Gestão e Governança em Segurança da Informação

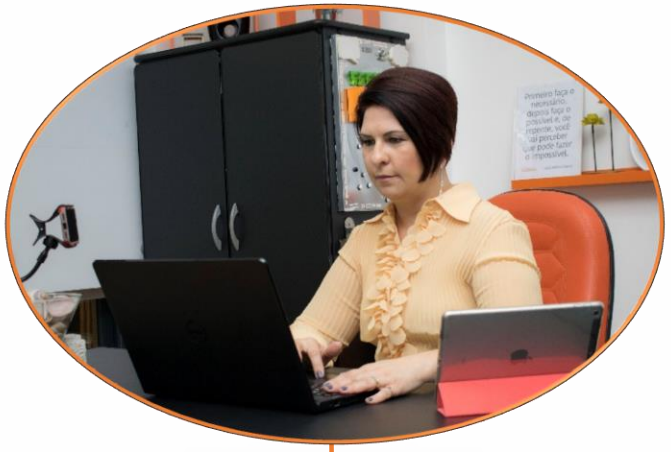
Estrutura da Mentoria

Expectativas

Em uma frase:

- Minha maior dor/dúvida é....

Whoami
Lado A



+ 29 anos de carreira

Estagiária
Assistente
Sênior
Supervisora
Gerente
Gerente Sr.
Diretora
Sócia

MdB, RME, WOMCY
Líder

Palestras e Aulas
em MBA e Pós

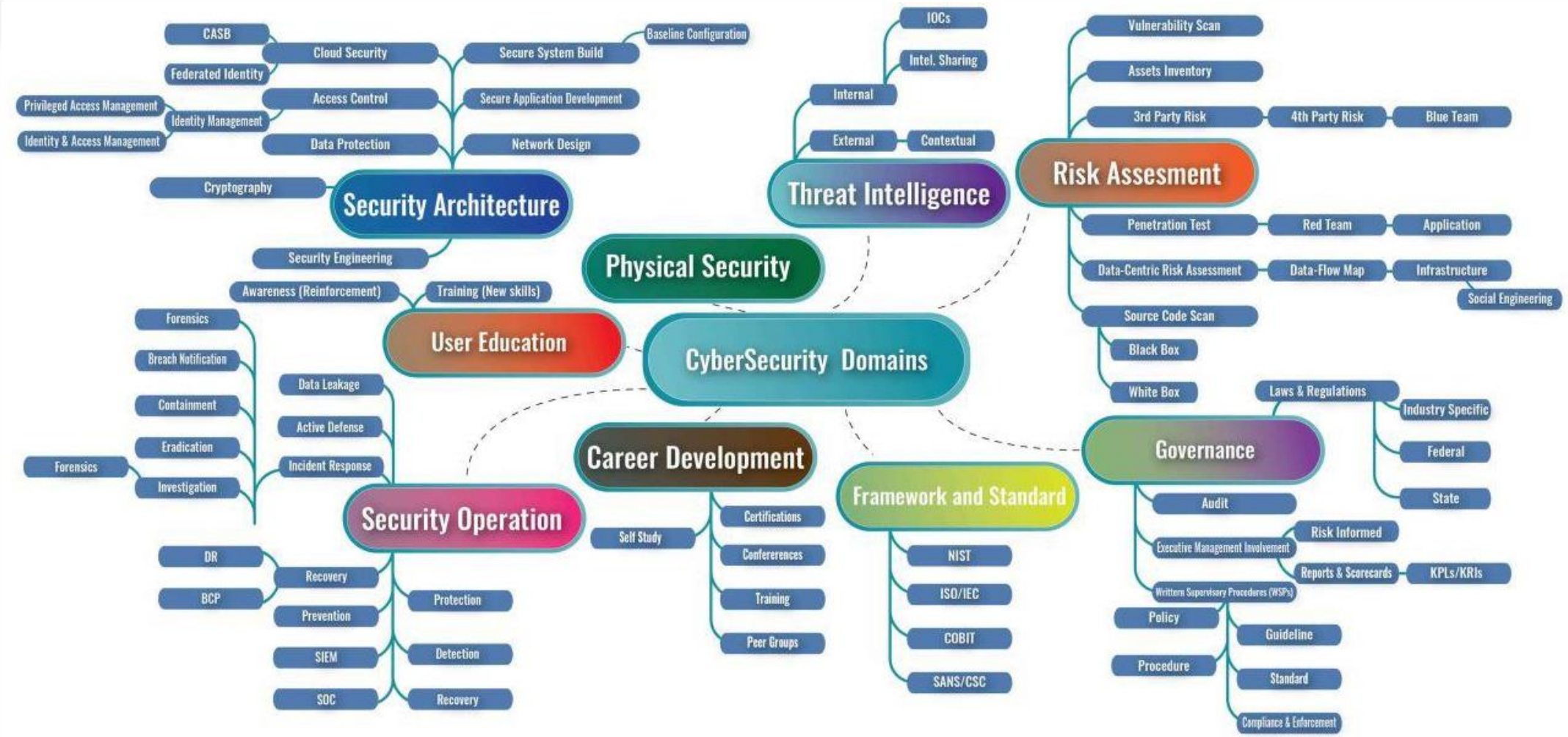
Auditoria, Consultoria,
Mentoria e Treinamento

Whoami
Lado B

Agenda

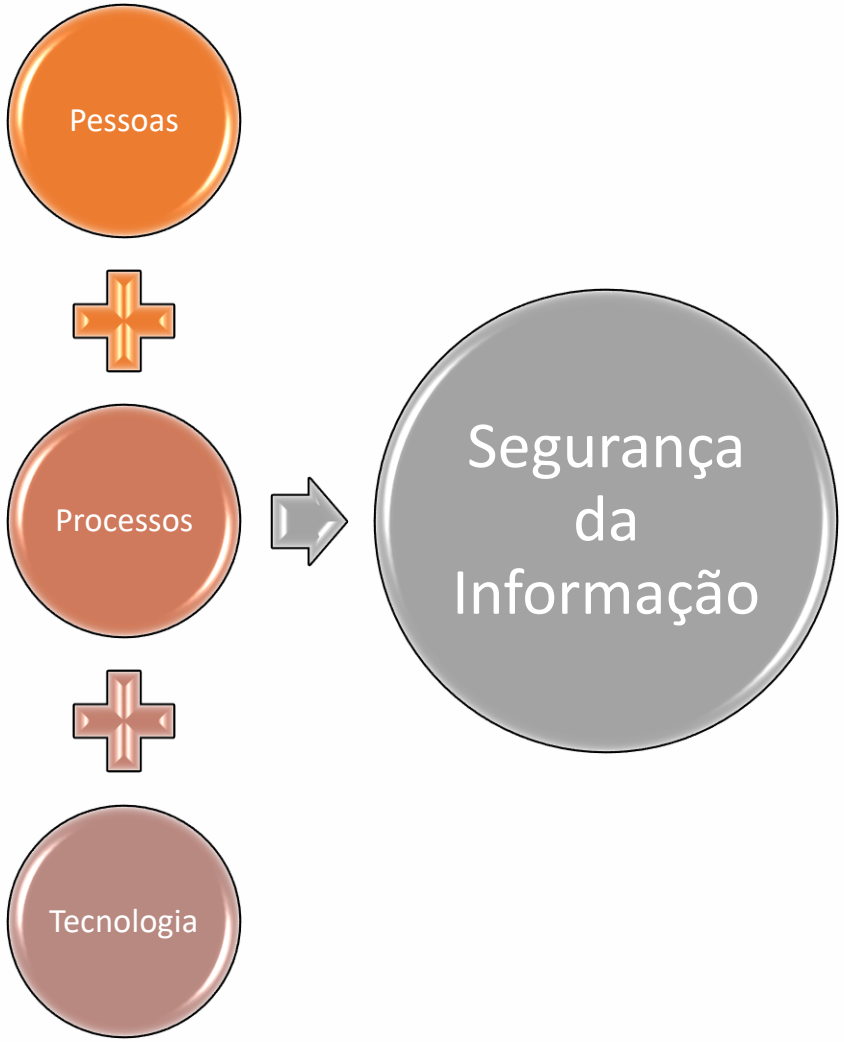
- Warm-up: Segurança da Informação, Cybersecurity e Fundamentos
- Gestão de Segurança da Informação
  - ISO 27001 - SGSI – Sistema de Gestão de Segurança da Informação
- Processos de Segurança da Informação
  - ISO 27002 – Processos de SI
  - Maturidade de processos
- Governança Corporativa e de SI

Domínios de Cybersecurity



Fonte: https://dementium2.com/seguranca-da-informacao/mais-de-35-iniciativas-para-obter-mais-mulheres-em/

Segurança da Informação, Cybersecurity e Fundamentos



- Segurança da Informação (Pessoas, Processos e TI)
- Segurança de TI
- *Cybersecurity*
- Segurança Empresarial
- Segurança Patrimonial
- Privacidade

Segurança da Informação, Cybersecurity e Fundamentos

C onfidencialidade

Informações e ativos protegidos de acesso não autorizado, perda, danos ou uso impróprio.

I ntegridade

Informações protegidas de modificações não autorizadas e que sejam confiáveis e completas.

D isponibilidade

Informações e ativos que as suportam estejam disponíveis para pessoas autorizadas a manuseá-los.

O que proteger?

 Estratégia	 Empresa	 Liderança	 Conselho	 Investidores
 Processos	 Gestores	 Indicadores	 Parceiros	 Profissionais
 Fornecedores	 Clientes	 Riscos	 Ativos	 Tecnologia

10

Segurança da Informação, Cybersecurity e Fundamentos
Ativos

Algo que possui valor para a organização e que portanto necessita de proteção:

- **Serviços:** processamento de dados, comunicação e fornecimento de energia
- **Sistemas computadorizados:** aplicativos, sistemas básicos, ferramentas de desenvolvimento
- **Equipamentos:** computadores, equipamentos de comunicação de dados, mídias (fitas e discos), equipamentos de fornecimento de energia alternativa, cofres
- **Documentos:** contratos, demonstrações financeiras
- **Pessoas:** funcionários, terceiros e clientes
- **Imagem e reputação** da organização
- **Informações** em quaisquer formas

11

Segurança da Informação, Cybersecurity e Fundamentos
Vulnerabilidades

Fraquezas associadas aos ativos da Organização, que caso exploradas por uma ameaça representam risco a Organização:

- Treinamento insuficiente
- Erros de configuração de dispositivos, serviços, etc.
- Falta de monitoração / auditoria
- Políticas de segurança inadequadas
- Segurança física e lógica inadequada
- Baixa conscientização de pessoas
- Vulnerabilidades de software
- Vulnerabilidades da arquitetura
- Vulnerabilidades de aplicações

"Lei do mínimo esforço“

Atacantes geralmente buscam alvos (empresas, processos, pessoas, sistemas) vulneráveis.

12

Segurança da Informação, Cybersecurity e Fundamentos

Ameaças

Agente ou ação que possa explorar as vulnerabilidades resultando em incidentes, que possam causar danos e / ou prejuízos.
Pessoas, códigos, softwares ou eventos de quaisquer tipos.

Motivações:

- Aprendizagem;
- Curiosidade ou busca de emoção;
- Espionagem doméstica ou industrial;
- Ganho financeiro;
- Idealismo;
- Ignorância;
- Necessidade de aceitação ou respeito;
- Vingança;

13

Atacantes e zonas propícias para ameaças

- Muitas vezes os riscos são gerados por nós mesmos
- Somos vulneráveis em áreas julgadas inofensivas

Segurança da Informação, Cybersecurity e Fundamentos

Riscos

Ativo: algo tem que valor para uma organização

Possibilidade de um ativo sujeitar-se a fatores e incidentes que possam resultar em perdas ou danos, comprometendo a continuidade das atividades de uma organização.

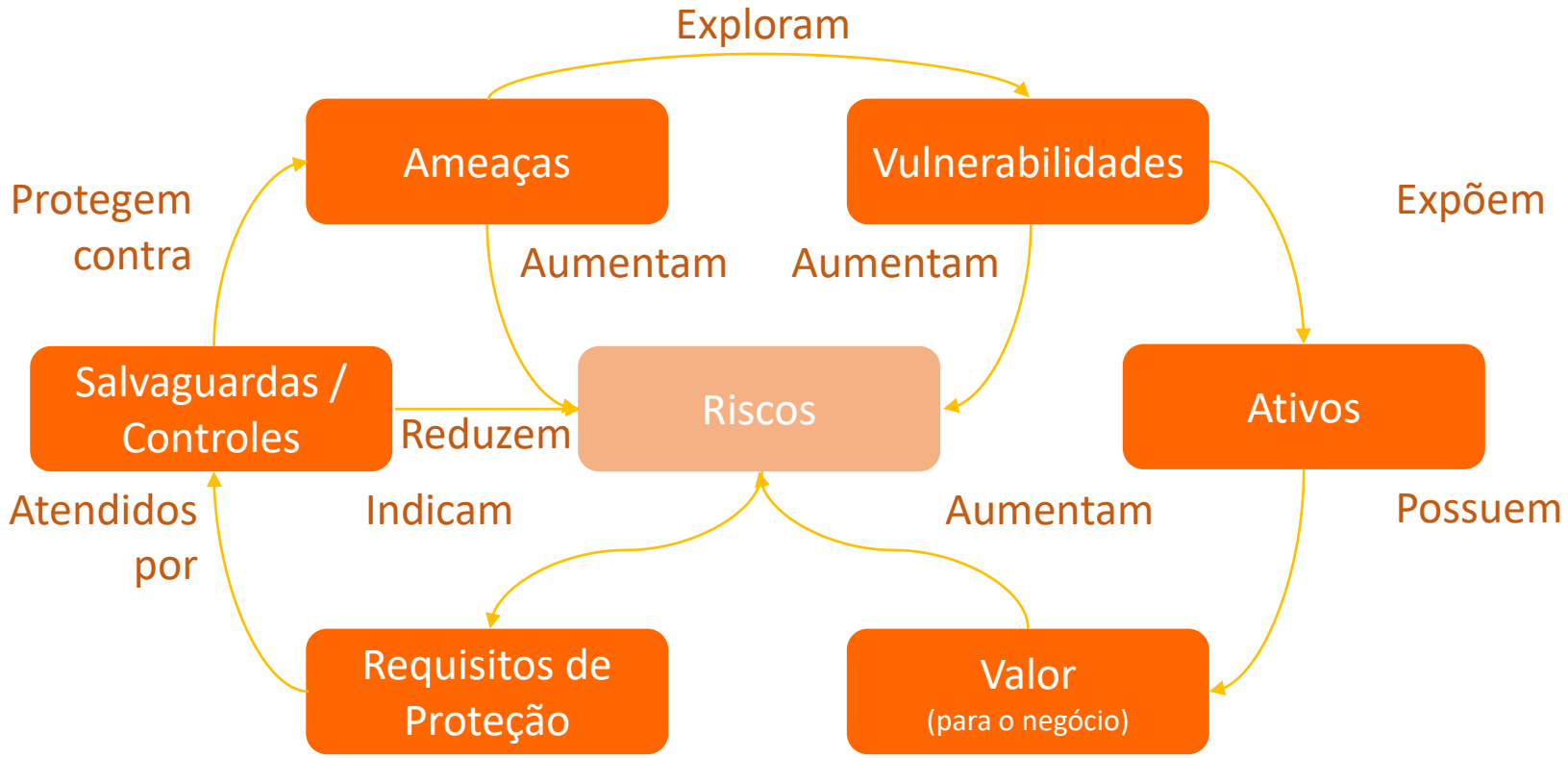
Fatores e Incidentes:
Vulnerabilidades (fraquezas na segurança)
Ameaças (ocorrência de exploração de uma vulnerabilidade)

Perdas ou Danos:
Consequências,
Fraudes e Incidentes

15

Segurança da Informação, Cybersecurity e Fundamentos

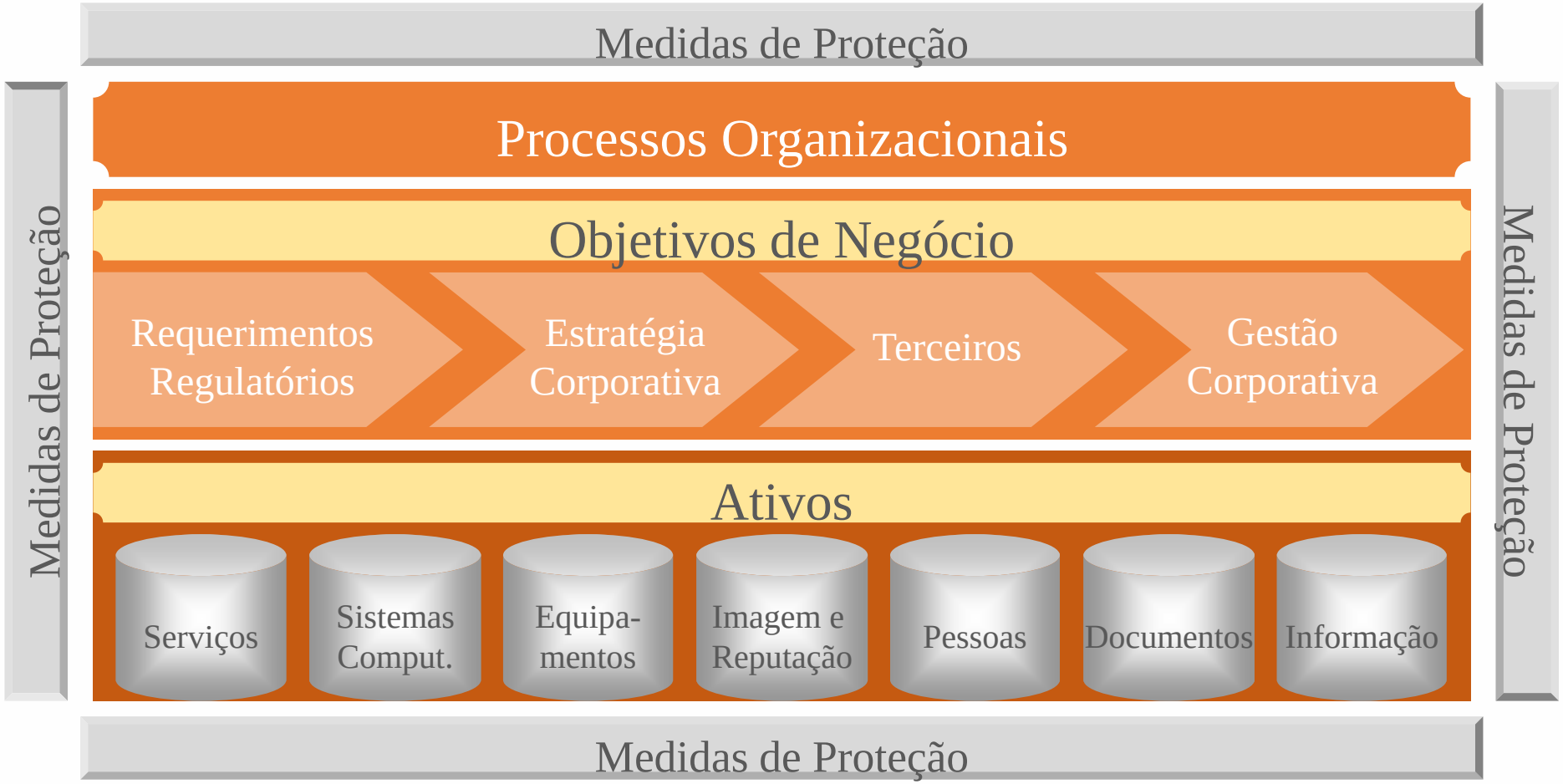
Riscos



16

Segurança da Informação, Cybersecurity e Fundamentos

Segurança Associada ao Negócio



Segurança da Informação, Cybersecurity e Fundamentos

Segurança Associada ao Negócio

Gestão de Segurança da Informação

ISO 27001

ISO/IEC 27001

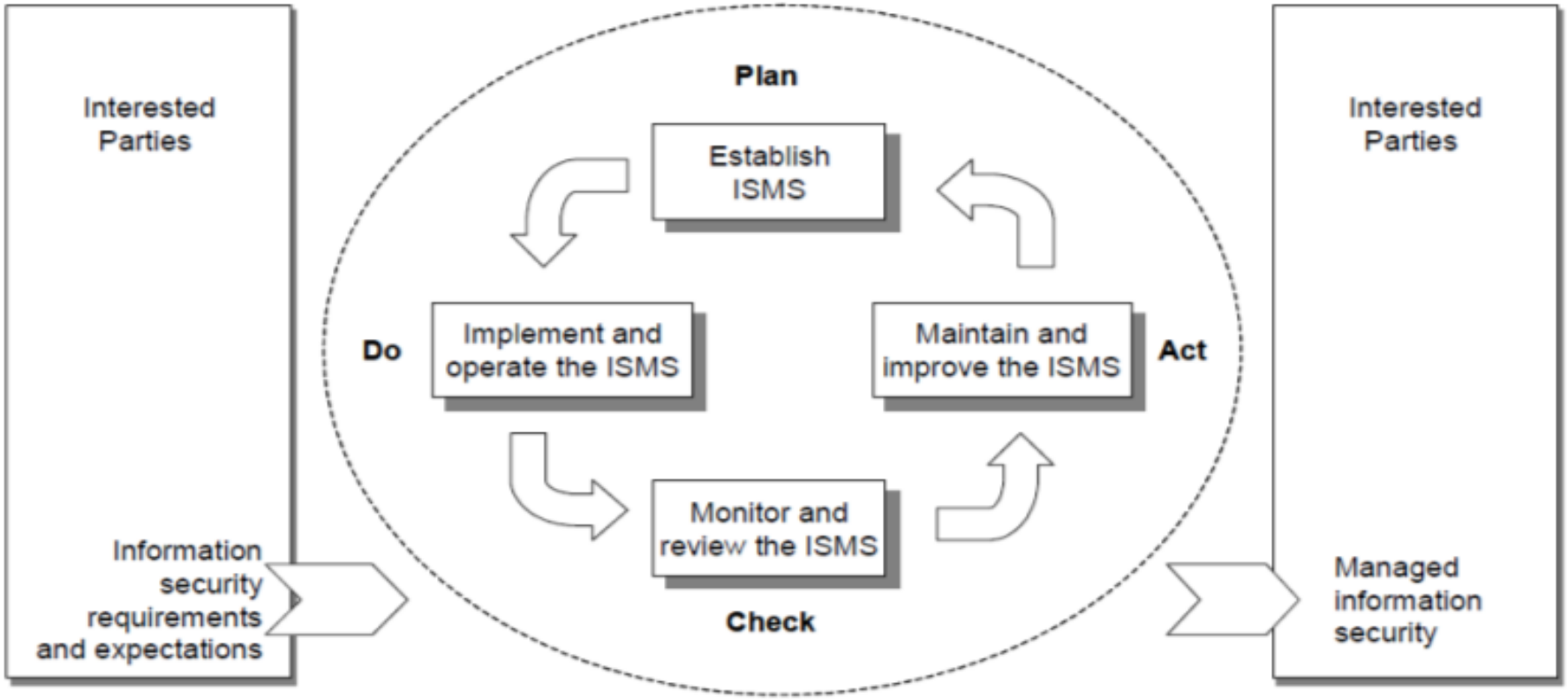


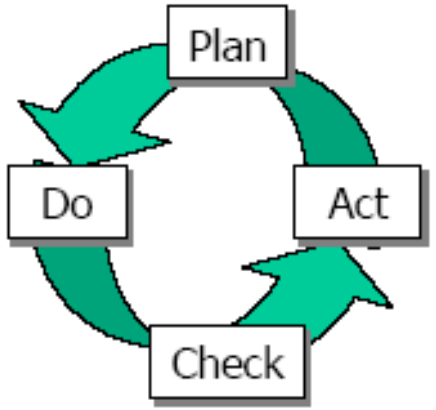
Figure 1 — PDCA model applied to ISMS processes

Fonte: *ISO 27001:2013*

Gestão de Segurança da Informação

ISO 27001

- Define ISMS Scope and policy
- Define a systematic approach to risk assessment
- Identify the risks
- Apply the systematic approach for assessing the risks
- Identify and evaluate options for the treatment of risks
- Select control objectives and controls for the treatment of risks



- Implement a specific management programme
- Implement controls that have been selected
- Manage operations
- Manage resources
- Implement procedures and other control processes

- Measure performance of the ISMS
- Identify improvements in the ISMS and effectively implement them.
- Take appropriate corrective and preventive actions.
- Communicate the results and actions and consult with all parties involved.
- Revise the ISMS where necessary.
- Ensure that the revisions achieve their intended objectives.

- Execute procedures to and other controls (e.g. to detect errors, identify failed and successful breaches)
- Undertake regular reviews of the effectiveness of the ISMS
- Review the level of residual risk and acceptable risk
- Execute the management procedures
- Undertake a formal review of its ISMS on a regular basis
- Record and report all actions and events

Fonte: *ISO 27001:2013*

Processos de Segurança da Informação

ISO 27002

ISO 27002

5 Política de Segurança da Informação	6 Organizando a Segurança da Informação	7 Gerenciamento de Ativos	8 Segurança em Recursos Humanos	9 Controle de Acesso
10 Criptografia	11 Segurança Física e do Ambiente	12 Segurança das Operações	13 Comunicação de Segurança	14 Aquisição, Desenvolvimento e Manutenção de SI
15 Relacionamento com Fornecedor	16 Gerenciamento de Incidentes de SI	17 Aspectos da segurança da informação no BCM	18 Conformidade	

Fonte: *ISO 27002:2013*

Processos de Segurança da Informação

Maturidade de Processos

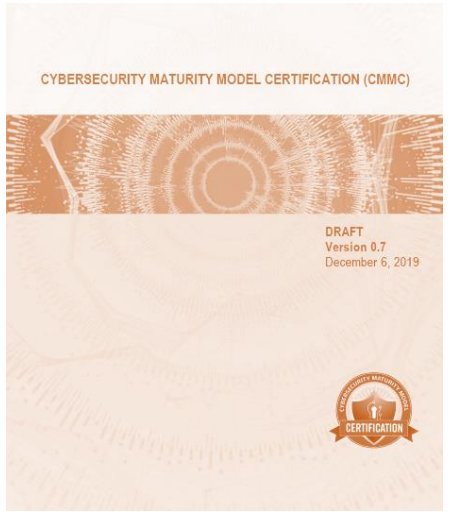


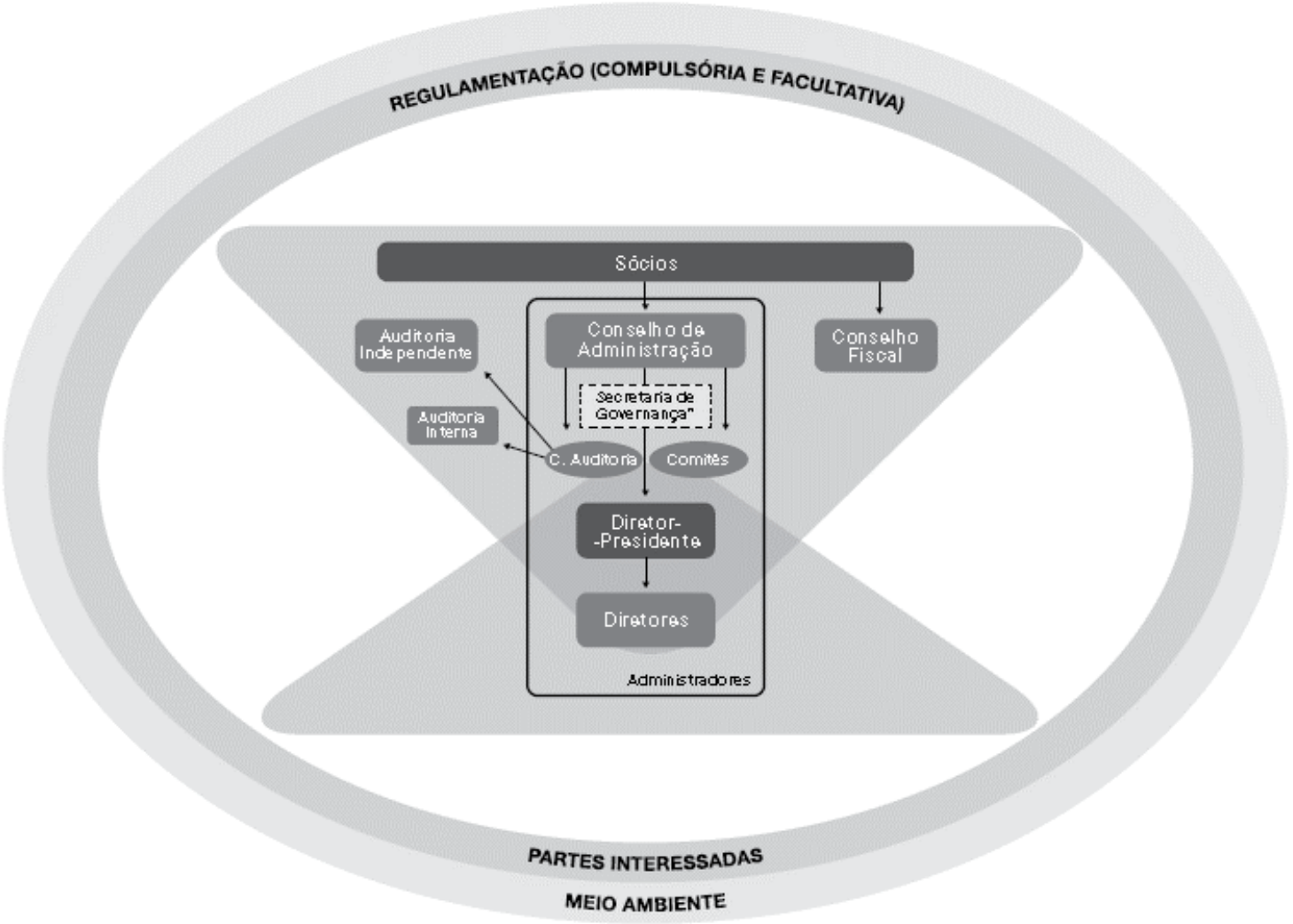
Table 3. Processes for each CMMC Maturity Level (ML)

Process Maturity Level	Processes
ML 1: Performed	*There are no maturity processes assessed at ML 1. A Level 1 organization performs Level 1 practices but does not exhibit process institutionalization.*
ML 2: Documented	1. Establish a policy that includes [DOMAIN NAME]. 2. Establish practices to implement the [DOMAIN NAME] policy. 3. Establish a plan that includes [DOMAIN NAME].
ML 3: Managed	1. Review [DOMAIN NAME] activities for adherence to policy and practices. 2. Provide adequate resources to meet the plan for [DOMAIN NAME] activities.
ML 4: Reviewed	1. Review and measure [DOMAIN NAME] activities for effectiveness. 2. Review the status and results of [DOMAIN NAME] activities with higher level management and resolve issues.
ML 5: Optimized	1. Standardize a documented approach for [DOMAIN NAME] across all applicable organizational units. 2. Share identified improvements to [DOMAIN NAME] activities across the organization.

Fonte: *Cybersecurity Maturity Model Certification (CMMC) – Carnegie Mellon University and Johns Hopkins University*

GOVERNANÇA CORPORATIVA E SI

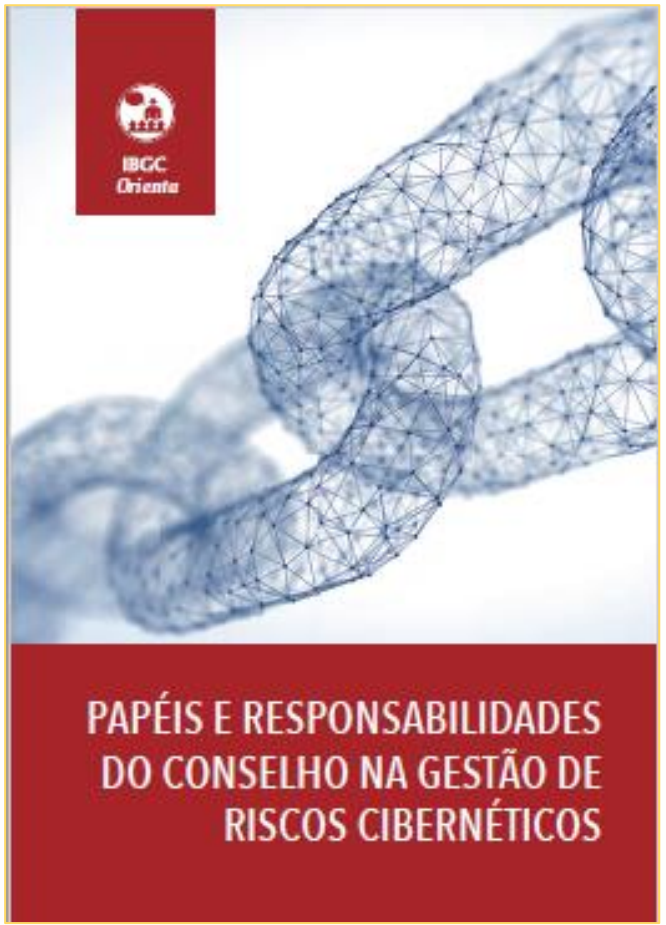
IBGC - Código das Melhores Práticas de Governança Corporativa



Comitês normalmente instituídos:

- **auditoria;**
- **finanças;**
- **pessoas;**
- **riscos;**
- **sustentabilidade.**

Papéis e Responsabilidades do Conselho na Gestão de Riscos Cibernéticos



... a gestão do risco cibernético deve ser uma **preocupação constante** dos **conselheiros** de administração, uma vez que ela tem **implicações na sustentabilidade** das empresas.

Ao conselho, **cabe supervisionar a gestão de riscos cibernéticos e a salvaguarda dos ativos** da empresa, evitando perdas de todos os tipos e danos à reputação...

ISO 27014 – Governança de SI

ISO/IEC 27001

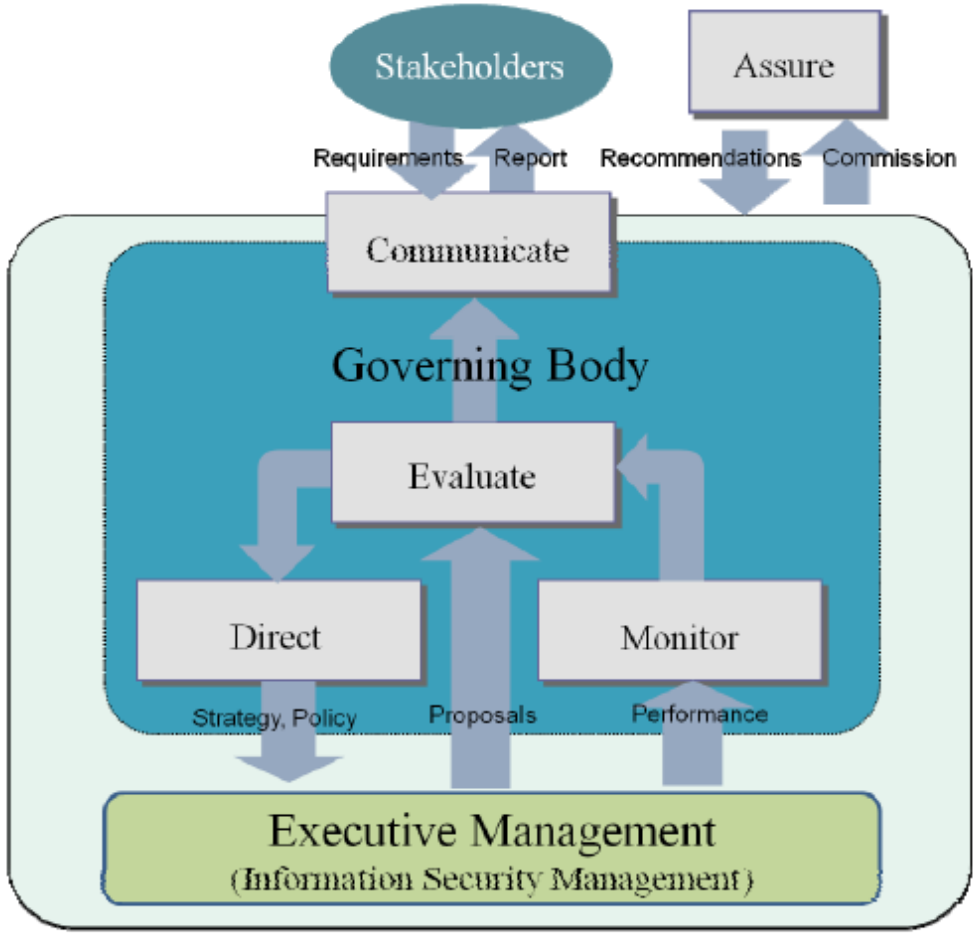
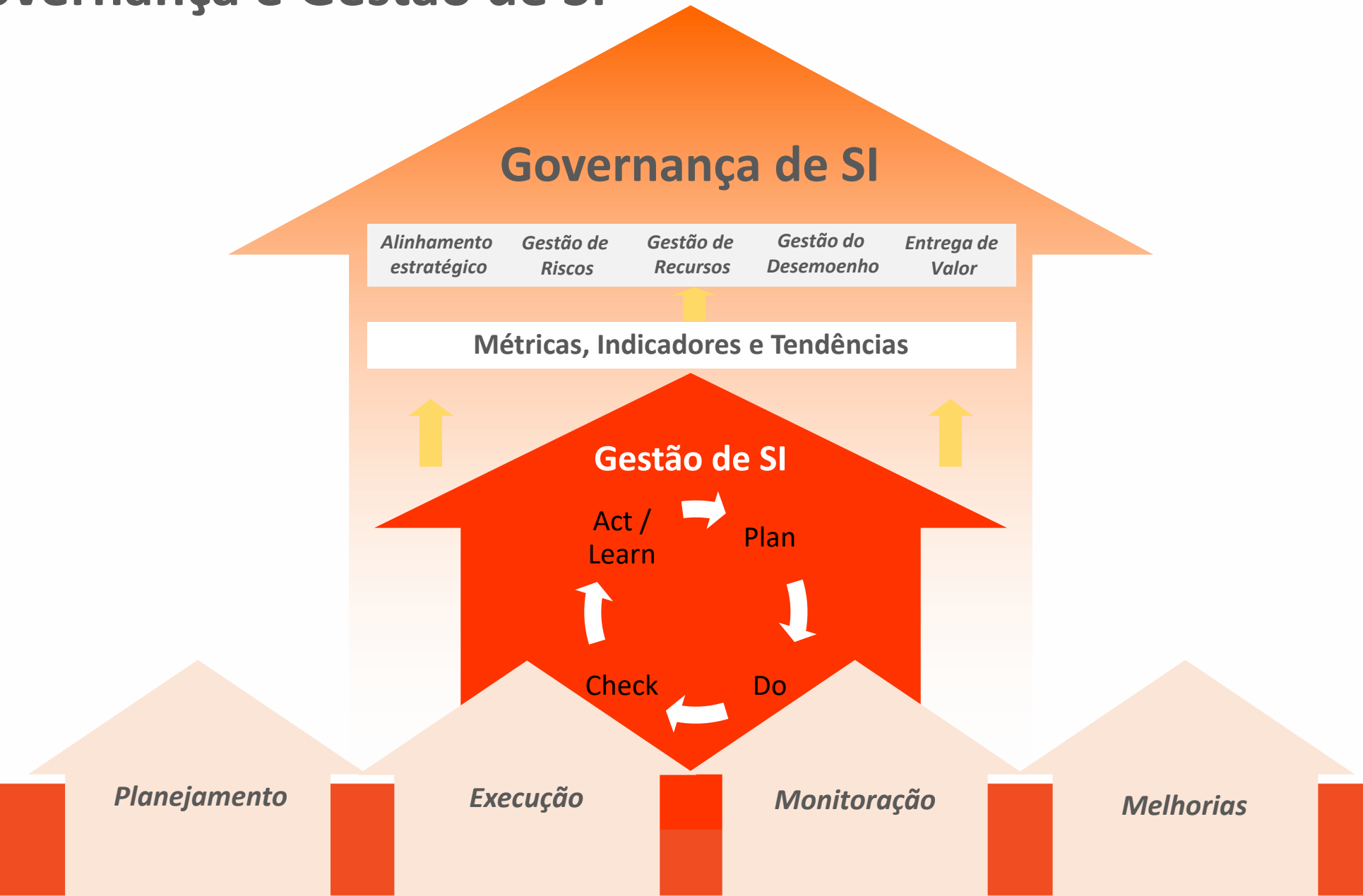


Figure 2 — Implementation of the governance model for information security

Governança e Gestão de SI



Disciplinas de Governança de SI

Alinhamento estratégico de SI com a estratégia do negócio para suportar os seus objetivos

Gestão de riscos com medidas para redução dos riscos a níveis aceitáveis

Gestão de recursos pelo uso do conhecimento e infra-estrutura de SI de forma eficiente e eficaz

Gestão do desempenho e através da mensuração, monitoração e reporte das métricas e indicadores de SI

Entrega de valor pela otimização de investimentos em SI suportando os objetivos organizacionais

Obrigad@!

athome@womcy.org
www.cybersecuritygirls.io

Processos de Segurança da Informação

ISO 27002

Fonte: *ISO 27002:2013*

Processos de Segurança da Informação

ISO 27002

Fonte: *ISO 27002:2013*

Processos de Segurança da Informação

ISO 27002

Fonte: *ISO 27002:2013*

Processos de Segurança da Informação

ISO 27002

Fonte: *ISO 27002:2013*

Processos de Segurança da Informação

ISO 27002

Fonte: *ISO 27002:2013*

Processos de Segurança da Informação

ISO 27002

Fonte: *ISO 27002:2013*

Processos de Segurança da Informação

ISO 27002

Fonte: *ISO 27002:2013*

Processos de Segurança da Informação

ISO 27002

Fonte: *ISO 27002:2013*