



Curso: 02.12.04 – INISO27001

Interpretação da Norma ISO 27001 - GSI

Máximo de Participantes: 09/12

Horas de Formação: 12/14

Data:

Horário:

Formador: João Carlos Martins Leitão Marques

CURRÍCULO SUCINTO DO FORMADOR:

Formação académica:

- Mestrado em Gestão de Sistemas de Informação pelo Instituto Superior das Ciências do Trabalho e da Empresa (ISCTE).
- Pós-graduação em Sistemas de Informação pelo Instituto Superior das Ciências do Trabalho e da Empresa (ISCTE).
- Pós-graduação em Estudos da Paz e da Guerra nas Novas Relações Internacionais pela Universidade Autónoma de Lisboa (UAL).
- Licenciatura em Informática de Gestão pela Universidade Moderna de Lisboa (UML).

Certificações:

- Project Management Professional (PMP) (PMP n.º 2004420) pelo Project Management Institute (PMI) em 11JAN17 e válido até 11JAN29 (membro n.º 4424218).
- Scrum Master Certified (SMC) (Certificate ID 1022964) pelo SCRUMstudy em 08ABR24 e válido até 08ABR27.
- Scrum Fundamentals Certified (SFC) (Certificate ID 1025440) pelo SCRUMstudy em 09ABR24 e válido *ad eternum*.

Experiência profissional:

- Coordenador do Gabinete de Gestão de Projectos (*Project Management Office* (PMO)) da Empresa de Gestão Partilhada de Recursos na Administração Pública, EPE (GeRAP). Esta actividade, de coordenação dos Directores de Programas/Gestores de Projectos, visa a normalização de procedimentos e a disponibilização da informação de acompanhamento e controlo dos programas/projectos para o Conselho de Administração. Foi o responsável pela criação do referido gabinete e do respectivo desenho e implementação do processo de Acompanhamento e Controlo de projectos na empresa.
- Militar da Força Aérea Portuguesa com o posto de Major, tendo sido na sua carreira responsável na área da manutenção de material electrotécnico de aeronaves, formador na área da electrotecnia e gestor da formação responsável pelo programa de Formação de Apoio à Gestão e Modernização Administrativa da FAP.
- Formador/Consultor Sénior (CAP n.º EDF 5349/98 DCR, E-FOR 188/2020) nas áreas de conhecimento Gestão de Projectos (PMBOK), Gestão Ágil de Projectos (Scrum), Gestão por Objectivos, Gestão da Mudança (numa perspectiva estruturada), Empreendedorismo, Inovação e Criatividade no Desenvolvimento de Produtos/Serviços, CANVAS (Modelos de Negócio / Gestão de Projectos), Análise de Negócios (Business Analysis (BA)), Gestão de Processos de Negócio (Business Process Management (BPM)), Modelo e Notação de Processos de Negócio (BPMN), Elaboração de Planos de Negócio e Elaboração de Planos de Continuidade de Negócios (PCN/BCM).
- Como docente Universitário (Professor Assistente Convocado), exerceu docência durante nove anos lectivos nas áreas científicas da Informática e Gestão, na Universidade Moderna de Lisboa.

APRESENTAÇÃO:

- Este curso tem como objectivo dotar os participantes de conhecimentos acerca da Norma ISO 27001.
- A Segurança da Informação está relacionada com a protecção de todos os activos de informação e infra-estruturas de suporte (Tecnológico, humanos e financeiros), no sentido de preservar e rentabilizar o valor que possuem para a Organização.

OBJECTIVOS:

No final deste curso os participantes saberão:

- Saber interpretar os requisitos estipulados na norma ISO 27001.
- Saber analisar e avaliar um Sistema de Gestão da Segurança da Informação em conformidade com os requisitos da ISO 27001.

CONTEÚDO PROGRAMÁTICO:

- Introdução/Conceitos Gerais.
- Conceitos Básicos de Ciclos de Vida e Evolução dos Sistemas de Informação.
- O Sistema de Gestão da Segurança da Informação.
- A Norma ISO 27001.
- Interpretação da Norma ISO 27001.
- Revisão/Reflexão.

DOCUMENTAÇÃO DE APOIO:

- Manual de enquadramento do formando.
- Colectânea de slides do formador.
- Documentos de trabalho.
- Enunciados com exercícios.

DESTINATÁRIOS:

- Empresários.
- Dirigentes.
- Quadros Superiores.

CONTEÚDO PROGRAMÁTICO (em detalhe):

Introdução/Conceitos Gerais:

- O Que É a Informação?
- O Que É um “Bem” na Organização?
- O Que É a Segurança da Informação?
- O Que São Vulnerabilidades e Ameaças?
- ISO 27001 - Contexto de Actuação
- Informação, Bem, Segurança da Informação, Vulnerabilidades e Ameaças.

Conceitos Básicos de Ciclos de Vida e Evolução dos Sistemas de Informação:

- Governança Corporativa - Governança IT.
- Registo, Dado, Informação, Conhecimento, Sabedoria.
- Definição de Sistema.
- Características dum Sistema.
- Definição de Sistema de Informação.
- Características dum Sistema de Informação.
- Recursos de um Sistema de Informação.
- Componentes da Infra-estrutura de Tecnologias de Informação.
- Sistema Informático vs Sistema Informação.
- Ciclo de Vida dum Sistema de Informação.
- Relações entre Ciclos de Vida.
- História da Função dos Sistemas de Informação nas Organizações.
- Evolução nos Conceitos Relacionados aos Sistemas de Informação.
- O Papel dos Sistemas de Informação numa Organização.
- Diagrama de Actuação de Elementos em Conjunto.
- Sistemas de Informação na Estratégia Organizacional.
- Arquitectura de Sistemas de Informação.
- Sistema de Informação - Enquadramento Geral.

O Sistema de Gestão da Segurança da Informação:

- Sistema de Gestão da Segurança da Informação (SGSI) - *Design*.
- SGSI - Elementos da Segurança.
- SGSI - Funções.
- O Que É um SGSI?
- SGSI - Que Modelo de Gestão É Utilizado?
- O Ciclo PDCA e o SGSI.
- Estrutura da ISO 27001 (Contexto PDCA).
- O Contexto da Gestão de Riscos.
- Gestão dos Riscos Corporativos.
- Gestão de Riscos e Outras Áreas de Gestão.
- Visão Geral dos Processos de Gestão de Riscos.
- Relacionamento entre Princípios, Estruturas e Processo.
- Cenários de Risco - Desenvolvimento.
- Cenários de Risco - Componentes.
- Gestão de Riscos - Causas e Efeitos.
- Análise e Avaliação de Riscos em Sistemas de Informação.
- Plano de Gestão do Risco - 5 Níveis Classificativos.
- Enquadramento dos Sistemas de Informação na Organização.
- Como Definir e Gerir o SGSI.
- SGSI - Enquadramento Geral.

A Norma ISO 27001:

- Sistemas de Gestão de Segurança da Informação (Normas).
- British Standard 7799 - O Que É?
- A Norma ISO 27001:
 - O Que É?
 - Para Que Serve?
 - Em Que Consiste?
 - Requisitos.
 - Controlos (Anexo A).
 - Estrutura Global.
 - Benefícios Para Quem Adopta.
- Plano de Implementação a ISO 27001.
- Processo de Certificação (*roadmap*).

Interpretação da Norma ISO 27001:

- Família ISO 27000 - Sistema de Gestão da Segurança da Informação.
- Resumo das Principais Mudanças na ISO 27001:2013 vs 27001:2022.
- 0. Introdução.
- 1. Âmbito.
- 2. Referências Normativas.
- 3. Termos e Definições.
- 4. Contexto da Organização.

- 5. Liderança.
- 6. Planeamento.
- 7. Suporte/Apoio.
- 8. Operação.
- 9. Avaliação da Performance.
- 10. Melhoria.
- Anexo A.

Revisão/Reflexão.