Tema 06: O Padrão Ouro da Segurança

Idealizado por Prentys Assis

Membros: Edmilson Araújo Castro Filho e Igor Santos Castro

Por que existem normas de segurança?

Normas são regras e boas práticas reconhecidas globalmente.

- Proteger dados contra perdas e vazamentos
- Reduzir riscos cibernéticos
- Garantir conformidade com leis (ex: GDPR)
- Criar confiança com clientes e parceiros

O que é a ISO/IEC 27002?

- **Não é uma norma de certificação.**
- É um manual prático com 93 controles de segurança.
- Responde à pergunta: “Como implementar segurança da informação?”
- Complementa diretamente a ISO/IEC 27001.

ISO 27001 vs ISO 27002 – Qual a diferença?

ISSO/EIC 27001	ISSO/EIC 27002
Define oque fazer	Explica como fazer
Sistema de Gestão (SGSI)	Catálogo de controles práticos
Certificável	Não certificável

Nova estrutura da ISO/IEC 27002:2022

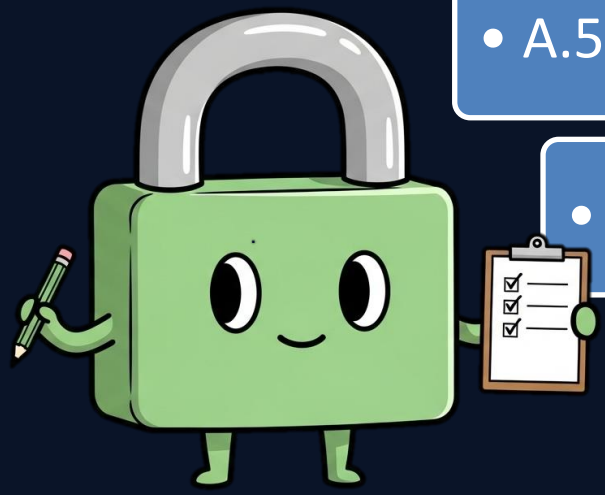
Antes (2013):
14 capítulos e 114 controles

Agora (2022):
- Organizacionais (37)
- Pessoas (8)
- Físicos (14)
- Tecnológicos (34)

Tema 1 – Controles Organizacionais

Exemplos:

- A.5.1 – Gestão de ativos
- A.5.2 – Gestão de riscos
- A.5.8 – Segurança em projetos de TI
- A.5.30 – Continuidade de negócios

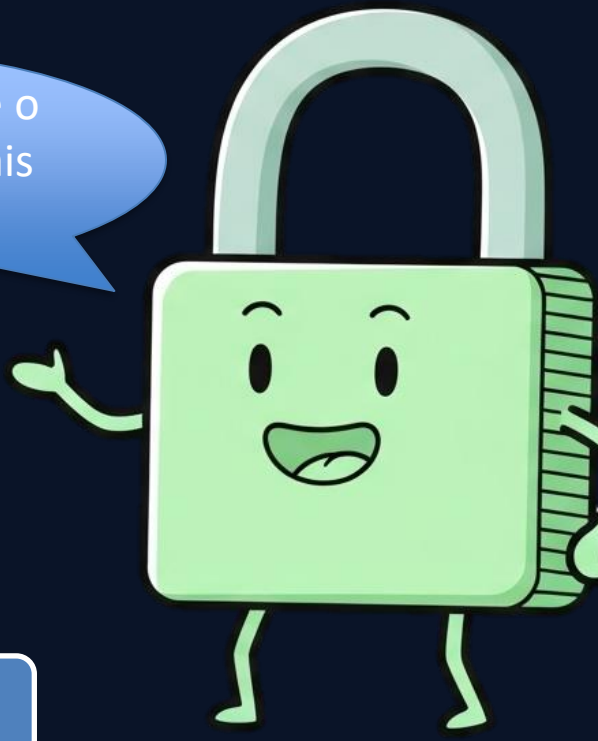


Tema 2 – Controles de Pessoas

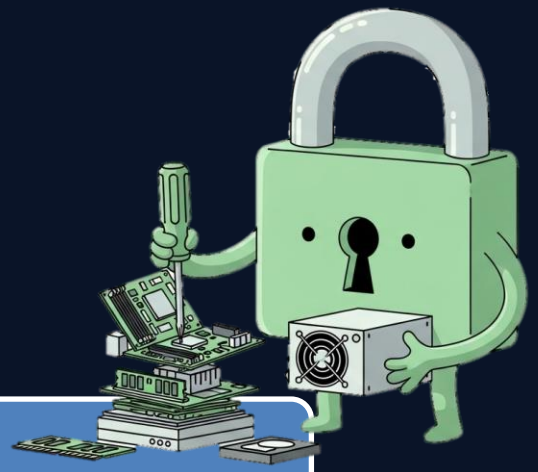
Exemplos:

- A.6.1 – Triagem de funcionários
- A.6.2 – Acordos de segurança
- A.6.3 – Treinamento e conscientização

O fator humano é o elo mais fraco ou mais forte.



Tema 3 – Controles Físicos



Exemplos:

- A.7.2 – Controles de acesso físico
- A.7.4 – Monitoramento de segurança (câmeras)
- A.7.11 – Utilitários de suporte (energia, ar).

Tema 4 – Controles Tecnológicos

Exemplos:

- A.8.2 – Gestão de identidade e acesso
- A.8.5 – Criptografia e autenticação segura
- A.8.13 – Backup
- A.8.28 – Codificação segura.

Exemplo prático – Controle de Acesso

A.8.3 – Restrição do acesso à informação (RBAC)

A.8.5 – Autenticação multifator (MFA) e senhas fortes.

Exemplo prático – Segurança Física

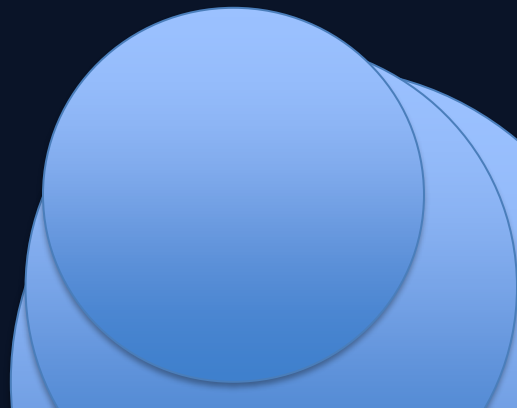
A.7.2: PORTAS COM CRACHÁ/BIOMETRIA

A.7.4: CÂMERAS DE MONITORAMENTO

A.7.12: PROTEÇÃO CONTRA INTERFERÊNCIA ELETROMAGNÉTICA.

Exemplo prático – Gestão de Ativos

A.5.1: Todo ativo tem proprietário, classificação e nível de proteção definido.



Benefícios reais da ISO/IEC 27002

Evita multas (GDPR), reduz custos com incidentes, fortalece confiança e facilita certificação ISO 27001.

Conclusão – Segurança é um ciclo, não um checklist

ISO/IEC 27002 ALIMENTA O SGSI. FUNCIONA COM ANÁLISE DE VULNERABILIDADES E PENTESTS.

NÃO É 'FAZER E ESQUECER' → É PDCA: PLANEJAR – EXECUTAR – AUDITAR – AGIR.

Chegamos ao fim da apresentação!

Conteúdo Completo