

---

**Ano Letivo** 2023-24

---

**Unidade Curricular** CIBERGOVERNANÇA, GESTÃO DE RISCO, CONFORMIDADE E NORMAS

---

**Cursos** CIBERSEGURANÇA

---

**Unidade Orgânica** Faculdade de Ciências e Tecnologia

---

**Código da Unidade Curricular** 19381016

---

**Área Científica** CIÊNCIAS INFORMÁTICAS

---

**Sigla**

---

**Código CNAEF (3 dígitos)** 481

---

**Contributo para os Objetivos de Desenvolvimento Sustentável - ODS (Indicar até 3 objetivos)** 4,9,11

---

**Línguas de Aprendizagem** Português/Inglês

---

**Modalidade de ensino**

B-Learning

---

**Docente Responsável**

JÚLIO CARLOS BOTEQUILHA FERNANDES

---

| DOCENTE                           | TIPO DE AULA | TURMAS  | TOTAL HORAS DE CONTACTO (*) |
|-----------------------------------|--------------|---------|-----------------------------|
| JÚLIO CARLOS BOTEQUILHA FERNANDES | PL; T        | T1; PL1 | 24.5T; 24.5PL               |

\* Para turmas lecionadas conjuntamente, apenas é contabilizada a carga horária de uma delas.

---

| ANO | PERÍODO DE FUNCIONAMENTO* | HORAS DE CONTACTO | HORAS TOTAIS DE TRABALHO | ECTS |
|-----|---------------------------|-------------------|--------------------------|------|
| 1º  | S2                        | 24.5T; 24.5PL     | 156                      | 6    |

\* A-Anual;S-Semestral;Q-Quadrimestral;T-Trimestral

---

**Precedências**

Sem precedências

---

**Conhecimentos Prévios recomendados**

NA

---

**Objetivos de aprendizagem (conhecimentos, aptidões e competências)**

A Unidade Curricular de CiberGovernança, Gestão de Risco, Conformidade e Normas pretende dotar o estudante de conhecimentos que lhe permita desenhar um Sistema de Gestão de Segurança da Informação através da aplicação duma framework de governança e análise de risco da segurança numa organização. Pretende também o desenvolvimento de competências na implementação de políticas de segurança e a realização de análises de risco da segurança da informação.

---

### **Conteúdos programáticos**

- Conceito de Governança de CiberSegurança numa Organização;
- Políticas, Normas e Procedimentos de Segurança da Informação;
- Legislação de CiberSegurança;
- Gestão e Análise de Risco da Segurança da Informação;
- Plano Resposta a Incidentes;
- Plano de Continuidade de Negócio;
- Certificação, Normas de Segurança e Auditorias;
- Privacidade de Dados.

---

### **Metodologias de ensino (avaliação incluída)**

A presente unidade curricular combina diversos métodos de ensino:

- Exposição dos conteúdos programáticos, através das aulas teóricas
- Práticas de planificação e implementação de frameworks de governança de cibersegurança, como trabalho autónomo;
- Apresentações orais dos trabalhos de grupo
- Atendimento individual ou em grupo para esclarecimento de dúvidas
- Apoio às atividades e esclarecimento sobre funcionamento da unidade curricular.

A avaliação é contínua, com exame final e inclui:

- Teste individual para a avaliação de conhecimentos (50%)
- Trabalho de grupo com apresentação oral/discussão (50%)
- Os estudantes que obtiverem uma classificação final igual ou superior a 9,5 valores em cada elemento de avaliação estão dispensados do exame final.

---

#### **Bibliografia principal**

- Publicação - NIST Special Publication 800-100 - Information Security Handbook: A Guide for Managers -  
[https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800\\_100.pdf](https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800_100.pdf)
- Publicação - 2nd Draft NISTIR 8286A - Identifying and Estimating Cybersecurity Risk for Enterprise Risk Management (ERM)
- Publicação - ENISA - National Cyber Security Strategy Good Practice Guide  
- <https://www.enisa.europa.eu/publications/ncss-good-practice-guide>
- Publicação - CNCS - Estratégia Nacional de Segurança do Ciberespaço 2019-2023 -  
<https://www.cncs.gov.pt/pt/estrategia-nacional/#documentos>

---

Academic Year 2023-24

---

Course unit

---

Courses CIBERSECURITY

---

Faculty / School FACULTY OF SCIENCES AND TECHNOLOGY

---

Main Scientific Area

---

Acronym

---

CNAEF code (3 digits) 481

---

Contribution to Sustainable Development Goals - SGD  
(Designate up to 3 objectives) 4, 9, 11

---

Language of instruction English

---

Teaching/Learning modality B-Learning

**Coordinating teacher** JÚLIO CARLOS BOTEQUILHA FERNANDES

| Teaching staff                    | Type  | Classes | Hours (*)     |
|-----------------------------------|-------|---------|---------------|
| JÚLIO CARLOS BOTEQUILHA FERNANDES | PL; T | T1; PL1 | 24.5T; 24.5PL |

\* For classes taught jointly, it is only accounted the workload of one.

| Contact hours | T    | TP | PL   | TC | S | E | OT | O | Total |
|---------------|------|----|------|----|---|---|----|---|-------|
|               | 24.5 | 0  | 24.5 | 0  | 0 | 0 | 0  | 0 | 156   |

T - Theoretical; TP - Theoretical and practical ; PL - Practical and laboratorial; TC - Field Work; S - Seminar; E - Training; OT - Tutorial; O - Other

#### Pre-requisites

no pre-requisites

#### Prior knowledge and skills

NA

#### The students intended learning outcomes (knowledge, skills and competences)

The curricular unit (CU) of Cyber governance, Risk Management, Standards and Compliance intends to provide students with knowledge that enables them to design an Information Security Management System by means of the implementing in an organization a risk management and governance framework. Building skills in designing information security policies and risk analysis are also desired goals of this CU.

#### Syllabus

- The Organizational Cyber Governance Concept;
- Information Security Policies, Standards and Procedures;
- Cyber Security Legislation;
- Information Security Risk Analysis and management.
- Security Incident Response Plan;
- Business Continuity Plan;
- Certification, Audit and Security Standards;
- Data Privacy and Protection.

---

### Teaching methodologies (including evaluation)

This curricular unit combines various teaching methods:

- Program content exhibition through theoretical lectures
- Practice laboratorial lessons, with an autonomous hands on project to plan and design a cybersecurity governance framework;
- Oral group presentations on developed work project
- Individual or group attendance for out of classroom support;
- Activity support and curricular unit functioning clarification

Evaluation is continuous with a final exam, and includes:

- Individual knowledge evaluation test (50%)
- Hands on Group Project development with oral presentation (50%)

Students that achieve a final grade of 9.5 or higher in each of the evaluation components, are excused from the final exam

---

### Main Bibliography

- Publication - NIST Special Publication 800-100 - Information Security Handbook: A Guide for Managers - <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-100.pdf>
- Publication - 2nd Draft NISTIR 8286A - Identifying and Estimating Cybersecurity Risk for Enterprise Risk Management (ERM)
- Publication - ENISA - National Cyber Security Strategy Good Practice Guide
- Publication - CNCS - Estratégia Nacional de Segurança do Ciberespaço 2019-2023 - <https://www.cncs.gov.pt/pt/estrategia-nacional/#documentos>