

Vamos falar de...

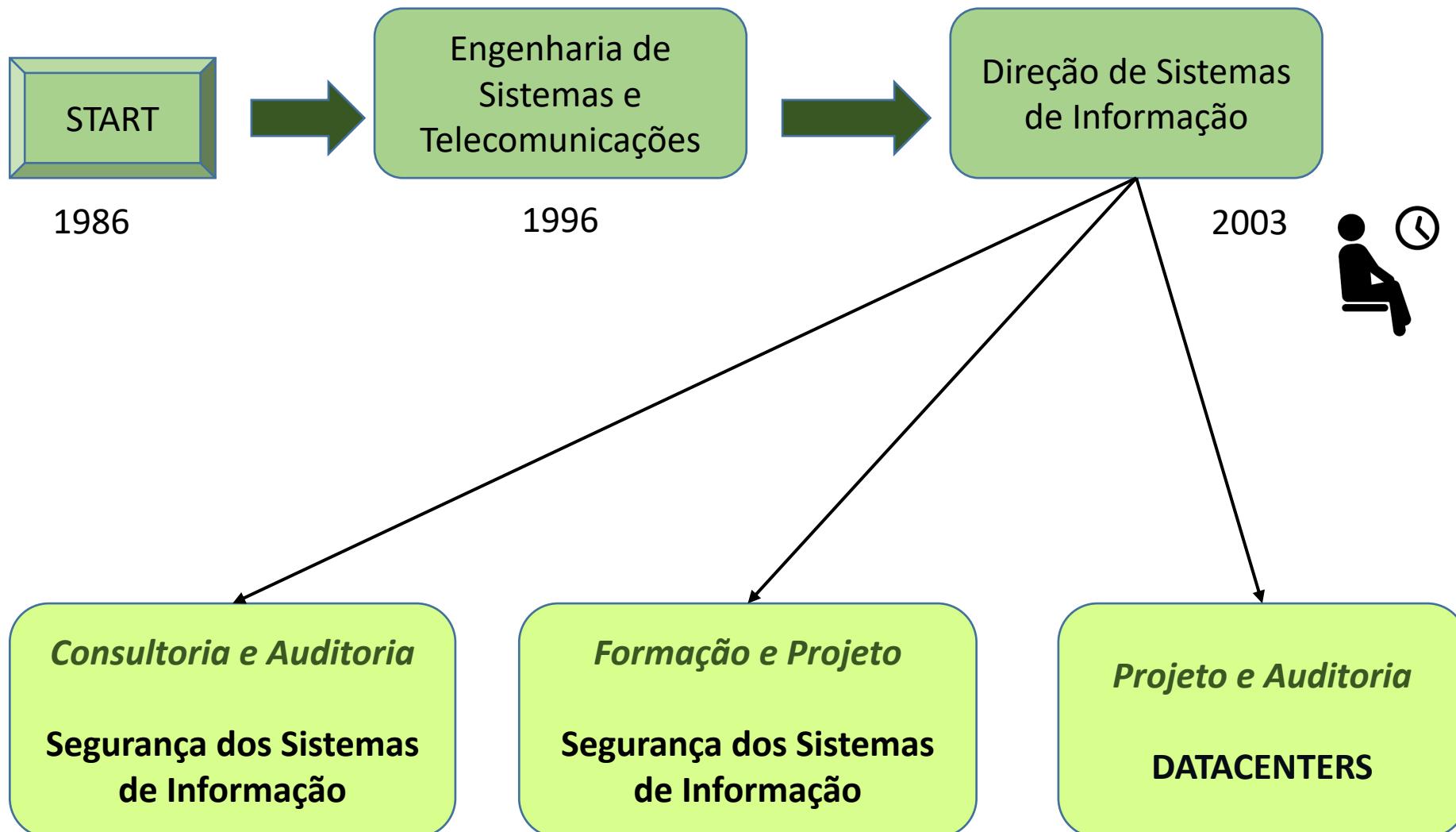


**CONSULTORIA
ASSESSORIA
AUDITORIA**



SEGURTI

Perfil do Orador



Perfil do Orador:

Acreditações pessoais:

BSI ISO/IEC 27001 - Implementação

BSI ISO/IEC 27001 - Auditor Coordenador

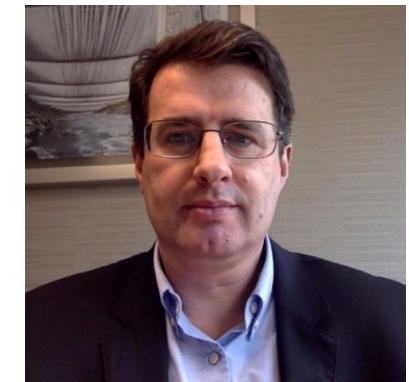
PECB ISO/IEC 22301 - Auditor Coordenador

PECB ISO/IEC 20000 - Auditor Coordenador

PECB ISO/IEC 27032 - Auditor Coordenador

Gabinete Nacional de Segurança - Auditor credenciado de PECP

APCER - Auditor qualificado ISO 27001, 20000, 22301 e eIDAS



Consultor - Auditor

Segurança da Informação

Gestão do Risco

Gestão da Continuidade de Negócio

Gestão de Níveis de Serviço

Gestão da Privacidade

Arquiteturas de Segurança, Alta Disponibilidade e Resiliência



Datacenters:

Plano estratégico e de negócio

“e-Procurement” de soluções técnicas

Desenho de projeto e auditoria de implementação

Planeamento de gestão operacional e exploração

Gestão do processo de certificação

Organizações Acreditadoras:



<https://pecb.com/>

When Recognition Matters



<https://www.bsigroup.com/>

British Standards Institution



<https://www.isaca.org/>

Information Systems Audit and Control Association



<https://www.apcergroup.com>

Associação Portuguesa Certificação



<https://www.gns.gov.pt/>



Sistemas e Tecnologias da Informação:

Lei de Murphy no seu meio natural

CYBER SECURITY

Software Development

MURPH

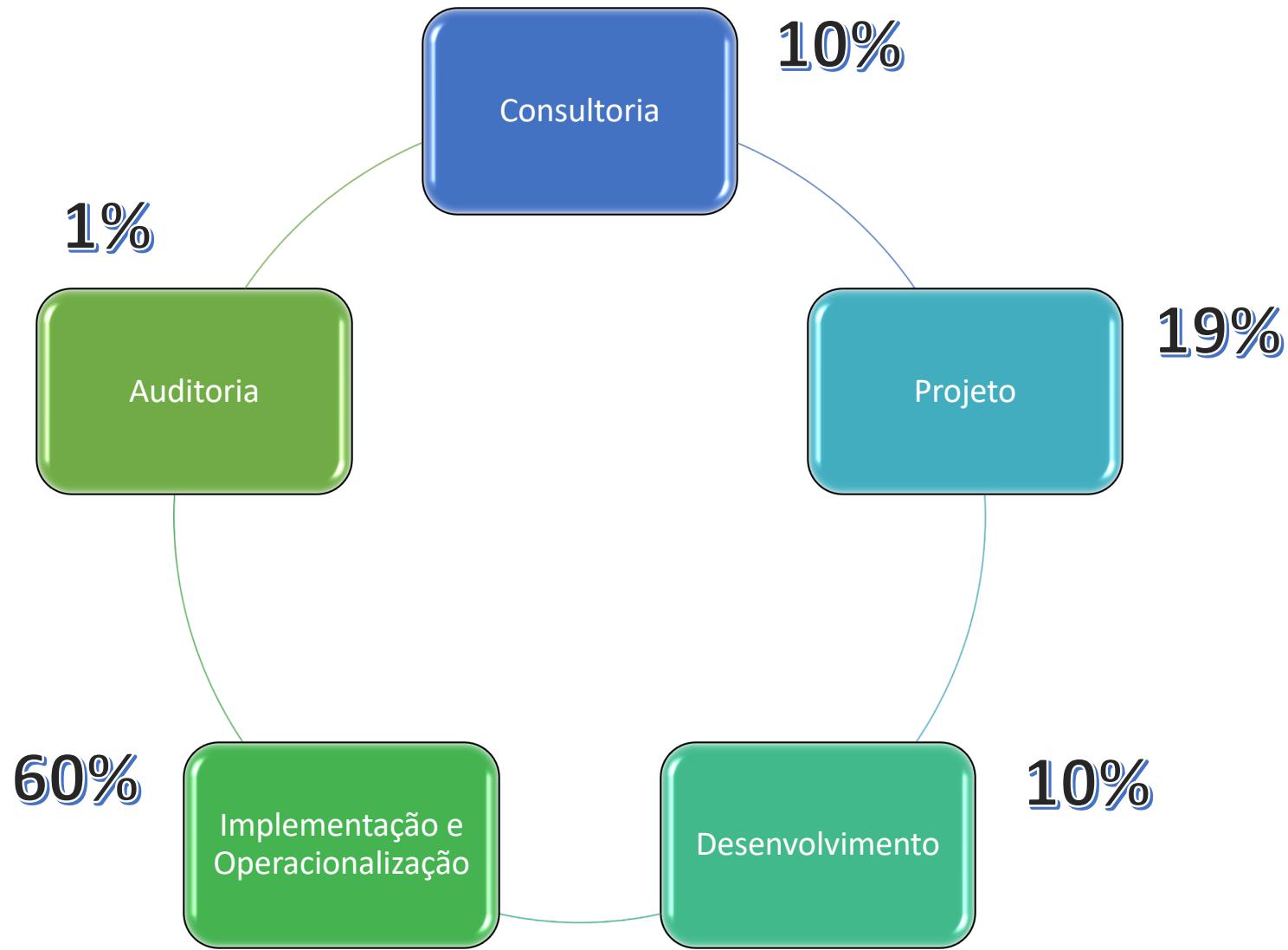


Network Security

Data Protection

“Qualquer coisa que possa ocorrer mal,
ocorrerá mal, no pior momento possível”

Ciclo de vida dos profissionais de Segurança da Informação



Consultoria de Segurança da Informação



- Realizar estudos
 - Emitir recomendações
 - Emitir pareceres
 - Apontar soluções
 - Realizar planos de projeto
 - Gerir execução de projetos
-
- Empresa consultora
 - Empresa tecnológica
 - Profissional Independente
 - Cuidado com a EXPERIÊNCIA !!!!

consultadaria

con.sul.ta.do.ri.a • kôsułtadu'ria

nome feminino

1. lugar onde se dão ou fazem consultas
2. aconselhamento especializado sobre determinada matéria
3. actividade de consultor; função desempenhada por quem é pago para dar pareceres sobre matérias em que é especialista
4. local de trabalho de um ou mais consultores

Assessoria de Segurança da Informação



- Procura de soluções
 - Emitir pareceres de decisão
 - Apoia a realização dos projetos
 - Supervisiona a execução
 - Analisar os resultados e eficácia
 - Propõe soluções
 - Apoio a gestão de topo
-
- Contratado para colaborador (interno ou externo)
 - Requer EXPERIÊNCIA !!!!

Auditoria de Segurança da Informação



- Utilizar normas para referência
 - Executa metodologia comprovada
 - Recolha de evidências
 - Análise e constatação
 - Não conformidades
 - Recomendações de melhoria
 - Relatórios de auditoria
 - Certificação de empresas
-
- Auditor interno
 - Auditor externo
 - Requer MUITA EXPERIÊNCIA !!!!

auditoria

au.di.to.ri.a • awditiu'rie

nome feminino

1. cargo de auditor
2. tribunal ou repartição onde se exercem as funções de auditor
3. ECONOMIA fiscalização da contabilidade e da gestão de uma empresa ou de um organismo
4. ECONOMIA diagnóstico que visa analisar a gestão e a situação financeira de uma empresa ou organismo

Tipos de Auditorias



- **Auditória de 1^a parte**

Auditória do tipo interna, mesmo sendo realizada por colaboradores externos

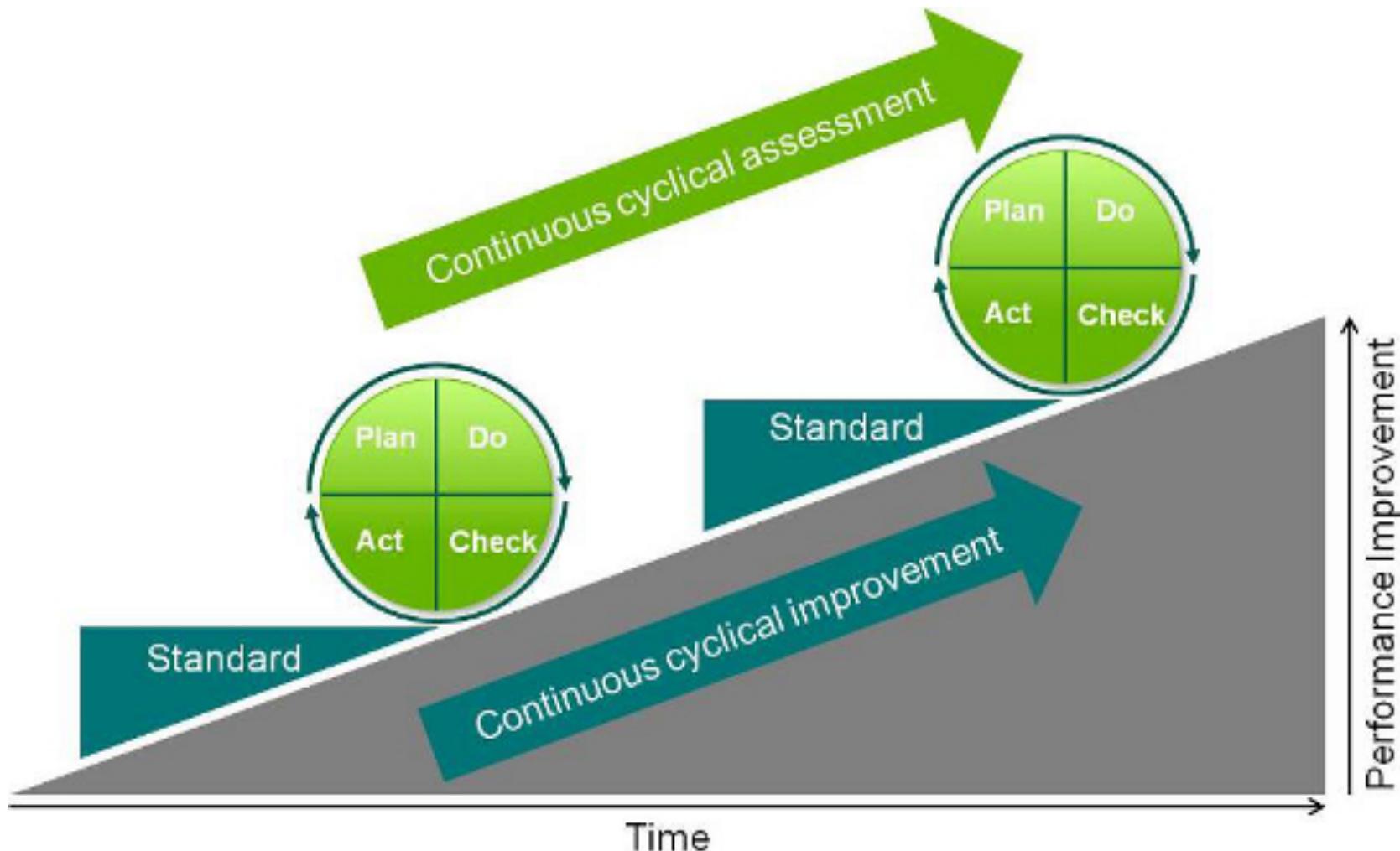
- **Auditória de 2^a parte**

Auditória a um fornecedor ou prestador de serviços

- **Auditória de 3^a parte**

Auditória realizada por uma entidade de certificação independente

Ciclo de vida da auditoria



Ciclo de vida da auditoria – Normas associadas

Cycle Phase	PKI Management tasks	ISO applicable standards
PLAN	<ul style="list-style-type: none">• Policies and requirements• Management Processes• Procedures• Risk Management• Incident Management• Business Continuity Management• Project Plan	<ul style="list-style-type: none">• ISO 9001 - Quality Management• ISO 31000 - Risk Management• ISO 20000 - Service Incidents and Request process• ISO 22301 - Business Continuity Management• ISO 27001 - Information Security• ISO 27017 – Cloud Security• ISO 27032 - Cybersecurity Controls• ISO 27033 – Network Security• ISO 27024 – Applications Security• ISO 27035 – Incident Management• ISO 27040 – Storage Security
DO	<ul style="list-style-type: none">• Implementation of Security Project Plan• Implementation of Security controls	<ul style="list-style-type: none">• ISO 27002 - Information Security Practices
ACT	<ul style="list-style-type: none">• Audit• Non Conformity Treatment Plan• Improvements Plan• Top Management review	<ul style="list-style-type: none">• ISO 19011 - Guidelines for auditing management systems
CHECK	<ul style="list-style-type: none">• Monitoring operations and efficiency• Alarms and Events management• Incident Management process and procedures	<ul style="list-style-type: none">• ISO 27037 – Guidelines for Security Digital Evidence• ISO 27044 – SIEM (Security Incident and event Management)

E agora ????



Posso ser útil?

Mensagens finais



- Normas internacionais são “boas práticas”
- Consultor é uma evolução natural do profissional
- Auditor é uma decisão de carreira
- São necessários MUITOS AUDITORES
- Existem oportunidades para auditores
ISO 27001 – RGPD - Cibersegurança
- Estágios profissionais estão disponíveis!
- Carreira internacional aliciante

Muito grato pela atenção dispensada.