



PLANO DE FORMAÇÃO – 2025

Informação mais pormenorizada sobre o presente Plano de Formação consta do caderno de encargos aprovado, no âmbito do procedimento público 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, serão disponibilizadas 14 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.

REGIÃO AUTÓNOMA DA MADEIRA
GOVERNO REGIONAL
SECRETARIA REGIONAL DAS FINANÇAS
Direção Regional da Administração Pública

Em termos de modalidade a formação do presente Plano caracteriza-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.

REGIÃO AUTÓNOMA DA MADEIRA
GOVERNO REGIONAL
SECRETARIA REGIONAL DAS FINANÇAS
Direção Regional da Administração Pública

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, 8 9000-224 Funchal	12/03/2025 (4.ªfeira)

REGIÃO AUTÓNOMA DA MADEIRA

GOVERNO REGIONAL

SECRETARIA REGIONAL DAS FINANÇAS

Direção Regional da Administração Pública

		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, 8 9000-224 Funchal	19/03/2025 (4.ªfeira)

REGIÃO AUTÓNOMA DA MADEIRA
GOVERNO REGIONAL
SECRETARIA REGIONAL DAS FINANÇAS
Direção Regional da Administração Pública

		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				
--	--	---	--	--	--	--

REGIÃO AUTÓNOMA DA MADEIRA

GOVERNO REGIONAL

SECRETARIA REGIONAL DAS FINANÇAS

Direção Regional da Administração Pública

3 – Formação em Cibersegurança para Dirigentes Intermédios da Administração Pública Regional – 1ª 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, 8 9000-224 Funchal	21/03/2025 (6.ªfeira)
--	------------------	---	--	----------------------	--	----------------------------------

REGIÃO AUTÓNOMA DA MADEIRA
GOVERNO REGIONAL
SECRETARIA REGIONAL DAS FINANÇAS
Direção Regional da Administração Pública

		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.				
--	--	--	--	--	--	--

REGIÃO AUTÓNOMA DA MADEIRA

GOVERNO REGIONAL

SECRETARIA REGIONAL DAS FINANÇAS

Direção Regional da Administração Pública

		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 – 2ª 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, 8 9000-224 Funchal	28/03/2025 (6.ªfeira)

REGIÃO AUTÓNOMA DA MADEIRA
GOVERNO REGIONAL
SECRETARIA REGIONAL DAS FINANÇAS
Direção Regional da Administração Pública

		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:				
--	--	--	--	--	--	--

REGIÃO AUTÓNOMA DA MADEIRA

GOVERNO REGIONAL

SECRETARIA REGIONAL DAS FINANÇAS

Direção Regional da Administração Pública

		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.				
--	--	--	--	--	--	--

REGIÃO AUTÓNOMA DA MADEIRA
GOVERNO REGIONAL
SECRETARIA REGIONAL DAS FINANÇAS
Direção Regional da Administração Pública

5 – Formação em Cibersegurança para Dirigentes Intermédios da Administração Pública Regional – 3ª 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, 8 9000-224 Funchal	04/04/2025 (6.ªfeira)
--	------------------	---	--	----------------------	--	----------------------------------

REGIÃO AUTÓNOMA DA MADEIRA

GOVERNO REGIONAL

SECRETARIA REGIONAL DAS FINANÇAS

Direção Regional da Administração Pública

		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;				
--	--	--	--	--	--	--

REGIÃO AUTÓNOMA DA MADEIRA
GOVERNO REGIONAL
SECRETARIA REGIONAL DAS FINANÇAS
Direção Regional da Administração Pública

		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, 8 9000-224 Funchal	11/04/2025 (6.ª feira)

REGIÃO AUTÓNOMA DA MADEIRA

GOVERNO REGIONAL

SECRETARIA REGIONAL DAS FINANÇAS

Direção Regional da Administração Pública

		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:				
--	--	---	--	--	--	--

REGIÃO AUTÓNOMA DA MADEIRA
GOVERNO REGIONAL
SECRETARIA REGIONAL DAS FINANÇAS
Direção Regional da Administração Pública

		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.				
--	--	--	--	--	--	--

REGIÃO AUTÓNOMA DA MADEIRA

GOVERNO REGIONAL

SECRETARIA REGIONAL DAS FINANÇAS

Direção Regional da Administração Pública

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)
---	------------------	---	--	----------------------	--	-------------------------------

REGIÃO AUTÓNOMA DA MADEIRA
GOVERNO REGIONAL
SECRETARIA REGIONAL DAS FINANÇAS
Direção Regional da Administração Pública

		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;				
--	--	--	--	--	--	--

REGIÃO AUTÓNOMA DA MADEIRA
GOVERNO REGIONAL
SECRETARIA REGIONAL DAS FINANÇAS
Direção Regional da Administração Pública

		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, 8 9000-224 Funchal	16/05/2025 (6.ª feira)

REGIÃO AUTÓNOMA DA MADEIRA
GOVERNO REGIONAL
SECRETARIA REGIONAL DAS FINANÇAS
Direção Regional da Administração Pública

		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:				
--	--	---	--	--	--	--

REGIÃO AUTÓNOMA DA MADEIRA

GOVERNO REGIONAL

SECRETARIA REGIONAL DAS FINANÇAS

Direção Regional da Administração Pública

		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.				
--	--	--	--	--	--	--

REGIÃO AUTÓNOMA DA MADEIRA
GOVERNO REGIONAL
SECRETARIA REGIONAL DAS FINANÇAS
Direção Regional da Administração Pública

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)
---	------------------	---	--	----------------------	--	-------------------------------

REGIÃO AUTÓNOMA DA MADEIRA

GOVERNO REGIONAL

SECRETARIA REGIONAL DAS FINANÇAS

Direção Regional da Administração Pública

		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;				
--	--	--	--	--	--	--

REGIÃO AUTÓNOMA DA MADEIRA
GOVERNO REGIONAL
SECRETARIA REGIONAL DAS FINANÇAS
Direção Regional da Administração Pública

		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, 8 9000-224 Funchal	30/05/2025 (6.ª feira)

REGIÃO AUTÓNOMA DA MADEIRA

GOVERNO REGIONAL

SECRETARIA REGIONAL DAS FINANÇAS

Direção Regional da Administração Pública

		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:				
--	--	---	--	--	--	--

REGIÃO AUTÓNOMA DA MADEIRA
GOVERNO REGIONAL
SECRETARIA REGIONAL DAS FINANÇAS
Direção Regional da Administração Pública

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.

REGIÃO AUTÓNOMA DA MADEIRA

GOVERNO REGIONAL

SECRETARIA REGIONAL DAS FINANÇAS

Direção Regional da Administração Pública

²11 – Gestão da Segurança da Informação - Fundamentos da ISO/IEC 27001:2022 - 1.ª Ação	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 a aspetos organizativos, da segurança lógica e	Dirigentes, técnicos superiores, especialistas de sistemas e tecnologias de informação, técnicos de sistemas e tecnologias de informação (Nível IV, V e VI) – <u>ATENÇÃO: esta formação é dirigida apenas aos responsáveis de cibersegurança, suplentes e eventuais elementos que trabalhem exclusivamente em</u>	António Bento	Plataforma Online: Moodle	20/06 e 24/06/2025 (6.ª e 3.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 11, 12, 13 e 14. 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, conforme indicado no presente Plano de Formação.

REGIÃO AUTÓNOMA DA MADEIRA
GOVERNO REGIONAL
SECRETARIA REGIONAL DAS FINANÇAS
Direção Regional da Administração Pública

		física nas organizações, incluindo os inerentes à gestão da privacidade (dados pessoais).	<u>cibersegurança, por esse motivo não serão aceites inscrições de formandos que não cumpram com esses requisitos.</u>			
² 12 – Gestão da Segurança da Informação - Fundamentos da ISO/IEC 27001:2022 - 2.ª Ação	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.	Dirigentes, técnicos superiores, especialistas de sistemas e tecnologias de informação, técnicos de sistemas e tecnologias de informação (Nível IV, V e VI) <u>ATENÇÃO: esta formação é dirigida</u>	António Bento	Plataforma Online: Moodle	20/06 e 24/06/2025 (6.ª e 3.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 11, 12, 13 e 14. 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, conforme indicado no presente Plano de Formação.

REGIÃO AUTÓNOMA DA MADEIRA

GOVERNO REGIONAL

SECRETARIA REGIONAL DAS FINANÇAS

Direção Regional da Administração Pública

		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).	<u>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.</u>			
²13 – Gestão da Segurança da Informação -	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:	Dirigentes, técnicos superiores, especialistas de sistemas e tecnologias de	António Bento	Plataforma Online: Moodle	23/06 e 25/06/2025 (2.ª e 4.ª feira

² Por motivos imprevistos, foi necessário efetuar a substituição do formador que havia sido inicialmente designado para ministrar as ações de formação n.º 11, 12, 13 e 14. 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, conforme indicado no presente Plano de Formação.

REGIÃO AUTÓNOMA DA MADEIRA
GOVERNO REGIONAL
SECRETARIA REGIONAL DAS FINANÇAS
Direção Regional da Administração Pública

Fundamentos da ISO/IEC 27001:2022 - 3.ª Ação		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 a aspetos organizativos, da segurança lógica e física nas organizações, incluindo os inerentes à gestão da privacidade (dados pessoais).	informação, técnicos de sistemas e tecnologias de informação (Nível IV, V e VI) <u>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.</u>			– período da manhã)
--	--	--	--	--	--	----------------------------

REGIÃO AUTÓNOMA DA MADEIRA
GOVERNO REGIONAL
SECRETARIA REGIONAL DAS FINANÇAS
Direção Regional da Administração Pública

² 14 – Gestão da Segurança da Informação -Fundamentos da ISO/IEC 27001:2022 - 4.ª Ação	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) <u>ATENÇÃO: esta formação é dirigida apenas aos responsáveis de cibersegurança, suplentes e eventuais elementos que</u>	António Bento	Plataforma Online: Moodle	23/06 e 25/06/2025 (2.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 11, 12, 13 e 14. 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, conforme indicado no presente Plano de Formação.

REGIÃO AUTÓNOMA DA MADEIRA
GOVERNO REGIONAL
SECRETARIA REGIONAL DAS FINANÇAS
Direção Regional da Administração Pública

		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).	<u>trabalhem exclusivamente em cibersegurança, por esse motivo não serão aceites inscrições de formandos que não cumpram com esses requisitos.</u>			
--	--	---	--	--	--	--

REGIÃO AUTÓNOMA DA MADEIRA

GOVERNO REGIONAL

SECRETARIA REGIONAL DAS FINANÇAS

Direção Regional da Administração Pública

¹15 – 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
¹16 – 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

¹ 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.

REGIÃO AUTÓNOMA DA MADEIRA
GOVERNO REGIONAL
SECRETARIA REGIONAL DAS FINANÇAS
Direção Regional da Administração Pública

¹17 – 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
¹18 – 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

¹ 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.

REGIÃO AUTÓNOMA DA MADEIRA

GOVERNO REGIONAL

SECRETARIA REGIONAL DAS FINANÇAS

Direção Regional da Administração Pública

¹19 – 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
¹20 – 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

¹ 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 reservada a cada Curso MOOC na plataforma NAU.

REGIÃO AUTÓNOMA DA MADEIRA

GOVERNO REGIONAL

SECRETARIA REGIONAL DAS FINANÇAS

Direção Regional da Administração Pública

¹21 – 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 <i>dashboards</i> 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
¹22 – 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

¹ 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 reservada a cada Curso MOOC na plataforma NAU.

REGIÃO AUTÓNOMA DA MADEIRA
GOVERNO REGIONAL
SECRETARIA REGIONAL DAS FINANÇAS
Direção Regional da Administração Pública

¹ 23 – 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
¹ 24 – 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 (<i>prompt engineering</i>);	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

¹ 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 reservada a cada Curso MOOC na plataforma NAU.