9º CURSO GERAL DE CIBERSEGURANÇA:
UMA PERSPETIVA WHOLE-OF-SOCIETY

SYLLABUS

O Centro Nacional de Cibersegurança (CNCS) assume, no âmbito das suas atribuições, um papel central na promoção da formação e qualificação de recursos humanos na área da Cibersegurança.

Sendo a qualificação e o reforço de competências nacionais de cibersegurança determinante para a capacitação nacional, a promoção do Curso Geral de Cibersegurança: Uma perspetiva *whole-of-society* (CGC), do qual se apresenta aqui o seu *Syllabus*, tem como principal objetivo responder à necessidade de existência de uma formação holística e de curta duração neste âmbito.

1 ÍNDICE

1.1 INFORMAÇÃO GERAL DO CURSO 3

1.2 DESCRIÇÃO 3
1.2.1 OBJETIVOS 3
1.2.2 PÚBLICO-ALVO 4
1.2.3 AVALIAÇÃO E GRADUAÇÃO 4

1.3 ORGANIZAÇÃO DO CURSO - MÓDULOS 4

1.4 HORÁRIO 8

Centro Nacional de Cibersegurança

Rua da Junqueira, 69, 1300-342 Lisboa | Tel (+351) 21 049 74 00 | cncs@cncs.gov.pt

1.1 INFORMAÇÃO GERAL DO CURSO

- Local – Centro Nacional de Cibersegurança, Rua da Junqueira, 69, 1300-342 Lisboa
- Data de Início e Fim – de 17/10/2018 a 18/10/2018
- Horário – das 09h00 às 17h00
- Contactos – Tel: (+351) 210 497 400 / e-mail: formacao@cncs.gov.pt

1.2 DESCRIÇÃO

O Curso Geral de Cibersegurança (CGC) pretende, de uma forma abrangente, contribuir para a sensibilização, educação e literacia em todas as questões que caracterizam, moldam, influenciam e conduzem ao estado-da-arte atual da cibersegurança e do ciberespaço.

1.2.1 Objetivos

Pretende-se incentivar e despertar nos formandos um espírito de participação na discussão das temáticas abordadas, sensibilizando-os para a importância e atualidade das mesmas e para a necessidade de conhecer as temáticas relacionadas com a cibersegurança de uma forma holística, nas suas variadas dimensões de atuação, no ecossistema em que desenvolve e em razão dos fatores (internos e externos) que a influenciam e tornam uma realidade indiscutivelmente atual e relevante.

São objetivos particulares do CGC:

- ✓ Criar nos formandos capacidade de apoio aos processos de decisão em assuntos e matérias de/relacionados com cibersegurança;
- ✓ Desenvolver capacidades analíticas que habilitem e potenciem o apoio e desenvolvimento de estratégias organizacionais de cibersegurança mais eficazes;
- ✓ Promover a formação para uma cultura nacional de cibersegurança e promover o estudo e a investigação científica nos domínios da segurança e defesa do ciberespaço, bem como em domínios conexos.

Centro Nacional de Cibersegurança
Rua da Junqueira, 69, 1300-342 Lisboa | Tel (+351) 21 049 74 00 | cncs@cncs.gov.pt

1.2.2 Público-alvo

Quadros intermédios e superiores das estruturas do Estado e da sociedade civil, bem como de elementos com potencial para o desempenho de funções de gestão de segurança numa vertente tecnológica.

1.2.3 Avaliação e graduação

O CGC não confere qualquer grau académico ou créditos de ensino. A certificação de conclusão do curso com sucesso atesta-se mediante a entrega ao formando de um diploma. São condições para a conclusão com sucesso do CGC, a presença efetiva do formando em, pelo menos, 11 dos 12 módulos do referido Curso (sendo o exercício final de presença obrigatória).

1.3 ORGANIZAÇÃO DO CURSO - MÓDULOS

O CGC está dividido em 12 módulos:

Diretiva SRI

A necessidade de desenvolver e implementar estratégias nacionais e supranacionais, capazes de salvaguardar os interesses nacionais e proteger as infraestruturas críticas, levou ao desenvolvimento da Estratégia Nacional de Segurança do Ciberespaço (ENSC) e da Estratégia da União Europeia para a Cibersegurança, bem como a Diretiva de Segurança das Redes e da Informação (SRI).

Estas medidas de política pública de cibersegurança demonstram a necessidade de garantir a complementaridade e a segurança do ciberespaço, numa perspetiva de segurança e continuidade da atividade dos Estados, bem como numa perspetiva de defesa e integridade das nações em cenários de crise. Neste módulo é apresentado o estado da arte das políticas públicas em matéria de cibersegurança no contexto internacional e nacional e as iniciativas internacionais e regionais para a redução da conflitualidade e tensões entre Estados, resultantes do uso das tecnologias da informação e comunicação: medidas de transparência, medidas de cooperação e medidas de estabilidade.

Engenharia Social

Uma das dimensões da cibersegurança envolve os utilizadores finais das aplicações. Estes utilizadores são, frequentemente, alvo de tentativas ilegítimas de fraudes que exploram a sua maior ou menor ingenuidade. Neste

Centro Nacional de Cibersegurança

Rua da Junqueira, 69, 1300-342 Lisboa | Tel (+351) 21 049 74 00 | cncs@cncs.gov.pt

módulo são analisados alguns casos de ataques de engenharia social e como se podem preparar os utilizadores para lhes resistirem.

Cibercrime

Neste modulo são apresentados os conceitos de Ciberconflitualidade, Ciberameaças e a sua expressão multidimensional (hacktivismo, cibercrime, ciberterrorismo, ciberespionagem, ciberguerra) - aspetos teleológicos e funcionais.

Entre a legislação e convenções internacionais nesta matéria estão a convenção de Budapeste (Convenção sobre cibercrime do Conselho da Europa); a Lei do Cibercrime, a Lei de Organização da Investigação Criminal e a Lei de Segurança Interna. É também abordada a cooperação e colaboração judiciária nacional no âmbito da Interpol e Europol (European Cybercrime Centre (EC3)).

Blockchain

Abordagem à tecnologia Blockchain, às suas características, potencialidades, implementações em curso e o contributo da mesma para a segurança do ciberespaço.

A mudança de paradigma de internet da informação para a internet de valor.

ENSC 2.0

Apresentação geral da estrutura e objetivos da Estratégia Nacional de Segurança do Ciberespaço 2018-2023, que atualiza a primeira Estratégia Nacional de Segurança do Ciberespaço, aprovada pela Resolução do Conselho de Ministros n.º 36/2015, de 12 de junho. Apresentação do papel do Conselho Superior de Segurança do Ciberespaço na Estratégia de Segurança do Ciberespaço.

Ciberdefesa

Neste módulo é apresentada a Orientação Política para a Ciberdefesa e os desafios subsequentes na organização das Forças Armadas para fazer face a um novo tipo de ameaças. A capacidade nacional de Ciberdefesa (DOTMLPFI) para uma maior garantia da soberania nacional e Cooperação Internacional. O Centro de Ciberdefesa das Forças Armadas (CCD).

Centro Nacional de Cibersegurança

Rua da Junqueira, 69, 1300-342 Lisboa | Tel (+351) 21 049 74 00 | cncs@cncs.gov.pt

Direito Internacional Público aplicado ao Ciberespaço

Direito Internacional Público aplicado ao Ciberespaço: as vontades *versus* os compromissos dos Estados no palco internacional. O Direito Internacional Público enquanto instrumento regulador e de aplicação formal em espaço não regulado e tutelado.

Ecossistema da cibersegurança e Perceção situacional

Neste módulo são apresentadas as dimensões estratégica, diplomática, económica, sociocultural, legal, militar e tecnológica da cibersegurança, numa perspetiva nacional e internacional. A construção social da Cibersegurança e os seus domínios de atuação: Proteção simples, prossecução criminal, defesa do estado e diplomacia.

Atores no sistema global de regulação e desenvolvimento do ciberespaço e da Cibersegurança - uma governação multistakeholder: United Nations Group of Governmental Experts (UN GGE); World Wide Web Consortium (W3C); European Union Agency for Network and Information Security (ENISA); Interpol, Europol e o European Cybercrime Centre (EC3); International Telecommunication Union (ITU).

O ecossistema da resposta a incidentes de segurança informática é composto por processos cíclicos e incrementais de aquisição, processamento e produção de conhecimento. O Conhecimento Situacional nacional é baseado na convergência de planos interdependentes de maturidade, de âmbito nacional, setorial e organizacional.

Ciber(in)segurança

Neste módulo será apresentada uma perspetiva prática de algumas tipologias comuns de incidentes de segurança informática. Apresentando a metodologia de um ciberataque (a sua infraestrutra ofensiva) e explicando/exemplificando cada uma das suas fases, pretende-se sensibilizar e demonstrar aos formandos a forma adequada de defesa perante os incidentes em demonstração.

Os incidentes apresentados materializam a tipologia de incidentes comuns aos utilizadores e que os afetam no seu ambiente profissional e pessoal, considerando a interdependência existente entre os mesmos.

Ciberterrorismo e ciberespionagem

Neste módulo é abordada a Estratégia Nacional de Combate ao Terrorismo (ENCT), incluindo questões como: fundamentalismos, nacionalismos e deterioração do desenvolvimento da ação dos Estados, capacidades e

Centro Nacional de Cibersegurança

Rua da Junqueira, 69, 1300-342 Lisboa | Tel (+351) 21 049 74 00 | cncs@cncs.gov.pt

assimetrias sociais, tecnológicas e ideológicas; o redesenho de fronteiras e a emergência dos novos atores - Estados de facto, Estados de jure e o indivíduo enquanto ator internacional.

Boas práticas para a segurança da informação, dos sistemas e das infraestruturas

Através deste módulo pretende-se realçar um conjunto de ameaças relevantes à segurança da informação nas organizações, complementadas, sempre que possível, com exemplos de incidentes recentes, suas causas e efeitos.

Adicionalmente, e focando aspetos como as palavras-passe, o correio eletrónico, as ligações USB, as redes sem fios e os dispositivos móveis, serão abordadas boas práticas e técnicas preventivas com o objetivo de incrementar a segurança da informação, visando igualmente questões mais genéricas relacionadas com a proteção dos seus sistemas e infraestruturas.

Internet das coisas (IoT)

Atualmente é fundamental compreender os conceitos inerentes à Internet das Coisas (IoT), a combinação das informações de dispositivos e sistemas e a abordagem à conetividade em rede em um ecossistema IoT. Este módulo compreende alguns desses conceitos e aborda o tema de forma abrangente.

Exercício

Condução, pelos formandos, de um exercício de aplicação dos conhecimentos transmitidos, perante um cenário definido.

Centro Nacional de Cibersegurança

Rua da Junqueira, 69, 1300-342 Lisboa | Tel (+351) 21 049 74 00 | cncs@cncs.gov.pt

1.4 HORÁRIO

	17/10/2018	18/10/2018
09h00 09h10	**ABERTURA** António Gameiro Marques (Autoridade Nacional de Segurança)	
09h10 09h50	**Diretiva SRI** Ana Geraldes (CNCS)	**Ecossistema da cibersegurança e Perceção situacional** Lino Santos (Coordenador CNCS)
09h50 10h40	**Engenharia Social** Rogério Raposo (Coordenador CERT.PT)	**Ciber(in)segurança** Ivo Vacas (CNCS)
	Coffee Break	Coffee Break
11h00 11h50	**Cibercrime** Rogério Bravo (PJ)	**Ciberterrorismo e ciberespionagem** Júlio César (CNCS)
11h50 12h50	**BlockChain** Agostinho Valente (GNS)	**Boas práticas para a segurança da informação, dos sistemas e das infraestruturas** Nuno Fernandes (CNCS)
	Almoço	Almoço
14h00 14h50	**ENSC 2.0** António Gameiro Marques (Autoridade Nacional de Segurança)	**Internet das coisas (IoT)** António Gameiro Marques (Autoridade Nacional de Segurança)
	Coffee Break	Coffee Break
15h10 16h00	**Ciberdefesa** Fialho de Jesus (Centro de Ciberdefesa)	**EXERCÍCIO** Daniela Santos (CNCS) Pedro Vian (CNCS)
16h00 16h50	**Direito Internacional Público aplicado ao Ciberespaço** Alexandre Leite (CNCS)	**EXERCÍCIO** Daniela Santos (CNCS) Pedro Vian (CNCS)
16h50 17h00		**FECHO** Lino Santos (Coordenador CNCS)

Programa sujeito a alterações.

Centro Nacional de Cibersegurança

Rua da Junqueira, 69, 1300-342 Lisboa | Tel (+351) 21 049 74 00 | cncs@cncs.gov.pt