

ESCOLA TÉCNICA JOAQUIM FERREIRA DO AMARAL

JOÃO GABRIEL RIBEIRO DA SILVA

LUCAS GABRIEL DE PAULA PINTO

NORMAS DE QUALIDADE DE TESTE DE SOFTWARES

JAHU – SP

2023

**RESUMO**

As organizações modernas dependem cada vez mais de informações digitais, e é vital que essas informações sejam mantidas seguras. Além disso, a qualidade do software é uma preocupação importante para garantir que ele atenda às necessidades dos usuários e às expectativas do mercado. Nesse contexto, a adoção de normas ISO/IEC pode ajudar as organizações a alcançar esses objetivos.

A norma ISO/IEC 27001 é um padrão para o gerenciamento de segurança da informação, que estabelece requisitos para a implementação e manutenção de um sistema de gestão de segurança da informação. A norma ISO/IEC 12207 estabelece requisitos para o ciclo de vida do software, incluindo atividades como planejamento, desenvolvimento, operação e manutenção. A norma ISO/IEC 25010 fornece um modelo de qualidade de software mais abrangente, que abrange características como segurança, compatibilidade, escalabilidade e desempenho. A norma ISO/IEC 25020 fornece um conjunto de métricas que podem ser usadas para medir a qualidade do software em termos dessas características. Por fim, a norma ISO/IEC 27004 fornece diretrizes para a medição da eficácia do sistema de gestão de segurança da informação, enquanto a norma ISO/IEC 25030 fornece orientação para a medição da qualidade do software em termos de desempenho e eficiência.

A aplicação dessas normas pode ajudar as organizações a desenvolver e implementar políticas e práticas efetivas para proteger as informações e melhorar a qualidade do software, permitindo que elas atinjam seus objetivos com maior eficiência e eficácia.

**ABSTRACT**

Modern organizations increasingly rely on digital information, and it is crucial that this information is kept secure. Additionally, software quality is an important concern to ensure that it meets the needs of users and market expectations. In this context, the adoption of ISO/IEC standards can help organizations achieve these objectives.

The ISO/IEC 27001 standard is a framework for information security management, which sets requirements for the implementation and maintenance of an information security management system. The ISO/IEC 12207 standard sets requirements for the software lifecycle, including activities such as planning, development, operation, and maintenance. The ISO/IEC 25010 standard provides a more comprehensive software quality model, which covers characteristics such as security, compatibility, scalability, and performance. The ISO/IEC 25020 standard provides a set of metrics that can be used to measure software quality in terms of these characteristics. Finally, the ISO/IEC 27004 standard provides guidelines for measuring the effectiveness of the information security management system, while the ISO/IEC 25030 standard provides guidance for measuring software quality in terms of performance and efficiency.

The application of these standards can help organizations develop and implement effective policies and practices to protect information and improve software quality, enabling them to achieve their objectives more efficiently and effectively.

**LISTA DE FIGURAS**

Figura 1 – Modelo de medição da ISO 27004..........................................................10

Figura 2 – Processos da ISO 12207........................................................................12

**LISTA DE TABELAS**

Tabela 1 - Requisitos da norma ISO 27001...............................................................8

**LISTA DE ABREVIATURAS E SIGLAS**

ABNT Associação Brasileira de Normas Técnicas

ISO Organização Internacional de Normalização

IEC Comissão Eletrotécnica Internacional

NBR Norma Brasileira

SGSI Sistema de Gerenciamento da Segurança da Informação

**SUMÁRIO**

1. **INTRODUÇÃO……………………………………………………………………...7**
2. **ABNT NBR ISO/IEC 27001..............................................................................8**
3. **ABNT NBR ISO/IEC 27004..............................................................................9**
4. **ABNT NBR ISO/IEC 12207............................................................................11**
5. **ABNT NBR ISO/IEC 25010............................................................................13**
6. **ABNT NBR ISO/IEC 25020............................................................................N**
7. **ABNT NBR ISO/IEC 25030............................................................................N**

7

**1 INTRODUÇÃO**

A segurança da informação e a qualidade do software são temas críticos para as organizações em um mundo cada vez mais digital. Garantir que as informações estejam protegidas e que o software seja entregue com qualidade é fundamental para a sobrevivência e sucesso das empresas. Nesse contexto, as normas ISO/IEC são referências importantes que fornecem diretrizes para a gestão de segurança da informação e para a melhoria da qualidade do software. Neste trabalho, serão abordadas seis normas ISO/IEC relevantes para a segurança da informação e a qualidade do software. A compreensão dessas normas é essencial para que as empresas possam adotar boas práticas e garantir que suas informações estejam protegidas e que seus softwares sejam entregues com qualidade, atendendo às necessidades e expectativas dos usuários e stakeholders.

8

**2 ABNT NBR ISO/IEC 27001**

A ABNT NBR ISSO/IEC 27001, 2013 representa um padrão de utilização quando se fala em gerenciamento e gestão de segurança da informação. A norma pode ser aplicada em organizações de qualquer porte ou tipo e sua aplicação caracteriza uma organização como confiável, disponibilizando assim maior segurança para os seus clientes.

A norma ISO 27001 provê e apresenta requisitos para que uma organização possa estruturar seu SGSI. A norma funciona como guia para implementar, operar, monitorar, analisar criticamente, manter e melhorar um SGSI. Ela incorpora um processo de escalonamento de risco e valorização de ativos, orientando quanto à análise e identificação de riscos e a implantação de controle para minimizá-los. A norma permite que as organizações no mundo todo possam se certificar de suas práticas de gestão de segurança da informação.

Na implantação de um SGSI apoiado na ISO 27001 a norma dá suporte para que a organização possa utilizar as melhores técnicas para monitoramento e controles, envolvendo recursos tecnológicos e humanos.

Para que isso ocorra é necessário o devido treinamento para todos os colaboradores da organização, gerando assim conscientização por parte dos colaboradores, os treinamentos devem ser todos registrados. Esse processo auxilia na avaliação das normas que estão sendo postas em práticas pelos colaboradores, identificando e avaliando vulnerabilidades, riscos e ameaças que possam ocorrer e os seus níveis de impacto na organização.

Esta norma inclui requisitos para a avaliação e tratamento de riscos da segurança da informação voltadas para as necessidades da organização (ABNT ISSO 27001, 2013). Com a alta direção compromissada e o treinamento eficaz dos colaboradores, é possível se reduzir o número de ameaças que exploram eventuais vulnerabilidades. Na Tabela 1 se apresentam requisitos existentes na norma ISO 27001.

Tabela 1: Requisitos da Norma ISO 27001

|  |  |  |
| --- | --- | --- |
| **Nº** | **Requisitos** | **Descrição** |
| 1 | Escopo | Abrangência da Norma |
| 2 | Referência Normativa | Normas e padrões relacionados à norma 27001 |
| 3 | Termos e Definições | Termos e definições relacionadas à segurança da informação |
| 4 | SGSI | Referente à criação, implementação,  monitoramento e melhoria do SGSI, documentação e registros de informações |
| 5 | Responsabilidade da Direção | Definição de responsabilidades, treinamento e  provisão de recursos do SGSI |
| 6 | Auditorias Internas | Auditorias internas realizadas por pessoal treinado e comprometido com o SGSI |
| 7 | Análise Crítica do SGSI | Análise realizada pelo corpo diretivo da  organização das ações efetuadas pelo SGSI |
| 8 | Melhoria do SGSI | Trata das ações corretivas e preventivas efetuadas  pelo SGSI |

9

**3 ABNT NBR ISO/IEC 27004**

A norma ABNT NBR ISO/IEC 27004 foi publicada em 2010. Ela sugere padrões para desenvolvimento de métricas e medidas de desempenho como forma de avaliar os SGSI. A norma fornece orientação e ajuda para as organizações, para que elas melhorem a eficácia e a eficiência dos seus SGSI, gerando dessa forma indicadores e formas para medir a eficácia e eficiência.

A norma permite que as organizações avaliem a eficiência dos seus controles sob a sua segurança da informação, e que avaliem a eficiência da implementação de um SGSI, para verificar métricas que indicam se os requisitos de segurança estão sendo corretamente aplicados, auxilia na melhoria do desempenho da segurança ao que se trata de riscos de negócios e fornece dados para a gestão visando auxiliar a tomada de decisão. Alguns dos objetivos das normas são:

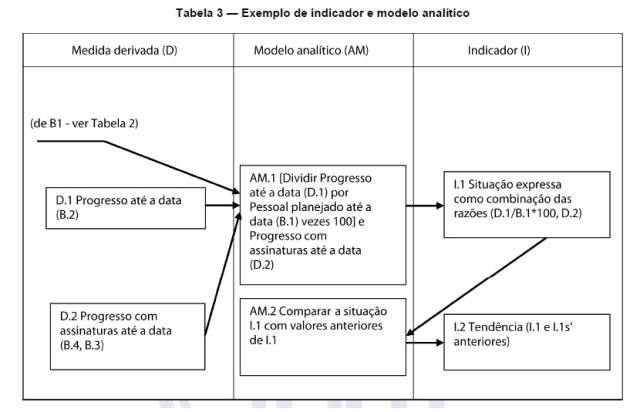
1. Avaliar a eficácia dos controles;
2. Avaliar a eficácia do SGSI;
3. Verificar se os requisitos da SI foram atendidos;
4. Melhorias nos controles implantados;
5. Melhorias na análise de riscos;
6. Auxiliar a tomada de decisões gerenciais;
7. SGSI sob uma perspectiva de negócios;
8. Facilitar decisão de investimento em SI.

A norma apresenta como implementar um Programa de Medição da Segurança da Informação (PMSI) que é um sistema de medição que possibilita uma visão adequada dos investimentos em segurança da informação, servindo de apoio para a tomada de decisão da alta administração. Um PMSI leva em conta a complexidade do SGSI, os seus papéis, responsabilidades e medidas implementadas além de considerar também os processos de negócios. Para ser considerado efetivo um PMSI deve incluir os seguintes processos:

1. Desenvolvimento de medidas e medições;
2. Operação de medição;
3. Relato do resultado da análise;
4. Melhorias nos controles implantados;

10

Figura 1: Modelo de medição da ISO 27004



Fonte: https://qualidadeonline.files.wordpress.com/2017/01/tabela-3\_medic3a7c3a3o.jpg

Objeto de medição é a caracterização de um item através da medição dos seus atributos. Ele está diretamente ligado a necessidade de informação e pode ser um produto, serviço ou um processo. O método de medição é uma sequência de operações usada na quantificação de um atributo dentro de uma escala. Medida básica é a medida definida e pode ser dividida em escalas. A medida derivada se trata da função realizada para combinar medidas básicas. Indicador é a medida do atributo conforme as necessidades de informação definidas. Os critérios de decisão são as margens, alvos ou os padrões usados para determinar a necessidade ou não de uma tomada de ação. E por fim o resultado da medição se trata dos indicadores e suas interpretações que atendam uma necessidade de informação.

11

**4 ABNT NBR ISO/IEC 12207**

A ISO/IEC 12207 é uma norma internacional que estabelece um modelo de ciclo de vida de software para desenvolvimento, operação e manutenção. Ela foi criada para auxiliar na gestão de projetos de software e para garantir que os produtos de softwares desenvolvidos atendam aos requisitos do cliente, sejam entregues dentro do prazo e dentro do orçamento.

O modelo de ciclo de vida de software descrito na ISO/IEC 12207 é composto por um conjunto de processos inter-relacionados que são realizados durante as fases do ciclo de vida de software. Esses processos são agrupados em três categorias principais: processos primários, processos de apoio e processos organizacionais.

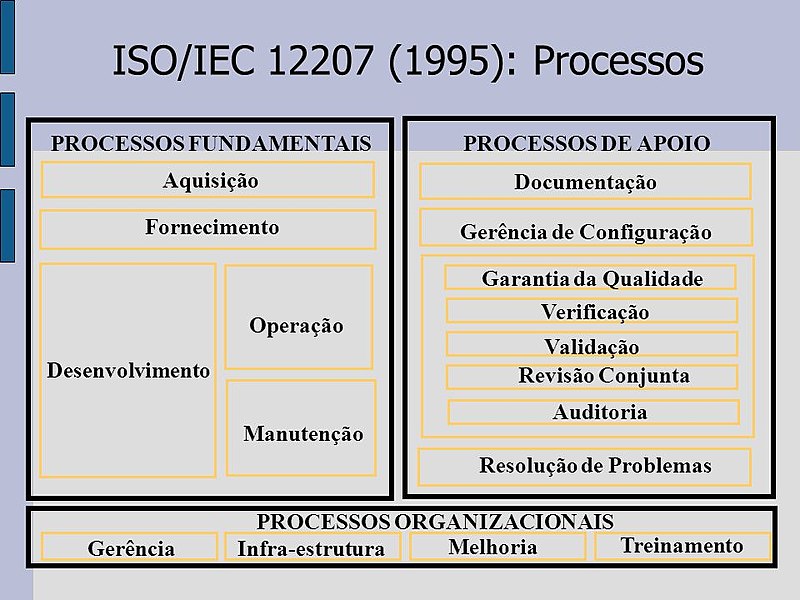
Os processos primários incluem aquisição, fornecimento, desenvolvimento, operação, manutenção e descarte de software. Os processos de apoio incluem gerenciamento de documentação, gerenciamento de configuração, gerenciamento de qualidade e verificação e validação. Os processos organizacionais incluem gerenciamento de projetos, gerenciamento de infraestrutura e gerenciamento de recursos humanos.

A norma ISO/IEC 12207 tem como objetivo fornecer um modelo abrangente para a gestão de projetos de software, garantindo a qualidade do software e a satisfação do cliente. Ela é aplicável a todos os tipos de software, desde sistemas simples até sistemas críticos de segurança.

A implementação da norma ISO/IEC 12207 pode trazer muitos benefícios para a organização, como a melhoria da qualidade do software, a redução de custos de desenvolvimento, a diminuição do tempo de desenvolvimento e a garantia de que o produto final atenda às necessidades do cliente.

12

Figura 2: Processos da ISO 12207



Fonte: https://pt.m.wikipedia.org/wiki/Ficheiro:Processos\_iso\_12207.jpg

13