SEGURANÇA DA INFORMAÇÃO EM ORGANIZAÇÕES

Pós-Graduação em Cibersegurança e Informática Forense

Código: 124005

Área Cientifica Predominante: Sistemas de Informação e Inteligência Artificial

Docente: Paulo Adriano Marques Sousa Teixeira

Idioma de Instrução: Português

Regime: S2

Carga Letiva: 30h Carga Trabalho: 0h

ECTS: 6,0

Objetivos

A Unidade Curricular apresenta os conceitos e princípios no âmbito da gestão da segurança da Informacãoem Organizações.

São introduzidos os procedimentos para a gestão do risco, as boas práticas de segurança e os controlos desegurança a adoptar, baseadas na família de normas da ISO/IEC 27000 e do NIST.

Resultados da Aprendizagem

1. Desenvolver políticas de segurança, programas, e guias de implementação, de acordo com normasreconhecidas.

2. Monitorizar e avaliar a eficiência dos controlos de Cibersegurança adotados por uma organização,com o objetivo de garantir que eles proporcionam o nível de segurança desejado.

3. Esta unidade curricular tem por objetivo apresentar a abordagem à Segurança da Informação comoum processo de gestão usando, como base principal, a norma ISO/IEC 27001. No final da UC, o alunodeve ser capaz de:

Delinear uma estratégia para a Cibersegurança, realçando a visão, a missão e os objetivos, egarantindo o alinhamento com o plano estratégico da organização.

Identificar requisitos de segurança específicos dos Sistemas de Informação organizacionais, em todasas fases do seu ciclo

Realizar uma avaliação de risco e delinear os controlos de segurança para mitigar os riscosidentificados.

Conteúdos Programáticos

I- Conceitos e definic?o?es

Seguranc?a da Informac?a?o (confidencialidade, integridade e disponibilidade)

Recursos e tipos de recursos (Informac?a?o, fi?sicos e software)

Valor e criticidade dos recursos cri?ticos organizacionais

Ameac?as e tipo de ameac?as (acidentais vs. Deliberadas; internas vs. Externas)

Vulnerabilidades e as suas categorias (fraquezas no SW, HW, fi?sicas, pessoas e procedimentos) Conceito de

politicas de seguranc?a da informac?a?o

II- Conceito de SGSI.

III- Normas e standards de seguranc?a

A fami?lia de normas ISO/IEC 27000 NIST

IV- Gesta?o do Risco

Modelos de gesta?o de risco

Processo da gestão do risco

Tratamento do risco

Objetivo dos controlos

Avaliação quantitativa/qualitativa do impacto Quantificação do valor dos recursos organizacionais

V- Políticas e controlos de segurança

Controlo de acessos dos utilizadores Formação e sensibilização Controlos de segurança técnicos

Monitorização

Auditoria

Bibliografia Recomendada

- ISO/IEC 27001:2013

- NIST CSF

Métodos de Ensino e de Aprendizagem

O primeiro módulo introduz conceitos e definições utilizados no contexto da cibersegurança com ênfase nas:

Ameaças
Vulnerabilidades
Recursos críticos da organização
Impacto da eventual ocorrência de um incidente

Estes conteúdos alinham com as competências 1 e 2.

No segundo e terceiro módulos são abordados os sistemas de gestão de segurança.A gestão neste domínio assenta num modelo de Análise de Risco, e é suportada por políticas e controlos de segurança que devem ser adequados aos objetivos da organização e dos recursos que pretende proteger.Estes conteúdos alinham com as competências 2, 3, 4 e, parcialmente, 1.

O quarto módulo apresenta uma síntese das políticas e controlos de segurança a serem implementados tendo em conta a avaliação de risco realizada.É colocada ênfase na medição da eficiência desses controlos no contexto da

Política de Segurança.Estes conteúdos alinham com as competências 3, 4 e 5.

Métodos de Avaliação

A Classificação Global (CG) desta unidade curricular é obtida através de uma participação nas atividades propostas (AP) e da participação e interesse demonstrado (PI) com a seguinte ponderação:

CG = 0,2 * PI + 0,8 * AP

AP: Realização de atividades propostas. Para aprovação, é necessário ter um mínimo de 8 valores.

Avaliação em exame:

CG: obtida através da realização de um teste escrito teórico-prático.