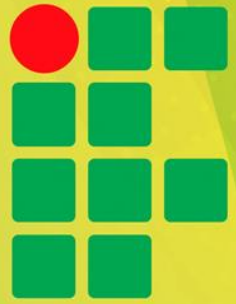
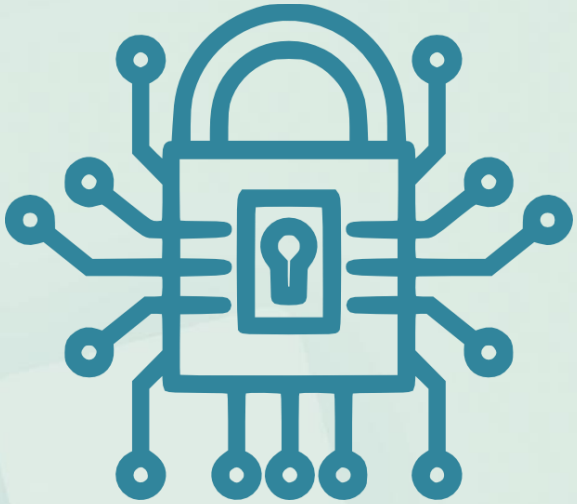


INSTITUTO FEDERAL

Sertão Pernambucano

Segurança da Informação



Leis e Normas

Prof. Heraldo Gonçalves Lima Junior

INSTITUTO FEDERAL
Sertão Pernambucano

1. SGSI

1.1. O que é o SGSI?

- Conjunto de **processos e procedimentos**, baseado em normas e na legislação, que uma organização implementa para **prover a segurança no uso de seus ativos tecnológicos**.
- É projetado para proteger os ativos da informação e proporcionar confiança às partes interessadas.

1.2. Escopo do SGSI

- A norma ISO 27001 adota o modelo PDCA (Plan-Do-Check-Act) para descrever a estrutura de um SGSI. A imagem a seguir, junto com descrição de cada uma das etapas provavelmente irá ajudá-lo a ganhar um pouco mais de intimidade com o conceito.

1.2. Escopo do SGSI

1.2.1. Estabelecer o SGSI

- É a etapa que da vida ao SGSI. Suas atividades devem estabelecer **políticas, objetivos, processos e procedimentos para a gestão de segurança da informação**.

1.2.2. Implementar o SGSI

- Consiste em implementar e operar a **política de segurança**, os controles / medidas de segurança, processos e procedimentos.

1.2.3. Monitorar e Analisar Criticamente o SGSI

- Reúne as práticas necessárias para **avaliar a eficiência e eficácia do sistema de gestão** e apresentar os resultados para a análise crítica pela direção. A política de segurança é usada para **comparar e desempenho alcançado com as diretrizes definidas**.

1.2.4. Manter e melhorar continuamente o SGSI

- Executar as **ações corretivas e preventivas**, com base nos resultados da auditoria interna do SGSI e da análise crítica pela direção ou outra informação pertinente, para alcançar a melhoria contínua do SGSI.

1.3. Por que definir o escopo do SGSI?

- O Escopo do Sistema de Gestão da Segurança da Informação é o que irá nortear a implementação da ISO 27001 na sua empresa.
- Com essa definição conseguimos enxergar de forma clara nosso trabalho de atuação na implementação do seu SGSI.

1.3. Como definir o escopo do SGSI?

1. **Conhecer seu contexto interno**. Entender de fato como está a sua empresa em relação à segurança da informação.
2. **Conhecer seu contexto externo**. Entender o mercado em que atua e analisar quais são as variáveis que interferem a sua empresa tanto de forma negativa ou positiva.

1.3. Como definir o escopo do SGSI?

3. **Identificar as partes** interessadas no que se tange a segurança das informações que sua empresa possui. Ou seja, pessoas ou organizações que de alguma forma tenham relações com as informações que sua empresa tem.

1.3. Como definir o escopo do SGSI?

3. **Entender as interfaces.** Pode ser que sua empresa tenha interfaces com terceiros como contabilidade, desenvolvimento de software, manutenção de infraestrutura, entre outros.

2. ISSO 27002

2.1. Objetivos da Norma

- O principal objetivo da ISO 27002 é estabelecer diretrizes e princípios gerais para **iniciar, implementar, manter e melhorar a gestão de segurança da informação** em uma organização. Isso também inclui a seleção, a implementação e o gerenciamento de controles, levando em conta os ambientes de risco encontrados na empresa.

2.2. Benefícios Para as Empresas

- Melhor **conscientização** sobre a segurança da informação;
- Maior **controle de ativos** e informações sensíveis;
- Oferece uma abordagem para **implantação de políticas de controles**;
- Oportunidade de **identificar e corrigir pontos fracos**;

2.2. Benefícios Para as Empresas

- **Redução do risco de responsabilidade** pela não implementação de um SGSI ou determinação de políticas e procedimentos;
- Torna-se um **diferencial competitivo** para a conquista de clientes que valorizam a certificação;

2.2. Benefícios Para as Empresas

- **Melhor organização** com processos e mecanismos bem desenhados e geridos;
- Promove **redução de custos** com a prevenção de incidentes de segurança da informação;
- **Conformidade com a legislação** e outras regulamentações.

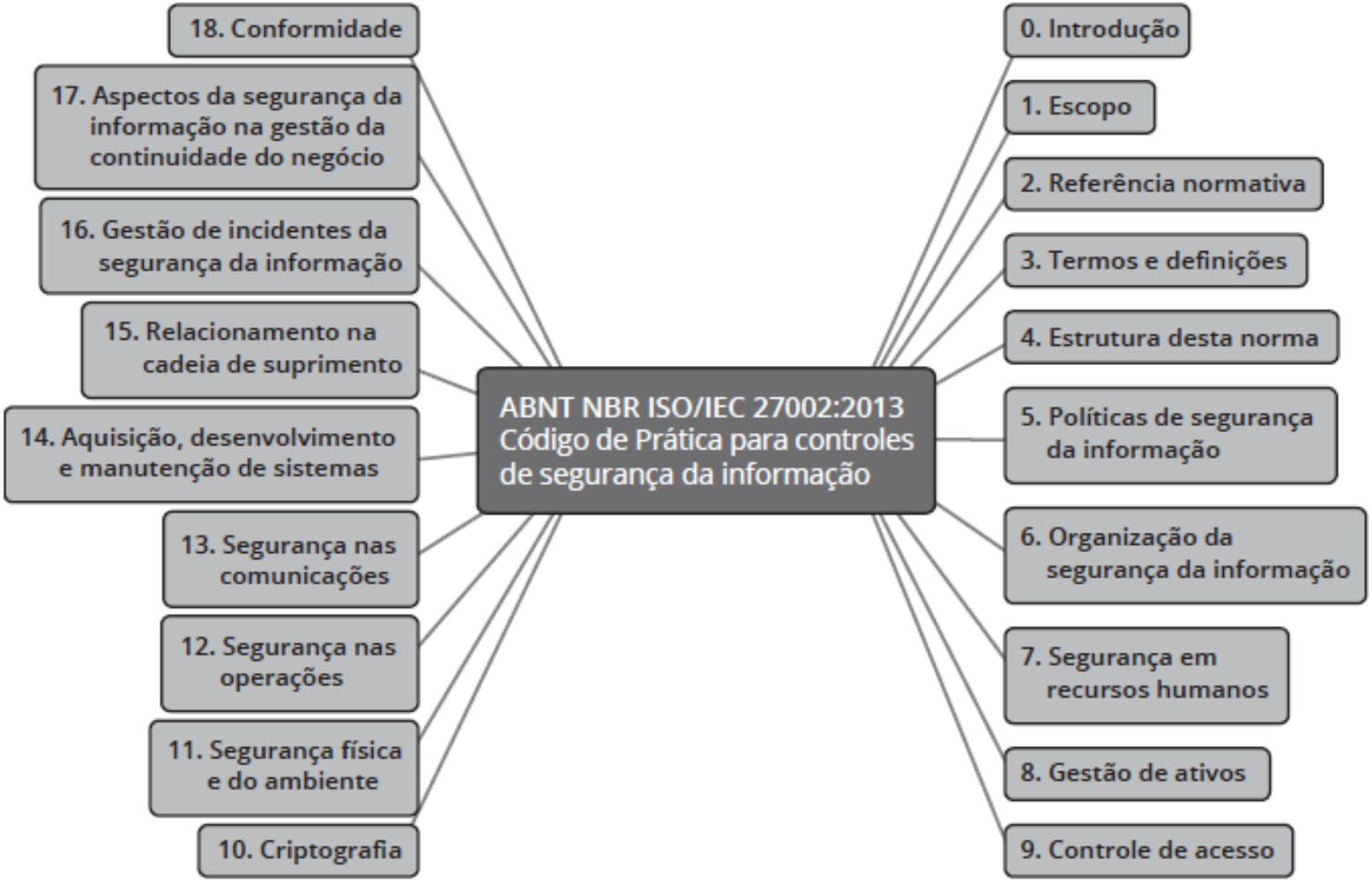
2.3. Estrutura da Norma

- Através do fornecimento de um guia completo de implementação, ela descreve como os **controles** podem ser estabelecidos. Estes controles, por sua vez, devem ser escolhidos com base em uma avaliação de riscos dos ativos mais importantes da empresa.

Os controles da norma são apresentados como boas praticas para que a organização adote uma postura preventiva e pró ativa diante das suas necessidades e requisitos de segurança da informação.

2.3. Estrutura da Norma

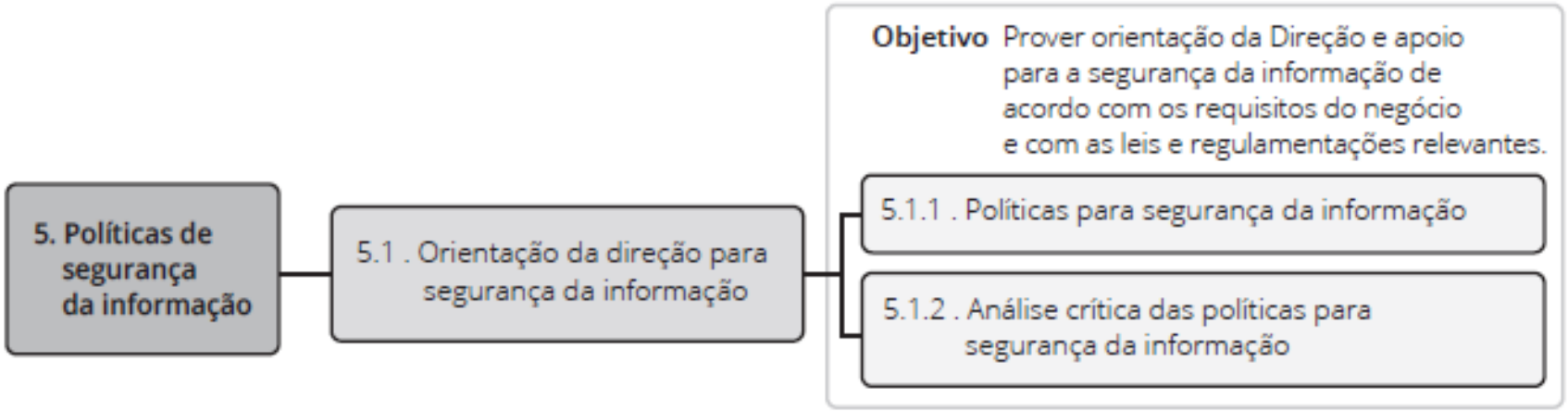
- A norma ABNT NBR ISO/IEC 27002, foi preparada para servir como um **guia prático para o desenvolvimento e a implementação de procedimentos e controles de segurança da informação** em uma organização.


ABNT NBR ISO/IEC 27002:2013
Código de Prática para controles de segurança da informação
0. Introdução
1. Escopo
2. Referência normativa
3. Termos e definições
4. Estrutura desta norma
5. Políticas de segurança da informação
6. Organização da segurança da informação
7. Segurança em recursos humanos
8. Gestão de ativos
9. Controle de acesso
10. Criptografia
11. Segurança física e do ambiente
12. Segurança nas operações
13. Segurança nas comunicações
14. Aquisição, desenvolvimento e manutenção de sistemas
15. Relacionamento na cadeia de suprimento
16. Gestão de incidentes da segurança da informação
17. Aspectos da segurança da informação na gestão da continuidade do negócio
18. Conformidade

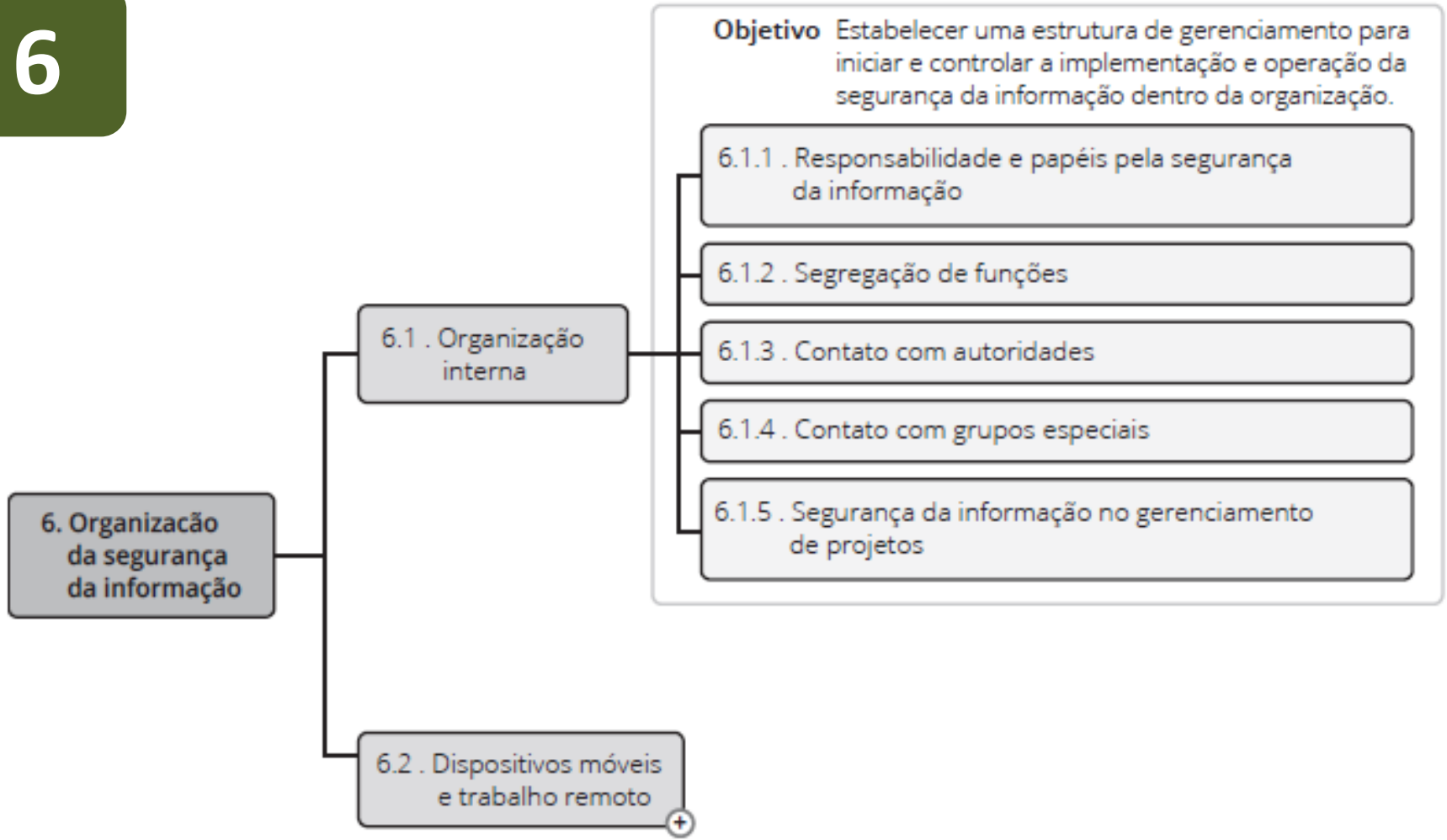
2.4. Principais itens da norma

- A parte principal da norma se encontra distribuída nas seguintes seções, que correspondem a **controles de segurança da informação**. Vale lembrar que a organização pode utilizar essas diretrizes como base para o desenvolvimento do SGSI. Sendo elas:

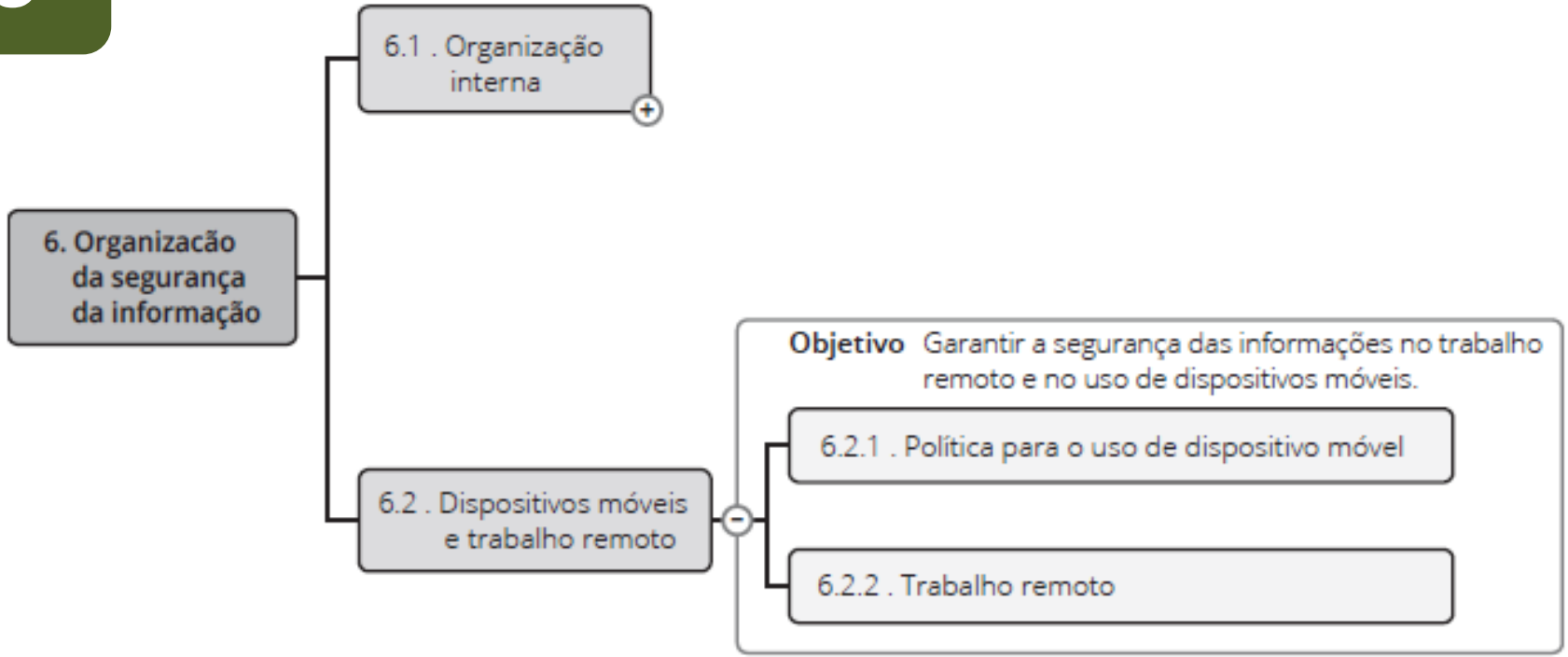
5


5. Políticas de segurança da informação
5.1 . Orientação da direção para segurança da informação
Objetivo Prover orientação da Direção e apoio para a segurança da informação de acordo com os requisitos do negócio e com as leis e regulamentações relevantes.
5.1.1 . Políticas para segurança da informação
5.1.2 . Análise crítica das políticas para segurança da informação

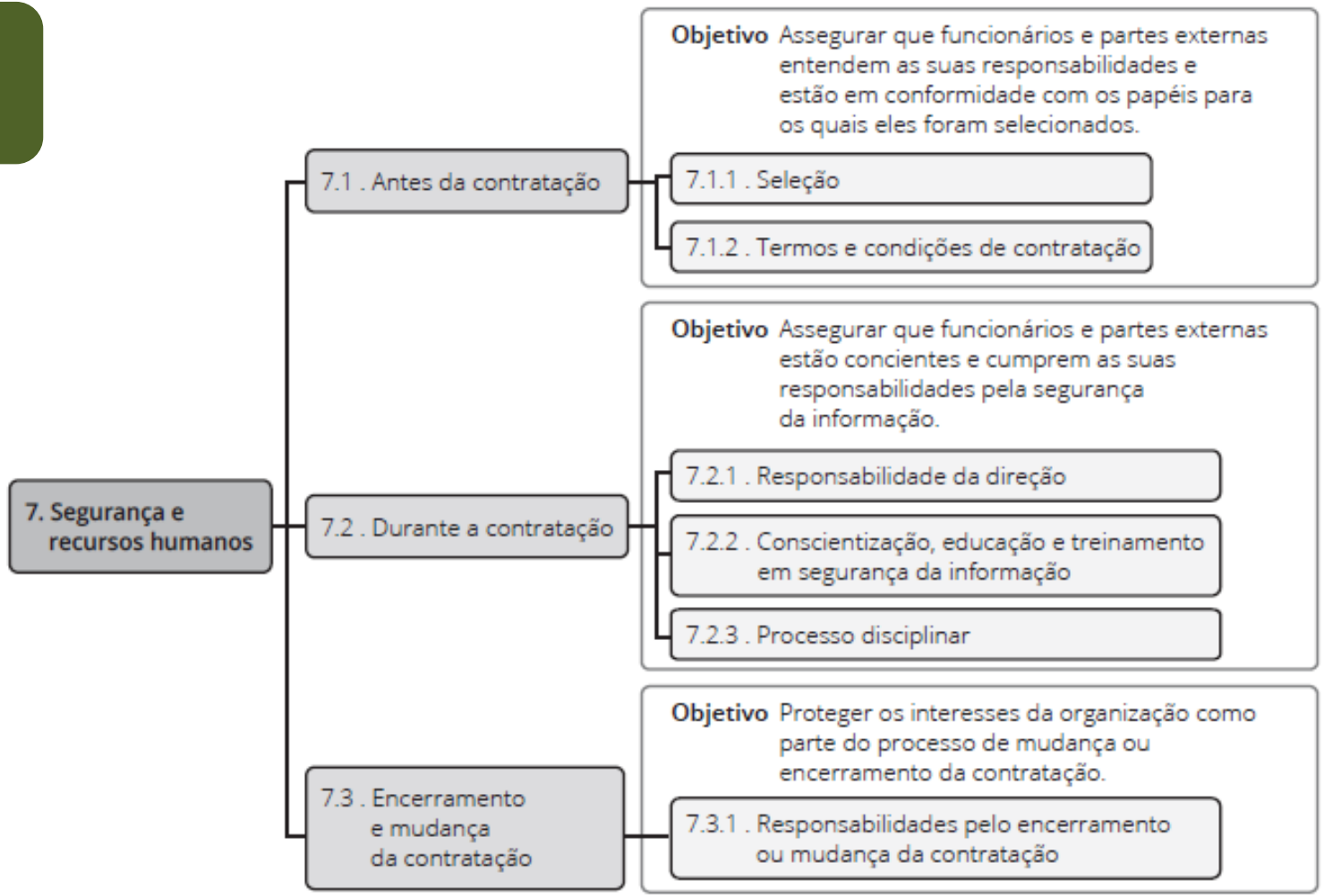
6


Objetivo Estabelecer uma estrutura de gerenciamento para iniciar e controlar a implementação e operação da segurança da informação dentro da organização.
6. Organizacão da segurança da informação
6.1 . Organização interna
6.1.1 . Responsabilidade 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

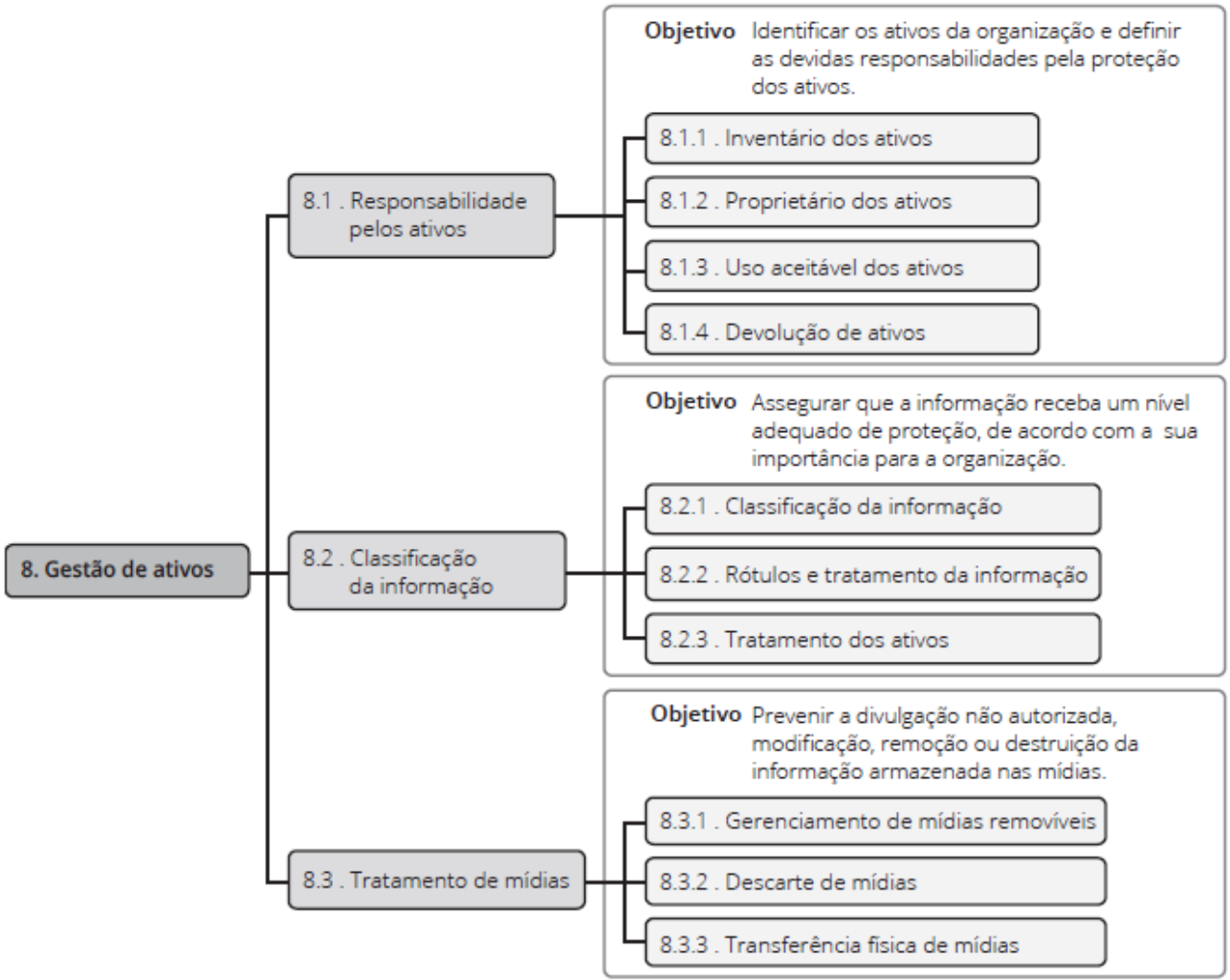
6


6. Organizacão da segurança da informação
6.1 . Organização interna
6.2 . Dispositivos móveis e trabalho remoto
Objetivo Garantir a segurança das informações no trabalho remoto e no uso de dispositivos móveis.
6.2.1 . Política para o uso de dispositivo móvel
6.2.2 . Trabalho remoto

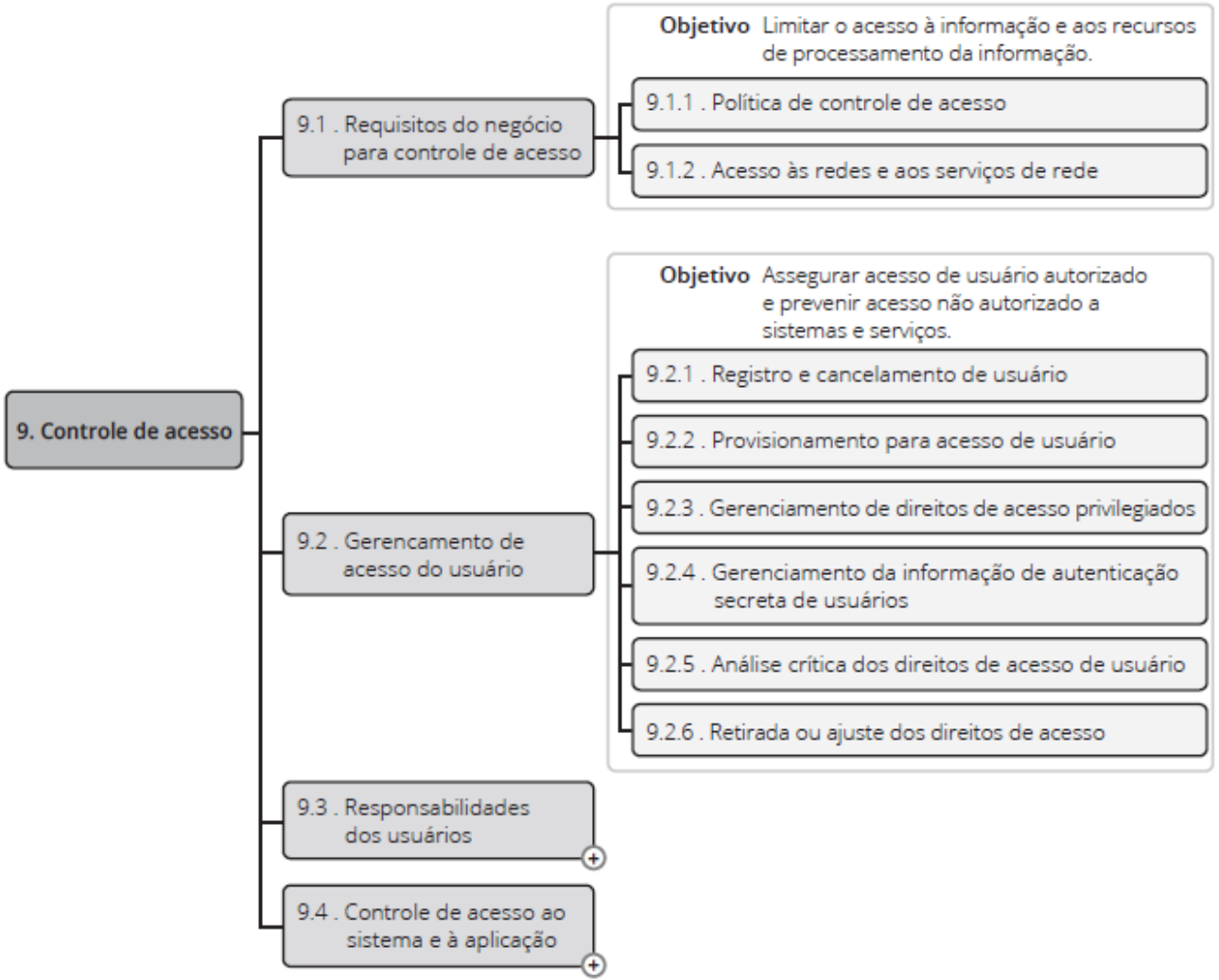
7


7. Segurança e recursos humanos
7.1 . Antes da contratação
Objetivo Assegurar que funcionários e partes externas entendem as suas responsabilidades e estão em conformidade com os papéis para os quais eles foram selecionados.
7.1.1 . Seleção
7.1.2 . Termos e condições de contratação
7.2 . Durante a contratação
Objetivo Assegurar que funcionários e partes externas estão concientes e cumprem as suas responsabilidades pela segurança da informação.
7.2.1 . Responsabilidade 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
Objetivo Proteger os interesses da organização como parte do processo de mudança ou encerramento da contratação.
7.3.1 . Responsabilidades pelo encerramento ou mudança da contratação

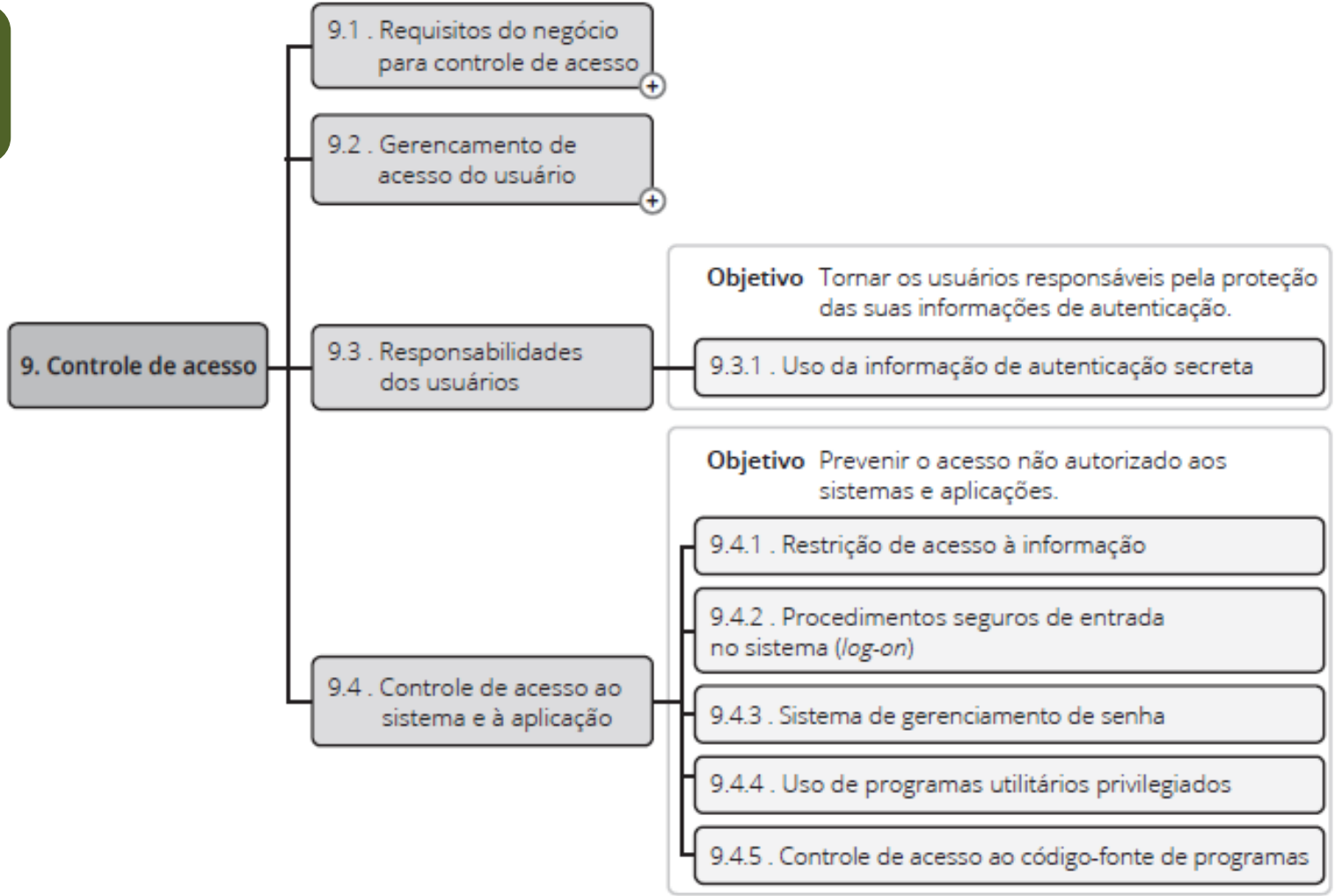
8


8. Gestão de ativos
8.1 . Responsabilidade pelos ativos
Objetivo Identificar os ativos da organização e definir as devidas responsabilidades pela proteção dos 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
Objetivo Assegurar que a informação receba um nível adequado de proteção, de acordo com a sua importância para a organização.
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
Objetivo Prevenir a divulgação não autorizada, modificação, remoção ou destruição da informação armazenada nas mídias.
8.3.1 . Gerenciamento de mídias removíveis
8.3.2 . Descarte de mídias
8.3.3 . Transferência física de mídias

9


9. Controle de acesso
9.1 . Requisitos do negócio para controle de acesso
Objetivo Limitar o acesso à informação e aos recursos de processamento da informação.
9.1.1 . Política de controle de acesso
9.1.2 . Acesso às redes e aos serviços de rede
9.2 . Gerencamento de acesso do usuário
Objetivo Assegurar acesso de usuário autorizado e prevenir acesso não autorizado a sistemas e serviços.
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
9.4 . Controle de acesso ao sistema e à aplicação

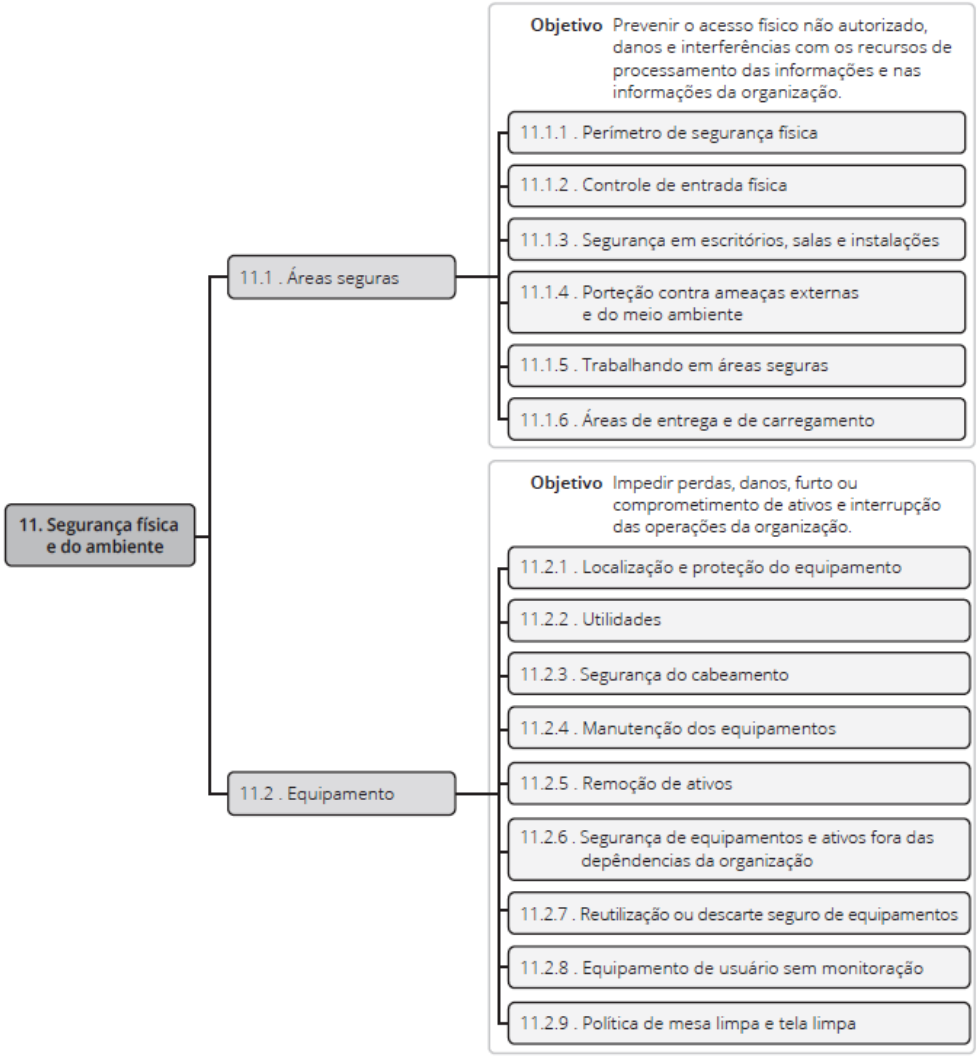
9


9. Controle de acesso
9.1 . Requisitos do negócio para controle de acesso
9.2 . Gerencamento de acesso do usuário
9.3 . Responsabilidades dos usuários
Objetivo Tornar os usuários responsáveis pela proteção das suas informações de autenticação.
9.3.1 . Uso da informação de autenticação secreta
9.4 . Controle de acesso ao sistema e à aplicação
Objetivo Prevenir o acesso não autorizado aos sistemas e aplicações.
9.4.1 . Restrição de acesso à informação
9.4.2 . Procedimentos seguros de entrada no sistema (log-on)
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

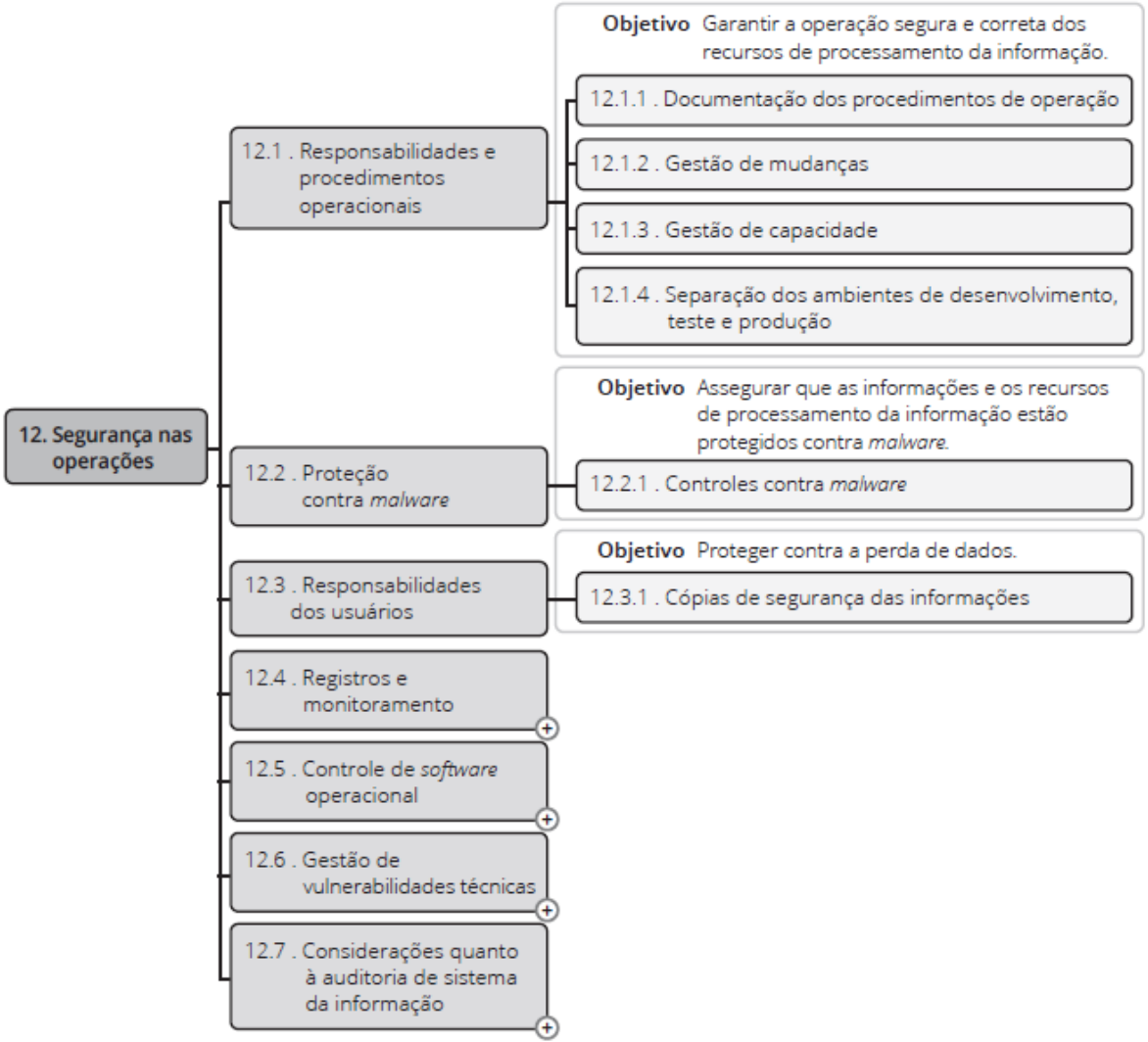
10


10. Criptografia
10.1 . Controles criptográficos
Objetivo Assegurar o uso efetivo e adequado da criptografia para proteger a confidencialidade, autenticidade e/ou a integridade da informação.
10.1.1 . Política para o uso de controles criptográficos
10.1.2 . Gerenciamento de chaves

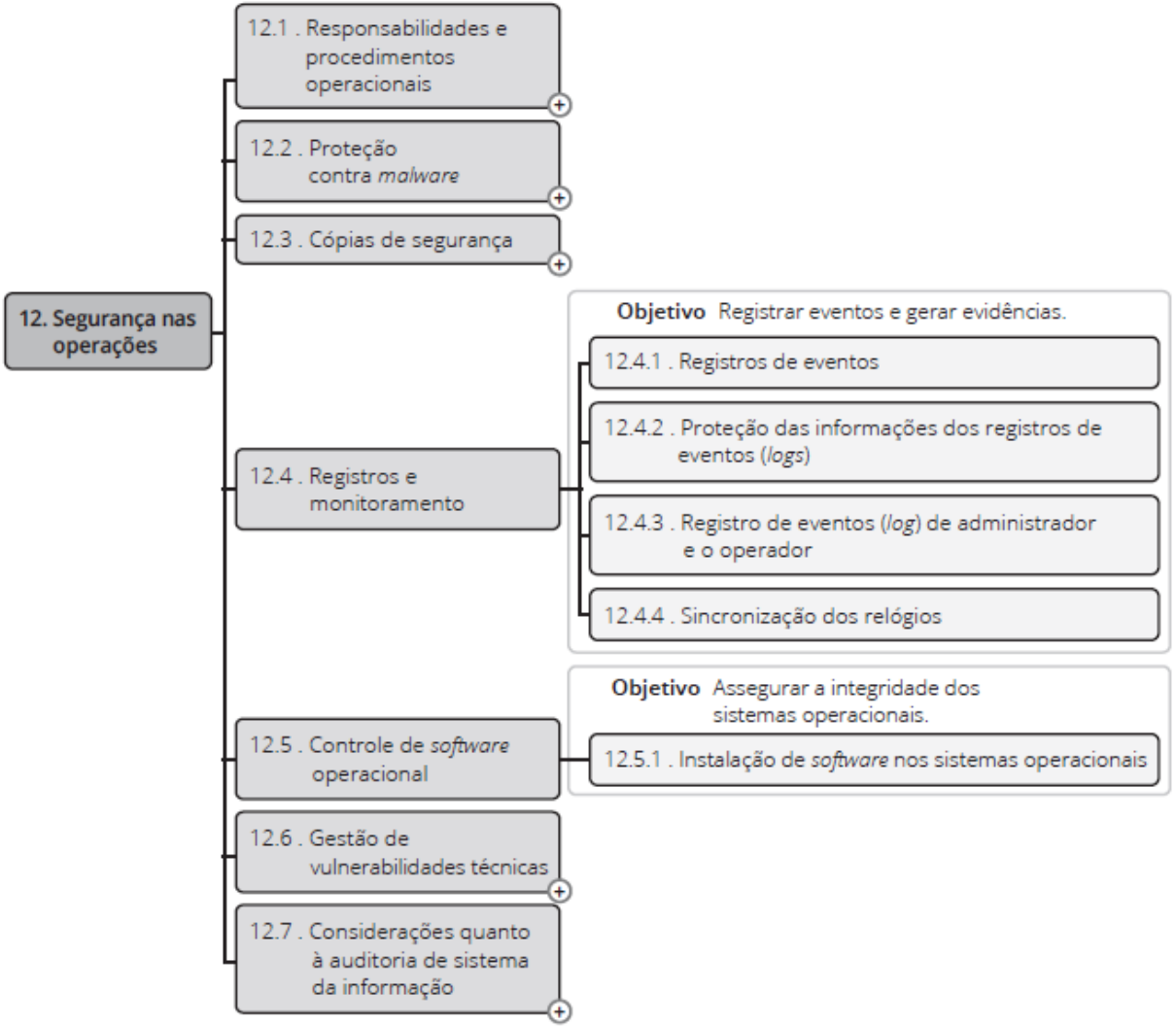
11


11. Segurança física e do ambiente
11.1 . Áreas seguras
Objetivo Prevenir o acesso físico não autorizado, danos e interferências com os recursos de processamento das informações e nas informações da organização.
11.1.1 . Perímetro de segurança física
11.1.2 . Controle de entrada física
11.1.3 . Segurança em escritórios, salas e instalações
11.1.4 . Porteção 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
Objetivo Impedir perdas, danos, furto ou comprometimento de ativos e interrupção das operações da organização.
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 depêndencias 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

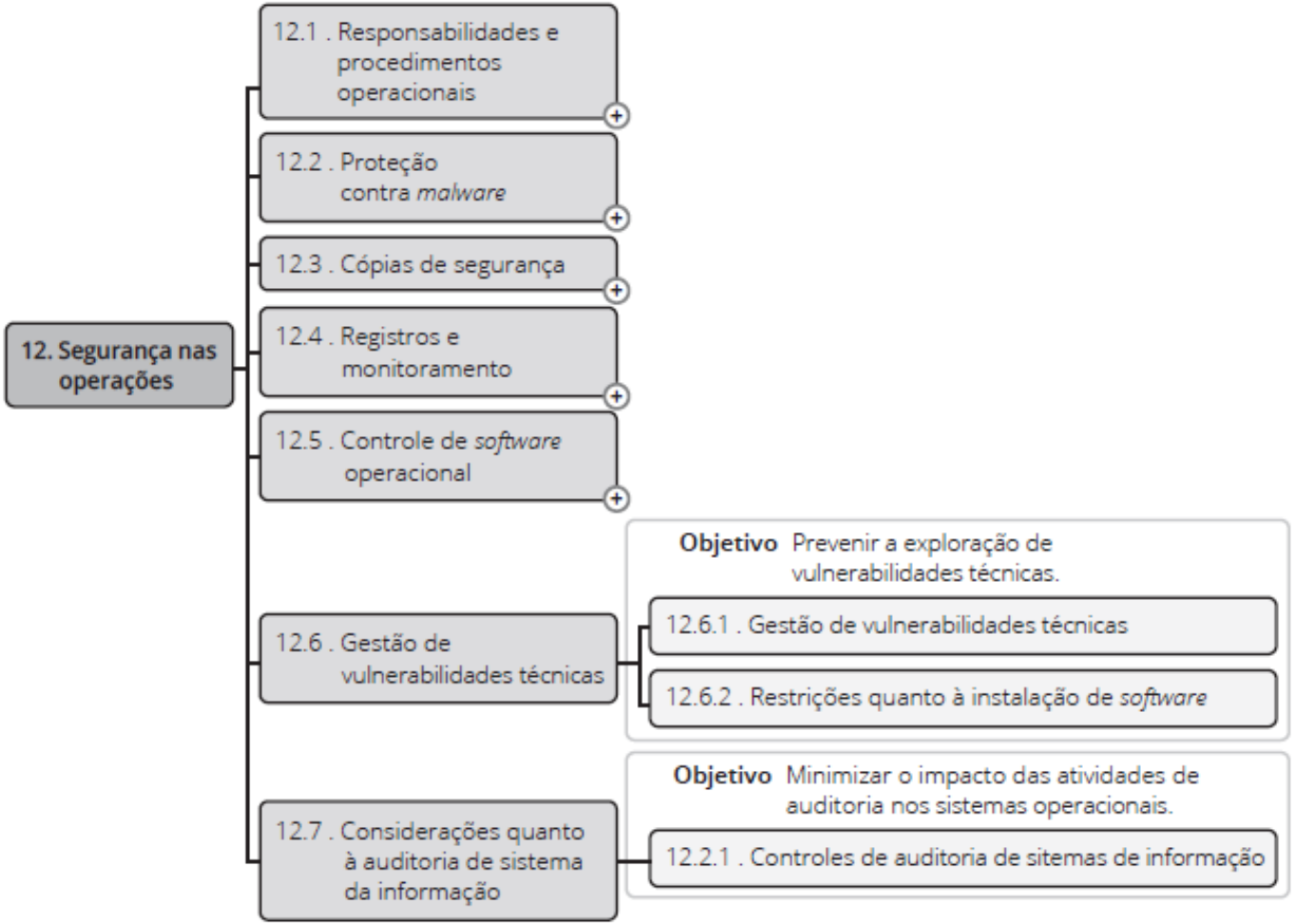
12


12. Segurança nas operações
12.1 . Responsabilidades e procedimentos operacionais
Objetivo Garantir a operação segura e correta dos recursos de processamento da informação.
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 *malware*
Objetivo Assegurar que as informações e os recursos de processamento da informação estão protegidos contra *malware*.
12.2.1 . Controles contra *malware*
12.3 . Responsabilidades dos usuários
Objetivo Proteger contra a perda de dados.
12.3.1 . Cópias de segurança das informações
12.4 . Registros e monitoramento
12.5 . Controle de *software* operacional
12.6 . Gestão de vulnerabilidades técnicas
12.7 . Considerações quanto à auditoria de sistema da informação

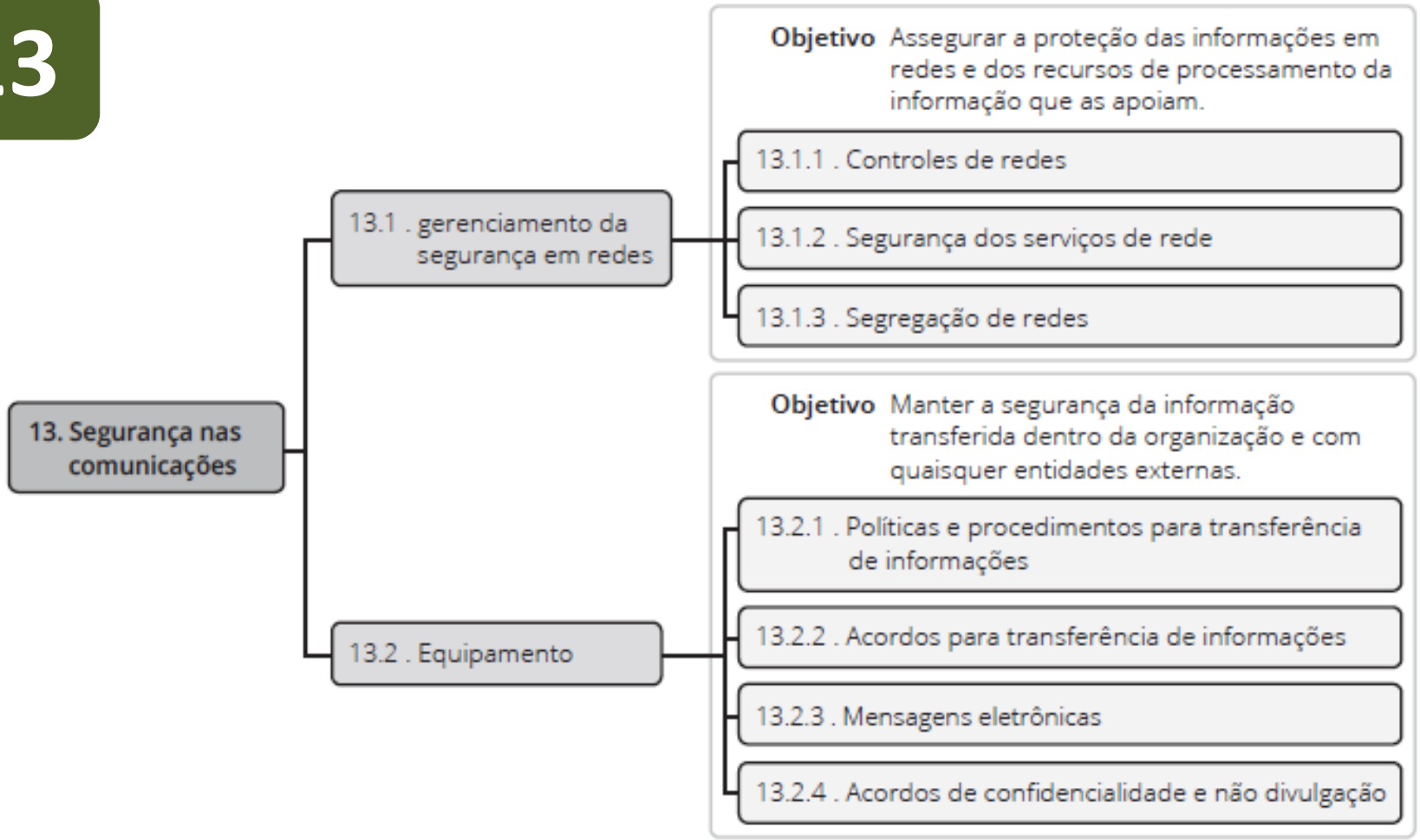
12


12. Segurança nas operações
12.1 . Responsabilidades e procedimentos operacionais
12.2 . Proteção contra *malware*
12.3 . Cópias de segurança
12.4 . Registros e monitoramento
Objetivo Registrar eventos e gerar evidências.
12.4.1 . Registros de eventos
12.4.2 . Proteção das informações dos registros de eventos (*logs*)
12.4.3 . Registro de eventos (*log*) de administrador e o operador
12.4.4 . Sincronização dos relógios
12.5 . Controle de *software* operacional
Objetivo Assegurar a integridade dos sistemas operacionais.
12.5.1 . Instalação de *software* nos sistemas operacionais
12.6 . Gestão de vulnerabilidades técnicas
12.7 . Considerações quanto à auditoria de sistema da informação

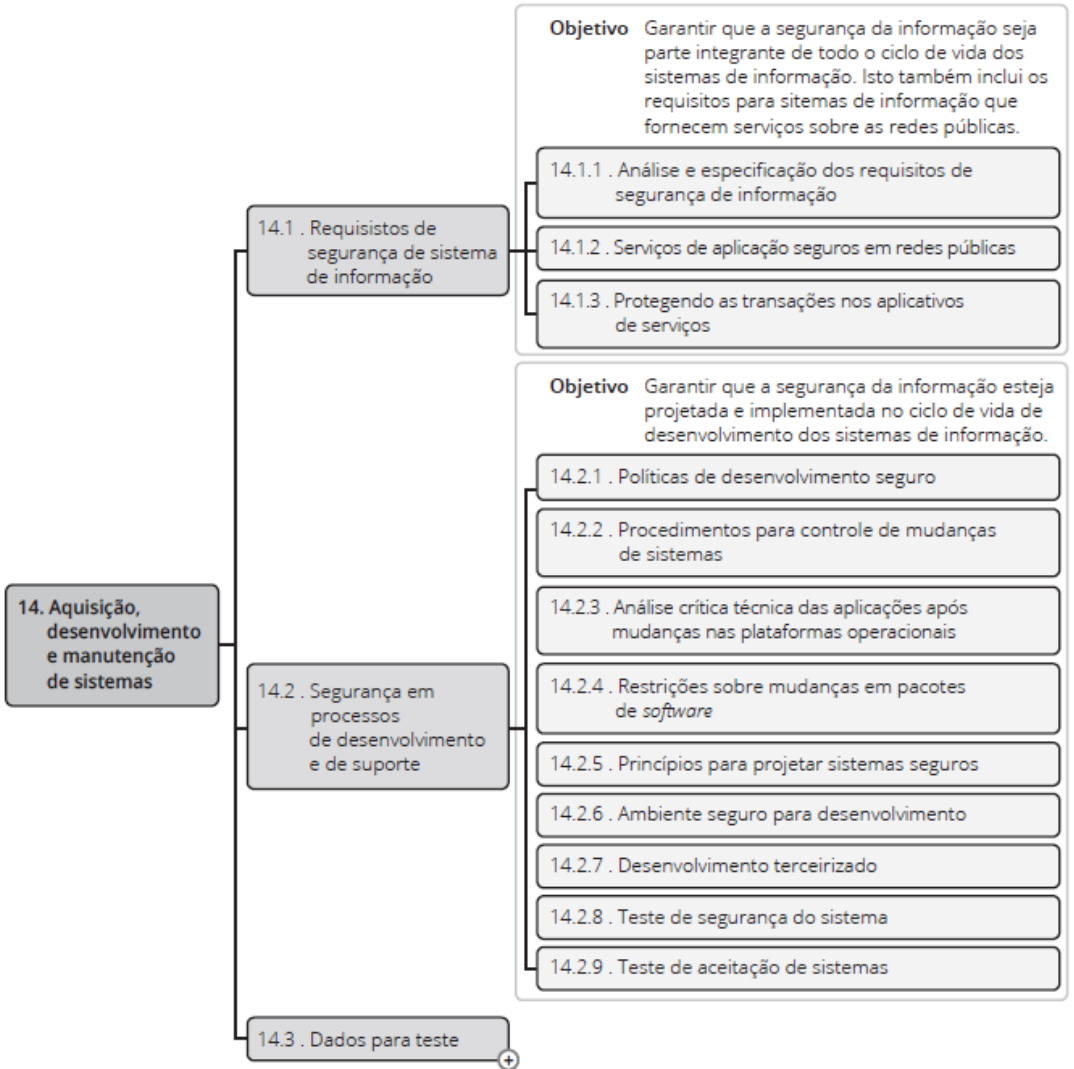
12


12. Segurança nas operações
12.1 . Responsabilidades e procedimentos operacionais
12.2 . Proteção contra *malware*
12.3 . Cópias de segurança
12.4 . Registros e monitoramento
12.5 . Controle de *software* operacional
12.6 . Gestão de vulnerabilidades técnicas
Objetivo Prevenir a exploração de vulnerabilidades técnicas.
12.6.1 . Gestão de vulnerabilidades técnicas
12.6.2 . Restrições quanto à instalação de *software*
12.7 . Considerações quanto à auditoria de sistema da informação
Objetivo Minimizar o impacto das atividades de auditoria nos sistemas operacionais.
12.2.1 . Controles de auditoria de sitemas de informação

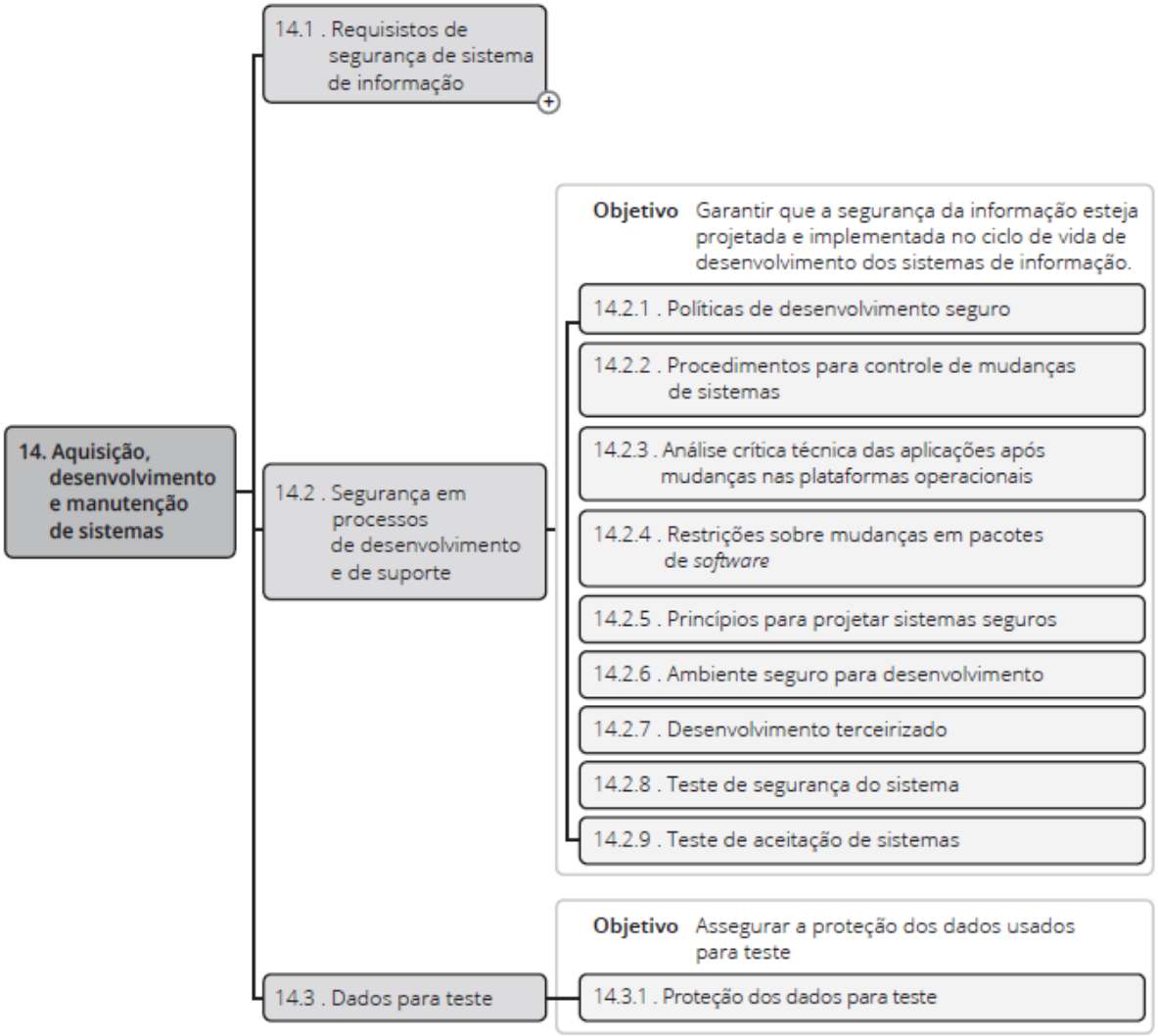
13


13. Segurança nas comunicações
13.1 . gerenciamento da segurança em redes
Objetivo Assegurar a proteção das informações em redes e dos recursos de processamento da informação que as apoiam.
13.1.1 . Controles de redes
13.1.2 . Segurança dos serviços de rede
13.1.3 . Segregação de redes
13.2 . Equipamento
Objetivo Manter a segurança da informação transferida dentro da organização e com quaisquer entidades externas.
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

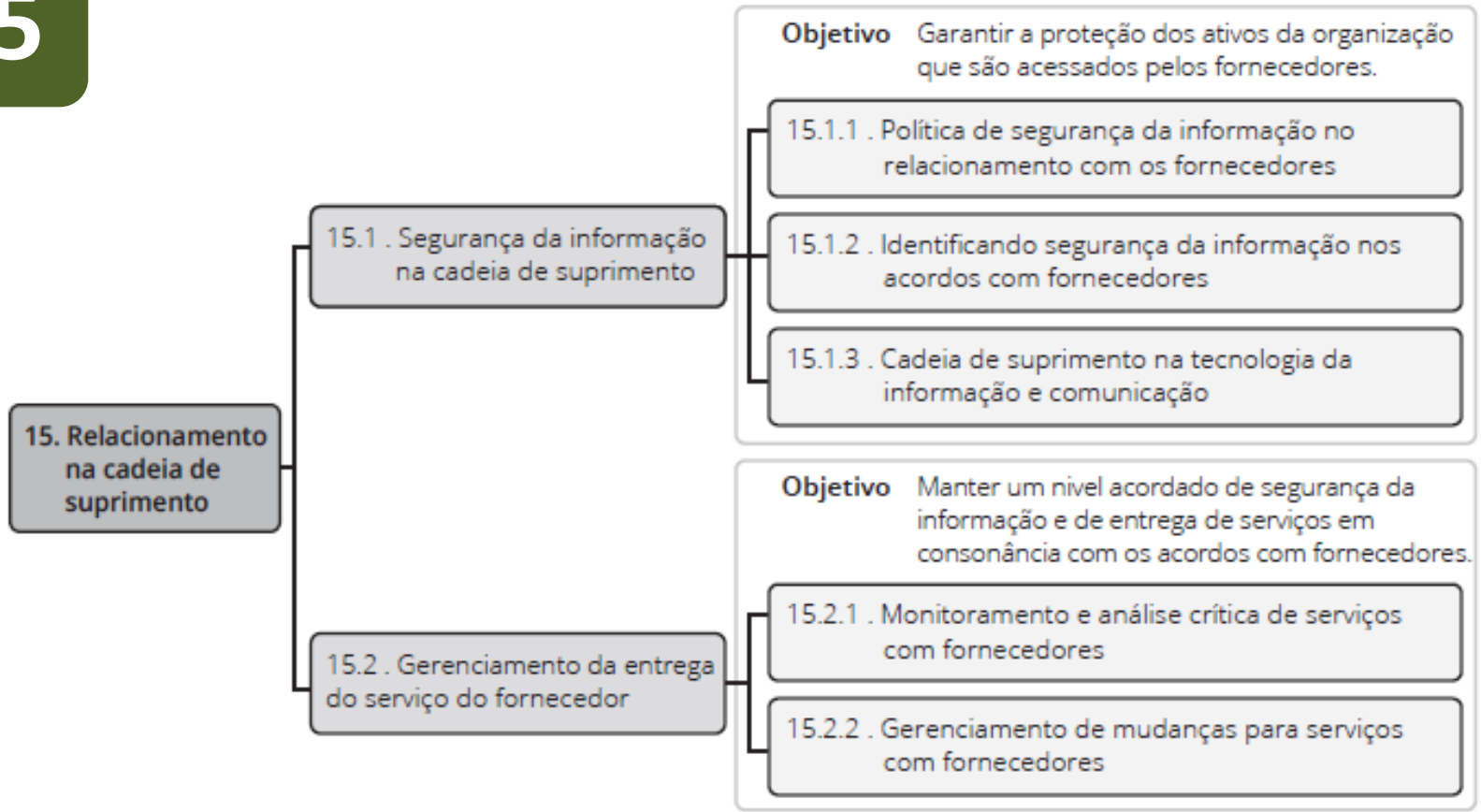
14


14. Aquisição, desenvolvimento e manutenção de sistemas
14.1 . Requisistos de segurança de sistema de informação
Objetivo Garantir que a segurança da informação seja parte integrante de todo o ciclo de vida dos sistemas de informação. Isto também inclui os requisitos para sitemas de informação que fornecem serviços sobre as redes públicas.
14.1.1 . Análise e especificação dos requisitos de segurança de 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
Objetivo Garantir que a segurança da informação esteja projetada e implementada no ciclo de vida de desenvolvimento dos sistemas de informação.
14.2.1 . Políticas 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 *software*
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

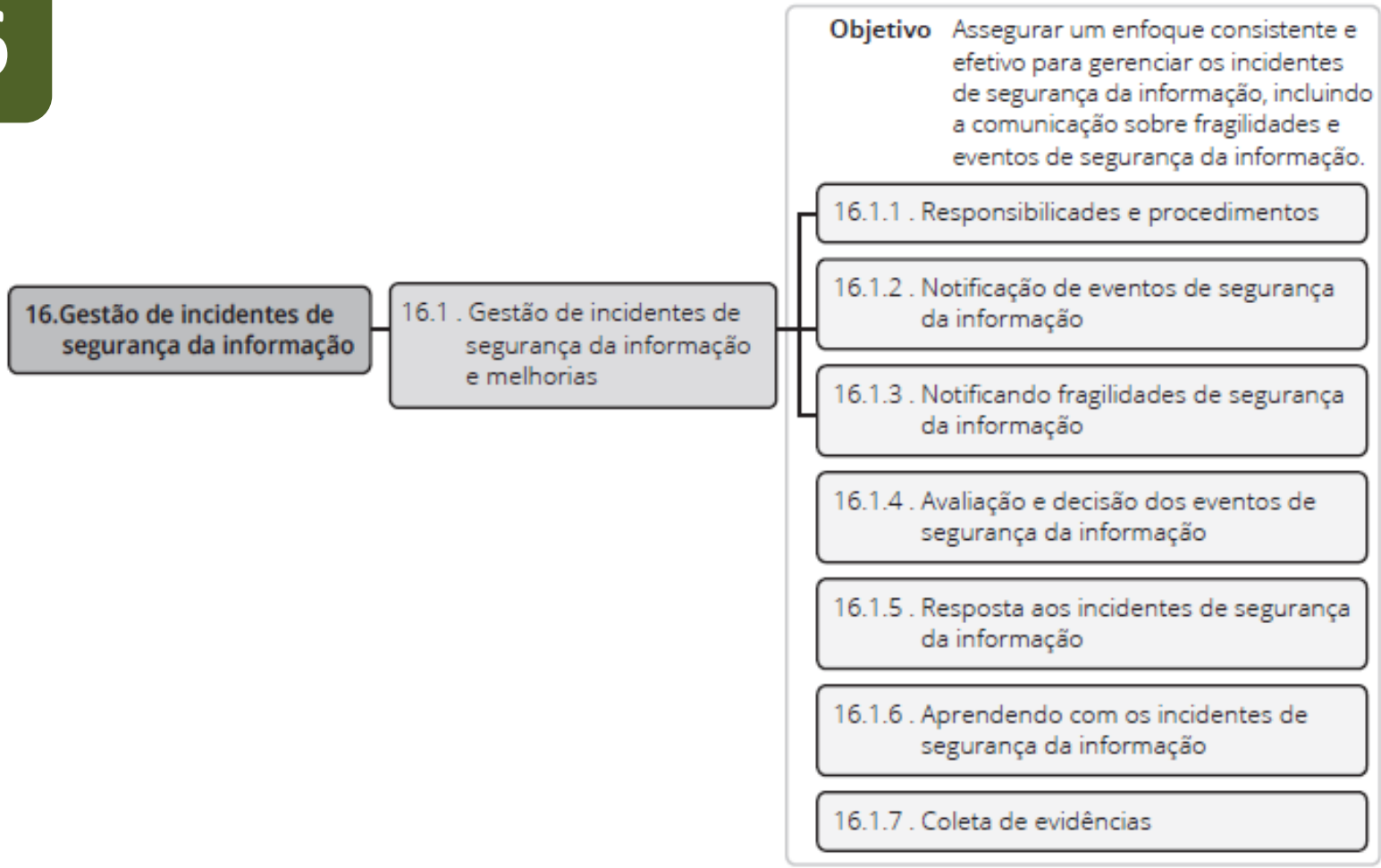
14


14. Aquisição, desenvolvimento e manutenção de sistemas
14.1 . Requisistos de segurança de sistema de informação
14.2 . Segurança em processos de desenvolvimento e de suporte
Objetivo Garantir que a segurança da informação esteja projetada e implementada no ciclo de vida de desenvolvimento dos sistemas de informação.
14.2.1 . Políticas 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 software
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
Objetivo Assegurar a proteção dos dados usados para teste
14.3.1 . Proteção dos dados para teste

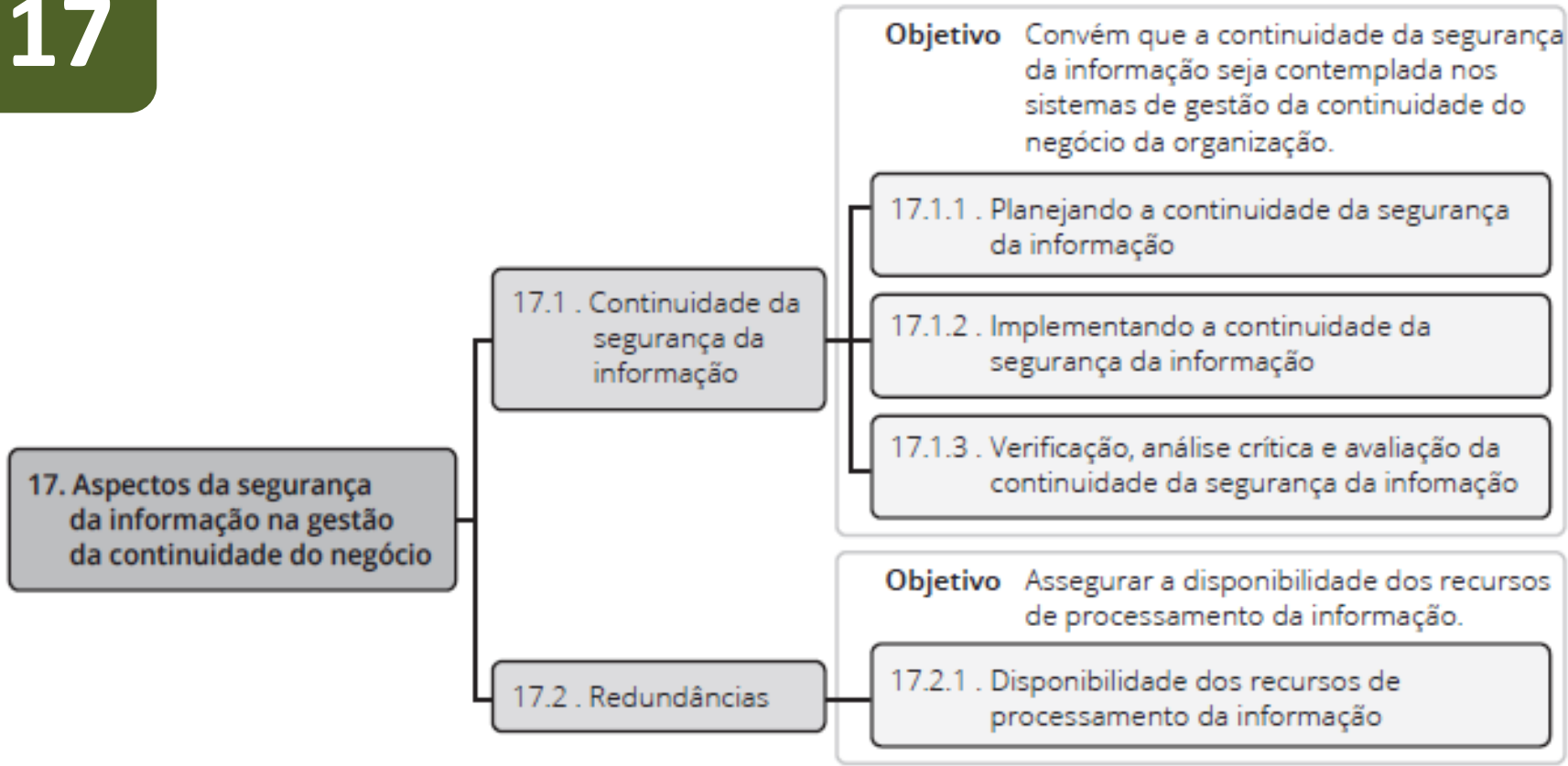
15


15. Relacionamento na cadeia de suprimento
15.1 . Segurança da informação na cadeia de suprimento
Objetivo Garantir a proteção dos ativos da organização que são acessados pelos fornecedores.
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
Objetivo Manter um nivel acordado de segurança da informação e de entrega de serviços em consonância com os acordos com fornecedores.
15.2.1 . Monitoramento e análise crítica de serviços com fornecedores
15.2.2 . Gerenciamento de mudanças para serviços com fornecedores

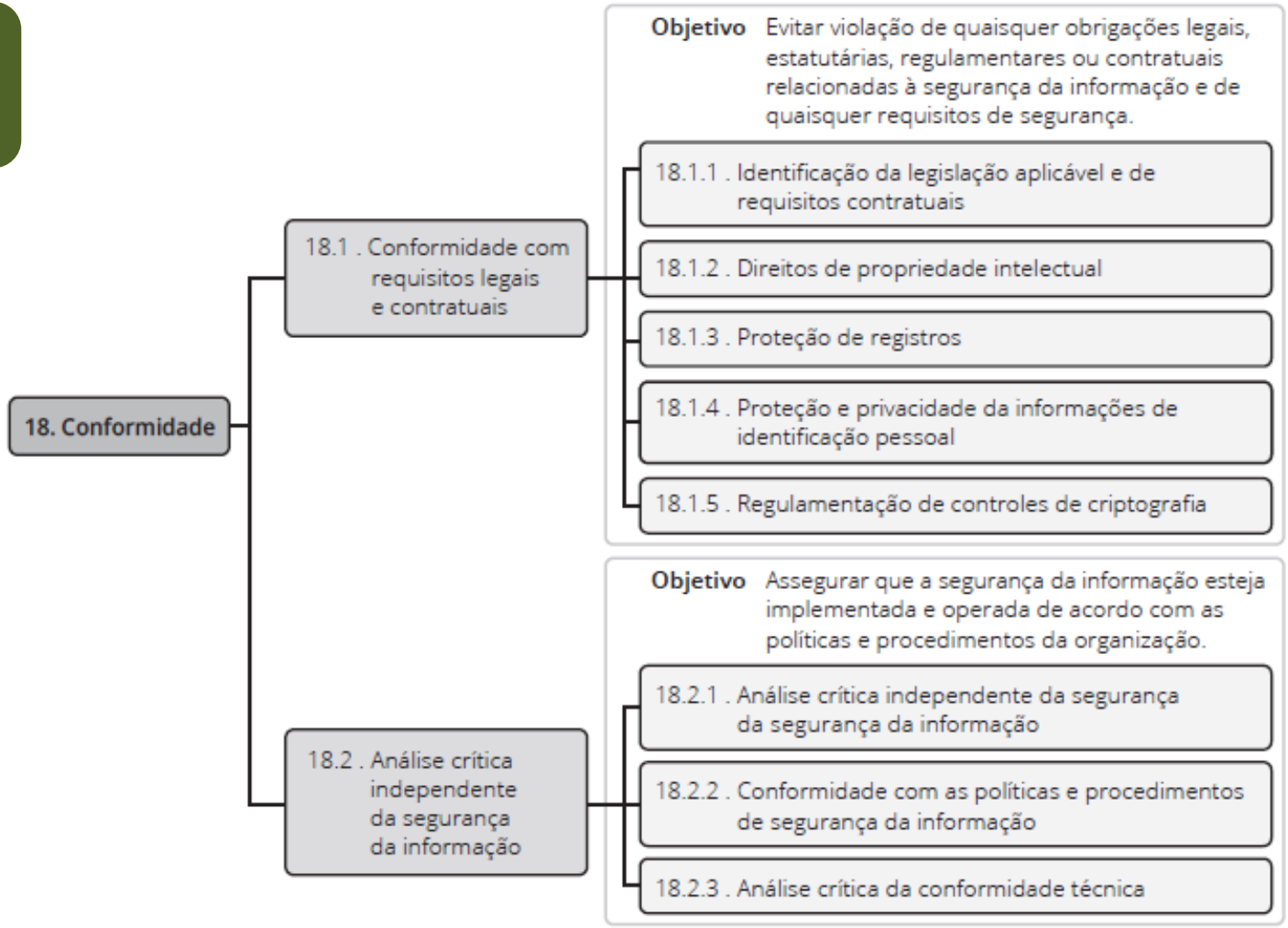
16


16.Gestão de incidentes de segurança da informação
16.1 . Gestão de incidentes de segurança da informação e melhorias
Objetivo Assegurar um enfoque consistente e efetivo para gerenciar os incidentes de segurança da informação, incluindo a comunicação sobre fragilidades e eventos de segurança da informação.
16.1.1 . Responsibilicades e procedimentos
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


17. Aspectos da segurança da informação na gestão da continuidade do negócio
17.1 . Continuidade da segurança da informação
Objetivo Convém que a continuidade da segurança da informação seja contemplada nos sistemas de gestão da continuidade do negócio da organização.
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 infomação
17.2 . Redundâncias
Objetivo Assegurar a disponibilidade dos recursos de processamento da informação.
17.2.1 . Disponibilidade dos recursos de processamento da informação

18


18. Conformidade
18.1 . Conformidade com requisitos legais e contratuais
Objetivo Evitar violação de quaisquer obrigações legais, estatutárias, regulamentares ou contratuais relacionadas à segurança da informação e de quaisquer requisitos de segurança.
18.1.1 . Identificação da legislação aplicável e de requisitos contratuais
18.1.2 . Direitos de propriedade intelectual
18.1.3 . Proteção de registros
18.1.4 . Proteção e privacidade da informações de identificação pessoal
18.1.5 . Regulamentação de controles de criptografia
18.2 . Análise crítica independente da segurança da informação
Objetivo Assegurar que a segurança da informação esteja implementada e operada de acordo com as políticas e procedimentos da organização.
18.2.1 . Análise crítica independente da segurança 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

2.5. Qual a relação entre esta norma e a LGPD?

- A **Lei Geral de Proteção de Dados**, como o nome propõe, é a legislação brasileira que tem como finalidade regular e **garantir que requisitos da proteção de dados pessoais sejam respeitados por empresas**.
- Percebemos então a importância da ISSO 27002.

2.5. Qual a relação entre esta norma e a LGPD?

- A **Lei Geral de Proteção de Dados**, como o nome propõe, é a legislação brasileira que tem como finalidade regular e garantir que requisitos da proteção de dados pessoais sejam respeitados por empresas.

2.6. Conclusão e Atividade

- Seguir os princípios da certificação ISO/IEC 27002 é um passo altamente relevante, para garantir a segurança da informação nas empresas.

- Atividade: Ler a LGP.

Obrigado!
Vlw! Flw!

INSTITUTO FEDERAL
Sertão Pernambucano