Gestão da Segurança da Informação

Ali Faiez Taha – CIRP
aftaha@cirp.usp.br

Gestão da Segurança da Informação

Objetivos:

Gerenciamento, proteção e distribuição dos recursos
Pilares: Confidencialidade, Integridade e Disponibilidade

Monitoramento dos processos
Gestão da Análise de Risco

Continuidade dos negócios
Recuperação de desastres

Políticas e normas de segurança

Necessidades da GSI

Minimizar os riscos inerentes à informação em sistemas computacionais.

Ideia de utilizar a segurança *apenas* para sistemas computacionais já está ultrapassada.

Preocupar-se com todas as formas de tráfego / criação de informação, em todos os meios.

Políticas e Normas: nortear as empresas para a GTSI.

Implantação: Gerenciar, protejer e distribuir os recursos necessários.

Foco principal: características humanas, organizacionais e estratégicas relativas à segurança da informação.

Definições

1 - Informação: Algo que se conhece e em que se baseia para racionalizar.

Ato ou efeito de informar, transmissão de notícias, instrução, ensinamento.
Transmissão de conhecimentos.

2 - Ameaça: Algo que pode agir voluntária ou involuntariamente em prejuízo de alguém ou alguma coisa.

Ato de ameaçar, perigo.
Gesto que exprime intenção de prejudicar ou provocar danos.

3 - Vulnerabilidade: Algo que represente falha ou fragilidade de alguém ou alguma coisa.
Característica que torna vulnerável.
Meio pelo qual algo se torna suscetível ou fragilizado em uma determinada circunstância

Definições

4 - Impacto: Resultado provocado pela ação de uma ameaça sobre uma vulnerabilidade.

Prejuízo, dano, consequência de uma investida, efeito.
Resultado apurado.

5 - Risco: Resultado objetivo da combinação da probabilidade de ocorrência de um evento e seu impacto resultante.
Possibilidade de acontecimento futuro incerto.
Perigo ou possibilidade de perigo.

6 - Gestão de riscos: Ato de estabelecer e operacionalizar processos contínuos de acompanhamento dos níveis de risco e adotar controles que eliminem vulnerabilidades, afastem ameaças e reduzam a probabilidade de uma ameaça explorar uma vulnerabilidade e provocar impactos à confidencialidade, integridade e disponibilidade da informação.

Os 3 pilares

A Gestão da Segurança da Informação visa à adoção de medidas alinhadas com as estratégias de negócio, a partir de um monitoramento contínuo dos processos, métodos e ações.

Tem por objetivo o pronto restabelecimento dos sistemas, evitar acesso indevido à informações, mitigar os riscos e se basear nos 3 pilares da GTSI :
Confidencialidade , Integridade e Disponibilidade.

Propriedades da Informação

1 - Confidencialidade: Propriedade da informação em estar a salvo de acesso e divulgação não-autorizados. Sua preservação é a garantia do resguardo das informações dadas pessoalmente em confiança e proteção contra a sua revelação não autorizada.

2 – Integridade: Propriedade da informação em se manter acurada, completa e atualizada. Sua preservação é a garantia de que a informação se manteve fiel à sua origem ou ainda, que qualquer alteração durante o processo tenha sido realizada com autoriação e controle.

3 – Disponibilidade: Propriedade da informação em se manter disponível para os agentes autorizados, quando estes dela necessitarem. Sua preservação é a garantia de que a informação se manteve acessível aos agentes autorizados sempre que precisou ser resgatada.

4 - Ciclo de vida: O ciclo de vida da informação é representado pelas macro-fases por onde passa a informação desde sua criação até o seu descarte. Manuseio, armazenamento, transporte, descarte.

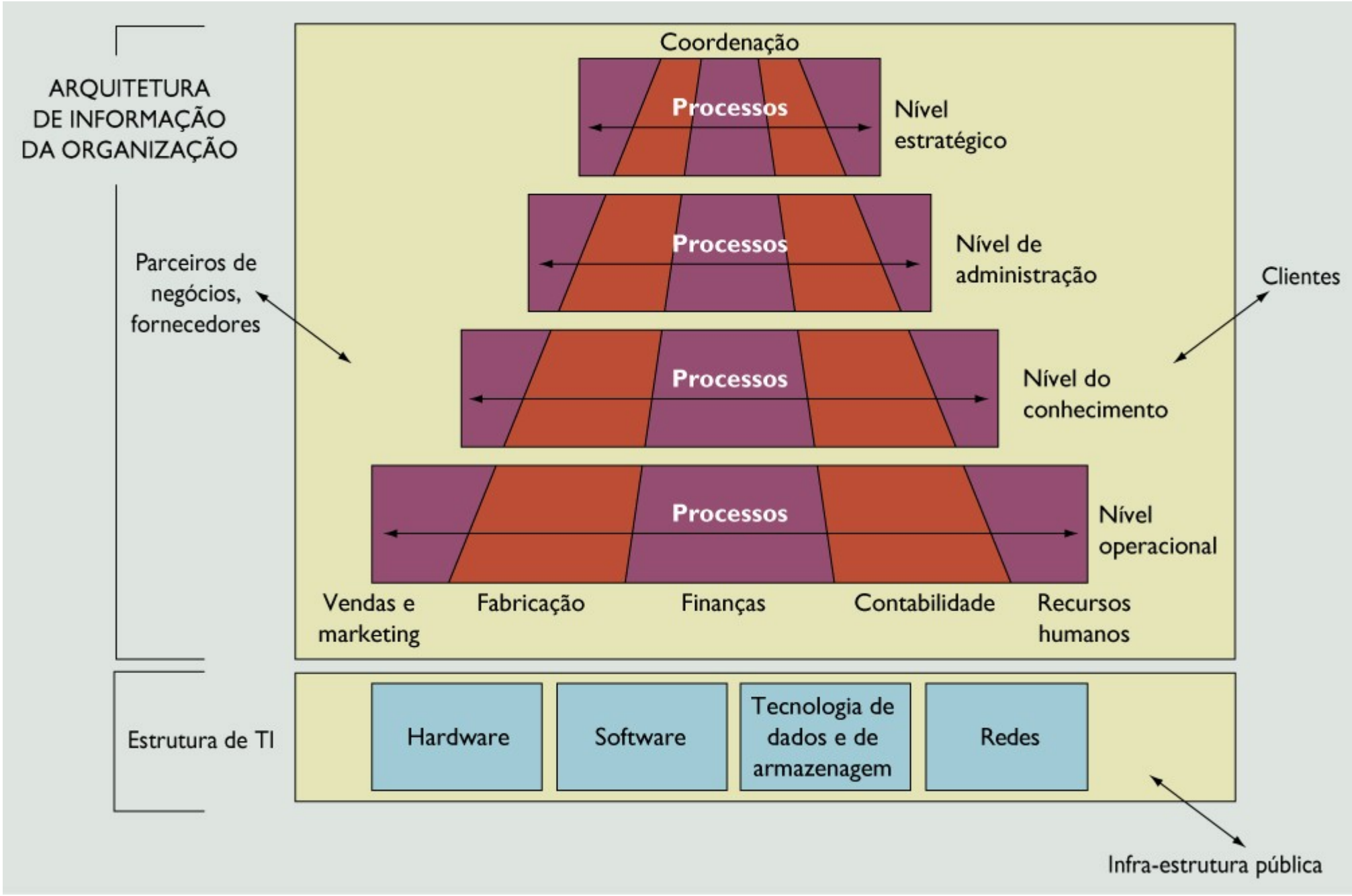

Integridade
Segurança
de
Informação
Confiden-
cialidade
Disponibi-
lidade

Ativos da empresa

1 - Pessoas: Um dos principais ativos do modelo de gestão de riscos da informação dado seu envolvimento em diversas fases do ciclo de vida da informação e sua autonomia para tomar decisões que revelam seu comportamento e perfil diante de uma situação de risco.

2 – Processos: Porção mais estável e duradoura do modelo de gestão de riscos da informação dado a natureza de seu propósito em regular, parametrizar e orientar ações, responsabilidades, procedimentos, entradas e saídas diante de uma situação de risco.

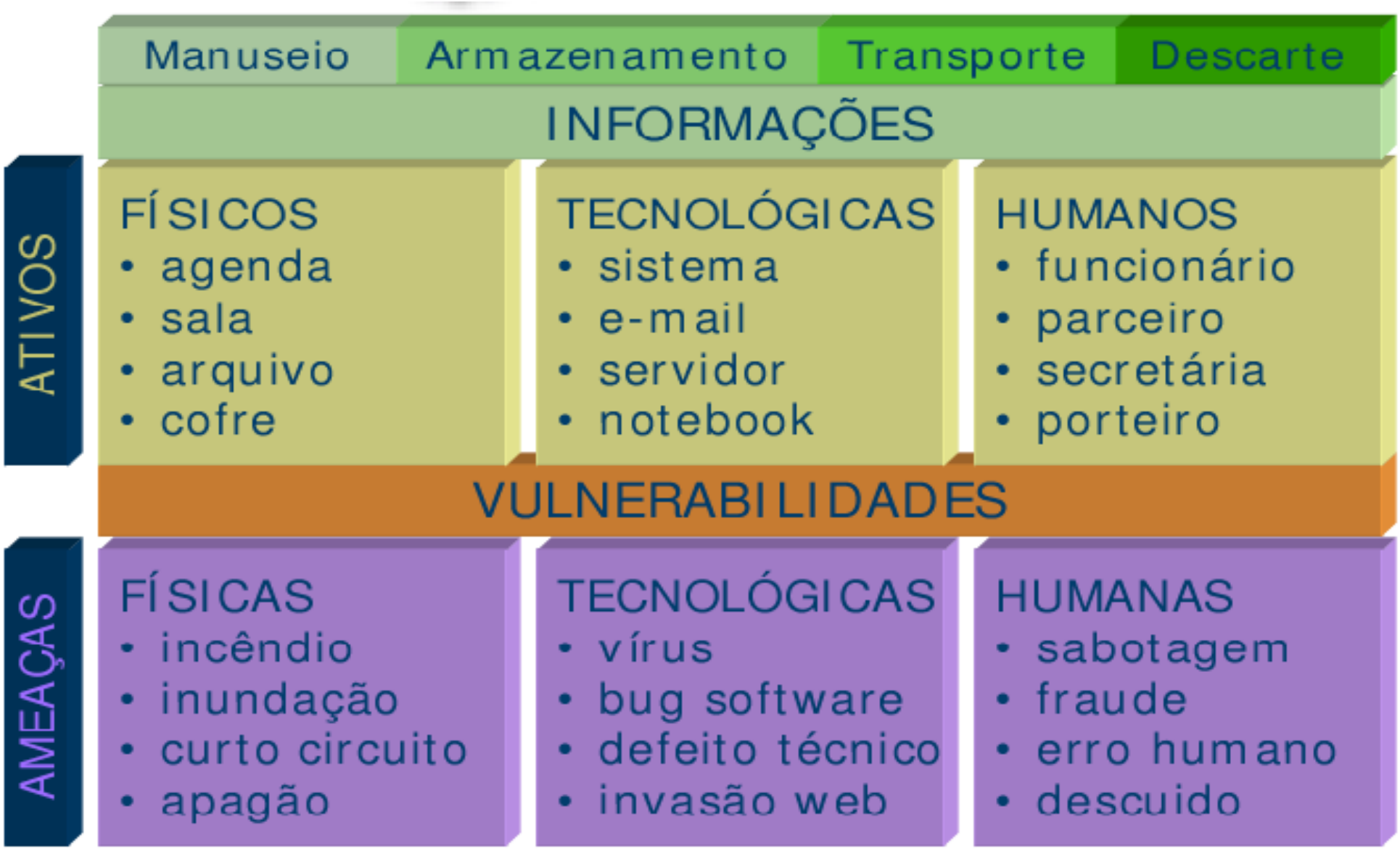
3 – Tecnologias: Porção mais dinâmica do modelo de gestão de riscos da informação dado a velocidade com que são desenvolvidas e introduzidas nos processos de especificação, implementação, automação e manutenção de controles de segurança.


ARQUITETURA DE INFORMAÇÃO DA ORGANIZAÇÃO
Coordenação
Processos
Nível estratégico
Processos
Nível de administração
Processos
Nível do conhecimento
Processos
Nível operacional
Parceiros de negócios, fornecedores
Clientes
Vendas e marketing
Fabricação
Finanças
Contabilidade
Recursos humanos
Estrutura de TI
Hardware
Software
Tecnologia de dados e de armazenagem
Redes
Infra-estrutura pública

Segurança da Informação

Adotar controles físicos, tecnológicos e humanos personalizados que viabilizem a redução e administração dos riscos, levando a empresa a atingir o nível de segurança adequado ao seu negócio.

Informação X Segurança



Cenário do mercado

- **Regulamentações**:
CVM, SOX, PCI (Cartões de crédito), Código Civil, Nota Fiscal Eletrônica, TCU, etc.

- **Boas práticas de gestão:**
Normas, regulamentações, certificações, padrões.

- Perfil do profissional de segurança:
·Visão consultiva
·Integração com outras áreas
·Foco no negócio
·Busca por indicadores
·Fundamentado em normas técnicas e frameworks de mercado
·Visão de risco
·Atuação mais normativa
·Multidisciplinar

Certificações

1 - CISM - Certified Information Security Manager
Certified Information Security Manager, é a nova certificação da ISACA especialmente desenhada para profissionais experientes em segurança da informação. A CISM é **orientada para o negócio e focada em gestão de risco da informação**, quando trata conceitualmente questões de segurança, sejam elas gerenciais, de desenho ou técnicas. **Destina-se a indivíduos que precisam manter uma visão ao gerenciar, desenhar, supervisionar e avaliar a segurança da informação da empresa.**

2 - CISSP é o acrônimo para Certified Information System Security Professional, um certificado profissional emitido e mantido pelo consórcio ISC2, fundado com o objetivo de **estabelecer critérios para avaliar profissionais que trabalham com segurança da informação.** Designada como a certificação ANSI ISO/IEC Padrão 17024:2003.

Certificações

3 - ISO/IEC 27001 é um padrão para sistema de gerência da segurança da informação, ISMS, publicado em outubro de 2005 pelo International Organization for Standardization e pelo International Electrotechnical Commision. Seu nome completo é ISO/IEC 27001:2005 - Tecnologia da informação - técnicas de segurança - sistemas de gerência da segurança da informação - requisitos mas conhecido como "ISO 27001".

4 - O PCI-DSS é um padrão mundial de segurança da informação para estabelecimentos que utilizam cartões como forma de pagamento. Suas diretrizes, desenvolvidas em conjunto pelas operadoras de cartões de crédito e débito, incluindo as bandeiras Visa, Mastercard e American Express, devem ser seguidas por organizações afiliadas às bandeiras de cartão de crédito e débito, processadoras, gateways de pagamento e, futuramente, bancos emissores. Essas exigências visam reduzir o número de fraudes com cartões de crédito. Profissionais podem se certificar PCI QSA - Qualified Security Assessor.

Certificações

5 - Outras:
CISM Certified Information Security Management
CISSP Certified Information Systems Security Professional
CISA Certified Information Systems Auditor
BS7799 Lead Auditor
SSCP Systems Security Certified Practitioner
PCI QSA Payment Card Industry Qualified Security Assessor
GIAC Global Information Assurance Certification
CBCP Certified Business Continuity Professional
CIA Certified Internal Auditor

Padrões e Normas

Análise e Gestão de Risco, baseadas na ISO 13335

Planejamento de Disaster Recovery e Continuidade de Negócios, baseados na BS 7799-2/ISO 27001

Desenvolvimento, Políticas e Normas de Segurança, baseados na BS 7799-1/ISO 17799 e ISO 27000.

Padrões e Normas

www.iso27001security.com

- BSI BS ISO/IEC 27001:2005 Information Security
- BSI BS7799-2:2002 Information Security
- BSI BS 25999 Business Continuity Management
- ISO 13335 IT Security Management
- ISO/IEC 17799:2000 Information Security
- ISO 18044 Security Incident Management
- ISO 15408 Common Criteria
- ISO 12207 Software Life Cycle Processes
- ISO 18028 IT Network Security
- NIST SP800-53 Recommended Security Controls
- ISACA COBIT | PCI QSA | OCTAVE Risk Assessment
- PCI DSS Payment Card Industry Data Security Standard

ISO 27000

www.27000.org

ISO 27001, ISO 27002....ISO 27008

ISO 27001

ISO/IEC 27001 é um padrão para sistema de gestão da segurança da informação (ISMS - Information Security Management System) publicado em outubro de 2005 pelo International Organization for Standardization e pelo International Electrotechnical Commision. Seu nome completo é ISO/IEC 27001:2005 - Tecnologia da informação - técnicas de segurança - sistemas de gerência da segurança da informação - requisitos mas conhecido como ISO 27001.

Seu objetivo é ser usado em conjunto com ISO/IEC 17799, o código de práticas para gerência da segurança da informação, o qual lista objetivos do controle de segurança e recomenda um conjunto de especificações de controles de segurança. Organizações que implementam um ISMS de acordo com as melhores práticas da ISO 17799 estão simultaneamente em acordo com os requisitos da ISO 27001, mas uma certificação é totalmente opcional.

Este padrão é o primeiro da família de segurança da informação relacionado aos padrões ISO, agrupados à série 27000.

ISO 27001

- **ISO 27000 - Vocabulário de Gestão da Segurança da Informação;**
- **ISO 27001 - Publicada em Outubro de 2005 e substituiu a norma BS 7799-2 para certificação de sistema de gestão de segurança da informação;**

- **ISO 27002 - Substitui o ISO 17799:2005 (Código de Boas Práticas);**

- **ISO 27003 - Aborda as diretrizes para Implementação de Sistemas de Gestão de Segurança da Informação, contendo recomendações para a definição e implementação de um sistema de gestão de segurança da informação;**

- **ISO 27004 – Atua nas métricas e relatórios de um sistema de gestão de segurança da informação;**
- **ISO 27005 - Indicações para implementação, monitoramento e melhoria contínua do sistema de controles. Conteúdo idêntico ao da norma BS 7799-3:2005 – "Information Security Management Systems - Guidelines for Information Security Risk Management";**

- **ISO 27006 - Especifica requisitos e fornece orientações para os organismos que prestem serviços de auditoria e certificação de um sistema de gestão da segurança da informação.**

Certificação ISO/IEC 27001

A série ISO 27000 está de acordo com outros padrões de sistemas de gerência ISO, como ISO 9001 (sistemas de gerência da qualidade) e ISO 14001 (sistemas de gerência ambiental), ambos em acordo com suas estruturas gerais e de natureza a combinar as melhores práticas com padrões de certificação.

Certificações de organização com ISMS ISO/IEC 27001 : meio de garantir que a organização certificada implementou um sistema para gerência da segurança da informação de acordo com os padrões. **Credibilidade** é a chave de ser certificado por uma terceira parte que é respeitada, independente e competente.
Esta garantia dá confiança à gerência, parceiros de negócios, clientes e auditores que uma organização é séria sobre gerência de segurança da informação - não perfeita, necessariamente, mas está rigorosamente no caminho certo de melhora contínua.

Associação Brasileira de Normas Técnicas (ABNT), elaborou a NBR ISO/IEC 27001:2006 - tradução da ISO/IEC 27001:2005, elaborada pelo Join Technical Committee Information Technology (ISO/IEC/JTC 1), subcommittee IT Security Tecchniques (SC 27).

Certificação ISO/IEC 27001

Razões para se adotar a ISO 27001

Proteger a informação crítica da organização contra:

- **Perda de dados**
- **Uso impróprio**
- **Divulgação não autorizada**
- **Roubo**
- **Assegurar continuidade do negócio.**
- **Assegurar aos parceiros de negócio, órgãos reguladores, fornecedores e clientes que a sua informação confidencial está segura.**
- **Manter a reputação e confiança**

A certificação ISO 27001 assegura aos Clientes, Parceiros e Partes Interessadas que a organização:

- **Identifica e gerencia os riscos aos ativos críticos de informação.**
- ***Avalia e reavalia continuamente os riscos, de forma proativa e sistemática***
- **Implementa controles de uma forma proporcional aos riscos.**
- **Detém e gerencia sistematicamente as brechas de segurança**
- **Audita de forma independente o SGSI com respeito à conformidade e eficácia.**

Boas práticas de gestão

- Norma ISO/IEC 27002, antiga ISO/IEC 17799 – Código de Prática para a Getão de Segurança da Informação
- Gestão da continuidade de negócios: BS 25999
- Desenvolvimento Seguro de Software : ISO 15408
- ISO 31000 – Gestão de riscos

- **Control Objectives for Information and related Technology (COBIT), é um guia de boas práticas apresentado como framework, dirigido para a gestão de tecnologia de informação.**
- **Gerência de Serviços de TI – ITIL : Subconjunto do COBIT - Information Technology Infrastructure Library (ITIL) é um conjunto de boas práticas a serem aplicadas na infraestrutura, operação e manutenção de serviços de tecnologia da informação.**

- Difundir as normas na empresa. Definir riscos para as diferentes áreas.
- **Riscos no ambiente acadêmico.**

- Estruturação departamental, intra departamental, envolver RH, Comercial, Jurídico, etc.

- **Funcionar com risco aceitável**

Política de Segurança da Informação

Documento que registra os princípios e as diretrizes de segurança adotado pela organização

Dirigentes participam do processo de implantação.
Aval da diretoria para que todos aceitem, respeitem as normas e procedimentos vinculados na política de segurança.

Aprovação da política de segurança pela diretoria

Análise interna e externa dos recursos a serem protegidos.
Estudar o que deve ser protegido, verificando o atual programa de segurança da empresa, se houver, enumerando as deficiências e fatores de risco.

Elaboração das normas e proibições, tanto física, lógica e humana.
Criar as normas relativas à utilização de programas, utilização da Internet, acessos físicos e lógicos, utilização do E-Mail, utilização dos recursos tecnológicos, etc.

Política de Segurança da Informação

Aprovação pelo Recursos Humanos
As normas e procedimentos devem ser lidas e aprovadas pelo departamento de Recursos Humanos, no que tange a leis trabalhistas e manual interno dos funcionários da organização.

Aplicação e treinamento da equipe
Treinamento prático com recursos didáticos
Apresentar a política de segurança da informação

Estar sempre disponível para todos os colaboradores da organização.

Avaliação periódica e revisão constante.

Feedback
Monitoração constante. Corrigir incoerências.
Cuidados com vulnerabilidades, mudanças em processos gerenciais ou infra-estrutura.

Funcionalidade = 1 / Segurança

O ciclo

Ameaças exploram as vulnerabilidades...

que expõem os ativos...

que tem valor para a organização...

que exigem medidas de segurança...

que podem proteger das ameaças...

...e o ciclo se repete...

Gestão de Riscos

- Baseia-se em atividades coordenadas para direcionar e controlar uma organização no que se refere a riscos.

- Envolve um processo criterioso e recursivo de documentação, avaliação e decisão durante todas as fases do ciclo de vida do projeto.

Segurança Corporativa

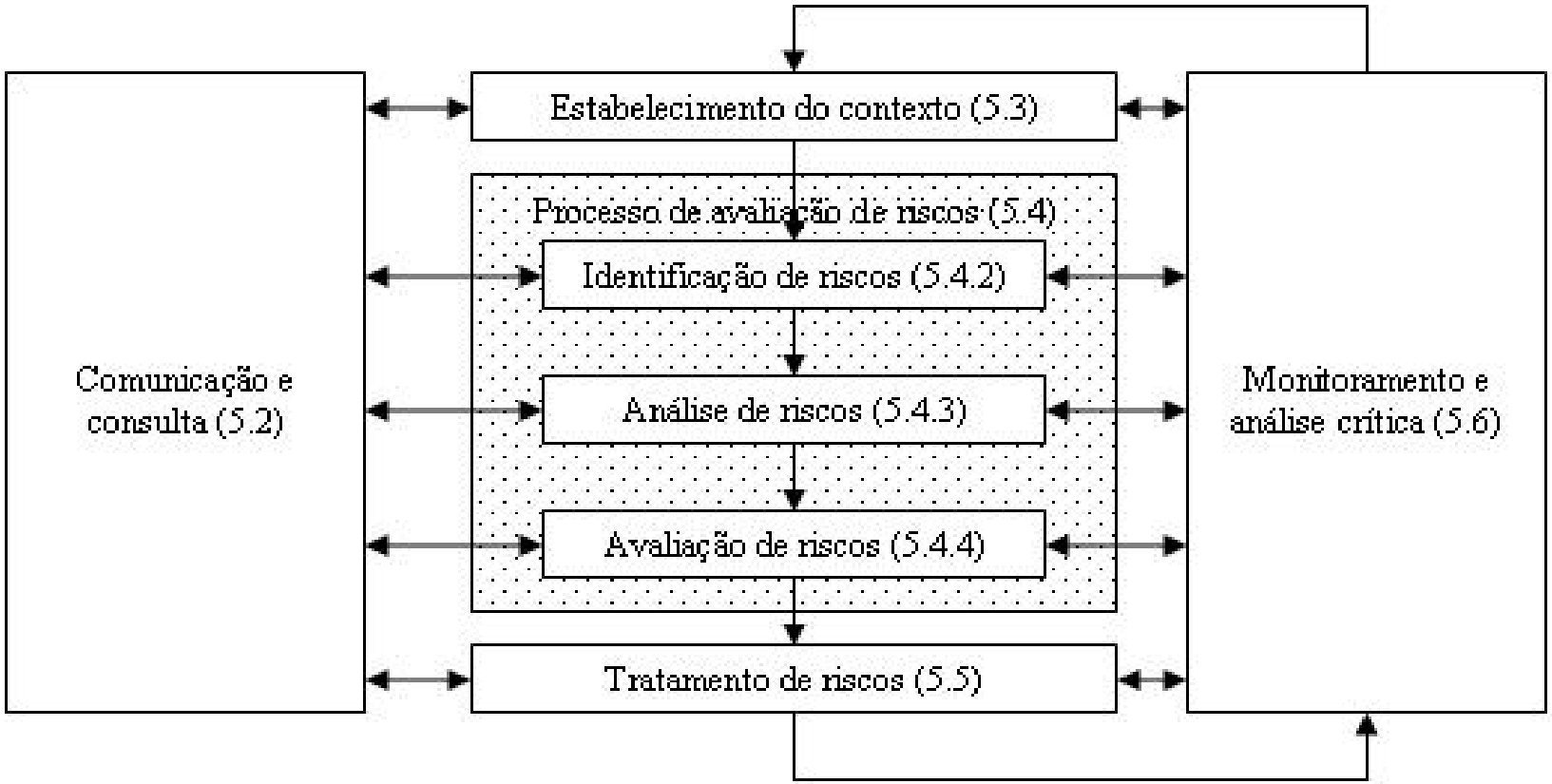
Padrões e normas

- **Normas de Gestão de Riscos :**
- **NIST SP800-30**
- **AS/NZS 4360, ISO 27005 e ISO 31000**

  O Brasil faz parte de grupo internacional de trabalho que criou a norma ISO 31000, lançada em 30/11/2009.

  ABNT NBR ISO 31000 – Gestão de Riscos, Princípios e Diretrizes.

Processo de Gestão de Riscos



Comunicação e Consulta

5.2 Comunicação e Consulta

A consulta as partes interessadas, tanto externas quanto internas é essencial num processo de gestão de riscos. Isso deverá ocorrer em todas as fases, tanto no estabelecimento dos critérios de risco, na identificação, avaliação e tratamento de riscos ou em ocorrências de sinistros. A cada momento é necessário que a organização tenha as ferramentas e técnicas adequadas para a comunicação. Um dos princípios da gestão de riscos é que o processo de gerenciar riscos deve ser parte integrante de todos os processos organizacionais, para que isso possa ser concretizado, um bom plano de comunicação deve ser planejados nas etapas iniciais.

5.3 Estabelecimento do Contexto

Nesse momento são definidos os critérios para gestão de riscos e o escopo da gestão. O contexto deve ser dividido em contexto interno e externo a organização. No contexto interno a organização deve analisar a sua estrutura organizacional, processos, responsabilidades, os sistemas de informação internos e o diálogo e relações com as partes interessadas internas. No contexto externo questões como o ambiente cultural, legal, social, político, financeiro, tecnológico, e econômico devem ser avaliados, assim como a relação com partes interessadas externas, sua percepção e valores.

Processo de avaliação de risco

5.4 Processo de Avaliação de Risco

5.4.2 Identificação de Riscos

Essa é a fase onde um conjunto de riscos devem ser identificados, nesta etapa o objetivo é gerar uma lista abrangente de riscos que possam criar, aumentar, evitar, reduzir, acelerar ou atrasar a realização dos objetivos. Um risco não identificado nesta fase não será incluído em análises posteriores, por isso é importante que muita atenção e esforço sejam feitas nessa análise. A tendência é que as organizações com o tempo passem a incrementar essa lista com novas fontes de risco, o processo deve melhorar continuamente.

5.4.3 Análise de Riscos

A análise de riscos vai fornecer uma compreensão sobre os riscos. Envolve a apreciação das causas e das fontes de risco, suas consequências positivas e negativas, e a probabilidade de que essas consequências possam ocorrer. Nessa etapa a organização deverá analisar todos os riscos identificados, verificando quais são as consequências e probabilidade dos riscos, isso será insumo para a etapa posterior.
Segundo a ISO 31000 "a análise de riscos pode ser realizada com diversos graus de detalhe, dependendo do risco, da finalidade da análise e das informações, dados e recursos disponíveis. Dependendo da circunstância a análise pode ser qualitativa, semiquantitativa, quantitativa ou uma combinação destas." Organizações menores com menos recursos tecnológicos terão mais dificuldade de conduzir uma análise quantitativa dos riscos, mas isso não impede que um processo de gestão possa ser estabelecido e traga resultados satisfatórios.

5.4.4 Avaliação de Riscos

Quais riscos precisam de tratamento? Qual a prioridade para implementação do tratamento? Este é o momento de dizer, por exemplo, se um risco deve ou não ser tratado e com qual prioridade. **Aceitável ou não.**
A avaliação de riscos envolve comparar o nível de risco encontrado durante o processo de análise com os critérios de risco estabelecidos quando o contexto foi considerado. Com base nesta comparação, a necessidade de tratamento pode ser considerada.

Tratamento de Riscos

5.5 Tratamento de Riscos

Segundo a ISO 31000 "O tratamento de riscos envolve a seleção de uma ou mais opções para modificar os riscos e a implementação dessas opções. Uma vez implementado, o tratamento fornece novos controles ou modifica os existentes" .

Em geral, riscos podem ser:

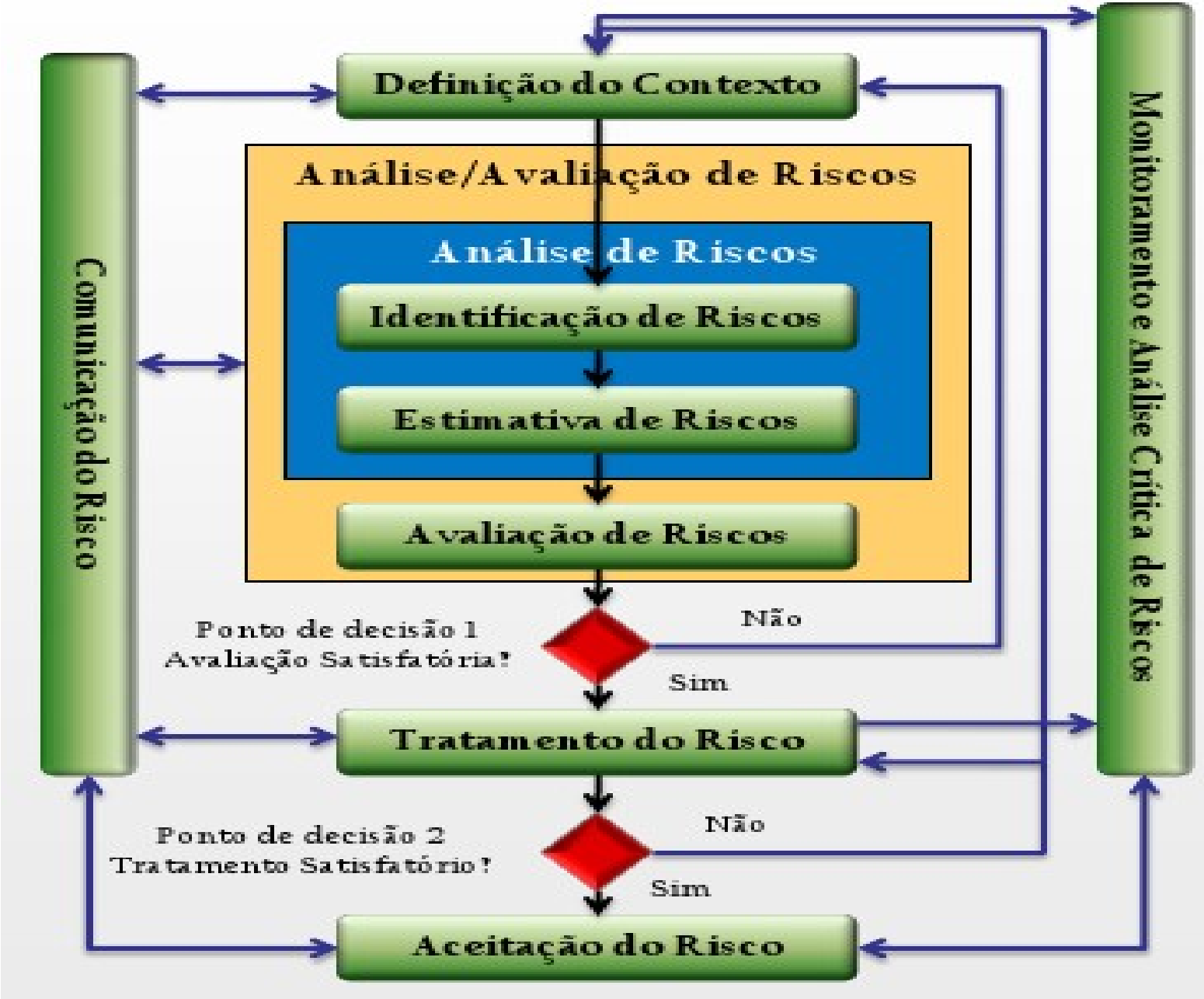
- **Evitados, não realizar a atividade;**
- **Aumentados, quando eles forem uma oportunidade (risco positivo);**
- **Remoção da fonte de risco;**
- **Redução da probabilidade de ocorrer;**
- **Redução da consequência;**
- **Compartilhados com terceiros (seguros por exemplo);**
- **Retidos por uma decisão bem consciente e embasada.**

5.6 Monitoramento e Análise Crítica

Ao longo do processo de gestão de riscos a melhoria contínua deverá acontecer. Ao longo da utilização da metodologia os critérios de riscos poderão ser alterados, novas ocorrências poderão incrementar as listas de riscos e oportunidades poderão ser consideradas. O contexto interno e externo podem sofrer alterações e a organização aprender com seus sucessos e falhas. Você poderá criar indicadores também para o seu processo de gestão de riscos e identificar pontos de melhoria a cada medição.

A ISO 31000 fornece as empresas uma excelente diretriz para a gestão de riscos, aproveitar essa ferramenta e integrá-la a sua estrutura de gestão poderá ser um bom ingrediente para manter o seu negócio equilibrado e sob controle numa visão de longo prazo.

Gestão ISO 27005



Norma ISO 31000

Integração das normas relacionadas a Riscos Corporativos

Necessidades da ISO 31000

Harmonia de padrões.
Norma regulamentadora.
Processo padrão a ser seguido, empresas de todos tamanhos, segmentos e áreas de atuação.
Lida com as incertezas e riscos, que podem afetar o objetivo empresarial.
Linkada com objetivo estratégico da empresa, sempre.

Objetivos relacionados a:

- **Atividade operacional**
- **Iniciativa estratégica**
- **Processos e projeto**

Trabalha tanto no lado negativo, quanto do lado da oportunidade e integra terminologia, conceitos, critérios e processos.

Desafios:

- **Estabelecer uma linguagem comum.**
- **Padronizar as melhores práticas.**
- **Convergência.**

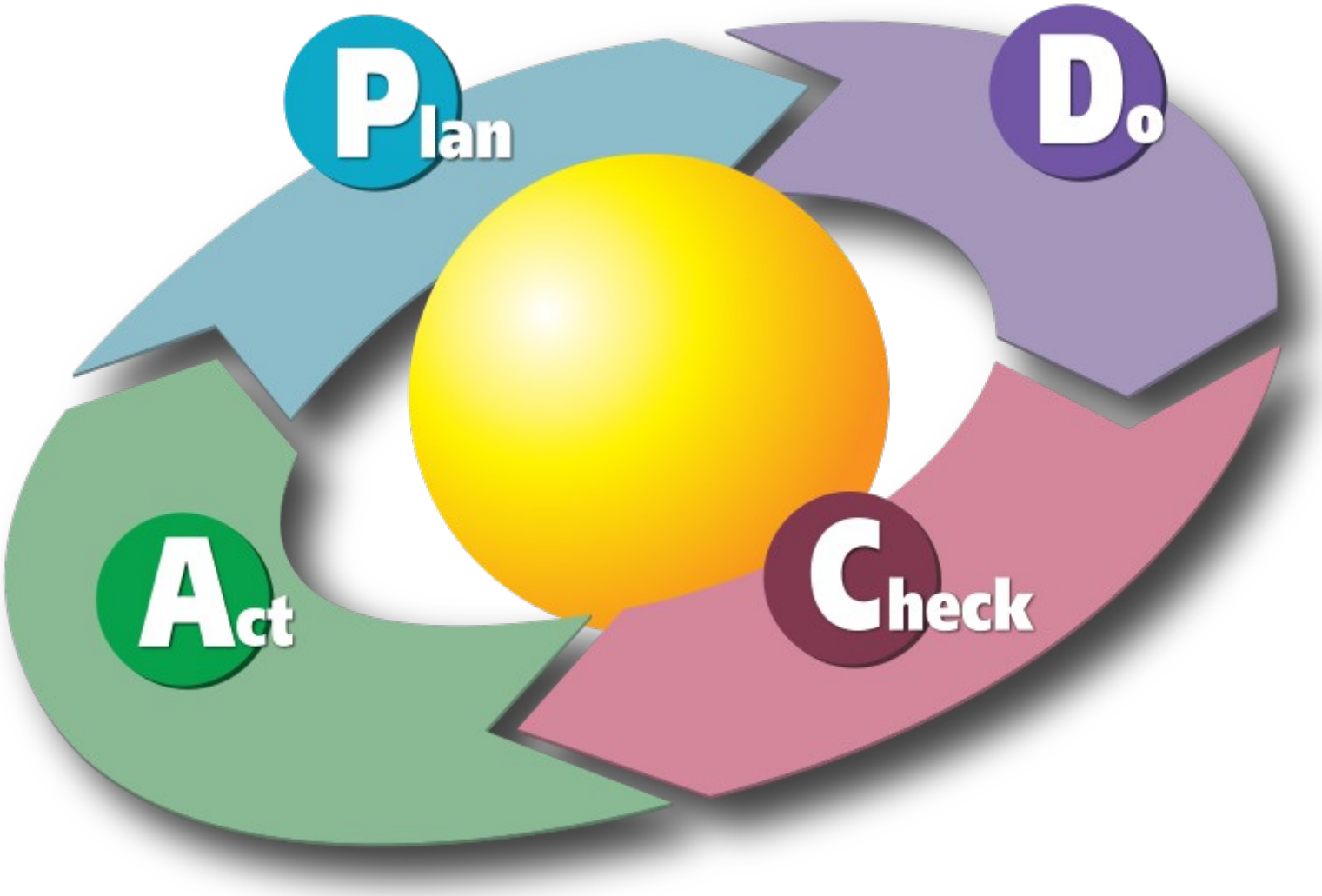
Framework ISO 31000

Sete passos a serem seguidos:

- **Comunicação e consulta com as áreas interessadas**
- **Estabelecer contextos, tratando de cenários e critérios**
- **Identificar perigos e fatores de risco**
- **Fazer a Análise de risco: Probabilidade versus impacto**
- **Classificação e avaliação do risco**
- **Tratamento do risco**
- **Monitoramento**

E, finalmente, o Ciclo do PDCA: Processo retroalimentativo

Ciclo PDCA



ISO 31000

Convergência das normas:

Muitas normas se adaptaram ao processo de risco da ISO 31000
Consenso entre 35 países.
Política de multidisciplinaridade.

Objetivos:

Criar valor para o processo da empresa
É parte integrante de qualquer processo da organização
Fazer parte de processo decisório
Tratar claramente a incerteza
Processo tem que ser sistemático e estruturado
Basear-se na melhor informação possível
Customizável (custo/benefício)
Considerar o fator humano
Transparente e incluir as partes interessadas
Dinâmica, interativa e responder a mudanças
Continuamente melhorada
Revisão contínua e aberta a melhorias.

Continuidade de Negócios

Risco de Indisponibilidade deve ser baixo para os clientes.
Velocidade de processamento e de decisões.
Alta disponibilidade, flexibilidade e foco em produtos.
Planejamento para Segurança e Contingência adequados

Definições

Plano de Contingência - Um plano para a resposta de emergência, operações backup, e recuperação de dados após um desastre em um sistema como a parte de um programa da segurança para assegurar a disponibilidade de recursos de sistema críticos e para facilitar a continuidade das operações durante uma crise.

Disponibilidade - A propriedade que um sistema ou um recurso de sistema de estarem acessíveis e utilizáveis sob demanda por uma entidade autorizada pelo sistema, de acordo com especificações de desempenho projetadas para o sistema; isto é, um sistema que está disponível para fornecer serviços de acordo com o projeto do sistema sempre que pedido por seu usuário.

Continuidade de Negócios

Confiabilidade - A habilidade de um sistema de executar uma função requerida sob condições indicadas por um período de tempo especificado.

Sobrevivência - A habilidade de um sistema de continuar em operação ou existindo apesar das condições adversas, inclui as ocorrências naturais, ações acidentais, e ataques ao sistema.

Estratégias

- **Inventariar ativos e processos**
- **Entender o negócio**
- **Identificar as exigências locais ou normativas**
- **Identificar os processos de negócio**
- ***Envolver o corpo executivo***
- **Definição das estratégias**
- **Alinhar as expectativas da corporação**
- **Formação organizacional**

Estratégias

- Estratégia de continuidade:
  - Ativo/Backup
  - Ativo/Ativo
  - Localidade alternativa

- Estratégia de Recuperação:
  - Usuários
  - Instalações
  - Logística
  - Dados
  - Operações

Estratégias

- **Cold Site : Proteger o Data Center**
- *Warm Site : Proteger o Data Center principal e espelhar os equipamentos de missão crítica.*
- **Espelhamento total (Alto custo, implementação e manutenção, Backup)**
- Análise de Riscos
  - **Levantar as ameaças e vulnerabilidades**
  - **Criticidade de processos**
  - Projetar Potenciais projetos
  - **Probabilidade versus Impacto**
  - **Riscos versus impactos**

Riscos são aleatórios e imprevisíveis

Impactos são previsíveis

Análise do Impacto do Negócio

- **Identifica e avalia os impactos resultantes da interrupção e dos cenários de desastre que afetam a organização.**
- **Técnicas para qualificar e quantificar os impactos.**
- **Define a criticidade dos processos de negócio e propriedades de recuperação.**
- **Avalia o custo da parada para cada processo analisado.**

Paradigmas

- Planos de Contingência e Continuidade são restritas a TI.
- PCN: somente em empresas de grande porte.
- Contingência garante Continuidade.
- Custo de PCN é muito elevado.
- Isso não vai acontecer aqui na nossa empresa.

Planos de Continuidade

- **PAC Plano de administração de Crises:**
- Ações a serem tomadas pré e pós ocorrência de um evento.
- Minimizar o tempo de resposta e agilizar as atividades necessárias, desde a confirmação do evento até as medidas necessárias para sua neutralização.

- **PRD Plano de Recuperação de Desastre:**
- Documento que define os recursos, ações, tarefas e dados requeridos para administrar o processo de recuperação dos componentes que suportam os Processos de Negócio.
- Plano projetado para ajudar o restabelecimento do processo de negócio empresarial dentro das metas de recuperação de desastre declaradas.

Planos de Continuidade

• **PCO Plano de Continuidade Operacional**:
• Visa a manutenção dos Processos de Negócio realizados pela empresa, independentemente das falhas ocorridas em seus componentes.
• Complementar ao Plano de Recuperação de Desastres, à medida que elimina o hiato entre a ocorrência de um evento e a retomada do Processo de Negócios afetado.

• **PRN Plano de Retorno a Normalidade**:
• **Ações coordeneadas e ordenadas de saída do regime de contigência.**

• **PTV Plano de Testes e Validação**:
• Documento que define os recursos e ações necessários para validação efetiva dos planos antes da ocorrência do incidente.

Planos de Continuidade

- **PCN Plano de Continuidade de Negócios:**
- Formado pelos planos **PRD, PRI, PCO, PRN e PTV**, monitorado por um Plano de Administração de Crises (PAC) que facilita sua gestão e atualização.

Consolida responsabilidades, locais e prazos.

Evidencia elementos para auditoria e atendimento de requisitos legais ou normativos.

Sistema de Gestão de Continuidade dos Negócios

É composto por:

- Política de Continuidade de Negócios
- Plano de Continuidade dos Negócios

O SGCN tem foco na manutenção da efetividades dos planos.

Casos

Apagão **- Prejuízos, custos, Backup/Energia**
Incêndios-**Tipos, causas e prejuízos**
Vazamento de informações - **criptografar ?**
Hackerismo – **crimes computacionais**
Violação do Direito Autoral – **prejuízo comercial e reputação**
Espionagem - **monitoração**
Falhas em Sistemas – **qualidade de produtos**
Ataques a servidores – **proteger mais**
Resposta a incidentes - **Conscientização**
Roubo de senhas e de dinheiro (mercado hacker) - **Botnets**
Nível de dependência de externos, de fornecedores de serviços – **custo de hora parada**
Fraudes e seus impactos - **$financeiro$, reputação**
outros …