UFOP
Universidade Federal de Ouro Preto

CSI303 – Segurança e Auditoria de Sistemas

Profa. Juliana Mara Lemos

Instituto de Ciências Exatas e Aplicadas

01

Norma e Certificações ISO/IEC 270001

O que são as Normas Técnicas?

As normas técnicas são **documentos** que estabelecem uma **série de especificações, diretrizes e regras** para a elaboração de processos, criação de produtos, oferta de serviços, terminologias que devem ser utilizadas e realização de pesquisas acadêmicas.

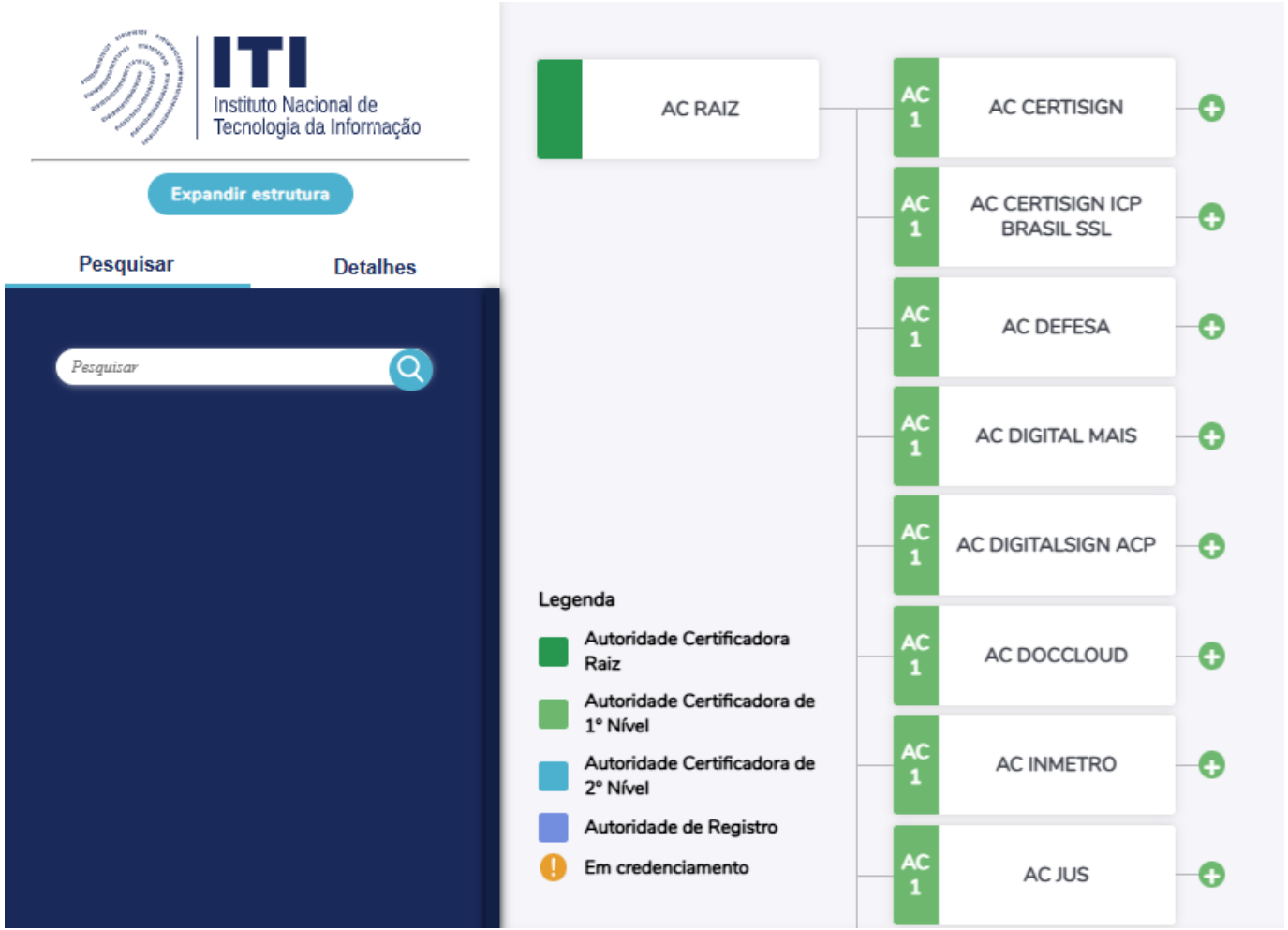
Qual o objetivo das Normas Técnicas?

O grande objetivo dessas normas é **contribuir** para a criação de um **padrão internacional** de desenvolvimento de determinadas atividades, para que **riscos** à segurança e saúde dos trabalhadores sejam **evitados** e os processos sejam realizados de forma correta, com qualidade, trazendo **eficiência** às empresas.

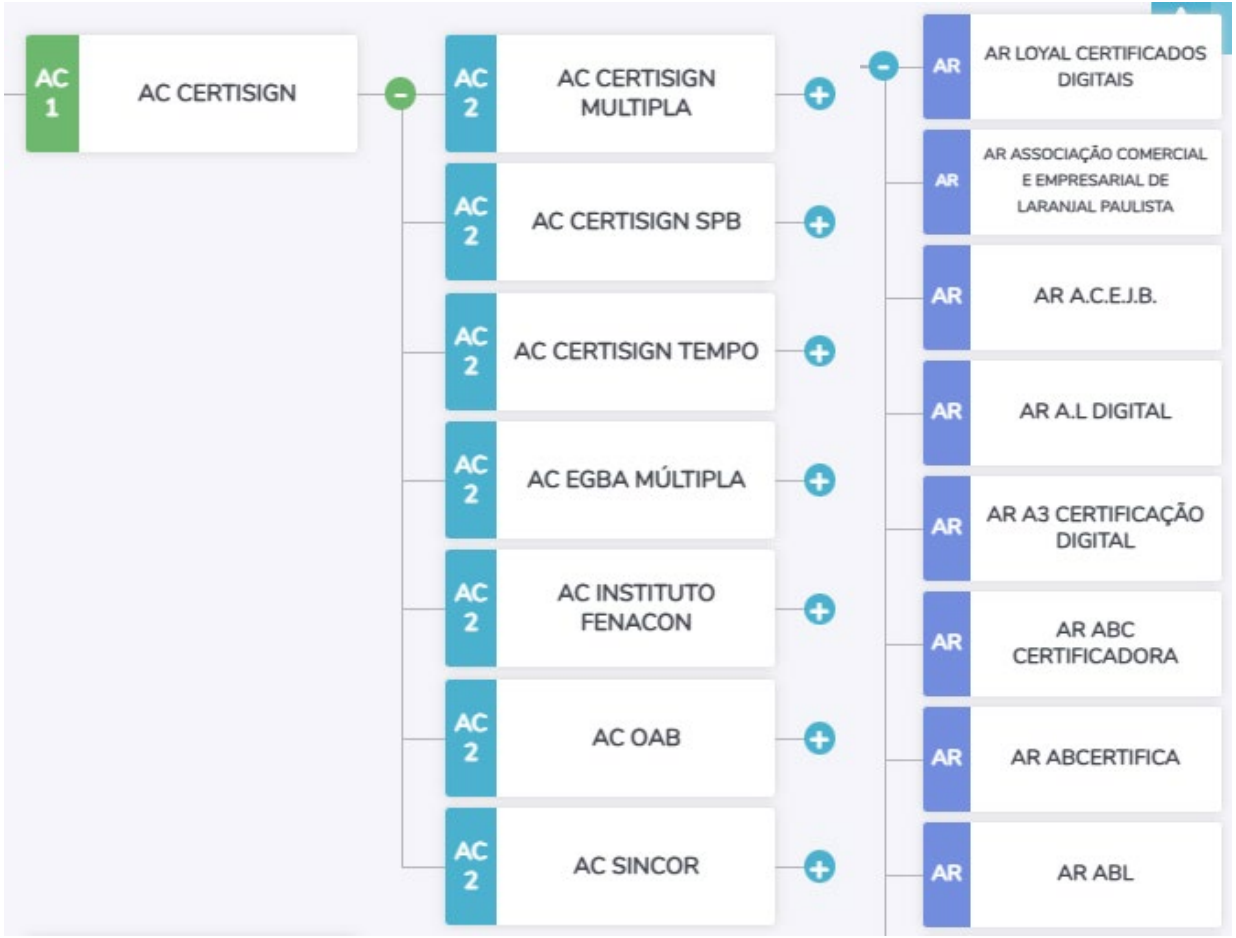
Certificação das instituições

- Para as instituições serem certificadas, elas passam por **auditorias** realizadas por **entidades certificadoras**, que checam todos os processos e conformidades.

- Realização de auditorias internas para verificação de inconformidades, adequação e auditorias externas.



Fonte: https://estrutura.iti.gov.br/



Fonte: https://estrutura.iti.gov.br/

Evolução

- BS7799, norma britânica desenvolvida pelo British Standards Institution.
- Foi aprovada pela ISO (International Organization for Standardization) e pela IEC (International Electrotechnical Commission) para utilização internacional e passou a ser conhecida como ISO/IEC 17799 em 2000.
- A partir de 2005, começaram a ser publicadas as normas da série 27000.
- Continua sendo considerada formalmente como 17799 para fins históricos.
- ISO 27001 foi baseada na ISO/IEC 17799 e substitui o BS7799.

Observação

- A aplicação das normas da série ISO/IEC 27000 não é obrigatória.
- Reúnem recomendações para uma gestão eficiente e que entregue bons resultados.
- Apenas a 27001 é passível de certificação.
- As demais funcionam como base para alcançar os resultados positivos (em especial a 27002).

ISO/IEC 27001 x ISO/IEC 27002

Enquanto **a ISO/IEC 27001** é uma **norma de requisitos** que define como estruturar e gerenciar um SGSI, a **ISO/IEC 27002 oferece orientações detalhadas** sobre como implementar os controles de segurança listados na ISO/IEC 27001. Juntas, elas ajudam as organizações a proteger seus ativos de informação de maneira eficaz.

ISO/IEC 27001

Objetivo: É uma norma que especifica os requisitos para estabelecer, implementar, manter e melhorar continuamente um Sistema de Gestão de Segurança da Informação (SGSI).

Certificação: As organizações podem ser certificadas conforme a ISO/IEC 27001, demonstrando que possuem um SGSI conforme os requisitos da norma.

Estrutura: Inclui cláusulas específicas sobre o contexto da organização, liderança, planejamento, suporte, operação, avaliação de desempenho e melhoria.

Requisitos de Documentação: Exige documentação e evidências das políticas e procedimentos implementados.

ISO/IEC 27002

Objetivo: Fornece diretrizes práticas para os controles de segurança listados no Anexo A da ISO/IEC 27001. Não especifica requisitos, mas sim boas práticas recomendadas.

Certificação: Não é certificável. Serve como uma referência para a implementação dos controles de segurança.

Estrutura: Organiza os controles em categorias e fornece detalhes sobre como cada controle pode ser implementado para mitigar riscos específicos.

Uso Prático: É usada para apoiar a implementação dos requisitos de controle definidos na ISO/IEC 27001.

02

Normas de Segurança da Informação

O que é a ISO/IEC 27001 - Gestão de Segurança da Informação?

É a norma internacional de gestão de segurança da informação. Ela descreve como colocar em prática um sistema de gestão de segurança da informação (SGSI) avaliado e certificado de forma independente.

Permite a projeção dos dados financeiros e confidenciais de maneira eficiente, minimizando a probabilidade de serem acessados ilegalmente ou sem permissão

ISO/IEC 27001

Define requisitos para implementação, operação, monitoramento, revisão, manutenção e melhoria de um Sistema de Gestão de Segurança da Informação (SGSI).

- Pode ser aplicada em qualquer organização, independentemente do porte ou setor.
- É ainda mais valorizada em empresas que priorizam a segurança da informação e a têm como fator crítico para as operações.
- Empresas de finanças, T.I. e setores públicos.

Vantagens da certificação

- Maior segurança para a rede corporativa.
- Diferencial para clientes que buscam empresas parceiras certificadas.
- Redução de custos com prevenção de incidentes de segurança da informação.
- Mais organização e produtividade.
- Conformidade com requisitos legais.
- Valor de mercado para divulgações e diferenciação em negociações.

Quais são os benefícios da ISO/IEC 27001?

- Identificação de riscos e definição de controles.
- Flexibilidade para adaptar os controles a todas as áreas.
- Ganha confiança das partes interessadas.
- Demonstra conformidade e permite obter o status de fornecedor preferencial.
- Atende às expectativas mais sensíveis, demonstrando conformidade.

ISO/IEC 27001:2006

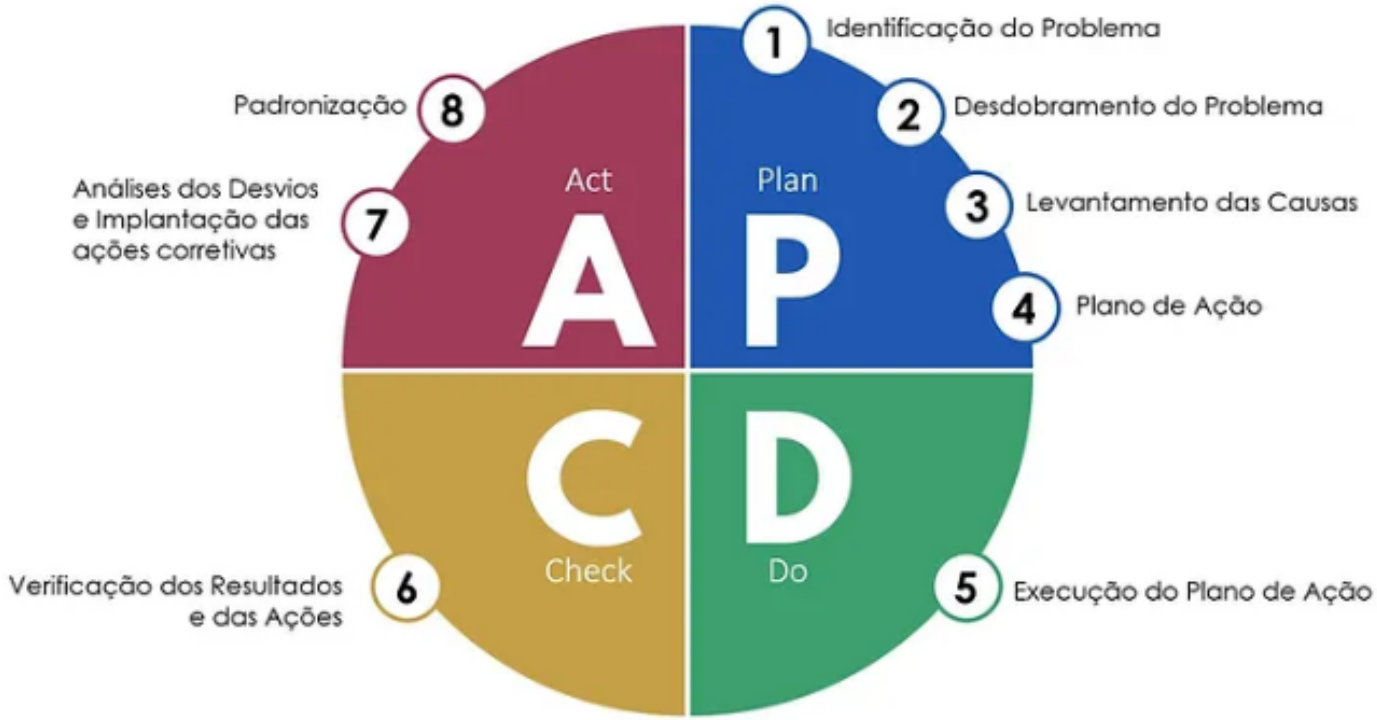
- Cancelada em 08/11/2013
- Substituída por: ABNT NBR ISO/IEC 27001:2013
- A norma foi publicada em 2013 pela ISO (International Organization for Standardization) e pela IEC (International Electrotechnical Commission). A versão atual é a ISO/IEC 27001:2022.
- Adota o modelo "Plan-Do-Check-Act” (PDCA), que é aplicado para estruturar todos os processos do SGSI

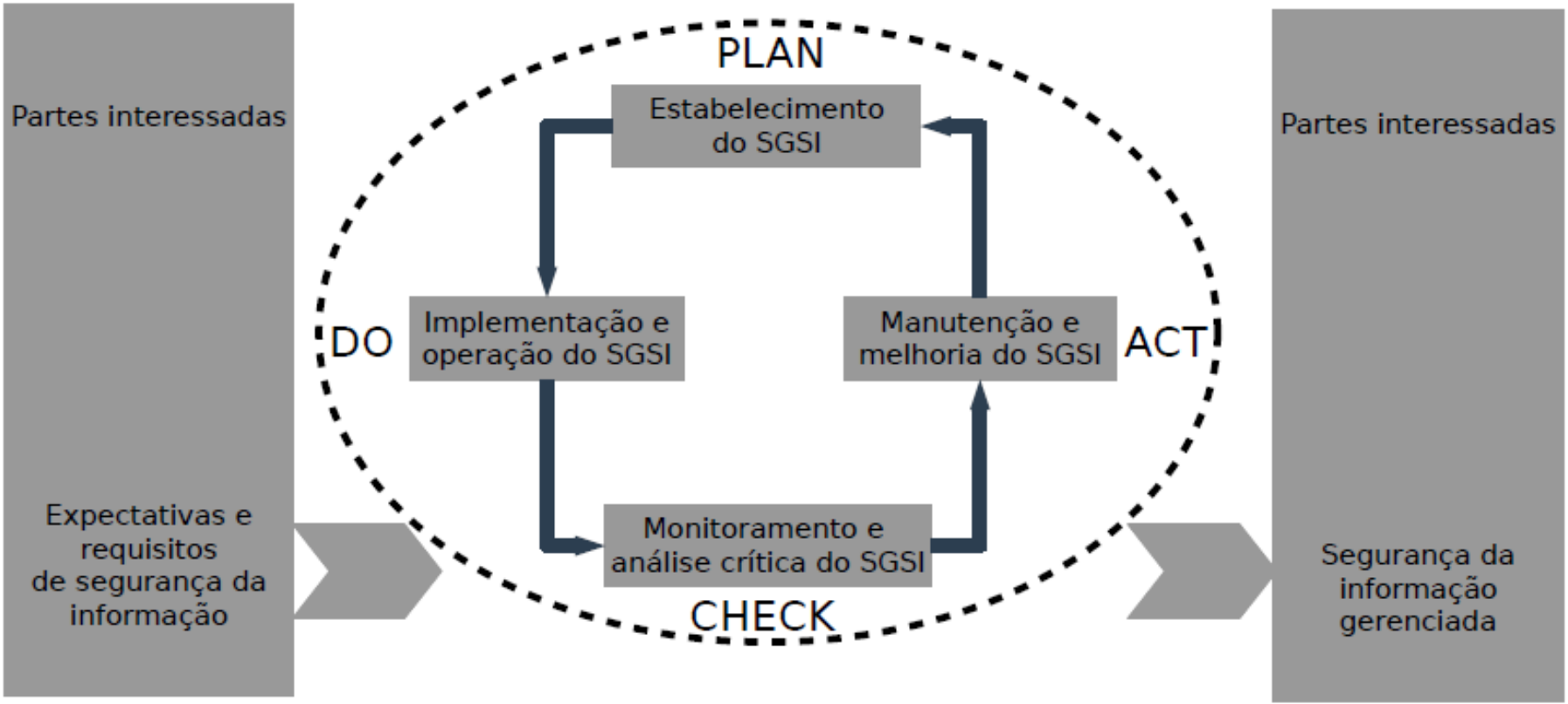
Fonte: https://www.iso.org/standard/27001

03

PDCA

O ciclo PDCA é o método de solução de problemas que visa a melhoria contínua dos resultados:





Modelo PDCA aplicado aos processos do SGSI Fonte: ABNT-NBRISOIEC27001-2006

Quais as mudanças?

ISO/IEC 27001:2013

- O número de seções aumentou.
- Criptografia ganhou uma seção própria (10)
- Outro item que ganhou uma seção própria foi Relacionamento com Fornecedor (15)
- Vários controles considerados muito específicos ou desatualizados foram excluídos

Quais as mudanças?

ISO/IEC 27001:2022

- Foi reduzido o número de controles de 114 para 93. Esses controles foram reorganizados em quatro seções principais: Organizacional, Pessoas, Físico e Técnico. Nenhum controle foi removido. Muitos foram fundidos para simplificar a estrutura.
- Algumas cláusulas foram reescritas ou reordenadas para melhor alinhamento com outras normas ISO, como a ISO 9001 (estabelece requisitos para um sistema de gestão da qualidade) e ISO 14001 (estabelece padrões para a gestão ambiental de empresas).

Quais as mudanças?

ISO/IEC 27001:2022

- A nova versão enfatiza a importância de entender as necessidades e expectativas das partes interessadas e adaptar o Sistema de Gestão da Segurança da Informação (SGSI) de acordo.
- A estrutura dos controles foi simplificada, facilitando a implementação prática e a gestão de riscos.
- Essas mudanças visam tornar a norma mais acessível e eficaz para as organizações que buscam implementar um SGSI robusto e adaptável às ameaças modernas.

03

Certificação

A certificação ISO/IEC 27001 é concedida pelo LRQA.

- O LRQA está entre os primeiros organismos de certificação a emitir um certificado ISO/IEC 27001 na América do Norte.
- O selo atesta a eficiência e o elevado padrão dos processos internos da empresa.
- Valido por **três anos** e, a cada novo ciclo, acontecerá um **processo de revalidação.**

Auditor Líder ISO 27001

Forma profissionais capazes de auditar um Sistema de Gerenciamento de Segurança da Informação (SGSI) e coordenar uma equipe em conformidade com a Norma ISO 27001.

- Política de segurança.
- Governança da segurança da informação.
- Gestão de ativos.
- Segurança de recursos humanos.
- Segurança física e ambiental.
- Comunicação e gestão de operações.
- Controles de acesso.
- Sistemas de aquisição de informação, desenvolvimento e manutenção.
- Gestão de riscos.
- Gestão de continuidade de negócios.
- Conformidade do negócio.

ISFS (Information Security Foundation) baseada na ISO 27002

- Ministrada pela EXIN, é indicada àqueles que pretendem iniciar sua carreira na área de Segurança da Informação.
- São mostrados os conceitos básicos de Segurança da Informação contribuindo para o entendimento de quais informações são vulneráveis e quais medidas são necessárias para protegê-las.
- Informação e Segurança – 10%
- Ameaças e riscos – 30%
- Abordagem e organização – 10%
- Medidas – 40%
- Legislação e regulamentação – 10%

03

Revisão

Revisão

1. Cite 2 dos 8 princípios da Segurança da Informação.
2. Qual é o ciclo de vida da informação?
3. Como são classificados os ativos da informação quanto a confidencialidade e integridade?
4. Defina Segurança da Informação.
5. Porque é importante garantir a segurança da informação?
6. O que são normas técnicas?
7. Como funciona e para que serve o PDCA.
8. Por que tantos clientes em potencial estão dando ênfase a ISO 27001?

Referências Bibliográficas

- LYRA, Maurício Rocha. Segurança e auditoria em sistemas de informação. Rio de Janeiro: Ciência Moderna, 2008.
- SÊMOLA, Marcos. Gestão da segurança da informação: uma visão executiva. 1.ed. Rio de Janeiro: Campus, 2003
- Notas de aula: CSI303 – Segurança e Auditoria de Sistemas, da Prof. Janniele Aparecida Soares Araujo (2023/1)