Instituto Politécnico de Beja Escola Superior de Tecnologia e Gestão Mestrado em Engenharia de Segurança Informática Criptografia e Criptanálise Aplicadas Trabalho de Grupo de Pesquisa e Desenvolvimento

Prof. Rui Miguel Silva

9 de novembro de 2022

1. Contextualização

Este trabalho, a realizar por grupos de 3 alunos, constitui a primeira componente do trabalho de grupo desta unidade curricular e conta 25% para a nota final.

O objetivo desta componente do trabalho de grupo é que possibilitar aos alunos a extensão das matérias abordadas nas aulas relativas à Base Conceptual dos conteúdos temáticos, estimulando-se o início das atividades de pesquisa científica relativos ao estudo do estado da arte num contexto específico no domínio desta unidade curricular.

2. Prazos

O resultado do trabalho, para avaliação em Época Normal, deverá ser entregue na plataforma Moodle até ao final do dia 14 de dezembro de 2022. Os alunos que não entregarem até esta data passam para avaliação em Época de Recurso e podem entregar o resultado do trabalho igualmente na plataforma Moodle até ao final do dia 13 de janeiro de 2023. A apresentação dos trabalhos para avaliação em Época Normal será no dia 1 de fevereiro e a apresentação dos trabalhos para avaliação em Época de Recurso será no dia 15 de fevereiro.

3. Trabalho a realizar

O tema do trabalho é a "Criptografia Quântica". Pretende-se que os alunos estudem esta temática (i) com base num documento conceptual disponibilizado pelo Professor, e, (ii) com base num conjunto de\até três artigos de índole científica a identificar pelos alunos e com a concordância do Professor, devendo estes artigos ser de produção científica ou de compilação de trabalhos científicos (Surveys). Sugere-se que os alunos realizem a leitura do documento conceptual e simultaneamente pesquisem por artigos científicos relacionados com o tema; após encontrarem um conjunto de artigos deverão enviar ao Professor por mensagem privada no Moodle para que lhes possam ser indicados os artigos que deverão considerar no trabalho.

Do estudo deverá resultar um relatório com um número de palavras não muito superior a 3000, com uma estrutura definida pelos alunos, e, uma apresentação em PowerPoint ou similar. Os alunos deverão entregar o relatório e a apresentação em formatos editáveis e em formato PDF, comprimindo tudo num único ficheiro em formato ZIP e cujo nome deverá ser no seguinte formato MESI-2223-CCA-TGPD-1C-G-a-b-c.ZIP onde as letras 'a', 'b' e 'c' deverão ser os números de estudante dos alunos do grupo. A apresentação a fazer pelos alunos deverá ser preparada para um máximo de 10 minutos, após os quais se seguirá uma fase de perguntas e respostas.

4. Normas para a elaboração do relatório

Os alunos deverão seguir as normas do "Manual de Normas Obrigatórias para a Elaboração de Documentos Institucionais e Trabalhos Académicos" do Instituto Politécnico de Beja, disponível na página desta unidade curricular na plataforma Moodle.

5. Avaliação

A avaliação do trabalho será ponderada entre a apreciação do relatório e a qualidade da apresentação e defesa do trabalho pelos alunos aos professores.

Quanto à apreciação do relatório entregue pelos alunos, serão tidos em conta os seguintes critérios: (i) qualidade geral do relatório, aspetos de forma e apresentação gráfica, 20%, sendo valorizada a utilização de LaTex; (ii) estrutura e dimensão ponderada do relatório, equilíbrio entre secções considerando a sua relevância, 25%; (iii) clareza na exposição escrita, facilidade de leitura e capacidade de síntese, 30%; (iv) análise crítica, conclusões, perspetivas de futuro, impacto na economia, na ciência e na sociedade em geral, 25%.

Quanto à qualidade da apresentação e defesa feita pelos alunos, serão tidos em conta os seguintes critérios: (i) clareza e segurança na exposição, 40%; (ii) qualidade das respostas às questões colocadas, 40%; (iii) controlo de tempo e capacidade de síntese, 20%.

Boa Sorte!