**ISO 27001 e ISO 27002**

Índice de Figuras

[Figura 1: Planificação para implementação da Norma ISO 27001 11](#_Toc150682140)

[Figura 2: Visualização geral dos requisitos genéricos da NP ISO/IEC 27001:2013 [Correia, 2016] 12](#_Toc150682141)

[Figura 3: Resumo da Norma ISO 27002 14](#_Toc150682142)

[Figura 6: Secção 5 – Políticas de segurança da informação 17](#_Toc150682143)

[Figura 7: Controlos da Secção 9 - Controlo de acesso 29](#_Toc150682144)

[Figura 8: Controlos da Secção 10 - Criptografia 31](#_Toc150682145)

[Figura 9: Controlos da 11 –segurança física e do ambiente 32](#_Toc150682146)

[Figura 10: Controlos da Secção 13 – Segurança nas operações 34](#_Toc150682147)

[Figura 11: Controlos da secção 13 – Segurança nas comunicações 37](#_Toc150682148)

[Figura 12: Controlos da secção 14 – Aquisição, desenvolvimento e manutenção de sistemas 39](#_Toc150682149)

[Figura 13: Controlos da secção 15 – Relacionamento com fornecedores 40](#_Toc150682150)

[Figura 14: Controlos da secção 16 – Gestão de incidentes de segurança da informação 41](#_Toc150682151)

[Figura 15: Controlos da secção 17 – Aspetos da segurança da informação na gestão da continuidade do negócio 42](#_Toc150682152)

[Figura 16: Controlos da secção 18 – Conformidade 43](#_Toc150682153)

[Figura 17: Exemplo da estrutura de uma Declaração de Aplicabilidade 45](#_Toc150682154)

Índice de Tabelas

[Tabela 1: Família de normas 27000 9](#_Toc150682155)

[Tabela 3: Critérios de avaliação dos ativos 27](#_Toc150682156)

*ta página foi intencionalmente deixada em branco*

Lista de Siglas

* ISO - International Organization for Standardization;
* UIMA – Unidade de Informática e Modernização Administrativa;
* IEC - International Electrotechnical Commission;
* SI - Sistema de Informação;
* RGPD - Regulamento Geral de Proteção de Dados;
* SGSI – Sistema de Gestão de Segurança de Informação;
* BYOD – Bring Your Own Device;

Índice

[Índice de Figuras 1](#_Toc150682180)

[Lista de Siglas 3](#_Toc150682181)

[As normas ISO/IEC 27001:2013 e ISO/IEC 27002:2013 6](#_Toc150682182)

[3.1. A norma ISO/IEC 27001:2013 6](#_Toc150682183)

[3.2 A norma ISO/IEC 27002:2013 9](#_Toc150682184)

[3.3. Diferenças entre as normas 27001 e 27002 11](#_Toc150682185)

[Controlos das normas ISO 27001 e ISO 27002 14](#_Toc150682186)

[4.2 Secção 5 – Políticas de segurança 14](#_Toc150682187)

[4.3 Secção 6 – Organização da segurança da informação 16](#_Toc150682188)

[4.4 Secção 7 – Organização da segurança da informação 20](#_Toc150682189)

[4.5 Secção 8 – Gestão de ativos 21](#_Toc150682190)

[4.6 Secção 9 – Controlo de Acesso 25](#_Toc150682191)

[4.7 Secção 10 – Criptografia 27](#_Toc150682192)

[4.8 Secção 11 – Segurança física e do ambiente 29](#_Toc150682193)

[4.9 Secção 12 – Segurança nas operações 30](#_Toc150682194)

[4.10 Secção 13 – Segurança nas comunicações 34](#_Toc150682195)

[4.11 Secção 14 – Aquisição, desenvolvimento e manutenção de sistemas 35](#_Toc150682196)

[4.12 Secção 15 – Relacionamento com fornecedores 37](#_Toc150682197)

[4.13 Secção 16 – Gestão de incidentes de segurança da informação 38](#_Toc150682198)

[4.14 Secção 17 – Aspetos da segurança da informação na gestão da continuidade do negócio 39](#_Toc150682199)

[4.15 Secção 18 – Conformidade 40](#_Toc150682200)

[Declaração de aplicabilidade 41](#_Toc150682201)

As normas ISO/IEC 27001:2013 e ISO/IEC 27002:2013

Este capítulo tem como objetivo explicar o em síntese as normas ISO 27001 e ISO 27002.

# 3.1. A norma ISO/IEC 27001:2013

A norma NP ISO/IEC 27001:20135 tem tradução na língua portuguesa, sendo a primeira norma portuguesa de segurança de informação, editada pelo IPQ em 2013-10-14. A motivação de editar esta norma como Norma Portuguesa foi “promover a implementação da ISO/IEC 27001 em Portugal, sabendo que alguns países com forte implementação desta norma e possuem traduções nacionais (por exemplo, Japão, Espanha, Brasil); disponibilizar uma norma portuguesa que possa ser referenciada em iniciativas de conformidade e padronizar a terminologia portuguesa de segurança de informação” [Coelho, 2013].

A norma ISO/IEC 27001 especifica os requisitos referentes a um Sistemas de Gestão de Segurança da Informação, permitindo que as organizações avaliem os seus riscos e implementem os procedimentos necessários para a preservação da confidencialidade, integridade e disponibilidade da informação. Tem como principal objetivo impedir que a informação seja utilizada por terceiros não desejados ou perdida de forma irremediável [Correia, 2016].

A série de normas ISO 27000, surge de um esforço conjunto da ISO (International Organization for standardization) e IEC (International Electrotechnical Commission) com o intuito de criar um sistema de gestão da segurança da informação semelhante em design ao sistema de gestão da qualidade já existente (a sério ISO 9000) [Simões, 2012]. O objetivo da criação destas normas foi ajudar as organizações a manter os seus ativos de informação de uma forma segura, de tal forma que definem diretrizes para a implementação de um SGSI.

A série ISO 27000 é então um conjunto de normas onde existem diretrizes e boas práticas de planeamento, implementação e gestão de segurança em segurança de informação. Esta série de normas é a evolução natural de normas anteriores. A norma ISO 27001 representa uma evolução da antiga BS 7799-2, a ISO 27002 a evolução da antiga ISO 17799 e a ISO 27005 a evolução da antiga BS 7799-3. As normas BS, de British Standards, têm origem nesta instituição Britânica com a função de criar normas e padrões a serem seguidos no Reino Unido, é um dos principais organismos colaboradores ISO, estando mesmo na origem de normas como a ISO 9001. Em Novembro de 2005 a ISO deu início à criação desta série com o objetivo de reorganizar um inúmero conjunto de normas de segurança da informação existentes na altura, sem ligação entre elas [Simões, 2012].

Desde já interessa salientar que deste conjunto/série de normas, a única passível a certificação é a norma 27001 (ISO/IEC 27001), sendo as outras complementos de auxílio à certificação em áreas específicas de atividade. Podendo afirmar que se o sistema de gestão de segurança da informação (SGSI) cumprir e implementar o especificado nas restantes normas, o processo de certificação da ISO 27001 será potencialmente melhor sucedido [Simões, 2012].

As normas 27000 e 27001 são introdutórias e referem-se a procedimentos de implementação, ao invés das restantes que são focadas em determinadas áreas específicas. A título de exemplo apresentam-se na Tabela 1 alguns dos domínios específicos entretanto cobertos:

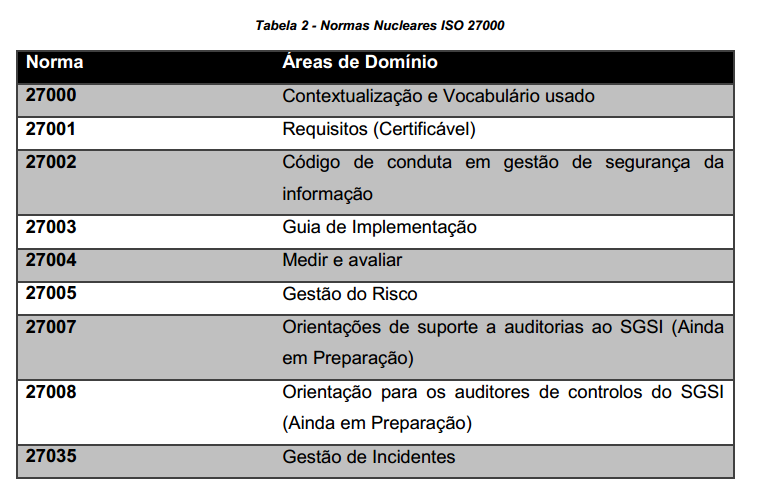


Tabela : Família de normas 27000

Na figura seguinte pode observa-se um plano de uma possível implementação da norma ISO 27001 (fonte: [Simões, 2016]):

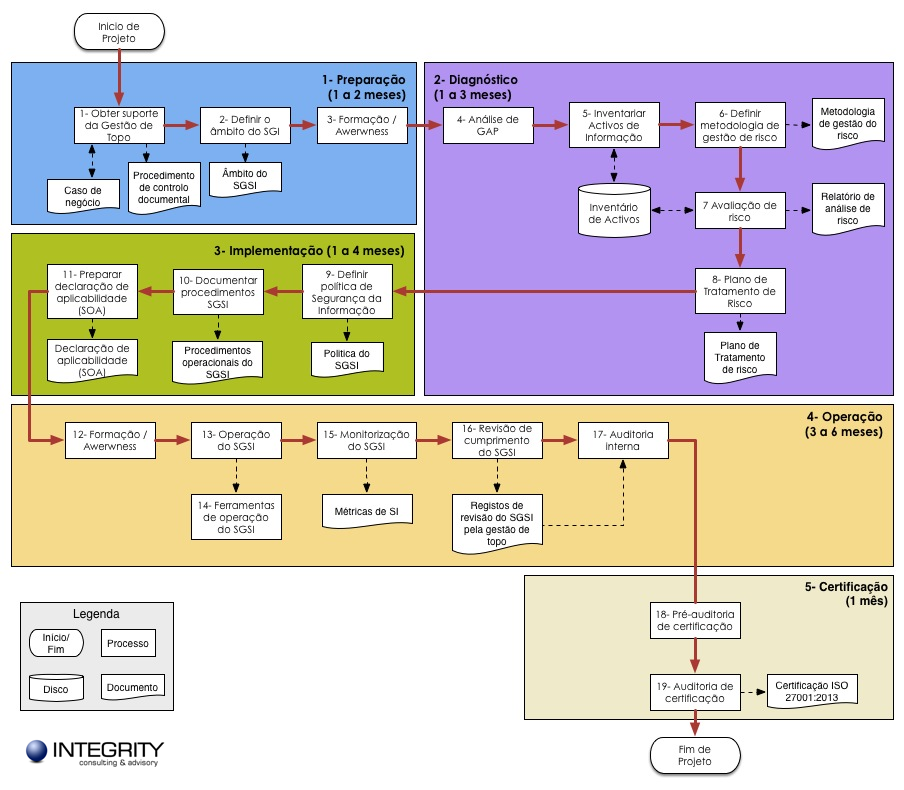


Figura : Planificação para implementação da Norma ISO 27001

Olhando para a imagem anterior, no âmbito deste trabalho, foi realizado algum trabalho do grupo de tarefas do 2 – Diagnóstico (nomeadamente com a identificação dos ativos) e do grupo 3 – Implementação, com a produção do documento de Declaração de Aplicabilidade.

A norma ISO/IEC 27001 é composta por duas componentes relativamente distintas:

1. Na primeira componente estão definidas as regras e os requisitos de cumprimento da norma, a que estes devem ser aplicáveis. “A exclusão de quaisquer dos requisitos especificados nas  
   secções 4 a 10 não é aceitável para uma organização que reivindica a sua conformidade face  
   a esta Norma.” (NP ISO/IEC 27001, p.6).

Esta componente abarca os seguintes elementos:

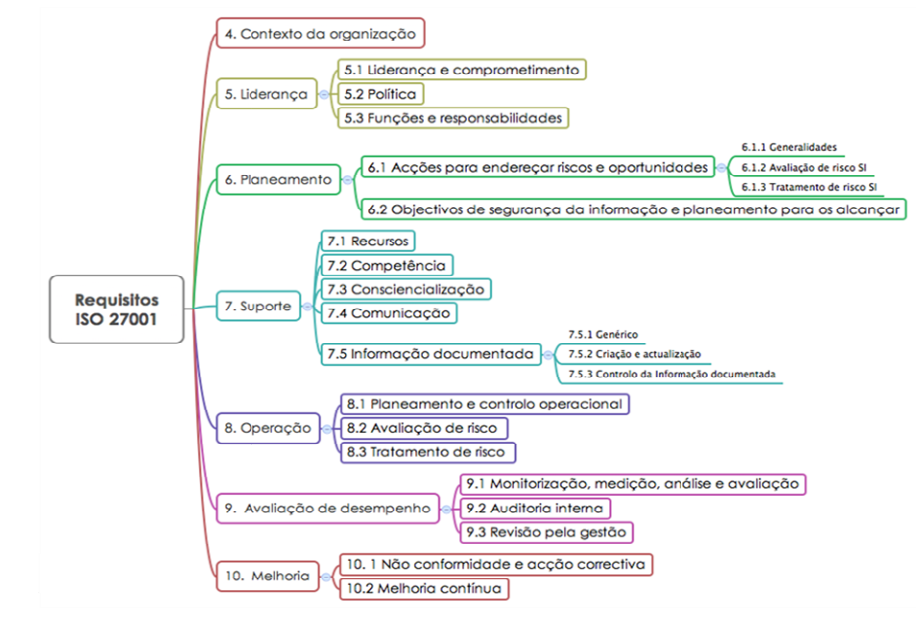


Figura : Visualização geral dos requisitos genéricos da NP ISO/IEC 27001:2013 [Correia, 2016]

1. A segunda componente da norma é denominada de Anexo A, especifica os objetivos de controlo e controlos de referência, denominados de A.5 a A.18 e “são derivados diretamente e são alinhados com os listados na ISO/IEC 27002:2013 nas secções 5 a 18” (NP ISO/IEC 27001) que a seguir se explica.

# 3.2 A norma ISO/IEC 27002:2013

A norma ISO 27001 representa o ponto de partida das restantes normas da série, pelo que considera-la de modo isolado não acrescente mais validas. A norma ISO 27001 especifica orientações e requisitos genéricos, necessários à implementação de um sistema de gestão de segurança de informação (SGSI).

A norma ISO 27002 surge como complemento à norma ISO 27001 dando suporte à implementação de um SGSI, fornecendo um conjunto de controlos mais específicos, pois conforme já descrito apesar do paralelo com o Anexo A da norma ISO 27001, na ISO 27002 os controlos são mais detalhados.

A norma ISO/27002:2013 (Tecnologia de Informação – Técnicas de segurança – Código de prática para controlos de segurança de informação), foi preparada para servir como um guia prático para o desenvolvimento e a implementação de procedimentos e controlos de segurança da informação numa organização.

Os controlos da norma são apresentados como boas práticas para que a organização adote uma postura preventiva e pró-ativa de acordo com as suas necessidades e requisitos de segurança de informação.

A norma possui 14 secções, 35 objetivos de controlo e 114 controlos. Está estruturada para fornecer um código de boas práticas para a gestão da segurança e é organizada em capítulos de 0 a 18. Os capítulos de 0 a 4 apresentam temas de Introdução (0), Âmbito (1), Referência normativa (2), Termos e definições (3) e Estrutura da norma (4).

A partir do capítulo 5, a norma passa a chamar cada capítulo de secção. Assim, existem catorze secções específicas apresentando os códigos de práticas da gestão da segurança.

Cada secção define um define um ou mais objetivos controlo. As catorze secções formam o total de 35 objetivos de controlo. A secção 4 da norma apresenta a sua estrutura.

Existem 114 controlos e eles são os elementos que definem o que a norma 27002 considera como importante para um processo de segurança de informação. Os controlos identificados por números (xx.xx.xx) são estruturados através de:

* **Controlo**: descrição e definição do controlo;
* **Diretrizes para a implementação**: informações auxiliares mais detalhadas na implementação do controlo;
* **Informações adicionais**: informações complementares;

Na figura seguinte, pode observar-se a sequência estrutural da norma:



Figura : Resumo da Norma ISO 27002

# Diferenças entre as normas 27001 e 27002

Conforme já foi referido, a norma ISO 27002 é muito mais detalhada, muito mais precisa que a norma ISO 27001. Então, mas sendo assim qual é o propósito da norma ISO 27001?

A primeira diferença, não é possível obter uma certificação ISO 27002 porque não é uma norma de gestão. O que significa ser uma norma de gestão? Significa que essa norma define como administrar um sistema. No caso da ISO 27001, ela define o SGSI, portanto, a [certificação](https://advisera.com/27001academy/pt-br/blog/2010/12/15/como-obter-a-certificacao-iso-27001/?icn=free-knowledgebase-27001&ici=top-certificacao-txt) para a ISO 27001 é possível.

Esse sistema de gestão significa que a segurança da informação deve ser planeada, implementada, monitorizada, analisada e melhorada. Significa que a gestão tem as responsabilidades definidas, que os objetivos devem ser estabelecidos, medidos e analisados, que deve haver auditorias internas. Todos esses elementos são definidos na norma ISO 27001, mas não na ISO 27002.

Os controlos da norma ISO 27002 têm os mesmos nomes do Anexo A da ISO 27001. Por exemplo, na norma ISO 27002 6.1.6, o controle tem a designação de Contato com Autoridades, enquanto na norma ISO 27001 é A.6.1.6 Contato com Autoridades. Porém, a diferença está no nível de detalhe – em média, a ISO 27002 explica um controlo numa página inteira, enquanto a ISO 27001 dedica apenas uma frase para cada controle.

Por fim, a diferença é que a ISO 27002 não faz distinção entre os controlos aplicáveis a uma determinada organização, e aqueles que não são. Por outro lado, a ISO 27001 determina uma avaliação de riscos a ser executada a fim de identificar, para cada controle, se ela é necessária para diminuir os riscos, e se for, em que medida deve ser aplicada.

A pergunta é: por que essas duas normas existem separadamente, porque não foram fundidas, reunindo os lados positivos de ambas? A resposta é a usabilidade: se fosse uma única norma, ela seria muito complexa e muito grande para uma utilização prática.

Para concluir, poderíamos dizer que, sem os detalhes fornecidos na norma ISO 27002, os controlos definidos no Anexo A da ISO 27001 não poderiam ser implementados. Porém, sem estrutura de gestão da ISO 27001, a ISO 27002 permaneceria apenas como um esforço isolado de alguns entusiastas da segurança da informação, sem aceitação da gestão de todo e, portanto, sem impacto real sobre a organização.

*(Inicia em página impar)*

Controlos das normas ISO 27001 e ISO 27002

*(Inicia em página impar)*

# 4.2 Secção 5 – Políticas de segurança

O objetivo desta secção é criar uma política de segurança de informação, é fornecer a orientação da direção e apoio para a segurança da informação de acordo com os requisitos do negócio e com as leis regulamentares relevantes.

Esta secção tem 2 controlos distribuídos da seguinte forma:

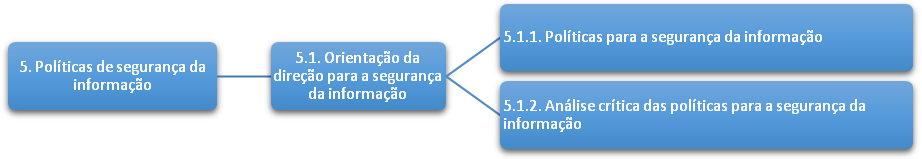


Figura : Secção 5 – Políticas de segurança da informação

A secção 5 da norma trata da política de segurança da informação e dos seus requisitos. O objetivo desta secção é apresentar como deve ser mantido e atualizado o documento da política.

O controlo **5.1.1 – Políticas para a segurança da informação**, define as diretrizes para a definição de uma política de segurança de informação na organização.

É fundamental definir um conjunto de políticas de segurança para a organização, garantir o apoio da gestão de topo e divulgar muito bem esse documento e essas políticas na organização por todos os trabalhadores.

Uma boa política de segurança deve cumprir os requisitos de fontes oriundas de:

1. da estratégia de negócio;
2. de Regulamentos, legislação e contratos;
3. do ambiente de ameaça da segurança da informação, atual e futuro;

Convém que a política da segurança da informação contenha declarações relativas a:

1. definição da segurança da informação, objetivos e princípios para orientar todas as atividades relativas à segurança da informação;
2. atribuição de responsabilidades, gerais e específicas, para a gestão da segurança da informação para os papéis definidos;
3. processos para o tratamento de desvios e exceções;

São exemplos de políticas com tópicos específicos:

1. controlo de acessos;
2. classificação e tratamento da informação;
3. tópicos orientados aos utilizadores finais;
4. uso aceitável dos ativos;
5. mesa limpa e monitor limpo;
6. transferência de informações;
7. dispositivos móveis e trabalho remoto;
8. restrições sobre a utilização e instalação de software;
9. cópias de segurança;
10. transferência da informação;
11. proteção contra códigos maliciosos;
12. gestão de vulnerabilidades técnicas;
13. controlos criptográficos;
14. segurança nas comunicações;
15. proteção e privacidade da informação de identificação pessoal;

Nesta seção existe ainda o controlo **5.1.2 – Análise crítica das políticas para a segurança da informação**, que consiste na definição de como fazer uma análise crítica com períodos bem definidos ou quando existam mudanças significativas, para assegurar a sua eficácia contínua.

Convém que cada política de segurança de informação tenha um gestor que tenha aprovado a responsabilidade pelo desenvolvimento, análise crítica e avaliações de políticas de segurança da informação. Convém que esta análise crítica inclua a avaliação de oportunidades de melhoria da política da segurança da informação.

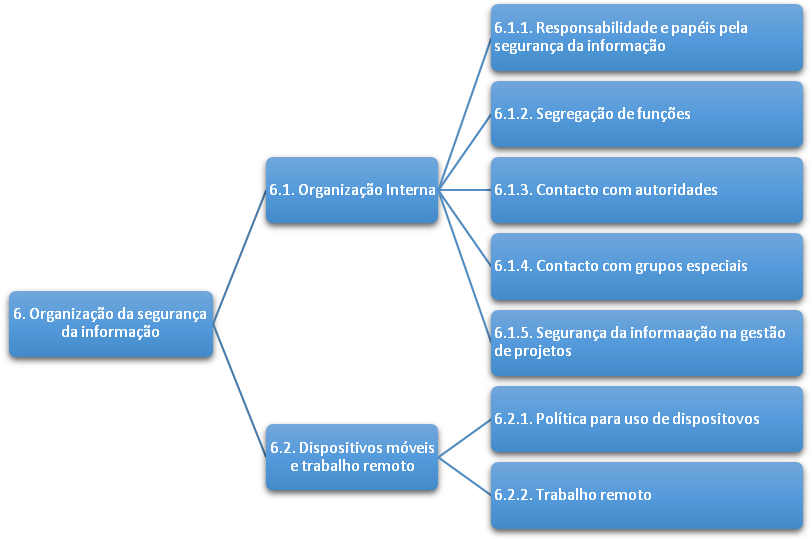
Algumas regras que podem ser seguidas na elaboração do documento da política de segurança são portanto:

* Definir o objetivo do documento;
* Usar textos curtos e objetivos, escritos na linguagem do público da organização;
* Definir papéis e responsabilidades;
* Evitar o uso de termos técnicos ou em língua estrangeira;
* Evitar o uso de “não”;
* Evitar o uso de “exceto” ou “em princípio”;
* Criar na política um item para as definições e conceitos;
* Penalização. Utilizar a colaboração do jurídico e dos RH;
* Criar regras e recomendações factíveis de serem aplicadas e cumpridas;
* Atentar para a correção gramatical Evitar gírias e termos de duplo sentido;
* Solicitar que o jurídico da organização avalie;
* Definir o objetivo do documento: descrever qual o objetivo do documento e o que a organização deseja comunicar com o documento da política;
* Usar textos curtos e objetivos, escritos na linguagem do público da organização;

# 4.3 Secção 6 – Organização da segurança da informação

A secção 6 tem como objetivo apresentar os controlos para que uma estrutura possa gerir a segurança da informação dentro da organização e os controlos para possa ser mantida a segurança dos recursos de processamento da informação, quando disponibilizados através de dispositivos móveis ou trabalho remoto.

Esta secção tem 7 controlos distribuídos da seguinte forma:



Enquanto que os controlos da categoria “6.1. Organização Interna” tem como objetivo estabelecer uma estrutura de gestão para iniciar e controlar a implementação e operação da segurança da informação dentro da organização, os da categoria “6.2. Dispositivos móveis e trabalho remoto” tem como objetivo garantir a segurança das informações no trabalho remoto e no uso de dispositivos móveis.

Resume-se a seguir uma descrição de cada controlo.

**6.1.1. Responsabilidade e papéis pela segurança da informação** – convém que cada área pelas quais as pessoas sejam responsáveis, estejam claramente definidas, em particular recomenda-se que os seguintes itens sejam cumpridos:

1. Cada ativo e processo de segurança da informação devem ser identificados e claramente definidos;
2. O gestor responsável por cada ativo ou processo de segurança de informação tenha atribuições definidas e os detalhes dessa responsabilidade sejam documentadas;
3. Os níveis de autorização sejam claramente definidos e documentados;
4. As pessoas indicadas sejam competentes e capazes de cumprir com as responsabilidades pela segurança da informação e a elas seja dada a oportunidade de manter-se atualizada com os desenvolvimentos;

**6.1.2. Segregação de funções** –as funções conflituantes de responsabilidade devem ser segregadas para reduzir as oportunidades de modificação não autorizada ou não intencional, ou uso indevido dos ativos da organização.

**6.1.3. Contacto com as autoridades** –é importante que organização tenha procedimentos implementados que especifiquem quando e quais autoridades a ser contactadas em casos de incidentes de segurança da informação. Exemplo: suspeita no caso de violação de uma lei.

**6.1.4. Contacto com grupos especiais** – convém que contactos com grupos profissionais, ou outros fóruns especializados em segurança da informação sejam mantidos.

**6.1.5. Segurança da informação em gestão de projetos** – é fundamental que a segurança de informação seja tida em conta na gestão de projetos.

**6.2.1. Política para uso de dispositivo móvel** – Convém que a segurança da informação seja adotada para os riscos decorrentes do uso de dispositivos móveis. A política de utilização de dispositivos móveis deverá considerar o seguinte:

1. Registo dos dispositivos móveis;
2. Requisitos para a proteção física;
3. Restrições quanto à instalação de softwares;
4. Requisitos para as versões dos softwares e aplicações de *patches*;
5. Restrições para a ligação aos serviços de informação;
6. Controlo de acesso;
7. Técnicas criptográficas;
8. Proteção contra códigos maliciosos;
9. Desativação, bloqueio e exclusão de forma remota;
10. Backups;
11. Uso dos serviços web e aplicações web;

É muito importante informar os utilizadores dos cuidados a ter com a utilização dos dispositivos móveis em locais públicos, salas de reuniões e outras áreas protegidas. Convém que sejam estabelecidas proteções para evitar o acesso não autorizado ou a divulgação de informações armazenadas e processadas nesses dispositivos, por exemplo, através da utilização de técnicas de criptografia e do uso de informação de autenticação secreta.

Também é importante que os dispositivos móveis possam ser protegidos fisicamente contra roubo, especialmente quando, deixados por exemplo, em carros ou em outros meios de transporte, quartos de hotéis, centros de conferências e locais de reuniões. Convém que seja estabelecido um procedimento específico que leve em consideração requisitos legais, e outros requisitos de segurança da organização para casos de roubo ou perda de dispositivos móveis.

Convém que os dispositivos móveis que contêm informações importantes, sensíveis e/ou críticas para o negócio, não sejam deixados sem observação e, quando possível, estejam fisicamente trancados com o uso de medidas especiais, para proteger esses dispositivos móveis.

Convém que seja definido um planto de formação para os colaboradores que usam dispositivos móveis, como forma de aumentar a conscientização quanto aos riscos adicionais decorrentes desta forma de trabalho, e os controlos que se recomendam implementar.

Onde a política de dispositivos móveis permita o uso de dispositivos pessoais (BYOD), convém que esta política e os controlos de segurança relacionados, também considerem:

* 1. a separação do uso do dispositivo para trabalho e para fins pessoais, incluindo os softwares para suportar esta separação e proteger os dados do negócio num dispositivo privado;
  2. prover acesso às informações do negócio somente após os utilizadores assinarem um termo de responsabilidades (quanto à proteção física, atualização do software, entre outros), renunciando direitos de autoria dos dados da organização, que permita a exclusão remota dos mesmos no caso de furto, roubo ou perda do dispositivo móvel ou ainda, quando deixar de haver autorização para o uso dos serviços. Esta política deve ter em consideração a legislação sobre privacidade.

**6.2.2. – Trabalho remoto** – Convém que uma política e medidas que apoiam a segurança da informação sejam implementadas para proteger as informações acedidas, processadas ou armazenadas em locais de trabalho remoto.

É fundamental que a organização permita atividade de trabalho remoto e que publique uma política que defina as condições e restrições para poder realizar trabalho remoto. Quando considerados aplicáveis e permitidos por lei, convém que os seguintes pontos sejam considerados:

1. a segurança física existente no local de trabalho remoto;
2. o ambiente físico proposto para o trabalho remoto;
3. os requisitos de segurança nas comunicações, levando em consideração a necessidade do acesso remoto aos sistemas internos da organização, a sensibilidade da informação que será acedida;
4. a provisão de acesso virtual às estações de trabalho dos utilizadores, para prevenir o processamento e o armazenamento da informação num equipamento particular;
5. a ameaça de acesso não autorizado por parte de familiares e amigos;
6. a utilização de redes domésticas e requisitos ou restrições na configuração de redes sem fio;
7. políticas e procedimentos para evitar disputas relativas a direitos de propriedade intelectual desenvolvidas em equipamentos de propriedade particular;
8. acesso a equipamentos de propriedade particular (para verificar a segurança da máquina ou

durante uma investigação), que pode ser proibido legalmente;

1. acordos de licenciamento de software que podem tornar as organizações responsáveis pelo

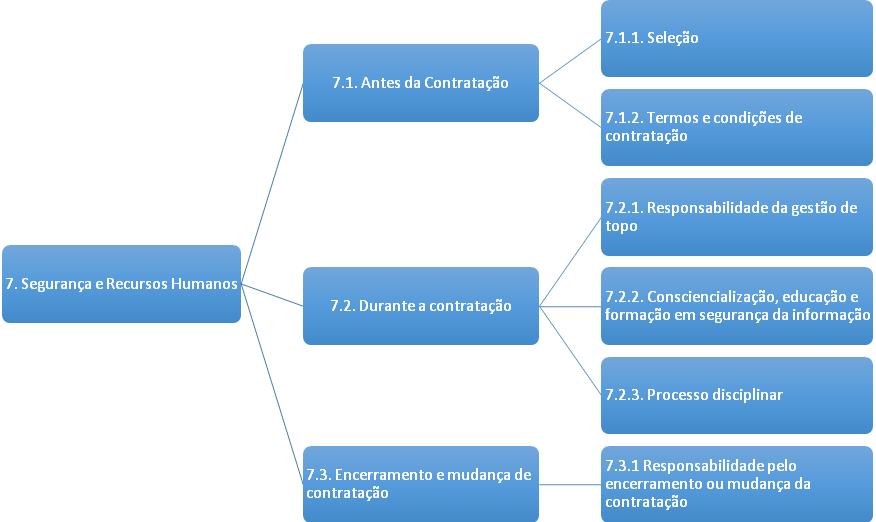
licenciamento do software cliente em estações de trabalho particulares de propriedade de funcionários, fornecedores ou terceiros;

1. requisitos de proteção contra vírus e requisitos de firewall.

# 4.4 Secção 7 – Organização da segurança da informação

O objetivo deste controlo é assegurar que os funcionários da organização e partes externas tenham a perceção exata das suas responsabilidades e estejam em conformidade com os papéis para os quais foram selecionados.

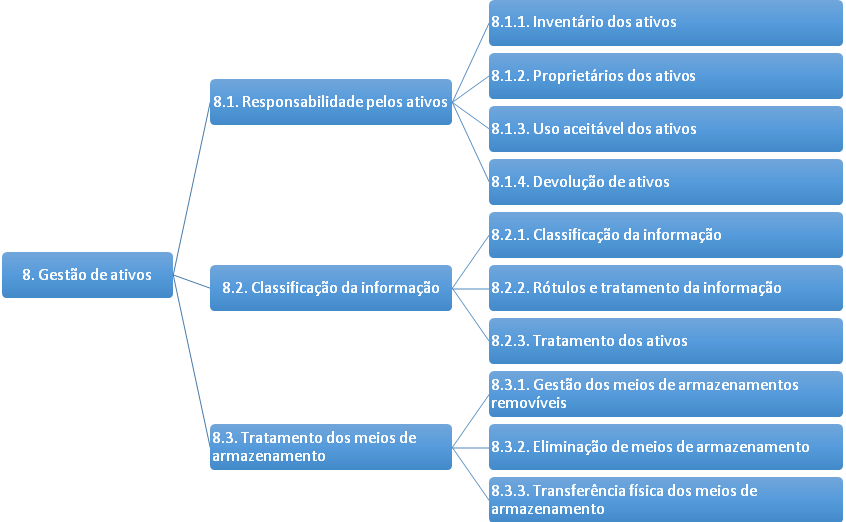
Este controlo divide-se em 3 categorias e 6 controlos:



# 4.5 Secção 8 – Gestão de ativos

O objetivo desta secção é identificar os ativos da organização e definir as responsabilidades para a proteção de ativos. Assegurar que a informação recebe um nível adequado de proteção, de acordo com a sua importância para a organização. Nesta seção são ainda definidas as diretrizes para prevenir a divulgação não autorizada, modificação, remoção ou destruição da informação armazenada nos dispositivos de armazenamento (CDs, Tapes, DVDs, etc).

Em resumo esta seção está assim definida:



A categoria **8.1 - Responsabilidade pelos ativos**, tem o objetivo de alcançar e manter a proteção adequada dos ativos da organização, apresentando os controlos que devem ser aplicados no tratamento da segurança da informação nos ativos. Esta categoria tem 4 controlos, que a seguir se descrevem.

**8.1.1. – Inventário dos ativos** – Convém que os ativos associados com informação e com os recursos de processamento da informação sejam identificados e um inventário destes ativos seja estruturado e mantido.

Nesse sentido é fundamental que a organização identifique os ativos relevantes no ciclo de vida da informação e documente a sua importância. Convém que o ciclo de vida da informação, inclua a criação, o processamento, o armazenamento, a transmissão, a remoção e a sua destruição. A documentação deve ser mantida e deve existir um inventário apropriado.

Este inventário deve ter para cada um dos ativos identificados o responsável (ver 8.1.2) e a classificação do ativo identificado (ver 8.2).

A compilação de um inventário de ativos é um pré-requisito importante para a gestão de riscos.

**8.1.2. – Proprietários dos ativos** –os ativos devem ter um proprietário. Convém que as pessoas e outras entidades que tenham responsabilidades aprovadas pelo executivo para qualificar o ciclo de vida do ativo e que sejam designadas como proprietário deste ativo.

Convém que seja implementado um processo para assegurar a atribuição em tempo útil, do proprietário de um ativo. O proprietário do ativo tem de:

1. assegurar que os ativos são inventariados;
2. assegurar que os ativos são adequadamente classificados e protegidos;
3. definir e periodicamente analisar criticamente as classificações e restrições ao acesso aos ativos importantes, levando em conta as políticas de controlo de acesso aplicáveis;
4. assegurar um adequado tratamento quando o ativo é removido ou destruído;

**8.1.3. – Uso aceitável dos ativos** - Convémque as regras para o uso aceitável das informações, dos ativos associados com a informação dos recursos de processamento da informação, sejam identificados, documentadas e implementadas.

Convém que os funcionários ou entidades externas que usam os ativos da organização estejam conscientes dos requisitos de segurança da informação dos ativos da organização.

**8.1.4. – Devolução dos ativos** – Convém que todos os funcionários e entidades externas devolvam todos os ativos da organização que estejam na sua posse, após o término dos seus projetos, do contrato ou acordo.

Convém que o processo de término de qualquer atividade com a organização seja formalizado para contemplar a devolução de todos os equipamentos físicos e eletrónicos cuja propriedade seja da organização.

Toda a informação que seja importante para as atividades da organização, deve ser documentada e obrigatoriamente transferida para a organização.

É conveniente que durante o período de cessão de contrato com a organização, esta monitorize possíveis cópias de informação relevantes (por exemplo, propriedade intelectual) pelos funcionários ou entidades externas que estão a sair da organização.

A categoria **8.2 – Classificação da informação**, tem como objetivo assegurar que a informação receba um nível adequado de proteção, de acordo com a sua importância para a organização. Esta categoria tem 3 controlos, que a seguir se descrevem.

**8.2.1. – Classificação de informação** – É fundamental que a informação seja classificada em termos do seu valor, requisitos legais, sensibilidade e criticidade para evitar modificação ou divulgação não autorizada.

Convém que os proprietários de ativos de informação sejam responsáveis pela sua classificação. A classificação deve ser incluída nos processos da organização e deve ser consistente e coerente em toda a organização. Convém que os resultados indiquem o valor dos ativos em função da sua sensibilidade e criticidade para a organização, em termos de confidencialidade, integridade e disponibilidade. É fundamental que os resultados da classificação sejam atualizados de acordo com as mudanças do seu valor, sensibilidade e criticidade ao longo do seu ciclo de vida.

A classificação de confidencialidade da informação pode ser baseado nos seguintes fatores:

* 1. quando a sua divulgação não causar qualquer dano;
  2. quando a divulgação causa pouco constrangimento ou inconveniência operacional;
  3. quando a divulgação tem um impacto pouco significativo nas operações ou objetivos táticos;
  4. quando a divulgação tem um impacto muito sério nos objetivos estratégicos a longo prazo, ou coloca a sobrevivência da organização em risco.

**8.2.2. – Rótulos e tratamento da informação –** os procedimentos para rotular e tratar a informação devem ser desenvolvidos e implementados de acordo com o esquema de classificação da informação adaptado na organização.

Por exemplo rotular informação como confidencial, pode levar a que seja mais apetecível o seu roubo, por pessoas internas ou externas.

**8.2.3. –Tratamento dos ativos –** os procedimentos para o tratamento dos ativos devem ser desenvolvidos e implementados de acordo com o esquema de classificação da informação adotada pela organização.

Neste controlo devem ser tidos em consideração os seguintes aspetos:

1. Restrições de acesso para apoiar os requisitos de proteção para cada nível de classificação;
2. Manutenção de um registo formal dos destinatários de ativos autorizados;
3. Armazenamento dos ativos de TI de acordo com as especificações dos fabricantes;
4. Identificação eficaz de todas as cópias para chamar a atenção dos destinatários autorizados.

A categoria **8.3 – Tratamento de dispositivos de armazenamento** -o objetivo desta categoria é prevenir a divulgação não autorizada, modificação, remoção ou destruição da informação armazenada nos dispositivos físicos de armazenamento.

Os controlos desta categoria não serão descritos porque não foi realizada a sua implementação prática.

A tabela seguinte resume os critérios de avaliação de cada ativo por cada vértice:

|  |  |
| --- | --- |
| **Valores para a Confidencialidade, Integridade e Disponibilidade** | |
| Pergunta genérica: qual a criticidade deste ativo para o negócio? Qual a importância dos requisitos em termos de Confidencialidade, Integridade ou Disponibilidade para a segurança da informação? | |
| Alta | 3 |
| Média | 2 |
| Baixa | 1 |

Tabela : Critérios de avaliação dos ativos

# 4.6 Secção 9 – Controlo de Acesso

O objetivo desta secção limitar o acesso à informação e aos recursos de processamento da informação.

Em resumo esta secção está assim definida:

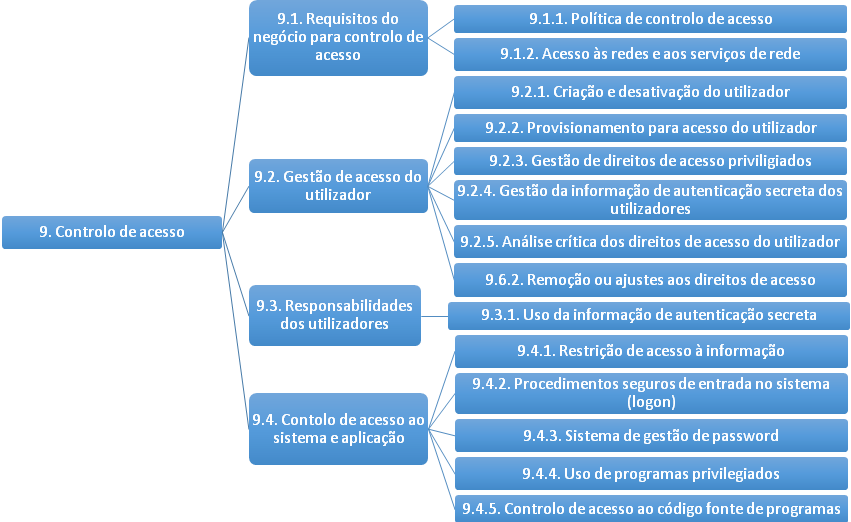


Figura : Controlos da Secção 9 - Controlo de acesso

Esta secção não será muito detalhada porque não resultou em nenhum *delivery* no âmbito deste trabalho. No entanto as políticas de controlo de acessos numa implementação da ISO 27001 e 27002 deve ser documentada e deve considerar pelo menos:

* Informações x negócios;
* Classificações das informações;
* Requisitos para autorização;
* Análise regular dos controlos.

A política de controlo de acessos deve ser definida e documentada para as organizações no sentido de garantir as devidas medidas e procedimentos de segurança aos recursos lógicos e físicos, em conformidade com os requisitos do negócio. Sendo assim, a política de controlo de acessos deve considerar, pelo menos:

* Informações manipuláveis por aplicações de negócio e riscos inerentes;
* A classificação das informações;
* Legislação, requisitos regulamentos e contratos vigentes pertinentes à proteção de acesso;
* Requisitos para autorização formal de pedidos de acesso e remoção de direitos;
* Requisitos para verificação regular dos controlos de acesso.

A política em questão deverá contemplar em conjunto, controlos de acesso lógico e físico.

As medidas e procedimentos para a proteção de recursos computacionais, como redes, ficheiros aplicações, entre outros deve considerar:

* Identificação dos recursos a proteger;
* Atribuição adequada de direitos de acesso e a sua devida monitorização;
* Educação para a segurança da informação;

Alguns exemplos de recomendações para a utilização de passwords, na sua gestão de controlos de acesso lógico:

* É dever da gestão de segurança, desabilitar contas inativas, sem passwords ou com senhas padrão;
* A password inicial do utilizador deve ser gerada de modo a que já esteja expirada, forçando a entrada de uma nova password no primeiro logon;
* Devem ser bloqueadas as contas dos utilizadores após determinado número de tentativas de acesso sem sucesso;
* O armazenamento das passwords deve ser feito de forma cifrada;

# 4.7 Secção 10 – Criptografia

O objetivo desta secção é assegurar o uso efetivo e adequado da criptografia para proteger a confidencialidade, autenticidade e/ou a integridade da informação.

Em resumo esta secção está assim definida:

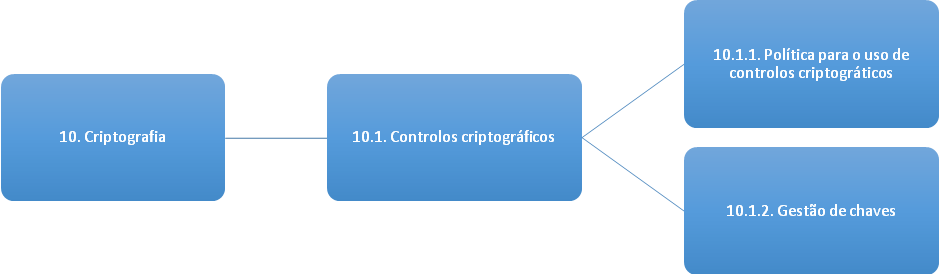


Figura : Controlos da Secção 10 - Criptografia

Convém que seja desenvolvida e implementada uma política para o uso de controlos criptográficos para a proteção de informação. Devem ser consideradas na implementação da política criptográfica da organização, as leis ou regulamentos e restrições nacionais aplicáveis à utilização de técnicas de criptografia.

Uma política sobre a utilização de controlos criptográficos é necessário para maximizar os benefícios, minimizar os riscos do uso de técnicas criptográficas e para evitar o uso incorreto ou inapropriado.

Deverá existir uma política para utilização e proteção do ciclo de vida das chaves criptográficas, incluindo a geração, armazenamento, arquivo, recuperação, distribuição, desativação e destruição de chaves.

A ISO/IEC 11770 fornece informação adicional sobre a gestão de chaves.

# 4.8 Secção 11 – Segurança física e do ambiente

O objetivo deste controlo é prevenir o acesso físico não autorizado, danos e interferências com os recursos de processamento de informações e as informações da organização.

Em resumo esta secção contempla os seguintes controlos:



Figura : Controlos da 11 –segurança física e do ambiente

Os controlos de acesso físico têm como objetivo aplicar medidas preventivas para proteger equipamentos, documentações, bens e informações contra acessos não autorizados. Assim sendo, estes controlos servem como uma barreira adicional de segurança ao controlo de acesso lógico.

Deverá ser considerada a utilização de áreas protegidas e perímetros de segurança. Nas áreas protegidas (com controlo de acesso rígido), recomenda-se o processamento de informações críticas para o negócio da organização. No que concerne ao controlo de acesso físico existem duas categorias:

* **Controlos administrativos** – compreendem medidas e procedimentos administrativos como por exemplo a identificação dos funcionários e visitantes;
* **Controlos explícitos** – compreendem medidas de uso de fechaduras, cadeados, alarmes, seguranças, etc.

Esta secção trata ainda os controlos ambientais que visam a proteção de recurso contra ameaças à disponibilidade e à integridade. É possível aplicar medidas preventivas e/corretivas. As ameaças que devem ser tidas em conta são por exemplo:

* Incêndios;
* Falhas no fornecimento de energia elétrica;
* Descargas elétricas;
* Ameaças que envolvam água;
* Problemas com temperatura e ventilação;

As boas práticas recomendam que:

* Haja um planeamento de alocação dos equipamentos e móveis;
* Manutenção da limpeza e conservação;
* Implementação de dispositivos de combate a incêndio e redução do impacto com problemas de energia elétrica;
* Vistoria regular de todos os elementos.

# 4.9 Secção 12 – Segurança nas operações

O objetivo deste controlo é garantir a operação segura e correta dos recursos de processamento da informação.

Em resumo esta secção contempla os seguintes controlos:



Figura : Controlos da Secção 13 – Segurança nas operações

É fundamental que os procedimentos de operação sejam documentados e disponibilizados a todos os utilizadores que necessitem deles.

**12.1.1. – Documentação dos procedimentos de operação –** os procedimentos devem ser documentados e preparados para as atividades operacionais associadas a recursos de processamento de comunicação e informações, tais como procedimentos de ligar e encerrar computadores, criação de cópias de segurança (backups), manutenção de equipamentos, tratamento de sistemas de armazenamento (discos, DVDs, tapes), segurança e gestão do tratamento dos centros de dados.

**12.1.2. – Gestão de mudanças –** convém que as mudanças na organização, nos processos do negócio, nos recursos de processamento da informação e nos sistemas que afetam a segurança da informação, sejam controladas. É fundamental estabelecer procedimentos e responsabilidades de gestão formais para garantir que haja um controlo satisfatório de todas as mudanças.

**12.1.3. – Gestão de capacidade –** convém que a utilização dos recursos seja monitorizada e ajustada para as necessidades de capacidade futura para garantir o desempenho requerido pelo sistema. Este controlo também considera a capacidade dos recursos humanos, bem como dos gabinetes e instalações.

**12.1.4. – Separação dos ambientes de desenvolvimento, teste e de produção –** convém que o ambiente de desenvolvimento, teste e produção sejam separados para reduzir os riscos de acessos ou modificações não autorizadas no ambiente de produção.

**12.2.1. – Controlos contra códigos maliciosos –** convém que sejam implementados controlos de deteção, prevenção e recuperação para proteger contra códigos maliciosos, combinado com um programa adequado de consciencialização do utilizador.

**12.3.1. – Cópias de segurança das informações –** convém que as cópias de segurança das informações, softwares e das imagens do sistemas sejam efetuadas regularmente conforme a política de criação de cópias de segurança definida.

**12.4.1. – Registo de eventos –** convém que os registos (log) de eventos de atividades dos utilizadores, exceções, falhas e eventos de segurança da informação sejam produzidos, mantidos e analisados criticamente com intervalos regulares.

**12.4.2. – Proteção das informações dos registos de eventos (logs) –** convém que as informações dos registos (logs) e os seus recursos sejam protegidos contra acessos não autorizados nem permitir adulteração dos mesmos.

**12.4.3. – Registo de eventos (log) de administrador e operador –** convém que as atividades dos administradores e operadores do sistema sejam registados e os registos (logs) protegidos e analisados criticamente em intervalos regulares.

**12.4.4. – Sincronização dos relógios–** convém que os relógios de todos os sistemas de processamento de informação relevantes, dentro da organização ou do domínio de segurança, sejam sincronizados com uma fonte de tempo precisa.

**12.5.1. – Instalação de software nos sistemas operativos –** convém que os procedimentos para controlar a instalação de software nos sistemas operativos sejam implementados.

**12.6.1. – Gestão de vulnerabilidades técnicas –** convém que informações sobre vulnerabilidades técnicas dos sistemas de informação em uso, sejam obtidas em tempo útil. As vulnerabilidades devem ser avaliadas e tomadas as medidas apropriadas para lidar com os riscos associados. É fundamental que as vulnerabilidades encontradas possam ser corrigidas rapidamente. Para tal é fundamental que:

1. a organização defina e estabeleça funções e responsabilidades associadas na gestão das vulnerabilidades técnicas, incluindo a monitorização das mesmas, a avaliação dos riscos, correções, acompanhamento dos ativos e qualquer responsabilidade de coordenação requerida;
2. os recursos de informação a serem utilizadores para identificar as vulnerabilidades técnicas relevantes e para manter a consciencialização sobre os mesmos, sejam identificados;
3. seja definido um prazo para a reação a notificações de potenciais vulnerabilidades relevantes;
4. aplicar as correções (*patches*) de software nos sistemas vulneráveis;
5. as correções antes de ser aplicadas sejam testadas;
6. se registe a auditoria realizada;
7. se contemple primeiro os sistemas de alto risco;
8. se defina um procedimento para contemplar a situação onde uma vulnerabilidade tenha sido identificada e não existam controlos adequados.

**12.6.2. – Restrições quanto à instalação de software –** convém que sejam estabelecidas e implementadas regras definindo critérios para a instalação de software pelos utilizadores.

**12.7.1. – Controlos de auditoria de sistemas de informação –** convém que os requisitos e atividades de auditoria envolvendo verificação nos sistemas operativos sejam cuidadosamente planeados e acordados para minimizar interrupção dos processos de negócio.

# 4.10 Secção 13 – Segurança nas comunicações

O objetivo deste controlo é garantir a proteção das informações em redes e dos recursos de processamento da informação que os apoiam.

Em resumo esta secção contempla os seguintes controlos:

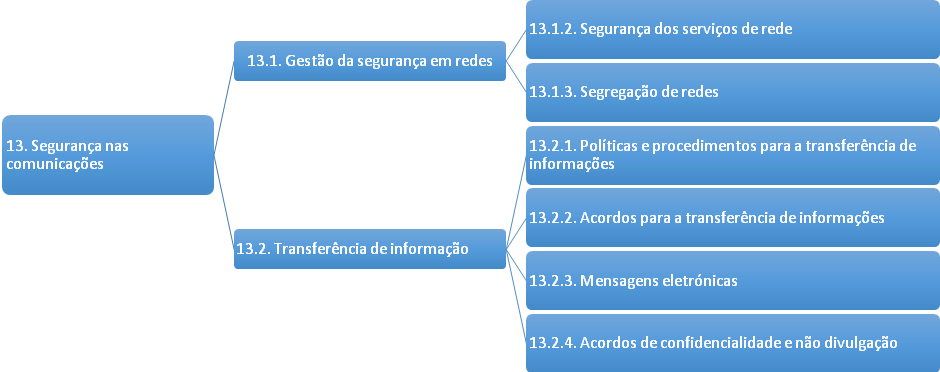


Figura : Controlos da secção 13 – Segurança nas comunicações

**13.1.1. – Controlos de redes –** convém que as redes sejam geridas e controladas para proteger as informações nos sistemas e aplicações. Devem ser identificados os responsáveis sobre a gestão de equipamentos de rede. As redes wireless devem ter mecanismos de encriptação para proteger os sistemas e aplicações a elas ligadas. A ligação à rede deve ser restrita e sujeita a uma autenticação forte.

A norma ISO/IEC 27033 aborda em pormenor as questões relativas à segurança de rede.

**13.1.2. – Segurança nos serviços de rede –** convém que os mecanismos de segurança, níveis e requisitos de gestão de todos os serviços de rede, sejam identificados e incluídos em qualquer contrato de serviços de rede, quer sejam providos internamente ou por terceiros.

**13.1.3. – Segregação de redes –** convém que os grupos de serviços de informação, utilizadores e sistemas de informação sejam segregados em redes.

**13.2.1. – Políticas e procedimentos para a transferência de informações –** convém que políticas, procedimentos e controlos de transferências formais, sejam estabelecidas para proteger a transferência de informações, utilizando todos os tipos de recursos de comunicações.

**13.2.2. – Acordos para transferência de informações –** convém que sejam estabelecidos acordos para a transferência segura de informações do negócio entre a organização e partes externas.

**13.2.3. – Mensagens eletrónicas –** convém que as informações que são transferidas em mensagens eletrónicas sejam adequadamente protegidas.

**13.2.4. – Acordos de confidencialidade e não divulgação –** convém que os requisitos para a confidencialidade ou acordos de não divulgação que contenham as necessidades da organização para a proteção da informação sejam identificados, analisados e criticamente documentados.

# 4.11 Secção 14 – Aquisição, desenvolvimento e manutenção de sistemas

O objetivo deste controlo é que a segurança da informação é parte integrante de todo o ciclo de vida dos sistemas de informação.

Em resumo esta secção contempla os seguintes controlos:

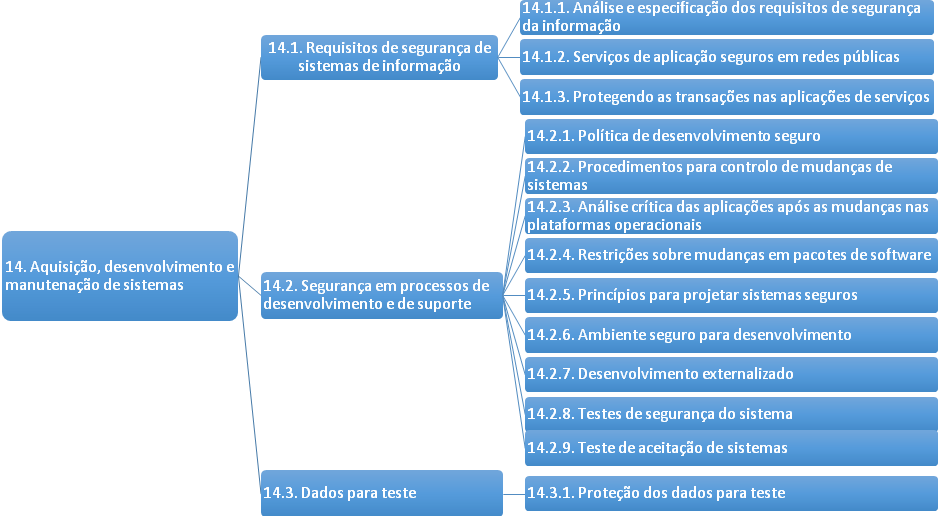


Figura : Controlos da secção 14 – Aquisição, desenvolvimento e manutenção de sistemas

Esta secção não será detalha, pois não resultou em nenhum *delivery* no âmbito deste trabalho. Esta secção visa as políticas relacionadas com a segurança de aquisição/desenvolvimento de novos sistemas de informação ou melhoria dos já existentes.

Começa por ter um controlo que tem como objetivo a análise e identificação de todos os requisitos de segurança da informação, utilizando vários métodos como requisitos de conformidade oriundos de política e legislação, modelos de ameaças, análises críticas de incidentes ou o uso de critérios de vulnerabilidades (limites).

Tem também um controlo que valida se as informações de serviços e aplicações que ocorrem sobre redes públicas, sejam protegidas de atividades fraudulentas. Os conteúdos que são transacionados na internet devem ser cifrados (*https*) e devem ser garantidas a privacidade dos dados dos utilizadores.

O objetivo de controlo 4.2 define os controlos que se devem implementar no desenvolvimento de aplicações na organização. Toda a informação deve esta assegurada com mecanismos de segurança que evitem o acesso indevido. São ainda definidas políticas sobre como proteger sistemas, documentados, mantidos e aplicados para qualquer implementação de um sistema de informação. Para a fase de testes das aplicações, são também definidas políticas seguras de realização de testes nas aplicações, incluindo os desenvolvimentos externalizados pela organização a terceiros.

# 4.12 Secção 15 – Relacionamento com fornecedores

O objetivo deste controlo é garantir a proteção dos ativos da organização que são acessíveis pelos fornecedores.

Em resumo esta secção contempla os seguintes controlos:

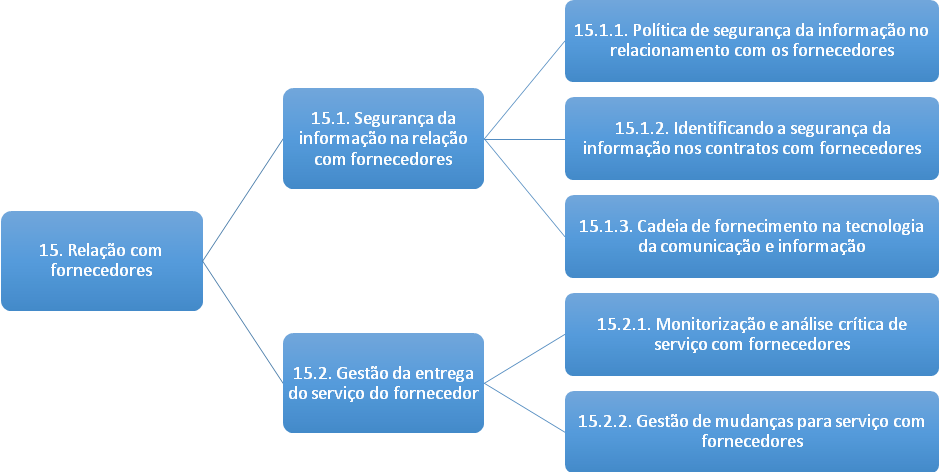


Figura : Controlos da secção 15 – Relacionamento com fornecedores

Esta secção tem como objetivo mitigar os riscos associados com o acesso dos fornecedores aos ativos da organização, nomeadamente acordados e documentados. Todos os requisitos de segurança da informação relevantes devem ser estabelecidos e acordados com cada fornecedor que possa aceder, processar, armazenar, comunicar, ou prover componentes de infraestrutura de TI para as informações da organização.

Convém que os contratos com os fornecedores incluam requisitos, para contemplar os riscos de segurança da informação, associados a cada cadeia de fornecimento de produtos e serviços de tecnologia de informação e comunicação.

# 4.13 Secção 16 – Gestão de incidentes de segurança da informação

O objetivo deste controlo é assegurar o foco consistente e efetivo para gerir os incidentes de segurança da informação, incluindo a comunicação sobre fragilidades e eventos de segurança da informação.

Em resumo esta secção contempla os seguintes controlos:

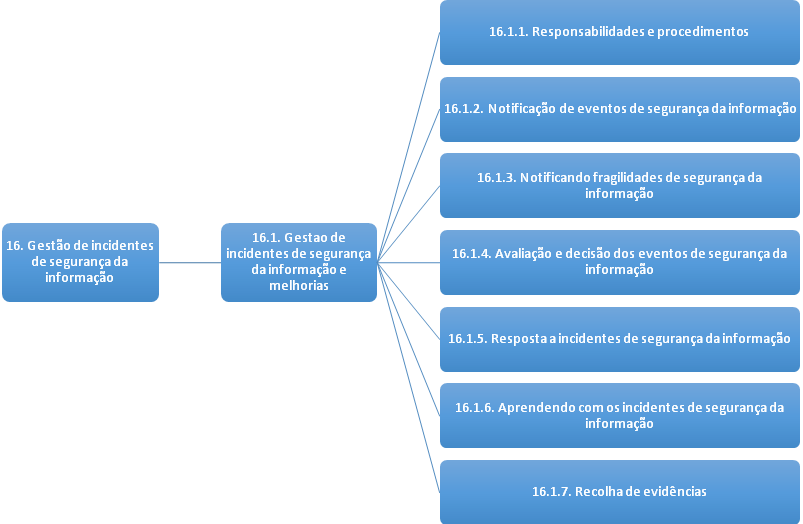


Figura : Controlos da secção 16 – Gestão de incidentes de segurança da informação

Convém que as responsabilidades e procedimentos de gestão sejam estabelecidos para assegurar respostas rápidas, efetivas a incidentes de segurança da informação. Esta secção também descreve diretrizes para que os eventos de segurança de informação sejam relatados através dos canais apropriados o mais rápido possível.

É fundamental que os eventos de segurança sejam avaliados e que seja decidido se são classificados como incidentes de segurança da informação.

Nesta secção também é definido como é que os incidentes de segurança são reportados e documentados, para que a organização possa analisar e aprender para reduzir a probabilidade ou o impacto de incidentes futuros.

# 4.14 Secção 17 – Aspetos da segurança da informação na gestão da continuidade do negócio

O objetivo deste controlo é garantir que a continuidade da segurança da informação seja considerada nos sistemas de gestão da continuidade do negócio da organização.

Em resumo esta secção contempla os seguintes controlos:

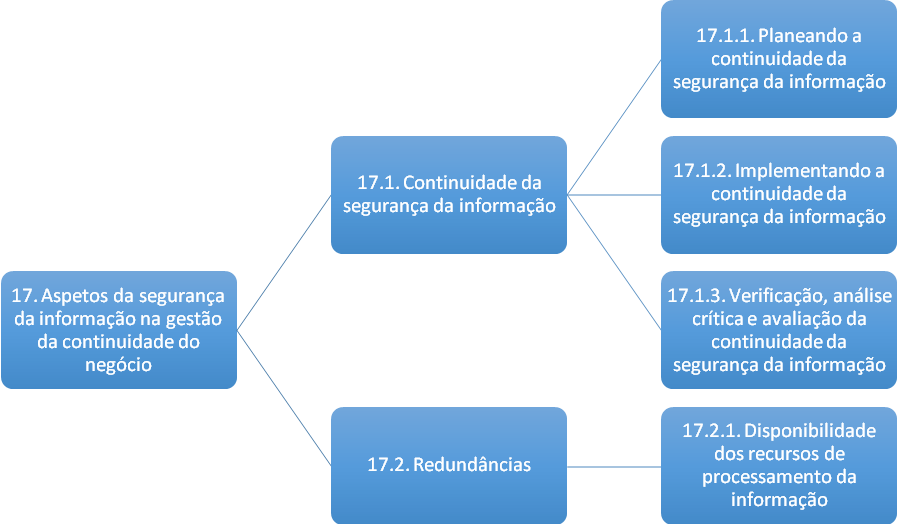


Figura : Controlos da secção 17 – Aspetos da segurança da informação na gestão da continuidade do negócio

Esta secção da norma ISO/27002 define os requisitos para a segurança da informação e a continuidade da gestão da segurança da informação em situações adversas, por exemplo, durante uma crise ou desastre. Convém que a organização estabeleça, documente, implemente e mantenha processos, procedimentos e controlos para assegurar o nível requerido de continuidade para a segurança da informação, durante uma situação adversa.

No objetivo de controlo 17.2. Redundâncias, são definidas políticas para que sejam implementadas redundâncias do SI para atender aos requisitos de disponibilidade.

# 4.15 Secção 18 – Conformidade

O objetivo deste controlo é evitar a violação de qualquer legislação, regulamento ou contrato relacionados com a segurança da informação e de quaisquer requisitos de segurança.

Em resumo esta secção contempla os seguintes controlos:

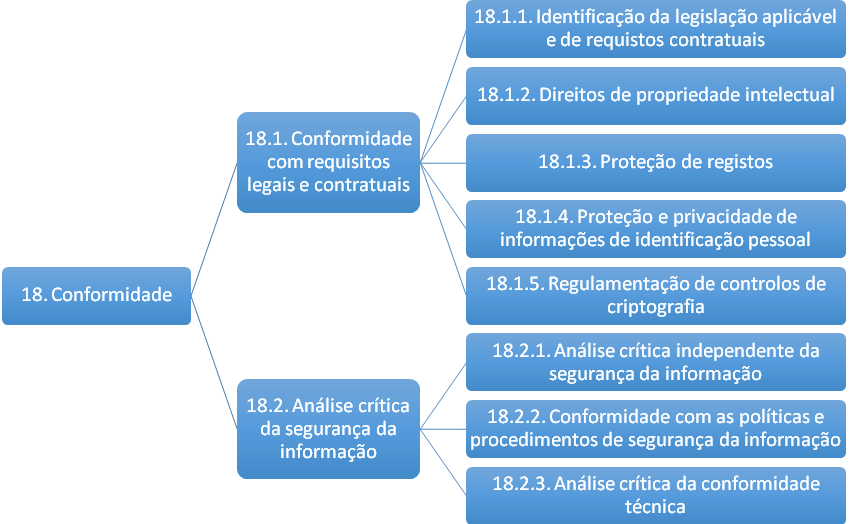


Figura : Controlos da secção 18 – Conformidade

Esta secção visa evitar que ocorram violações à lei ou a outros instrumentos de requisitos legais necessários cumprir por qualquer organização. Todos os aspetos relacionados com a segurança da informação devem ser documentados e comunicados a toda a organização.

Convém ainda que os procedimentos adequados sejam implementados para garantir a conformidade com os requisitos legislativos, regulamentares e contratuais relacionados com os direitos de propriedade intelectual e sobre o uso de software proprietário.

O controlo 18.1.2. Direitos de propriedade intelectual versa princípios que devem estar plasmados na política de segurança da organização, nomeadamente na proibição de instalação de software sem a aquisição das respetivas licenças, assim como proíbe a cópia de software adquirido para instalações que possam violar a propriedade intelectual.

É fundamental que os registos de base dados sejam protegidos contra perda, destruição, falsificação, acesso não autorizado e fornecimento não autorizado, de acordo com os requisitos regulamentares do negócio.

Muito naquilo que é hoje uma realidade que todas as organizações terão de implementar até maio de 2018, o Regulamento Geral de Proteção de Dados, que define regras para a implementação de políticas para proteção de dados pessoais, refere o controlo 18.1.4. Proteção e privacidade de informações de identificação pessoal. É fundamental e agora ainda mais com obrigação legal, implementar políticas para a proteção e privacidade da informação de identificação pessoal.

É portanto crucial para a organização que os SI sejam analisados criticamente, em intervalos regulares, para verificação da conformidade com as normas e políticas de segurança da informação definidos na organização. Uma das ações a implementar pode por exemplo ser, a realização de testes de invasão e avaliações de vulnerabilidades (18.2.3. Análise crítica da conformidade técnica).

Declaração de aplicabilidade

A declaração de aplicabilidade é um plano para a implementação da norma ISO 27001 numa organização.

Define por exemplo quais os controlos que são aplicáveis ou não para a organização.

Exemplo:

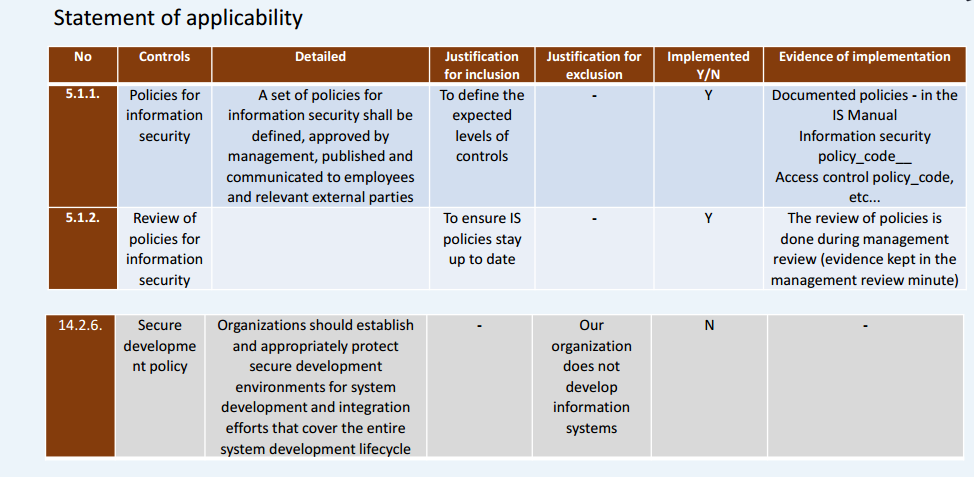


Figura : Exemplo da estrutura de uma Declaração de Aplicabilidade

A **Declaração de Aplicabilidade** é portanto um documento de relevante importância e utilidade no processo de implementação da NP ISO/IEC 27001:2013 e um dos principais *deliverables* da fase de planeamento. Este documento é a principal ligação entre a avaliação, tratamento de riscos e a implementação do sistema de segurança da informação onde está definido, o que se pretende, ou seja, o que fazer com a segurança da informação, fornecendo uma visão geral mas, efetiva do que precisa de ser feito, porque é que precisa de ser feito e como precisa de ser feito. É um documento direcionado aos gestores de topo/intermédios e auditores, pelo que deverá apresentar uma linguagem e um interface com adequada leitura, não sendo direcionado para o quotidiano operacional. Em síntese, a Declaração de Aplicabilidade deve conter:

* Controlos selecionados
* Razão ou razões para a seleção dos controlos
* Objetivos de controlos e controlos atualmente implementados
* Exclusões (incluindo justificação para a exclusão)
* Interface com fácil leitura

No âmbito deste trabalho resultou portanto o documento Declaração de Aplicabilidade [*Delivery 5*].