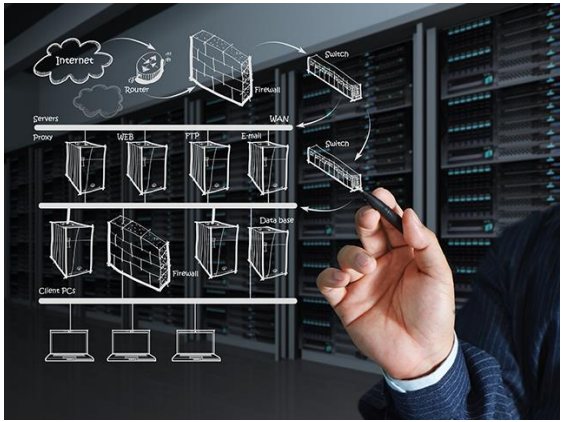
ISSO-17799

Faber Henrique

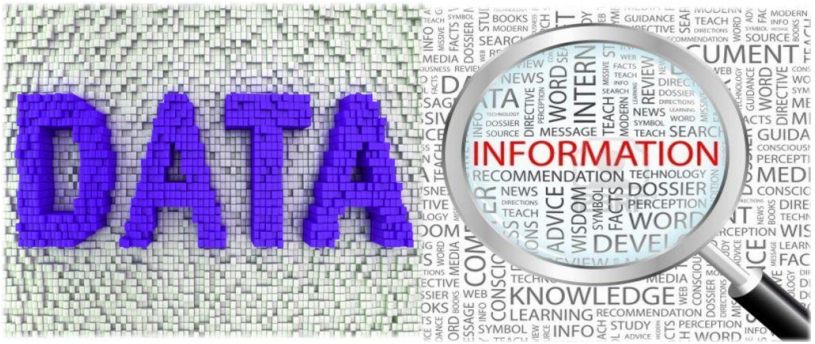
PUC MINAS

SISTEMAS DE INFORMAÇÃO

ISSO 17799

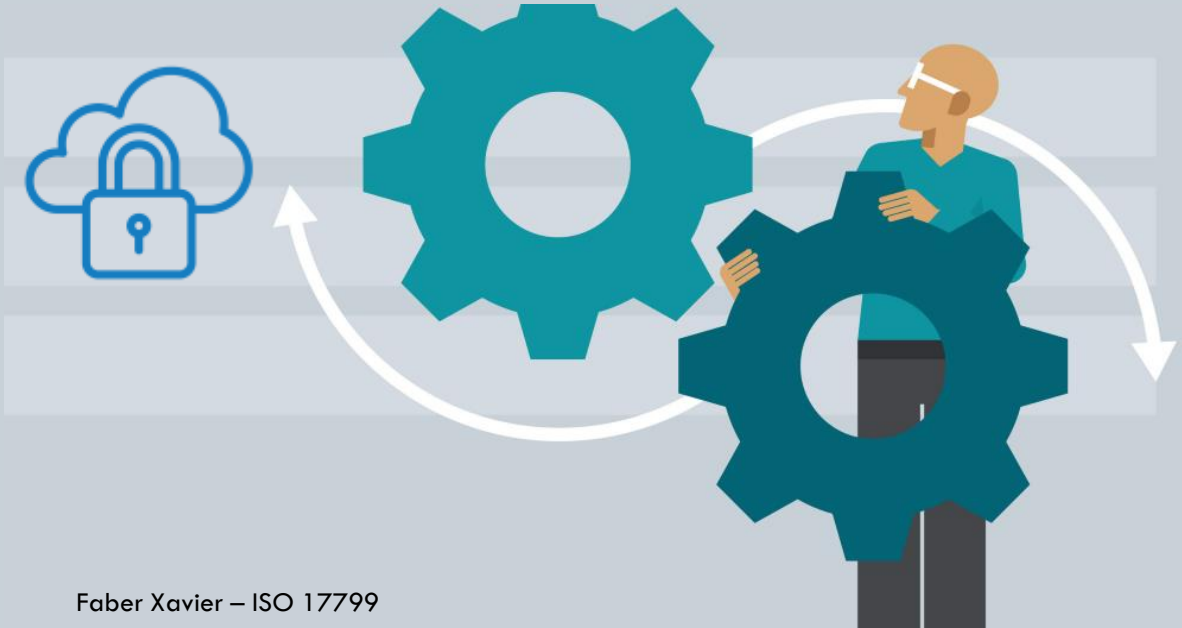


Infra-estrutura da segurança da informação



Gestão de ativos

- Definição de mecanismos que irão promover a segurança da Informação
  - Controle
    - Metas
    - Políticas
    - Planos
    - Tarefas
    - ***Coordenação***



- Coordenar atividades por representantes de diferentes partes da organização
  - Garantir conformidade das atividades
  - Identificar não conformidades
  - Aprovar metodologias
  - Identificar ameaças
  - Avaliar adequação dos controles
  - Promover treinamento
  - **Definir responsabilidades**

- Todas as atividades devem estar devidamente definidas pelo gestor e apoiado pela diretoria
  - As informações e os **processos** devem estar identificados e claramente definidos
  - **As atividades de cada gestor ou responsável seja detalhada e documentada**
  - Os níveis de autorização devem estar claramente definidos e documentados

- Processos de autorização de recursos
  - Novos recursos tenham autorização adequada
  - Hardware e software são compatíveis com outros recursos do sistema
  - Definição de mecanismos de controle para eventuais ameaças da inclusão de ***novos recursos***

- Acordos de confidencialidade
  - Definição da informação à ser protegida
  - Tempo de duração do acordo
  - Ações para encerramento do acordo
  - Responsabilidades
  - Proprietário da informação, segredos comerciais
  - Uso permitido
  - Termos para informar destruição da informação

PUC Minas

PUC Minas

- Identificação dos riscos ao acesso à informação as partes externas
- Controle de acesso
  - Equipamentos
  - Banco de dados
  - Rede
  - Acesso externo
- Verificar valor e sensibilidade da informação envolvida
- Partes externas não devem ter conhecimento dos controles

PUC Minas

Gestão de ativos

- Alcançar e manter a proteção adequada dos ativos da organização.
  - Todos os ativos sejam inventariados e tenham um proprietário responsável.
  - Identificar proprietários
    - Responsável pela manutenção dos controles

PUC Minas

- Todos os ativos devem estar devidamente identificados. Tipos de ativos:
  - Ativos de informação
  - Ativos de software
  - Ativos Físicos
  - Serviços
  - Pessoas
  - Intangíveis (Reputação e imagem da organização)

- Todas os ativos devem ter um **proprietário**
  - Garantir que as informações e os ativos associados com os recursos de processamento da informação estejam adequadamente classificados;
  - Definir e periodicamente analisar criticamente as classificações e restrições ao acesso, levando em conta as políticas de controle de acesso, aplicáveis.

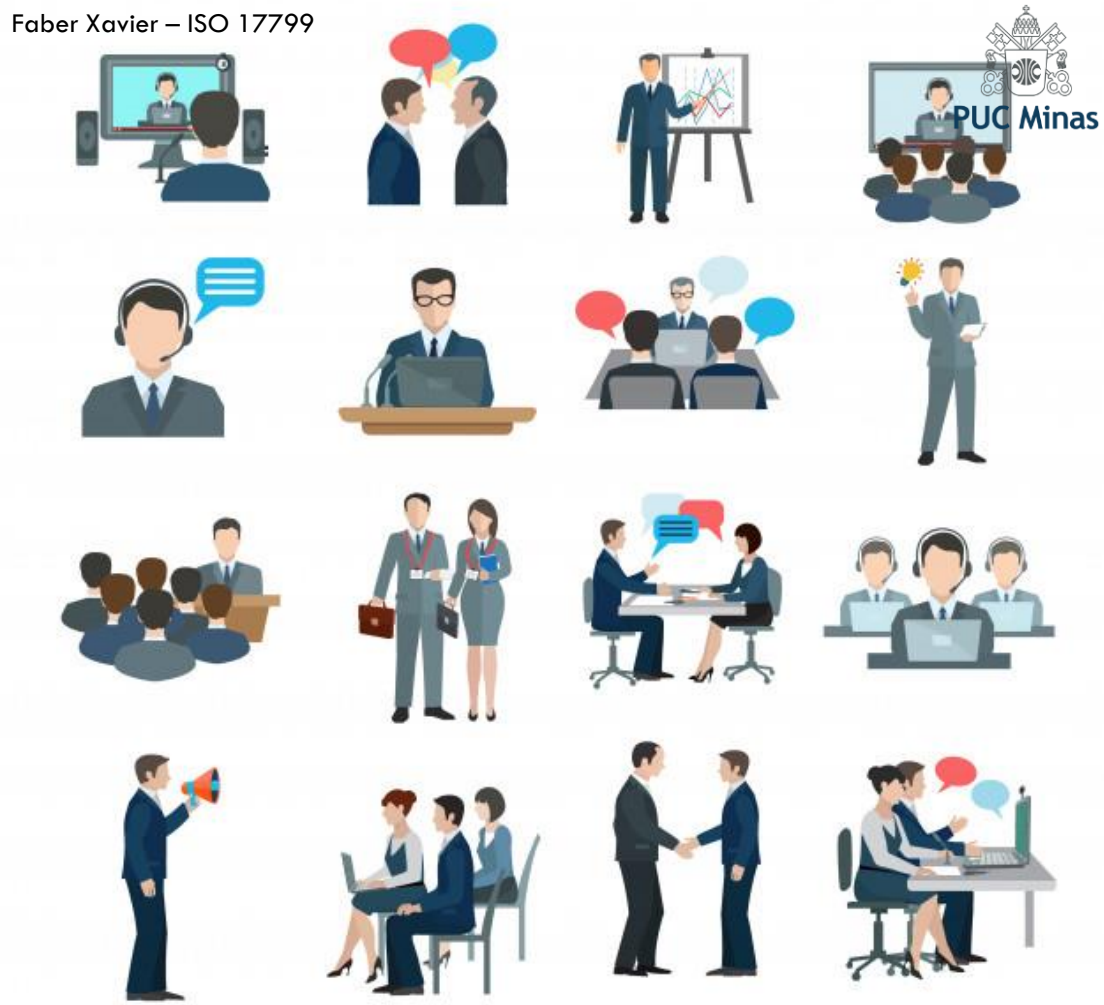
PUC Minas

- Uso aceitável dos ativos
  - Regras de uso da Internet
  - Diretrizes de uso de dispositivos móveis
  - Diretrizes de uso de dispositivos móveis fora da organização

PUC Minas

- **Classificação da informação**

- Segurança em RH
  - Garantir que todos os funcionários, fornecedores e terceiros entendam suas responsabilidades e ciente da sua colaboração para reduzir eventuais falhas.



PUC Minas

- Papeis e responsabilidade
- Seleção
- Termos e condições de contratação
- Processo de contratação
  - Evidenciar as politicas e preocupações da empresa
- Conscientização
- Treinamento
- Processo Disciplinar
- Encerramento de atividades
  - Devolução de ativos
  - Retirada de direitos

PUC Minas

Segurança Física e do Ambiente

- Perímetro de segurança
- Controles de entrada
- Segurança em escritórios, salas e instalações
  - Instalações-chave devem ser localizadas de maneira a evitar o acesso do público

"os edifícios sejam discretos e dêem a menor indicação possível da sua finalidade, sem letreiros evidentes, fora ou dentro do edifício, que identifiquem a presença de atividades de processamento de informações, quando for aplicável;"

PUC Minas

- Proteção contra ameaças externas e do meio ambiente
  - Equipamentos para contingência
  - Armazenamento materiais fora do alcance de materiais perigosos
  - Equipamentos contra Incêndio
- Pessoal tenha ciência das áreas de segurança somente se necessário
- Controle de acesso ao público, carregamento, entregas

- Acessos de carregamento e entregas devem ser restrita à pessoal autorizado
- Áreas restritas sejam trancadas quando não utilizadas

- Segurança do cabeamento
- Manutenção do equipamento

OBRIGADO.