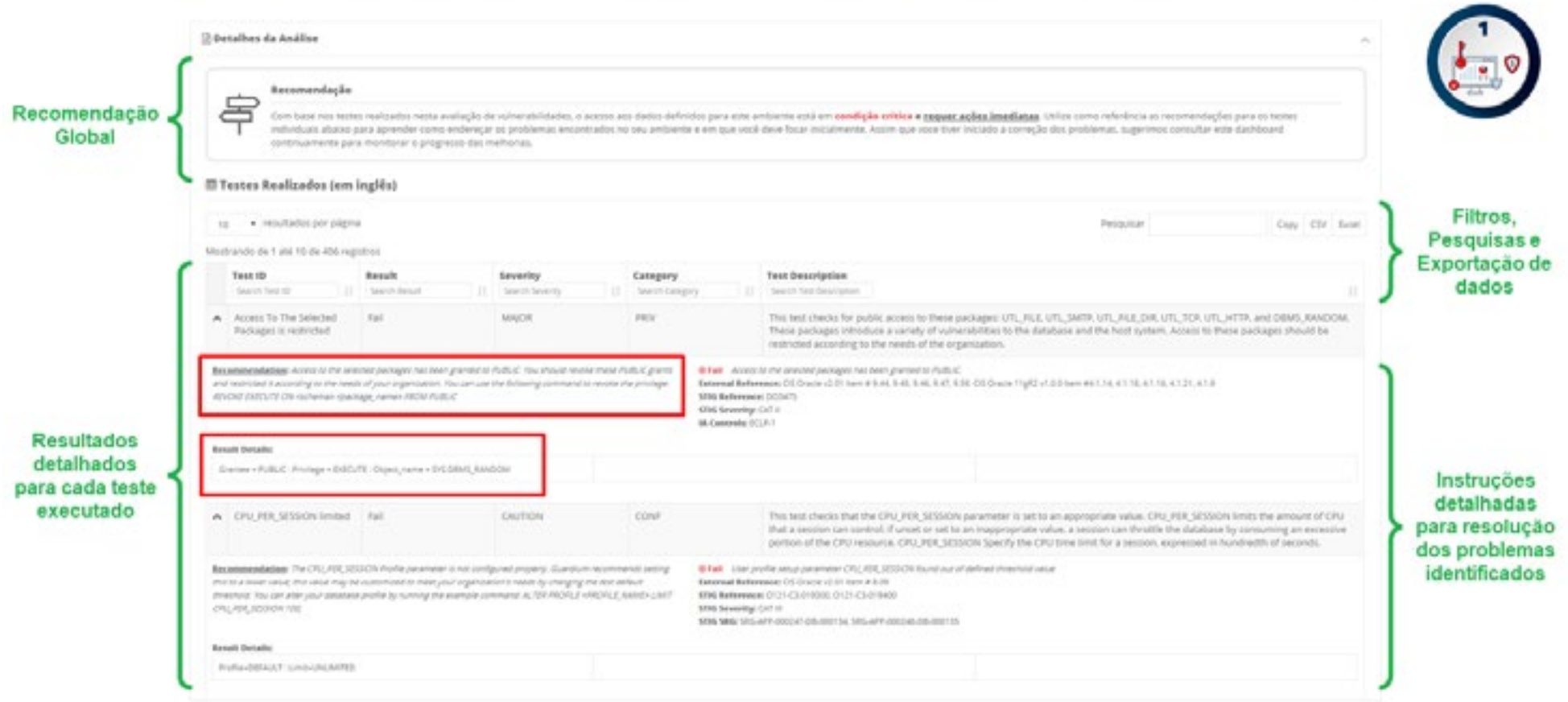
Utiliza padrões da Indústria CVE,STIG,CIS

Principais problemas por indice CVSS

leadcomm

integranet

Reduzir a vulnerabilidade a incidentes de segurança

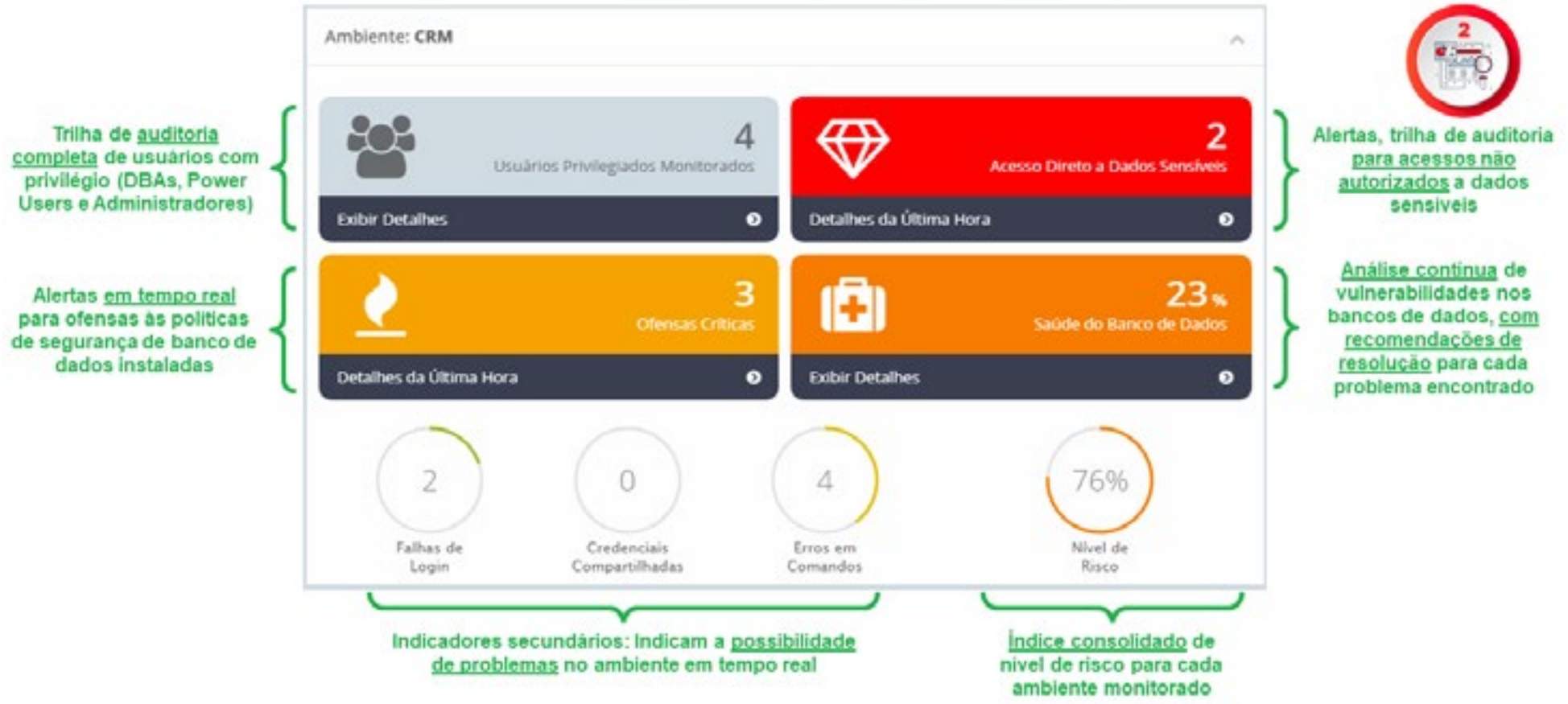


leadcomm

Controles específicos para rastreabilidade e garantia da segurança de dados sensíveis

- Monitoração de acesso aos dados **em tempo real**
  - Monitora, em tempo real, todo acesso ao SGBD independente do meio de acesso e do usuário, inclusive usuários privilegiados, administradores e DBAs
  - Monitora tráfego criptografado (Oracle, MSSQL, DB2, e outros) sem necessitar das chaves de criptografia
  - Gera alertas em tempo real para acessos indevidos
  - Permite criptografar os dados armazenados no SGBD e no Sistema Operacional (*Requer módulo opcional)

Controles Específicos: Garantia da Segurança dos Dados Sensíveis



Controles Específicos: Garantia da Segurança dos Dados Sensíveis

integranet

Alertas

Indicadores secundários: Indicam a possibilidade de problemas no ambiente em tempo real

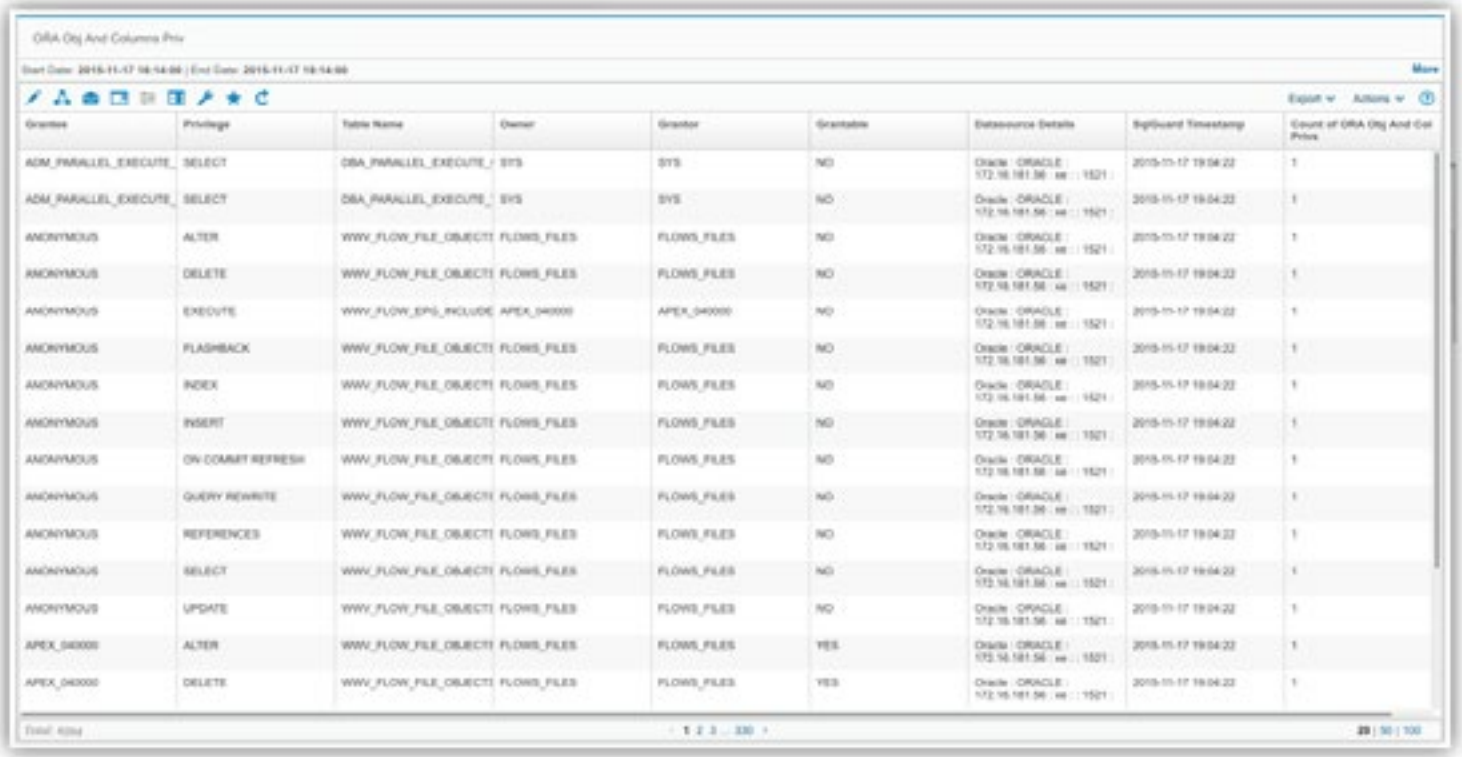
Alertas em tempo real para violações dos indicadores de segurança secundários:

1. **Falhas de Login:** Pode ser indicação de ataque do tipo "força bruta" ao banco de dados;
2. **Credenciais Compartilhadas:** Podem indicar acesso utilizando credenciais roubadas (personificação), que é um dos principais vetores de ataque para roubo de informações;
3. **Erros em Comandos:** Pode indicar que existe um ataque em andamento, sendo executado por alguém (ou algum software) sem conhecimento prévio do modelo de dados da aplicação;

Controles Específicos: Garantia da Segurança dos Dados Sensíveis

integranet

Descoberta de Privilégios



leadcomm

integranet

Controles Específicos: Rastreabilidade da Informação

Data/Hora

Comando SQL executado

sucesso / falha

Detalhamento das Atividades

Data/Hora	Usuário (SO)	Usuário (BD)	SQL Completo	IP do Servidor	IP do Cliente	Sucesso	Nome do Serviço	Programa Utilizado
29/08/2017 03:00:08	TOMCAT	SYSTEM	ALTER SESSION SET NLS_TIMESTAMP_FORMAT = 'YYYY-MM-DD HH24:MI:SS.FF' NLS_TIMESTAMP_TZ_FORMAT = 'YYYY-MM-DD HH24:MI:SS.FF TZH:TZM'	172.16.1.53	172.16.1.211	1	XE	COM.IBM.GUARDIUM.JDBC.ORACLEBASE.DDAK
29/08/2017 03:00:08	TOMCAT	SYSTEM	select USER from DUAL	172.16.1.53	172.16.1.211	1	XE	COM.IBM.GUARDIUM.JDBC.ORACLEBASE.DDAK
29/08/2017 03:00:08	TOMCAT	SYSTEM	select TZ_OFFSET(DBTIMEZONE) from dual	172.16.1.53	172.16.1.211	1	XE	COM.IBM.GUARDIUM.JDBC.ORACLEBASE.DDAK
29/08/2017 03:00:08	TOMCAT	SYSTEM	SELECT PROPERTY_VALUE FROM DATABASE_PROPERTIES WHERE PROPERTY_NAME = 'DEFAULT_EDITION'	172.16.1.53	172.16.1.211	1	XE	COM.IBM.GUARDIUM.JDBC.ORACLEBASE.DDAK
29/08/2017 03:00:08	TOMCAT	JOHN	SELECT DISTINCT 'Grantee = ' || GRANTEE || ' ' || Privilege = ' || PRIVILEGE || ' ' || Object = ' || OWNER || '.' || TABLE_NAME FROM DBA_TAB_PRIVS WHERE TABLE_NAME LIKE 'DBA_%' AND GRANTEE NOT IN ('GDAMONITOR','GDAMONITOR','APPQOSSYS','AQ_ADMINISTRATOR_ROLE','CTXSYS','EXFSYS','MDSYS', 'OLAP_XS_ADMIN','OLAPSYS','ORDSYS','OWBSYS_AUDIT','OWBSYS','SELECT_CATALOG_ROLE', 'WM_ADMIN_ROLE','WMSYS','XDBADMIN','ADM_PARALLEL_EXECUTE_TASK','GDMADMIN_INTERNAL', 'DVSYS','DV_SECANALYST','AUDIT_ADMIN','LBACSYS','AUDIT_VIEWER','CAPTURE_ADMIN','SYSMV', 'DV_MONITOR','AUDIT_VIEWER','XDB','SYSDG','DV_ACCTMGR','SYS','SYSTEM','DBA') AND TABLE_NAME NOT IN ('DBA_SDO_MAPS','DBA_SDO_STYLES','DBA_SDO_THEMES') AND GRANTEE NOT LIKE 'APEX_%' AND NOT EXISTS (SELECT GRANTEE FROM DBA_ROLE_PRIVS RP WHERE DBA_TAB_PRIVS.GRANTEE = RP.GRANTEE AND RP.GRANTED_ROLE IN ('DBA','DBM_MONITOR','GDMADMINTOP')	172.16.1.53	172.16.1.211	1	XE	COM.IBM.GUARDIUM.JDBC.ORACLEBASE.DDAK
29/08/2017 03:00:09	TOMCAT	SYSTEM	BEGIN DBMS_SESSION.SET_IDENTIFIER ('com.ibm.guardium.jdbc.oraclebase.ddak'); END;	172.16.1.53	172.16.1.211	1	XE	COM.IBM.GUARDIUM.JDBC.ORACLEBASE.DDAK
29/08/2017 03:00:09	TOMCAT	SYSTEM	BEGIN DBMS_APPLICATION_INFO.SET_MODULE ('com.ibm.guardium.jdbc.oraclebase.ddak', ''); END;	172.16.1.53	172.16.1.211	1	XE	COM.IBM.GUARDIUM.JDBC.ORACLEBASE.DDAK
29/08/2017 03:00:09	TOMCAT	SYSTEM	SELECT TO_CHAR(NLS_CHARSET_ID('NCHAR_CS')) from dual	172.16.1.53	172.16.1.211	1	XE	COM.IBM.GUARDIUM.JDBC.ORACLEBASE.DDAK
29/08/2017 03:00:09	TOMCAT	SYSTEM	ALTER SESSION SET TIME_ZONE = '-3:0'	172.16.1.53	172.16.1.211	1	XE	COM.IBM.GUARDIUM.JDBC.ORACLEBASE.DDAK
29/08/2017 03:00:09	TOMCAT	SYSTEM	ALTER SESSION SET NLS_TIMESTAMP_FORMAT = 'YYYY-MM-DD HH24:MI:SS.FF' NLS_TIMESTAMP_TZ_FORMAT = 'YYYY-MM-DD HH24:MI:SS.FF TZH:TZM'	172.16.1.53	172.16.1.211	1	XE	COM.IBM.GUARDIUM.JDBC.ORACLEBASE.DDAK

Usuários do Sistema Operacional e do Banco de Dados

Endereços do SERVIDOR e do CLIENTE

Identificação da instância / serviço e do software utilizado

leadcomm

Capacidade de prevenir, detectar e reduzir a vulnerabilidade a incidentes cibernéticos

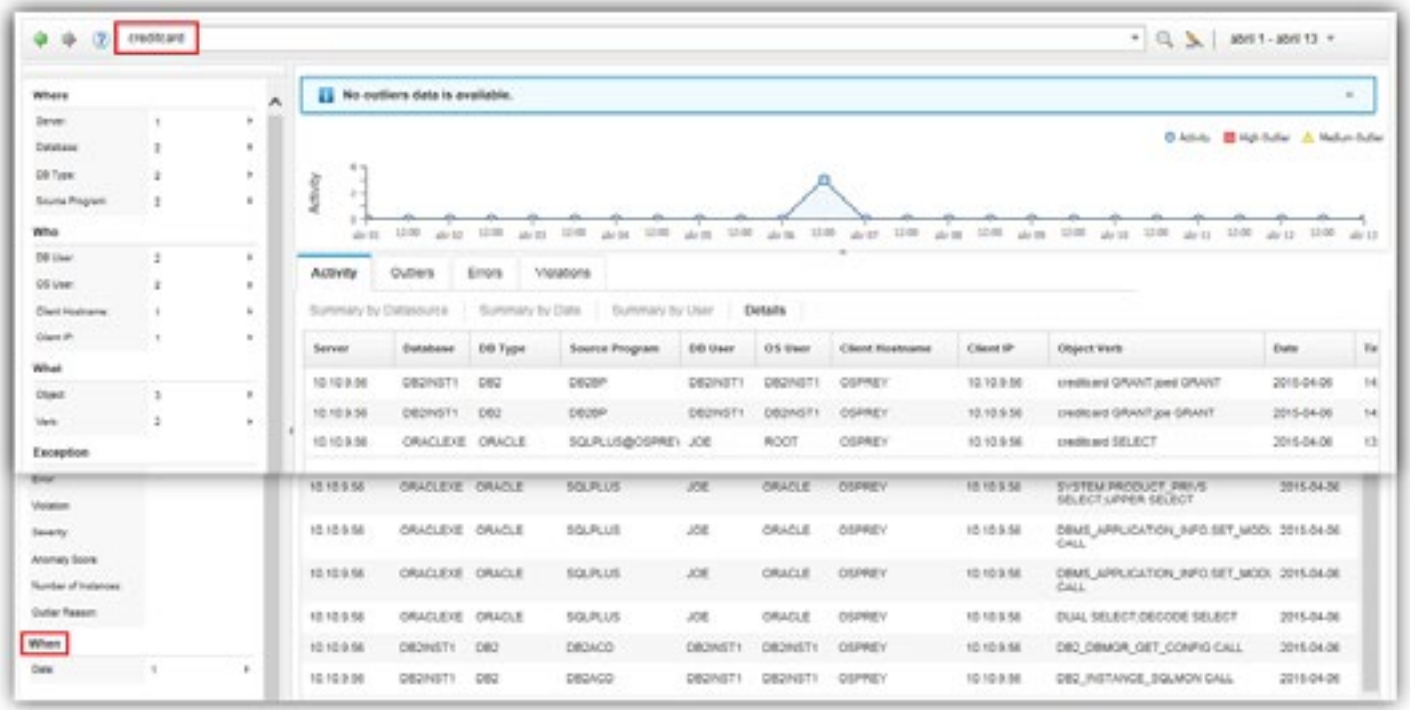
integranet

- A monitoração de atividade dos bancos de dados cria uma trilha de auditoria completa e inteligente, com recursos sofisticados de pesquisa
  - Pesquisa de atividades em qualquer banco de dados, objeto, usuário, faixa de tempo, meio de acesso e outros parâmetros
  - Machine Learning: Identificação automática de atividades fora do padrão normal
  - Identificação e classificação automática de possíveis ataques à bancos de dados, com alertas em tempo real
  - Permite a criação de relatórios e dashboards personalizados

integranet

Capacidade de prevenir, detectar e reduzir a vulnerabilidade a incidentes cibernéticos

Enterprise Search



integranet

Capacidade de prevenir, detectar e reduzir a vulnerabilidade a incidentes cibernéticos

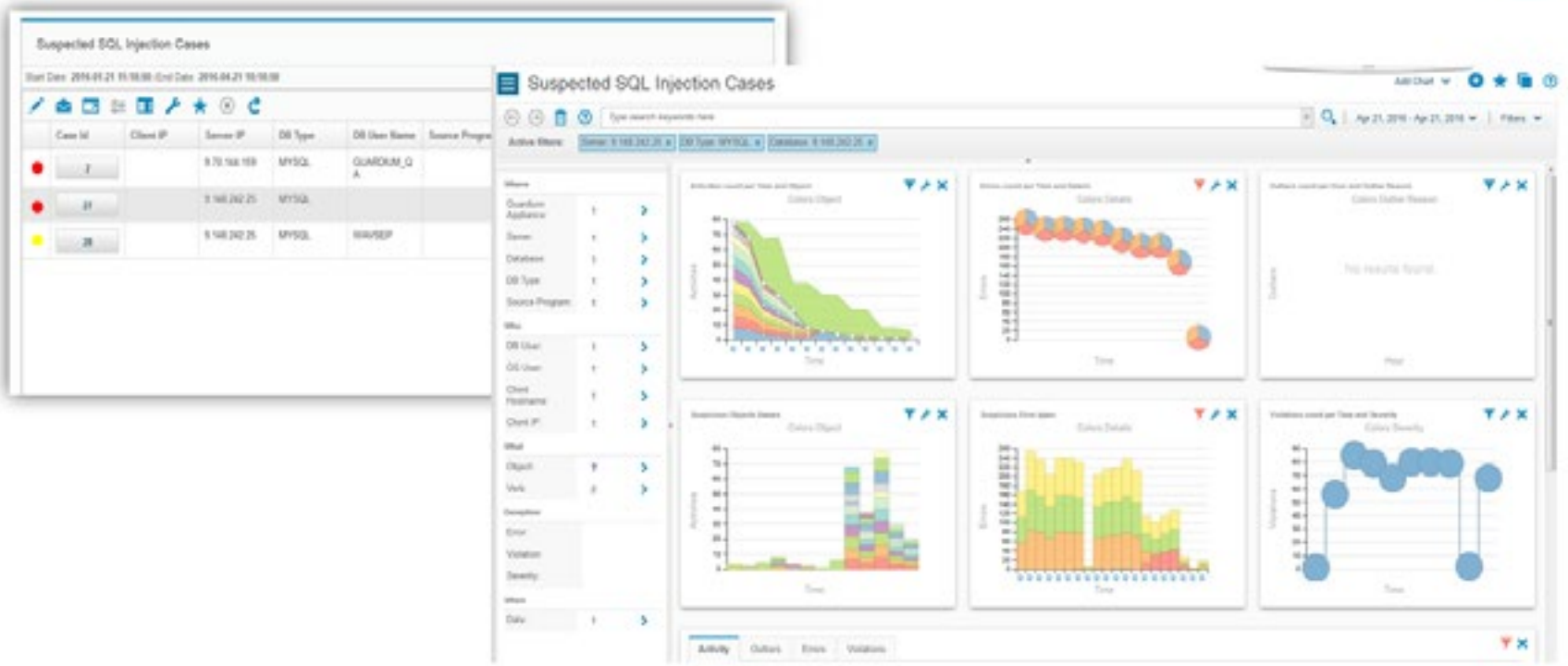
Outliers Detection

leadcomm

integranet

Capacidade de prevenir, detectar e reduzir a vulnerabilidade a incidentes cibernéticos

Threat Diagnostics Center

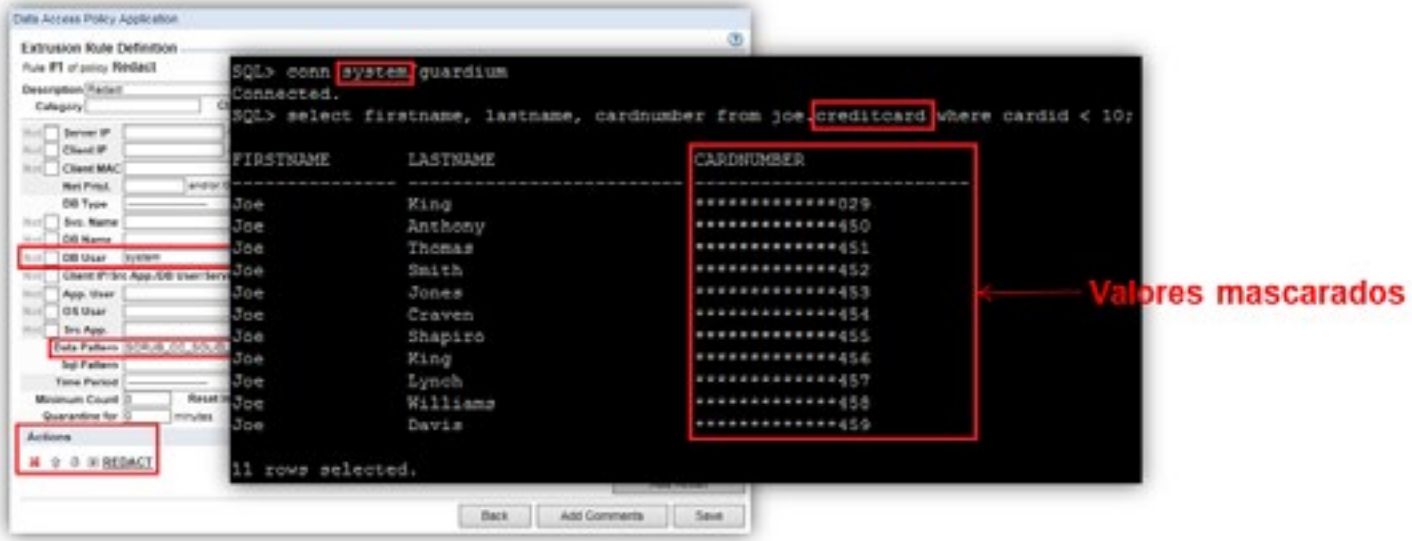


Controles específicos: Prevenção de vazamento de informações

- Controles proativos, em tempo real (independente de controles nativos do SGBD)
  - Políticas definidas pelo IP ou aplicativo origem, usuário do BD ou do SO, hora, comando SQL, objeto, etc.
  - Bloqueio de usuários não autorizados, incluindo administradores, a informações sensíveis
  - Relatórios de direitos de acesso para coletar e entender os direitos concedidos aos usuários nos SGBDs

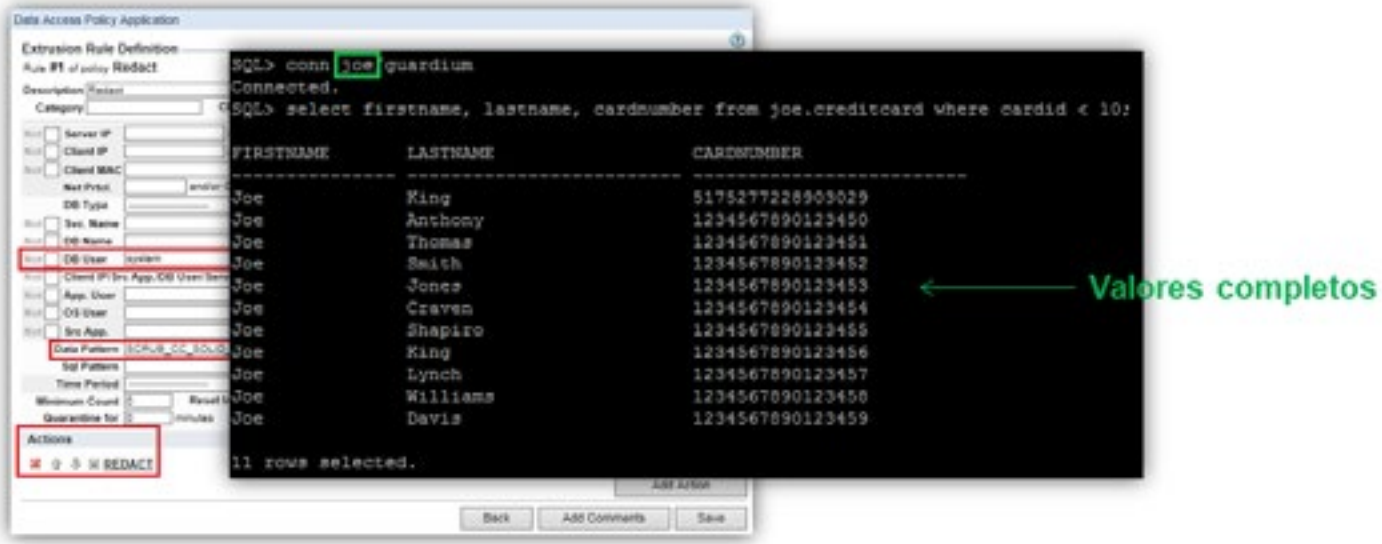
Controles específicos: Prevenção de vazamento de informações

Mascaramento



Controles específicos: Prevenção de vazamento de informações

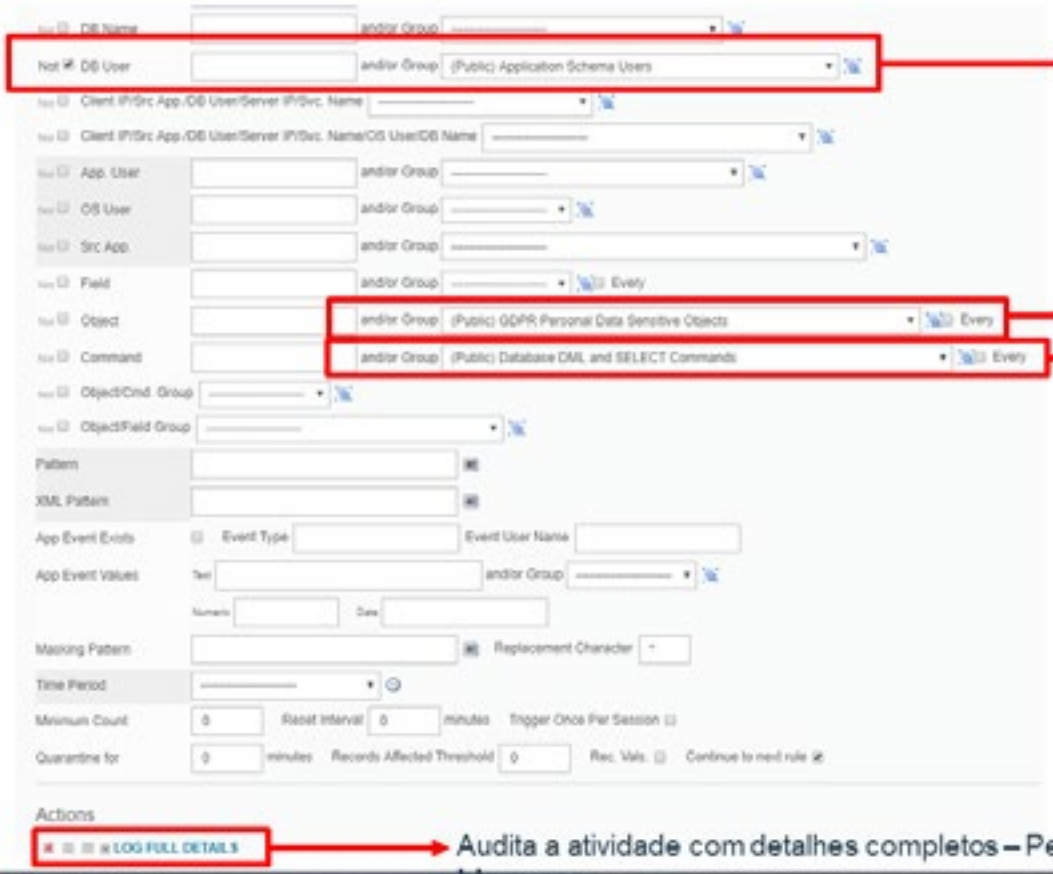
Mascaramento



integranet

Controles específicos: Prevenção de vazamento de informações

Regras para acesso a dados sensíveis



Não é um usuário autorizado para esta aplicação

Está acessando objetos sensíveis

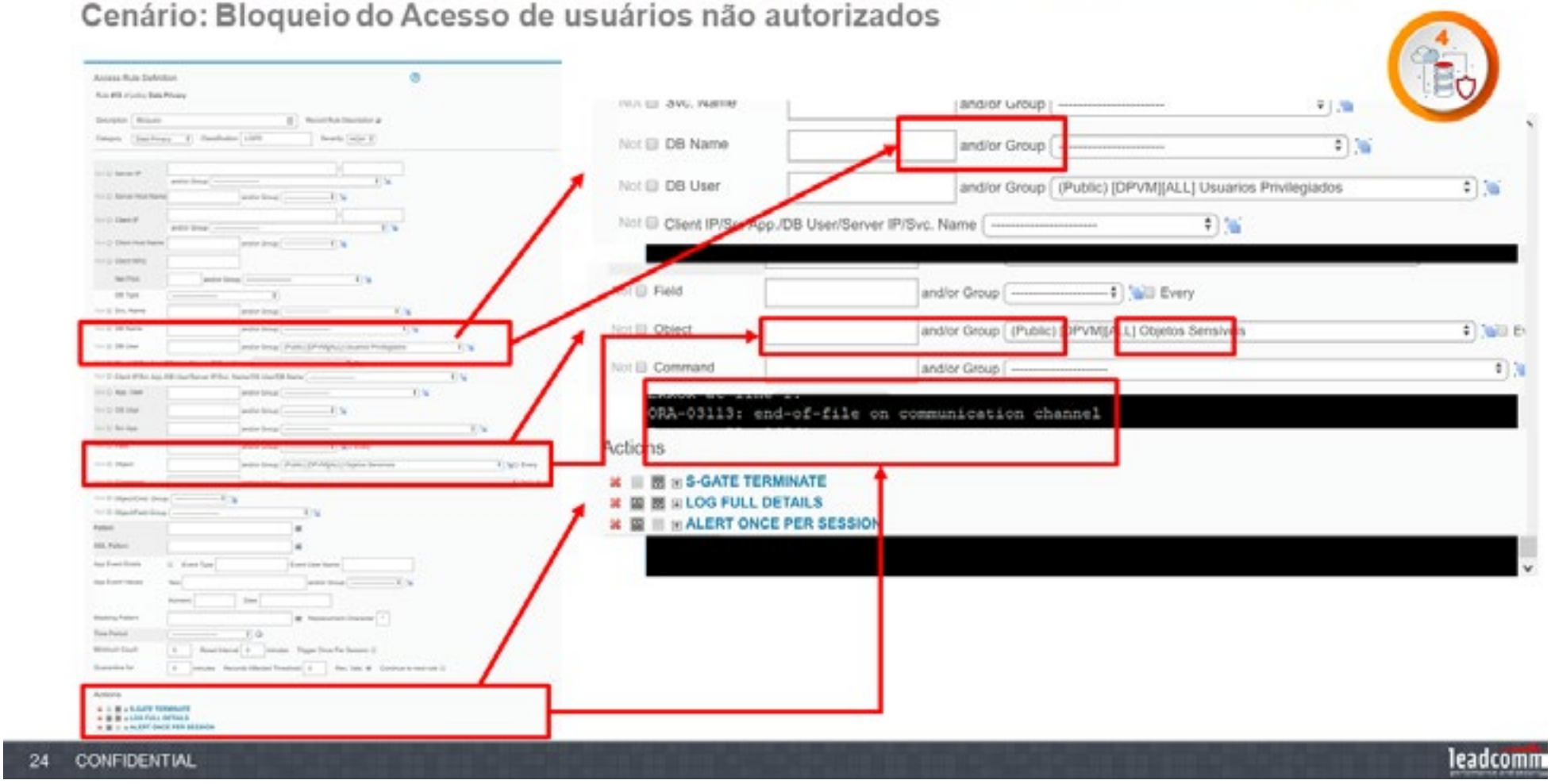
Fazendo consulta ou alteração

Audita a atividade com detalhes completos – Permite também bloquear

integranet

Controles específicos: Prevenção de vazamento de informações

Cenário: Bloqueio do Acesso de usuários não autorizados



leadcomm

Descobrir e classificar dados sensíveis em bancos de dados

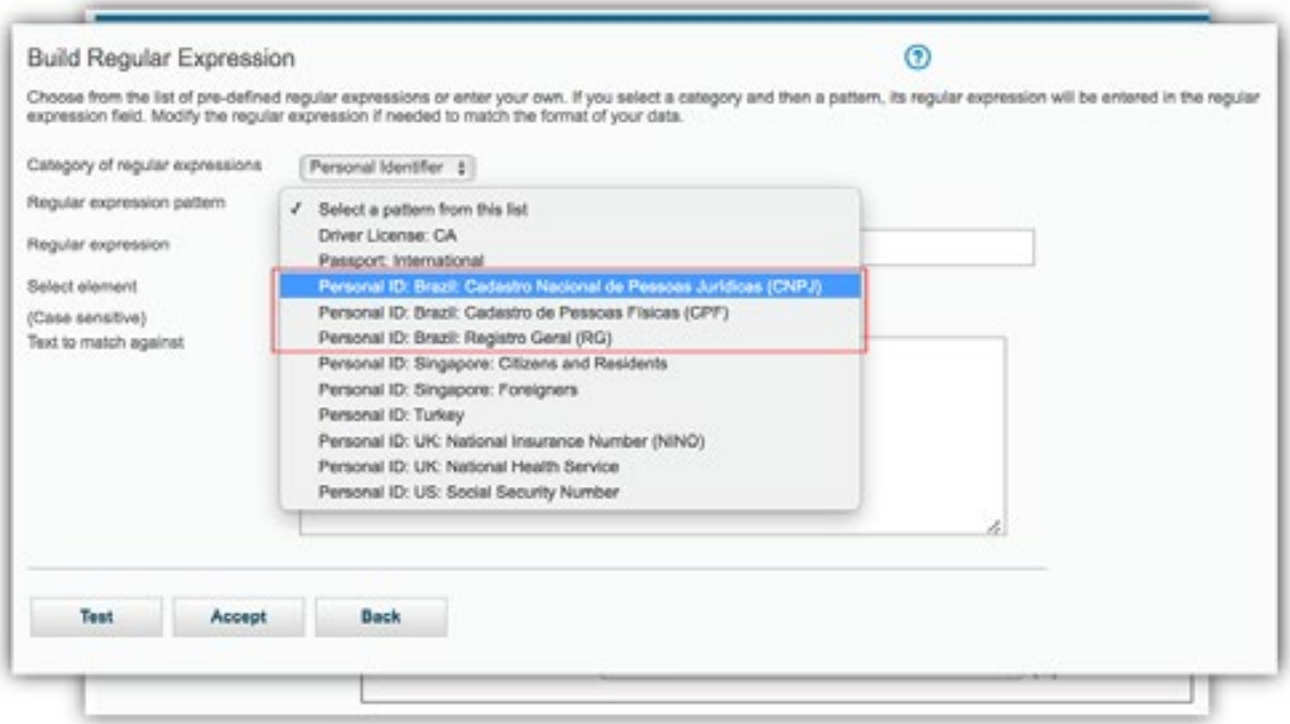
integranet

- Permite a descoberta e classificação automatizada de dados sensíveis armazenados em bancos de dados, através da análise seletiva dos dados utilizando:
  - NLP (Natural Language Processing / Machine Learning)
  - Expressões Regulares
  - Dicionários de dados personalizados
  - Algoritmos de validação especificos (CPF, CNPJ, RG)
- Capaz de identificar:
  - Nomes
  - Endereços
  - Valores
  - Locais
  - Religiões
  - Partidos Politicos
  - Sexo

Descobrir e classificar dados sensíveis em bancos de dados

integranet

- Classificação de dados



LEADCOMM DATA PROTECTION for Vertical Markets

integranet

Central de Gerenciamento LEADCOMM

VPN

- ✓ Verificação [illegible]de do ambiente e correções contínuas;
- ✓ Alertas em tempo real para problemas críticos
- ✓ Ações de manutenção preventivas
- ✓ Recomendações de atualização para as políticas de monitoração;

HIGHLIGHTS da Solução

NÃO HÁ NECESSIDADE DE INVESTIMENTOS EM:

- INFRAESTRUTURA
- RECURSOS HUMANOS
- HARDWARE E SOFTWARE

integranet

Bancos de Dados Suportados

leadcomm

Modelo de Contratação

integranet

Planos Disponíveis

BASIC

- Serviços gerenciados
- Instalação Standard
- Suporte 8x5
- Dashboard de Proteção de Dados
- Saúde do banco de dados
- Recurso avançado de visualização de relatórios
- Treinamento para o usuário
- Apenas relatórios padrão disponíveis

STANDARD

- Serviços gerenciados
- Instalação Standard
- Suporte 8x5
- Dashboard de Proteção de Dados
- Saúde do banco de dados
- Recurso avançado de visualização de relatórios
- Treinamento para o usuário
- 10 relatórios customizados
- 8 horas de consultoria/mês

PREMIUM

- Serviços gerenciados
- Instalação Standard
- Suporte 24x7
- Dashboard de Proteção de Dados
- Saúde do banco de dados
- Recurso avançado de visualização de relatórios
- Treinamento para o usuário
- 20 relatórios customizados
- 24 horas de consultoria/mês

OBRIGADO!

Edson Carlotti
edson@leadcomm.com.br

ENTRE EM CONTATO CONOSCO:

leadcomm.com.br/dpvm
contato@leadcomm.com.br
+55 (11) 5505-0505

SIGA NOSSAS REDES SOCIAIS:

@leadcomm
linkedin.com/company/leadcomm-performance-&-security/

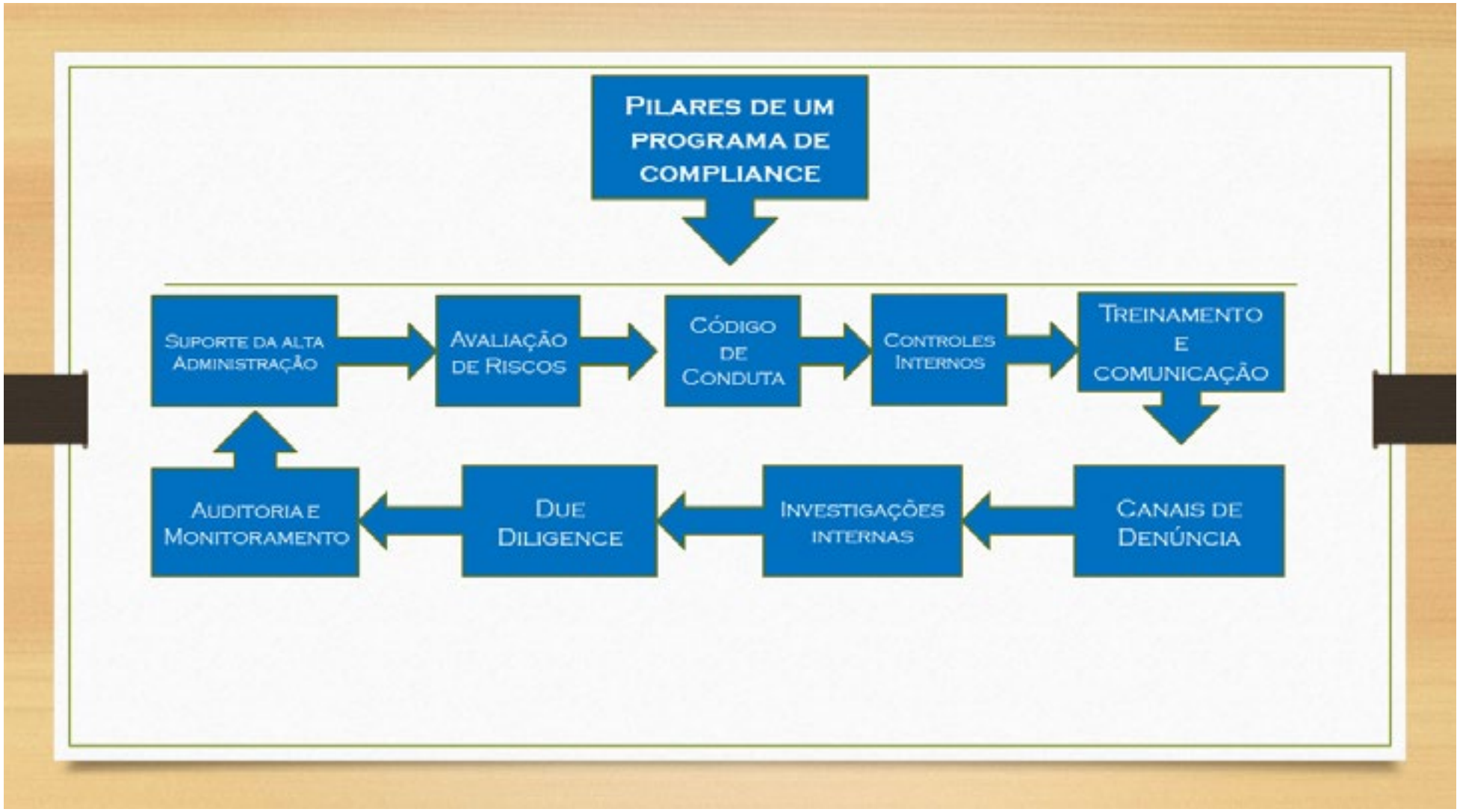
Apresentação 14:

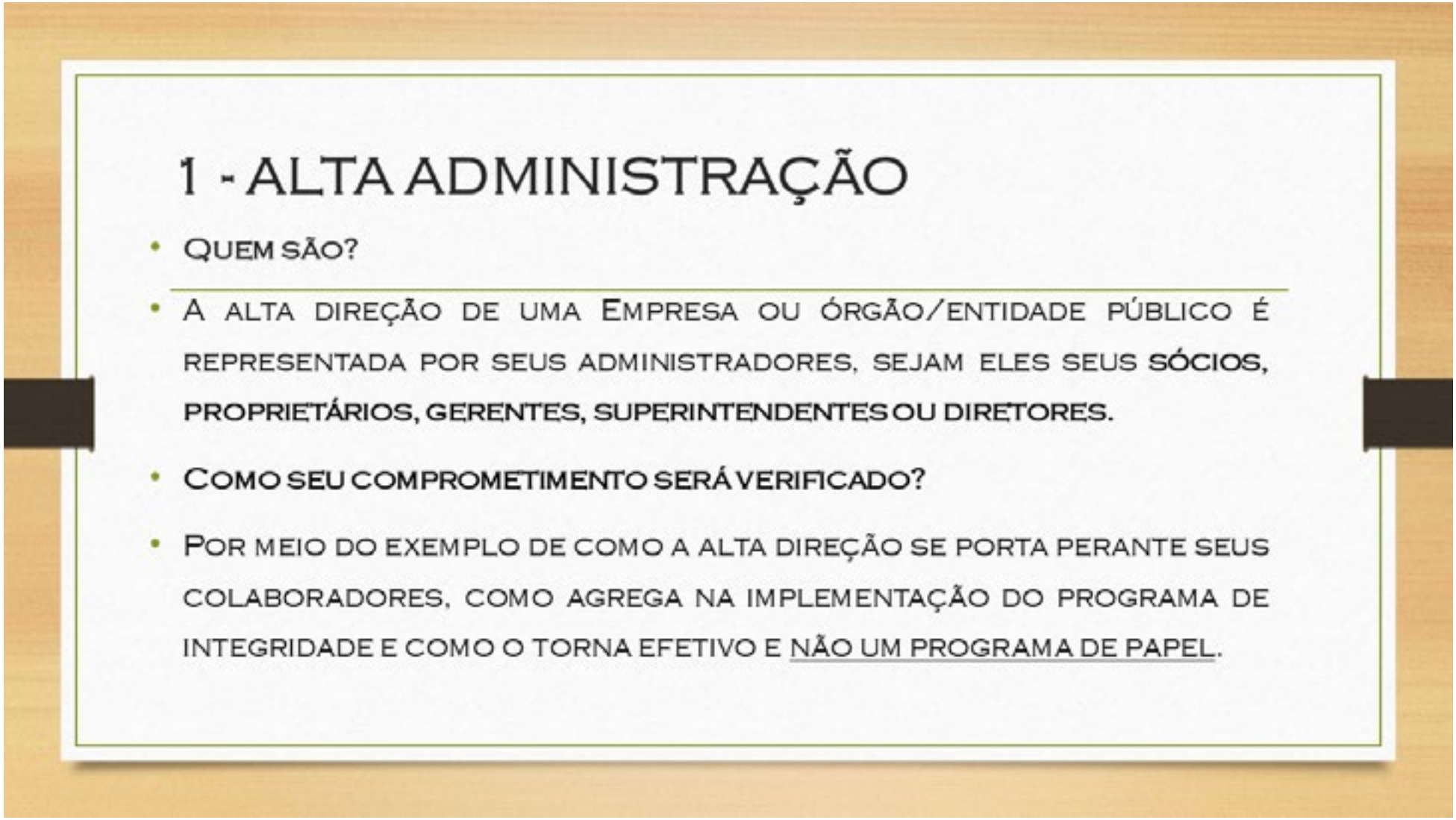
Compliance na Esfera Trabalhista

JULIANA DATO


Dato Leal
Consultoria em Compliance
COMPLIANCE NA ESFERA TRABALHISTA


NOÇÕES GERAIS
O QUE É COMPLIANCE?
• O TERMO COMPLIANCE TEM ORIGEM NO VERBO EM INGLÊS *"TO COMPLY WITH"*, QUE SIGNIFICA "AGIR DE ACORDO COM", PODENDO SER UMA REGRA, UMA INSTRUÇÃO INTERNA, UM COMANDO OU UM PEDIDO, OU SEJA, ESTAR EM "COMPLIANCE" É ESTAR EM CONFORMIDADE COM **LEIS E REGULAMENTOS EXTERNOS E INTERNOS.**
• UM PROGRAMA DE COMPLIANCE, ANTES DE MAIS NADA, VISA O COMPROMETIMENTO DA ALTA ADMINISTRAÇÃO COM A CONDUÇÃO DOS NEGÓCIOS, BASEADA EM VALORES ÉTICOS E MORAIS PARA O CUMPRIMENTO DAS NORMAS E REGULAMENTOS E NA INSTRUÇÃO (TREINAMENTO) DOS SEUS COLABORADORES PARA QUE ESTES POSSAM ATUAR DE FORMA PROBA.

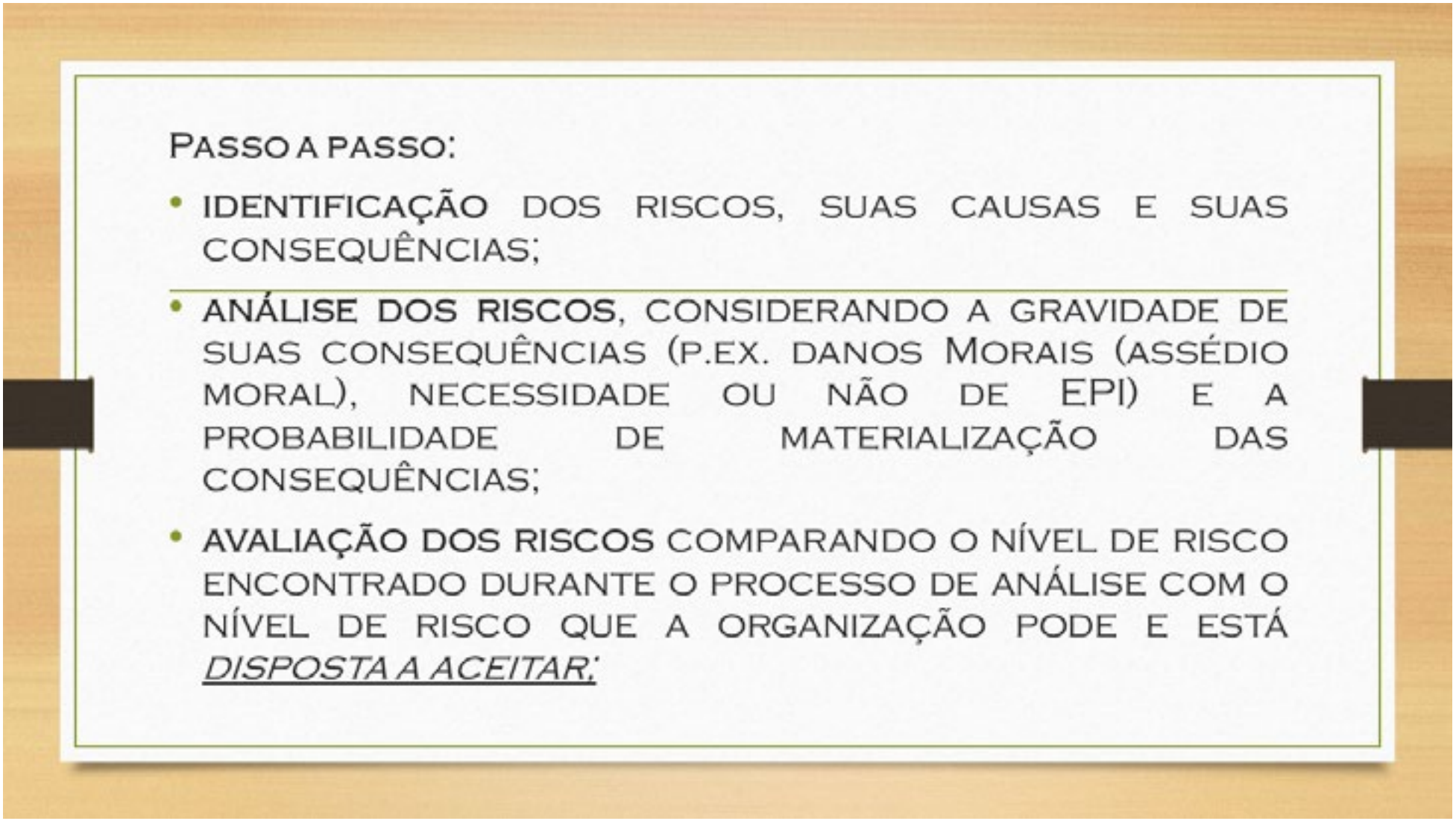

PILARES DE UM PROGRAMA DE COMPLIANCE
SUPORTE DA ALTA ADMINISTRAÇÃO
AVALIAÇÃO DE RISCOS
CÓDIGO DE CONDUTA
CONTROLES INTERNOS
TREINAMENTO E COMUNICAÇÃO
CANAIS DE DENÚNCIA
INVESTIGAÇÕES INTERNAS
DUE DILIGENCE
AUDITORIA E MONITORAMENTO


1 - ALTA ADMINISTRAÇÃO
QUEM SÃO?
A ALTA DIREÇÃO DE UMA EMPRESA OU ÓRGÃO/ENTIDADE PÚBLICO É REPRESENTADA POR SEUS ADMINISTRADORES, SEJAM ELES SEUS SÓCIOS, PROPRIETÁRIOS, GERENTES, SUPERINTENDENTES OU DIRETORES.
COMO SEU COMPROMETIMENTO SERÁ VERIFICADO?
POR MEIO DO EXEMPLO DE COMO A ALTA DIREÇÃO SE PORTA PERANTE SEUS COLABORADORES, COMO AGREGA NA IMPLEMENTAÇÃO DO PROGRAMA DE INTEGRIDADE E COMO O TORNA EFETIVO E NÃO UM PROGRAMA DE PAPEL.

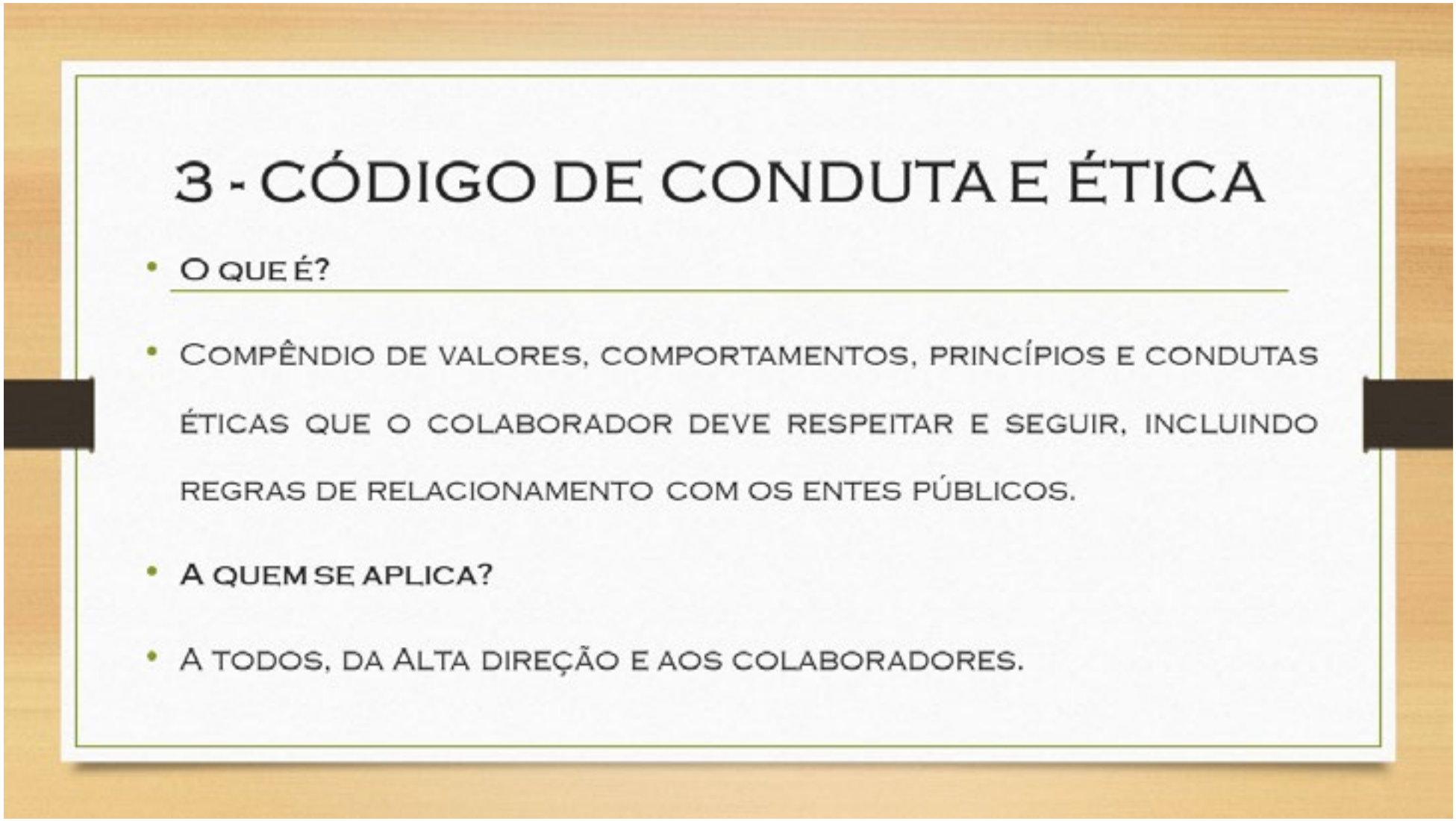
- **Quais os deveres da Alta Direção?**

1. Disseminar a cultura de Compliance, sendo um exemplo de gestor que respeita e atua em conformidade com as regras e normas da empresa.
2. Atuar na execução das medidas estabelecidas;
3. Tornar público seu compromisso com o tema, por meio dos canais de comunicação da empresa (site, redes sociais, declarações públicas, propagandas);
4. Disponibilizar Cursos, palestras e debates sobre ética e integridade;
5. Fomentar a participação dos colaboradores promovendo a cultura da integridade, ética e boas práticas.


2 - AVALIAÇÃO DE RISCOS
• FUNÇÃO:
• VERIFICAR AS POSSÍVEIS FALHAS E EVENTOS COM IMPACTOS DANOSOS NA IMAGEM DA EMPRESA.
• BUSCAR A MINORARAÇÃO DAS SITUAÇÕES QUE PREJUDIQUEM O ALCANCE DOS OBJETIVOS DEFINIDOS PELA EMPRESA.


PASSO A PASSO:
• IDENTIFICAÇÃO DOS RISCOS, SUAS CAUSAS E SUAS CONSEQUÊNCIAS;
• ANÁLISE DOS RISCOS, CONSIDERANDO A GRAVIDADE DE SUAS CONSEQUÊNCIAS (P.EX. DANOS MORAIS (ASSÉDIO MORAL), NECESSIDADE OU NÃO DE EPI) E A PROBABILIDADE DE MATERIALIZAÇÃO DAS CONSEQUÊNCIAS;
• AVALIAÇÃO DOS RISCOS COMPARANDO O NÍVEL DE RISCO ENCONTRADO DURANTE O PROCESSO DE ANÁLISE COM O NÍVEL DE RISCO QUE A ORGANIZAÇÃO PODE E ESTÁ DISPOSTA A ACEITAR;

- **AVALIAÇÃO DA ADEQUAÇÃO E EFICÁCIA DOS CONTROLES** EXISTENTES NA EMPRESA, VISANDO MITIGAR OS RISCOS AVALIADOS (ALGO ESTA SENDO FEITO?);
- **DETERMINAÇÃO DA FORMA DE GESTÃO DOS RISCOS**, CONSIDERANDO A NECESSIDADE DE IMPLEMENTAÇÃO DE CONTROLES E TRATAMENTO PARA OS RISCOS *NÃO ACEITÁVEIS*;
- **NOVA AVALIAÇÃO** DOS RISCOS PERIODICAMENTE, POR OCASIÃO DE MUDANÇAS INTERNAS SIGNIFICATIVAS DE: ATIVIDADES/PRODUTOS/SERVIÇOS/ESTRUTURA/ESTRATÉGIA/OBRIGAÇÕES OU;
- EXTERNAS (P.EX. CIRCUNSTÂNCIAS ECONÔMICO-FINANCEIRAS, CONDIÇÕES DE MERCADO, PASSIVOS E RELACIONAMENTO COM O CLIENTE), E EM FUNÇÃO DE DENÚNCIAS/NÃO CUMPRIMENTO DE REQUISITOS E ETC.


3 - CÓDIGO DE CONDUTA E ÉTICA
O QUE É?
COMPÊNDIO DE VALORES, COMPORTAMENTOS, PRINCÍPIOS E CONDUTAS ÉTICAS QUE O COLABORADOR DEVE RESPEITAR E SEGUIR, INCLUINDO REGRAS DE RELACIONAMENTO COM OS ENTES PÚBLICOS.
A QUEM SE APLICA?
A TODOS, DA ALTA DIREÇÃO E AOS COLABORADORES.

- COMO APLICAR?

1. DIVULGAÇÃO A TODOS OS COLABORADORES, GARANTINDO QUE TENHAM RECEBIDO (GARANTIA DE FUTURA DOCUMENTAÇÃO PARA RECLAMATÓRIAS TRABALHISTAS);
2. FIXAÇÃO DE CARTAZES, PLACAS, SINAIS E MENSAGENS SOBRE OS PADRÕES DE CONDUTA E OS PROCEDIMENTOS QUE CADA COLABORADOR E GESTOR DEVEM OBSERVAR E APLICAR EM SEU DIA –A – DIA.

4 – CONTROLES INTERNOS

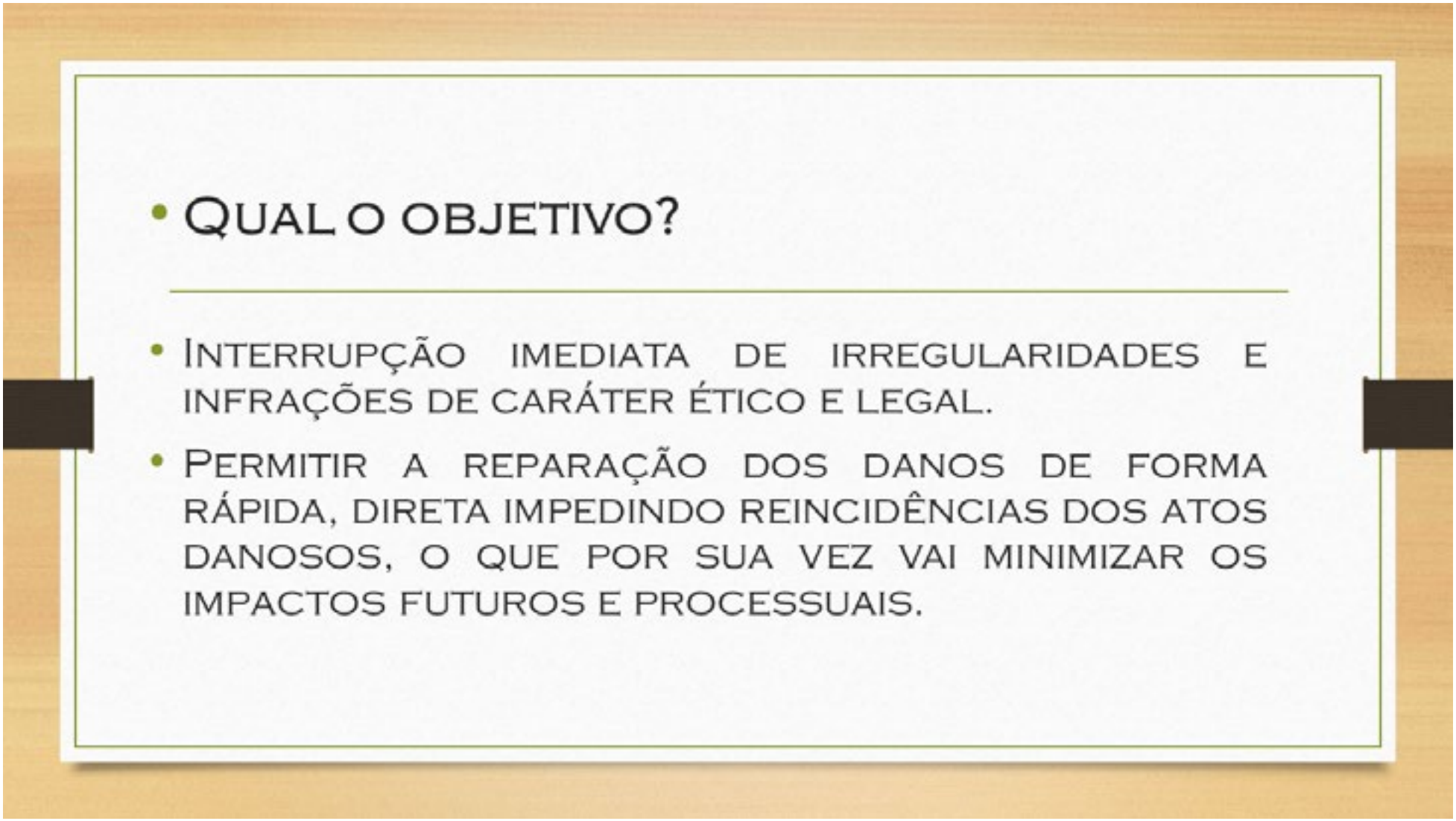
- MECANISMOS PARA MINIMIZAR OS RISCOS E ASSEGURAR QUE REGISTROS CONTÁBEIS, FINANCEIROS E DOCUMENTAÇÕES REFLITAM OS NEGÓCIOS DA EMPRESA **(DOCUMENTOS CONTAM A HISTÓRIA DA EMPRESA)**;
- VISA PRIMAR PELA TRANSPARÊNCIA;
- MANTER DOCUMENTOS PRIMORDIAIS ARQUIVADOS E ORGANIZADOS (FOLHAS DE PONTO, TRCT'S, COMPROVANTES DE PAGAMENTO, RECIBOS DE ENTREGA DE CTPS) NO INTUITO DE EVITAR PASSIVOS TRABALHISTAS POR FALTA DE DOCUMENTAÇÃO OU EXTRAVIO.

- QUAL SUA FUNÇÃO?

1. APONTAR E CORRIGIR ERROS;
2. ATUAR DE FORMA PREVENTIVA, VISANDO DIMINUIR A OCORRÊNCIA DE FRAUDES E IRREGULARIDADES;
3. CONFERIR RECEITAS E DESPESAS COM OS REGISTROS CONTÁBEIS REALIZADOS, VISANDO A CONFORMIDADE ENTRE OS DOIS E A DUPLA CHECAGEM;
4. ESTABELECER REGRAS SOBRE PAGAMENTO E TRANSAÇÕES QUE PRECISEM DE AUTORIZAÇÃO ESPECÍFICA POR SE TRATAR DE ALTAS QUANTIAS;
5. ESTABELECER CONDUTAS PARA SANAR OS PROBLEMAS QUE GEREM RISCOS, INCLUSIVE COM RELAÇÃO À TRANSAÇÕES COM OS ENTES PÚBLICOS

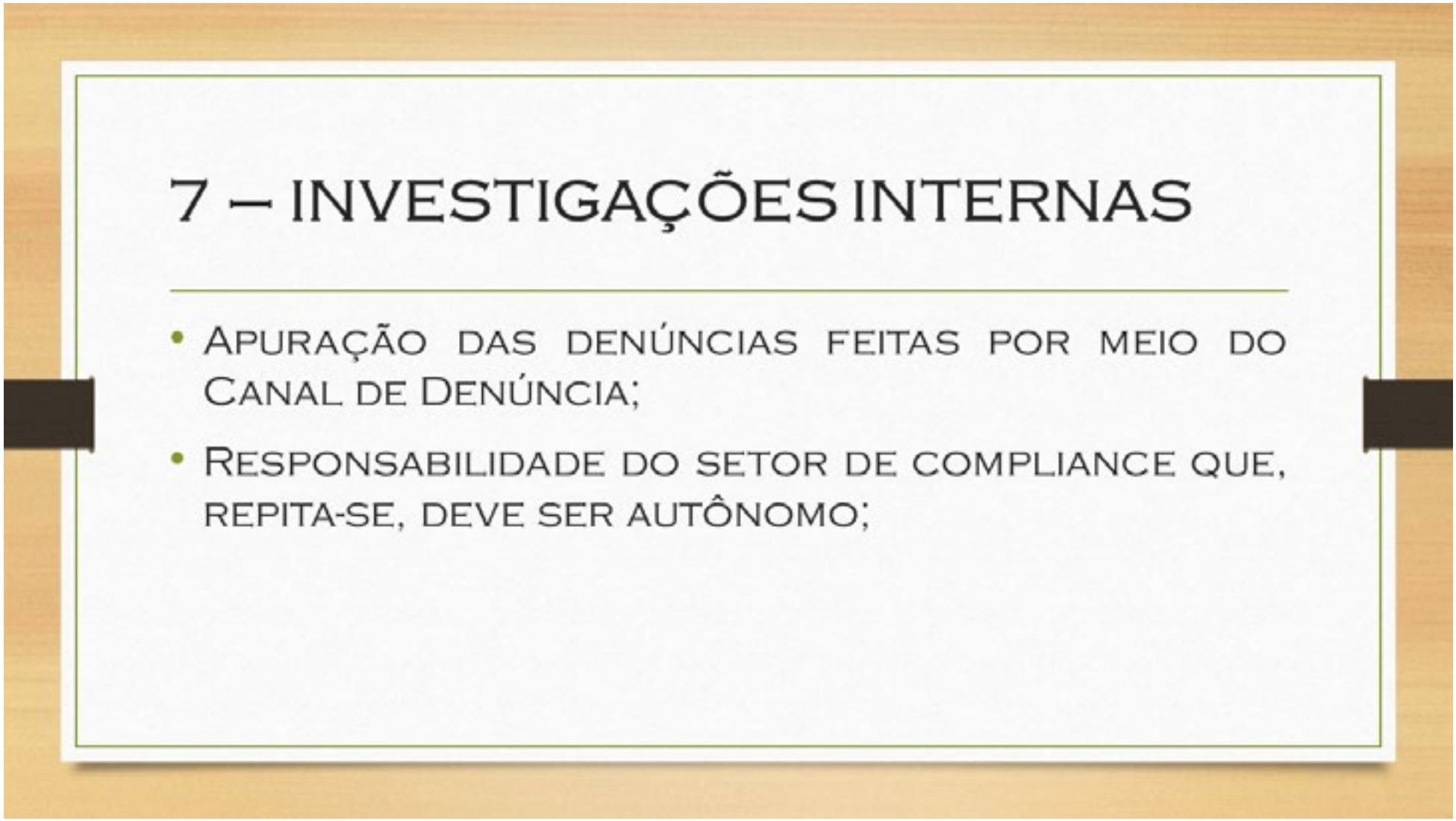

5 – TREINAMENTO E COMUNICAÇÃO
• TREINAR O COLABORADOR PARA QUE ELE ENTENDA O OBJETO SOCIAL DA EMPRESA, NO QUE ELE TRABALHA EFETIVAMENTE, OS INTERESSES DA EMPRESA, OS PORMENORES DO PRODUTO OU DO SERVIÇO;
• AS REGRAS DA EMPRESA E O SEU PAPEL PARA GARANTIR O SUCESSO DE TODO O PROGRAMA DE COMPLIANCE;
• O QUE PODE OU NÃO SER FEITO E TIRAR QUALQUER DÚVIDA QUE PERMANEÇA.


6 - Canais de Denúncia
• No que consiste?
1. Para denuncias de irregularidades sem retaliações;
2. A Denuncia será feita para um responsável pelo Compliance da empresa;
3. Responsável este que deverá ser autônomo e munido de subsídios para apurar os fatos (carta branca para apuração e recursos necessários), bem como aplicar as sanções cambíveis.


• QUAL O OBJETIVO?
• INTERRUPÇÃO IMEDIATA DE IRREGULARIDADES E INFRAÇÕES DE CARÁTER ÉTICO E LEGAL.
• PERMITIR A REPARAÇÃO DOS DANOS DE FORMA RÁPIDA, DIRETA IMPEDINDO REINCIDÊNCIAS DOS ATOS DANOSOS, O QUE POR SUA VEZ VAI MINIMIZAR OS IMPACTOS FUTUROS E PROCESSUAIS.


MEDIDAS DISCIPLINARES
• O QUE SIGNIFICA?
• ESTABELECER PENALIDADES E PROCEDIMENTOS DE PUNIÇÃO DE COLABORADORES QUE VIOLAREM O CÓDIGO DE CONDUTA ÉTICA, INDEPENDENTE DA POSIÇÃO OU CARGO.
• COMO SERÃO DEFINIDAS?
• DE FORMA OBJETIVA;
• RAZOÁVEL, PROPORCIONAL E IGUALITÁRIA;
• APÓS A DEVIDA APURAÇÃO, ASSEGURADO O DIREITO DE DEFESA (DEVIDO PROCESSO LEGAL).


• Exemplos:
1. Advertência;
2. Suspensão;
3. Demissão.


7 – INVESTIGAÇÕES INTERNAS
• APURAÇÃO DAS DENÚNCIAS FEITAS POR MEIO DO CANAL DE DENÚNCIA;
• RESPONSABILIDADE DO SETOR DE COMPLIANCE QUE, REPITA-SE, DEVE SER AUTÔNOMO;


8 - Due diligence
• Refere-se ao processo de investigação de uma oportunidade de negócio que o investidor deverá proceder para poder avaliar os riscos da transação.
• Embora tal investigação deva ser feita por obrigação legal, o termo refere-se normalmente a investigações voluntárias.
• Na verdade, uma *due diligence* compreende um conjunto de atos investigativos que devem ser realizados antes de uma operação empresarial, seja pelo interessado em ingressar societariamente ou mesmo adquirir uma empresa, seja por parte de quem está repassando seu negócio.


9 – AUDITORIA E MONITORAMENTO
• Processo constante para identificação de acertos e erros após a implementação do Programa de Compliance;
• Responsável por adequar o programa caso algum pilar não esteja funcionando adequadamente;
• Monitora todo o programa, desde a gestão do risco, bem como para concluir se o risco foi extirpado ou não.

CONCLUSÃO

- Com o atual cenário político, social e econômico em que o Brasil se encontra, mais do que nunca, se mostra necessária a incansável difusão da "Cultura de Conformidade" (Compliance).
- As empresas precisam se adequar aos novos moldes da legislação anticorrupção, visando melhorar sua imagem, confiabilidade social e jurídica e principalmente minorar passivos Trabalhistas.
- Vamos abraçar o **Compliance**!


Dato Leal
Consultoria em Compliance
OBRIGADA!
DATOJULIANA@GMAIL.COM