Revisão: 4ª Versão
Data: 29/05/2025
Aprovado.

A Diretora Regional,

Andreia Jardim

PRR Plano de Recuperação e Resiliência

REGIÃO AUTÓNOMA DA MADEIRA

REPÚBLICA PORTUGUESA

Financiado pela União Europeia NextGenerationEU

PLANO DE FORMAÇÃO – 2025

Informação mais pormenorizada sobre o presente Plano de Formação consta dos cadernos de encargos aprovados, no âmbito dos procedimentos públicos de aquisição da formação em apreço.

No âmbito deste Plano de Formação da DRAP, em articulação com o Gabinete Regional para a Conformidade Digital, Proteção de Dados e Cibersegurança–GCPD, são disponibilizadas 19 ações de formação/ seminários, na área de Informática (Literacia Digital) sobre Cibersegurança na Administração Pública. Este Plano de Formação integra ainda os 10 Cursos em formato MOOC (Massive Open Online Courses - Cursos de Formação Online Abertos e Massivos) do Projeto Formativo DigicAP - Capacitação Digital a Distância na Administração Pública da RAM, desenvolvido pela Direção Regional da Administração Pública – DRAP, em parceria com a DTIM (Associação para o Desenvolvimento das Tecnologias de Informação da Madeira), entidade formadora da RAM, detentora de protocolo com a Fundação para a Ciência e Tecnologia – FCT para utilizar a Plataforma NAU.

Em termos de modalidade a formação do presente Plano carateriza-se por ser contínua. A nível de organização teremos intervenções formativas enquadradas no modelo à distância e formações executadas através do formato presencial. Os meios, recursos e metodologia de avaliação a utilizar em cada intervenção formativa constam do referido caderno de encargos e serão, oportunamente, também refletidos no Balanço de Atividade Formativa da DRAP do corrente ano.

Todas as intervenções formativas constantes do atual Plano de Formação da DRAP para 2025 são abrangidas pelo Plano de Recuperação e Resiliência–PRR, Eixo Transição Digital da Administração Pública da RAM, sub-investimento C19-i05_02-Transição Digital da Administração Pública da RAM–DRAP.

No que toca a parcerias regista-se que as ações de formação incluídas neste Plano de Formação são concretizadas em colaboração com a DTIM – Associação para o Desenvolvimento das Tecnologias de Informação da Madeira e a Rumos II, Formação, S.A.

CURSO	CARGA HORÁRIA	CONTEÚDO PROGRAMÁTICO	DESTINATÁRIOS	FORMADOR	LOCAL/PLATAFORMA PARA FORMAÇÃO À DISTÂNCIA	DATA
1 – Formação em Cibersegurança para Dirigentes Superiores da Administração Pública Regional – 1ª Ação	2 horas	1 - Introdução: a) Enquadramento; b) Objetivos; c) Estrutura do Documento; d) Definições e Abreviaturas; e) Gestão de Risco; f) Âmbito e Aplicabilidade; g) Estrutura do QNRCS; h) Contextualização. 2 - Introdução à cibersegurança para dirigentes: a) O que é Cibersegurança? b) Responsabilidade da administração / organização; c) Funções do responsável de segurança; d) Como Dirigente, pode ser alvo; e) Cibersegurança: o que precisa de saber? f) Porque é que a organização está em risco? g) Quem está por trás dos ciberataques? 3 - Incorporação da cibersegurança na organização. 4 - Desenvolvimento de uma cultura positiva de cibersegurança. 5 - Desenvolvimento de competências em cibersegurança.	Titulares de cargos de direção superior da Administração Pública e equiparados (Nível VI)	Vitorino Gouveia	CEHA – Centro de Estudos de História do Atlântico- Rua das Mercês, n.º 8, 9000-224, Funchal	12/03/2025 (4.ªfeira)

		6 - Identificação dos ativos críticos da organização. 7 - Conhecer o panorama das ameaças atuais. 8 - Gestão de riscos para cibersegurança. 9 - Aplicação de medidas eficazes de segurança. 10 - Colaboração com a sua cadeia de valor e parceiros. 11 - Esquema de certificação QNRCS e selo de maturidade digital da cibersegurança; 12 - Planeamento da resposta a incidentes cibernéticos, incluindo a comunicação (Referencial de Comunicação de Crise). 13 - Síntese de legislação aplicável à cibersegurança				
2 – Formação em Cibersegurança para Dirigentes Superiores da Administração Pública Regional – 2ª Ação	2 horas	1 - Introdução: a) Enquadramento; b) Objetivos; c) Estrutura do Documento; d) Definições e Abreviaturas; e) Gestão de Risco; f) Âmbito e Aplicabilidade; g) Estrutura do QNRCS; h) Contextualização. 2 - Introdução à cibersegurança para dirigentes: a) O que é Cibersegurança?	Titulares de cargos de direção superior da Administração Pública e equiparados (Nível VI)	Vitorino Gouveia	CEHA – Centro de Estudos de História do Atlântico- Rua das Mercês, n.º 8, 9000-224, Funchal	19/03/2025 (4.ªfeira)

		b) Responsabilidade da administração / organização; c) Funções do responsável de segurança; d) Como Dirigente, pode ser alvo; e) Cibersegurança: o que precisa de saber? f) Porque é que a organização está em risco? g) Quem está por trás dos ciberataques? 3 - Incorporação da cibersegurança na organização. 4 - Desenvolvimento de uma cultura positiva de cibersegurança. 5 - Desenvolvimento de competências em cibersegurança. 6 - Identificação dos ativos críticos da organização. 7 - Conhecer o panorama das ameaças atuais. 8 - Gestão de riscos para cibersegurança. 9 - Aplicação de medidas eficazes de segurança. 10 - Colaboração com a sua cadeia de valor e parceiros. 11 - Esquema de certificação QNRCS e selo de maturidade digital da cibersegurança; 12 - Planeamento da resposta a incidentes cibernéticos, incluindo a comunicação (Referencial de Comunicação de Crise). 13 - Síntese de legislação aplicável à cibersegurança				

3 – Formação em Cibersegurança para Dirigentes Intermédios da Administração Pública Regional – 1.ª Ação	3,5 horas	1- Introdução: a) Enquadramento; b) Objetivos; c) Estrutura do Documento; d) Definições e Abreviaturas; e) Gestão de Risco; f) Âmbito e Aplicabilidade; g) Estrutura do QNRCS; h) Contextualização. 2- Introdução à cibersegurança para dirigentes: a) O que é Cibersegurança? b) Responsabilidade da administração / organização; c) Funções do responsável de segurança; d Como Dirigente, pode ser alvo; e) Cibersegurança: o que precisa de saber? f) Porque é que a organização está em risco? g) Quem está por trás dos ciberataques? 3 - Incorporação da cibersegurança na organização. 4 - Desenvolvimento de uma cultura positiva de cibersegurança. 5 - Desenvolvimento de competências em cibersegurança. 6 - Identificação dos ativos críticos da organização. 7- Conhecer o panorama das ameaças atuais. 8 - Gestão de riscos para cibersegurança.	Titulares de cargos de direção intermédia da Administração Pública e equiparados (Nível VI)	Filipe Feitas	CEHA – Centro de Estudos de História do Atlântico- Rua das Mercês, n.º 8, 9000-224, Funchal	21/03/2025 (6.ªfeira)

		9 - Aplicação de medidas eficazes de segurança. 10 - Colaboração com a sua cadeia de valor e parceiros. 11 - Esquema de certificação QNRCS e selo de maturidade digital da cibersegurança; 12 - Planeamento da resposta a incidentes cibernéticos, incluindo a comunicação (Referencial de Comunicação de Crise). 13 - Síntese de legislação aplicável à cibersegurança. 14 - Identidade digital. 15 - Credenciais de acesso. 16 - Palavras-passe. 17 - Fatores de autenticação. 18 - Gestão segura credenciais de acesso. 19 - Cuidados a ter no trabalho: a) Como proteger a sua Identidade digital da organização; b) Como ajudar a proteger a rede da sua organização; c) Comportamentos seguros; d) Principais tipos de ciberameaças (Social Engineering, Phishing, Malware, ...); e) Como proteger o seu posto de trabalho; 20 - Cuidados a ter no exterior: a) Recomendações gerais; b) Em viagem.				

		21 - Cuidados a ter em casa, em teletrabalho: a) Como proteger a sua Identidade digital; b) Como proteger a sua rede doméstica; c) Como navegar na Internet com segurança e privacidade; d) Comportamento social seguro; e) Como proteger o posto de trabalho doméstico.				
4 – Formação em Cibersegurança para Dirigentes Intermédios da Administração Pública Regional – 2.ª Ação	3,5 horas	1- Introdução: a) Enquadramento; b) Objetivos; c) Estrutura do Documento; d) Definições e Abreviaturas; e) Gestão de Risco; f) Âmbito e Aplicabilidade; g) Estrutura do QNRCS; h) Contextualização. 2- Introdução à cibersegurança para dirigentes: a) O que é Cibersegurança? b) Responsabilidade da administração / organização; c) Funções do responsável de segurança; d Como Dirigente, pode ser alvo; e) Cibersegurança: o que precisa de saber? f) Porque é que a organização está em risco? g) Quem está por trás dos ciberataques?	Titulares de cargos de direção intermédia da Administração Pública e equiparados (Nível VI)	Filipe Feitas	CEHA – Centro de Estudos de História do Atlântico- Rua das Mercês, n.º 8, 9000-224 Funchal	28/03/2025 (6.ª feira)

		3 - Incorporação da cibersegurança na organização. 4 - Desenvolvimento de uma cultura positiva de cibersegurança. 5 - Desenvolvimento de competências em cibersegurança. 6 - Identificação dos ativos críticos da organização. 7- Conhecer o panorama das ameaças atuais. 8 - Gestão de riscos para cibersegurança. 9 - Aplicação de medidas eficazes de segurança. 10 - Colaboração com a sua cadeia de valor e parceiros. 11 - Esquema de certificação QNRCS e selo de maturidade digital da cibersegurança; 12 - Planeamento da resposta a incidentes cibernéticos, incluindo a comunicação (Referencial de Comunicação de Crise). 13 - Síntese de legislação aplicável à cibersegurança. 14 - Identidade digital. 15 - Credenciais de acesso. 16 - Palavras-passe. 17 - Fatores de autenticação. 18 - Gestão segura credenciais de acesso. 19 - Cuidados a ter no trabalho:				

		a) Como proteger a sua Identidade digital da organização; b) Como ajudar a proteger a rede da sua organização; c) Comportamentos seguros; d) Principais tipos de ciberameaças (Social Engineering, Phishing, Malware, ...); e) Como proteger o seu posto de trabalho; 20 - Cuidados a ter no exterior: a) Recomendações gerais; b) Em viagem. 21 - Cuidados a ter em casa, em teletrabalho: a) Como proteger a sua Identidade digital; b) Como proteger a sua rede doméstica; c) Como navegar na Internet com segurança e privacidade; d) Comportamento social seguro; e) Como proteger o posto de trabalho doméstico.				

5 – Formação em Cibersegurança para Dirigentes Intermédios da Administração Pública Regional – 3.ª Ação	3,5 horas	1- Introdução: a) Enquadramento; b) Objetivos; c) Estrutura do Documento; d) Definições e Abreviaturas; e) Gestão de Risco; f) Âmbito e Aplicabilidade; g) Estrutura do QNRCS; h) Contextualização. 2- Introdução à cibersegurança para dirigentes: a) O que é Cibersegurança? b) Responsabilidade da administração / organização; c) Funções do responsável de segurança; d Como Dirigente, pode ser alvo; e) Cibersegurança: o que precisa de saber? f) Porque é que a organização está em risco? g) Quem está por trás dos ciberataques? 3 - Incorporação da cibersegurança na organização. 4 - Desenvolvimento de uma cultura positiva de cibersegurança. 5 - Desenvolvimento de competências em cibersegurança. 6 - Identificação dos ativos críticos da organização. 7- Conhecer o panorama das ameaças atuais.	Titulares de cargos de direção intermédia da Administração Pública e equiparados (Nível VI)	Filipe Feitas	CEHA – Centro de Estudos de História do Atlântico- Rua das Mercês, n.º 8, 9000-224, Funchal	04/04/2025 (6.ª feira)

		8 - Gestão de riscos para cibersegurança. 9 - Aplicação de medidas eficazes de segurança. 10 - Colaboração com a sua cadeia de valor e parceiros. 11 - Esquema de certificação QNRCS e selo de maturidade digital da cibersegurança; 12 - Planeamento da resposta a incidentes cibernéticos, incluindo a comunicação (Referencial de Comunicação de Crise). 13 - Síntese de legislação aplicável à cibersegurança. 14 - Identidade digital. 15 - Credenciais de acesso. 16 - Palavras-passe. 17 - Fatores de autenticação. 18 - Gestão segura credenciais de acesso. 19 - Cuidados a ter no trabalho: a) Como proteger a sua Identidade digital da organização; b) Como ajudar a proteger a rede da sua organização; c) Comportamentos seguros; d) Principais tipos de ciberameaças (Social Engineering, Phishing, Malware, ...); e) Como proteger o seu posto de trabalho; 20 - Cuidados a ter no exterior: a) Recomendações gerais;				

		b) Em viagem. 21 - Cuidados a ter em casa, em teletrabalho: a) Como proteger a sua Identidade digital; b) Como proteger a sua rede doméstica; c) Como navegar na Internet com segurança e privacidade; d) Comportamento social seguro; e) Como proteger o posto de trabalho doméstico.				
6 – Formação em Cibersegurança para Dirigentes Intermédios da Administração Pública Regional – 4.ª Ação	3,5 horas	1- Introdução: a) Enquadramento; b) Objetivos; c) Estrutura do Documento; d) Definições e Abreviaturas; e) Gestão de Risco; f) Âmbito e Aplicabilidade; g) Estrutura do QNRCS; h) Contextualização. 2- Introdução à cibersegurança para dirigentes: a) O que é Cibersegurança? b) Responsabilidade da administração / organização; c) Funções do responsável de segurança; d Como Dirigente, pode ser alvo; e) Cibersegurança: o que precisa de saber? f) Porque é que a organização está em risco?	Titulares de cargos de direção intermédia da Administração Pública e equiparados (Nível VI)	Filipe Feitas	CEHA – Centro de Estudos de História do Atlântico- Rua das Mercês, n.º 8, 9000-224, Funchal	11/04/2025 (6.ª feira)

		g) Quem está por trás dos ciberataques? 3 - Incorporação da cibersegurança na organização. 4 - Desenvolvimento de uma cultura positiva de cibersegurança. 5 - Desenvolvimento de competências em cibersegurança. 6 - Identificação dos ativos críticos da organização. 7- Conhecer o panorama das ameaças atuais. 8 - Gestão de riscos para cibersegurança. 9 - Aplicação de medidas eficazes de segurança. 10 - Colaboração com a sua cadeia de valor e parceiros. 11 - Esquema de certificação QNRCS e selo de maturidade digital da cibersegurança; 12 - Planeamento da resposta a incidentes cibernéticos, incluindo a comunicação (Referencial de Comunicação de Crise). 13 - Síntese de legislação aplicável à cibersegurança. 14 - Identidade digital. 15 - Credenciais de acesso. 16 - Palavras-passe. 17 - Fatores de autenticação. 18 - Gestão segura credenciais de acesso. 19 - Cuidados a ter no trabalho:				

		a) Como proteger a sua Identidade digital da organização; b) Como ajudar a proteger a rede da sua organização; c) Comportamentos seguros; d) Principais tipos de ciberameaças (Social Engineering, Phishing, Malware, ...); e) Como proteger o seu posto de trabalho; 20 - Cuidados a ter no exterior: a) Recomendações gerais; b) Em viagem. 21 - Cuidados a ter em casa, em teletrabalho: a) Como proteger a sua Identidade digital; b) Como proteger a sua rede doméstica; c) Como navegar na Internet com segurança e privacidade; d) Comportamento social seguro; e) Como proteger o posto de trabalho doméstico.				

7 – Formação em Cibersegurança para Dirigentes Intermédios da Administração Pública Regional – 5.ª Ação	3,5 horas	1- Introdução: a) Enquadramento; b) Objetivos; c) Estrutura do Documento; d) Definições e Abreviaturas; e) Gestão de Risco; f) Âmbito e Aplicabilidade; g) Estrutura do QNRCS; h) Contextualização. 2- Introdução à cibersegurança para dirigentes: a) O que é Cibersegurança? b) Responsabilidade da administração / organização; c) Funções do responsável de segurança; d Como Dirigente, pode ser alvo; e) Cibersegurança: o que precisa de saber? f) Porque é que a organização está em risco? g) Quem está por trás dos ciberataques? 3 - Incorporação da cibersegurança na organização. 4 - Desenvolvimento de uma cultura positiva de cibersegurança. 5 - Desenvolvimento de competências em cibersegurança. 6 - Identificação dos ativos críticos da organização. 7- Conhecer o panorama das ameaças atuais.	Titulares de cargos de direção intermédia da Administração Pública e equiparados (Nível VI)	Filipe Feitas	Casa-Museu Frederico de Freitas, Calçada de Santa Clara, n.º 7, 9000-036, Funchal	09/05/2025 (6.ª feira)

		8 - Gestão de riscos para cibersegurança. 9 - Aplicação de medidas eficazes de segurança. 10 - Colaboração com a sua cadeia de valor e parceiros. 11 - Esquema de certificação QNRCS e selo de maturidade digital da cibersegurança; 12 - Planeamento da resposta a incidentes cibernéticos, incluindo a comunicação (Referencial de Comunicação de Crise). 13 - Síntese de legislação aplicável à cibersegurança. 14 - Identidade digital. 15 - Credenciais de acesso. 16 - Palavras-passe. 17 - Fatores de autenticação. 18 - Gestão segura credenciais de acesso. 19 - Cuidados a ter no trabalho: a) Como proteger a sua Identidade digital da organização; b) Como ajudar a proteger a rede da sua organização; c) Comportamentos seguros; d) Principais tipos de ciberameaças (Social Engineering, Phishing, Malware, ...); e) Como proteger o seu posto de trabalho; 20 - Cuidados a ter no exterior: a) Recomendações gerais;				

		b) Em viagem. 21 - Cuidados a ter em casa, em teletrabalho: a) Como proteger a sua Identidade digital; b) Como proteger a sua rede doméstica; c) Como navegar na Internet com segurança e privacidade; d) Comportamento social seguro; e) Como proteger o posto de trabalho doméstico.				
8 – Formação em Cibersegurança para Dirigentes Intermédios da Administração Pública Regional – 6.ª Ação	3,5 horas	1- Introdução: a) Enquadramento; b) Objetivos; c) Estrutura do Documento; d) Definições e Abreviaturas; e) Gestão de Risco; f) Âmbito e Aplicabilidade; g) Estrutura do QNRCS; h) Contextualização. 2- Introdução à cibersegurança para dirigentes: a) O que é Cibersegurança? b) Responsabilidade da administração / organização; c) Funções do responsável de segurança; d Como Dirigente, pode ser alvo; e) Cibersegurança: o que precisa de saber? f) Porque é que a organização está em risco?	Titulares de cargos de direção intermédia da Administração Pública e equiparados (Nível VI)	Filipe Feitas	CEHA – Centro de Estudos de História do Atlântico- Rua das Mercês, n.º 8, 9000-224, Funchal	16/05/2025 (6.ª feira)

		g) Quem está por trás dos ciberataques? 3 - Incorporação da cibersegurança na organização. 4 - Desenvolvimento de uma cultura positiva de cibersegurança. 5 - Desenvolvimento de competências em cibersegurança. 6 - Identificação dos ativos críticos da organização. 7- Conhecer o panorama das ameaças atuais. 8 - Gestão de riscos para cibersegurança. 9 - Aplicação de medidas eficazes de segurança. 10 - Colaboração com a sua cadeia de valor e parceiros. 11 - Esquema de certificação QNRCS e selo de maturidade digital da cibersegurança; 12 - Planeamento da resposta a incidentes cibernéticos, incluindo a comunicação (Referencial de Comunicação de Crise). 13 - Síntese de legislação aplicável à cibersegurança. 14 - Identidade digital. 15 - Credenciais de acesso. 16 - Palavras-passe. 17 - Fatores de autenticação. 18 - Gestão segura credenciais de acesso. 19 - Cuidados a ter no trabalho:				

		a) Como proteger a sua Identidade digital da organização; b) Como ajudar a proteger a rede da sua organização; c) Comportamentos seguros; d) Principais tipos de ciberameaças (Social Engineering, Phishing, Malware, ...); e) Como proteger o seu posto de trabalho; 20 - Cuidados a ter no exterior: a) Recomendações gerais; b) Em viagem. 21 - Cuidados a ter em casa, em teletrabalho: a) Como proteger a sua Identidade digital; b) Como proteger a sua rede doméstica; c) Como navegar na Internet com segurança e privacidade; d) Comportamento social seguro; e) Como proteger o posto de trabalho doméstico.				

9 – Formação em Cibersegurança para Dirigentes Intermédios da Administração Pública Regional – 7.ª Ação	3,5 horas	1- Introdução: a) Enquadramento; b) Objetivos; c) Estrutura do Documento; d) Definições e Abreviaturas; e) Gestão de Risco; f) Âmbito e Aplicabilidade; g) Estrutura do QNRCS; h) Contextualização. 2- Introdução à cibersegurança para dirigentes: a) O que é Cibersegurança? b) Responsabilidade da administração / organização; c) Funções do responsável de segurança; d Como Dirigente, pode ser alvo; e) Cibersegurança: o que precisa de saber? f) Porque é que a organização está em risco? g) Quem está por trás dos ciberataques? 3 - Incorporação da cibersegurança na organização. 4 - Desenvolvimento de uma cultura positiva de cibersegurança. 5 - Desenvolvimento de competências em cibersegurança. 6 - Identificação dos ativos críticos da organização. 7- Conhecer o panorama das ameaças atuais.	Titulares de cargos de direção intermédia da Administração Pública e equiparados (Nível VI)	Filipe Feitas	Casa-Museu Frederico de Freitas, Calçada de Santa Clara, n.º 7, 9000-036, Funchal	23/05/2025 (6.ª feira)

		8 - Gestão de riscos para cibersegurança. 9 - Aplicação de medidas eficazes de segurança. 10 - Colaboração com a sua cadeia de valor e parceiros. 11 - Esquema de certificação QNRCS e selo de maturidade digital da cibersegurança; 12 - Planeamento da resposta a incidentes cibernéticos, incluindo a comunicação (Referencial de Comunicação de Crise). 13 - Síntese de legislação aplicável à cibersegurança. 14 - Identidade digital. 15 - Credenciais de acesso. 16 - Palavras-passe. 17 - Fatores de autenticação. 18 - Gestão segura credenciais de acesso. 19 - Cuidados a ter no trabalho: a) Como proteger a sua Identidade digital da organização; b) Como ajudar a proteger a rede da sua organização; c) Comportamentos seguros; d) Principais tipos de ciberameaças (Social Engineering, Phishing, Malware, ...); e) Como proteger o seu posto de trabalho; 20 - Cuidados a ter no exterior: a) Recomendações gerais;				

		b) Em viagem. 21 - Cuidados a ter em casa, em teletrabalho: a) Como proteger a sua Identidade digital; b) Como proteger a sua rede doméstica; c) Como navegar na Internet com segurança e privacidade; d) Comportamento social seguro; e) Como proteger o posto de trabalho doméstico.				
10 – Formação em Cibersegurança para Dirigentes Intermédios da Administração Pública Regional – 8.ª Ação	3,5 horas	1- Introdução: a) Enquadramento; b) Objetivos; c) Estrutura do Documento; d) Definições e Abreviaturas; e) Gestão de Risco; f) Âmbito e Aplicabilidade; g) Estrutura do QNRCS; h) Contextualização. 2- Introdução à cibersegurança para dirigentes: a) O que é Cibersegurança? b) Responsabilidade da administração / organização; c) Funções do responsável de segurança; d Como Dirigente, pode ser alvo; e) Cibersegurança: o que precisa de saber? f) Porque é que a organização está em risco?	Titulares de cargos de direção intermédia da Administração Pública e equiparados (Nível VI)	Filipe Feitas	CEHA – Centro de Estudos de História do Atlântico- Rua das Mercês, n.º 8, 9000-224, Funchal	30/05/2025 (6.ª feira)

		g) Quem está por trás dos ciberataques? 3 - Incorporação da cibersegurança na organização. 4 - Desenvolvimento de uma cultura positiva de cibersegurança. 5 - Desenvolvimento de competências em cibersegurança. 6 - Identificação dos ativos críticos da organização. 7- Conhecer o panorama das ameaças atuais. 8 - Gestão de riscos para cibersegurança. 9 - Aplicação de medidas eficazes de segurança. 10 - Colaboração com a sua cadeia de valor e parceiros. 11 - Esquema de certificação QNRCS e selo de maturidade digital da cibersegurança; 12 - Planeamento da resposta a incidentes cibernéticos, incluindo a comunicação (Referencial de Comunicação de Crise). 13 - Síntese de legislação aplicável à cibersegurança. 14 - Identidade digital. 15 - Credenciais de acesso. 16 - Palavras-passe. 17 - Fatores de autenticação. 18 - Gestão segura credenciais de acesso. 19 - Cuidados a ter no trabalho:			

		a) Como proteger a sua Identidade digital da organização; b) Como ajudar a proteger a rede da sua organização; c) Comportamentos seguros; d) Principais tipos de ciberameaças (Social Engineering, Phishing, Malware, ...); e) Como proteger o seu posto de trabalho; 20 - Cuidados a ter no exterior: a) Recomendações gerais; b) Em viagem. 21 - Cuidados a ter em casa, em teletrabalho: a) Como proteger a sua Identidade digital; b) Como proteger a sua rede doméstica; c) Como navegar na Internet com segurança e privacidade; d) Comportamento social seguro; e) Como proteger o posto de trabalho doméstico.				
11 – Certified Information System Security Professional (CISSP) – 1.ª Ação	35 horas	1 - O Ambiente de Segurança Informática. • Justificar um código de ética organizacional; • Relacionar os princípios de confidencialidade, integridade, disponibilidade, não-repúdio, autenticação, privacidade e segurança com os princípios de devido cuidado e diligência devida;	Dirigentes, técnicos superiores, especialistas de sistemas e tecnologias de informação, técnicos de	Hugo Rodrigues	Plataforma Online: Teams	de 02/06 a 06/06/2025 (de 2.ª feira a 6.ª feira)

		• Relacionar governança de segurança da informação com as estratégias de negócio, as metas, as missões e os objetivos organizacionais; • Aplicar conceitos de cibercrime a situações de violação de dados e a outras situações que comprometam a segurança da informação; • Relacionar os requisitos legais, contratuais e regulamentares de privacidade e proteção de dados de acordo com os objetivos de segurança da informação; • Relacionar a circulação transfronteiriça de dados e as questões de importação-exportação de acordo com a proteção de dados, a privacidade e a proteção da propriedade intelectual; 2 - Segurança dos Ativos de Informação • Relacionar os modelos de gestão de ativos de TI e de ciclo de vida de segurança de dados com a segurança da informação; • Explicar a utilização da classificação e da categorização da informação, como dois processos distintos, mas relacionados; • Descrever os diferentes estados dos dados e as suas considerações em matéria de segurança da informação;	sistemas e tecnologias de informação (Nível IV, V e VI) **– ATENÇÃO: esta formação é dirigida apenas aos responsáveis de cibersegurança, suplentes e eventuais elementos que trabalhem exclusivamente em cibersegurança, por esse motivo não serão aceites inscrições de formandos que não cumpram com esses requisitos.**			

		• Descrever os diferentes cargos diretamente envolvidos no uso da informação e as considerações de segurança para os mesmos; • Descrever os diferentes tipos e categorias de controlos de segurança da informação e a sua utilização; • Selecionar as normas de segurança de dados adequadas aos requisitos de conformidade da organização; 3 - Gestão de Identidade e de Acesso (IAM). • Explicar o ciclo de vida de identidade e como se aplica a utilizadores humanos e não humanos; • Comparar e contrastar modelos, mecanismos e conceitos de controlo de acesso; • Explicar o papel da autenticação, autorização e contabilidade no alcance de metas e objetivos de segurança da informação; • Explicar como as implementações de IAM devem proteger os ativos físicos e lógicos; • Descrever o papel das credenciais e do armazenamento de identidade nos sistemas IAM; 4 - Arquitetura e Engenharia de Segurança.				

		• Descrever os principais componentes das normas de engenharia de segurança; • Explicar os principais modelos de arquitetura para a segurança da informação; • Explicar as capacidades de segurança implementadas no hardware e no firmware; • Aplicar princípios de segurança a diferentes arquiteturas de sistemas de informação e respetivos ambientes; • Determinar a melhor aplicação de abordagens criptográficas para resolver as necessidades de segurança da informação organizacional; • Gerir a utilização de certificados e de assinaturas digitais adequados às necessidades organizacionais de segurança da informação; • Descobrir as implicações da não utilização de técnicas criptográficas para proteger a cadeia de abastecimento; • Aplicar diferentes soluções de gestão criptográfica adequadas às necessidades organizacionais de segurança da informação; • Verificar se as soluções criptográficas estão a funcionar e a responder à evolução das ameaças do mundo real; • Descrever as defesas contra-ataques criptográficos comuns;				

		• Desenvolver uma lista de verificação de gestão para determinar o estado de saúde e a prontidão criptográfica de uma organização; 5 - Segurança da Comunicação e Redes. • Descrever as características arquitetónicas, as tecnologias relevantes, os protocolos e as considerações de segurança de cada uma das camadas do modelo OSI; • Explicar a aplicação de práticas de conceção seguras no desenvolvimento de infraestruturas de rede; • Descrever a evolução dos métodos de segurança dos protocolos de comunicação IP; • Explicar as implicações de segurança dos ambientes de rede ligados (cabo e fibra) e não ligados (sem fios); • Descrever a evolução e as implicações de segurança dos principais dispositivos de rede; • Avaliar e contrastar os problemas de segurança das comunicações de voz em infra-estruturas tradicionais e VoIP; • Descrever e contrastar as considerações de segurança para as principais tecnologias de acesso remoto;				

		• Explicar as implicações de segurança das tecnologias de rede definida por software (SDN) e de virtualização de rede; 6 - Segurança do Desenvolvimento de Software. • Reconhecer os muitos elementos de software que podem pôr em risco a segurança dos sistemas de informação; • Identificar e explicar as principais causas de fragilidades de segurança no código-fonte; • Explicar as principais causas de fragilidades de segurança em sistemas de base de dados e de data warehouse; • Esclarecer a aplicabilidade da estrutura OWASP a diversas arquiteturas web; • Selecionar estratégias de mitigação de malware adequadas às necessidades organizacionais de segurança da informação; • Comparar as formas como diferentes metodologias, estruturas e directrizes de desenvolvimento de software contribuem para a segurança dos sistemas; • Explicar a implementação de controlos de segurança para ecossistemas de desenvolvimento de software; • Escolher uma combinação adequada de testes de segurança, avaliação, controlos e			

		métodos de gestão para diferentes sistemas e ambientes de aplicações; 7 - Avaliação e Testes de Segurança. • Descrever a finalidade, o processo e os objetivos da avaliação e dos testes de segurança formais e informais; • Aplicar a ética profissional e organizacional à avaliação e aos testes de segurança; • Explicar a avaliação e os testes internos, externos e de terceiros; • Explicar as questões de gestão e de governança relacionadas com o planeamento e a realização de avaliações de segurança; • Explicar o papel da avaliação na tomada de decisões de segurança baseadas em dados; 8 - Operações de Segurança. • Demostrar como se recolhe e avalia dados de segurança de forma eficiente e eficaz; • Explicar os benefícios de segurança de uma gestão e controlo eficazes das alterações; • Desenvolver políticas e planos de resposta a incidentes; • Relacionar a resposta a incidentes com as necessidades de controlo de segurança e a sua utilização operacional;				

		• Relacionar os controlos de segurança com a melhoria e a obtenção da disponibilidade necessária dos bens e sistemas de informação; • Compreender as ramificações de segurança e de proteção de diferentes instalações, sistemas e características de infraestruturas; 9 – Outros. • Explicar como os frameworks e os processos de governança se relacionam com a utilização operacional dos controlos de segurança da informação; • Relacionar o processo de realização de investigações forenses com as operações de segurança da informação; • Relacionar a continuidade do negócio e a preparação para a recuperação de desastres com as operações de segurança da informação; • Explicar como utilizar a educação, a formação, a consciencialização e o envolvimento de todos os membros da organização como forma de reforçar e aplicar os processos de segurança da informação; • Demostrar como se operacionaliza os sistemas de informação e a gestão de riscos da cadeia de fornecimento de TI;				

		• Preparação para o exame de certificação CISSP, através de debate e realização de exercícios por domínio;				
12 – Certified Information System Security Professional (CISSP) – 2.ª Ação	35 horas	1 - O Ambiente de Segurança Informática. • Justificar um código de ética organizacional; • Relacionar os princípios de confidencialidade, integridade, disponibilidade, não-repúdio, autenticação, privacidade e segurança com os princípios de devido cuidado e diligência devida; • Relacionar governança de segurança da informação com as estratégias de negócio, as metas, as missões e os objetivos organizacionais; • Aplicar conceitos de cibercrime a situações de violação de dados e a outras situações que comprometam a segurança da informação; • Relacionar os requisitos legais, contratuais e regulamentares de privacidade e proteção de dados de acordo com os objetivos de segurança da informação; • Relacionar a circulação transfronteiriça de dados e as questões de importação-exportação de acordo com a proteção de	Dirigentes, técnicos superiores, especialistas de sistemas e tecnologias de informação, técnicos de sistemas e tecnologias de informação (Nível IV, V e VI) **– ATENÇÃO: esta formação é dirigida apenas aos responsáveis de cibersegurança, suplentes e eventuais elementos que trabalhem exclusivamente em cibersegurança,**	Hugo Rodrigues	Plataforma Online: Teams	De 11/06 a 17/06/2025 (4.ª feira, 5.ª feira, 6.ª feira, 2.ª e 3.ª feira)

		dados, a privacidade e a proteção da propriedade intelectual; 2 - Segurança dos Ativos de Informação • Relacionar os modelos de gestão de ativos de TI e de ciclo de vida de segurança de dados com a segurança da informação; • Explicar a utilização da classificação e da categorização da informação, como dois processos distintos, mas relacionados; • Descrever os diferentes estados dos dados e as suas considerações em matéria de segurança da informação; • Descrever os diferentes cargos diretamente envolvidos no uso da informação e as considerações de segurança para os mesmos; • Descrever os diferentes tipos e categorias de controlos de segurança da informação e a sua utilização; • Selecionar as normas de segurança de dados adequadas aos requisitos de conformidade da organização; 3 - Gestão de Identidade e de Acesso (IAM). • Explicar o ciclo de vida de identidade e como se aplica a utilizadores humanos e não humanos;	**por esse motivo não serão aceites inscrições de formandos que não cumpram com esses requisitos.**			

		• Comparar e contrastar modelos, mecanismos e conceitos de controlo de acesso; • Explicar o papel da autenticação, autorização e contabilidade no alcance de metas e objetivos de segurança da informação; • Explicar como as implementações de IAM devem proteger os ativos físicos e lógicos; • Descrever o papel das credenciais e do armazenamento de identidade nos sistemas IAM; 4 - Arquitetura e Engenharia de Segurança. • Descrever os principais componentes das normas de engenharia de segurança; • Explicar os principais modelos de arquitetura para a segurança da informação; • Explicar as capacidades de segurança implementadas no hardware e no firmware; • Aplicar princípios de segurança a diferentes arquiteturas de sistemas de informação e respetivos ambientes; • Determinar a melhor aplicação de abordagens criptográficas para resolver as necessidades de segurança da informação organizacional;				

		• Gerir a utilização de certificados e de assinaturas digitais adequados às necessidades organizacionais de segurança da informação; • Descobrir as implicações da não utilização de técnicas criptográficas para proteger a cadeia de abastecimento; • Aplicar diferentes soluções de gestão criptográfica adequadas às necessidades organizacionais de segurança da informação; • Verificar se as soluções criptográficas estão a funcionar e a responder à evolução das ameaças do mundo real; • Descrever as defesas contra-ataques criptográficos comuns; • Desenvolver uma lista de verificação de gestão para determinar o estado de saúde e a prontidão criptográfica de uma organização; 5 - Segurança da Comunicação e Redes. • Descrever as características arquitetónicas, as tecnologias relevantes, os protocolos e as considerações de segurança de cada uma das camadas do modelo OSI; • Explicar a aplicação de práticas de conceção seguras no desenvolvimento de infraestruturas de rede;				

		• Descrever a evolução dos métodos de segurança dos protocolos de comunicação IP; • Explicar as implicações de segurança dos ambientes de rede ligados (cabo e fibra) e não ligados (sem fios); • Descrever a evolução e as implicações de segurança dos principais dispositivos de rede; • Avaliar e contrastar os problemas de segurança das comunicações de voz em infra-estruturas tradicionais e VoIP; • Descrever e contrastar as considerações de segurança para as principais tecnologias de acesso remoto; • Explicar as implicações de segurança das tecnologias de rede definida por software (SDN) e de virtualização de rede; 6 - Segurança do Desenvolvimento de Software. • Reconhecer os muitos elementos de software que podem pôr em risco a segurança dos sistemas de informação; • Identificar e explicar as principais causas de fragilidades de segurança no código-fonte; • Explicar as principais causas de fragilidades de segurança em sistemas de base de dados e de data warehouse;				

		• Esclarecer a aplicabilidade da estrutura OWASP a diversas arquiteturas web; • Selecionar estratégias de mitigação de malware adequadas às necessidades organizacionais de segurança da informação; • Comparar as formas como diferentes metodologias, estruturas e directrizes de desenvolvimento de software contribuem para a segurança dos sistemas; • Explicar a implementação de controlos de segurança para ecossistemas de desenvolvimento de software; • Escolher uma combinação adequada de testes de segurança, avaliação, controlos e métodos de gestão para diferentes sistemas e ambientes de aplicações; 7 - Avaliação e Testes de Segurança. • Descrever a finalidade, o processo e os objetivos da avaliação e dos testes de segurança formais e informais; • Aplicar a ética profissional e organizacional à avaliação e aos testes de segurança; • Explicar a avaliação e os testes internos, externos e de terceiros; • Explicar as questões de gestão e de governança relacionadas com o planeamento e a realização de avaliações de segurança;			

		• Explicar o papel da avaliação na tomada de decisões de segurança baseadas em dados; 8 - Operações de Segurança. • Demostrar como se recolhe e avalia dados de segurança de forma eficiente e eficaz; • Explicar os benefícios de segurança de uma gestão e controlo eficazes das alterações; • Desenvolver políticas e planos de resposta a incidentes; • Relacionar a resposta a incidentes com as necessidades de controlo de segurança e a sua utilização operacional; • Relacionar os controlos de segurança com a melhoria e a obtenção da disponibilidade necessária dos bens e sistemas de informação; • Compreender as ramificações de segurança e de proteção de diferentes instalações, sistemas e características de infraestruturas; 9 – Outros. • Explicar como os frameworks e os processos de governança se relacionam com a utilização operacional dos controlos de segurança da informação;				

		• Relacionar o processo de realização de investigações forenses com as operações de segurança da informação; • Relacionar a continuidade do negócio e a preparação para a recuperação de desastres com as operações de segurança da informação; • Explicar como utilizar a educação, a formação, a consciencialização e o envolvimento de todos os membros da organização como forma de reforçar e aplicar os processos de segurança da informação; • Demostrar como se operacionaliza os sistemas de informação e a gestão de riscos da cadeia de fornecimento de TI; • Preparação para o exame de certificação CISSP, através de debate e realização de exercícios por domínio;				

[1] **13– Gestão da Segurança da Informação - Fundamentos da ISO/IEC 27001:2022 – 1.ª Ação (2.º Reagendamento)**	8 horas	1 - Segurança da Informação e Gestão do Risco Conceitos e terminologia. 2 - Gestão da Segurança de Informação de acordo com a Norma de referência NP ISO/IEC 27001- Sistemas de Gestão de Segurança da Informação – Requisitos: a) Estrutura da Norma ISO/IEC 27001: seguindo as regulamentações da ISO para todas as novas versões de normas de sistemas de gestão. b) Análise dos requisitos com exemplos ilustrativos. c) Análise Anexo A da Norma – Objetivos de Controlo e Controlos de Referência. 3 - O suporte à implementação de um SGSI seguindo as linhas de orientação da Norma ISO/IEC 27002: "Code of practice for information security controls". 4 - Exemplo de aplicação de gestão do risco para a segurança da informação, para utilização de controlos do Anexo A – relativos	Dirigentes, técnicos superiores, especialistas de sistemas e tecnologias de informação, técnicos de sistemas e tecnologias de informação (Nível IV, V e VI) – **ATENÇÃO: esta formação é dirigida apenas aos responsáveis de cibersegurança, suplentes e eventuais elementos que trabalhem**	António Bento	Plataforma Online: Moodle	20/06 e 23/06/2025 (6.ª e 2.ª feira – *período da manhã*)

[1] Por motivos imprevistos, foi necessário efetuar a substituição do formador que havia sido inicialmente designado para ministrar as ações de formação n.º 13, 14, 15 e 16. Não obstante terem sido envidados todos os esforços, por parte da entidade formadora contratada DTIM, no sentido de solucionar esta situação, não foi exequível manter as datas inicialmente programadas, pelo que foi necessário proceder não só à substituição do formador, mas também ao reagendamento das ações de formação em causa. Posteriormente, houve necessidade de proceder ao reagendamento do 2.º dia de formação, novamente, por motivos imprevistos, conforme indicado no presente Plano de Formação.

		a aspetos organizativos, da segurança lógica e física nas organizações, incluindo os inerentes à gestão da privacidade (dados pessoais).	**exclusivamente em cibersegurança, por esse motivo não serão aceites inscrições de formandos que não cumpram com esses requisitos.**			
[1] **14– Gestão da Segurança da Informação - Fundamentos da ISO/IEC 27001:2022 – 2.ª Ação (2.º Reagendamento)**	8 horas	1 - Segurança da Informação e Gestão do Risco Conceitos e terminologia. 2 - Gestão da Segurança de Informação de acordo com a Norma de referência NP ISO/IEC 27001- Sistemas de Gestão de Segurança da Informação – Requisitos: a) Estrutura da Norma ISO/IEC 27001: seguindo as regulamentações da ISO para todas as novas versões de normas de sistemas de gestão. b) Análise dos requisitos com exemplos ilustrativos.	Dirigentes, técnicos superiores, especialistas de sistemas e tecnologias de informação, técnicos de sistemas e tecnologias de informação (Nível IV, V e VI)	António Bento	Plataforma Online: Moodle .	20/06 e 23/06/2025 (6.ª e 2.ª feira *– período da tarde*)

[1] Por motivos imprevistos, foi necessário efetuar a substituição do formador que havia sido inicialmente designado para ministrar as ações de formação n.º 13, 14, 15 e 16. Não obstante terem sido envidados todos os esforços, por parte da entidade formadora contratada DTIM, no sentido de solucionar esta situação, não foi exequível manter as datas inicialmente programadas, pelo que foi necessário proceder não só à substituição do formador, mas também ao reagendamento das ações de formação em causa. Posteriormente, houve necessidade de proceder ao reagendamento do 2.º dia de formação, novamente, por motivos imprevistos, conforme indicado no presente Plano de Formação.

		c) Análise Anexo A da Norma – Objetivos de Controlo e Controlos de Referência. 3 - O suporte à implementação de um SGSI seguindo as linhas de orientação da Norma ISO/IEC 27002: "Code of practice for information security controls". 4 - Exemplo de aplicação de gestão do risco para a segurança da informação, para utilização de controlos do Anexo A – relativos a aspetos organizativos, da segurança lógica e física nas organizações, incluindo os inerentes à gestão da privacidade (dados pessoais).	– **ATENÇÃO: esta formação é dirigida apenas aos responsáveis de cibersegurança, suplentes e eventuais elementos que trabalhem exclusivamente em cibersegurança, por esse motivo não serão aceites inscrições de formandos que não cumpram com esses requisitos.**			

[2] **15– Gestão da Segurança da Informação - Fundamentos da ISO/IEC 27001:2022 – 3.ª Ação (2.º Reagendamento)**	8 horas	1 - Segurança da Informação e Gestão do Risco Conceitos e terminologia. 2 - Gestão da Segurança de Informação de acordo com a Norma de referência NP ISO/IEC 27001- Sistemas de Gestão de Segurança da Informação – Requisitos: a) Estrutura da Norma ISO/IEC 27001: seguindo as regulamentações da ISO para todas as novas versões de normas de sistemas de gestão. b) Análise dos requisitos com exemplos ilustrativos. c) Análise Anexo A da Norma – Objetivos de Controlo e Controlos de Referência. 3 - O suporte à implementação de um SGSI seguindo as linhas de orientação da Norma ISO/IEC 27002: "Code of practice for information security controls". 4 - Exemplo de aplicação de gestão do risco para a segurança da informação, para	Dirigentes, técnicos superiores, especialistas de sistemas e tecnologias de informação, técnicos de sistemas e tecnologias de informação (Nível IV, V e VI) – **ATENÇÃO: esta formação é dirigida apenas aos responsáveis de cibersegurança, suplentes e eventuais elementos que**	António Bento	Plataforma Online: Moodle	24/06 e 25/06/2025 (3.ª e 4.ª feira *– período da manhã)*

[2] Por motivos imprevistos, foi necessário efetuar a substituição do formador que havia sido inicialmente designado para ministrar as ações de formação n.º 13, 14, 15 e 16. Não obstante terem sido envidados todos os esforços, por parte da entidade formadora contratada DTIM, no sentido de solucionar esta situação, não foi exequível manter as datas inicialmente programadas, pelo que foi necessário proceder não só à substituição do formador, mas também ao reagendamento das ações de formação em causa. Posteriormente, houve necessidade de proceder ao reagendamento do 1.º dia de formação, novamente, por motivos imprevistos, conforme indicado no presente Plano de Formação.

		utilização de controlos do Anexo A – relativos a aspetos organizativos, da segurança lógica e física nas organizações, incluindo os inerentes à gestão da privacidade (dados pessoais).	**trabalhem exclusivamente em cibersegurança, por esse motivo não serão aceites inscrições de formandos que não cumpram com esses requisitos.**			
[2] **16– Gestão da Segurança da Informação - Fundamentos da ISO/IEC 27001:2022 – 4.ª Ação (2.º Reagendamento)**	8 horas	1 - Segurança da Informação e Gestão do Risco Conceitos e terminologia. 2 - Gestão da Segurança de Informação de acordo com a Norma de referência NP ISO/IEC 27001- Sistemas de Gestão de Segurança da Informação – Requisitos: a) Estrutura da Norma ISO/IEC 27001: seguindo as regulamentações da ISO para todas as novas versões de normas de sistemas de gestão. b) Análise dos requisitos com exemplos ilustrativos.	Dirigentes, técnicos superiores, especialistas de sistemas e tecnologias de informação, técnicos de sistemas e tecnologias de informação (Nível IV, V e VI)	António Bento	Plataforma Online: Moodle	24/06 e 25/06/2025 (3.ª e 4.ª feira *– período da tarde)*

[2] Por motivos imprevistos, foi necessário efetuar a substituição do formador que havia sido inicialmente designado para ministrar as ações de formação n.º 13, 14, 15 e 16. Não obstante terem sido envidados todos os esforços, por parte da entidade formadora contratada DTIM, no sentido de solucionar esta situação, não foi exequível manter as datas inicialmente programadas, pelo que foi necessário proceder não só à substituição do formador, mas também ao reagendamento das ações de formação em causa. Posteriormente, houve necessidade de proceder ao reagendamento do 1.º dia de formação, novamente, por motivos imprevistos, conforme indicado no presente Plano de Formação.

		c) Análise Anexo A da Norma – Objetivos de Controlo e Controlos de Referência. 3 - O suporte à implementação de um SGSI seguindo as linhas de orientação da Norma ISO/IEC 27002: "Code of practice for information security controls". 4 - Exemplo de aplicação de gestão do risco para a segurança da informação, para utilização de controlos do Anexo A – relativos a aspetos organizativos, da segurança lógica e física nas organizações, incluindo os inerentes à gestão da privacidade (dados pessoais).	– **ATENÇÃO: esta formação é dirigida apenas aos responsáveis de cibersegurança, suplentes e eventuais elementos que trabalhem exclusivamente em cibersegurança, por esse motivo não serão aceites inscrições de formandos que não cumpram com esses requisitos.**			

[3] **17 – Curso DigiCAp 1. Conteúdos Digitais: Guardar e Organizar Ficheiros**	6 horas	1 - Organizar, guardar e recuperar dados, informação e conteúdos em ambientes digitais; 2 - Usar suportes de armazenamento físico e virtual; 3 - Partilhar informação e conteúdos na nuvem; 4 - Aplicar regras de segurança na partilha de ficheiros sensíveis;	Dirigentes, Técnicos Superiores, Coordenadores Técnicos, outras Chefias Administrativas e Assistentes Técnicos (Nível I a VI)	Não aplicável	Plataforma Online: NAU	MOOC -disponível entre 11-03 e 30-06-2025
[3] **18 – Curso DigiCAp 2. Cibersegurança: Trabalhar de Forma Segura na Era Digital**	6 horas	1 - Reconhecer o impacto da segurança digital na vida pessoal e profissional; 2 - Aplicar boas práticas para a proteção de dados e privacidade; 3- Implementar métodos eficazes para a criação de senhas seguras; 4 - Implementar medidas de segurança na Internet; 5 - Reconhecer e evitar ataques cibernéticos;	Dirigentes, Técnicos Superiores, Coordenadores Técnicos, outras Chefias Administrativas e Assistentes Técnicos (Nível I a VI)	Não aplicável	Plataforma Online: NAU	MOOC - disponível entre 11-03 e 30-06-2025

[3] Informação mais detalhada concernente ao programa deste Curso pode ser acedida através da página web especificamente criada para o projeto formativo DigicAP (https://dtim.pt/digicap/) que possibilita o ingresso direto para a área adstrita a cada Curso MOOC na plataforma NAU.

[3] **19 – Curso DigiCAp 3. Competências Digitais em Informática: Microsoft Word**	6 horas	1 - Criar e guardar documentos no Word; 2 - Introduzir e formatar texto (títulos, listas, parágrafos, estilos); 3 - Criar e formatar tabelas, gráficos e recursos visuais; 4 - Aplicar ferramentas de revisão e colaboração; 5 - Inserir sumário automático e referências cruzadas;	Dirigentes, Técnicos Superiores, Coordenadores Técnicos, outras Chefias Administrativas e Assistentes Técnicos (Nível I a VI)	Não aplicável	Plataforma Online: NAU	MOOC - disponível entre 01-04 e 30-06-2025
[3] **20 – Curso DigiCAp 4. Competências Digitais em Informática: Microsoft Excel**	6 horas	1 - Criar e guardar folhas de cálculo no Excel; 2 - Editar e formatar folhas de cálculo; 3 - Criar fórmulas simples para analisar dados; 4 - Organizar e apresentar dados;	Dirigentes, Técnicos Superiores, Coordenadores Técnicos, outras Chefias Administrativas e Assistentes Técnicos (Nível I a VI)	Não aplicável	Plataforma Online: NAU	MOOC - disponível entre 01-04 e 30-06-2025

[3] Informação mais detalhada concernente ao programa deste Curso pode ser acedida através da página web especificamente criada para o projeto formativo DigicAP (https://dtim.pt/digicap/) que possibilita o ingresso direto para a área adstrita a cada Curso MOOC na plataforma NAU.

[3] **21 – Curso DigiCAp 5. Competências Digitais em Informática: Microsoft PowerPoint**	6 horas	1 - Criar e guardar apresentações em PowerPoint; 2 - Aplicar noções básicas de formatação; 3 - Aplicar transições e animações; 4 - Inserir elementos multimédia numa apresentação;	Dirigentes, Técnicos Superiores, Coordenadores Técnicos, outras Chefias Administrativas e Assistentes Técnicos (Nível I a VI)	Não aplicável	Plataforma Online: NAU	MOOC - disponível entre 01-04 e 30-06-2025
[3] **22 – Curso DigiCAp 6. Competências Digitais em Informática: Microsoft Outlook**	6 horas	1 - Enviar e receber mensagens de correio eletrónico; 2 - Criar listas de contactos; 3 - Gerir as pastas de correio; 4 - Utilizar o calendário como agenda;	Dirigentes, Técnicos Superiores, Coordenadores Técnicos, outras Chefias Administrativas e Assistentes Técnicos (Nível I a VI)	Não aplicável	Plataforma Online: NAU	MOOC - disponível entre 06-05 e 30-06-2025

[3] Informação mais detalhada concernente ao programa deste Curso pode ser acedida através da página web especificamente criada para o projeto formativo DigicAP (https://dtim.pt/digicap/) que possibilita o ingresso direto para a área adstrita a cada Curso MOOC na plataforma NAU.

[3] **23 – Curso DigiCAp 7. Competências Digitais em Informática: Power BI**	6 horas	1 - Identificar as potencialidades do Power BI; 2 - Importar e transformar dados de diferentes fontes; 3 - Criar visualizações e *dashboards* simples;	Dirigentes, Técnicos Superiores, Coordenadores Técnicos, outras Chefias Administrativas e Assistentes Técnicos (Nível I a VI)	Não aplicável	Plataforma Online: NAU	MOOC - disponível entre 06-05 e 30-06-2025
[3] **24 – Curso DigiCAp 8. Acessibilidade Web: Criar Conteúdos para Todos**	6 horas	1 - Reconhecer as diretrizes de acessibilidade para conteúdo web; 2 - Aplicar normas de acessibilidade na criação de conteúdos digitais; 3 - Utilizar verificadores de acessibilidade,	Dirigentes, Técnicos Superiores, Coordenadores Técnicos, outras Chefias Administrativas e Assistentes Técnicos (Nível I a VI)	Não aplicável	Plataforma Online: NAU	MOOC - disponível entre 06-05 e 30-06-2025

[3] Informação mais detalhada concernente ao programa deste Curso pode ser acedida através da página web especificamente criada para o projeto formativo DigicAP (https://dtim.pt/digicap/) que possibilita o ingresso direto para a área adstrita a cada Curso MOOC na plataforma NAU.

[3] **25 – Curso DigiCAp 9. Colaboração e Partilha de Informação no Teams**	6 horas	1 - Partilhar documentos e colaborar com o Teams; 2 - Fazer agendamento de reuniões e gerir o calendário; 3 - Configurar equipas e canais; 4 - Criar e organizar planos no Microsoft Planner;	Dirigentes, Técnicos Superiores, Coordenadores Técnicos, outras Chefias Administrativas e Assistentes Técnicos (Nível I a VI)	Não aplicável	Plataforma Online: NAU	MOOC - disponível entre 03-06 e 30-06-2025
[3] **26 – Curso DigiCAp 10. Introdução à Inteligência Artificial**	6 horas	1 - Identificar as potencialidades do uso da IA; 2 - Usar ferramentas de IA nas tarefas diárias; 3 - Identificar as limitações e desafios no uso da IA; 4 - Criar conteúdos com IA (texto, imagem, áudio e vídeo); 5 - Usar técnicas de interação com a IA (*prompt engineering*);	Dirigentes, Técnicos Superiores, Coordenadores Técnicos, outras Chefias Administrativas e Assistentes Técnicos (Nível I a VI)	Não aplicável	Plataforma Online: NAU	MOOC - disponível entre 03-06 e 30-06-2025

[3] Informação mais detalhada concernente ao programa deste Curso pode ser acedida através da página web especificamente criada para o projeto formativo DigicAP (https://dtim.pt/digicap/) que possibilita o ingresso direto para a área adstrita a cada Curso MOOC na plataforma NAU.