Segurança de Redes

Curso Superior de Tecnologia em Redes de Computadores
Prof. Macêdo Firmino

Sistema de Gestão da Segurança da Informação (SGSI)

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Segurança da Informação

Segurança da Informação compreende a proteção das informações, sistemas, recursos e demais ativos contra desastres, erros (intencionais ou não) e manipulação não autorizada, objetivando a redução da probabilidade e do impacto de incidentes de segurança.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Controle

A segurança da informação é obtida como resultado da implementação de um **conjunto de controles**, compreendendo políticas, processos, procedimentos, diretrizes, estruturas organizacionais e funções de *hardware* e *software*. Esses controles são medidas para tratar vulnerabilidades e reduzir o risco de incidentes de segurança da informação. Elas podem ser de natureza administrativa, técnica, de gestão ou legal.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Vulnerabilidade

Para implementar esses controles, precisamos conhecer as **vulnerabilidades e analisar os riscos**. Entretanto, elas surgem diariamente. Dessa forma, precisamos fazer essas análises de forma dinâmica e atualizada, permitindo o levantamento das vulnerabilidades, dos níveis dos riscos e da forma de tratá-los.

Vulnerabilidade é qualquer fraqueza (falhas) que possa ser explorada e comprometer a segurança de sistemas ou informações. A partir dessa falha, as ameaças exploram as vulnerabilidades, que, quando concretizadas, resultam em danos para o computador, para a organização ou para os dados pessoais.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Análise de Riscos

Análise de riscos é uma combinação da probabilidade (chance da ameaça se concretizar) de um evento ocorrer e de suas consequências para a organização, ou seja, algo que pode ocorrer e seus efeitos na organização.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Legislação

Também é necessário conhecer a **legislação** que a organização é obrigada a seguir e a levantar os requisitos de segurança necessários para a organização.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Pergunta???

Se eu empresa lhe contratasse para implementar a segurança da informação dela, o que você faria?

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Passos

Resumidamente para implementar mecanismos de segurança da informação devemos:

- Conhecendo a organização.
- Levantamento dos requisitos de segurança.
- Análise e avaliação de riscos.
- Seleção de controles.
- Itens relevantes.
- Atividades envolvidas.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Conhecendo a Organização

- O que proteger?
- Contra o quê ou quem?
- Qual a importância de cada recurso?
- Qual o grau de proteção desejado?
- Quanto tempo, recursos financeiros e humanos se pretende gastar para atingir os objetivos de segurança desejados?
- Quais as expectativas dos diretores, clientes e usuários em relação à segurança da informação?

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Requisitos de Segurança

- Identificar as vulnerabilidades e ameaças que pretendemos evitar. Levando em conta a probabilidade de ocorrência e o impacto para o negócio.
- Legislação vigente, estatutos, regulamentações e cláusulas contratuais da organização.
- Conjunto de princípios, objetivos e requisitos do negócio.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Análise e Avaliação de Riscos

- Como não se pode garantir que jamais ocorrerá riscos à segurança, precisamos determinar a importância dos riscos para a organização.
- Os gastos com controles precisam ser balanceados de acordo com o impacto que falhas potenciais de segurança causarão aos negócios.
- Essa análise e avaliação devem ser feitas periódicamente, para contemplar mudanças na organização.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Seleção de Controles

- Após a identificação de requisitos de segurança e análise/avaliação dos riscos, pode-se, enfim, selecionar e implementar os controles adequados para garantir a **redução de riscos**.
- Inclui políticas, procedimentos, diretrizes, práticas ou estruturas organizacionais, que podem ser de natureza administrativa, técnica, de gestão ou legal.
- Podem ser selecionados a partir de normas preestabelecidas ou de conjunto de controles específicos. Por exemplo, as normas:
  - ABNT NBR ISO/IEC 27001:2013 (Requisitos de Sistemas de Gestão de Segurança da Informação).
  - ABNT NBR ISO/IEC 27002:2013 (Código de Prática para controles na Gestão de Segurança da Informação).

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Seleção de Controles

Exemplos de controle:

- Barreiras, portas, cartazes de "proibida a entrada" e catracas;
- Crachás, controle de visitantes e CFTV;
- Senhas, fechaduras e controles biométricos;
- Políticas de segurança e termos de responsabilidade;
- Conscientização, educação e treinamento em segurança da informação.
- Antivírus, firewall, VPN, IDS, backup e controle de acesso lógico.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Itens Relevantes para a Segurança da Informação

São definidos na ABNT NBR ISO/IEC 27002:2013, são eles:

- Política de segurança da informação.
- Segurança organizacional e operacional.
- Gestão de ativos.
- Segurança em Recursos Humanos.
- Segurança física, de ambiente e controle de acesso.
- Gerenciamento de operações e comunicações.
- Aquisição, desenvolvimento e manutenção de SI.
- Gestão de incidentes de segurança.
- Gestão da continuidade do negócio.
- Segurança nas comunicações e Criptografia.

Atividades Envolvidas

- Gerência dos serviços e mecanismos de segurança disponíveis para atender aos requisitos de segurança da organização.
- Gerência da auditoria de segurança, revisando e verificando registros e eventos de segurança, com o objetivo de avaliar a adequação dos controles do sistema, sua aderência à política de segurança, e de recomendar mudanças adequadas ou necessárias aos controles empregados na organização.
- Conseguir o apoio e o comprometimento de todos os níveis gerenciais da organização;
- Os requisitos de segurança da informação, a análise, avaliação e gestão de riscos devem ser bem entendidos (e em detalhes);

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Atividades Envolvidas

- Divulgar, de modo eficiente, as normativas de segurança da informação a todas as entidades da organização (presidentes, diretores, gerentes, funcionários, contratados etc.).
- Garantir recursos financeiros para a gestão da segurança da informação.
- Prover meios de conscientização, treinamento e educação adequados.
- Estabelecer um processo eficiente para a gestão de incidentes de segurança da informação.
- Implantar um mecanismo para medir e avaliar a efetividade da gestão da segurança da informação, com subsequentes sugestões de melhorias.

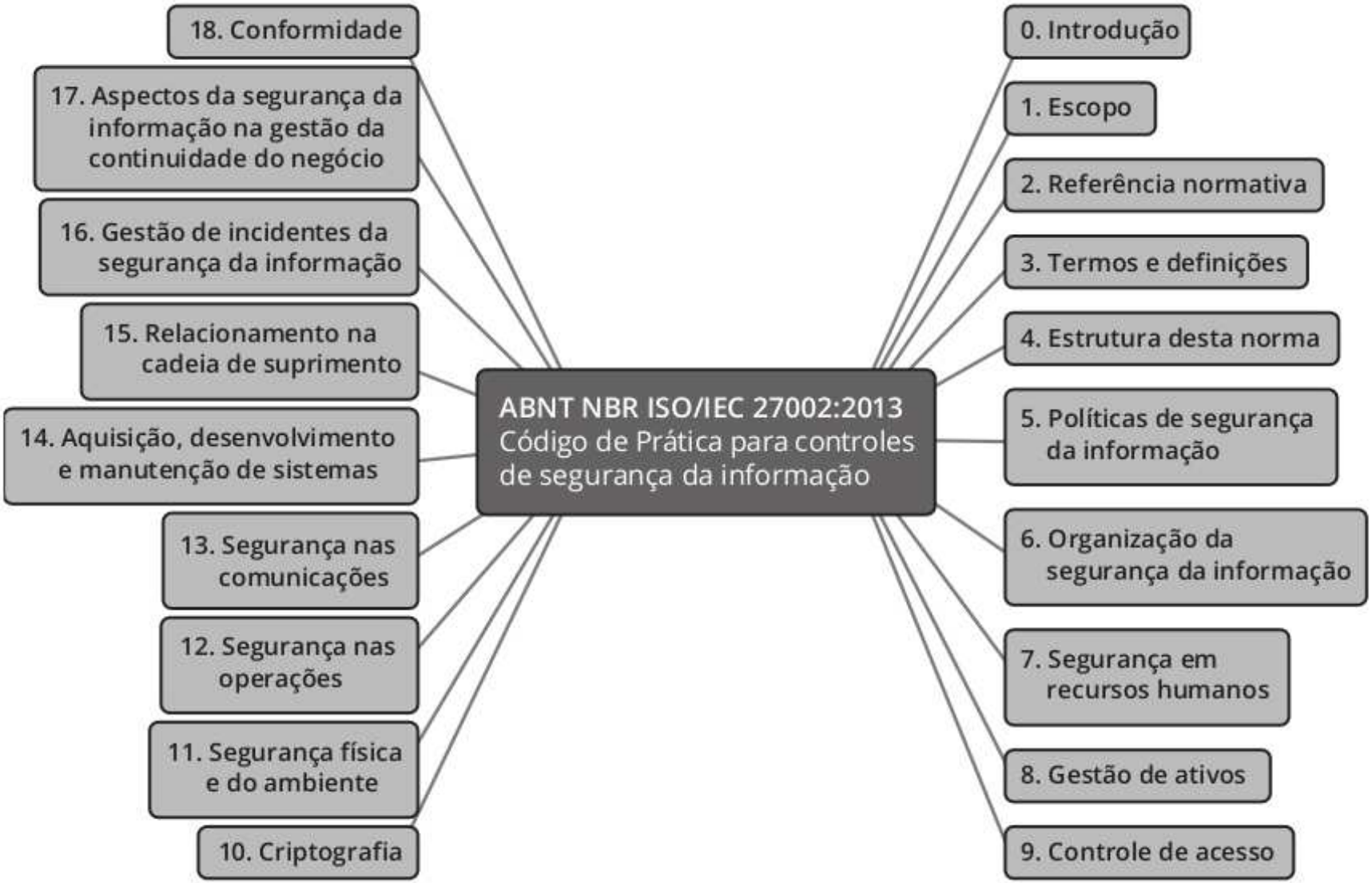
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Norma ABNT NBR ISO/IEC 27002:2013

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. A versão atual possui 114 controles.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Norma ABNT NBR ISO/IEC 27002:2013

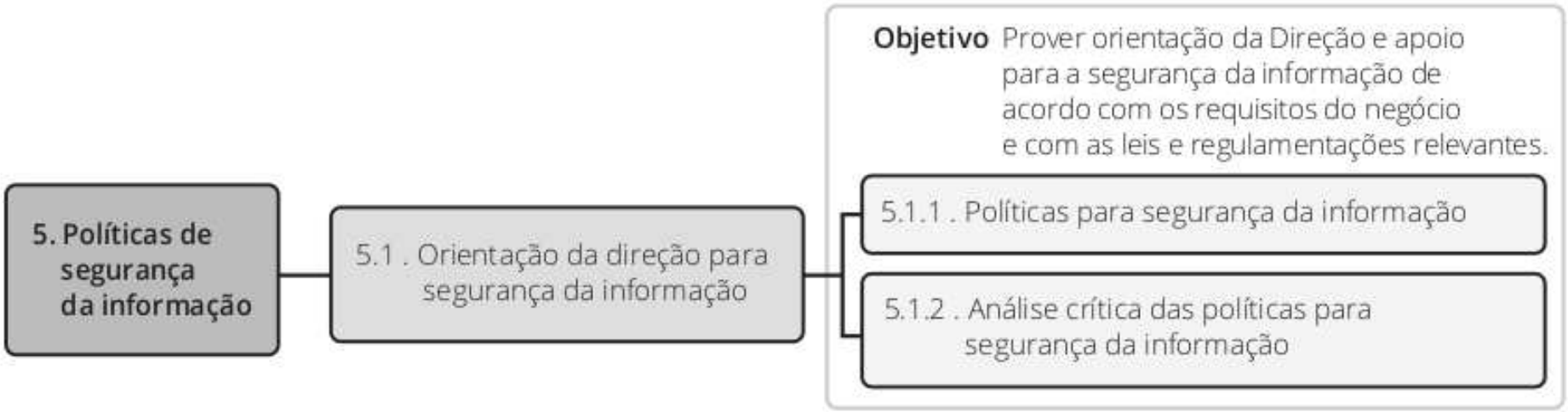


Política de Segurança da Informação

Tem o objetivo de prover orientação e apoio para a segurança da informação de acordo com os requisitos do negócio e com as leis e regulamentações vigentes. Não deve ser definida de modo genérico, para cada organizações devem ser analisadas, de forma a identificar suas necessidades de segurança para que, assim, seja desenvolvida e implantada uma política adequada.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Política de Segurança da Informação



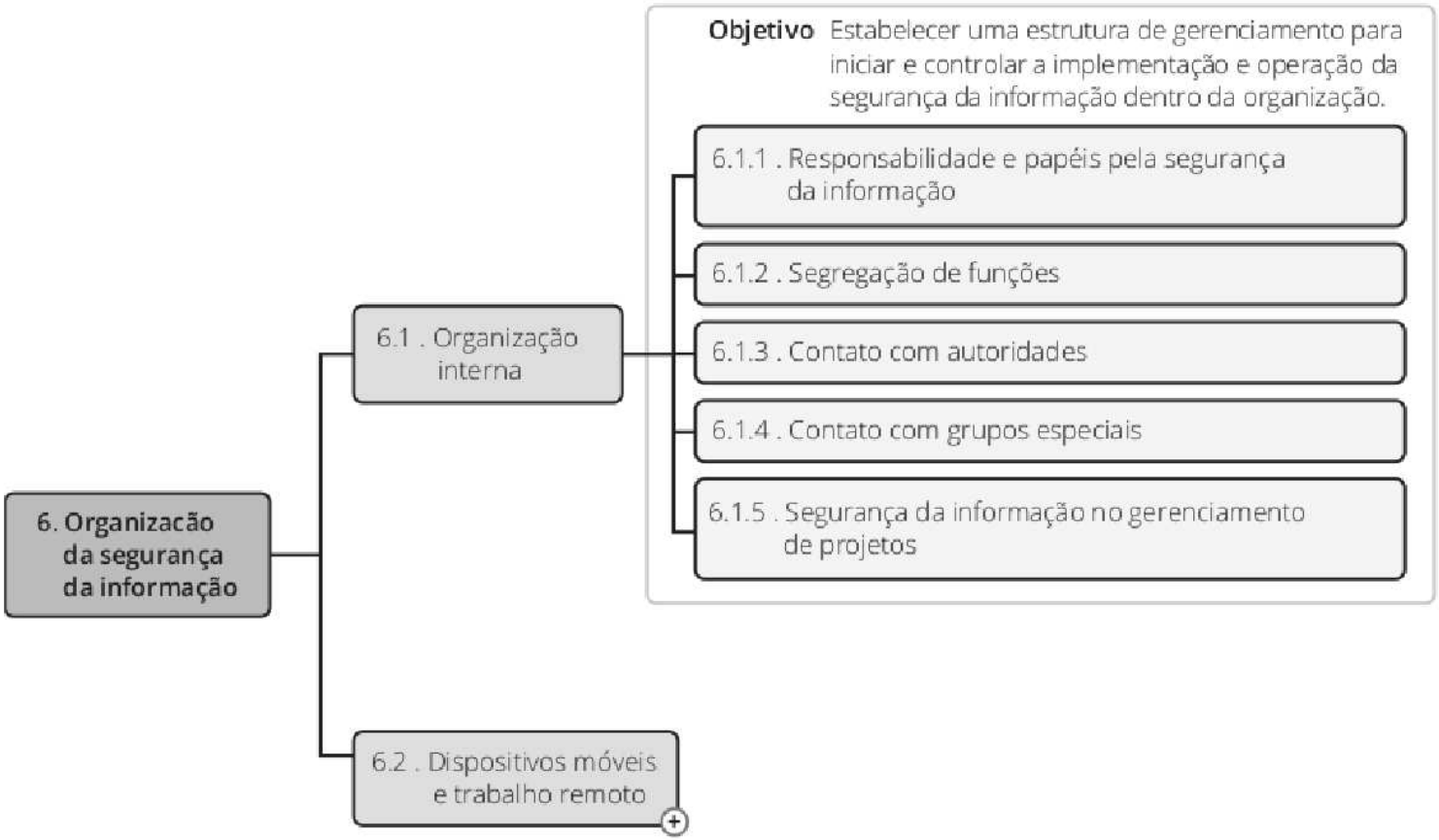
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Organização da Segurança da Informação

Tem como objetivos apresentar controles para uma estrutura para gerenciar a segurança da informação dentro da organização e também os controles para que possa ser mantida a segurança dos recursos de processamento da informação, quando disponibilizados através de dispositivos móveis ou trabalho remoto.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Organização da Segurança da Informação



INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

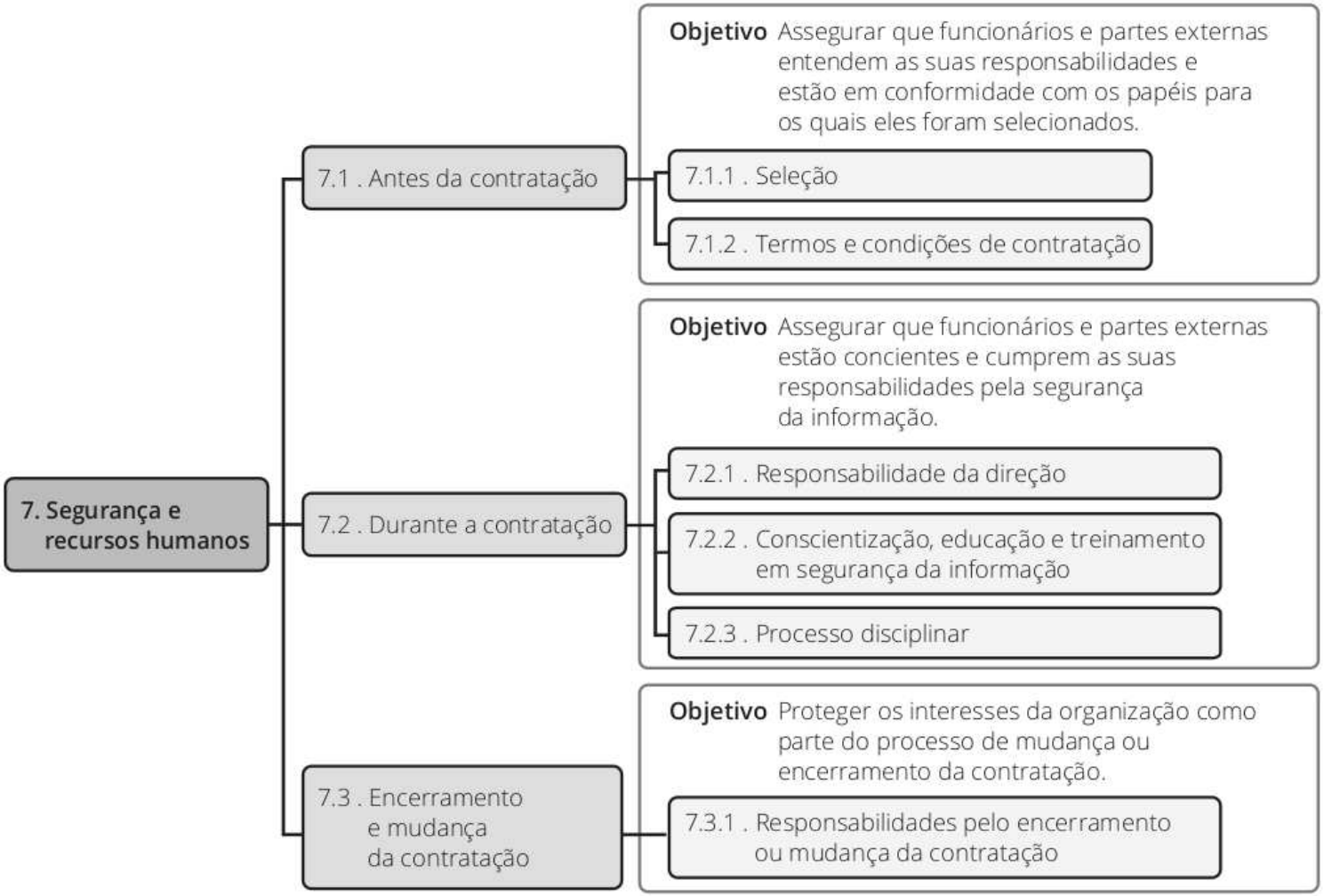
Segurança em Recursos Humanos

Trata dos controles de segurança da informação durante o ciclo de vida da prestação de serviços por profissional na organização.

- Antes da contratação: assegurar que os funcionários e partes externas entendam suas responsabilidades e estejam em conformidade com os papéis para os quais eles foram selecionados.
- Durante a contratação: assegurar que os funcionários e partes externas estejam conscientes e cumpram as suas responsabilidades de segurança da informação.
- Encerramento e mudança da contratação: proteger os interesses da organização como parte do processo de mudança ou encerramento da contratação.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Segurança em Recursos Humanos



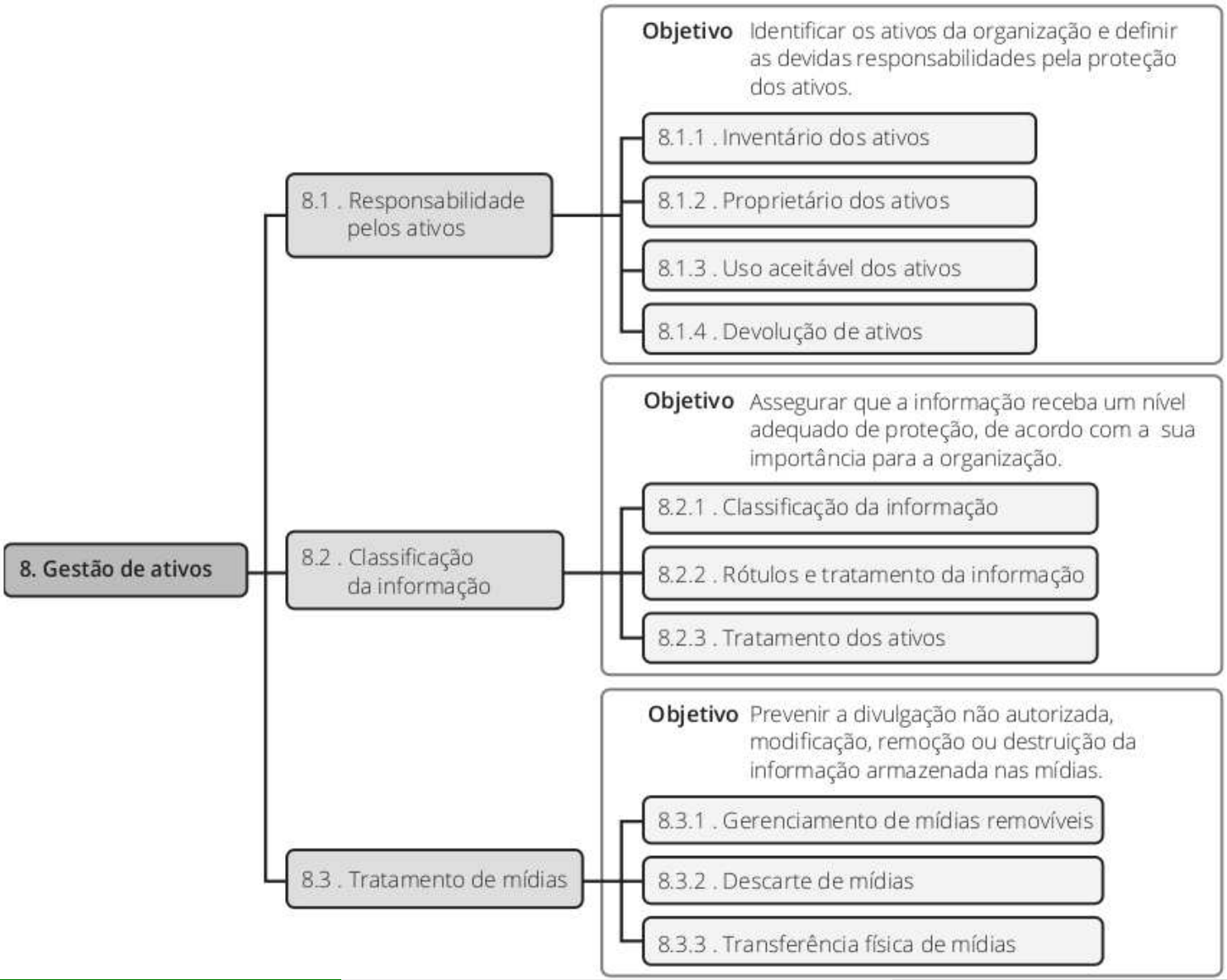
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Gestão de Ativos

- Responsabilidade pelos ativos: identificar os ativos da organização e definir as devidas responsabilidades pela proteção dos ativos. Apresentando os controles que devem ser aplicados no tratamento da segurança da informação nos ativos.
- Classificação das informações: assegurar que a informação receba um nível adequado de proteção, de acordo com a sua importância para a organização.
- Tratamento de mídias: prevenir a divulgação não autorizada, modificação, remoção ou destruição da informação armazenada nas mídias.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Gestão de Ativos



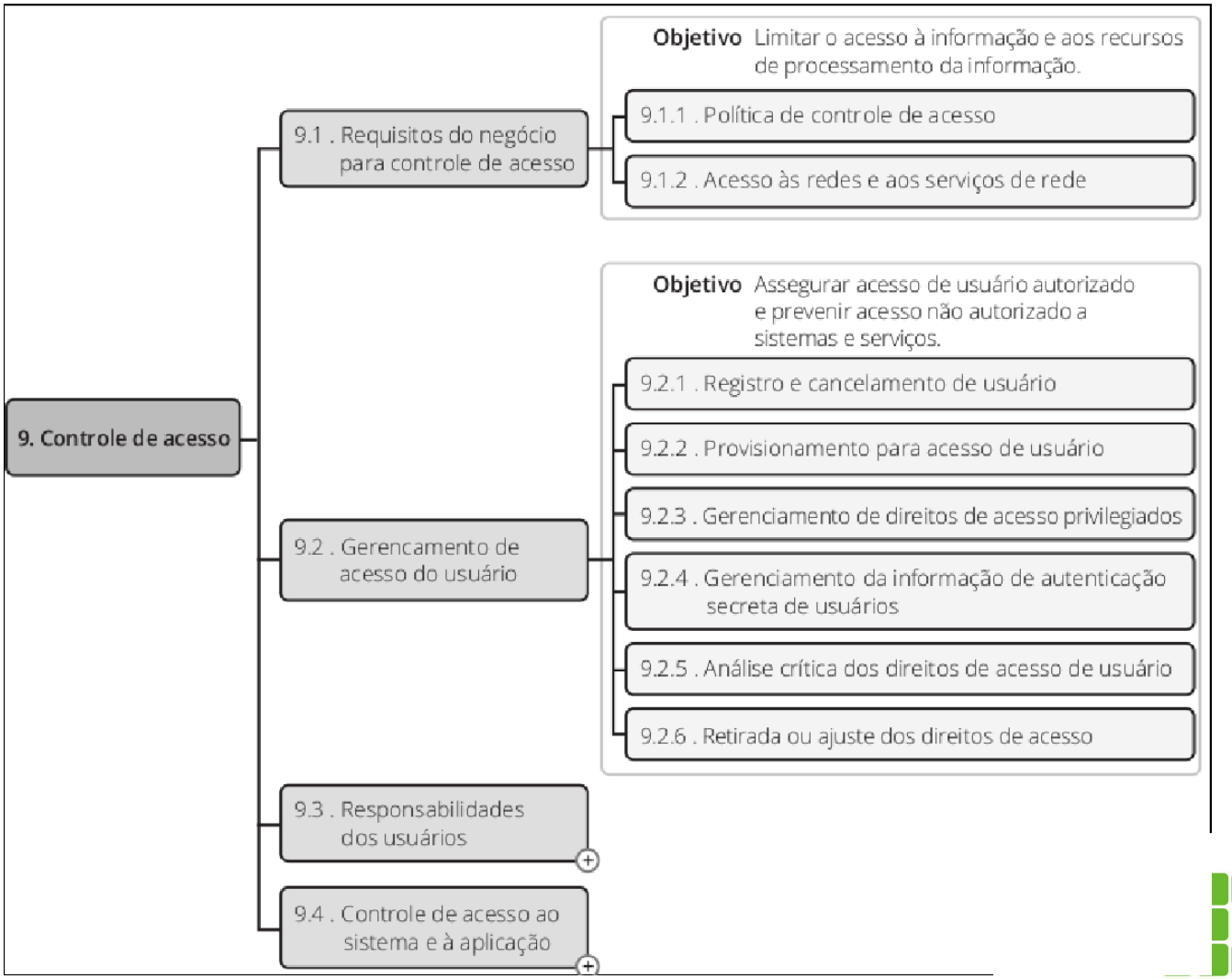
ITUTO FEDERAL DE
CAÇÃO, CIÊNCIA E TECNOLOGIA
RANDE DO NORTE

Controle de Acesso

São encontradas as categorias que tratam dos controles necessários ao controle de acesso lógico. O objetivo são: limitar o acesso à informação e aos recursos de processamento da informação, assegurar o acesso de usuário autorizado e prevenir acesso não autorizado a sistemas e serviços, tornar os usuários responsáveis pela proteção das suas informações de autenticação, prevenir o acesso não autorizado aos sistemas e aplicações.

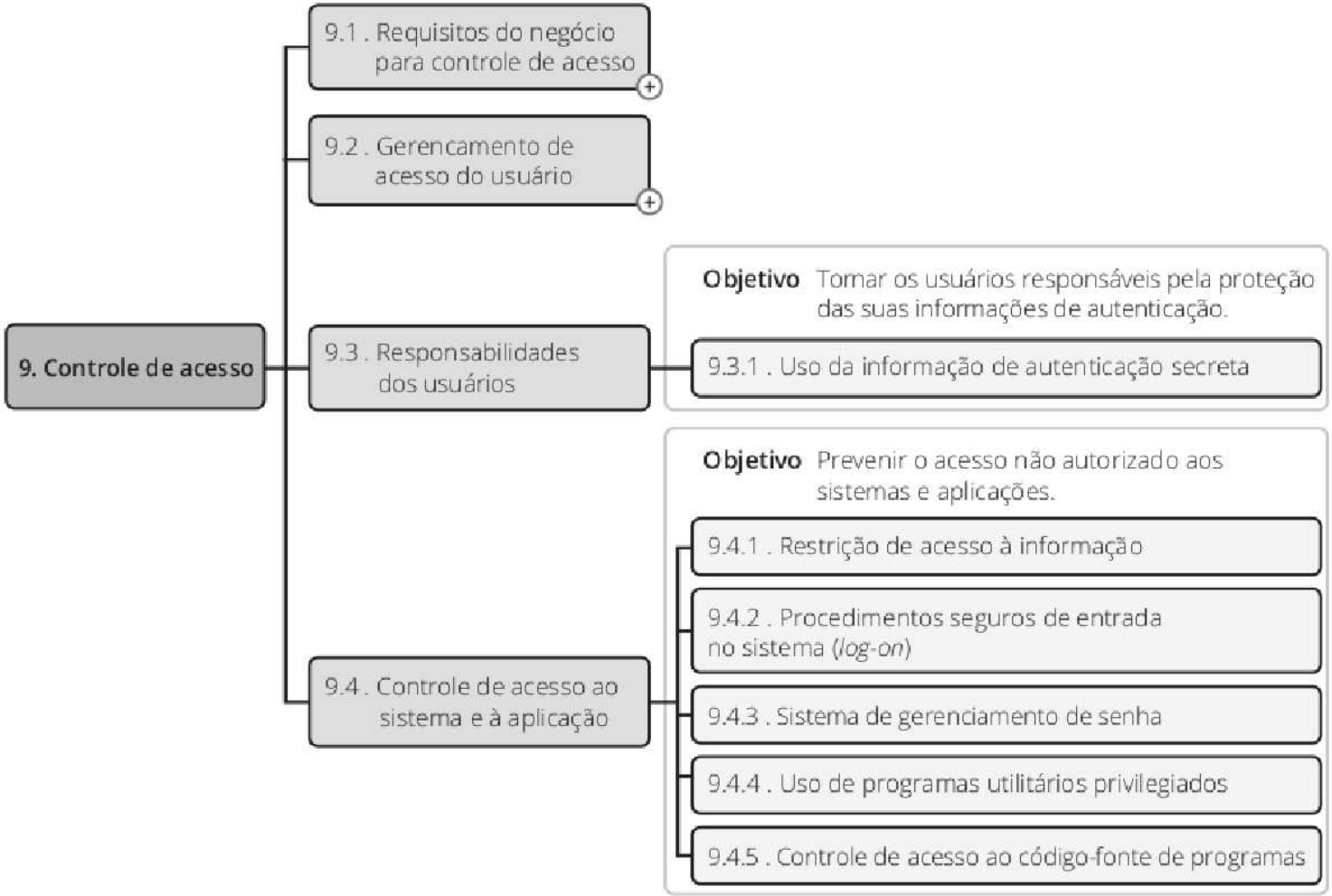
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Controle de Acesso



INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

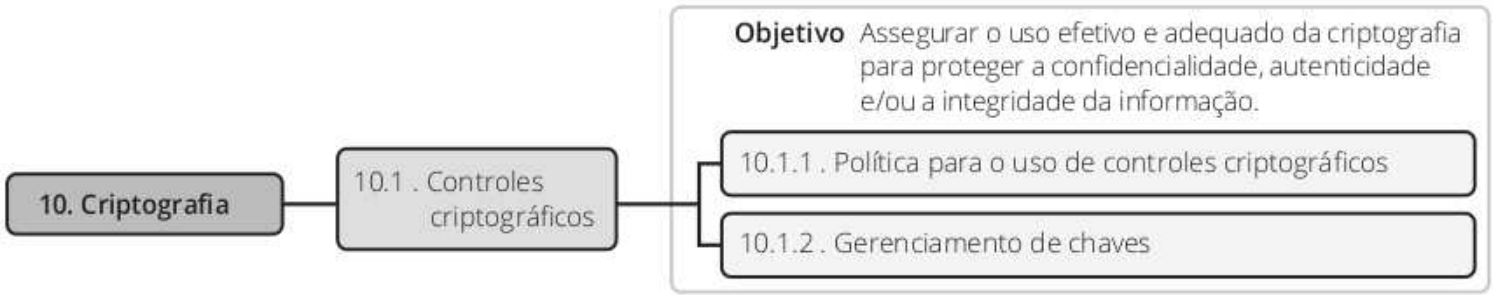
Controle de Acesso



INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Criptografia

Tem como objetivo assegurar o uso efetivo e adequado da criptografia. Além de apresentar o uso, proteção e tempo de vida das chaves criptográficas.



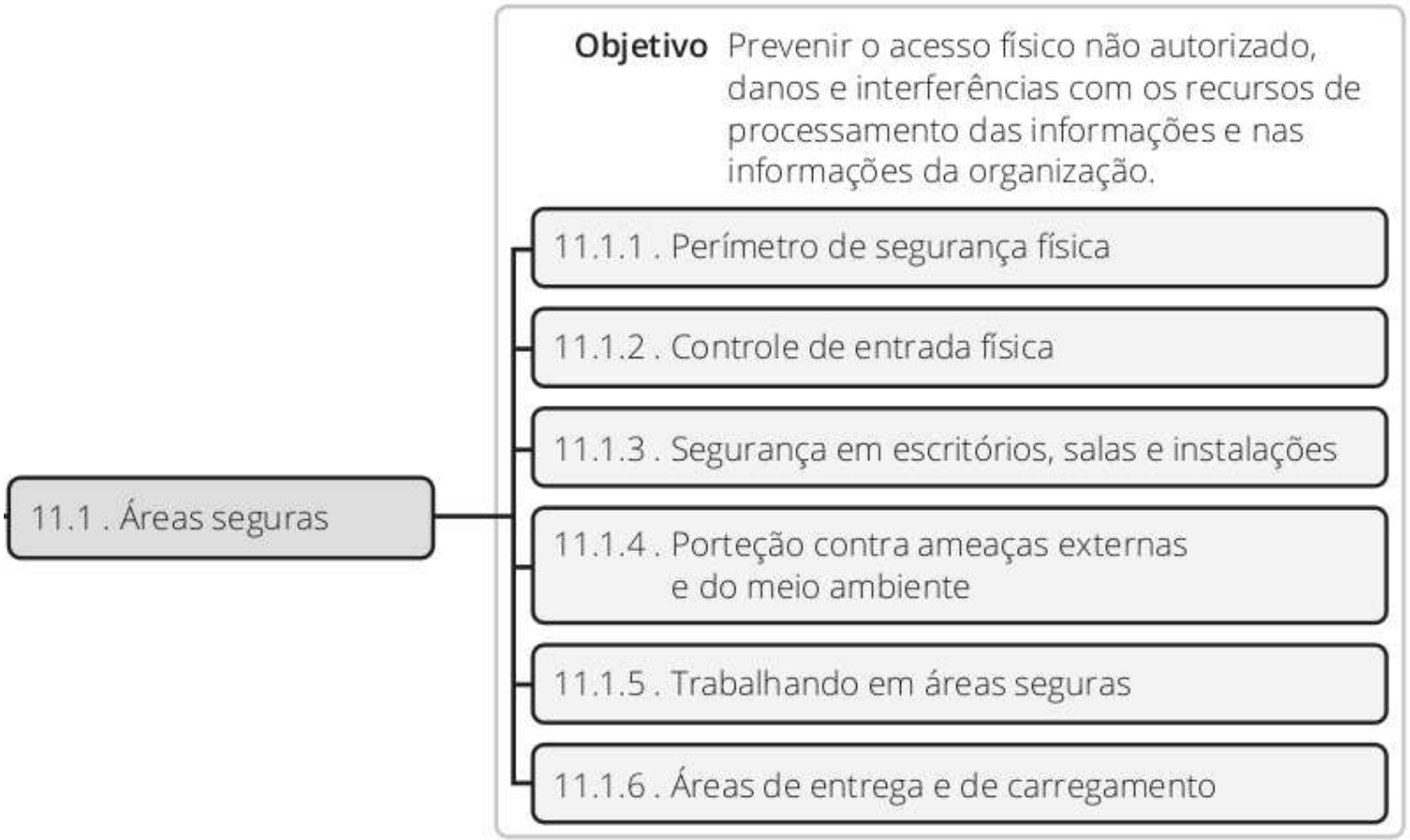
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Segurança Física e do Ambiente

- Previnir o acesso físico não autorizado;
- Impedir perdas, danos, furto, ou comprometimento de ativos e interrupção das operações da organização.

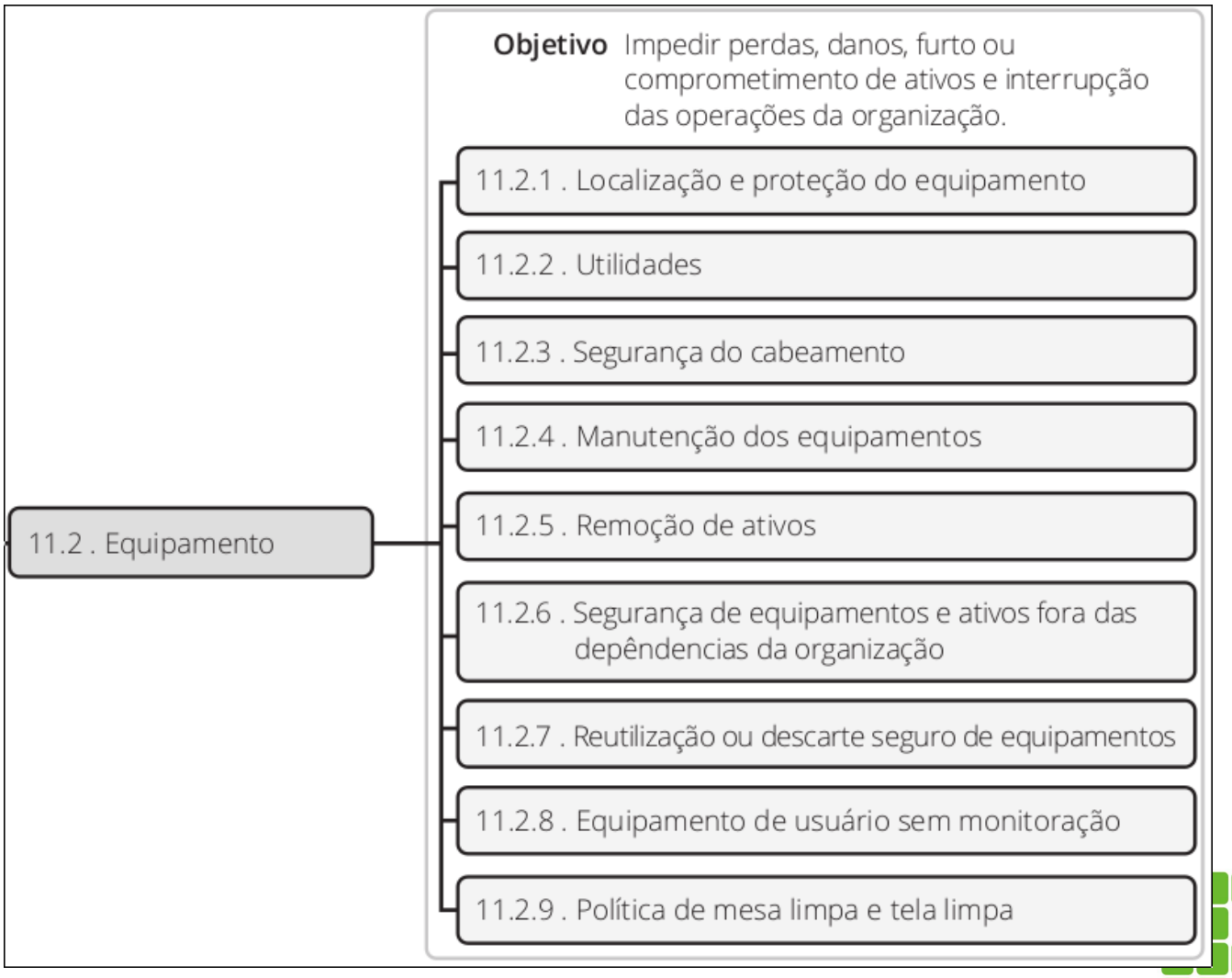
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Segurança Física e do Ambiente



INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Segurança Física e do Ambiente



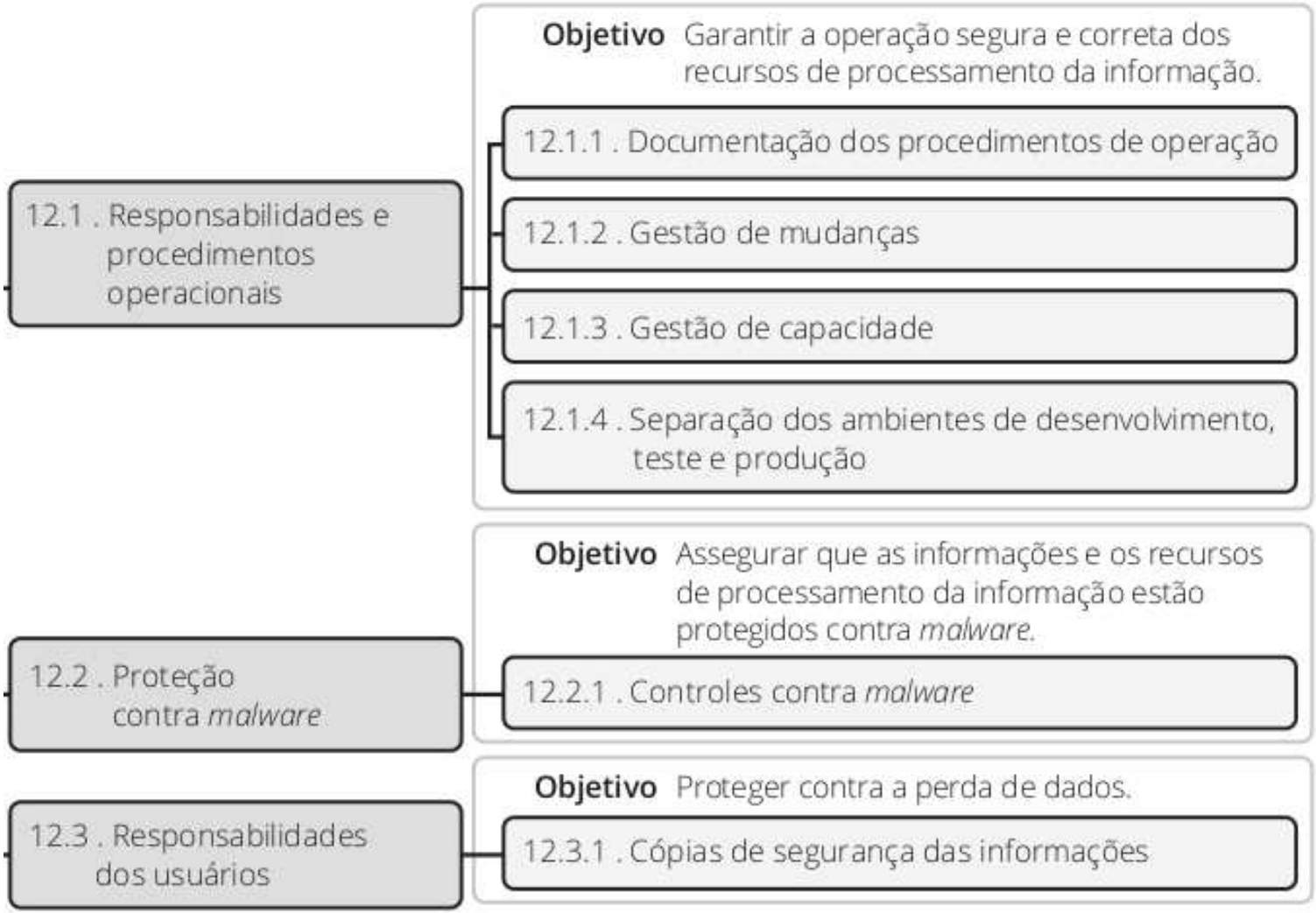
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Segurança nas Operações

- Garantir a operação segura e correta dos recursos de processamento da informação;
- Assegurar que as informações e os recursos de processamento da informação estão protegidos contra malware;
- Proteger contra a perda de dados;
- Registrar eventos e gerar evidências;
- Assegurar a integridade dos sistemas operacionais;
- Prevenir a exploração de vulnerabilidades técnicas;
- Minimizar o impacto das atividades de auditoria nos sistemas operacionais.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

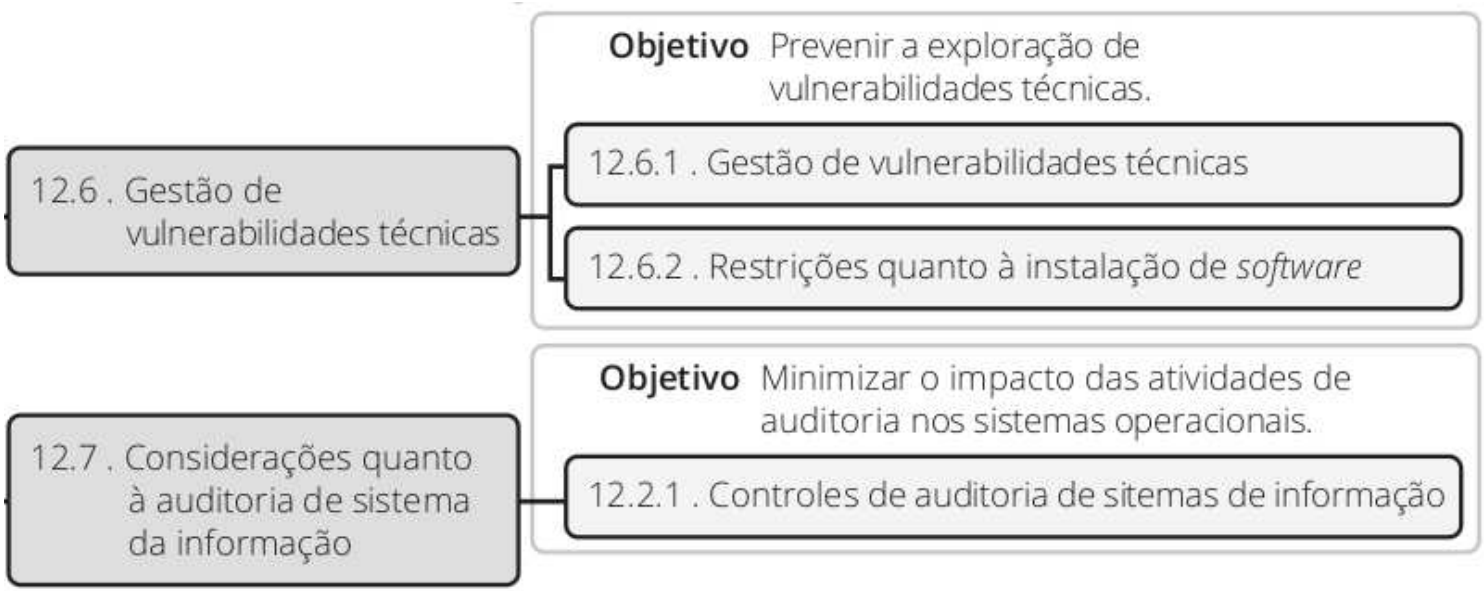
Segurança nas Operações



Segurança nas Operações

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Segurança nas Operações



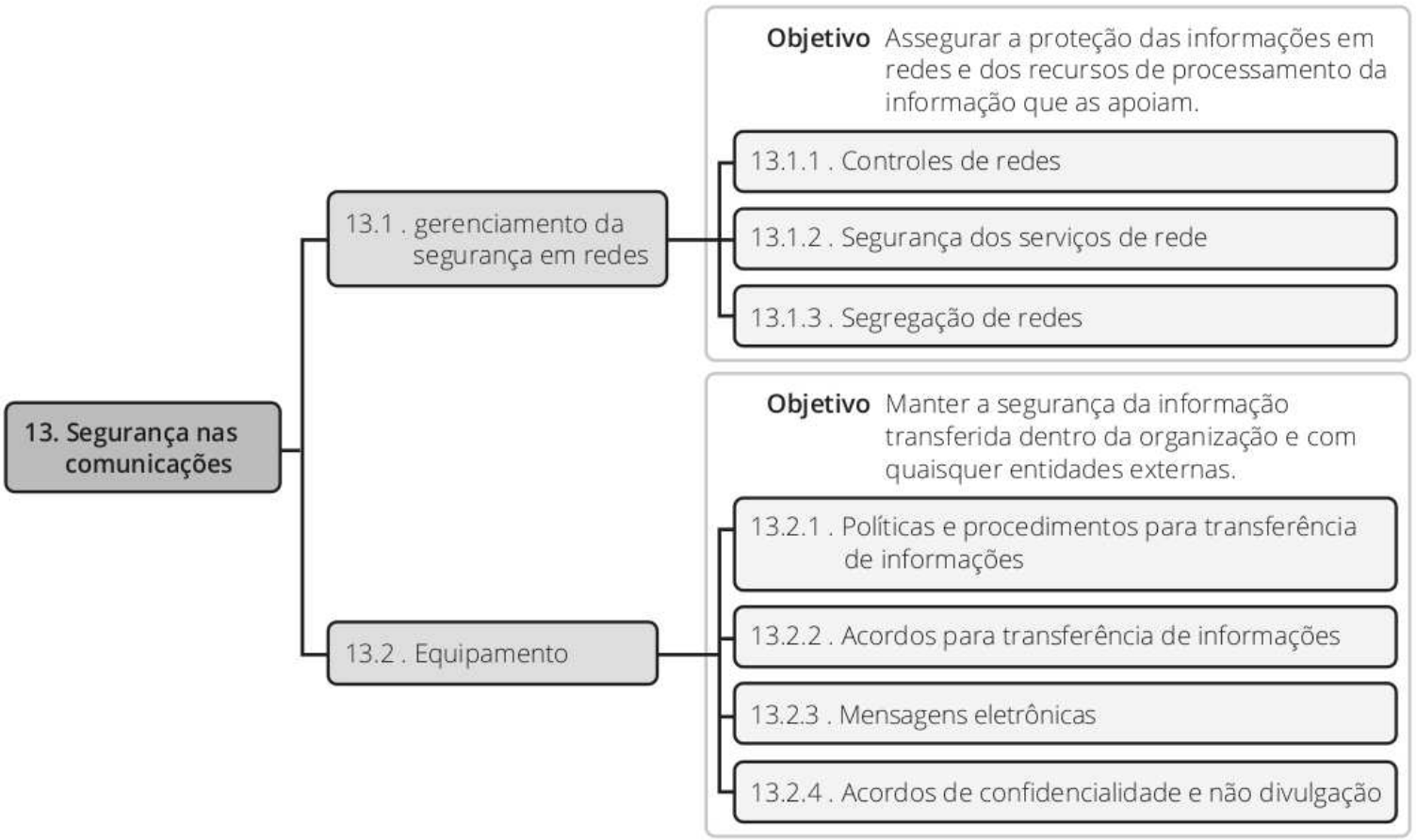
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Segurança nas Comunicações

- Objetiva garantir a proteção das informações em redes e a proteção da infraestrutura de suporte, incluindo segurança dos serviços e segregação de redes;
- Manter a segurança na troca de informações internamente e com entidades externas. Incluindo, requisitos para confidencialidade ou acordos de não divulgação sejam identificados e analisados.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Segurança nas Comunicações



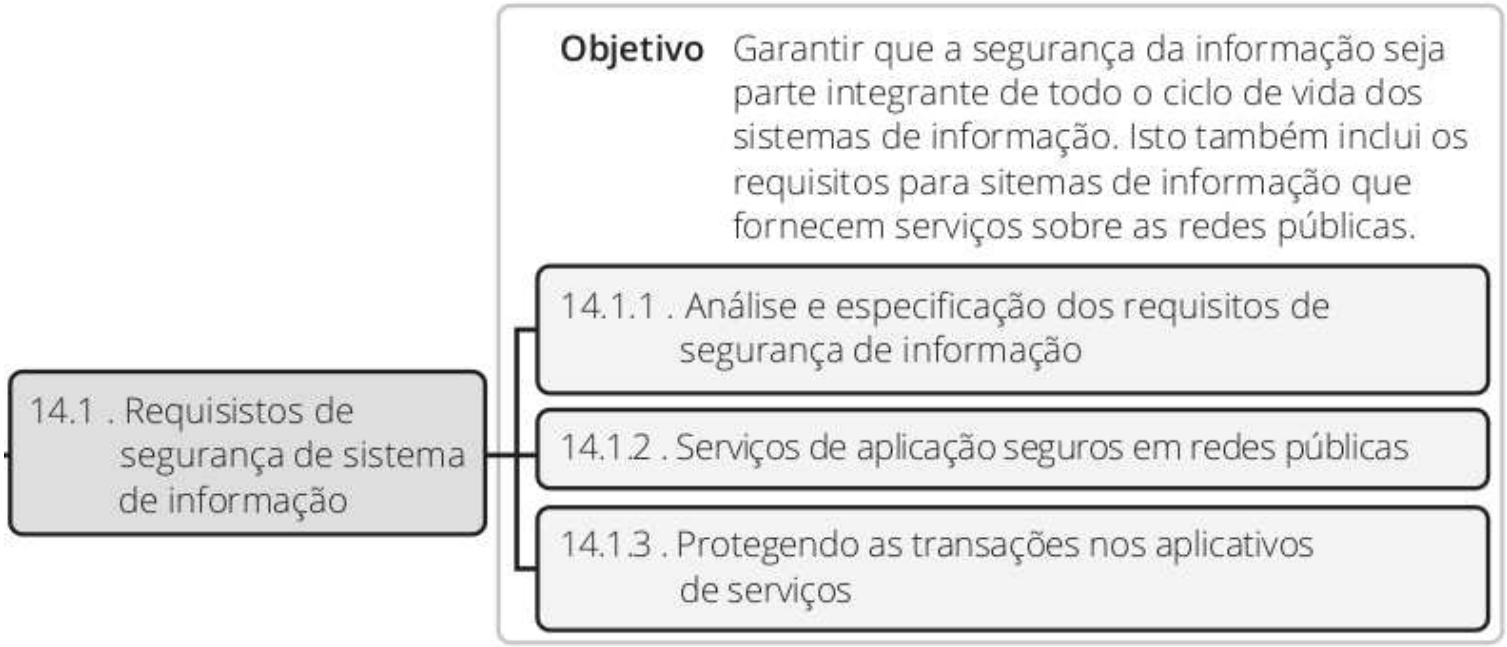
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Aquisição, Desenvolvimento e Manutenção de Sistemas

- Garantir que a segurança da informação esteja projetada e implementada no ciclo de vida de desenvolvimento dos sistemas de informação.
- Assegurar a proteção dos dados usados para testes.

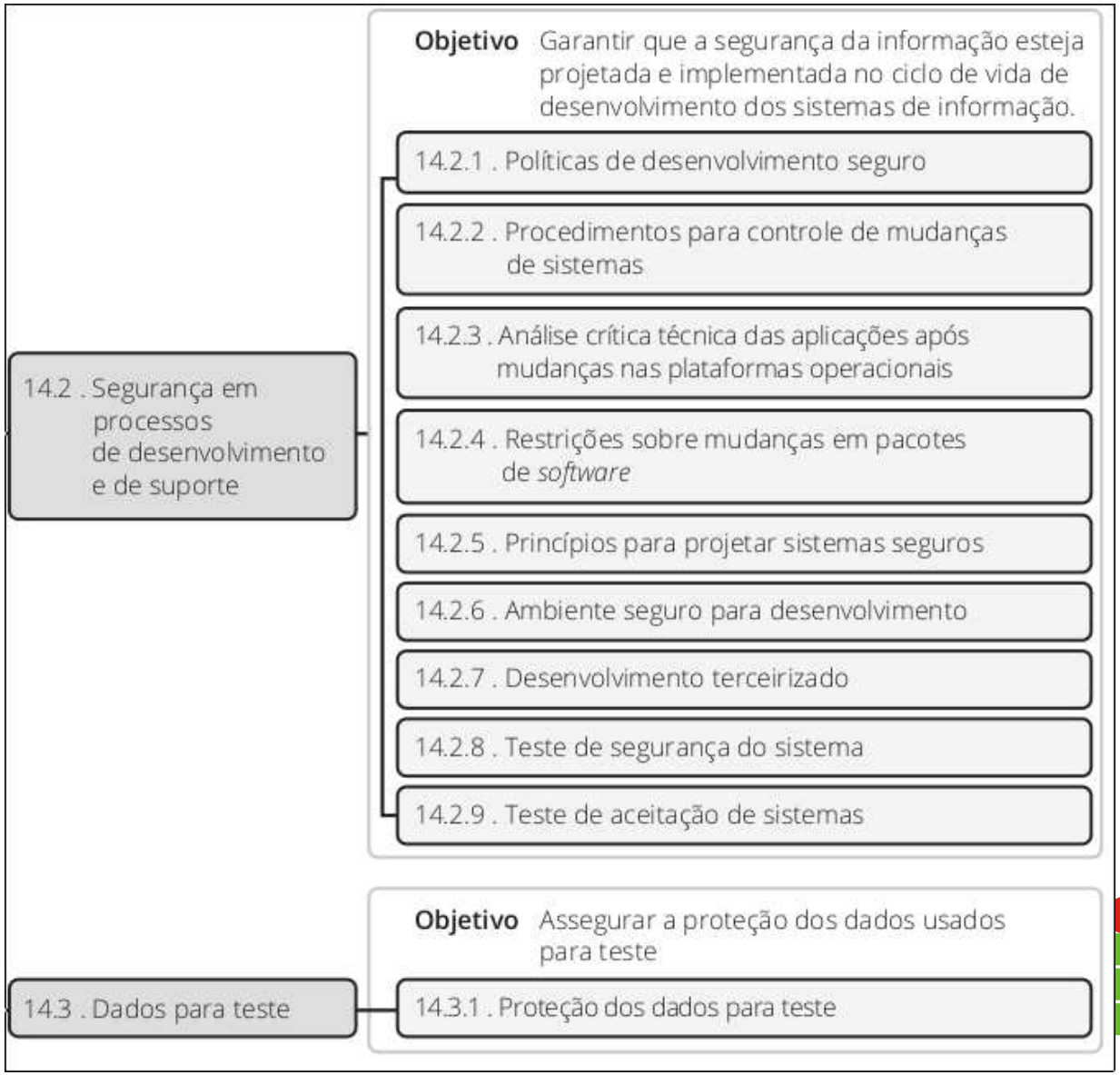
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Aquisição, Desenvolvimento e Manutenção de Sistemas



INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Aquisição, Desenvolvimento e Manutenção de Sistemas



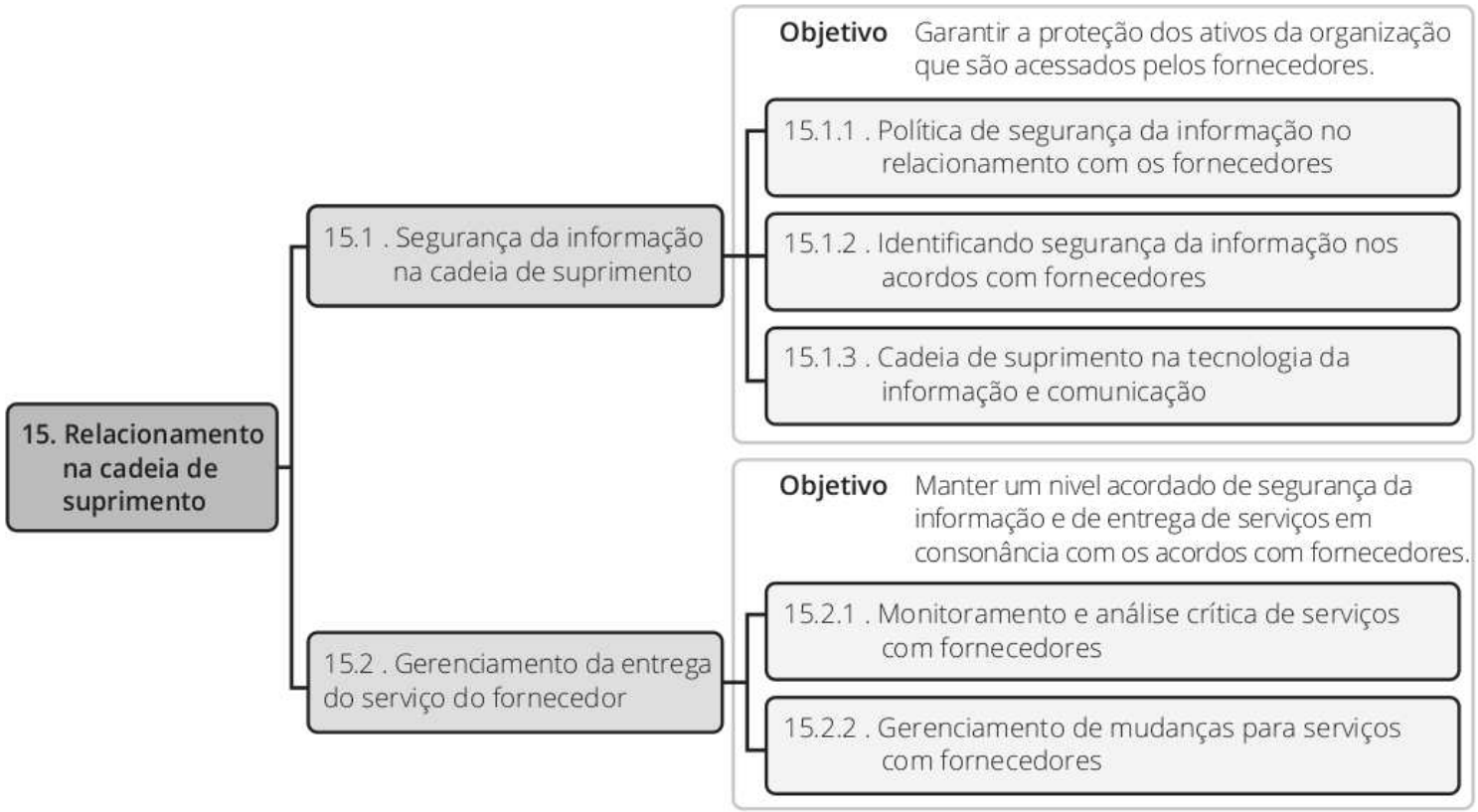
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Relacionamento na Cadeia de Suprimento

Trata do processo de segurança nos relacionamentos com os fornecedores. Definindo que sejam acordados e documentados os requisitos de segurança para mitigar os riscos.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Relacionamento na Cadeia de Suprimento



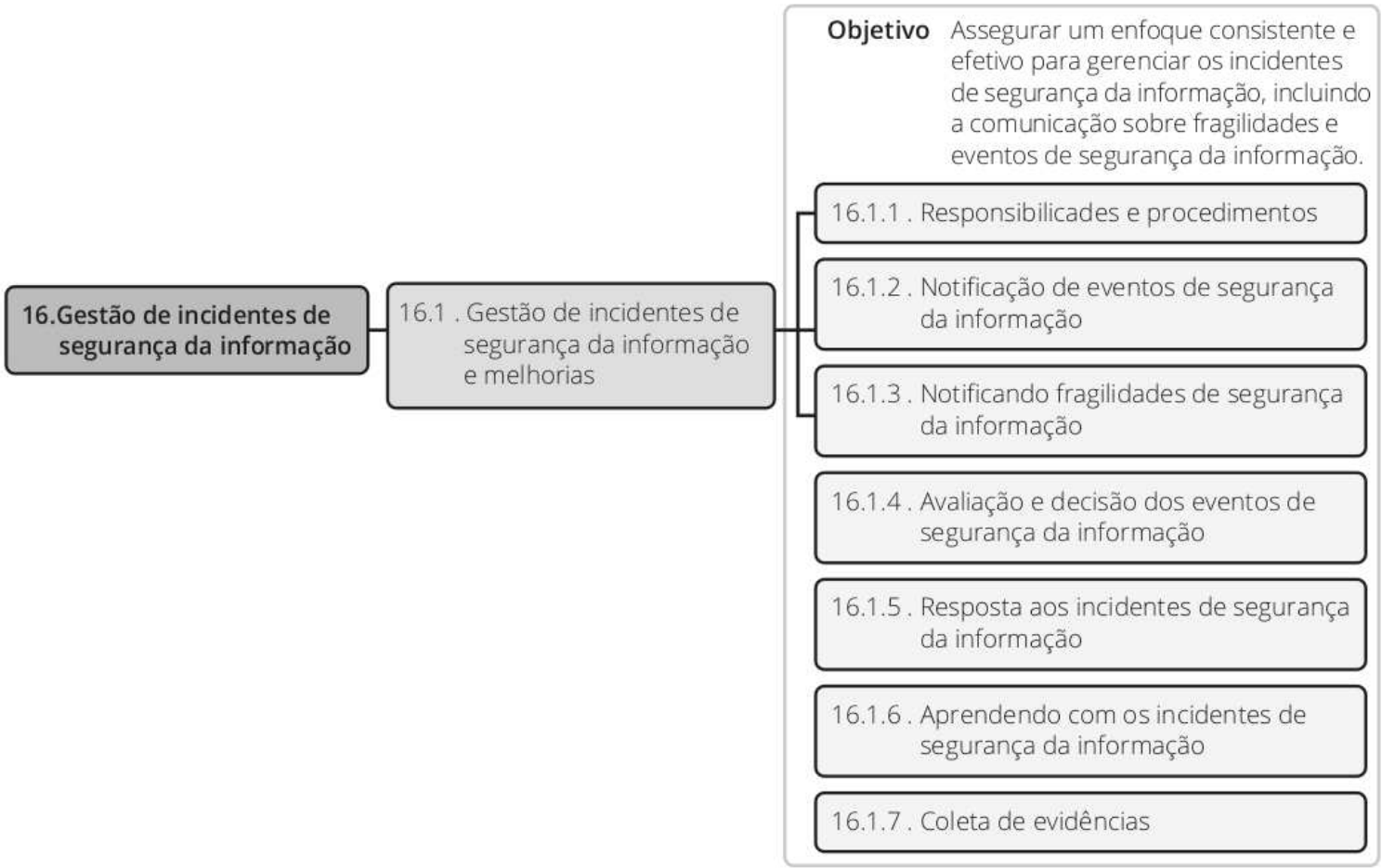
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Gestão de Incidentes

- Trata do processo de notificação de eventos de segurança, responsabilidades e coleta de evidências.
- Assegurar que fragilidades e eventos de segurança sejam comunicados, permitindo a tomada de ação corretiva em tempo real.
- Responsabilidades e procedimentos sejam estabelecidos para assegurar respostas rápidas;
- Monitorar os tipos e custos dos incidentes;
- Necessidade de que evidências sejam coletadas, armazenadas e apresentadas em conformidade com a legislação pertinente.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Gestão de Incidentes



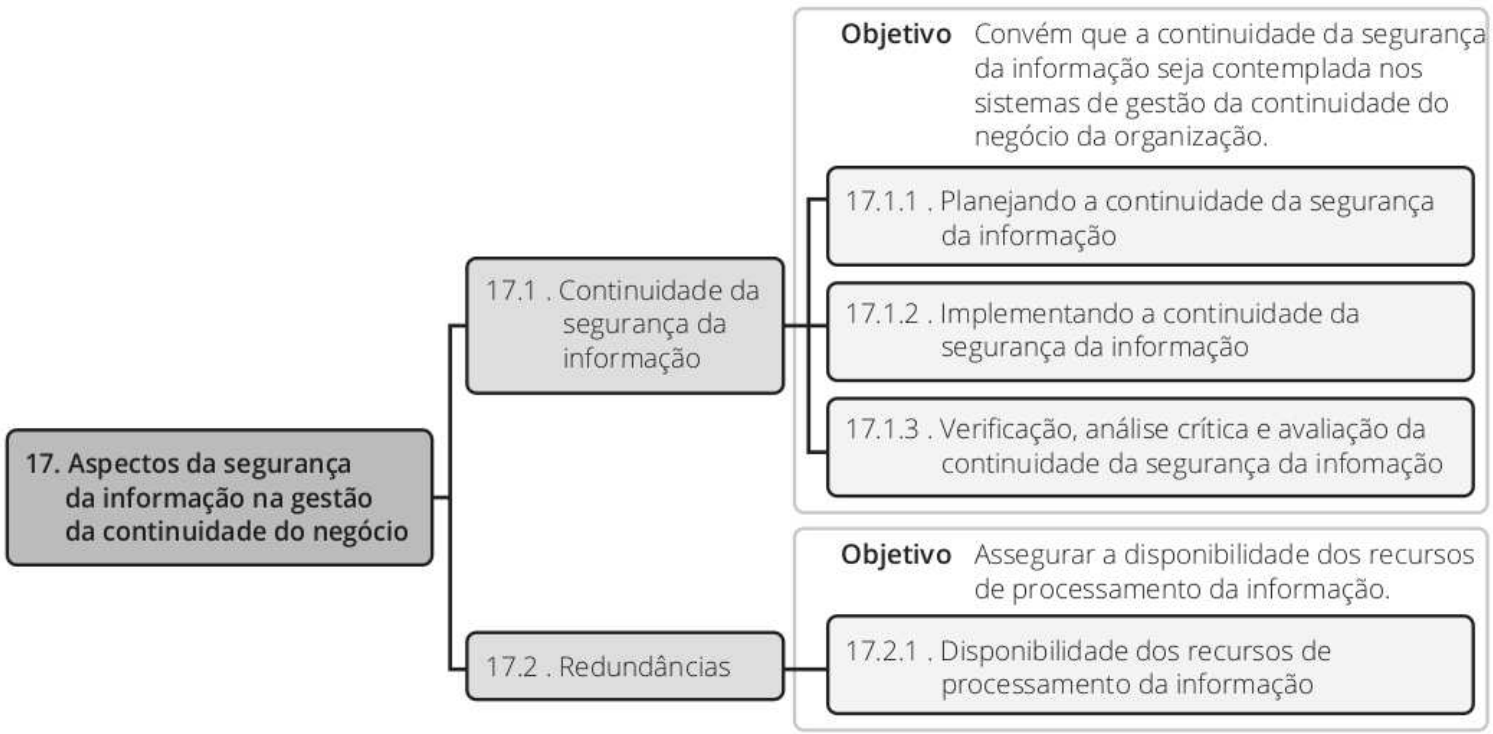
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Gestão da Continuidade do Negócio

- Trata dos aspectos de continuidade no caso de ocorrência de um desastre.
- Não permitir a interrupção das atividades do negócio e proteger os processos críticos contra efeitos de falhas ou desastres significativos, além de assegurar a sua retomada em tempo hábil, se for o caso.
- Questões relacionadas a backup e redundância.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Gestão da Continuidade do Negócio



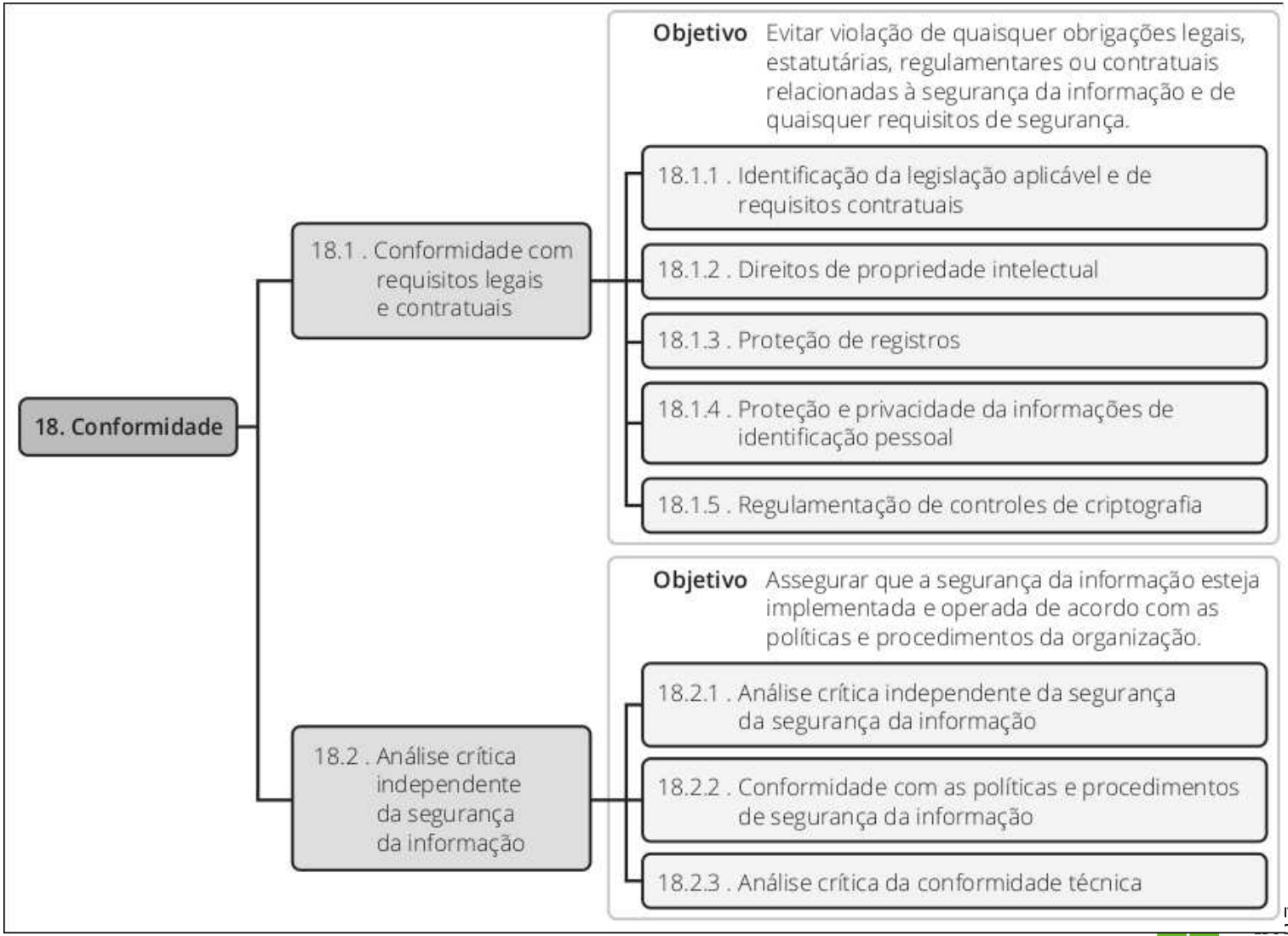
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Conformidade

Estabelece que os requisitos de segurança da informação estejam de acordo com qualquer legislação, como regulamentações, estatutos ou obrigações contratuais.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Conformidade



Pergunta???

A norma ABNT NBR ISO/IEC 27002:2013 mostra alguns procedimentos e controles. Mas existe alguma norma que nos auxilie a estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar um Sistema de Gestão de Segurança da Informação (SGSI)?

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

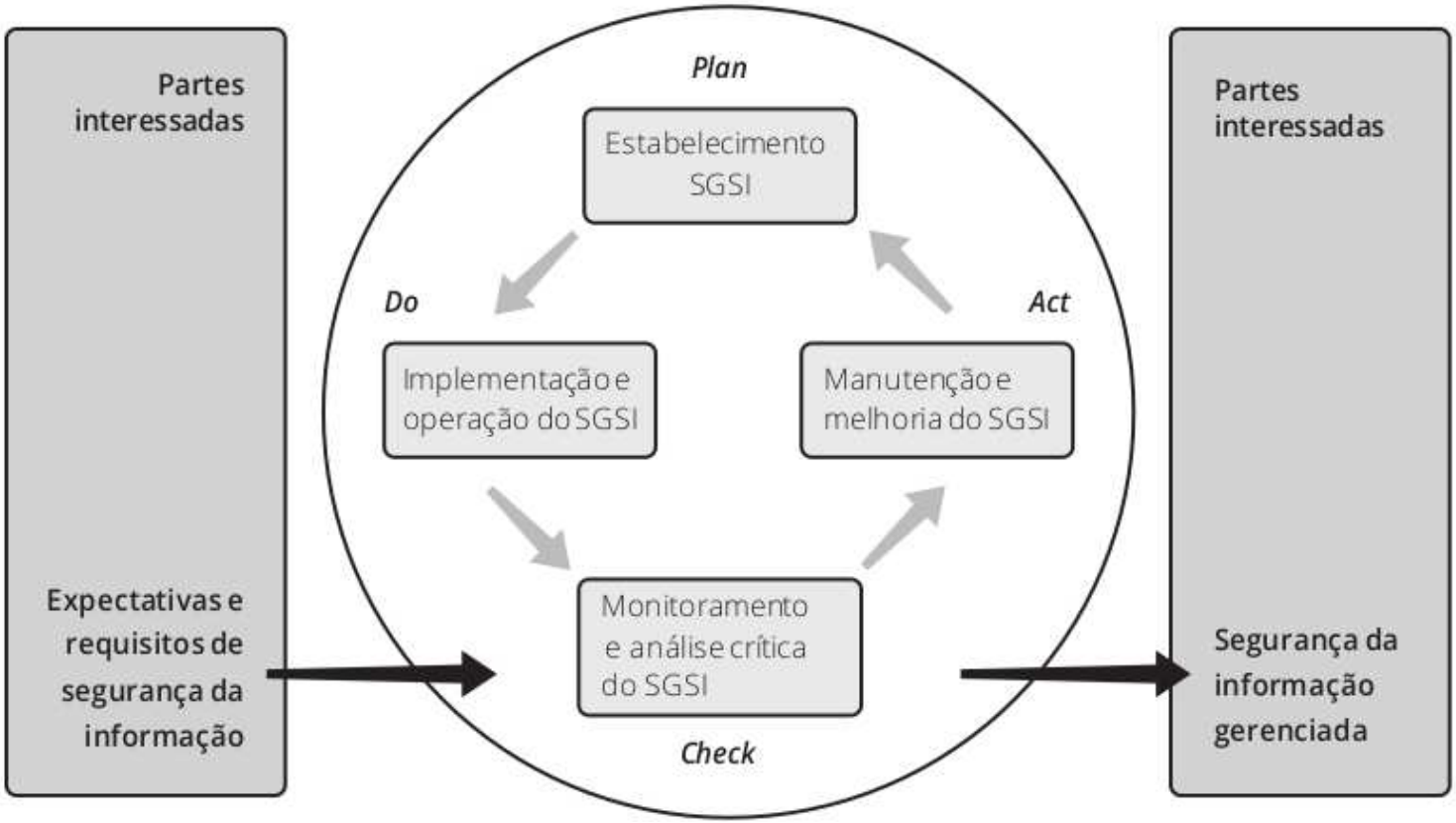
Norma ABNT NBR ISO/IEC 27001:2013

A norma ABNT NBR ISO/IEC 27001:2013 foi preparada para prover um modelo para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar um Sistema de Gestão de Segurança da Informação (SGSI).

Essa norma adota o modelo conhecido como "Plan-Do-Check-Act". P (plan: planejar), D (do: fazer, executar), C (check: verificar, controlar) e finalmente o A (act: agir, atuar corretivamente).

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Modelo PDA



INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

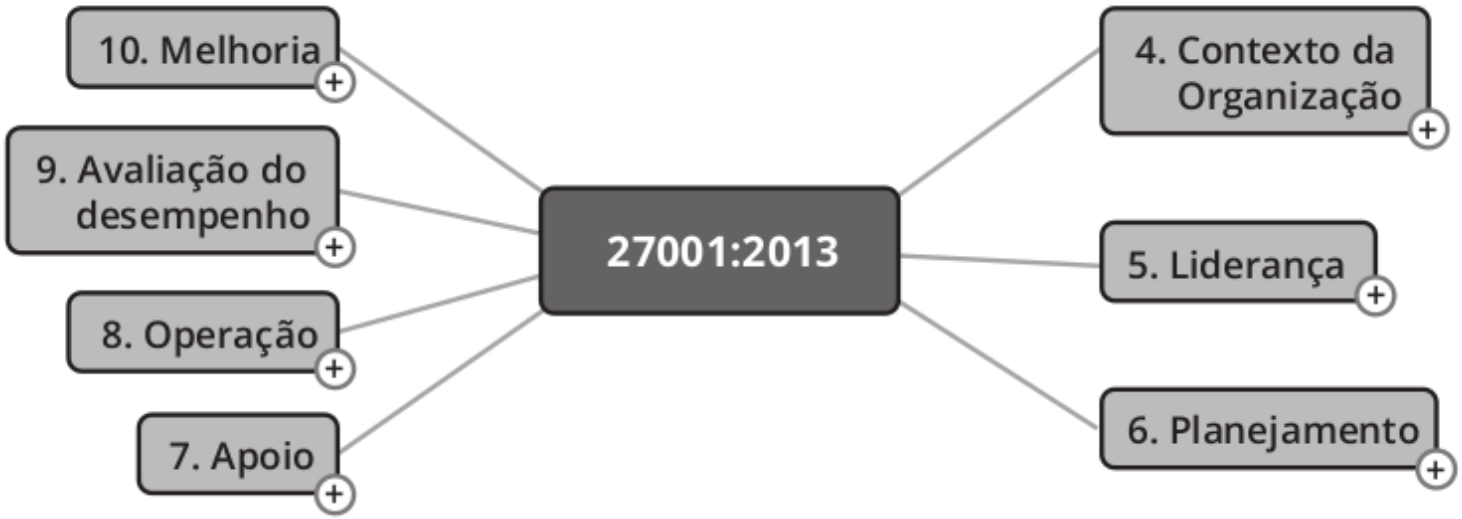
Modelo PDA

- Planejar: estabelecer a política, objetivos, processos e procedimentos do SGSI relevantes para a gestão de riscos e melhoria da segurança da informação;
- Fazer: implementar e operar a política, controles, processos e procedimentos do SGSI;
- Checar: avaliar e, quando aplicável, medir o desempenho do SGSI e apresentar os resultados para a análise da direção;
- Agir: executar as ações corretivas e preventivas, com base nos resultados da auditoria interna do SGSI e na análise crítica realizada pela direção ou para alcançar a melhoria contínua do SGSI.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Norma NBR ISO/IEC 27001:2013

A norma NBR ISO/IEC 27001:2013 busca de forma objetiva e genérica apresentar os requisitos aplicáveis a todas as organizações, independentemente do tipo, tamanho ou natureza. Esses requisitos são divididos em 7 categorias.



INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Norma NBR ISO/IEC 27001:2013

Contexto da Organização

Analisar toda a organização, entendendo as necessidades e as expectativas, para determinar as questões internas e externas que possam afetar a capacidade do sistema de gestão da segurança da informação.

Liderança

O envolvimento da Alta Direção, através da sua liderança e comprometimento, devem ser demonstrados durante todo o processo.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Norma NBR ISO/IEC 27001:2013

Planejamento

Definir e aplicar um processo de avaliação de riscos de segurança da informação.

Apoio

Trata dos recursos necessários para o estabelecimento, implementação, manutenção e melhoria contínua do SGSI. Trata ainda das competências necessária das pessoas.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Norma NBR ISO/IEC 27001:2013

Operação

Trata das atividades ligadas a operação do SGSI. A organização deve manter tudo documentado, processos e mudanças, para que possa gerar confiança de que tudo esta seguindo o planejado.

Avaliação do desempenho

Destaca a importância do monitoramento para verificar a eficácia do SGSI, através da determinação do que deve ser monitorado e medido.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Norma NBR ISO/IEC 27001:2013

Melhorias

Aborda os aspectos de melhoria e aperfeiçoamento do SGSI, quando uma não conformidade ocorre, a fim de que a organização possa tomar as ações necessárias para controlar e corrigir.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE