| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Designação | Responsável de Cibersegurança (C-Academy) | | | | | | | Área Científica | - | | | | | | |
| Classificação | Unidade/Projeto Extracurricular | | | | | | | Escola | Escola Superior de Tecnologia e de Gestão de Bragança | | | | | | |
| Ano Letivo | 2023/2024 | Ano Curricular | 1 | | | | | Nível | - | | | Créditos ECTS | 2.0 | | |
| Tipo | Modular | Semestre | - | | | | | Código | 9929-949-1004-00-23 | | | | | | |
| Horas totais de trabalho | 54 | Horas de Contacto | T | - | TP | 35 | PL | - | TC | - | S | - | E | - | OT | - | O | - |

T - Ensino Teórico; TP - Teórico Prático; PL - Prático e Laboratorial; TC - Trabalho de Campo; S - Seminário; E - Estágio; OT - Orientação Tutórica; O - Outra

Nome(s) do(s) docente(s): Tiago Miguel Ferreira Guimaraes Pedrosa

## Resultados da aprendizagem e competências

No fim da unidade curricular o aluno deve ser capaz de:
1. Identificar e implementar as principais normas e regulamentos relacionados com a cibersegurança nas organizações
2. Aplicar frameworks como CIS, COBIT, ISO/IEC e NIST para estabelecer e manter práticas robustas de cibersegurança
3. Realizar análises de risco e desenvolver planos de gestão de risco utilizando ferramentas especializadas como o Monarc
4. Desenvolver e implementar planos de resposta a incidentes para minimizar o impacto e assegurar a recuperação rápida de processos e serviços
5. Criar políticas de segurança da informação (PSI) e planos de segurança abrangentes, alinhados com as necessidades da organização e as melhores práticas de cibersegurança

## Pré-requisitos

Antes da unidade curricular o aluno deve ser capaz de:
1. Possuir formação ou experiência profissional em área relacionada com as TIC
2. Conhecimentos do funcionamento de sistemas operativos e de redes de comunicação
3. Conhecimentos técnicos ao nível da segurança dos sistemas de informação

## Conteúdo da unidade curricular

Legislação aplicável à Cibersegurança; Frameworks; Análise de risco; gestão de ativos; gestão de incidentes; Regime Jurídico da Segurança do Ciberespaço (RJSC); políticas de segurança; certificação e selos de maturidade.

## Conteúdo da unidade curricular (versão detalhada)

1. Legislação aplicável à Cibersegurança
2. Frameworks CIS, COBIT, ISO/IEC, NIST
3. Análise e gestão de risco
4. Ferramenta Monarc
5. Medidas técnicas e organizativas
6. Auditoria e monitorização da Cibersegurança
7. Inventário de ativos
8. Gestão de incidentes de cibersegurança
9. Política de Segurança da Informação (PSI)
10. Plano de Segurança
11. Relatório Anual de Cibersegurança
12. Plano para conformidade com o RJSC
13. Esquema de certificação QNRCS
14. Selo de maturidade digital da cibersegurança

## Bibliografia recomendada


1. Diversas leis, regulamentos e directivas aplicáveis na área
2. “Handbook” de suporte às sessões de sensibilização do Roadshow Nacional 2022 (CNCS)
3. UK National Cyber Security Center, https://www.ncsc.gov.uk/, 2024
4. RGPD para cidadãos atentos | INA-Direção-Geral da Qualificação dos Trabalhadores em Funções Públicas


## Métodos de ensino e de aprendizagem

O método expositivo será utilizado para apresentar conteúdos e exemplos. Para tópicos tecnológicos e ferramentas, adotaremos o método demonstrativo. O método ativo envolverá a criação de pequenos exercícios práticos. A resolução autónoma destes exercícios, com acompanhamento docente, permitirá ao formando pesquisar, refletir e aplicar os conteúdos aprendidos.

## Alternativas de avaliação

- Teste Final (100%) - (Ordinário, Trabalhador) (Final, Especial)

## Língua em que é ministrada

Português

## Validação Eletrónica

| Tiago Miguel Ferreira Guimaraes Pedrosa | José Luís Padrão Exposto | José Carlos Rufino Amaro |
|---|---|---|
| 01-07-2024 | 01-07-2024 | 04-07-2024 |