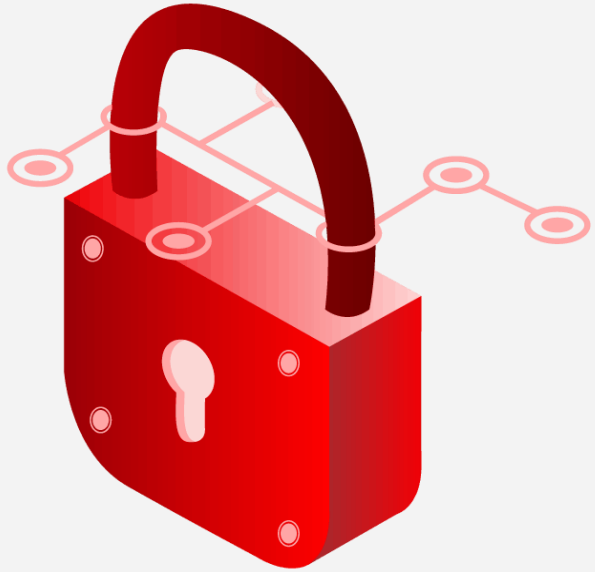
Modelo de Governança em Segurança da Informação

Baseado no *Framework CIS Controls V8*

Fernanda Mara Cruz
Luís Paulo Toniette França
Orientador: Prof Me Eduardo Alves Moraes

Introdução

- Necessidade crítica na era digital;
- Constante evolução da tecnologia;
- Aumento das ameaças cibernéticas;
- Desafios na proteção de dados e ativos.



Justificativa

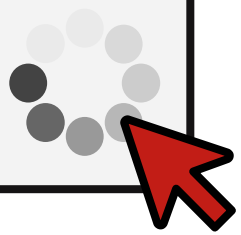
➔ A justificativa para este estudo está na necessidade de proporcionar uma visão de como implementar efetivamente o CIS Controls V8, aos profissionais de TI, considerando sua relevância na mitigação de ameaças cibernéticas e na melhoria da postura de segurança das organizações.

Objetivo Geral

➔ Propor um modelo de aplicação dos controles do CIS Controls V8, alinhada com as práticas de governança em segurança da informação, voltado para profissionais de TI.

Objetivos Específicos

- ➔ Compreender a estrutura do CIS Controls V8 e sua aplicabilidade no cenário atual de ameaças cibernéticas;
- ➔ Analisar pontos relevantes da governança em segurança da informação para a gestão efetiva da segurança da informação;
- ➔ Desenvolver um modelo simplificado e prático para a implementação do CIS Controls V8, levando em conta o contexto de governança em segurança da informação por equipes de TI em ambientes organizacionais;
- ➔ Demonstrar a importância da manutenção regular dos controles para garantir a eficácia contínua e a conformidade com as diretrizes propostas.



Metodologia

- ➔ Revisão bibliográfica;
- ➔ Documentação oficial;
- ➔ Artigos científicos;
- ➔ Dissertações e teses.

Fatec Ourinhos

Governança em Segurança da Informação

Aspectos Essenciais

- Lideranças, estruturas e processos;
- Cultura de segurança;
- Gerenciamento eficaz de incidentes;

Aspectos Essenciais

- ➔ Modelo Organizacional;
- ➔ Responsabilidade Compartilhada;
- ➔ Redução de custos operacionais.

Framework CIS Controls V8

- 18 controles com 153 salvaguardas;
- Ações para defesa e proteção cibernética, com foco na prevenção e mitigação de ataques;
- Permitem uma abordagem escalável conforme as necessidades e recursos da organização;

Fonte: https://www.cisecurity.org/insights/white-papers/cis-critical-security-controls-v8-poster

- Alinhado com padrões reconhecidos globalmente, como o NIST CSF e a ISO/IEC 27001;
- Demonstra conformidade com diversas diretrizes de segurança;
- Cumprimento de regulamentações e comunicação à postura de segurança organizacional.

Grupos de Implementação

O que são ?

- Três Níveis de Implementação;
- Estrutura Modular;
- Alinhamento de Necessidades Organizacionais.

IG1 - Controles Básicos

- ➔ Conjunto Mínimo de 56 Salvaguardas;
- ➔ Controles de Higienização Cibernética;
- ➔ Configurações seguras para hardware e software;
- ➔ Ênfase na Segurança Fundamentada.

IG2 - Controles Fundacionais

- ➔ Enfoque Técnico;
- ➔ 74 Salvaguardas Moderadas;
- ➔ Defesa contra Malware;
- ➔ Controle e Gerenciamento.

IG3 - Controles Organizacionais

- ➔ 23 salvaguardas estratégicas;
- ➔ Formação e Conscientização;
- ➔ Relacionamento com Terceiros.

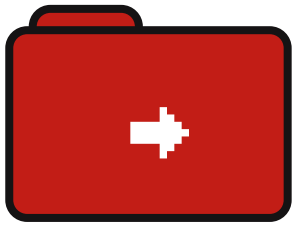
Etapas de implementação

Reconhecimento da Liderança

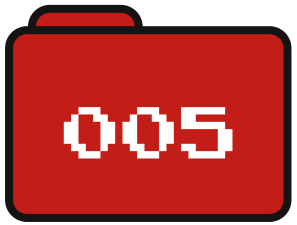
Formação da Equipe de Implementação

Avaliação do Ambiente Atual

Mapeamento e Priorização dos Controles



Etapas de implementação



Desenvolvimento do Plano de Implementação

Execução do Plano de Implementação

Verificação e Validação

Revisão e Melhoria Contínua

Resultados

- ➔ Exploração de Melhores Práticas;
- ➔ Desenvolvimento do Modelo;
- ➔ Operacionalização Eficiente;
- ➔ Adaptação e Manutenção Contínua;
- ➔ Contribuição para a Resiliência Cibernética.

Conclusão

- Construção de um modelo de governança adaptável e prático baseado nos controles do framework CIS Controls V8;

- Destacaram a viabilidade e a eficácia do modelo, enfatizando sua aplicabilidade em diversas organizações.

Fatec Ourinhos

Centro Paula Souza

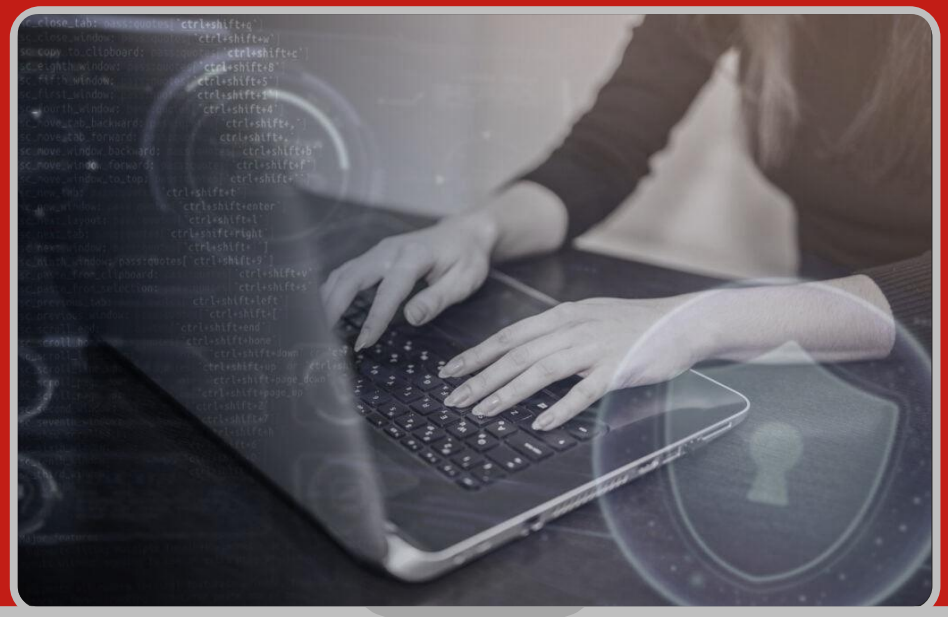
Trabalhos futuros incluem:

-Validação Empírica;

-Personalização Contextual;

-Integração de Tecnologia;

-Avaliação Contínua da Eficácia.



Referências

CENTER FOR INTERNET SECURITY. CIS Controls V8. 2021.

Disponível em: https://www.cisecurity.org/controls/cis-controls-list/. Acesso em: Março de 2023.

BARROS, A.

Desafios da segurança da informação no Brasil. Revista Brasileira de Segurança da Informação, 2(1), 1-10, 2019.

COSTA, E.

Implementação de controles de segurança da informação: uma abordagem pragmática. Revista Brasileira de Gestão e Inovação, 4(2), 1-20, 2017.

SANTARCANGELO, V.

An Overview of the NIST Special Publication 800-53, Revision 5 Security and Privacy Controls for Information Systems and Organizations. Journal of Information Security, 12, 85-98, 2021.

TIPTON, H.; NOZAKI,M.

Information Security Management Handbook (6thed.). CRC Press, 2012

OBRIGADO!