

## EDITAL

ESCOLA SUPERIOR DE TECNOLOGIA E GESTÃO DE OLIVEIRA DO HOSPITAL (ESTGOH)

ANO LETIVO 2025/2026

### MICROCREDENCIAÇÃO EM AUTOMAÇÃO, SEGURANÇA E VIRTUALIZAÇÃO DE REDES

Nos termos do Despacho n.º 5051/2017, de 6 de junho, do Instituto Politécnico de Coimbra, faz-se saber que está aberto concurso de acesso ao curso de Microcredenciação em Automação, Segurança e Virtualização de Redes, o qual se rege pelas seguintes disposições:

#### 1 - Condições de admissão

Podem candidatar-se ao curso de Microcredenciação em Automação, Segurança e Virtualização de Redes, titulares da escolaridade obrigatória (12º ano ou equivalente).

Recomenda-se, contudo, a detenção prévia de noções de redes informáticas, endereçamento IP e configuração básica de dispositivos de comunicação.

#### 2 - Número de vagas

Sob proposta da Presidente da Escola Superior de Tecnologia e Gestão de Oliveira do Hospital (ESTGOH), ouvido o respetivo Conselho Técnico-Científico, fixa-se o seguinte número de vagas para ingresso: 27 vagas.

N.º mínimo de inscritos para funcionamento do curso: 15.

#### 3 - Critérios de seleção e de seriação dos candidatos

Os candidatos admitidos no concurso de acesso à Microcredenciação serão classificados pelo júri tendo em atenção os seguintes critérios:

- Cronológico: a seriação será realizada através da data/hora da lacragem da candidatura, sendo os candidatos colocados sucessivamente até ao número limite de vagas.

#### 4 - Normas e prazos de candidatura

4.1 - As candidaturas são efetuadas on-line, através do endereço <https://infoestudante.ipc.pt/>. Os prazos de candidatura e matrícula decorrem de acordo com o seguinte calendário:

Ação	Prazos
Apresentação da candidatura	Até 29 de janeiro de 2026
Validação das candidaturas pelos Serviços	Até 30 de janeiro de 2026
Disponibilização de lista de seriação provisória	02 de fevereiro de 2026
Reclamações	03 de fevereiro de 2026
Decisão sobre reclamações / lista de seriação definitiva	04 de fevereiro de 2026
Matrícula e inscrição de candidatos colocados	De 05 a 06 de fevereiro de 2026

As reclamações deverão ser submetidas, no prazo indicado, na plataforma de gestão académica – *Inforestudante*, através de “requerimento para reclamação no âmbito de uma candidatura”. Eventuais reclamações realizadas por outra via não serão objeto de análise.

4.2 - No processo de candidatura devem ser anexados os seguintes documentos em suporte digital, sob pena de não admissão pelo Júri:

- a) Digitalização de documento comprovativo de identificação civil (bilhete de identidade, cartão de cidadão ou passaporte com a devida autorização do próprio para utilização exclusiva no âmbito da candidatura (a não submissão deste documento implica a apresentação do original nos Serviços Académicos da ESTGOH dentro do prazo da candidatura);
- b) Digitalização do NIF (Número de Identificação Fiscal com a devida autorização do próprio para utilização exclusiva no âmbito da candidatura (a não submissão deste documento implica a apresentação do original nos Serviços Académicos da ESTGOH dentro do prazo da candidatura);
- c) Comprovativo de IBAN pessoal (a utilizar para a devolução dos montantes pagos no caso de não abertura da Microcredenciação ou para pagamento da bolsa Impulso, se aplicável);
- d) Certificado de habilitações.

4.3 - A taxa de candidatura é criada no momento da formalização da candidatura, devendo ser regularizada através da referência bancária gerada e disponibilizada na finalização do processo de candidatura.

4.4 - A não apresentação, no prazo de candidatura, dos documentos exigidos, é motivo de exclusão do concurso.

## 5. Taxas e propina

### 5.1 – Montantes

Taxa de candidatura – 25,00€
Taxa de matrícula/inscrição – 25,00€
Propina para Estudantes da ESTGOH – 125,00€ <sup>(a)</sup>
Propina para outros Estudantes – 150,00€ <sup>(a)</sup>

<sup>(a)</sup> 50% a pagar até 16 de fevereiro e os restantes 50% a pagar até 16 de março de 2026.

5.2 - O não pagamento da taxa de candidatura até ao termo do prazo de apresentação de candidaturas implica a caducidade da candidatura e inviabiliza a sua apreciação.

5.3 - O não funcionamento da Microcredenciação por decisão do órgão competente confere direito à devolução da taxa de candidatura e, se aplicável, do montante de propinas pago.

## 6. Bolsas

Os formandos que frequentem a Microcredenciação em Automação, Segurança e Virtualização de Redes podem beneficiar de uma Bolsa Impulso (apoio financeiro para comparticipação de encargos com as propinas do curso).

Número de bolsas a atribuir: 27.

Valor da bolsa: 150,00€; a bolsa será paga no final do curso, mediante aproveitamento escolar.

## 7. Conteúdos programáticos

O plano de estudos e os respetivos conteúdos programáticos constam do anexo I, tendo sido aprovados pelo Conselho Técnico-Científico da ESTGOH na reunião n.º 217, de 7 de novembro de 2025.

## 8. Júri

O júri de seleção, classificação e seriação dos candidatos é constituído pelos seguintes elementos:

- Presidente: Doutor Luís Alberto Morais Veloso
- Vogal: Doutor Gonçalo Miguel Santos Marques
- Vogal: Doutor Nuno Miguel Gil Fonseca

## 9. Funcionamento do Curso

9.1 – Local de funcionamento: ESTGOH

9.2 – O curso tem a duração de **30 horas de contacto em regime *b-learning*** e as aulas decorrerão a partir do dia **9 de fevereiro**, em horário e cronograma a definir oportunamente.

9.3 – A conclusão da Microcredenciação, com aproveitamento, confere direito à emissão de um certificado de conclusão (a requerer no *Inforestudante* mediante pagamento do emolumento aplicável).

9.4 – A avaliação em época normal decorrerá durante ou imediatamente após a lecionação da unidade curricular.

9.5 – Época de recurso e melhoria de nota: Não aplicável.

9.6 – Os métodos de avaliação da unidade curricular serão definidos na respetiva ficha de edição.

## 10. Calendário Escolar

Período letivo (incluindo avaliações na época normal): de 9 de fevereiro a 31 de março de 2026.

## 11. Creditação

Não aplicável.

## 12. Dúvidas e casos omissos

As dúvidas de interpretação e os casos omissos serão decididos pela Presidente da ESTGOH, ouvido o Coordenador do Curso.

A Vice-Presidente da Escola Superior de Tecnologia e Gestão de Oliveira do Hospital,

Paula Cristina Mendes dos Santos Coelho

(Ao abrigo da delegação de competências prevista no Despacho n.º 4634/2025, de 3 de abril, publicado no Diário da República n.º 74, 2.ª Série, de 15 de abril)

## Anexo I – Plano de estudos e conteúdos programáticos

### Plano de estudos

Unidade Curricular	Módulos	Horas de trabalho	Horas de contacto (presenciais)	ECTS
Automação, Segurança e Virtualização de Redes	1. Conceitos de Encaminhamento e OSPFv2	81	2,5 TP	3
	2. Configuração e Verificação de Encaminhamento Dinâmico		2,5 TP	
	3. Fundamentos de Segurança de Redes		2,5 TP	
	4. Controlo de Acesso e Filtragem de Tráfego		2,5 TP	
	5. Implementação de Políticas de Acesso IPv4		2,5 TP	
	6. Network Address Translation (NAT)		2,5 TP	
	7. Conectividade Empresarial, VPN e Comunicação Segura		2,5 TP	
	8. Qualidade de Serviço (QoS) e Gestão de Tráfego		2,5 TP	
	9. Gestão e Monitorização de Equipamentos e Serviços		2,5 TP	
	10. Desenho e Escalabilidade de Redes Empresariais		2,5 TP	
	11. Virtualização e Software Defined Networking (SDN)		2,5 TP	
	12. Automação de Redes e Gestão Centralizada		2,5 TP	
<b>Total</b>		<b>81h</b>	<b>30h</b>	<b>3</b>

### Conteúdos programáticos por módulos

#### Módulo 1 – Conceitos de Encaminhamento e OSPFv2

- Conceito de encaminhamento dinâmico.
- Estrutura e funcionamento de protocolos de encaminhamento.
- Funcionamento do OSPF em redes ponto-a-ponto e multiacesso.
- Tipos de pacotes e estabelecimento de vizinhança.

#### Módulo 2 – Configuração e Verificação de Encaminhamento Dinâmico

- Configuração de redes com OSPFv2.
- Propagação de rotas e definição de identificadores.
- Verificação de tabelas de encaminhamento e resolução de falhas.

#### Módulo 3 – Fundamentos de Segurança de Redes

- Conceitos de ameaças, vulnerabilidades e ataques.
- Vetores de ataque e boas práticas de mitigação.
- Tipos de malware e riscos de segurança em redes.
- Princípios de autenticação, integridade e confidencialidade.

#### **Módulo 4 – Controlo de Acesso e Filtragem de Tráfego**

- Objetivos e aplicação de políticas de acesso.
- Funcionamento e tipos de ACL (standard e extended) e máscaras wildcard.
- Boas práticas de criação e manutenção de políticas de acesso.

#### **Módulo 5 – Implementação de Políticas de Acesso IPv4**

- Configuração e edição de ACLs em dispositivos de rede.
- Filtragem de tráfego e controlo de acessos administrativos.
- Utilização de ACLs para mitigação de ameaças.

#### **Módulo 6 – Network Address Translation (NAT)**

- Conceito e finalidade da tradução de endereços.
- Tipos de NAT: estática, dinâmica e overload (PAT).
- Implementação prática e verificação de funcionamento.
- Transição entre IPv4 e IPv6 (NAT64).

#### **Módulo 7 – Conectividade Empresarial, VPN e Comunicação Segura**

- Conceitos de redes de longa distância (WAN) e conectividade empresarial.
- Tipos de ligações WAN (tradicional, moderna e baseada em Internet).
- Virtual Private Networks (VPN): fundamentos e aplicações.
- Estrutura de uma comunicação segura (IPsec).

#### **Módulo 8 – Qualidade de Serviço (QoS) e Gestão de Tráfego**

- Conceito de QoS e sua importância nas redes modernas.
- Tipos de tráfego (voz, vídeo, dados) e requisitos mínimos.
- Algoritmos de escalonamento e priorização.
- Técnicas de implementação de QoS.

#### **Módulo 9 – Gestão e Monitorização de Equipamentos e Serviços**

- Descoberta de dispositivos na rede.
- Protocolos de monitorização e gestão (LLDP, NTP, SNMP, Syslog).
- Registo e análise de eventos.
- Cópias de segurança e atualização de software de rede.

#### **Módulo 10 – Desenho e Escalabilidade de Redes Empresariais**

- Princípios de desenho de redes escaláveis.
- Hierarquização, redundância e convergência de serviços.
- Equipamentos e topologias em redes de média dimensão.

#### **Módulo 11 – Virtualização e Software Defined Networking (SDN)**

- Conceitos de virtualização e computação em nuvem.
- Virtualização de dispositivos e serviços de rede.
- Fundamentos de Software Defined Networking (SDN).
- Arquiteturas baseadas em controladores e separação de planos de rede.

#### **Módulo 12 – Automação de Redes e Gestão Centralizada**

- Conceito e benefícios da automação de redes.
- Comunicação entre sistemas: APIs e formatos de dados (JSON, XML, YAML).
- Ferramentas de gestão de configuração (Ansible, Chef, Puppet, SaltStack).
- Gestão de redes baseada em políticas centralizadas.