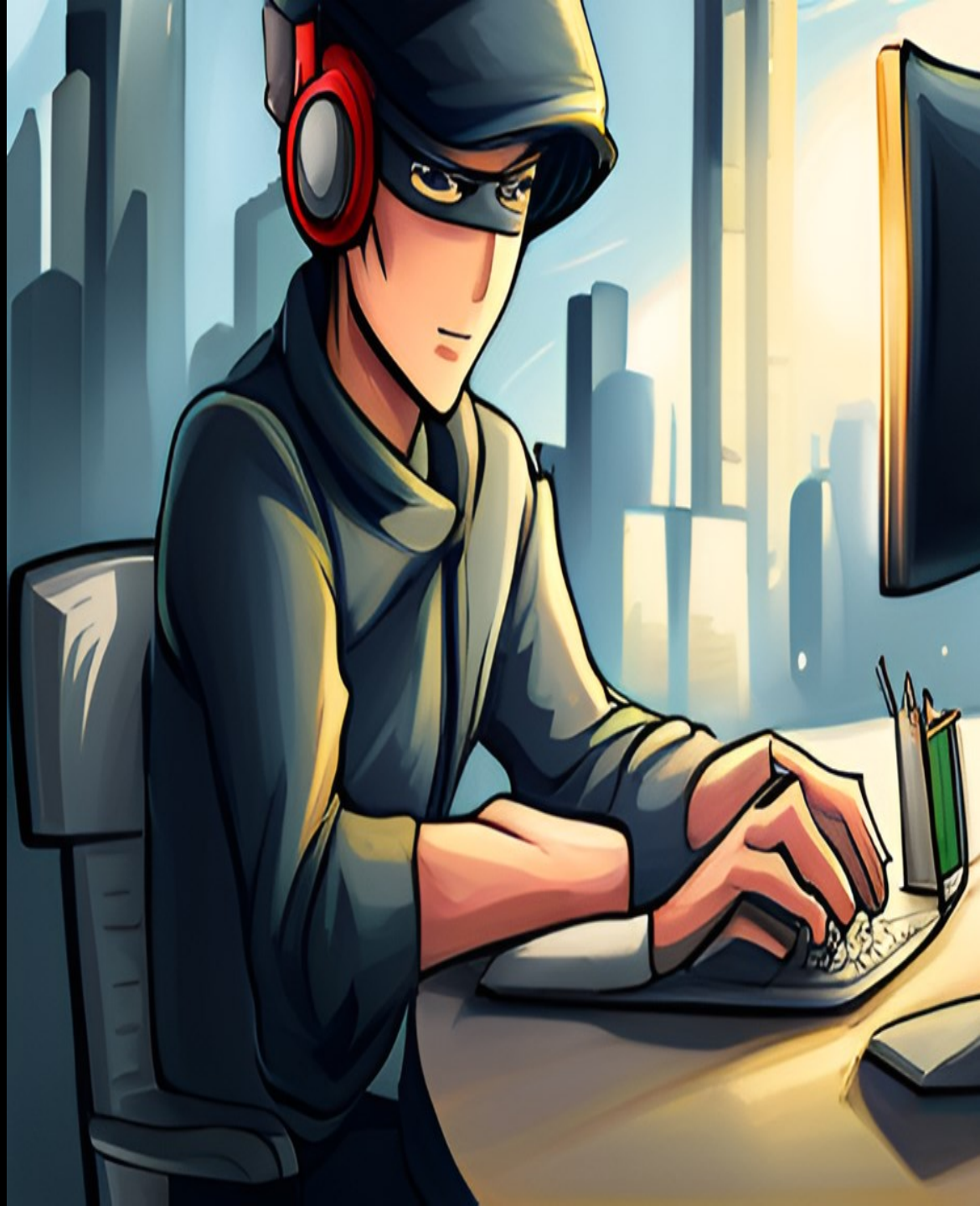
Segurança da Informação

Aula9 _ Normas de Segurança

Curso de Ciência da Computação

Prof. Dr. Rodrigo Xavier de Almeida Leão



As normas e os padrões de segurança da informação exercem um papel importante para as organizações, sob dois pontos de vista principais. Primeiramente, as normas e os padrões auxiliam as organizações na definição dos controles de segurança e também no estabelecimento do sistema de gestão que, por sua vez, é o responsável pelo ciclo efetivo da segurança da informação. Além da segurança da informação, é importante considerar também a gestão de riscos e a gestão de continuidade de negócios, que possuem um relacionamento direto entre elas, com intersecções compostas por controles equivalentes.

O segundo ponto de vista sobre a importância das normas e padrões é que elas demonstram a abordagem mais comprometida da organização com a segurança da informação, que é alcançada com a obtenção de certificação. A certificação mais conhecida em segurança da informação é a ISO/IEC 27001, que atesta organizações que possuem um sistema de gestão de segurança da informação.

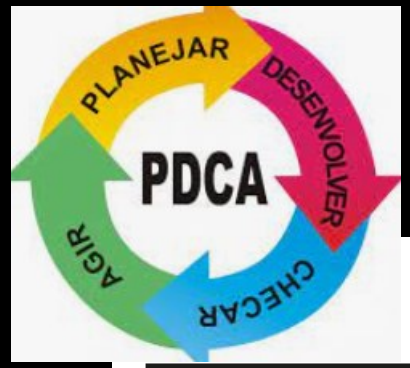
As principais normas e os padrões que envolvem a segurança da informação, que serão discutidos nesta aula, são:

- Segurança da informação: ABNT NBR ISO/IEC 27001:2013 e ABNT NBR ISO/IEC 27002:2013.
- Riscos: ABNT NBR ISO 31000:2009 e ABNT NBR ISO/IEC 27005:2011.
- Continuidade de negócios: ABNT NBR ISO/IEC 27031:2015 e ABNT NBR ISO 22301:2013.
- Governança de TI: COBIT.
- Serviços de TI: ITIL.

Norma de gestão de segurança da informação: ABNT NBR ISO/IEC 27001:2013

A principal norma de segurança da informação é a ABNT NBR ISO/IEC 27001:2013, que define os requisitos para Sistemas de Gestão da Segurança da Informação (SGSI) e faz parte da família de normas ISO 27000, que possui o foco em segurança da informação (ISO 27001, 2013).

Uma característica da ISO 27001 é que uma organização pode ser certificada na norma, o que indica que ela possui e segue um sistema de gestão de segurança da informação.



| Estrutura de uma política de segurança

Partes interessadas

Expectativas e requisitos de segurança da informação

Plan
Estabelecimento SGSI

Do
Implementação e operação do SGSI

Check
Monitoramento e análise crítica do SGSI

Act
Manutenção e melhoria do SGSI

Partes interessadas

Segurança da informação gerenciada

4. Identificar os riscos, de acordo com a abordagem de avaliação de riscos.
5. Analisar e avaliar os riscos, aplicando os critérios da abordagem de avaliação de riscos.
6. Identificar e avaliar as opções para o tratamento dos riscos.
7. Selecionar os objetivos de controles e os controles para o tratamento dos riscos.
8. Obter aprovação gerencial para os riscos residuais.
9. Obter autorização gerencial para implementar e operar o SGSI.
10. Preparar a declaração de aplicabilidade com as justificativas para os controles que deverão ser implementados e para os que foram excluídos.

Norma de código de prática para controles de segurança da informação: ABNT NBR ISO/IEC 27002:2013

A importância da norma ABNT NBR ISO/IEC 27002:2013, que trata do código de prática para controles de segurança da informação, existe devido aos processos 6 e 7 do estabelecimento do SGSI, que identificam e selecionam os controles de segurança para o tratamento dos riscos. Os objetivos de controles da ISO 27002 incluem (ISO 27002, 2013): política de segurança da informação; conformidade; gestão de continuidade do negócio; gestão de incidente de segurança da informação; aquisição, desenvolvimento e manutenção de sistemas de informação; controle de acessos; gerenciamento de operações e comunicações; segurança física e do ambiente; segurança de recursos humanos; gestão de ativo; organização da segurança da informação.

Normas de gestão de riscos: ABNT NBR ISO 31000:2009 e ABNT NBR ISO/IEC 27005:2011

A gestão de riscos possui uma estreita relação com a segurança da informação, de modo que para a obtenção de uma certificação ISO 27001 é preciso que a organização tenha estabelecida a gestão de riscos. Há duas normas principais que direcionam a gestão de riscos (ISO 27005, 2011), (ISO 31000, 2009):

- ABNT NBR ISO 31000:2009, que estabelece princípios e diretrizes da gestão de riscos de uma forma mais ampla, sem ser específico para a segurança da informação.
- ABNT NBR ISO/IEC 27005:2011, que estabelece a gestão de riscos de segurança da informação.

As normas ABNT NBR ISO 31000:2009 e ABNT NBR ISO/IEC 27005:2011 tratam dos processos de gestão de riscos:

- Estabelecimento e definição de contexto.
- Identificação de riscos.
- Estimativa e análise de riscos.
- Avaliação de riscos.
- Tratamento de riscos.
- Comunicação e consulta de riscos.
- Monitoramento, revisão e análise crítica de riscos.

Além da ABNT NBR ISO 31000:2009 e ABNT NBR ISO/IEC 27005:2011, outras normas relacionadas à gestão de riscos são relevantes (ABNT, 2016):

- ABNT ISO GUIA 73:2009, que trata do vocabulário da gestão de riscos.
- ABNT ISO/TR 31004:2015, que é um guia para implementação da ABNT NBR ISO 31000.
- ABNT NBR ISO/IEC 31010:2012, que trata de técnicas para o processo de avaliação de riscos.

Normas de gestão de continuidade de negócios

A gestão de continuidade de negócios possui uma relação direta com a segurança da informação, com foco na disponibilidade, visando à manutenção e ao restabelecimento dos negócios após um incidente de segurança, que também é tratado pela gestão de riscos e pela gestão de segurança da informação (ISO 22301, 2013).

As duas principais normas são a ABNT NBR ISO 22301:2013, que trata do sistema de gestão de continuidade de negócios, de uma forma mais ampla, e a norma ABNT NBR ISO/IEC 27031:2015, que foca na continuidade dos negócios com enfoque na tecnologia da informação e comunicação.

Um sistema de gestão de continuidade de negócios deve possuir pelo menos os seguintes documentos:

- Escopo e objetivos do sistema de gestão de continuidade de negócios.
- Política de continuidade de negócios.
- Descrição de regras e responsabilidades.
- Resultados da avaliação de riscos e da análise de impacto nos negócios.
- Plano de continuidade de negócios.
- Plano de comunicação, treinamento e conscientização.
- Procedimentos de exercícios e testes.

- Plano de comunicação, treinamento e conscientização.
- Procedimentos de exercícios e testes.

Norma e padrão de governança de TI

O COBIT (*Control Objectives for Information and Related Technology*) é um *framework* composto por ferramentas, recursos e guias para a governança e gerenciamento de TI. O COBIT é formado por duas camadas principais: a de governança corporativa de TI e a de gestão corporativa de TI.

A camada de governança é composta por cinco processos no domínio "Avaliar, Direcionar e Monitorar (*Evaluate, Direct and Monitor,* EDM)", que tratam de definição de um *framework* de governança, do estabelecimento das responsabilidades em termos de valor para a organização, de fatores de risco e recursos, bem como da transparência da TI para as partes interessadas (CHIARI, 2016).

Já a camada de gerenciamento é definida por quatro domínios:

- Alinhar, Planejar e Organizar (*Align*, *Plan* and *Organize*, APO): relacionada à identificação de como a TI pode contribuir com os objetivos de negócios.
- Construir, Adquirir e Implementar (*Build*, *Acquire* and *Implement*, BAI): relacionada aos investimentos e projetos para tornar concreta a estratégia de TI.
- Entregar, Servir e Suportar (*Deliver*, *Service and Support*, DSS): relacionada à entrega dos serviços de TI necessários para atender à estratégia e à tática.
- Monitorar, Analisar e Avaliar (*Monitor*, *Evaluate* and *Assess*, MEA).

Além do COBIT, a norma ABNT NBR ISO/IEC 38500:2009 também trata a governança corporativa de tecnologia da informação.

Norma e padrão de gestão de serviços de TI

O ITIL (*Information Technology Infrastructure Library*) é um conjunto de cinco livros que definem processos para o gerenciamento de serviços de TI. Apesar de não ser focado em segurança da informação, estão relacionados ao assunto os processos de gerenciamento da continuidade do serviço e, também, o gerenciamento da segurança da informação (TUPPENCE, 2010).

Além do ITIL, são importantes as seguintes normas de gestão de serviços (ABNT, 2016):

- ABNT NBR ISO/IEC 20000-1:2011, requisitos do sistema de gestão de serviços.
- ABNT NBR ISO/IEC 20000-2:2013, um guia de aplicação do sistema de gestão de serviços.
- ABNT ISO/IEC TR 20000-5:2011, exemplo de um plano de implementação da ABNT NBR ISO/IEC 20000-1.

O PRESIDENTE DA REPÚBLICA Faço saber que o Congresso Nacional decreta e eu sanciono a seguinte Lei:

CAPÍTULO I
DISPOSIÇÕES PRELIMINARES

Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Parágrafo único. As normas gerais contidas nesta Lei são de interesse nacional e devem ser observadas pela União, Estados, Distrito Federal e Municípios. (Incluído pela Lei nº 13.853, de 2019) Vigência

Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos:

I - o respeito à privacidade;

II - a autodeterminação informativa;

III - a liberdade de expressão, de informação, de comunicação e de opinião;

IV - a inviolabilidade da intimidade, da honra e da imagem;

V - o desenvolvimento econômico e tecnológico e a inovação;

VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e

VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

Prof. Dr. Rodrigo Xavier de Almeida Leão