Segurança da Informação e Proteção ao Conhecimento

Aula 04 – Estrutura da norma ABNT NBR ISO/IEC 27002:2005

Prof. Dalton Martins
dmartins@gmail.com

Gestão da Informação
Faculdade de Informação e Comunicação
Universidade Federal de Goiás

Estrutura da norma

Apresentação da norma ABNT NBR ISO/IEC 27002:2005:

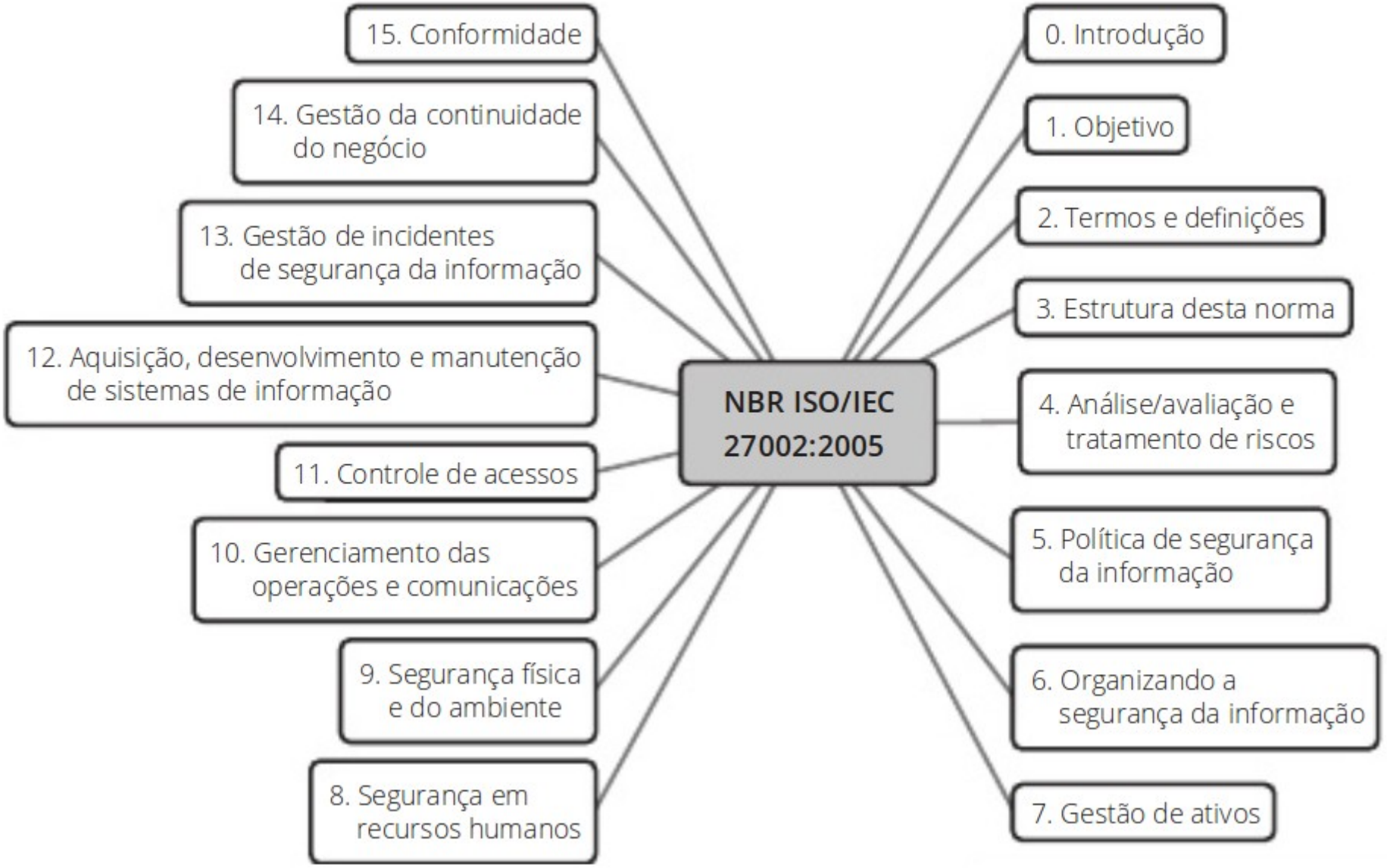
- Possui 11 seções.
- Possui 39 categorias principais de segurança.
- Contém uma seção introdutória sobre análise/avaliação e tratamento de riscos.
- A versão atual possui 133 controles.

Estruturada para fornecer um código de boas práticas para gestão da segurança, a norma é organizada em capítulos de 0 a 15. Os capítulos de 0 a 4 apresentam os temas de introdução (0), objetivo da norma (1), termos e definições adotados pela norma (2), a estrutura da norma (3) e análise/avaliação e tratamento de riscos (4), considerados como a seção introdutória.

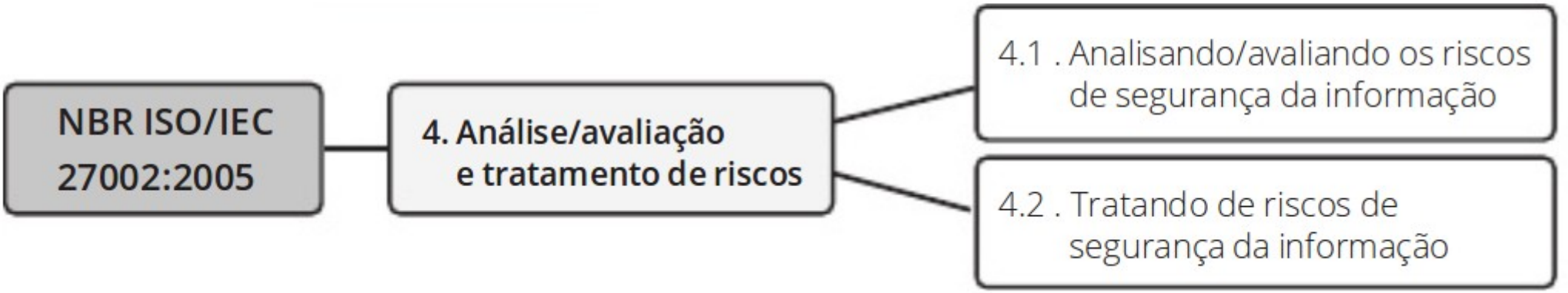
A partir do capítulo 5, a norma passa a chamar cada capítulo de seção. Assim, existem onze seções específicas apresentando os códigos de práticas da gestão da segurança.

Existem 133 controles e eles são os elementos que definem o que a norma 27002 considera como importante para um processo de segurança da informação. Os controles identificados por números (xx.xx.xx) são estruturados através de:

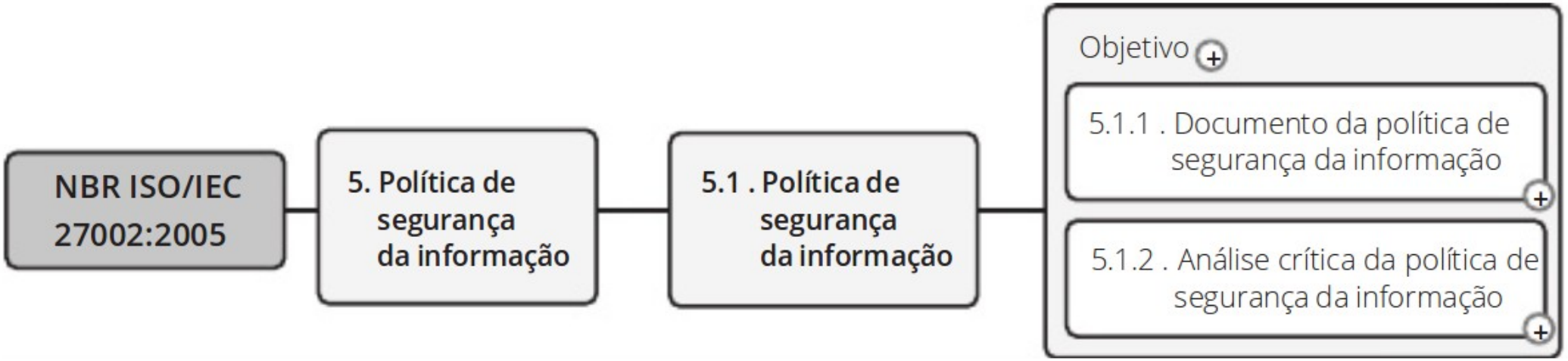
- **Controle** – descrição e definição do controle;
- **Diretrizes para a implementação** – informações auxiliares na implementação do controle;
- **Informações adicionais** – informações complementares.


NBR ISO/IEC 27002:2005
0. Introdução
1. Objetivo
2. Termos e definições
3. Estrutura desta norma
4. Análise/avaliação e tratamento de riscos
5. Política de segurança da informação
6. Organizando a segurança da informação
7. Gestão de ativos
8. Segurança em recursos humanos
9. Segurança física e do ambiente
10. Gerenciamento das operações e comunicações
11. Controle de acessos
12. Aquisição, desenvolvimento e manutenção de sistemas de informação
13. Gestão de incidentes de segurança da informação
14. Gestão da continuidade do negócio
15. Conformidade

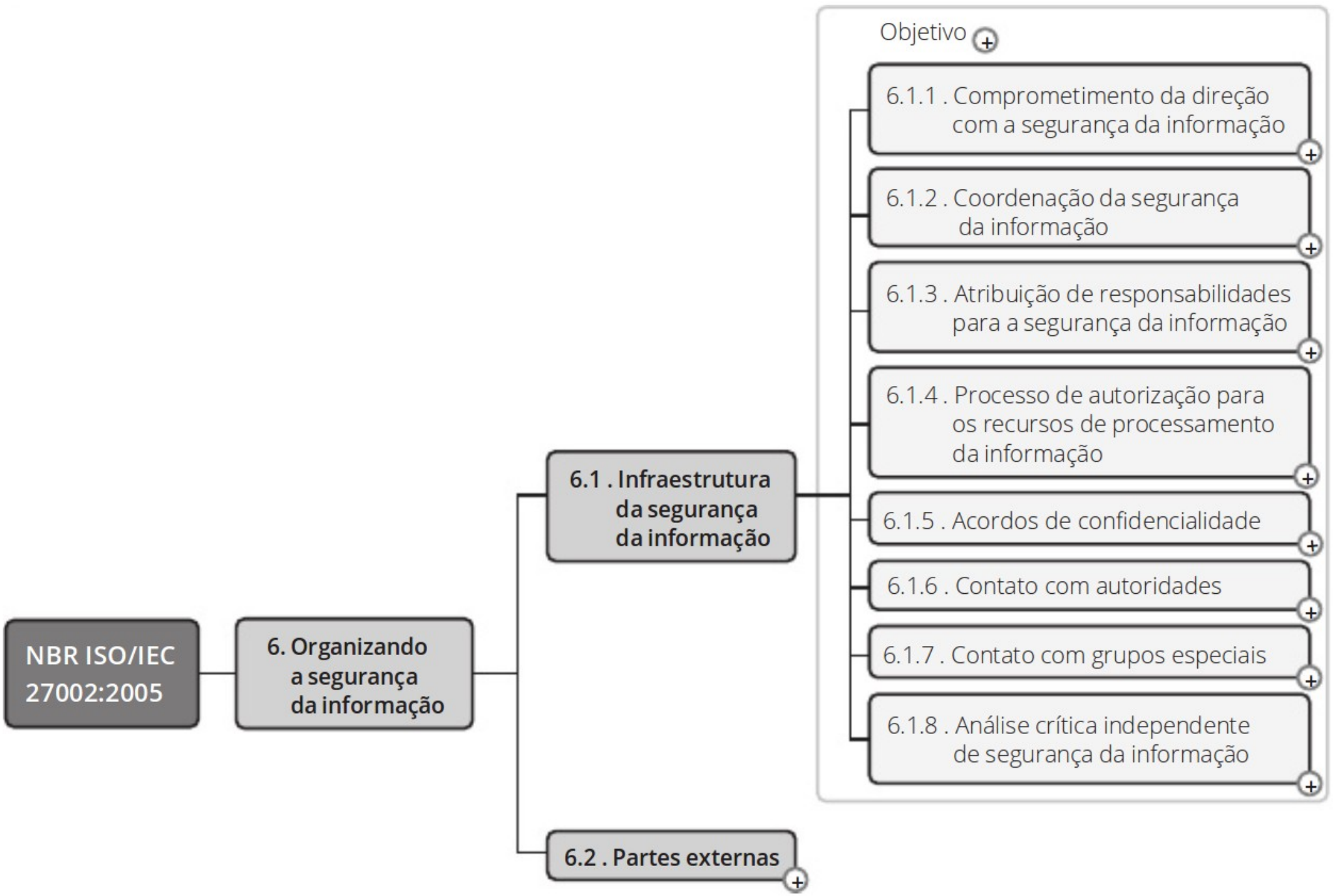
Seção 4 – Análise/avaliação e tratamento de riscos



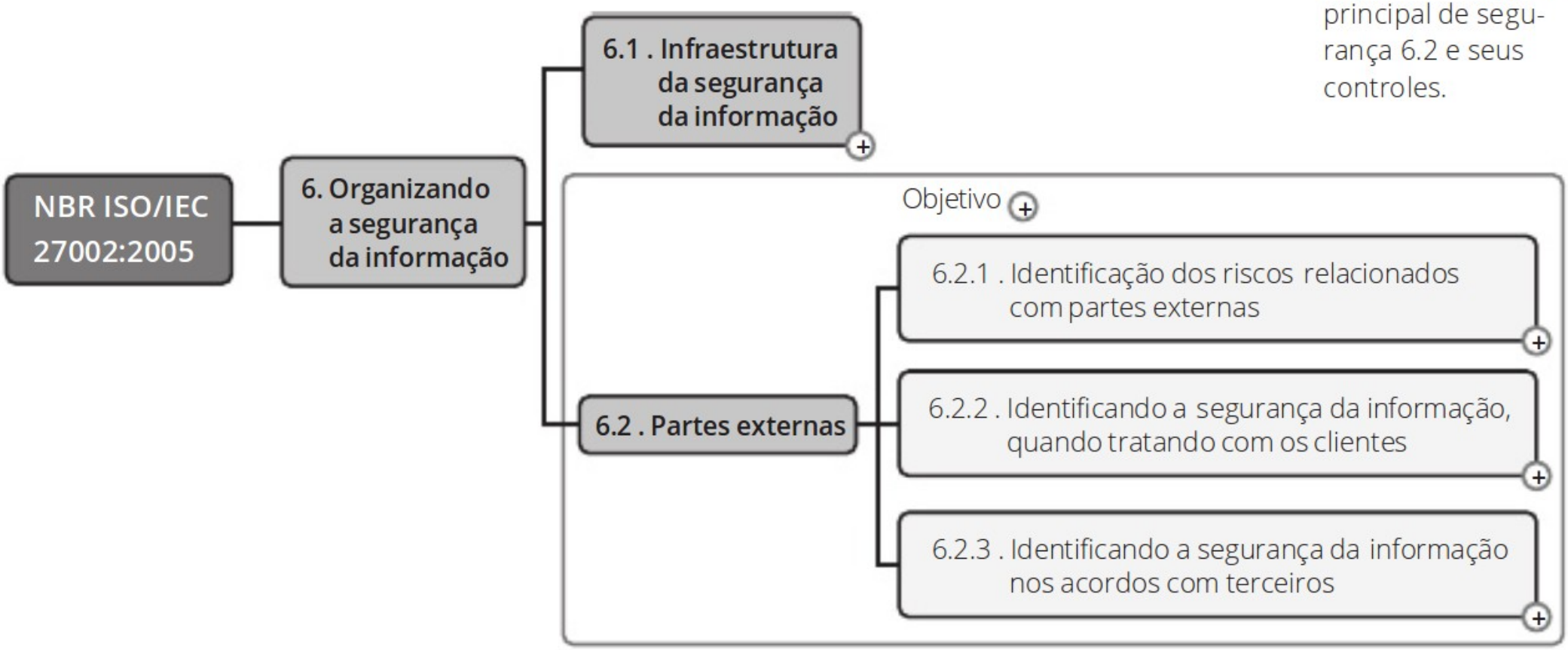
Seção 5 – Política de segurança



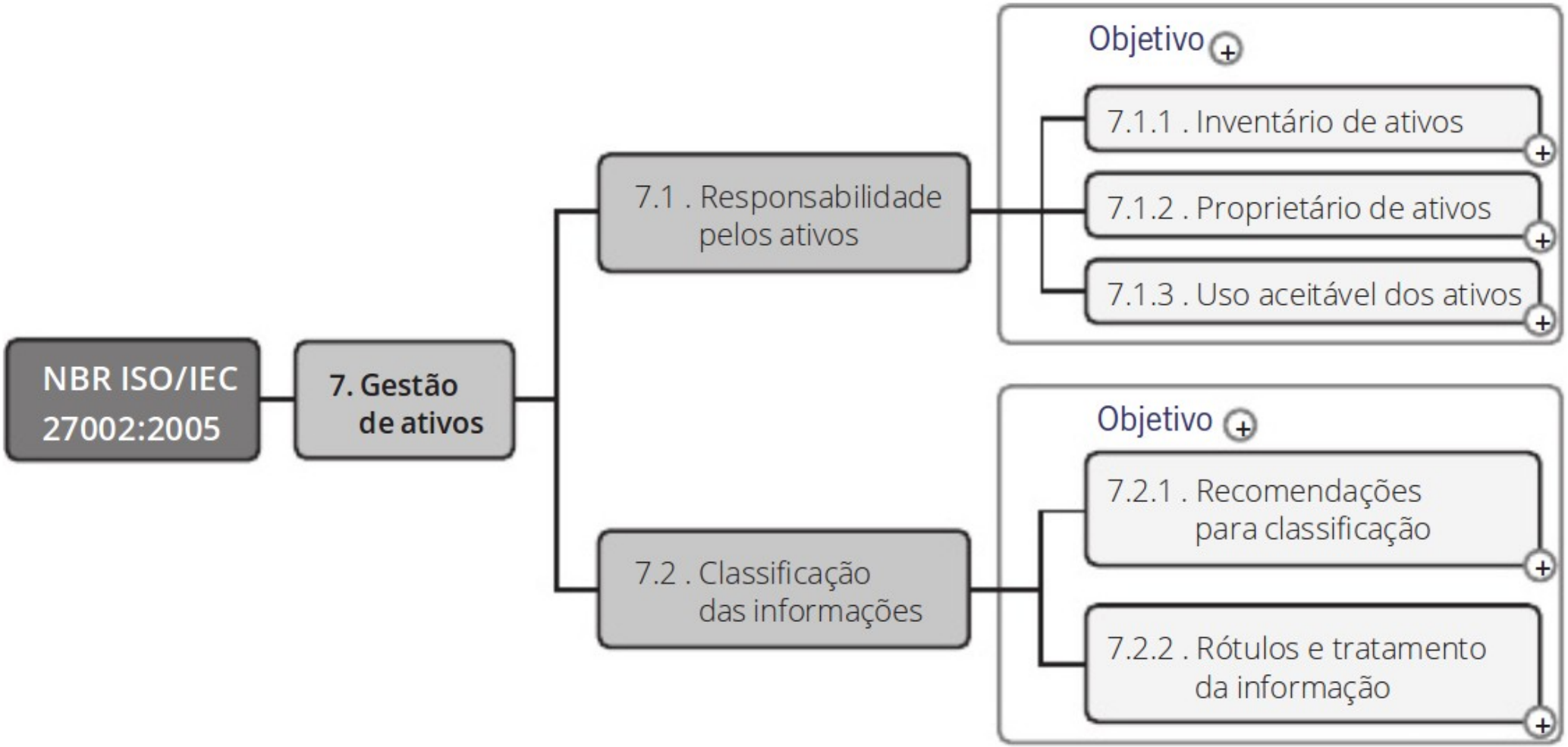
Seção 6 – Organizando a segurança da informação


NBR ISO/IEC 27002:2005
6. Organizando a segurança da informação
6.1 . Infraestrutura da segurança da informação
6.2 . Partes externas
Objetivo
6.1.1 . Comprometimento da direção com a segurança da informação
6.1.2 . Coordenação da segurança da informação
6.1.3 . Atribuição de responsabilidades para a segurança da informação
6.1.4 . Processo de autorização para os recursos de processamento da informação
6.1.5 . Acordos de confidencialidade
6.1.6 . Contato com autoridades
6.1.7 . Contato com grupos especiais
6.1.8 . Análise crítica independente de segurança da informação

principal de segu-
rança 6.2 e seus
controles.

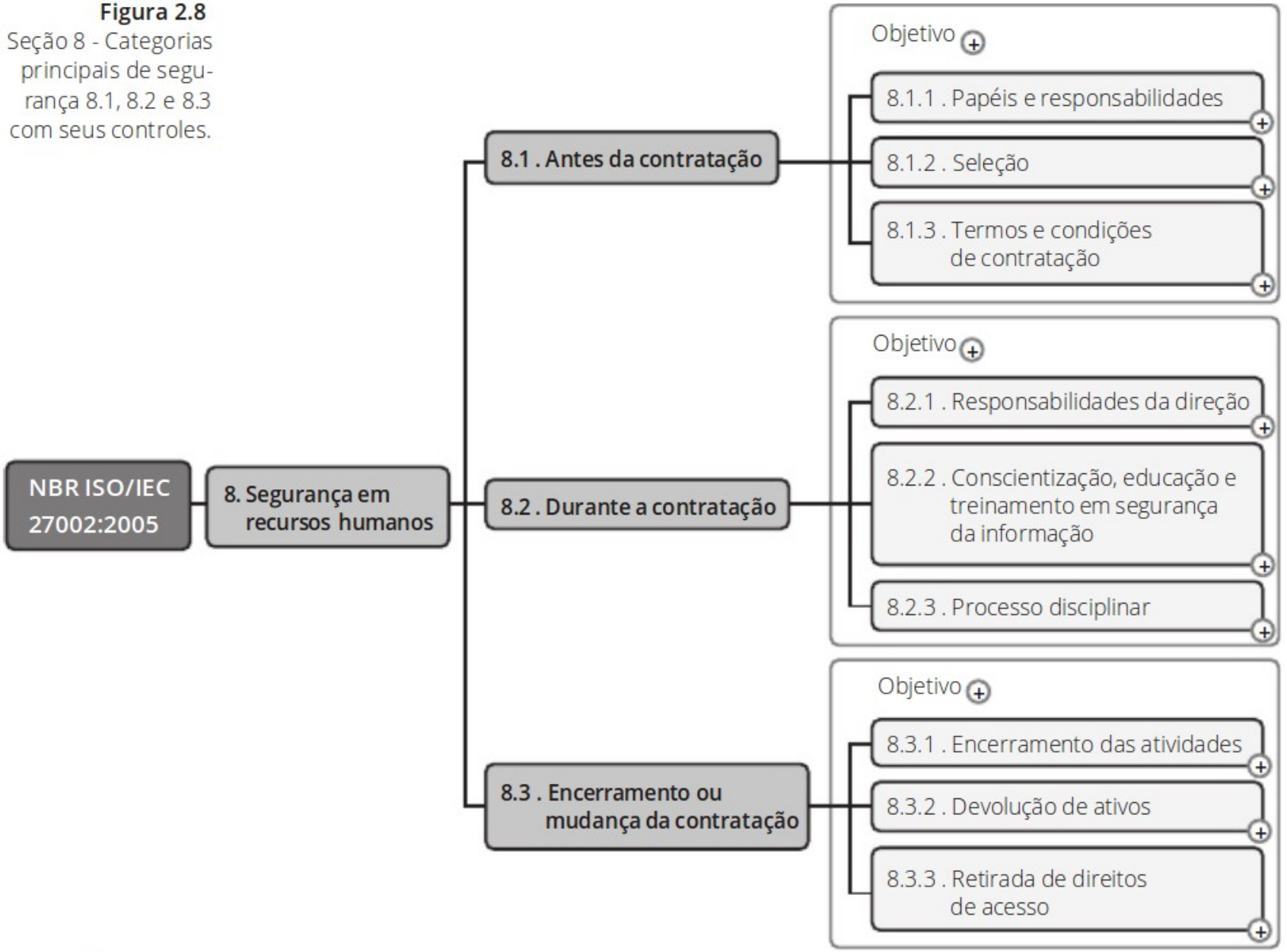


Seção 7 – Gestão de ativos

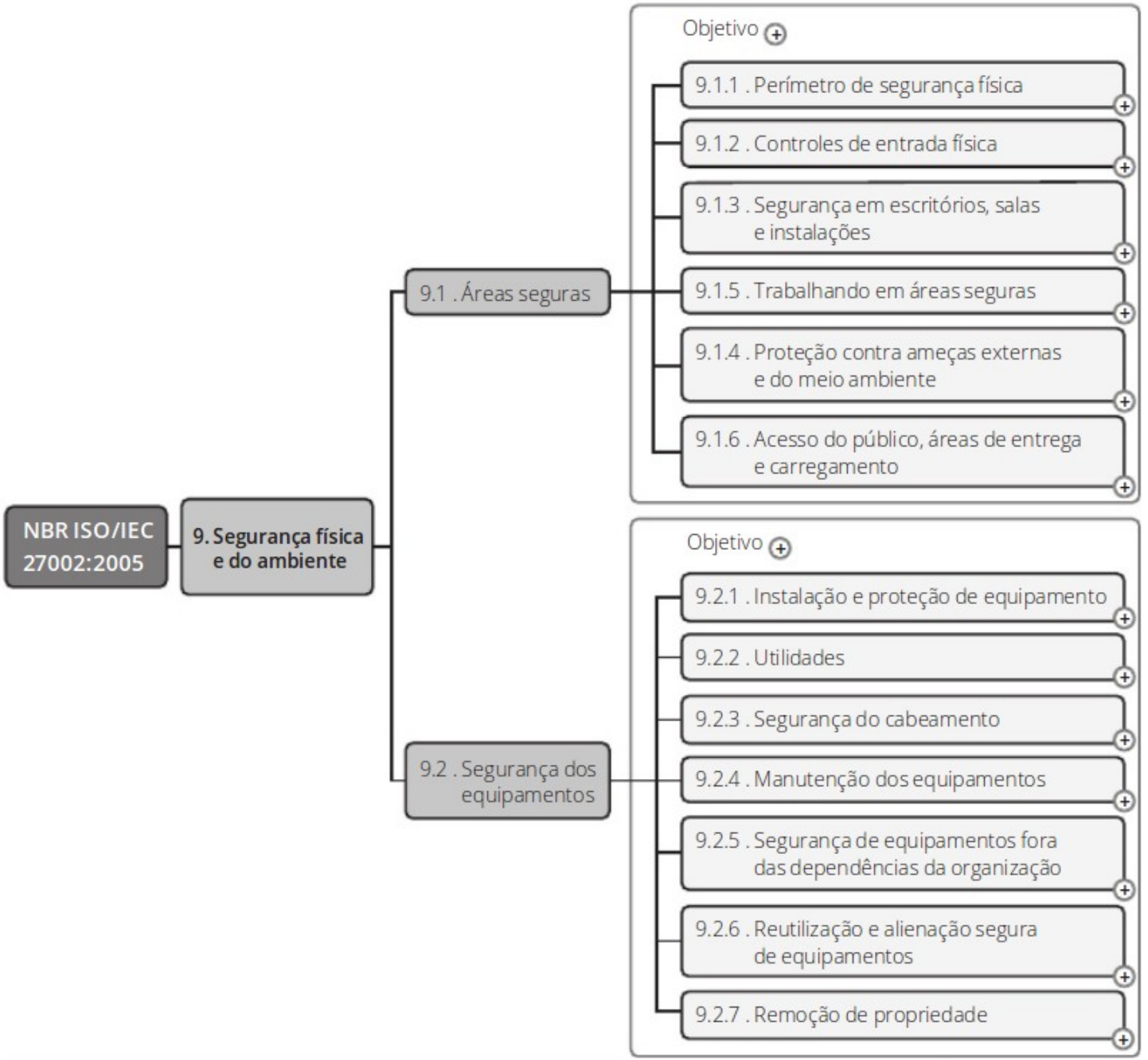


Seção 8 – Segurança em Recursos Humanos

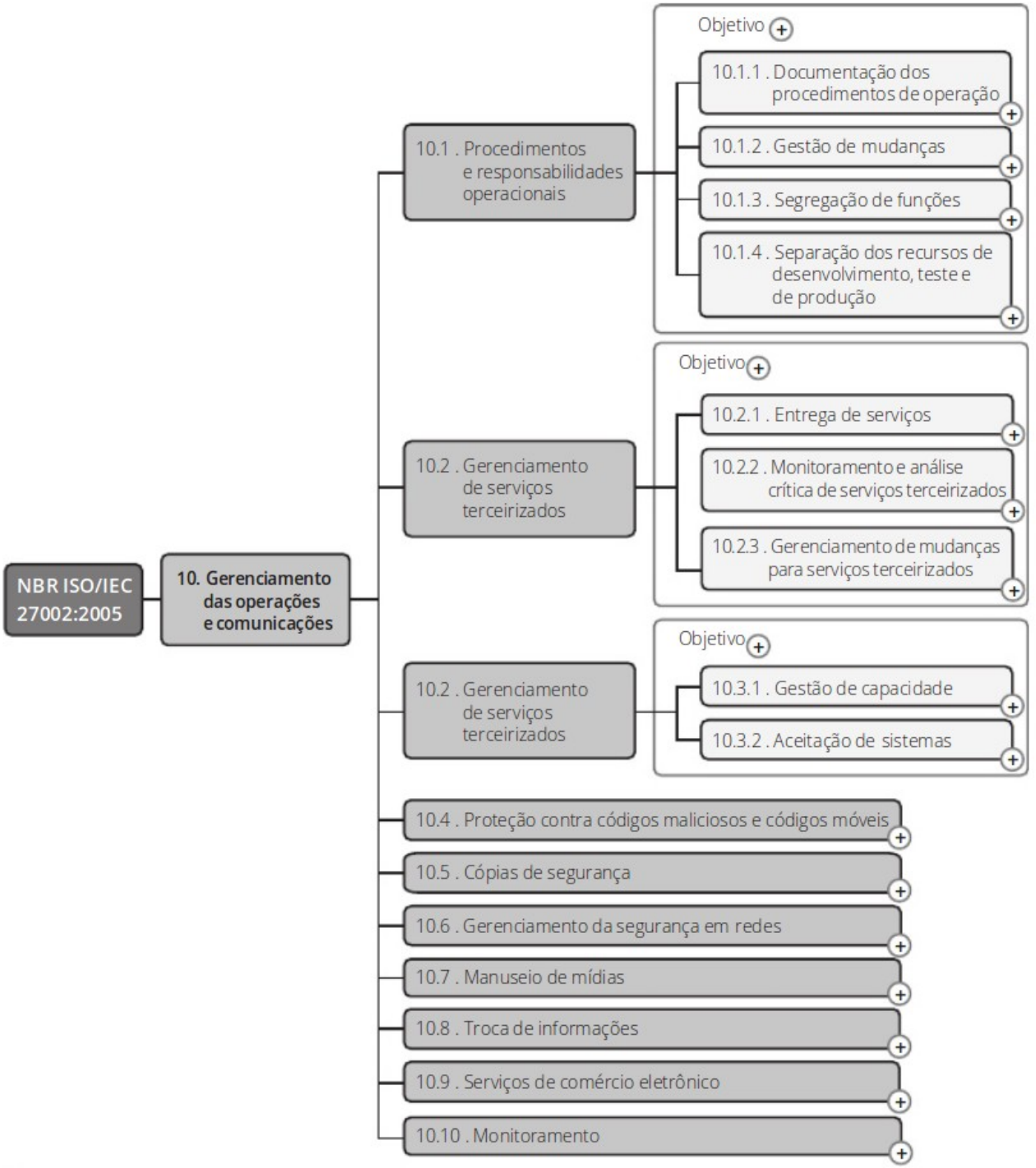
Figura 2.8
Seção 8 - Categorias principais de segurança 8.1, 8.2 e 8.3 com seus controles.

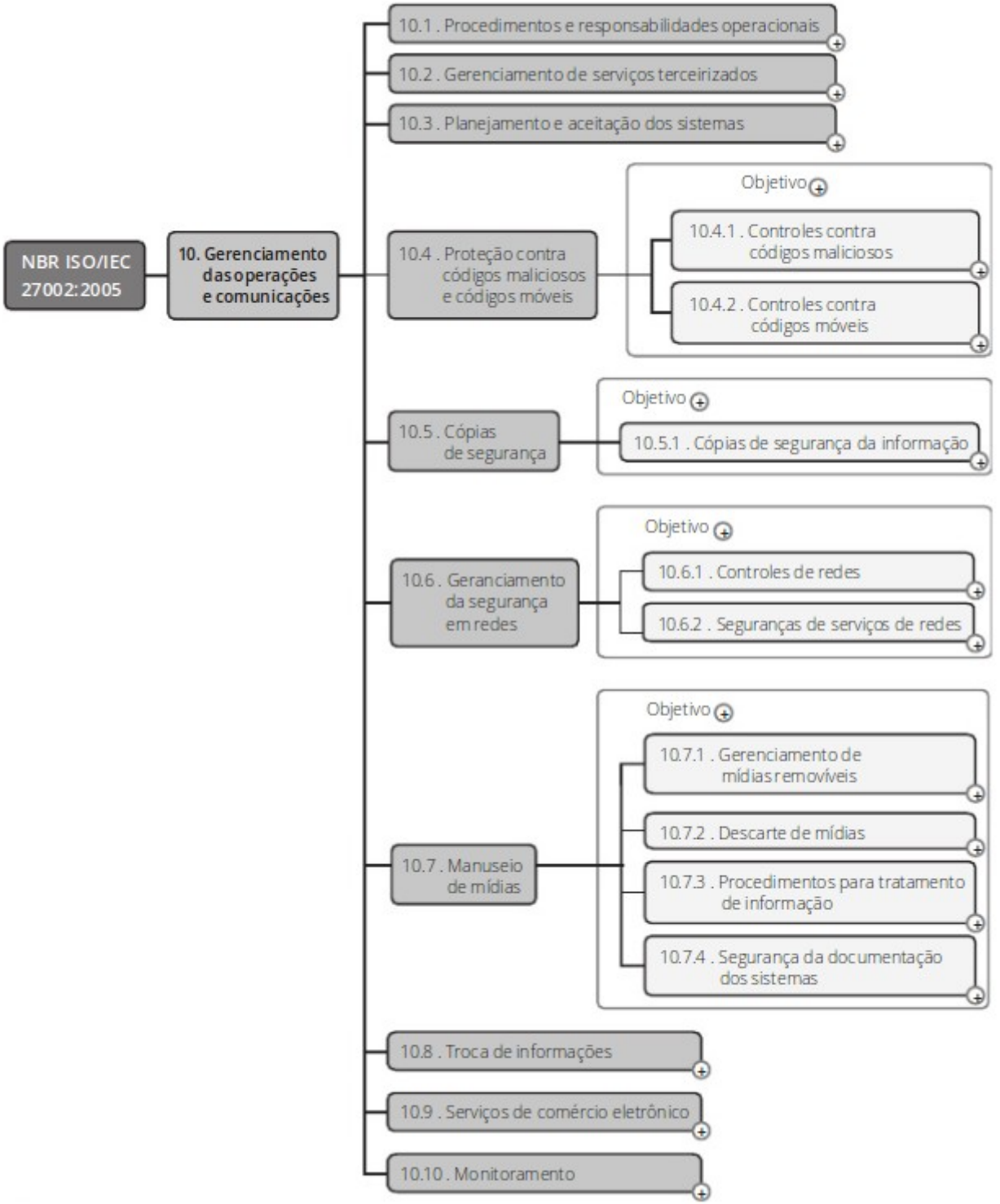


Seção 9 – Segurança física e do ambiente



Seção 10 – Gerenciamento das operações e comunicações




NBR ISO/IEC 27002:2005
10. Gerenciamento das operações e comunicações
10.1 . Procedimentos e responsabilidades operacionais
10.2 . Gerenciamento de serviços terceirizados
10.3 . Planejamento e aceitação dos sistemas
10.4 . Proteção contra códigos maliciosos e códigos móveis
Objetivo
10.4.1 . Controles contra códigos maliciosos
10.4.2 . Controles contra códigos móveis
10.5 . Cópias de segurança
Objetivo
10.5.1 . Cópias de segurança da informação
10.6 . Geranciamento da segurança em redes
Objetivo
10.6.1 . Controles de redes
10.6.2 . Seguranças de serviços de redes
10.7 . Manuseio de mídias
Objetivo
10.7.1 . Gerenciamento de mídias removíveis
10.7.2 . Descarte de mídias
10.7.3 . Procedimentos para tratamento de informação
10.7.4 . Segurança da documentação dos sistemas
10.8 . Troca de informações
10.9 . Serviços de comércio eletrônico
10.10 . Monitoramento

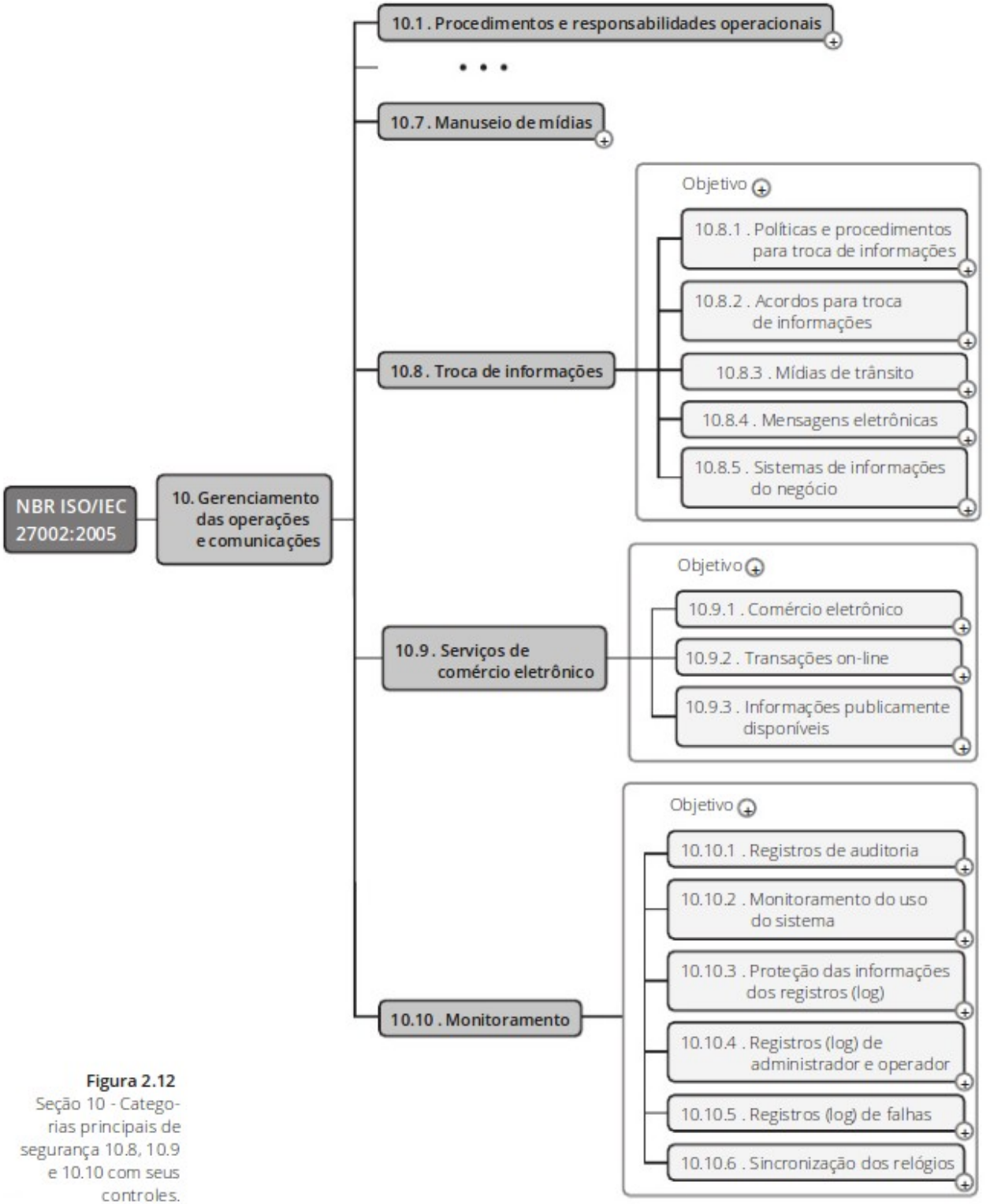
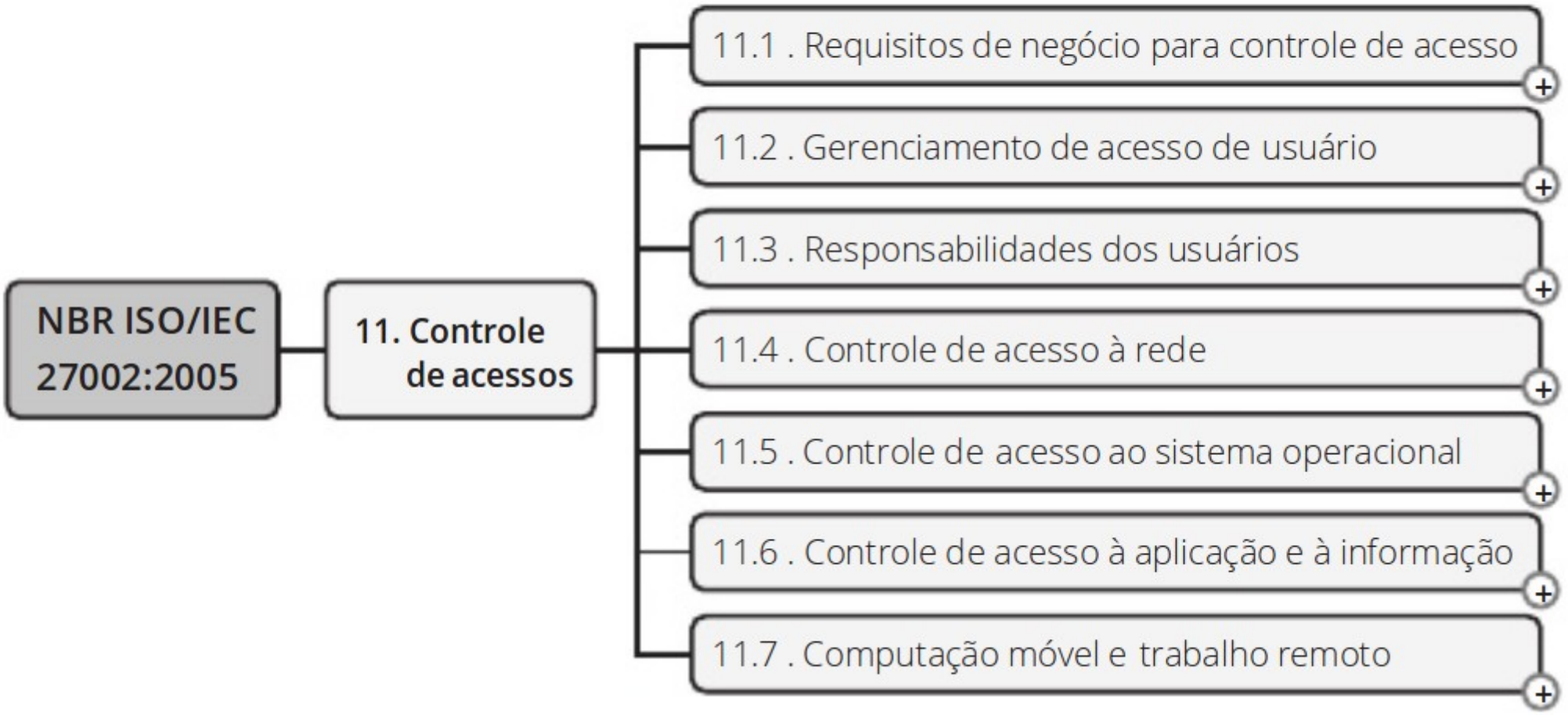
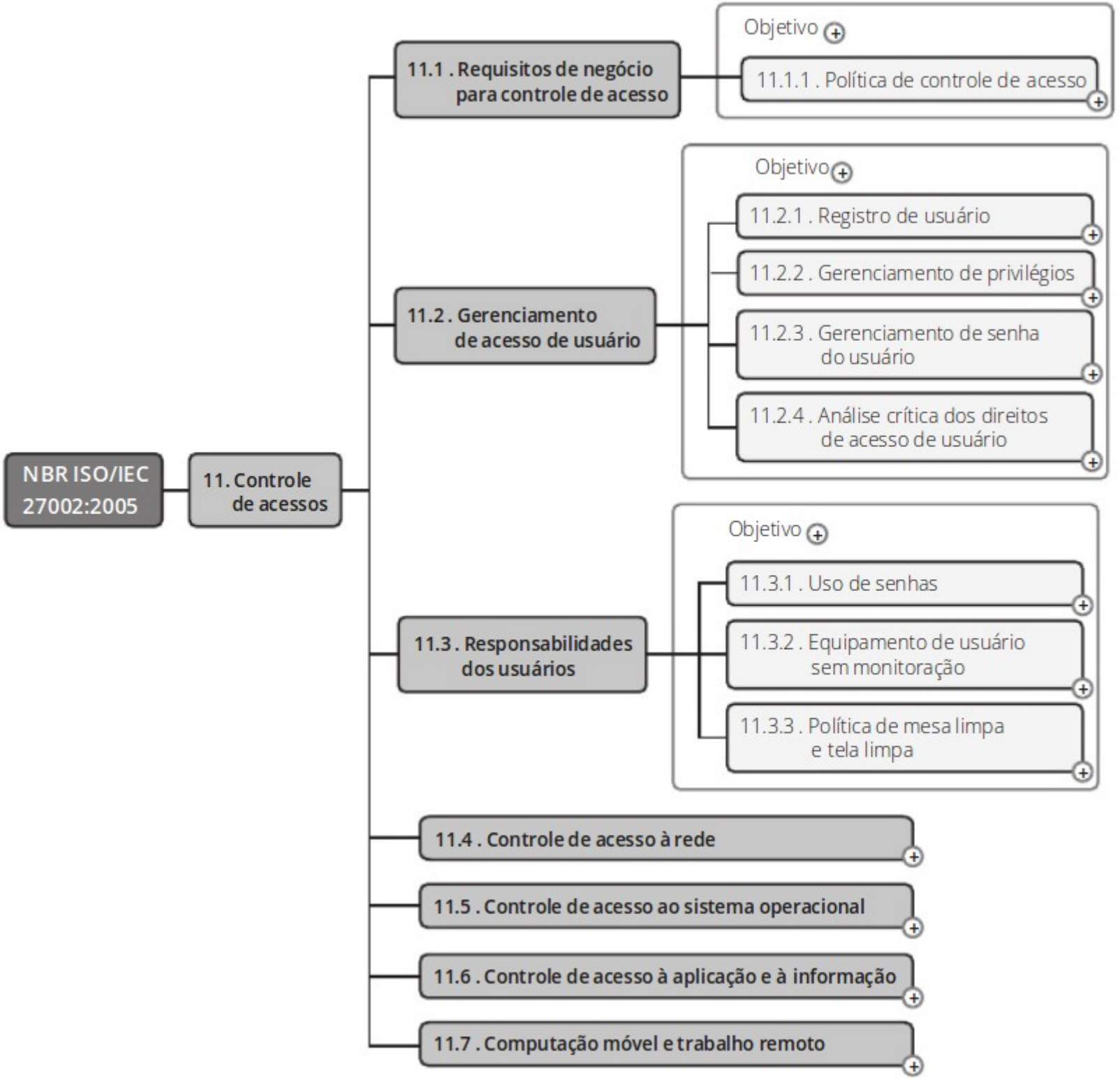


Figura 2.12
Seção 10 - Categorias principais de segurança 10.8, 10.9 e 10.10 com seus controles.

Seção 11 – Controle de acessos




NBR ISO/IEC 27002:2005
11. Controle de acessos
11.1 . Requisitos de negócio para controle de acesso
Objetivo
11.1.1 . Política de controle de acesso
11.2 . Gerenciamento de acesso de usuário
Objetivo
11.2.1 . Registro de usuário
11.2.2 . Gerenciamento de privilégios
11.2.3 . Gerenciamento de senha do usuário
11.2.4 . Análise crítica dos direitos de acesso de usuário
11.3 . Responsabilidades dos usuários
Objetivo
11.3.1 . Uso de senhas
11.3.2 . Equipamento de usuário sem monitoração
11.3.3 . Política de mesa limpa e tela limpa
11.4 . Controle de acesso à rede
11.5 . Controle de acesso ao sistema operacional
11.6 . Controle de acesso à aplicação e à informação
11.7 . Computação móvel e trabalho remoto

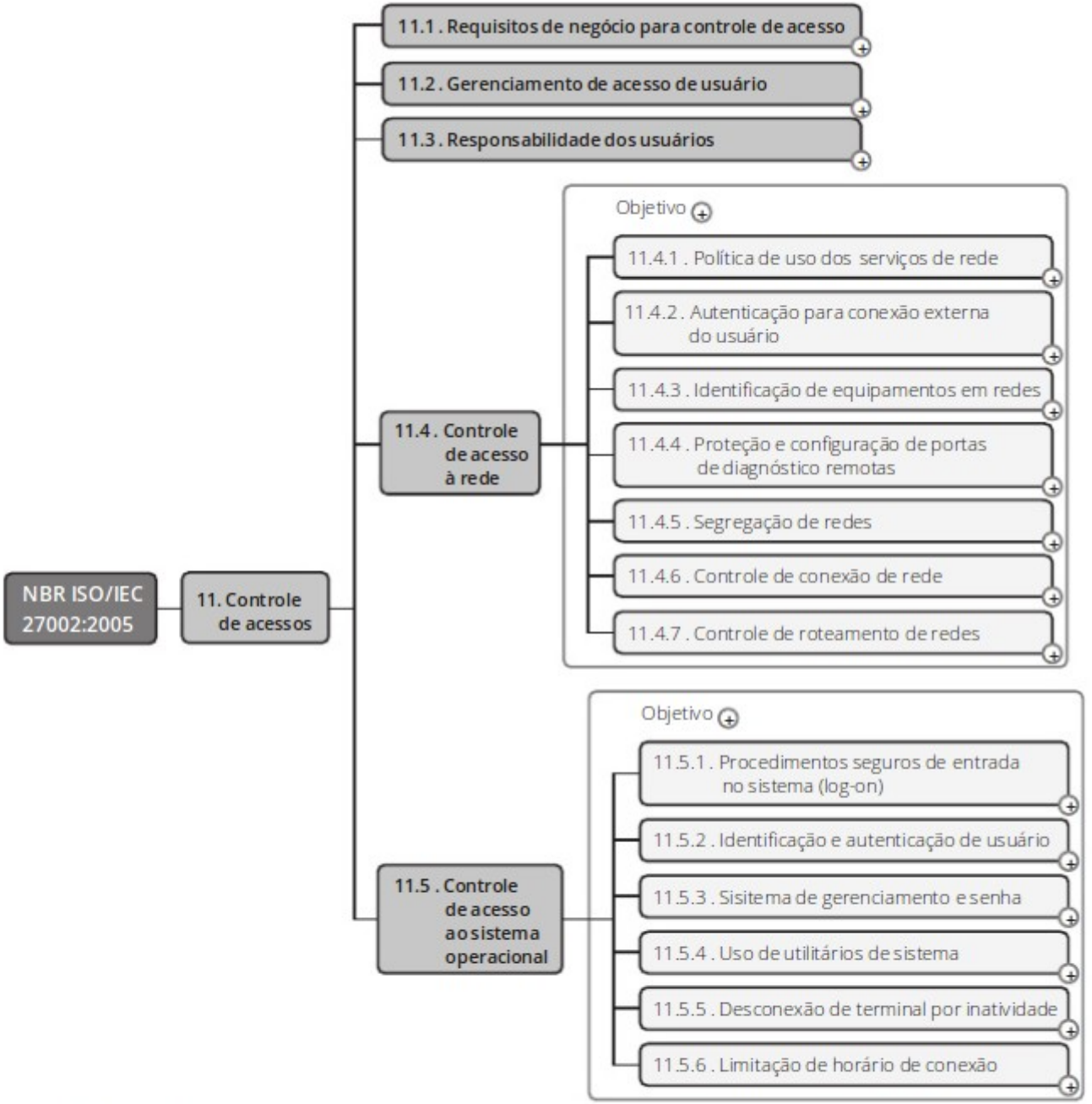
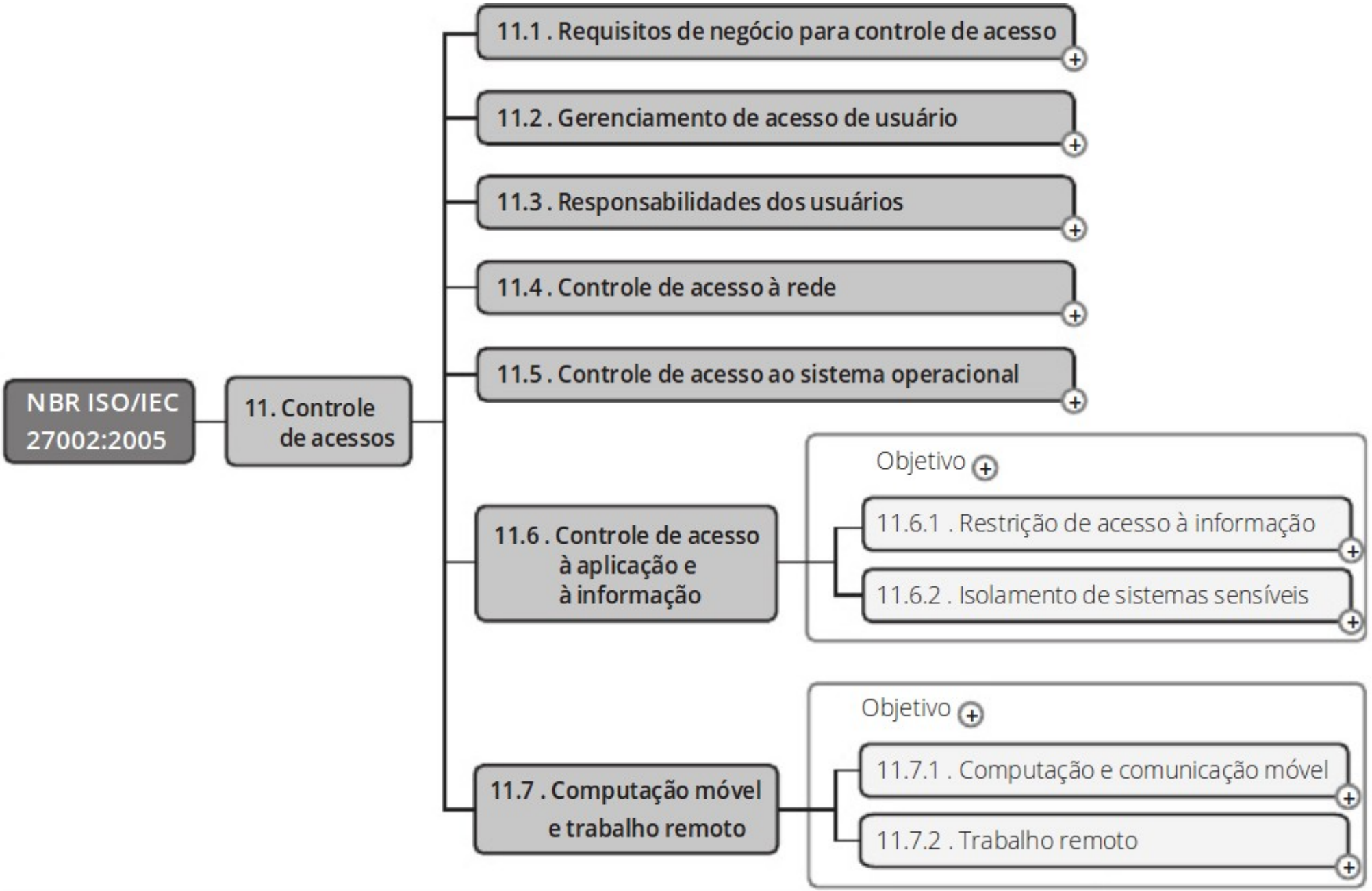
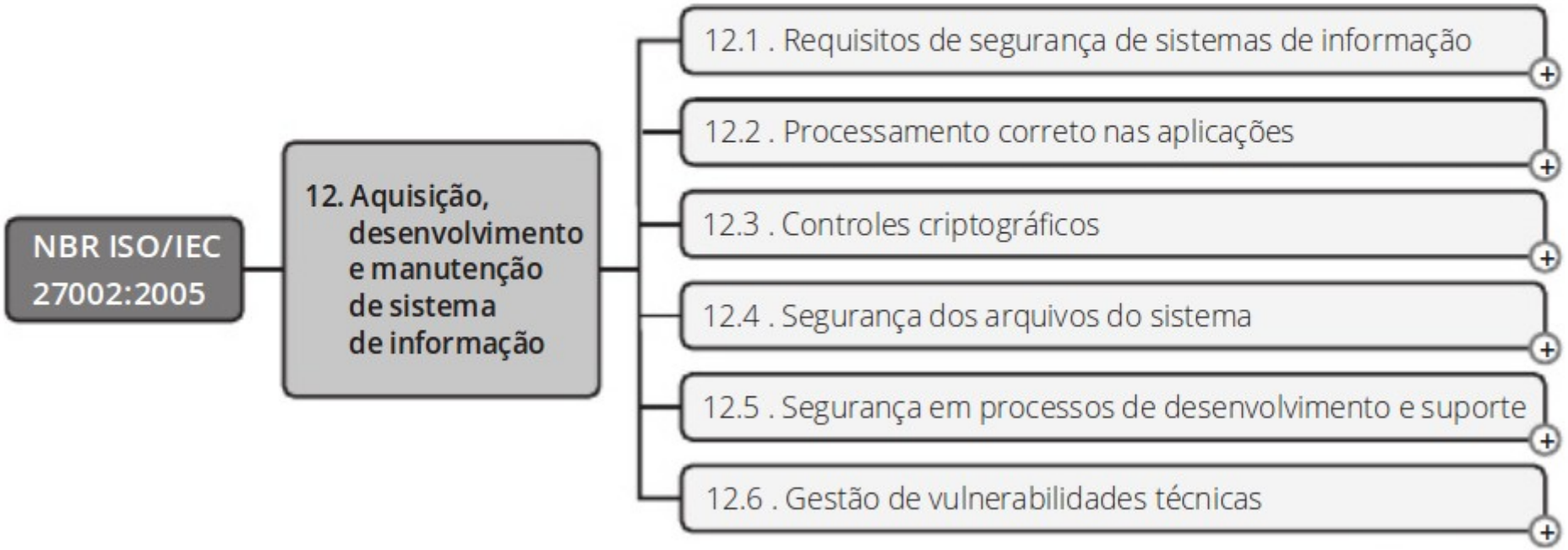
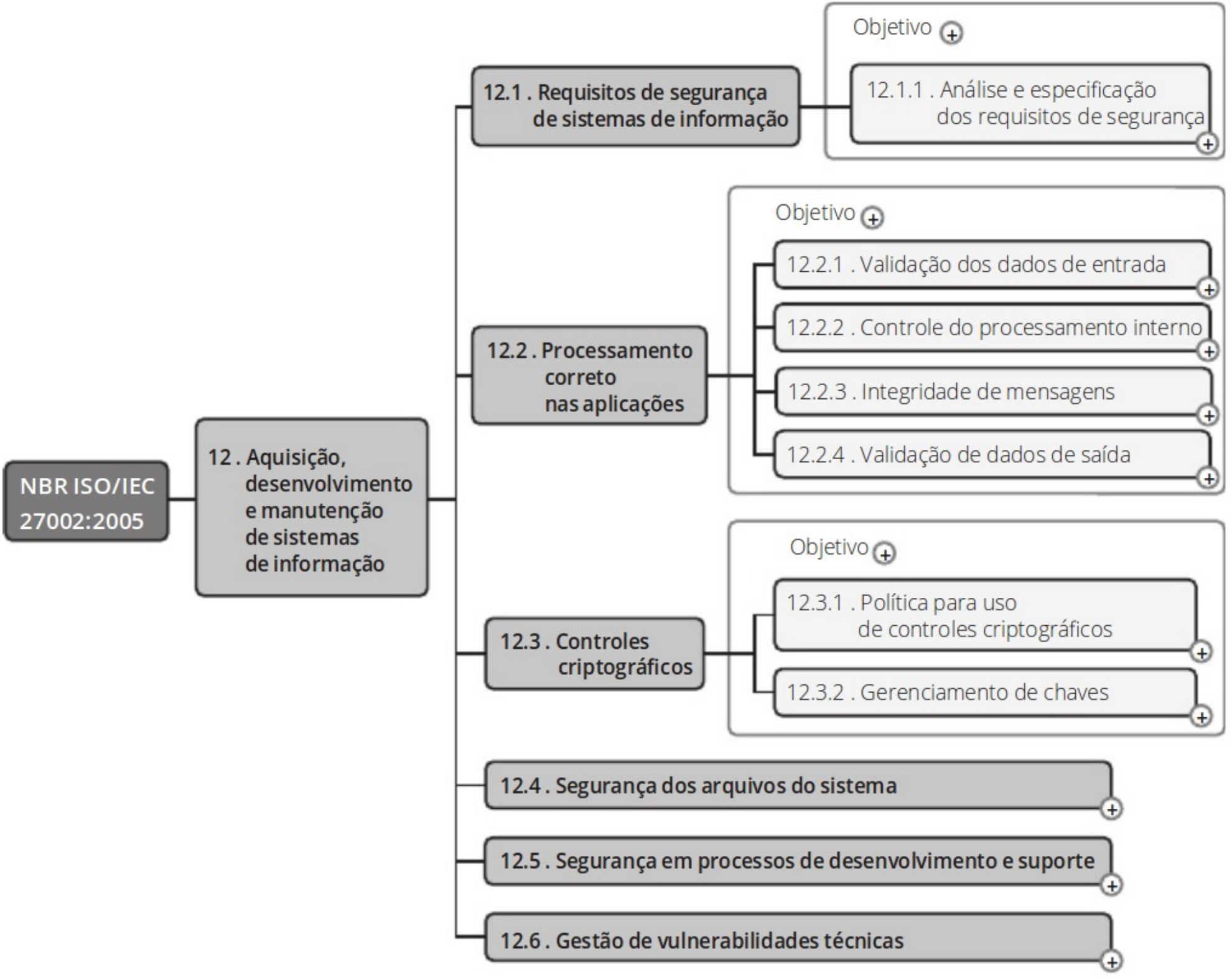


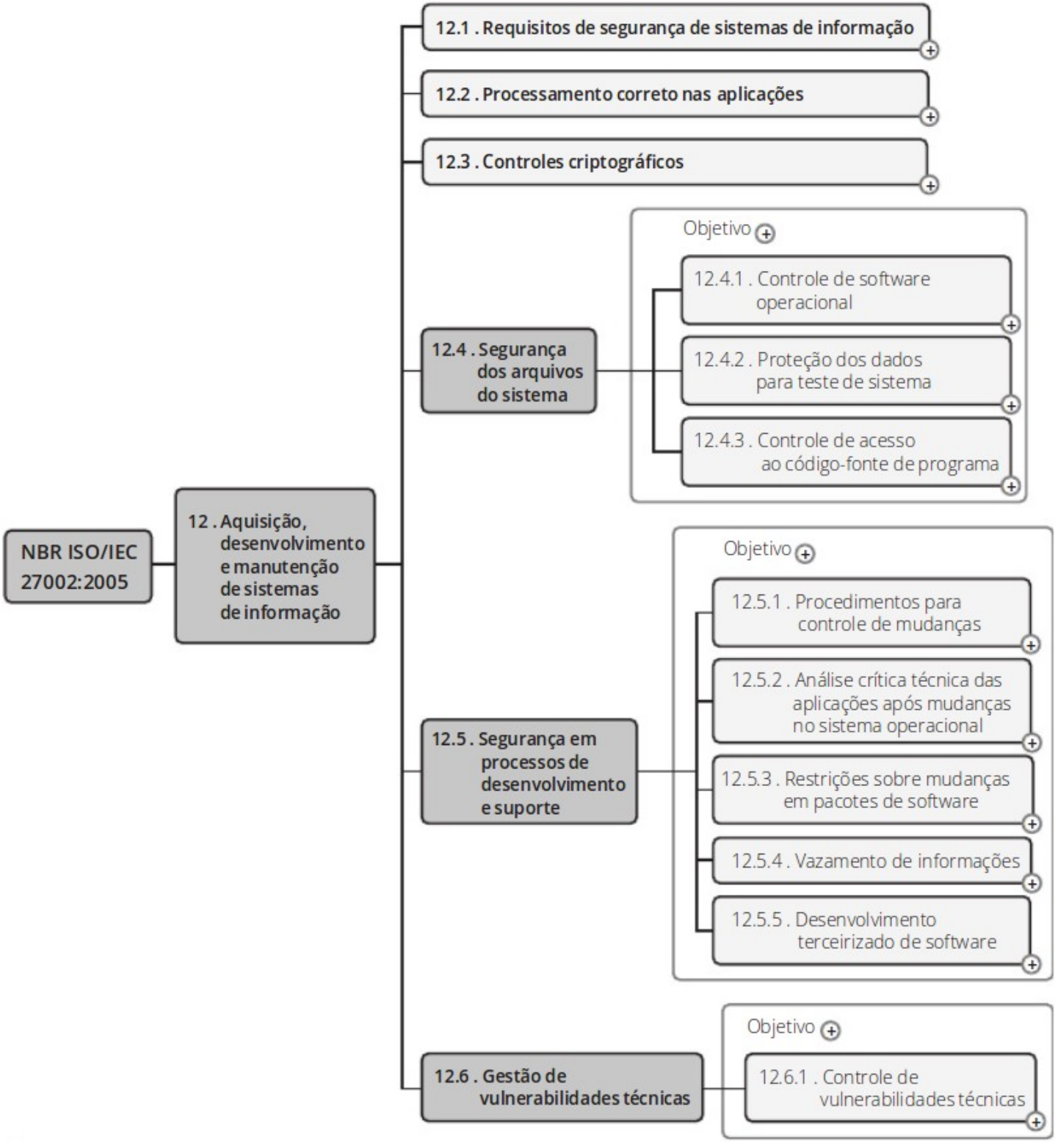
Figura 2.15
Seção 11 - Categorias principais de segurança 11.4 e 11.5 com seus controles.


NBR ISO/IEC 27002:2005
11. Controle de acessos
11.1 . Requisitos de negócio para controle de acesso
11.2 . Gerenciamento de acesso de usuário
11.3 . Responsabilidades dos usuários
11.4 . Controle de acesso à rede
11.5 . Controle de acesso ao sistema operacional
11.6 . Controle de acesso à aplicação e à informação
Objetivo
11.6.1 . Restrição de acesso à informação
11.6.2 . Isolamento de sistemas sensíveis
11.7 . Computação móvel e trabalho remoto
Objetivo
11.7.1 . Computação e comunicação móvel
11.7.2 . Trabalho remoto

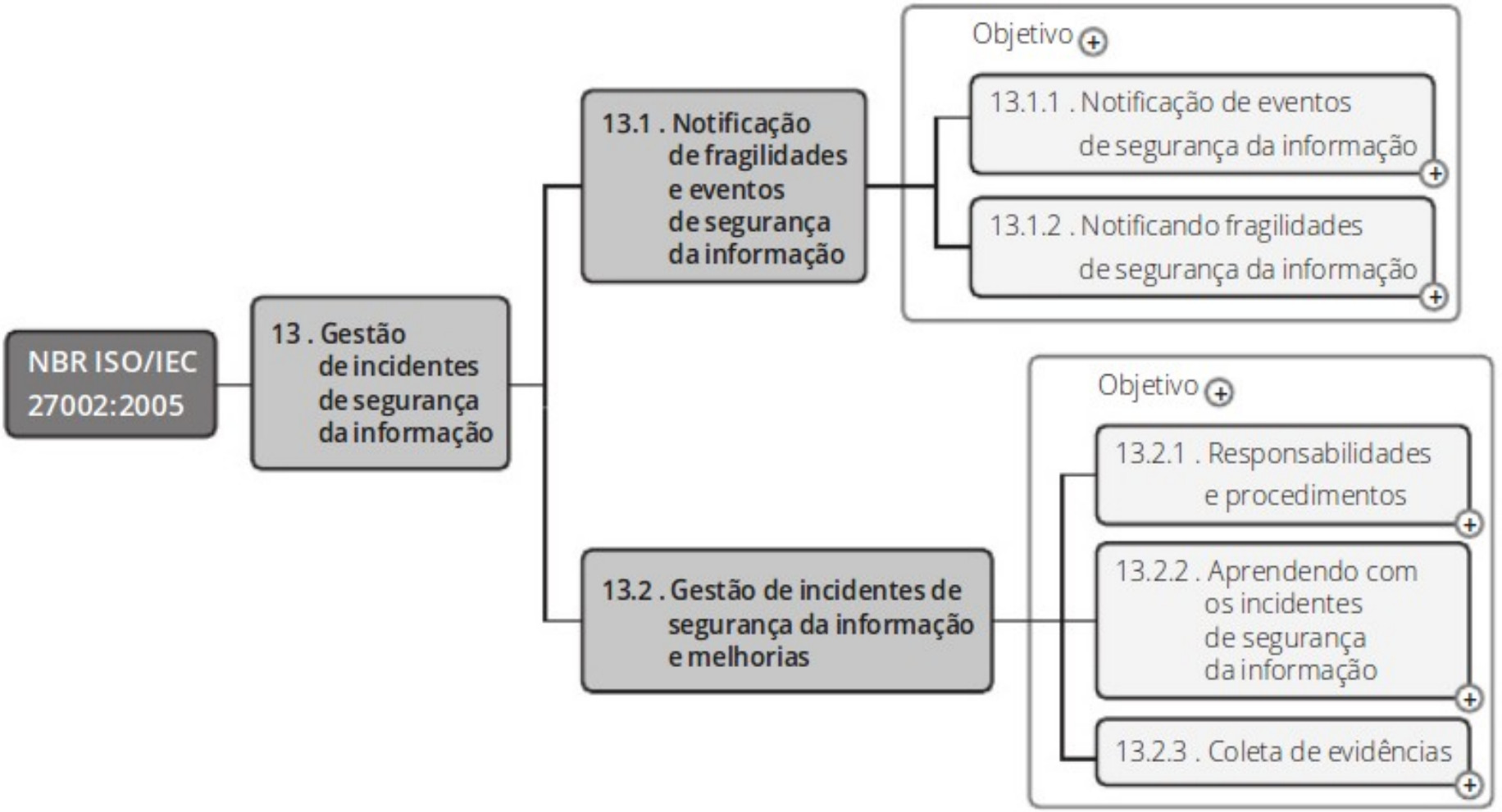
Seção 12 – Aquisição, desenvolvimento e manutenção de sistemas de informação



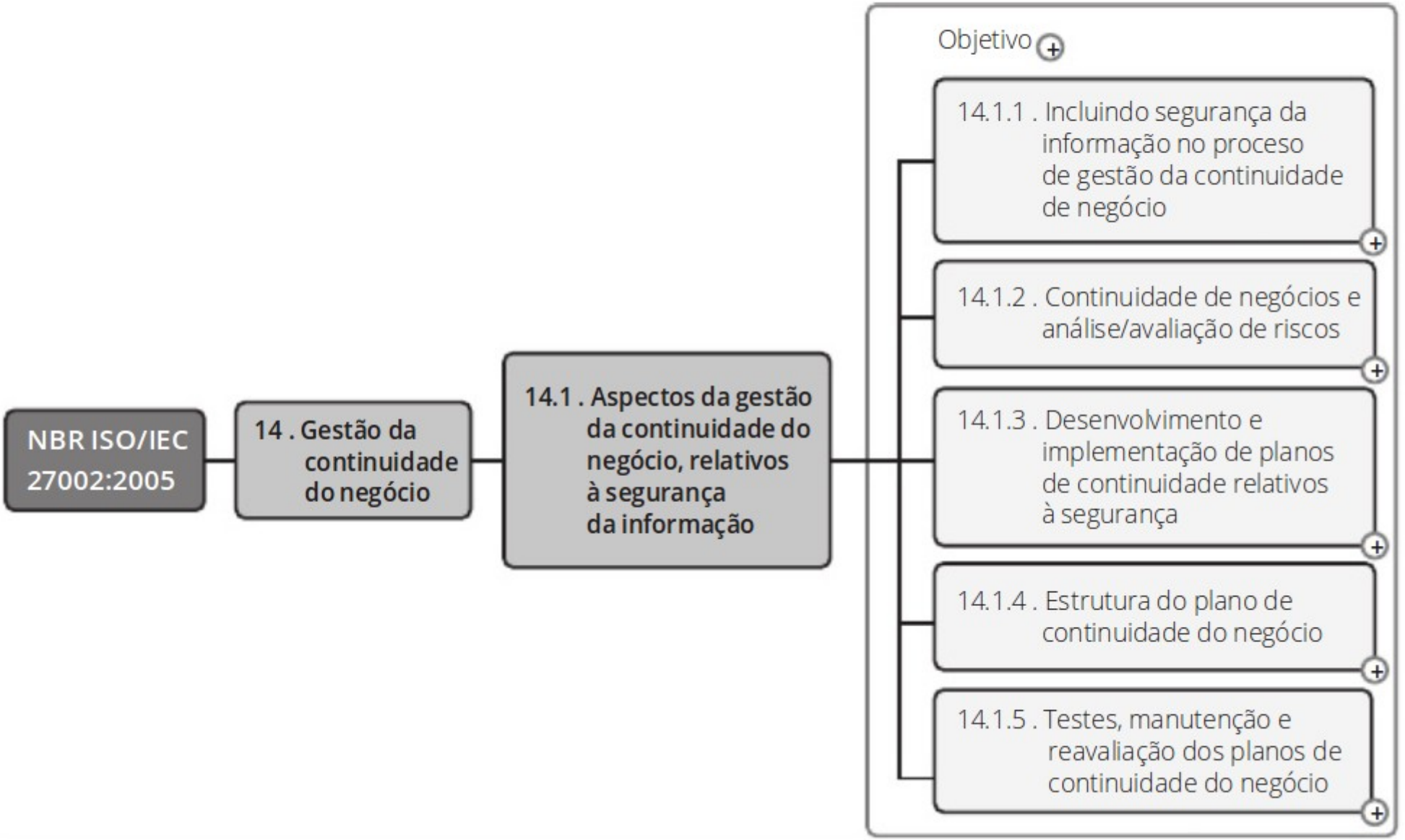

NBR ISO/IEC 27002:2005
12 . Aquisição, desenvolvimento e manutenção de sistemas de informação
12.1 . Requisitos de segurança de sistemas de informação
Objetivo
12.1.1 . Análise e especificação dos requisitos de segurança
12.2 . Processamento correto nas aplicações
Objetivo
12.2.1 . Validação dos dados de entrada
12.2.2 . Controle do processamento interno
12.2.3 . Integridade de mensagens
12.2.4 . Validação de dados de saída
12.3 . Controles criptográficos
Objetivo
12.3.1 . Política para uso de controles criptográficos
12.3.2 . Gerenciamento de chaves
12.4 . Segurança dos arquivos do sistema
12.5 . Segurança em processos de desenvolvimento e suporte
12.6 . Gestão de vulnerabilidades técnicas


NBR ISO/IEC 27002:2005
12 . Aquisição, desenvolvimento e manutenção de sistemas de informação
12.1 . Requisitos de segurança de sistemas de informação
12.2 . Processamento correto nas aplicações
12.3 . Controles criptográficos
12.4 . Segurança dos arquivos do sistema
Objetivo
12.4.1 . Controle de software operacional
12.4.2 . Proteção dos dados para teste de sistema
12.4.3 . Controle de acesso ao código-fonte de programa
12.5 . Segurança em processos de desenvolvimento e suporte
Objetivo
12.5.1 . Procedimentos para controle de mudanças
12.5.2 . Análise crítica técnica das aplicações após mudanças no sistema operacional
12.5.3 . Restrições sobre mudanças em pacotes de software
12.5.4 . Vazamento de informações
12.5.5 . Desenvolvimento terceirizado de software
12.6 . Gestão de vulnerabilidades técnicas
Objetivo
12.6.1 . Controle de vulnerabilidades técnicas

Seção 13 – Gestão de incidentes de segurança da informação



Seção 14 – Gestão da continuidade do negócio



Seção 15 – Conformidade