5º 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

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 17/10/2017 a 18/10/2017
- Horário – das 09h00 às 17h00
- A entrada nas instalações deve ser efetuada 30 minutos antes do início da 1.ª sessão do dia.
- 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 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.

Governação da Internet

Desenvolvimento e aplicação, pelos Estados, pelo setor privado e pela sociedade civil, no âmbito das suas responsabilidades, das normas, procedimentos e decisões que definem a Internet como a mesma é, a cada momento.

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

Este módulo irá abordar os conceitos: Neutralidade da Internet, Internet Corporation for Assigned Names and Numbers (ICANN), Internet Governance Forum (IGF) e Internet Society (ISOC).

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.

Ecossistema da cibersegurança

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).

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.

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

Centro Nacional de Cibersegurança

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

Capacitação nacional

Capacitação nacional através dos Modelos de Maturidade de Reação, Deteção, 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.

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.

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.

Perceção situacional

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.

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.

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

	17/10/2017	18/10/2017
09h00 – 09h50	**ABERTURA** CALM António Gameiro Marques (Autoridade Nacional de Segurança), Pedro Veiga (Coordenador CNCS)	**Capacitação nacional** Catarina Sousa Rego (CNCS)
09h50 – 10h40	**Diretiva SRI e ENSC** Ana Geraldes (CNCS)	**Perceção situacional** Rogério Raposo (CNCS - Coordenador CERT.PT)
	Coffee Break	Coffee Break
11h10 – 12h00	**Governação da Internet** Pedro Veiga (Coordenador CNCS)	**Ciber(in)segurnça** André Garrido (CNCS)
12h00 – 12h50	**Painel de Desafios** CALM António Gameiro Marques (Autoridade Nacional de Segurança), Pedro Veiga (Coordenador CNCS)	**Boas práticas para a segurança da informação, dos sistemas e das infraestruturas** Nuno Fernandes (CNCS)
	Almoço	Almoço
14h00 – 14h50	**Ecossistema da cibersegurança** Gonçalo Silva (CNCS)	**Direito Internacional Público aplicado ao Ciberespaço** Alexandre Leite (CNCS)
	Coffee Break	Coffee Break
15h10 – 16h00	**Ciberterrorismo e ciberespionagem** Júlio César (CNCS)	**EXERCÍCIO** Manuel Barros (ANACOM – Diretor), Pedro Veiga (Coordenador CNCS)
16h00 – 16h50	**Engenharia Social** Pedro Veiga (Coordenador CNCS)	**EXERCÍCIO** Manuel Barros (ANACOM – Diretor), Pedro Veiga (Coordenador CNCS)
16h50 – 17h00		**FECHO** Pedro Veiga (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