

1 Descrição do Problema

Pretende-se implementar um sistema de voto eletrónico nas eleições legislativas (para a Assembleia da República), tendo como objetivo o seu uso pelo governo da República Portuguesa. Assim, os eleitores deverão escolher um dos partidos que se encontram numa dada lista, sendo também aceite uma resposta em branco, ou seja, sem que esteja escolhido qualquer partido.

De acordo com a Lei Portuguesa, é necessário garantir o anonimato das respostas ou seja, é ilegal manter um registo que identifique a opção escolhida por cada votante. Contudo, é ainda necessário garantir que cada votante só vota uma vez, sendo que a sua identificação é feita através do seu número de bilhete de identidade (BI) ou do seu número do cartão de cidadão (CC).

2 Funcionamento Pretendido

2.1 Fase 1 – Funcionamento Base

2.1.1 Servidor de Recenseamento Eleitoral (SRE)

Este servidor consulta um ficheiro de texto facilmente editável, que contém a lista de todos os eleitores. Estão presentes no ficheiro os seguintes campos:

- Número do BI ou número do Cartão do Cidadão;
- Indicação de qual cartão o eleitor está a usar;
- Código de voto (0→Não votou; 1→Já votou)

No início da votação a lista conterá todos os números dos Bis/CCs de todos os eleitores e o código *zero* à sua frente. Com o decorrer da votação os códigos de voto dos eleitores que já votaram vão sendo alterados para *um*, não sendo assim possível votarem novamente.

Este servidor é consultado pelo servidor de contagem de votos cada vez que alguém vota.

2.1.2 Servidor de Contagem de Votos (SCV)

Este servidor mantém e atualiza os seguintes contadores:

- Número de partidos que estão em disputa nestas eleições;
- Número de respostas positivas para cada um dos partidos;
- Número de respostas em BRANCO.

Este servidor recebe um voto de um terminal de recolha de votos, de seguida consulta o servidor de recenseamento eleitoral para validar o número do BI/CC e verificar se o eleitor pode votar. O voto recebido por este servidor deve ter a informação sobre o tipo de cartão usado pelo eleitor.

Podem acontecer duas situações:

- Caso o voto seja aceite:
 - Informa o servidor de recenseamento eleitoral de que o voto foi contabilizado;
 - Incrementa o contador respetivo;
 - Informa o terminal de que o voto foi contabilizado com sucesso;
- Caso o voto seja rejeitado informa desse facto o terminal de voto juntamente com o motivo da rejeição:
 - Número de BI ou CC inválido;
 - Voto já efetuado sob o mesmo número de BI ou CC;
 - Tempo para completar a operação excedido;
 - Falta de comunicação;
 - Falta do servidor SRE;
 - Falta do servidor SCV.

2.1.3 Terminais de Recolha de Votos (TRV)

É nos terminais de recolha de votos que os eleitores vêm a lista de partidos a partir da qual vão escolher um deles, inserem o seu número de BI ou CC, assinalam a sua escolha com um número de ordem/identificação do partido e submetem o voto.

De seguida o voto é enviado ao servidor de contagem de votos que responde com uma mensagem de sucesso ou insucesso da votação.

Existe um limite temporal (*timeout*) para completar a operação globalmente no terminal.

Este limite temporal é configurado inicialmente no servidor de contagem de votos e comunicado, juntamente com a pergunta, a todos os terminais de recolha de votos.

Os terminais de recolha de votos não estabelecem, nunca, qualquer comunicação com o servidor de recenseamento eleitoral.

2.2 Fase 2- Funcionamento Avançado

2.2.1 Terminal de Recolha de Informação (TRI)

Este terminal deve permitir o acesso, a um utilizador autenticado com permissões para o efeito, aos votos já contabilizados durante a votação. Para tal será necessário persistir numa estrutura predefinida, os utilizadores com tal permissão.

O TRI deve comunicar com o SCV e obter os dados lá existentes e escrever no ecrã a seguinte informação:

Partido	Nº de Votos	% de Votos
partido1	12	6
partido2	50	25
...		
brancos	6	3
TOTAL VOTOS	200	100

O SCV deve de ser alterado de forma a poder lidar com este terminal em paralelo com o TRV.

2.3 Fase 3 – Opções Extra

2.3.1 Módulo de Segurança: Cifragem dos dados comunicados

Pretende-se também avaliar a hipótese de implementar um protocolo de encriptação dos dados transmitidos entre os vários intervenientes.

2.3.2 Controlo da Concorrência e Recuperação

O ato de votar, a partir dum TRV, envolve várias sub-operações e comunicações entre os computadores $TRV \leftrightarrow SCV \leftrightarrow SRE$. Pode faltar um servidor ou uma comunicação no decorrer da operação global.

Como tal, é necessário garantir a consistência dos dados e controlar a concorrência das sub-operações através dum protocolo que garanta que caso alguma sub-operação falhe (por falta na comunicação ou no computador), então o resultado de todas as sub-operações efetuadas até então é reposto ao estado anterior (imediatamente antes do início da operação global) sem prejuízo da consistência dos dados.

Exemplos de problemas que podem ocorrer:

- Quando o BI/CC do eleitor é validado e assinalado no SRE como tendo votado, tal vai ser comunicado ao SCV. Se este SCV é desligado por alguma falha, então o protocolo deve repor o estado anterior à validação do BI/CC no SRE.
- O SCV tenta contactar o SRE e este último não responde (está desligado).

Deve ser feita uma análise das faltas possíveis de ocorrerem de acordo com a implementação feita da fase 1.

Deve basear-se nas competências adquiridas nas aulas teóricas e práticas para especificar o protocolo de controlo da concorrência englobando os três computadores comunicantes e as sub-operações envolvidas. É obrigatória a apresentação da especificação do protocolo planeado para esta fase: primitivas de serviço, formato das unidades de dados trocadas e diagramas temporais das trocas de dados.

3 Desenvolvimento do Trabalho

3.1 Implementação

As aplicações deverão ser desenvolvidas na linguagem de programação C#, recorrendo às técnicas e mecanismos lecionados nas aulas laboratoriais.

Deverão começar por desenvolver a Fase 1, só depois a Fase 2 e finalmente a Fase 3. Na Fase 3 é necessário desenvolver **apenas uma** das opções extra à sua escolha.

O código deverá ser escrito tendo em conta as regras de boa programação.

Deverá ser dada especial atenção à especificação dos protocolos de comunicação do nível aplicação entre os vários computadores intervenientes.

3.2 Relatório

O relatório deverá ser constituído por dois manuais:

3.2.1 Manual de utilizador

Este manual deverá conter todas as instruções necessárias para que um utilizador, com conhecimentos básicos de informática, possa utilizar e tirar partido da aplicação.

3.2.2 Manual técnico

No manual técnico, para além de tudo o que julgue necessário para ilustrar a arquitetura, instalação e manutenção do funcionamento da aplicação, terão de constar obrigatoriamente as seguintes secções:

- Apresentação da aplicação;
- Justificação de todas as opções de implementação;
- Arquitetura da solução;

- Descrição pormenorizada e especificação dos protocolos de comunicação desenvolvidos ao nível aplicação;
- Análise das limitações do programa;
- Anexo com código fonte comentado.

4 Critérios de Avaliação

Os trabalhos serão avaliados segundo o plano de desenvolvimento:

- Trabalhos que implementem somente a Fase 1 serão cotados até 13 valores no máximo;
- Trabalhos que implementem a Fase 1 e Fase 2 serão cotados até 17 valores no máximo;
- Trabalhos que implementem a Fase 1, Fase 2 e Fase 3 serão cotados até 20 valores.

Os valores máximos de cada componente avaliada são os seguintes:

- Manual de utilizador – 2 valores
- Manual técnico – 2 valores
- Apresentação e discussão – 3 valores
- Solução e implementação – 13 valores

À soma das parcelas atrás descritas serão subtraídas as penalizações por não cumprimento das regras e instruções descritas no ponto seguinte deste enunciado.

5 Regras e Instruções

- Cada trabalho prático deverá ser elaborado por **dois alunos** (só excecionalmente, e com a devida autorização, serão aceites grupos de três alunos e terão uma avaliação mais exigente).
- Os grupos devem ser constituídos por elementos que frequentem o mesmo horário de laboratório
- As notas dos trabalhos práticos serão atribuídas individualmente a cada um dos elementos do grupo após a discussão.

Trabalho Prático
Aplicações em Redes de Computadores
Departamento de Sistemas e Informática

2014/2015

- Todos os constituintes do Trabalho Prático deverão estar devidamente identificados com o **número, nome e turma** dos seus autores e o nome do **docente** a que se destina.
- O trabalho deverá ser entregue na plataforma Moodle até às **23h59** do dia **8 de Junho de 2015**, utilizando a opção (link) correspondente ao respetivo docente de laboratório.
- O material entregue deverá conter os ficheiros do manual técnico e manual do utilizador em formato **pdf** e as aplicações desenvolvidas (projeto compactado no formato **zip** cujo o nome do ficheiro deverá seguir a estrutura indicada:

numeroAluno1_NomeAluno1-numeroAluno2_NomeAluno2_Turma_NomeDocente

NomeAluno: PrimeiroUltimo

Turma: relativa ao horário que frequentam

NomeDocente: PrimeiroUltimo
- Os projetos entregues após a data indicada terão uma penalização de 1 valor por dia de atraso, até um máximo de 3 dias, limite a partir do qual os projetos não serão aceites.
- Não serão aceites trabalhos entregues que não cumpram na íntegra os pontos anteriores.
- Após a entrega dos trabalhos, as datas das discussões serão publicadas também na plataforma Moodle.