UNI
METRO
CAMP

wyden

Introdução à Segurança da Informação - ARA0064

Prof. José Luiz Alonso Silva, MsC
E-mail: jose.lsilva@unimetrocamp.edu.br

3.2 Aplicação das Normas

UNI
METRO
CAMP
wyden

Temas da Aula

- SGSI
- Implantação de SGSI
- Nível de Maturidade Segurança da Informação
- Prepare-se para próxima aula

Melhores Momentos

International Electrotechnical Commission

Organizaçoes

SGSI

BS - *British Standard*

- **BS7799-1** – É a primeira parte
- Referência para implementar "Boas Práticas" para a segurança da informação
- **BS7799-2** – Segunda parte
- Base para a criação de um sistema de Gestão da Segurança da Informação

ISO - *International Standardization Organization*

- **A ISO/IEC 17799:2000**
- Versão internacional da BS7799, homologada pela ISO

ABNT

- **A NBR ISO/IEC 17799:2001**
- Versão brasileira "tradução" da norma ISO, homologada pela ABNT

Normas

Estratégia PENTEST

UNI METRO CAMP wyden

Temas de Aprendizagem

1. PRINCÍPIOS DA SEGURANÇA E O CICLO DE VIDA DA INFORMAÇÃO
1.1 SEGURANÇA DA INFORMAÇÃO
1.2 SEGURANÇA FÍSICA, LÓGICA E CONTROLE DE ACESSO

2. AMEAÇAS E VULNERABILIDADES À SEGURANÇA DE INFORMAÇÃO
2.1 TIPOS DE AMEAÇAS E VULNERABILIDADES
2.2 ATAQUES CIBERNÉTICOS

3. NORMAS DE SEGURANÇA DA INFORMAÇÃO
3.1 FINALIDADES E BENEFÍCIOS DAS NORMAS
3.2 APLICAÇÃO DAS NORMAS

4. BOAS PRÁTICAS EM SEGURANÇA DA INFORMAÇÃO
4.1 SENHAS, TREINAMENTO E PROTEÇÃO
4.2 CONTROLE DE ACESSO, VÍRUS E BACKUPS
4.3 CRIPTOGRAFIA DE DADOS E CERTIFICADO DIGITAL

5. GESTÃO DE RISCO
5.1 PRESERVAÇÃO DA CONFIDENCIALIDADE, INTEGRIDADE E DISPONILIDADE (CID)
5.2 ETAPAS DA GESTÃO DE RISCOS

6. GESTÃO DE CONTINUIDADE DO NEGÓCIO (ATIVIDADE PRÁTICA SUPERVISIONADA)
6.1 PLANO DE CONTINUIDADE DE NEGÓCIOS (PCN) 6.2 ETAPAS DO PCN
6.3 PGCN E BIBLIOTECA ITIL

Objetivo da Aula

- Identificar as aplicações das normas ISO/IEC 27001 e 27002

Imagem: Autor wordart

UNI METRO CAMP wyden

Situação Problema

- Qual a importância de um Sistema de Gestão de Segurança da Informação?

- Conhecer ambiente tecnológico
- Necessidades do negócio
- Manutenção Negócio
- Padronizar Processos organizacionais

Imagem: Desconhecido

Situação Problema Complementar

- Itens segurança da informação indispensáveis
  - Atualização de softwares e ferramentas segurança
  - Backups automatizados
  - Entender novas tecnologias e nível de segurança, ex. IA, Cloud ...
  - Gestão de Riscos
  - Políticas de Segurança da Informação
  - Senhas fortes e criptografadas
  - Treinamento/Capacitação

Conceito SGSI

- Sistema de Gestão de Segurança da Informação - SGSI

Conjunto de regras e normas adotado por uma empresa, com o objetivo de garantir a segurança de suas informações quanto a controles, perdas, roubos, alterações e consultas indevidas

Conceito SGSI

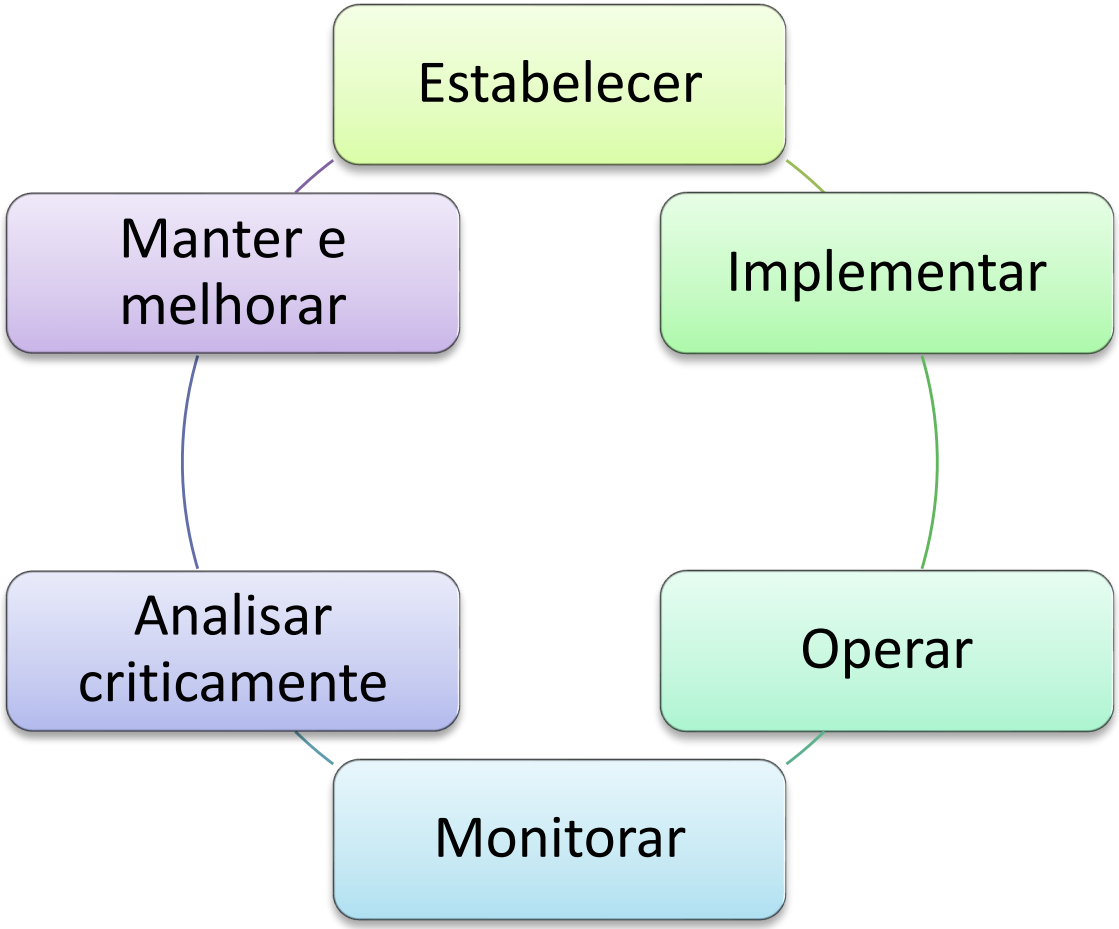
Abordagem organizacional para que os dados e informações de uma empresa estejam protegidos

- Utiliza estratégias, controles, políticas e planos

Ferramentas, técnicas, instrumentos para monitorar, analisar, implementar e estabelecer a Segurança da Informação

SGSI – Visão ISO 27001

- A norma ABNT NBR ISO/IEC 27001 foi elaborada para prover um modelo para SGSI



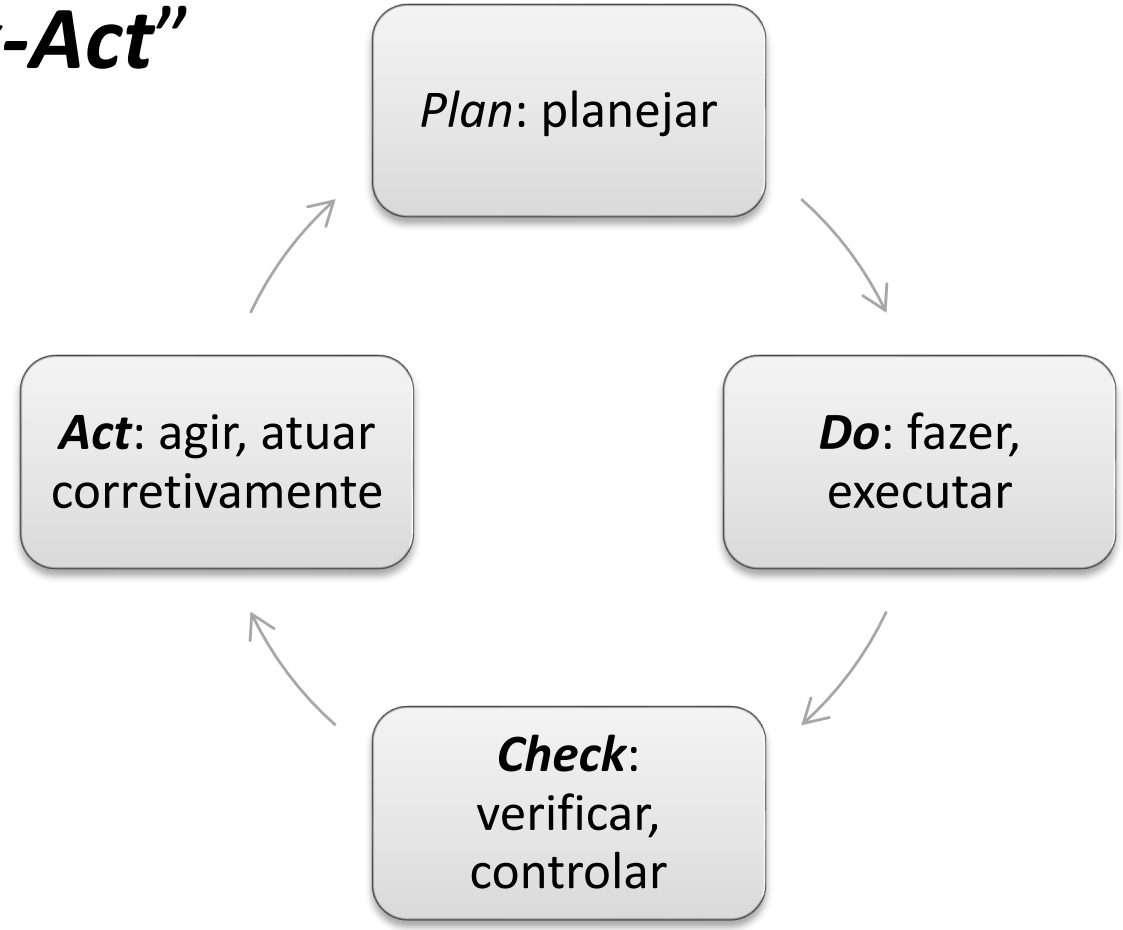
UNI METRO CAMP wyden

SGSI – Visão ISO 27001

UNI METRO CAMP wyden

SGSI – Visão ISO 27001

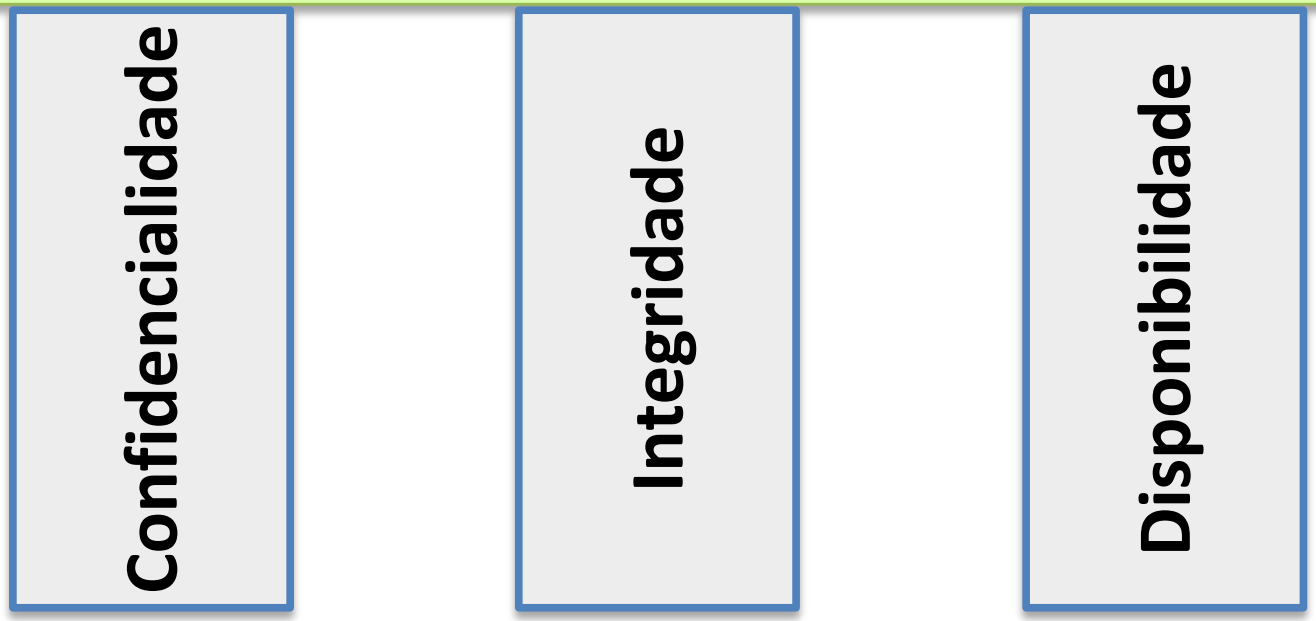
- Norma adota o modelo PDCA - "***Plan-Do-Check-Act***"



UNI METRO CAMP wyden

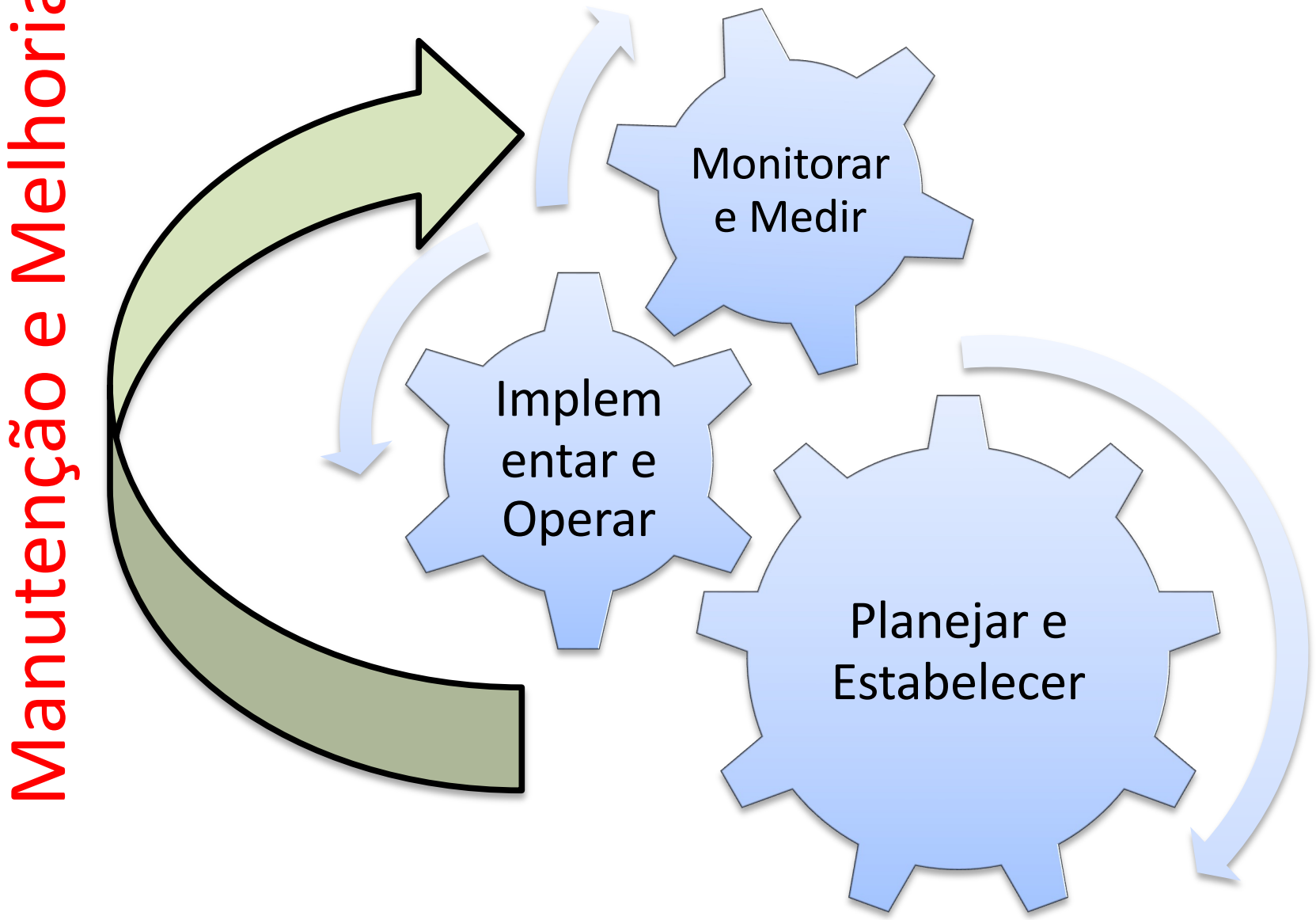
Implantação SGSI

Implantar e manter processo para administrar de maneira eficiente a proteção de dados



UNI METRO CAMP wyden

Implementação SGSI



UNI METRO CAMP wyden

Fatores Críticos Sucesso Implantar SGSI

- Conhecer o objetivo e metas a serem alcançados
- Coletar os resultados em tempo hábil
- Apresentar resultados válidos e confiáveis
- Criar métricas que permitam monitorar o SGSI
- Desenvolver metas desafiadoras

Implantação SGSI

Planejar e Estabelecer

- Definir as etapas
- Identificar os Ativos
- Responsável pelas Etapas

Objetivo

- Responsáveis pela segurança
- Processos que devem ser protegidos
- Políticas de segurança
- Recursos necessários (Implantação, manutenção e Operação

Implantação SGSI

Implementar e Operar

- Colocar em prática o planejado

Objetivo

- Avaliar riscos e tratamento
- Aplicar controles de segurança (físico e lógico)
- Planos Gerenciamento de Segurança
- Capacitar
- Definir métricas
- Documentar

Implantação SGSI

Monitorar e Medir

- Acompanhar o funcionamento
- Avaliar métricas e realizar ações

Objetivo

- Auditorias de Segurança
- Revisão de indicadores e métricas
- Avaliar vulnerabilidades
- Testes de penetração
- Análise de *gap*
- Níveis de Maturidade
- Revisão do SGSI

Implantação SGSI

Manutenção e Melhorias

- Avaliar, Planejar e implementar melhorias

Objetivo

- Tratamento de Não Conformidades
- Ações Corretivas para melhoria contínua

Níveis de Maturidade

- Medidos pelo cumprimento das metas específicas e genéricas associadas a cada conjunto predefinido de áreas para Segurança da Informação

Processos confiáveis e melhoria contínua em segurança da informação

Níveis de Maturidade

0 (Zero) Inexistente	• Não existe o controle e planejamento
1 Inicial	• Ad-hoc, informal, sem confiabilidade • Não possuem práticas definidas
2 Básico	• Alguns *templates* ou *checklist*
3 Definido	• Formalmente documentado • Processos são consistentes
4 Gerenciado	• Formal • Medido e controlado
5 Otimizado	• Maduro • Melhoria contínua

Duvidas, considerações ...

Imagem Ícones MS-Power Point

UNI METRO CAMP wyden

Referência Bibliográfica

- BAARS, Hans. **Fundamentos de Segurança da Informação: com base na ISO 27001 e na ISO 27002?** Rio de Janeiro ? RJ ? Editora Brasport, 2018. Capítulo 4. Disponível em: https://plataforma.bvirtual.com.br/Acervo/Publicacao/160044
- GALVÃO, Michele da Costa, Agnaldo Aragon. **Fundamentos em Segurança da Informação?** Rio de Janeiro ? RJ: Editora Pearson, 2015. Capítulo 4. Disponível em: https://plataforma.bvirtual.com.br/Acervo/Publicacao/26525

Referência

- Rodrigo Valinor. **ISO 27001: o que é e como implementa**. Disponível em: <remessaonline.com.br/blog/iso-27001/>. Acesso em 01/04/24
- Dejan Kosutic. **Como definir o escopo do SGSI.** Disponível em: <https://advisera.com/27001academy/pt-br/knowledgebase/como-definir-o-escopo-do-sgsi/>. Acesso em 01/04/24

UNI METRO CAMP wyden

Referências

- IBM. **Adapte-se e responda a riscos com um plano de continuidade de negócios (BCP)**. Disponível em: < https://www.ibm.com/br-pt/services/business-continuity/plan>. Acesso em 01/04/24

Referências

- TND Brasil. **O que é a maturidade da segurança da informação?** Disponível em: <https://tndbrasil.com.br/o-que-e-a-maturidade-da-seguranca-da-informacao/>. Acesso em 01/04/24
- Poder Judiciário de SC. **Sistema de Gestão de Segurança da Informação**. Disponível em: <https://www.tjsc.jus.br/web/tecnologia-da-informacao/si/sistema-de-gestao-de-seguranca-da-informacao-sgsi>. Acesso em 01/04/24

Atividade Aula 7

Estudo de Caso Empresa Versatile Credit – VC

Implantação SGSI

Elaborar um roteiro para implantação SGSI, e apresentar em sala de aula

Equipe até 6 pessoas

Responder no Forms

https://forms.office.com/r/TE5u0TZ70m

Estudo de Caso Empresa Versatile Credit – VC – Aula 7

A Empresa VC, uma empresa de médio porte no setor de serviços financeiros, percebeu a necessidade de aprimorar sua segurança da informação para proteger seus dados e garantir a confiança de seus clientes.

A VC opera em um ambiente altamente competitivo e depende fortemente da tecnologia da informação para oferecer seus produtos e serviços. Com o aumento das ameaças cibernéticas e regulamentações mais rígidas, a VC reconheceu a necessidade urgente de fortalecer suas práticas de segurança da informação

Para implementar um SGSI com o objetivo de fortalecer suas práticas de segurança da informação e cumprir as regulamentações do setor. Durante o processo, enfrentou diversos desafios, como a resistência à mudança por parte dos funcionários e a falta de conscientização sobre segurança da informação em todos os níveis da organização.

Estudo de Caso Empresa Versatile Credit – VC – Aula 7

1. Considerando os desafios apresentados, como a empresa pode lidar a resistência à mudança por parte dos funcionários?
2. Qual a importância do comprometimento da alta direção com o projeto de SGSI?
3. Como medir o sucesso da implementação do SGSI? Cite 1 exemplo.
4. Roteiro para Implantação SGSI

Para Próxima Aula
Assista aos vídeos

- O que é BRUTE FORCE?: https://www.youtube.com/watch?v=esuyHyBkDXY&t=11s
- Criando
- um *script* para *Brute Force* em FTP: https://www.youtube.com/watch?v= LmGrvOM3ZE

UNI METRO CAMP

wyden