

Número:

Nome:

## LEIC/LERC – 2009/10

### 1º Exame de Sistemas Distribuídos

18 de Junho de 2010

**Responda no enunciado, apenas no espaço fornecido. Identifique todas as folhas.**

Duração: 2h30m

#### Grupo I [2,3v]

Considere a figura com a IDL do DCE RPC.

<pre>[   uuid(00918A0C-4D50-1C17-9BB3-92C1040B0000),   Version(1.0) ] Interface domotica {   typedef enum {     SUCESSO,     ERRO,     DISPOSITIVO_INEXISTENTE   } resultado;    typedef enum {     LUZ,     VIGILANCIA,     TERMOMETRO   } tipoOperacao;    typedef struct {     long dia;     long mes;     long ano;   } data;    typedef struct {     data dataOp;     tipoOperacao operacao;     resultado resultadoOperacao;     long idDispositivo;   } dadosOperacao;</pre>	<pre>typedef struct {     long anguloX;     long anguloY;   } coordenadas;    Idempotent resultado luz ([in] handle_t h,     [in] long id,     [in] string comando);    resultado vigiar ([in] handle_t h,     [in] long id,     [in] coordenadas orientacao);    Idempotent resultado temperatura ([in] handle_t h,     [in] long id,     [out] long *valor);    Idempotent resultado historicoOperacoes (     [in] handle_t h,     [in] long *nOperacoes,     [out, ptr] dadosOperacao log[100]); }</pre>
---	---

1. O compilador IDL do RPC é utilizado para gerar os stubs e a rotina de despacho no servidor usados pela aplicação de Domótica.

a. [0,7v] Indique as funções desempenhadas pelos stubs, pela rotina de despacho no servidor e pela runtime library.

I. Stubs


II. Rotina de despacho no servidor


III. Runtime library


- b. [0,4v] No DCE RPC, os *binding handles* podem ser usados pelos *stubs* de uma forma implícita ou explícita. Indique, justificando, as vantagens e desvantagens da utilização de binding handles implícitas versus explícitas para o programador.


2. O IDL da figura descreve várias operações disponibilizadas pelo serviço

- a. [0,4v] A operação *luz* muda o estado de um dispositivo de iluminação (o qual pode ter dois estados: ON e OFF), ligando ou desligando este (conforme o comando). É seguro invocar a operação luz mais do que uma vez no caso do pedido ser eventualmente recebido em duplicado? Justifique.


- b. [0,8v] Considere a implementação da função vigiar do serviço de Domótica:

```

resultado vigiar (long id, coordenadas orientacao)
{
    resultado result;
    if(!existeDispositivo(id))
        result= DISPOSITIVO_INEXISTENTE;
    else
        if (outBounds(orientacao))
            result=ERRO;
        else
            {
                anguloTeta = anguloTeta + orientacao.anguloX;
                anguloTilt = anguloTilt + orientacao.anguloY;
                result=SUCESSO;
            }
    return result;
}
    
```

3. Suponha que a mesma é invocada de forma distribuída através da plataforma de RPC. Considere que as variáveis `anguloTeta` e `anguloTilt` são globais e que os seus valores são ambos iguais a 10 inicialmente.

A função é invocada pelo cliente com o valor de `orientacao.X` e `orientacao.Y` unitário (de modo a que `anguloTeta = anguloTilt`).

Responda às seguintes questões indicando o valor da variável global `anguloTeta` no contexto da invocação do RPC apresentado em cada alínea.

No caso de não poder deterministicamente definir o valor indique **ND**.

Assuma que o canal de comunicação **pode perder mensagens** mas **não introduz mensagens duplicadas** (isto é, se uma mensagem `m` é enviada para o canal, ou se perde ou chega apenas uma vez).

	Semântica de invocação Talvez		Semântica de invocação pelo-menos-uma-vez	Semântica de invocação no máximo-uma-vez
O RPC retornou o resultado à aplicação cliente			O pedido foi reenviado duas vezes pelo runtime, sendo sempre executado pelo servidor mas perdendo-se sempre a resposta. Só à 3ª vez a resposta chegou ao cliente.	
O RPC retornou erro ao cliente			O RPC foi repetido 10 vezes e o servidor nunca respondeu tendo o cliente considerado que o RPC falhou	

## Grupo II [3v]

## 1. O seguinte WSDL descreve a interface de um Web Service semelhante ao RPC do Grupo I.

<pre> &lt;?xml version="1.0" encoding="UTF-8"?&gt;  &lt;definitions name="Domotica"   targetNamespace="http://exemploTesteSD.com/domotica/domotica"   xmlns:tns="http://exemploTesteSD.com/domotica/domotica"   xmlns="http://schemas.xmlsoap.org/wsdl/"   xmlns:xsd="http://www.w3.org/2001/XMLSchema"   xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/"&gt;  &lt;types&gt;   &lt;xsd:schema elementFormDefault="qualified"     targetNamespace="http://exemploTesteSD.com/domotica/domotica"&gt;     &lt;xsd:simpleType name="Resultado"&gt;       &lt;xsd:restriction base='xsd:string' &gt;         &lt;xsd:enumeration value="SUCESSO" /&gt;         &lt;xsd:enumeration value="ERRO" /&gt;         &lt;xsd:enumeration value="DISPOSITIVO_INEXISTENTE" /&gt;       &lt;/xsd:restriction&gt;     &lt;/xsd:simpleType&gt;     &lt;xsd:simpleType name="TipoOperacao"&gt;       &lt;xsd:restriction base='xsd:string' &gt;         &lt;xsd:enumeration value="LUZ" /&gt;         &lt;xsd:enumeration value="VIGILANCIA" /&gt;         &lt;xsd:enumeration value="TERMOMETRO" /&gt;       &lt;/xsd:restriction&gt;     &lt;/xsd:simpleType&gt;     &lt;xsd:complexType name="Data"&gt;       &lt;xsd:sequence&gt;         &lt;xsd:element name="dia" type="xsd:long"/&gt;         &lt;xsd:element name="mes" type="xsd:long"/&gt;         &lt;xsd:element name="ano" type="xsd:long"/&gt;       &lt;/xsd:sequence&gt;     &lt;/xsd:complexType&gt;     &lt;xsd:complexType name="Coordenadas"&gt;       &lt;xsd:sequence&gt;         &lt;xsd:element name="anguloX" type="xsd:long"/&gt;         &lt;xsd:element name="anguloY" type="xsd:long"/&gt;       &lt;/xsd:sequence&gt;     &lt;/xsd:complexType&gt;     &lt;xsd:complexType name="DadosTemperatura"&gt;       &lt;xsd:sequence&gt;         &lt;xsd:element name="resultadoOperacao"           type="tns:Resultado"/&gt;         &lt;xsd:element name="valor" type="xsd:long"/&gt;       &lt;/xsd:sequence&gt;     &lt;/xsd:complexType&gt;     &lt;xsd:complexType name="DadosOperacao"&gt;       &lt;xsd:sequence&gt;         &lt;xsd:element name="dataOp" type="tns:Data"/&gt;         &lt;xsd:element name="operacao"           type="tns:TipoOperacao"/&gt;         &lt;xsd:element name="resultadoOperacao"           type="tns:Resultado"/&gt;         &lt;xsd:element name="idDispositivo" type="tns:long"/&gt;       &lt;/xsd:sequence&gt;     &lt;/xsd:complexType&gt;     &lt;xsd:complexType name="ListaDadosOperacao"&gt;       &lt;xsd:sequence&gt;         &lt;xsd:element name="ElementoDadosOperacao"           minOccurs="0" maxOccurs="100" type="tns:DadosOperacao"/&gt;       &lt;/xsd:sequence&gt;     &lt;/xsd:complexType&gt;   &lt;/xsd:schema&gt; &lt;/types&gt;  &lt;binding name="DomoticaHTTP_B" type="tns:DomoticaPortType"&gt;   &lt;soap:binding style="rpc"     transport="http://schemas.xmlsoap.org/soap/http"/&gt;   &lt;operation name="luz"&gt;     &lt;soap:operation soapAction=""/&gt;     &lt;input&gt; &lt;soap:body use="literal"       namespace="http://exemploTesteSD.com/domotica/domotica"/&gt;     &lt;/input&gt;     &lt;output&gt; &lt;soap:body use="literal"       namespace="http://exemploTesteSD.com/domotica/domotica"/&gt;     &lt;/output&gt;   &lt;/operation&gt;   &lt;operation name="vigiar"&gt;     &lt;soap:operation soapAction=""/&gt; </pre>	<pre>     &lt;input&gt; &lt;soap:body use="literal"       namespace="http://exemploTesteSD.com/domotica/domotica"/&gt;     &lt;/input&gt;     &lt;output&gt; &lt;soap:body use="literal"       namespace="http://exemploTesteSD.com/domotica/domotica"/&gt;     &lt;/output&gt;   &lt;/operation&gt;   &lt;operation name="temperatura"&gt;     &lt;soap:operation soapAction=""/&gt;     &lt;input&gt; &lt;soap:body use="literal"       namespace="http://exemploTesteSD.com/domotica/domotica"/&gt;     &lt;/input&gt;     &lt;output&gt; &lt;soap:body use="literal"       namespace="http://exemploTesteSD.com/domotica/domotica"/&gt;     &lt;/output&gt;   &lt;/operation&gt;   &lt;operation name="historicoOperacoes"&gt;     &lt;soap:operation soapAction=""/&gt;     &lt;input&gt; &lt;soap:body use="literal"       namespace="http://exemploTesteSD.com/domotica/domotica"/&gt;     &lt;/input&gt;     &lt;output&gt; &lt;soap:body use="literal"       namespace="http://exemploTesteSD.com/domotica/domotica"/&gt;     &lt;/output&gt;   &lt;/operation&gt; &lt;/binding&gt;  &lt;message name="luzInMessage"&gt;   &lt;part name="id" type="xsd:long"/&gt;   &lt;part name="comando" type="xsd:string"/&gt; &lt;/message&gt; &lt;message name="luzOutMessage"&gt;   &lt;part name="resultado" type="tns:Resultado"/&gt; &lt;/message&gt; &lt;message name="vigiarInMessage"&gt;   &lt;part name="id" type="xsd:long"/&gt;   &lt;part name="orientacao"     type="tns:Coordenadas"/&gt; &lt;/message&gt; &lt;message name="vigiarOutMessage"&gt;   &lt;part name="resultado" type="tns:Resultado"/&gt; &lt;/message&gt; &lt;message name="temperaturaInMessage"&gt;   &lt;part name="id" type="xsd:long"/&gt; &lt;/message&gt; &lt;message name="temperaturaOutMessage"&gt;   &lt;part name="temperatura"     type="tns:DadosTemperatura"/&gt; &lt;/message&gt; &lt;message name="historicoInMessage"&gt;   &lt;part name="nOperacoes" type="xsd:long"/&gt; &lt;/message&gt; &lt;message name="historicoOutMessage"&gt;   &lt;part name="log"     type="tns:ListaDadosOperacao"/&gt; &lt;/message&gt;  &lt;portType name="DomoticaPortType"&gt;   &lt;operation name="luz"&gt;     &lt;input message="tns:luzInMessage"/&gt;     &lt;output message="tns:luzOutMessage"/&gt;   &lt;/operation&gt;   &lt;operation name="vigiar"&gt;     &lt;input message="tns:vigiarInMessage"/&gt;     &lt;output message="tns:vigiarOutMessage"/&gt;   &lt;/operation&gt;   &lt;operation name="temperatura"&gt;     &lt;input message="tns:temperaturaInMessage"/&gt;     &lt;output message="tns:temperaturaOutMessage"/&gt;   &lt;/operation&gt;   &lt;operation name="historicoOperacoes"&gt;     &lt;input message="tns:historicoInMessage"/&gt;     &lt;output message="tns:historicoOutMessage"/&gt;   &lt;/operation&gt; &lt;/portType&gt;  &lt;service name="DomoticaS"&gt;   &lt;documentation&gt;My exam one service&lt;/documentation&gt;   &lt;port name="DomoticaPort" binding="tns:DomoticaHTTP_B"&gt;     &lt;soap:address location="http://testeSD.com/ExDomWS/endpoint"/&gt;   &lt;/port&gt; &lt;/service&gt; &lt;/definitions&gt; </pre>
--	--

- a. [0,4v] Qual a semântica de execução garantida para a invocação deste web service? Justifique com base no WSDL apresentado.


- b. [0,4v] Se a base do desenvolvimento do servidor e do cliente for este documento, está a usar uma aproximação contract-first. O que seria uma aproximação implementation first? Descreva esta aproximação.


- c. [0,6v] WSDL é um documento mais completo que um IDL de RPC. Qual a informação adicional que o WSDL define?


- d. [0,6v] Na norma Web Services seria possível enviar o pedido anterior usando transporte por SMTP e Binding Style "Document" em vez de HTTP/rpc. Indique a informação que deveria ser acrescentada ao WSDL do web service, e aonde iria inserir essa informação.


2. Considere a mensagem SOAP criada durante a invocação à operação temperatura deste serviço.

- a. [0,6v] Para aceder às várias operações domésticas disponibilizadas pelo serviço de domótica o utilizador deverá estar autenticado.

Apresente as alterações que faria ao pedido, nomeadamente qual a informação a inserir na mensagem SOAP para garantir a autenticidade da mensagem, onde inserir esta informação, e como o fazer sem alterar a aplicação.


- b. [0,4v] Classifique a abordagem seguida pelo SOAP para a resolução da heterogeneidade, no que toca à estrutura das mensagens e à política de conversão dos dados. Justifique.


### Grupo III [3v]

Considere o seguinte extracto de um programa que descreve a classe GraphicalObject e a classe do programa cliente de uma aplicação de armazenamento de objectos gráficos (exemplo do livro da cadeira).

```

1  package examples.RMIShape;
2  import java.rmi.*;
3  import java.rmi.server.*;
4  import java.awt.Rectangle;
5  import java.awt.Color;
6
7  public class GraphicalObject implements Serializable{
8      public String type;
9      public Rectangle enclosing;
10     public Color line;
11     public Color fill;
12     public boolean isFilled;
13
14     public GraphicalObject(String aType, Rectangle anEnclosing,
15         Color aLine,Color aFill, boolean anIsFilled) {...}
16
17     public void setWidth(int w){
18         width = w;
19     }
20 }
21
22 public class ShapeListClient{
23     public static void main(String args[]){
24         String shapeType = "Rectangle";
25         if(args.length > 0) shapeType = args[0];          // specify Circle, Line etc
26         System.setSecurityManager(new RMISecurityManager());
27         ShapeList aShapeList = null;
28         try{
29             aShapeList = (ShapeList) Naming.lookup("//Jean.torriano.net/ShapeList");
30             System.out.println("Found server");
31             GraphicalObject g = new GraphicalObject(shapeType,
32                 new Rectangle(50,50,300,400),Color.red,Color.blue, false);
33             aShapeList.newShape(g);
34         }catch(RemoteException e) {System.out.println("allShapes: " + e.getMessage());
35     }
36 }

```

1. Na linha 29 o cliente invoca o serviço de nomes.
  - a. [0,4v] O resultado dessa invocação é uma referência para um objecto. Explique que informação está armazenada no servidor de nomes e que relação tem com a referência retornada pela função de lookup. Justifique.


- b. [0,4v] Como resultado dessa invocação é instanciado um objecto no espaço de endereçamento do cliente. Qual? Justifique a resposta


- c. [0,6v] Compare o funcionamento descrito acima com o do RPC, ilustrando os aspectos semelhantes e os que são diferentes. Indique 3 aspectos.


2. Considere a linha 33 do programa e a classe `GraphicalObject`

- a. [0,4v] O objecto `g` é usado como parâmetro da chamada ao método `newShape` do objecto `aShapeList`. Como é que é passado este objecto para o servidor? Justifique.


- b. A classe tem um método `setWidth`.

- i. [0,3v] O servidor pode invocar esse método sobre o objecto `g`? Explique como.


- ii. [0,3v] O método executar-se-á no cliente ou no servidor?

--

- iii. [0,3v] Suponha que `setWidth` é invocado com um valor diferente do especificado na criação, o objecto gráfico no cliente e no servidor ficam com os mesmos valores? Justifique.


- iv. [0,3v] Se a classe `GraphicObject` herdasse de `Remote` a resposta à alínea anterior seria a mesma? Justifique.


### Grupo IV [3v]

Considere o seguinte cabeçalho de uma mensagem http de invocação de um Web service

```
POST /ExemploHelloWS/endpoint HTTP/1.1
Host: www.server.com
Content-Type: text/xml; charset="utf-8"
Content-Length: 322
SOAPAction: ""
```

1. [0,4v] Um Web Service é invocado através do seu endpoint que genericamente é um nome que lhe está associado. Qual o endpoint deste Web Service que se pretende invocar?

--

2. [0,4v] O nome do endpoint é um URL ou um URN? Justifique com base nas propriedades dos nomes.


3. [0,4v] O nome do endpoint é heterogéneo. Quantos espaços de nomes o constituem? Justifique


4. [0,6v] O nome do endpoint não é puro.

a. Qual a principal vantagem na utilização do Web service? Justifique.


b. Qual a principal desvantagem na gestão do servidor do Web Service? Justifique.


5. [0,4v] Uma maneira de ultrapassar a limitação indicada na alínea b) é utilizar um serviço de nomes como o UDDI. Explique como, indicando o que deve ser feito pelo servidor e pelo cliente para ultrapassar a limitação referida.


6. [0,8v] Na resolução de um nome são normalmente envolvidos diversos espaços de nomes até se atingir um endereço de um objecto físico. Considere o nome hierarquico [www.server.com](http://www.server.com) e a cadeia de traduções necessária até aceder à placa de rede do servidor. Preencha a tabela seguinte, substituindo X, Y, A, B e C



Nome	Traduzido para um nome do tipo	Resolução efectuada por
<a href="http://www.server.com">www.server.com</a>	X	A
X	Y	B
Y	MAC Address	C

### Grupo V [4,2v]

Considere a seguinte função, que cifra e decifra o conteúdo de um ficheiro:

```
void cipherfile(char mode, FILE *infile, FILE *outfile, unsigned long k[]) {
    /* mode is 'e' for encrypt, 'd' for decrypt, k[] is the key.*/
    /* The same key should be used when encrypting and decrypting. */
    char ch, Text[8]; int i;
    while(!feof(infile)) {
        /* read 8 bytes from infile into Text */
        i = fread(Text, 1, 8, infile);
        if (i <= 0) break;
        /* pad last block with spaces */
        while (i < 8) { Text[i++] = ' ';}
        switch (mode) {
            case 'e':
                encrypt(k, (unsigned long*) Text); break;
            case 'd':
                decrypt(k, (unsigned long*) Text); break;
        }
        /* write 8 bytes from Text to outfile */
        fwrite(Text, 1, 8, outfile);
    }
}
```

1. Este programa usa um algoritmo de cifra (implementado pelas funções encrypt e decrypt).

c. [0,4v] Como o classifica: cifra simétrica ou assimétrica? Justifique.


d. [0,3v] Indique o nome de um algoritmo que esteja na categoria que indicou acima.

--

2. [0,6v] A função cipherfile tem uma vulnerabilidade grave, que permite a um atacante que escute textos cifrados descobrir aspectos da mensagem original, mesmo sem conhecer a chave secreta.

Explique sucintamente porquê, justificando com referências às linhas do código.


3. [1,4v] Re-implemente a função `cipherfile` para que use o método CBC.

```
void cipherfile(char mode, FILE *infile, FILE *outfile, long IV, unsigned long k[]) {
```

4. Ao início de cada dia, a Alice indica ao Bob o local secreto onde se irão encontrar. Para isso, a Alice escreve a morada secreta ( $M$ ) num ficheiro que guarda cifrado ( $C=\{M\}_k$ ) num servidor de ficheiros público (usando a função `cipherfile`), o qual o Bob posteriormente lê. Assuma que tanto a Alice como o Bob têm certificados da respectiva chave pública, emitidos por uma CA bem conhecida e confiável.
- a. [0,8v] Ambos precisam conhecer a chave  $k$ . Descreva em pseudo-código um protocolo para a Alice gerar a chave  $k$  e a entregar ao Bob de forma segura.

- b. [0,7v] Para além da mensagem cifrada  $C$ , o que deveria a Alice guardar no ficheiro de forma a oferecer ao Bob a possibilidade de verificar que a morada que lê é autêntica e íntegra?

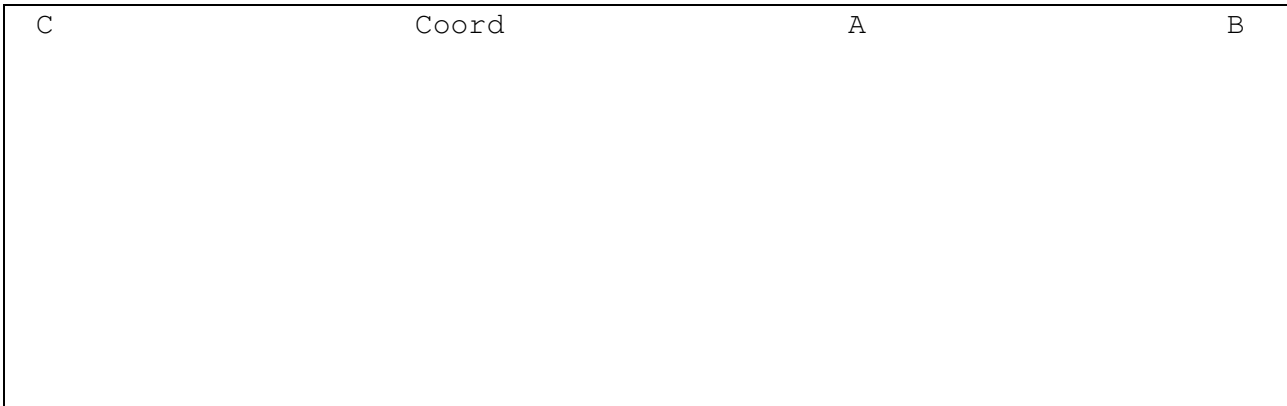

**Grupo VI [2,9v]**

1. Considere o seguinte programa que invoca procedimentos (LerSaldo e ActualizaSaldo) em servidores remotos distintos (servidor do Banco A e servidor do Banco B) no âmbito de uma transacção distribuída.

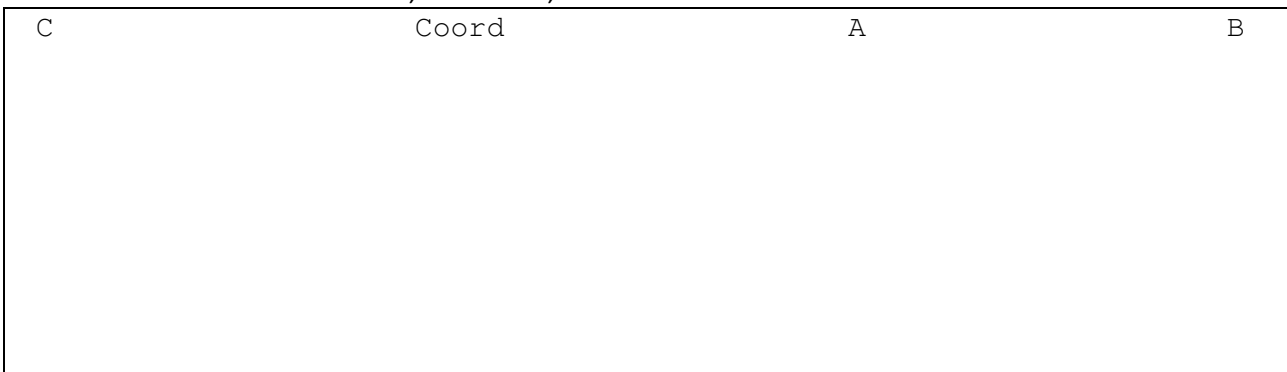
O protocolo de confirmação atómica usado é o 2-Phase Commit.

```
1 transferencia (bancoA, bancoB, Valor)
2 {
3     begin_transaction;
4     LerSaldo (bancoA, SaldoA);
5     LerSaldo (bancoB, SaldoB);
6     if (Valor > SaldoA) abort
7     else
8     {
9         ActualizarSaldo (bancoA, saldoA-Valor);
10        ActualizarSaldo (bancoB, saldoB+Valor);
11        commit;
12    }
13 }
```

- a. [0,7v] Assuma uma execução sem qualquer falha, em que a transacção distribuída é concluída com sucesso. Indique as mensagens trocadas através da rede entre o cliente C, servidor A, servidor B e coordenador Coord.



- b. [0,7v] Assuma agora uma execução em que a função *transferência* é chamada com um valor maior que o saldo da conta de origem ( $\text{Valor} > \text{SaldoA}$ ). Indique as mensagens trocadas através da rede entre o cliente C, servidor A, servidor B e coordenador Coord.



- c. [0,7v] Finalmente, assumo uma execução em que a transferência se executa com sucesso até à linha 11; no entanto, imediatamente antes do cliente executar a linha 11 (commit), o servidor B falha permanentemente. Indique as mensagens trocadas através da rede entre o cliente C, servidor A, servidor B e coordenador Coord.

C	Coord	A	B
---	-------	---	---

5. [0,4v] Na situação em que o coordenador envia a decisão aos participantes, eles devem responder a confirmar que aplicaram a decisão localmente. Porque razão esta última mensagem é necessária?


6. [0,4v] Dê dois exemplos que levem um participante a votar Não no 2PC.


### Grupo VII [1,6v]

Para tolerar faltas do Portal do Utilizador do seu projecto, instalaram-se 2 servidores secundários (para além do servidor principal) e se usava o protocolo Primary-Backup de replicação passiva.

1. [0,4v] Dê um exemplo de uma falta densa neste sistema.


2. [0,6v] “Diminuindo o período de envio de mensagens “I’m alive” (P), aumentamos a disponibilidade do sistema”. Esta afirmação é verdadeira? Justifique.


3. [0,6v] Suponha que tinha de optar entre esta solução e uma solução com replicação activa (com o mesmo número de servidores). Partindo do pressuposto de que não é expectável que falhem dois ou mais servidores simultaneamente, indique dois argumentos a favor ou contra a segunda.
