

8º 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

1.1 INFORMAÇÃO GERAL DO CURSO

- Local – Centro Nacional de Cibersegurança, Rua da Junqueira, 69, 1300-342 Lisboa
- Data de Início e Fim – de 3/07/2018 a 4/07/2018
- 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.

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 e ENSC

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

Políticas públicas de cibersegurança: a complementaridade e necessidade de segurança do ciberespaço, numa perspetiva de segurança e continuidade da atividade dos Estados, e também numa perspetiva de defesa e integridade das nações em cenários de crise; o estado da arte das políticas públicas em matéria de cibersegurança no contexto internacional e nacional; 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.

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.

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

Através de uma breve demonstração centrada no comportamento individual, mas focando igualmente alguns aspetos mais genéricos relacionados com a proteção dos sistemas e das infraestruturas, pretende-se abordar um conjunto de técnicas preventivas que visam melhorar a segurança da informação nas organizações.

Ciberterrorismo e ciberespionagem

Estratégia Nacional de Combate ao Terrorismo (ENCT); fundamentalismos, nacionalismos e deterioração do desenvolvimento da ação dos Estados; capacidades e 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.

Painel de Desafios

Painel dedicado a dúvidas e, onde, num espírito de colaboração e debate, serão colocados alguns desafios com base no conteúdo já lecionado.

Capacitação nacional

Capacitação nacional através dos Modelos de Maturidade de Reação, Detecção, Prevenção de ciberincidentes - conhecer, avaliar, evoluir e partilhar: uma aproximação coerente e compreensiva da maturidade organizacional para a cibersegurança.

Modelo de Governance: responsabilidades, normas, procedimentos e decisões que contextualizam, definem e materializam a cibersegurança, no estado em que a mesma se encontra a cada momento.

Exercícios nacionais e internacionais, testar processos e conhecimentos.

Standards, modelos conceptuais de segurança da informação, vantagens de aceitação de critérios de responsabilidade de acreditação e modelos de certificação.

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.

Ecosistema da cibersegurança e Perceção situacional

As dimensões estratégica, diplomática, económica, sociocultural, legal, militar e tecnológica da cibersegurança; numa perspetiva nacional e internacional. 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 informáticos: Processos cíclicos e incrementais de aquisição, processamento e produção de conhecimento. O Conhecimento Situacional nacional 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 infraestrutura 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.

Ciberdefesa

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).

Internet das coisas

Atualmente é fundamental compreender os conceitos inerentes à Internet das Coisas (IoT), a combinação das informações de dispositivos e sistemas e a abordagem à conectividade em rede em um ecossistema IoT.

Cibercrime

Ciberconflitualidade, Ciberameaças e a sua expressão multidimensional (hacktivismo, cibercrime, ciberterrorismo, ciberespionagem, ciberguerra) - aspetos teleológicos e funcionais.

A convenção de Budapeste (Convenção sobre cibercrime do Conselho da Europa); Cibercrime e cibercrime organizado: aspetos teleológicos e funcionais - Lei do Cibercrime, Lei de Organização da Investigação Criminal e Lei de Segurança Interna; a cooperação e colaboração judiciária nacional no âmbito da Interpol e Europol (European Cybercrime Centre (EC3)).

Exercício

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

1.4 HORÁRIO

3/07/2018		4/07/2018
09h00	ABERTURA	
09h10	CALM António Gameiro Marques (Autoridade Nacional de Segurança)	
09h10	Diretiva SRI e ENSC	Ecosistema da cibersegurança e Perceção situacional
09h50	Ana Geraldès (CNCS)	MAJ Rogério Raposo (Coordenador CERT.PT)
09h50	BlockChain	Ciber(in)segurança
10h40	TCOR Agostinho Valente (GNS)	André Garrido (CNCS) Duarte Sousa (CNCS)
Coffee Break		Coffee Break
11h00	Ciberterrorismo e ciberespionagem	Ciberdefesa
11h50	Júlio César (CNCS)	CFR Fialho de Jesus (Centro de Ciberdefesa)
11h50	Capacitação nacional	Internet das coisas (IoT)
12h50	Catarina Sousa Rego (CNCS)	CALM António Gameiro Marques (Autoridade Nacional de Segurança)
Almoço		Almoço
14h00	Painel de Desafios	Cibercrime
14h50	CALM António Gameiro Marques (Autoridade Nacional de Segurança) Eng. Lino Santos (Coordenador CNCS)	Rogério Bravo (PJ)
Coffee Break		Coffee Break
15h10	Boas práticas para a segurança da informação, dos sistemas e das infraestruturas	EXERCÍCIO
16h00	Nuno Fernandes (CNCS)	Catarina Sousa Rego (CNCS) Pedro Vian (CNCS)
16h00	Direito Internacional Público aplicado ao Ciberespaço	EXERCÍCIO
16h50	Ana Geraldès (CNCS)	Catarina Sousa Rego (CNCS) Pedro Vian (CNCS)
16h50		FECHO
17h00		Eng. Lino Santos (a confirmar)

Programa sujeito a alterações.