MASTER PROGRAM

A (IN) SEGURANÇA DA INFORMAÇÃO NA SAÚDE

4 FEVEREIRO 2022

apcer education & training

P O R Q U Ê O MAS T E R P R O G R A M
A SEGURANÇA DA INFORMAÇÃO NA SAÚDE?

A segurança dos sistemas de suporte à prestação de cuidados médicos é colocada à prova todos os dias. Facilmente são identificadas dezenas de ameaças, que exploram diversas vulnerabilidades associadas à presença de pessoas, equipamentos, pela necessidade de partilha de dados que são privados e sensíveis por natureza.

Os dados de pacientes, fármacos e tratamentos utilizados, entre muitas outras informações disponíveis nos sistemas em uso na saúde, são destino de ataques diários internacionalmente. Representam risco para a credibilidade do setor, danos tangíveis e intangíveis para as entidades e profissionais envolvidos, e uma fonte de receita apetecível para atacantes profissionais.

Este curso de especialização avançada dirige-se a profissionais de saúde que têm interesse e necessidade de compreender este ambiente de (in)segurança e, como corolário, apoia as organizações na implementação de controlos de segurança adequados para cada caso.

Este curso será ministrado totalmente online, com sessões síncronas, numa plataforma de e-learning.

COORDENAÇÃO CIENTÍFICA-PEDAGÓGICA

Dora Gonçalo (APCER)
Diretora do Curso

Unit Leader – APCER Education & Training. Docente e Formadora. Coach. Oradora. Auditora. Membro da Comissão de Coordenação do curso de Pós-Graduação em Gestão da Qualidade em Saúde (parceria APCER/Católica-Instituto de Ciências da Saúde). Membro da Comissão Científico-Pedagógica do Curso de Técnico Superior em Gestão de Segurança e Saúde no Trabalho (parceria APCER/UNAVE-Universidade de Aveiro). Licenciatura em Engenharia Química-FCTUC. Mestre em Engenharia do Ambiente-FEUP. Master Executive em Gestão de Recursos Humanos e MBA em Gestão-UCP Porto. Licensed Coaching Practitioner. Anteriormente, desenvolveu atividade profissional como Diretora (Executiva-Certificação, Certificação e Auditores, Auditores e Formação, Comercial e Operações), Coordenadora e Gestora de Cliente também na APCER. Foi também Gestora de Projetos/Consultora/Técnica na AEP-Associação Empresarial de Portugal e Engenheira de Processos na NESTE-Produtos Químicos (atual REPSOL-Complexo Industrial de Sines).

Joana Freitas (APCER)
Coordenadora Pedagógica

Manager - APCER Education & Training. Coordenadora de Formação. Auditora Coordenadora da APCER e Formadora de Sistemas de Gestão da Qualidade. Membro da Comissão de Coordenação do Curso de Pós-Graduação em Gestão da Qualidade em Saúde (parceria APCER/Católica-Instituto de Ciências da Saúde). Docente da Pós-Graduação em Gestão da Qualidade, Ambiente e Segurança-ISEP. Membro da Comissão Técnica CT187, ISO 21001 - Educational Organizations Management Systems. Mestranda em Engenharia de Serviços e Gestão-FEUP. Especialização em Gestão Industrial-AEP. Especialização em Engenharia e Gestão Ambiental (Parceria IEP/FEUP). Licenciatura em Engenharia Química-FEUP. Anteriormente desenvolveu atividade profissional como Comercial/Business Manager na Unidade de Educação e Formação da APCER e de Gestora de Cliente da Unidade de Certificação da APCER.

COORDENAÇÃO CIENTÍFICA-PEDAGÓGICA

Paulo Borges
Coordenador Pedagógico e Formador

Mais de 35 anos de experiência no mercado das Tecnologias da Informação, 16 deles em paralelo com atividades e Projetos em Angola, Brasil, Marrocos, Cabo Verde e outras zonas de África.
Lead Auditor das normas ISO/IEC 27001 (Gestão da Segurança da Informação), ISO 22301 (Continuidade de Negócio), ISO/IEC 20000 (Gestão de Serviços) e ISO/IEC 27032 (Gestão de Cibersegurança), com dezenas de projetos implementados e certificados.
Consultor, Auditor interno, CISO e DPO de várias empresas nacionais e internacionais em matérias de segurança, tecnologias da informação, criptografia aplicada, continuidade de negócio e proteção de dados pessoais.
Auditor de credenciação ISO/IEC 27001 e ISO/IEC 20000 qualificado pela APCER.
Auditor Coordenador eIDAS qualificado pela APCER para serviços de confiança digital. Auditor de segurança credenciado pelo Gabinete Nacional de Segurança para o sector de atividade das PECP - Plataformas eletrónicas de contratação pública.
Acreditado pelo "The UpTime Institute" como ATS desde Setembro de 2011, e como AOS desde Abril de 2017. Experiência comprovada no desenho, gestão de projeto, comissionamento de obra e operacionalização e gestão do processo de certificação de Datacenters em Tier II, Tier III e Tier IV em várias regiões do mundo.
Membro individual do "The Green Grid".
Membro individual do "Bicsi - Building Industry Consulting Service International".
Membro individual da "Blockchain Alliance".
Professor convidado do INPT - *Institut National des Postes et Télécommunication* de Rabat, Marrocos, para lecionar em mestrados e pós-graduações em matérias de Cibersegurança, Criptografia aplicada e infraestruturas Datacenter.

FORMADORES

Liliana Mota
Formadora

Professora Adjunta na Escola Superior de Saúde Norte da Cruz Vermelha Portuguesa (ESS Norte CVP). Presidente do Conselho Pedagógico da ESS Norte CVP e Coordenadora Científica da Unidade de Investigação e Desenvolvimento da ESS Norte CVP. Editor-Chefe da Revista de Investigação & Inovação em Saúde. Investigadora integrada no CINTESIS. Doutora em Ciências de Enfermagem pelo Instituto Ciências Biomédicas Abel Salazar da Universidade do Porto. Mestre em Informática Médica pela Faculdade de Medicina da Universidade do Porto. Mestre em Enfermagem Médico-Cirúrgica pela Escola Superior de Enfermagem do Porto. Exerceu funções, enquanto enfermeira, no Centro Hospitalar e Universitário do Porto, tendo sido interlocutora da Qualidade e Sistemas de Informação.

P R O G RAMA CURRICULAR

São 5 as unidades curriculares (UC) que estão na base deste *Master Program* que, sendo um curso modular, permite a inscrição para todos os módulos ou para módulos específicos.

As duas primeiras UC abordam a definição do que são dados, informação e sistemas de gestão na área da Saúde, utilizando uma linguagem oriunda e praticada pelos profissionais do setor. As restantes direcionam-se para a identificação de ameaças, vulnerabilidades, riscos e casos práticos de ataques e métodos de defesa para proteção das organizações profissionais e dos pacientes como cidadãos.

Serão apresentadas normas, sistemas de gestão, boas práticas, casos de sucesso na implementação e eventual certificação destes modelos de gestão para a segurança da informação, e dos dados pessoais potencialmente expostos e indevidamente utilizados por profissionais do mundo do crime em todo o mundo.

A temática da Cibersegurança é incluída não numa abordagem puramente tecnológica, mas sim como uma ferramenta de gestão e proteção das organizações, dos seus colaboradores e de todos os envolvidos nos processos clínicos.

PROJETO BUSINESS CASE

Cada aluno terá de desenvolver e apresentar um trabalho de desenvolvimento temático com aplicação prática, que constitui um método de aprofundamento dos conhecimentos adquiridos.

UNIDADES CURRICULARES

UC 1 - Sistemas de Informação na Saúde - 12 horas

Objetivos Gerais

- Compreender a importância da gestão, organização e tratamento da informação nos Sistemas de Saúde;
- Analisar criticamente os Sistemas de Informação em Saúde;
- Identificar as componentes específicas da documentação nos registos eletrónicos em Saúde;
- Compreender a problemática do acesso aos dados em saúde;
- Relacionar a avaliação dos sistemas de informação com a política de garantia da qualidade dos cuidados;
- Incorporar a melhor evidência disponível e os "standards em uso" na avaliação dos sistemas de informação.

Conteúdo Programático

1. Desenvolvimento e implementação de sistemas de informação
2. Ontologias e terminologias
3. Registos de saúde eletrónicos
4. Avaliação de sistemas de informação

Calendário

- 4 fevereiro (14h00-20h00)
- 11 fevereiro (14h00-20h00)

UC 2 – A Segurança da Informação na Saúde – 12 horas

Objetivos Gerais

- Conhecer e implementar um sistema de gestão que permite apoiar a gestão hospitalar na definição de compromissos, implementação de controlos operacionais e para a supervisão da eficácia da segurança da informação.
- Como implementar o RGPD e os seus requisitos?
- Como integrar o RGPD no contexto de um sistema de gestão da segurança da informação.

Conteúdo Programático

1. O significado de informação .... e da segurança da informação
2. Porquê (in)segurança da informação?
3. Significado de Confidencialidade – Privacidade – Integridade – Disponibilidade – Não repúdio
4. Interpretação e aplicação da norma ISO 27001 e 27002
5. O que representa a norma ISO 27799 Health informatics — Information security management in health using ISO/IEC 27002?
6. A implementação de um SGSI – Sistema de Gestão da Segurança da Informação
7. O impacto do RGPD na segurança da informação e no sector da Saúde em particular
8. Implementação RGPD com suporte da Segurança da Informação com recurso à norma ISO 27701
9. Casos de sucesso na Saúde

Calendário

- 18 fevereiro (14h00-20h00)
- 25 fevereiro (14h00-20h00)

UC 3 – Gestão da Informação nas Organizações de Saúde – 12 horas

Objetivos Gerais

- Usar ferramentas de processamento de informação, no suporte à prática e à tomada de decisão na saúde;
- Delimitar os elementos centrais de um Resumo Mínimo de Dados (RMD);
- Identificar as oportunidades associadas aos RMD no âmbito da governação em saúde.

Conteúdo Programático

1. Resumo mínimo de dados
2. Sistemas de apoio à tomada de decisão
3. Integração dos sistemas de informação

Calendário

- 4 março (14h00-20h00)
- 11 março (14h00-20h00)

UC 4 - Normas e Boas Práticas de Segurança na Saúde - 12 horas

Objetivos Gerais

- Conhecer os sistemas de certificação dos sistemas de gestão da informação na saúde;
- Conhecer as componentes mais relevantes que deverão ser operacionalizadas para a gestão da segurança da informação e de dados privados sensíveis;
- Compreender, definir, decidir e implementar práticas de forma eficaz de controlos de segurança;
- Como operacionalizar controlos de segurança da informação e da privacidade dos dados pessoais.

Conteúdo Programático

1. O que são "boas práticas"?
2. O papel das normas, regulamentação e legislação no setor da Saúde
3. Uma abordagem preliminar aos requisitos da HIMSS, *Joint Commission*, NIST, ISO entre outras para a segurança da informação na saúde
4. A origem das "boas práticas" e a utilização prática da norma ISO 27799
5. Políticas, processos e procedimentos de segurança
6. Gestão do Risco
7. Gestão de Incidentes
8. Gestão da Continuidade de Negócio
9. Controlos de segurança da informação e privacidade de dados pessoais
10. A implementação eficaz de controlos de segurança da informação e da privacidade de dados pessoais

Calendário

- 18 março (14h00-20h00)
- 25 março (14h00-20h00)

UC 5 - Ciberespaço, Cibersegurança, Ataques e Defesas na Saúde - 12 horas

Objetivos Gerais

- Compreender o significado de Ciberespaço e que ameaças representa a sua ligação com a Internet, a Darknet e os ataques de "ransomware";
- Identificar ameaças, e preparar proteções eficazes para diminuir a probabilidade e impacto de ataques;
- Conhecer a correta definição e operacionalização de Cibersegurança.

Conteúdo Programático

1. A origem do Ciberespaço
2. A necessidade de Cibersegurança – Deep Web, Darknet e conceitos associados
3. Como gerir e implementar Cibersegurança?
4. O papel do NIST e da ISO/IEC 27032 na implementação da Cibersegurança nas organizações
5. Vetores de ataque e métodos de defesa em Cibersegurança
6. A "kill chain" dos 15 vetores de ataque definidos pela ENISA
7. Casos práticos de ataques e consequências no setor da Saúde
8. O futuro ... agora! O uso de Blockchain em Projetos no sector da Saúde
9. Próximos passos

Calendário

- 1 abril (14h00-20h00)
- 8 abril (14h00-20h00)

LOCAL

Porto

DURAÇÃO

85 horas (60 horas aulas + 25 horas Projeto)

EXAMES

No final de cada Unidade Curricular será disponibilizado um exame de avaliação de conhecimentos, composto de 20 perguntas. Haverá lugar à possibilidade de realizar exames de recurso, entre as datas de 18 a 23 de abril de 2022.

PROJETO BUSINESS CASE

A entrega do "*Business Case*" terá de ser realizada até à data de 29 de abril de 2022.

Haverá suporte de tutoria por parte dos formadores, durante a realização desta atividade.

VALOR

Curso Completo:

Taxa de inscrição – **97,5 €** (valor a descontar no pagamento completo do curso)

Inscrição no curso completo – **975 €**

Valor de inscrição em unidade isolada – **225 €**

Exames recurso:

Valor de cada exame de recurso - **25€**

(Os valores apresentados estão isentos de IVA nos termos do nº 10 do art.º 9 do CIVA)

DESCONTOS

10% para pagamento completo antes do início do Curso;

5% para 2 inscrições da mesma organização nesta ação;

10% para 3 ou mais inscrições da mesma organização nesta ação.

Os descontos não são acumuláveis.

AVALIAÇÃO

- Avaliação Contínua;
- Observação direta de comportamentos, formulação de perguntas e resolução de exercícios práticos;
- Avaliação de conhecimentos por exame no final de cada módulo de formação;
- Projeto “Business Case”;
- Avaliação Final do *Master Program*: $\frac{\sum_1^6 UCn}{6} * 0.8 + Business\ Case * 0.2$

  (80% resultado da avaliação dos módulos + 20% classificação do *Business Case*)

CERTIFICAÇÃO DA FORMAÇÃO PROFISSIONAL

Para efeitos de qualificação, aos formandos que obtiveram uma classificação final positiva será emitido o Certificado de Formação Profissional, emitido pelo SIGO. Aos restantes formandos, será emitido um Certificado de Frequência de cada Unidade Curricular.

DATA DE INÍCIO

04 de fevereiro de 2022

CONDIÇÕES GERAIS

A inscrição na ação de formação só será considerada definitiva mediante o envio do respetivo pagamento, devendo o mesmo ser efetuado após a confirmação da realização do curso via email, pelo coordenador da ação.

É obrigatório o envio da requisição ou nota de encomenda com a identificação do(s) formando(s), sempre que aplicável.

Em caso de desistência (obrigatoriamente comunicada por escrito), os formandos pagam metade do valor das propinas, sendo aceite que o façam através do sistema de mensalidades.

A não comunicação por escrito do impedimento da presença, até 24 horas da data de início, obriga ao pagamento de 50% do valor da inscrição.

O nº de participantes para cada ação é limitado, pelo que as inscrições serão aceites por ordem de cronológica de chegada.

Regras complementares encontram-se no Regulamento de Funcionamento da Formação Inter Empresas - Condições Particulares para Cursos de Especialização Avançada.

FAÇA A SUA INSCRIÇÃO AQUI

CONTACTOS

Esclarecemos as suas questões.

Entre em contacto connosco através dos meios abaixo:

E-mail:
educacaoeformacao@apcer.pt
joana.freitas@apcer.pt

Tel:
+351 22 999 36 00
+351 96 157 81 01

apcer education & training