

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



MdB, RME, WOMCY
Líder



Palestras e Aulas
em MBA e Pós



Auditoria, Consultoria,
Mentoria e Treinamento



Estagiária
Assistente
Sênior
Supervisora
Gerente
Gerente Sr.
Diretora
Sócia



Cyber Security Girls



Whoami
Lado B

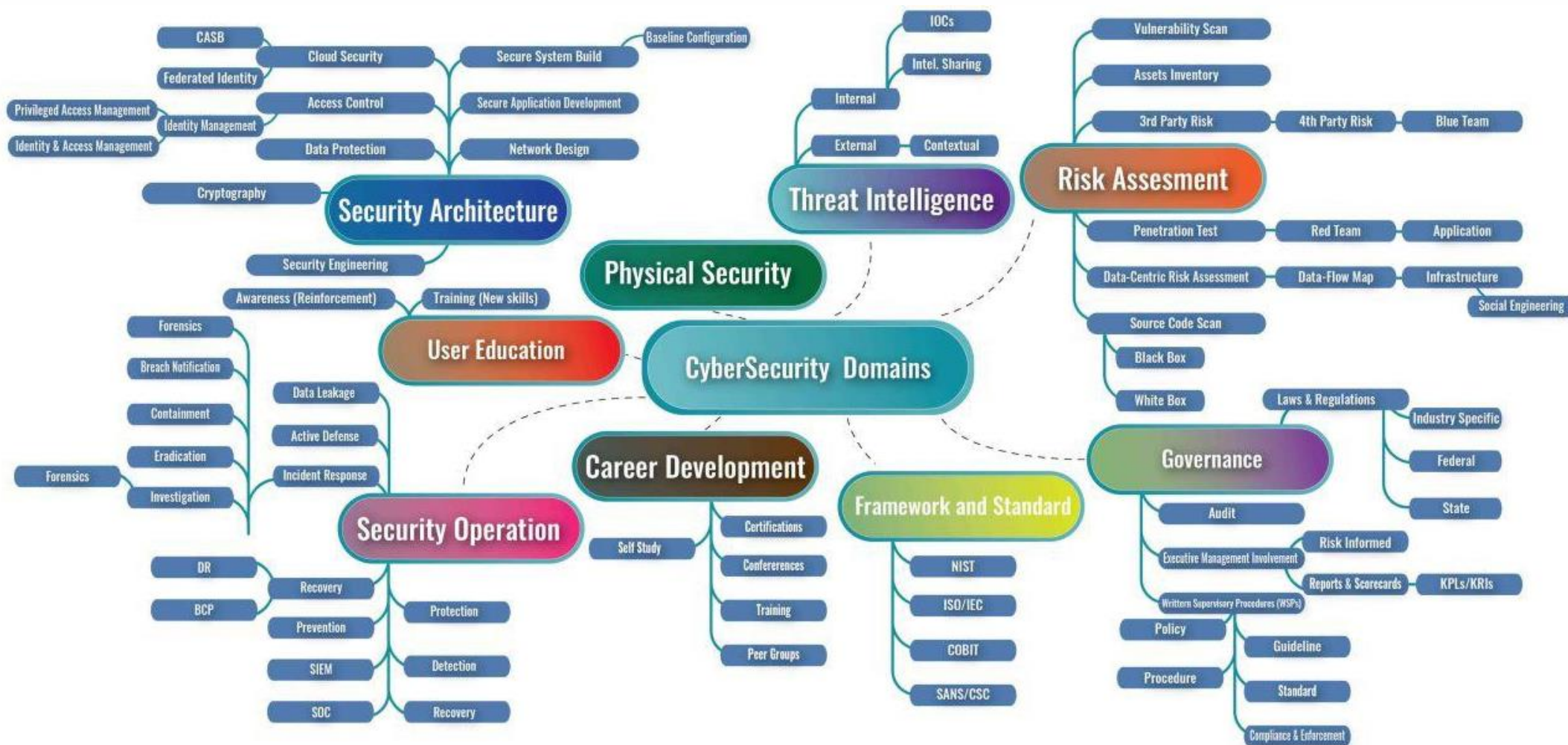


Agenda

- 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

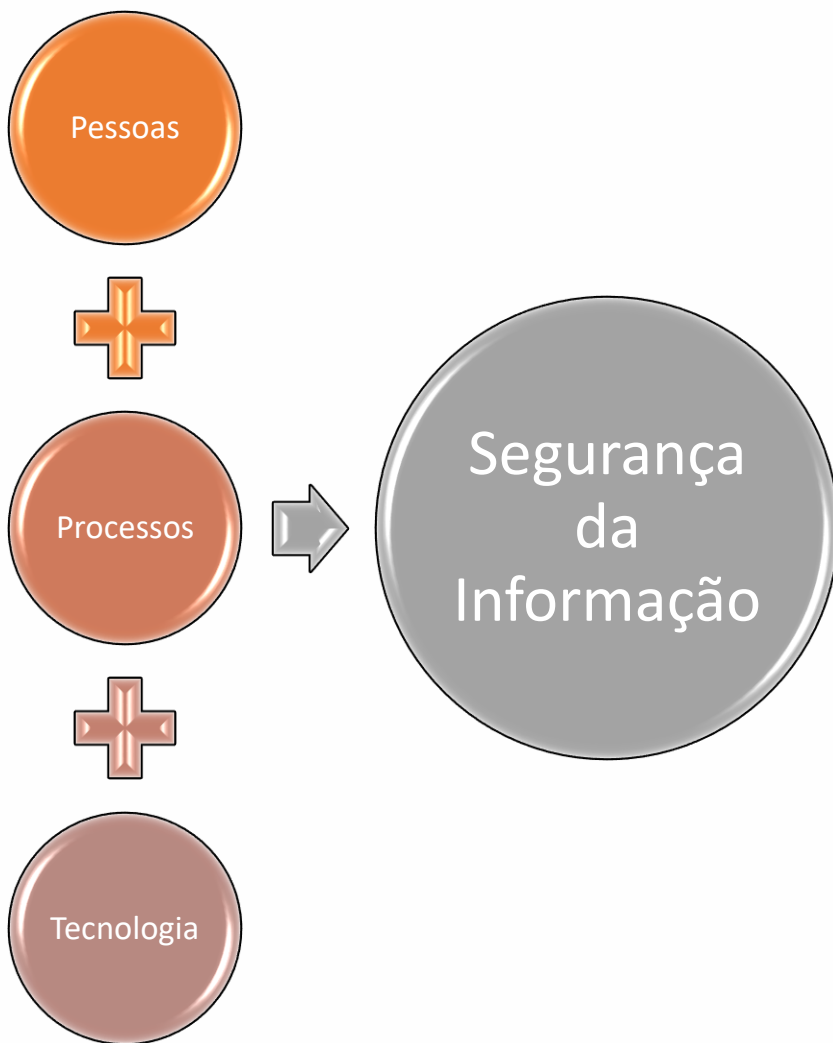


Domínios de Cybersecurity





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



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



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.



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;



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)

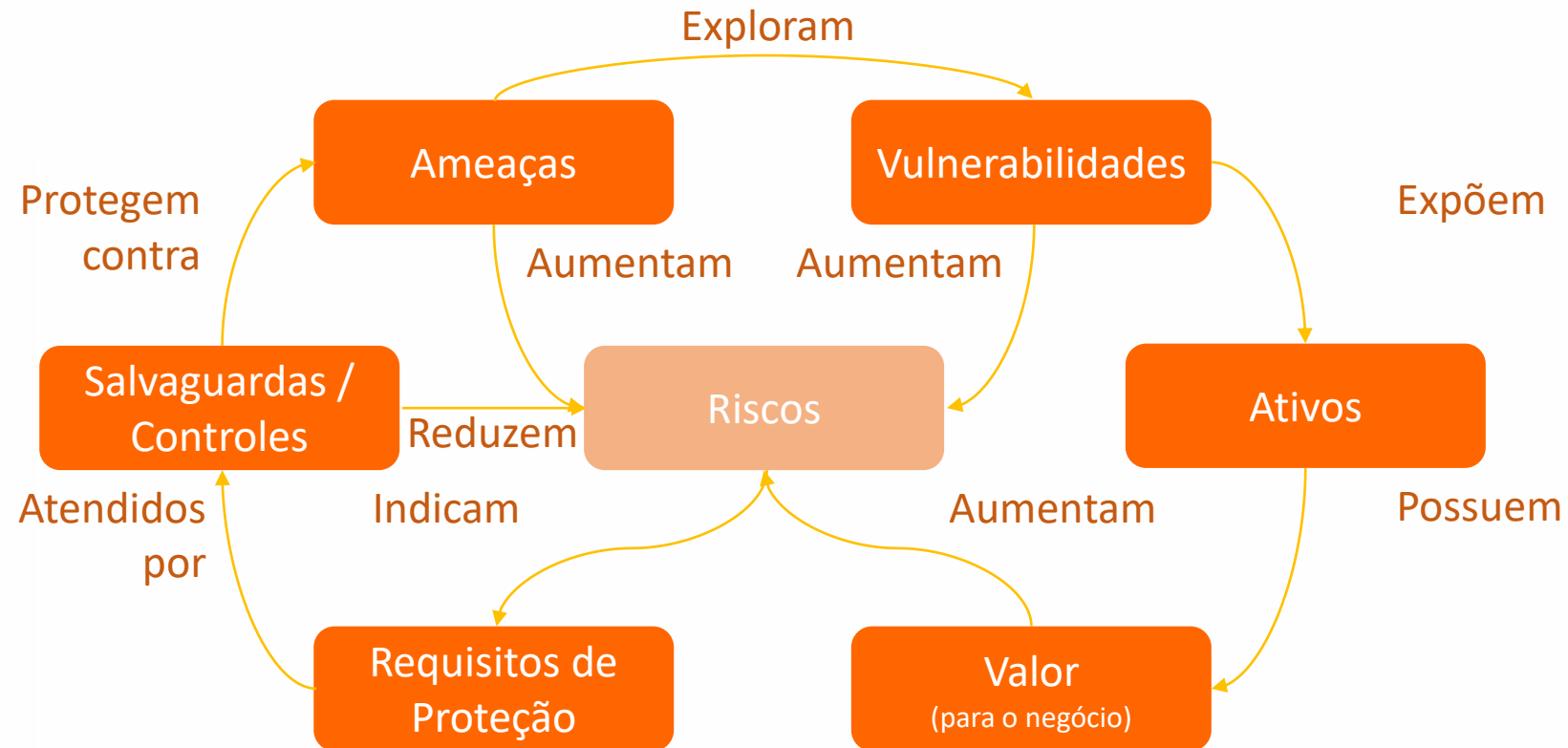
Ameaças (ocorrência de exploração de uma vulnerabilidade)

Perdas ou Danos:

Consequências,
Fraudes e Incidentes

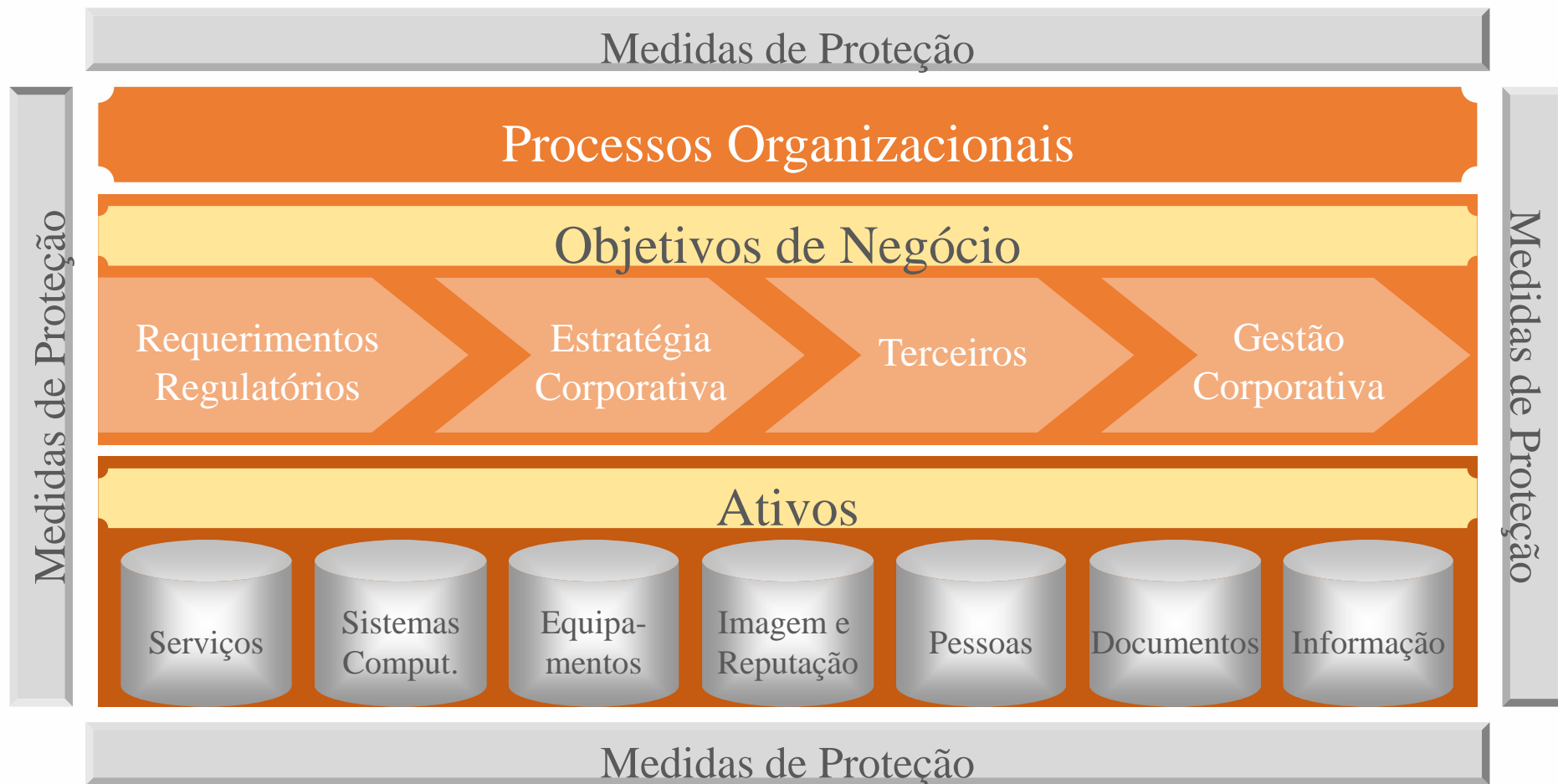


Segurança da Informação, Cybersecurity e Fundamentos *Riscos*





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

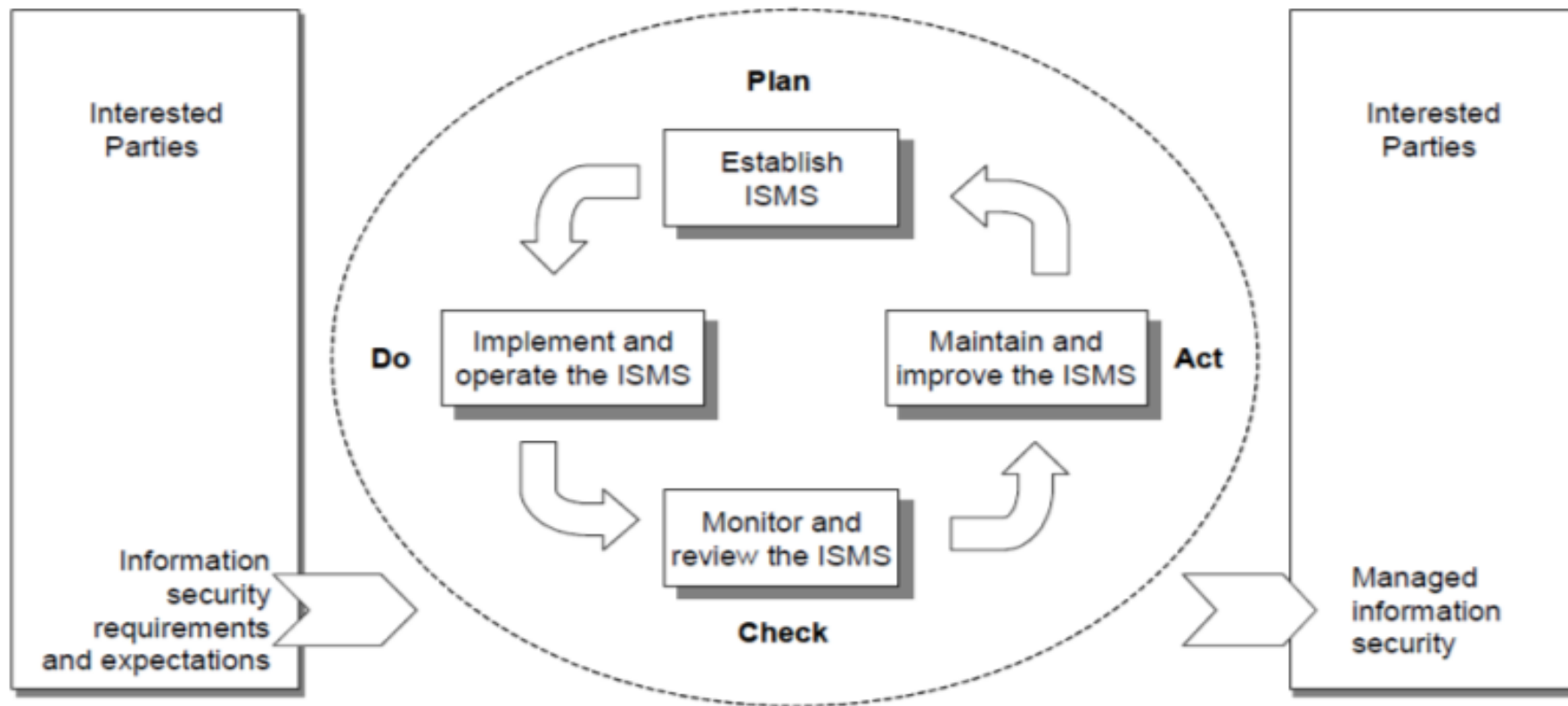
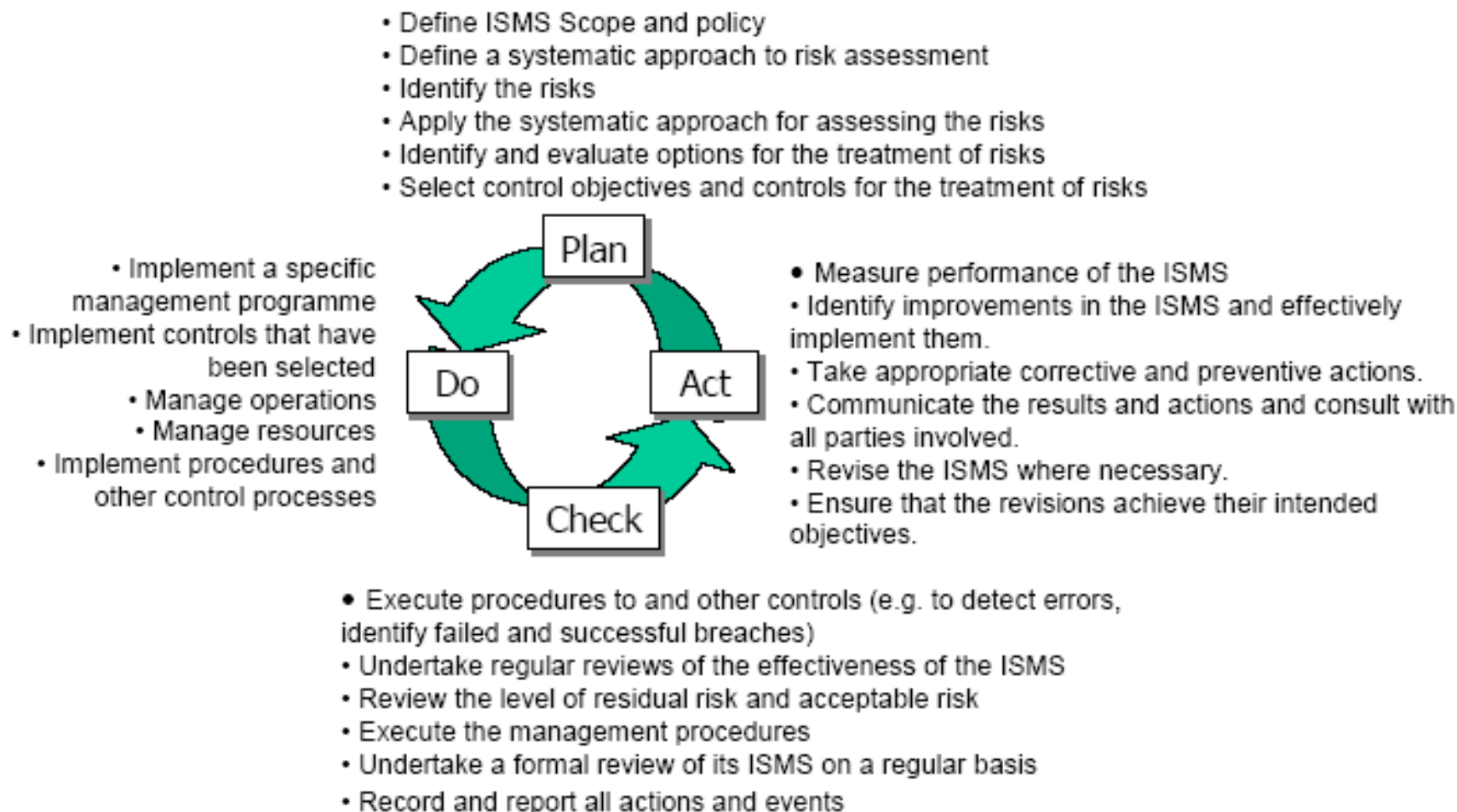


Figure 1 — PDCA model applied to ISMS processes



Gestão de Segurança da Informação ISO 27001





Processos de Segurança da Informação 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



Processos de Segurança da Informação

Maturidade de Processos

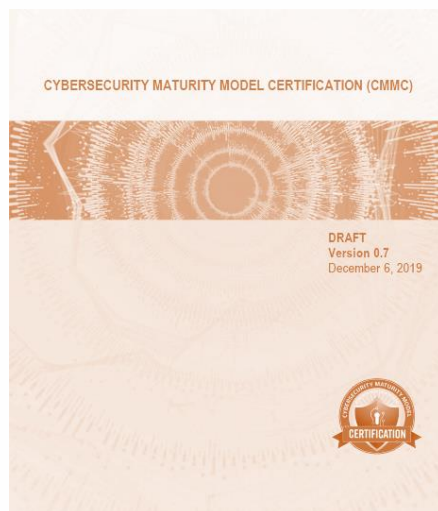


Table 3. Processes for each CMMC Maturity Level (ML)

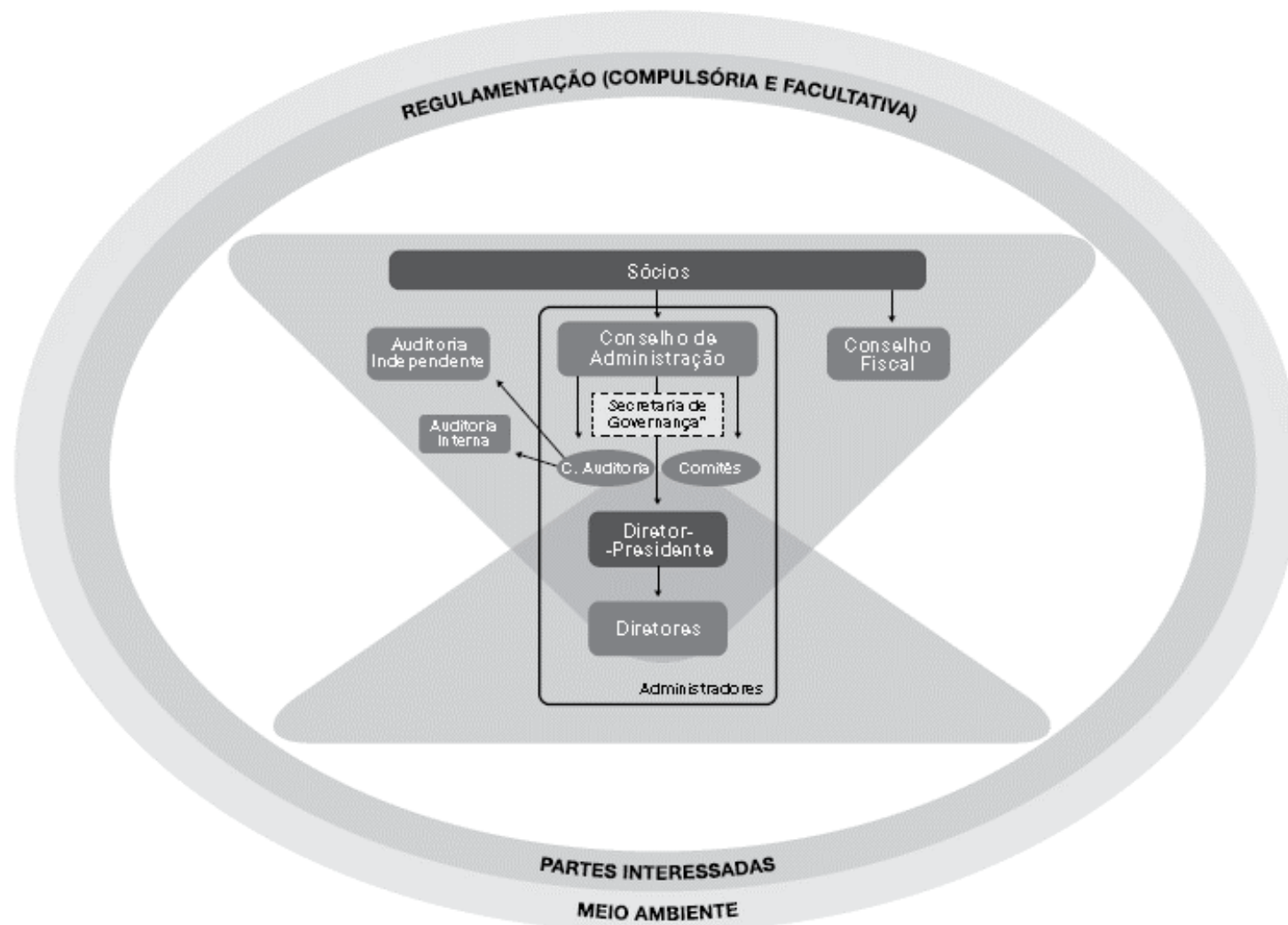
| Process Maturity Level | Processes |
|------------------------|--|
| ML 1: Performed | <i>There are no maturity processes assessed at ML 1. A Level 1 organization performs Level 1 practices but does not exhibit process institutionalization.</i> |
| ML 2: Documented | <ol style="list-style-type: none">1. 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 | <ol style="list-style-type: none">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 | <ol style="list-style-type: none">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 | <ol style="list-style-type: none">1. Standardize a documented approach for [DOMAIN NAME] across all applicable organizational units.2. Share identified improvements to [DOMAIN NAME] activities across the organization. |



GOVERNANÇA CORPORATIVA E SI



IBGC - Código das Melhores Práticas de Governança Corporativa

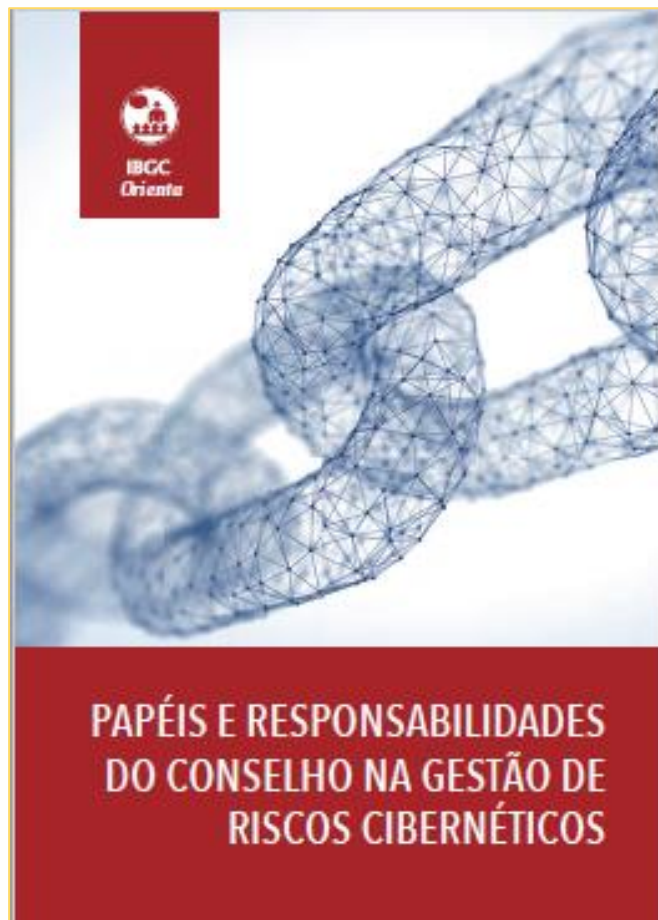


Comitês normalmente instituídos:

- 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

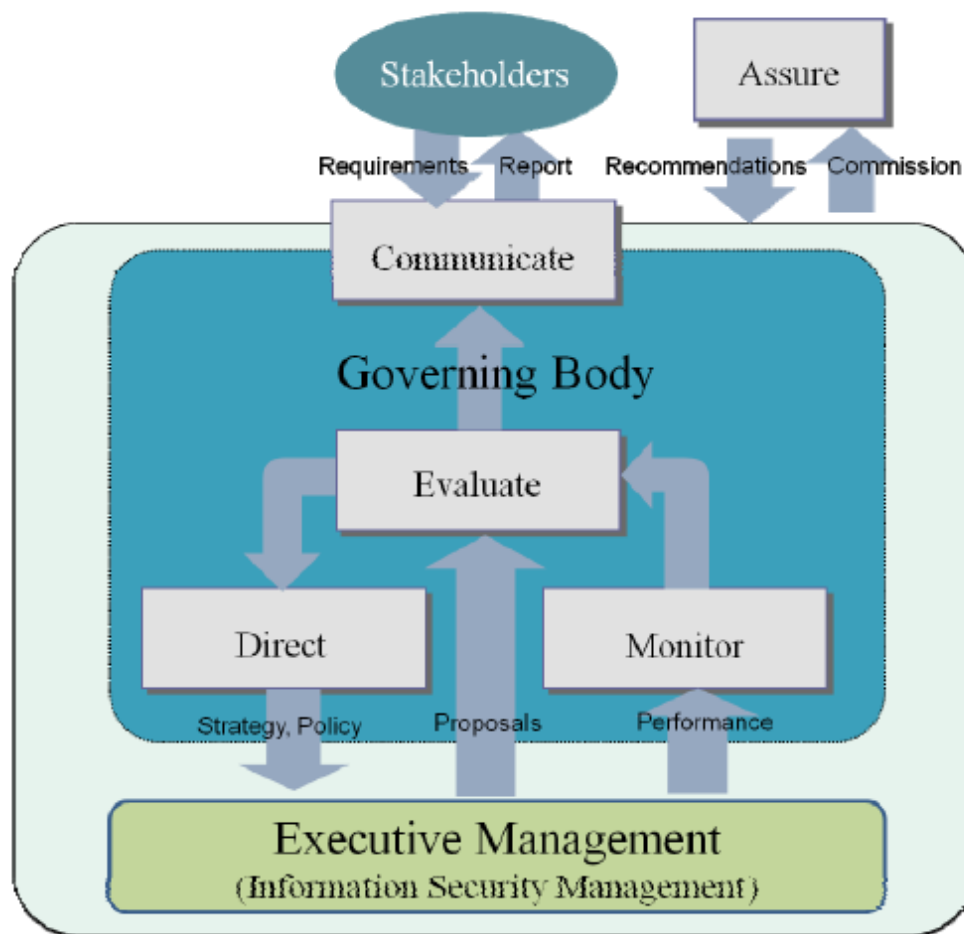
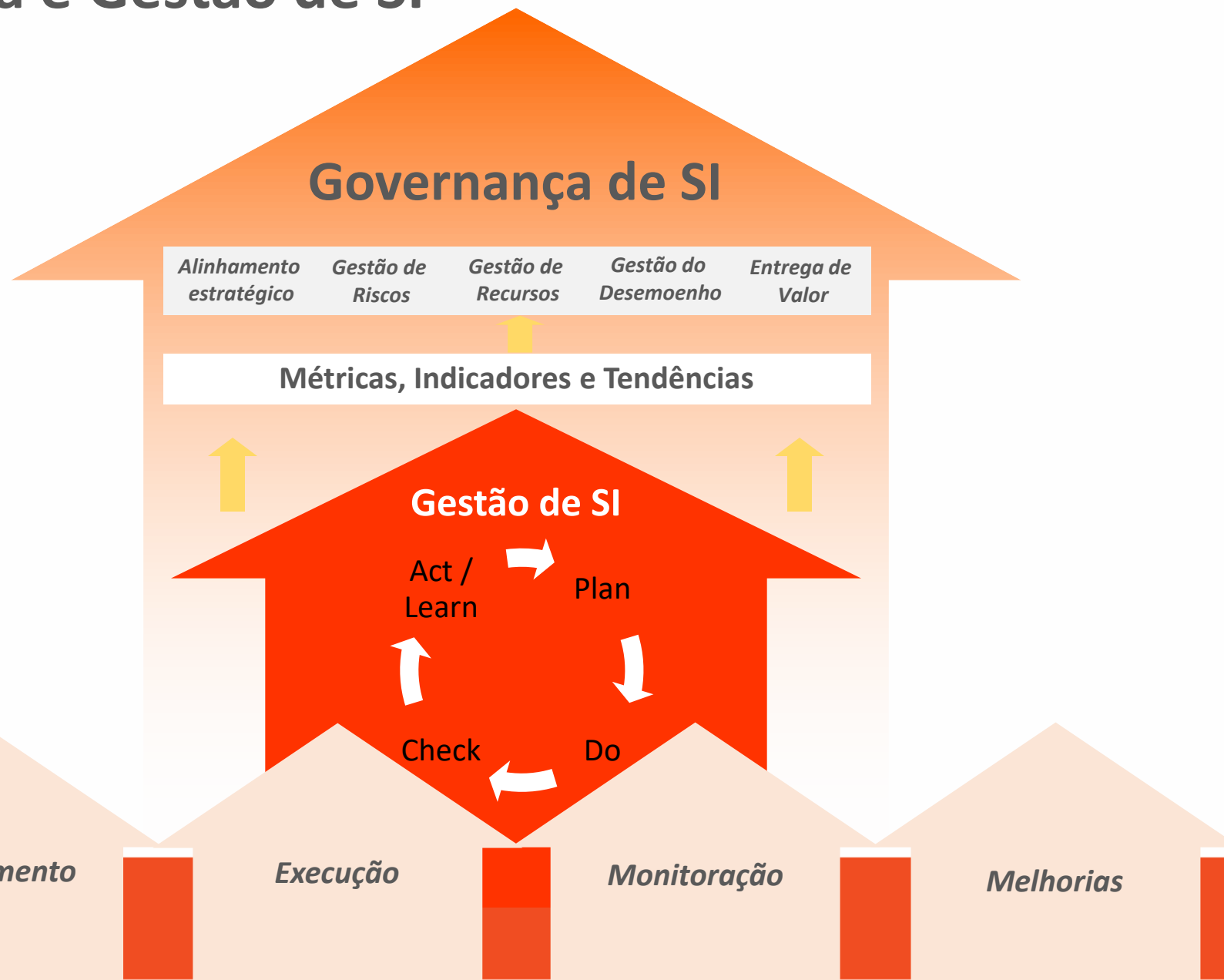


Figure 2 — Implementation of the governance model for information security



Governança e Gestão de SI





Disciplinas de Governança de SI

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



Obrigad@!

athome@womcy.org

www.cybersecuritygirls.io



Processos de Segurança da Informação

ISO 27002

| | |
|-------|--|
| 5 | Políticas de segurança da informação |
| 5.1 | Orientação da direção para segurança da informação |
| 5.1.1 | Políticas para segurança da informação..... |
| 5.1.2 | Análise crítica das políticas para segurança da informação |
| 6 | Organização da segurança da informação |
| 6.1 | Organização interna |
| 6.1.1 | Responsabilidades e papéis pela segurança da informação |
| 6.1.2 | Segregação de funções |
| 6.1.3 | Contato com autoridades |
| 6.1.4 | Contato com grupos especiais |
| 6.1.5 | Segurança da informação no gerenciamento de projetos |
| 6.2 | Dispositivos móveis e trabalho remoto |
| 6.2.1 | Política para o uso de dispositivo móvel |
| 6.2.2 | Trabalho remoto |
| 7 | Segurança em recursos humanos..... |
| 7.1 | Antes da contratação |
| 7.1.1 | Seleção |
| 7.1.2 | Termos e condições de contratação |
| 7.2 | Durante a contratação |
| 7.2.1 | Responsabilidades da Direção |
| 7.2.2 | Conscientização, educação e treinamento em segurança da informação |
| 7.2.3 | Processo disciplinar |
| 7.3 | Encerramento e mudança da contratação |
| 7.3.1 | Responsabilidades pelo encerramento ou mudança da contratação..... |



| | |
|-------|--|
| 8 | Gestão de ativos..... |
| 8.1 | Responsabilidade pelos ativos |
| 8.1.1 | Inventário dos ativos..... |
| 8.1.2 | Proprietário dos ativos |
| 8.1.3 | Uso aceitável dos ativos..... |
| 8.1.4 | Devolução de ativos |
| 8.2 | Classificação da informação |
| 8.2.1 | Classificação da informação |
| 8.2.2 | Rótulos e tratamento da informação |
| 8.2.3 | Tratamento dos ativos |
| 8.3 | Tratamento de mídias |
| 8.3.1 | Gerenciamento de mídias removíveis |
| 8.3.2 | Descarte de mídias..... |
| 8.3.3 | Transferência física de mídias |
| 9 | Controle de acesso |
| 9.1 | Requisitos do negócio para controle de acesso |
| 9.1.1 | Política de controle de acesso |
| 9.1.2 | Acesso às redes e aos serviços de rede |
| 9.2 | Gerenciamento de acesso do usuário |
| 9.2.1 | Registro e cancelamento de usuário..... |
| 9.2.2 | Provisionamento para acesso de usuário |
| 9.2.3 | Gerenciamento de direitos de acesso privilegiados |
| 9.2.4 | Gerenciamento da informação de autenticação secreta de usuários..... |
| 9.2.5 | Análise crítica dos direitos de acesso de usuário |
| 9.2.6 | Retirada ou ajuste dos direitos de acesso |
| 9.3 | Responsabilidades dos usuários |
| 9.3.1 | Uso da informação de autenticação secreta |
| 9.4 | Controle de acesso ao sistema e à aplicação |
| 9.4.1 | Restrição de acesso à informação |
| 9.4.2 | Procedimentos seguros de entrada no sistema (log-on) |



Processos de Segurança da Informação

ISO 27002

| | |
|--------|--|
| 9.4.3 | Sistema de gerenciamento de senha |
| 9.4.4 | Uso de programas utilitários privilegiados |
| 9.4.5 | Controle de acesso ao código-fonte de programas..... |
| 10 | Criptografia |
| 10.1 | Controles criptográficos..... |
| 10.1.1 | Política para o uso de controles criptográficos |
| 10.1.2 | Gerenciamento de chaves |
| 11 | Segurança física e do ambiente..... |
| 11.1 | Áreas seguras..... |
| 11.1.1 | Perímetro de segurança física |
| 11.1.2 | Controles de entrada física |
| 11.1.3 | Segurança em escritórios, salas e instalações |
| 11.1.4 | Proteção contra ameaças externas e do meio ambiente..... |
| 11.1.5 | Trabalhando em áreas seguras..... |
| 11.1.6 | Áreas de entrega e de carregamento |
| 11.2 | Equipamento..... |



Processos de Segurança da Informação

ISO 27002

| | |
|--------|---|
| 11.2.1 | Localização e proteção do equipamento |
| 11.2.2 | Utilidades |
| 11.2.3 | Segurança do cabeamento..... |
| 11.2.4 | Manutenção dos equipamentos..... |
| 11.2.5 | Remoção de ativos..... |
| 11.2.6 | Segurança de equipamentos e ativos fora das dependências da organização |
| 11.2.7 | Reutilização ou descarte seguro de equipamentos..... |
| 11.2.8 | Equipamento de usuário sem monitoração..... |
| 11.2.9 | Política de mesa limpa e tela limpa |
| 12 | Segurança nas operações |
| 12.1 | Responsabilidades e procedimentos operacionais..... |
| 12.1.1 | Documentação dos procedimentos de operação |
| 12.1.2 | Gestão de mudanças |
| 12.1.3 | Gestão de capacidade |
| 12.1.4 | Separação dos ambientes de desenvolvimento, teste e produção |
| 12.2 | Proteção contra <i>malware</i> |
| 12.2.1 | Controles contra <i>malware</i> |
| 12.3 | Cópias de segurança |
| 12.3.1 | Cópias de segurança das informações..... |
| 12.4 | Registros e monitoramento..... |
| 12.4.1 | Registros de eventos |
| 12.4.2 | Proteção das informações dos registros de eventos (<i>logs</i>) |
| 12.4.3 | Registros de eventos (<i>log</i>) de administrador e operador..... |
| 12.4.4 | Sincronização dos relógios..... |
| 12.5 | Controle de <i>software</i> operacional |
| 12.5.1 | Instalação de <i>software</i> nos sistemas operacionais..... |



Processos de Segurança da Informação ISO 27002

| | |
|--------|---|
| 12.6 | Gestão de vulnerabilidades técnicas |
| 12.6.1 | Gestão de vulnerabilidades técnicas |
| 12.6.2 | Restrições quanto à instalação de <i>software</i> |
| 12.7 | Considerações quanto à auditoria de sistemas da informação |
| 12.7.1 | Controles de auditoria de sistemas de informação |
| 13 | Segurança nas comunicações |
| 13.1 | Gerenciamento da segurança em redes |
| 13.1.1 | Controles de redes |
| 13.1.2 | Segurança dos serviços de rede |
| 13.1.3 | Segregação de redes |
| 13.2 | Transferência de informação |
| 13.2.1 | Políticas e procedimentos para transferência de informações |
| 13.2.2 | Acordos para transferência de informações |
| 13.2.3 | Mensagens eletrônicas |
| 13.2.4 | Acordos de confidencialidade e não divulgação |
| 14 | Aquisição, desenvolvimento e manutenção de sistemas |
| 14.1 | Requisitos de segurança de sistemas de informação |



Processos de Segurança da Informação

ISO 27002

| | |
|--------|---|
| 14.1.1 | Análise e especificação dos requisitos de segurança da informação..... |
| 14.1.2 | Serviços de aplicação seguros em redes públicas |
| 14.1.3 | Protegendo as transações nos aplicativos de serviços..... |
| 14.2 | Segurança em processos de desenvolvimento e de suporte |
| 14.2.1 | Política de desenvolvimento seguro |
| 14.2.2 | Procedimentos para controle de mudanças de sistemas |
| 14.2.3 | Análise crítica técnica das aplicações após mudanças nas plataformas operacionais |
| 14.2.4 | Restrições sobre mudanças em pacotes de <i>software</i> |
| 14.2.5 | Princípios para projetar sistemas seguros..... |
| 14.2.6 | Ambiente seguro para desenvolvimento |
| 14.2.7 | Desenvolvimento terceirizado..... |
| 14.2.8 | Teste de segurança do sistema |
| 14.2.9 | Teste de aceitação de sistemas |
| 14.3 | Dados para teste |
| 14.3.1 | Proteção dos dados para teste |
| 15 | Relacionamento na cadeia de suprimento |
| 15.1 | Segurança da informação na cadeia de suprimento |
| 15.1.1 | Política de segurança da informação no relacionamento com os fornecedores..... |
| 15.1.2 | Identificando segurança da informação nos acordos com fornecedores |
| 15.1.3 | Cadeia de suprimento na tecnologia da informação e comunicação |
| 15.2 | Gerenciamento da entrega do serviço do fornecedor..... |
| 15.2.1 | Monitoramento e análise crítica de serviços com fornecedores..... |
| 15.2.2 | Gerenciamento de mudanças para serviços com fornecedores..... |
| 16 | Gestão de incidentes de segurança da informação |
| 16.1 | Gestão de incidentes de segurança da informação e melhorias..... |
| 16.1.1 | Responsabilidades e procedimentos |



Processos de Segurança da Informação

ISO 27002

| | |
|--------|---|
| 16.1.2 | Notificação de eventos de segurança da informação..... |
| 16.1.3 | Notificando fragilidades de segurança da informação..... |
| 16.1.4 | Avaliação e decisão dos eventos de segurança da informação..... |
| 16.1.5 | Resposta aos incidentes de segurança da informação |
| 16.1.6 | Aprendendo com os incidentes de segurança da informação |
| 16.1.7 | Coleta de evidências..... |
| 17 | Aspectos da segurança da informação na gestão da continuidade do negócio |
| 17.1 | Continuidade da segurança da informação |
| 17.1.1 | Planejando a continuidade da segurança da informação |
| 17.1.2 | Implementando a continuidade da segurança da informação..... |
| 17.1.3 | Verificação, análise crítica e avaliação da continuidade da segurança da informação 90 |
| 17.2 | Redundâncias..... |
| 17.2.1 | Disponibilidade dos recursos de processamento da informação..... |
| 18 | Conformidade |
| 18.1 | Conformidade com requisitos legais e contratuais..... |



Processos de Segurança da Informação

ISO 27002

| | |
|--------|---|
| 18.1.1 | Identificação da legislação aplicável e de requisitos contratuais |
| 18.1.2 | Direitos de propriedade intelectual |
| 18.1.3 | Proteção de registos..... |
| 18.1.4 | Proteção e privacidade de informações de identificação pessoal |
| 18.1.5 | Regulamentação de controles de criptografia |
| 18.2 | Análise crítica da segurança da informação |
| 18.2.1 | Análise crítica independente da segurança da informação |
| 18.2.2 | Conformidade com as políticas e procedimentos de segurança da informação..... |
| 18.2.3 | Análise crítica da conformidade técnica..... |
| | Bibliografia..... |