

*Este examen consta de 11 preguntas con un total de 15 puntos. Tres preguntas incorrectas restan un punto. Sólo una opción es correcta a menos que se indique algo distinto. No está permitido el uso de calculadora. La duración máxima de este examen será de 30 minutos.*

Apellidos: \_\_\_\_\_ Nombre: \_\_\_\_\_ Grupo: \_\_\_\_\_

**1** [1p] ¿Qué entendemos por servicio en un sistema distribuido?

- ☐ a) Un componente gestionando un conjunto de recursos relacionados y que provee una funcionalidad a usuarios y aplicaciones.
- ☐ b) Un programa ejecutándose en un computador que acepta peticiones de otros programas a través de un API.
- ☐ c) Un conjunto de reglas que habilita la comunicación entre dos entidades.
- ☐ d) Un conjunto de operaciones o API.

**2** [1p] En un sistema distribuido ¿qué problema resuelve el uso de sistemas abiertos y estándares?

- ☐ a) La heterogeneidad
- ☐ b) La escalabilidad
- ☐ c) La transparencia
- ☐ d) La seguridad

**3** [1p] ¿Cuál es el principal beneficio de usar un middleware?

- ☐ a) Aumento de la productividad del equipo de programación.
- ☐ b) Por usarlo, te proporciona gestión de fallos en cualquier tipo de sistema distribuido de forma automática.
- ☐ c) Por usarlo, te proporciona gestión de la escalabilidad en cualquier tipo de sistema distribuido de forma automática.
- ☐ d) Todas las otras respuestas son correctas.

**4** [1p] ¿Qué tipo de transparencia te proporciona una URL?

- ☐ a) Localización
- ☐ b) Concurrencia
- ☐ c) Fallo
- ☐ d) Prestaciones

**5** [1p] ¿Qué clases de fallos involucran al canal en un sistema distribuido?

- ☐ a) Omisión y arbitrario
- ☐ b) Arbitrario
- ☐ c) Omisión
- ☐ d) Fallo-parada

E. [5p] Usted ha sido seleccionado para diseñar un protocolo de servicio basado en cliente/servidor que debe proporcionar el siguiente conjunto de operaciones:

- *op1*: leer el número de versión de un fichero.
- *op2*: incrementar el número de versión de un fichero.
- *op3*: resetear el número de versión de un fichero.

> **6** ¿Cuál de las siguientes opciones define de manera más eficiente (mínimo mensaje necesario con el mínimo payload) la sintaxis del mensaje de petición de la operación *op2*? Considere que *x* es el número exacto de caracteres del nombre del fichero.

- ☐ a) Id. Operación (1 byte) + longitud nombre fichero (2 bytes) + nombre fichero (x bytes)
- ☐ b) Id. Operación (1 byte) + nombre fichero (512 bytes)
- ☐ c) Id. Operación (1 byte) + nombre fichero (x bytes) + carácter FIN (1 byte)
- ☐ d) Id. Operación (1 byte) + nombre fichero (x bytes) + carácter FIN (1 byte) + versión (1 byte)

> **7** Suponga que se le solicita añadir a este protocolo la característica de integridad de datos. ¿Qué campo(s) debería añadir a los mensajes para soportar dicha característica?

- ☐ a) CRC
- ☐ b) Timestamp
- ☐ c) Identificador origen/destino
- ☐ d) Versión del protocolo

> **8** ¿Cuál de las siguientes opciones es la más adecuada para representar los mensajes de petición y respuesta del protocolo utilizando Google Protocol Buffers versión 3?

a)

```
message VERSION {
    enum Operation {READ=0; INC=1; RESET=2; UNKNOWN=3;}
    Operation VersionOp = 1;
    string filename = 2;
}
message RESPONSE { int32 version= 1;}
```

c)

```
message VERSION {
    enum Operation {READ=0; INC=1; RESET=2; UNKNOWN=3;}
    required Operation VersionOp = 1;
    required string filename = 2;
    optional int version = 3;
}
```

b)

```
message VERSION {
    enum Operation {READ=0; INC=1; RESET=2; UNKNOWN=3;}
    Operation VersionOp = 1;
    string filename = 2;
    int32 version = 3;
}
```

d)

```
message VERSION {
    enum Operation {READ=0; INC=1; RESET=2; UNKNOWN=3;}
    required Operation VersionOp = 1;
    required string filename = 2;
    required int version = 3;
}
```

- ☐ a)
- ☐ b)
- ☐ c)
- ☐ d)

> **9** La herramienta *wireshark*, cuando se usa para capturar los mensajes de protocolo, no puede ayudar a:

- ☐ a) Identificar errores de sintaxis de protocolo.
- ☐ b) Reducir el tamaño de los datos enviados.
- ☐ c) Verificar las entidades que comunican.
- ☐ d) Comprobar el encapsulado de los mensajes de aplicación sobre TCP/IP.

> **10** ¿Qué indica el bit más significativo (MSB) del último byte que compone el tipo *varint* en los buffers de protocolo de Google si este byte toma el valor '0'?

- ☐ a) El signo del número representado en ese byte.
- ☐ b) Ese byte contiene información de control.
- ☐ c) El tipo de datos representado en ese byte.
- ☐ d) Es el último byte

**11** [1p] ¿Qué paradigma de comunicación se asemeja más al *paso de mensajes* (message passing)?

- ☐ a) cliente-servidor
- ☐ b) colas de mensajes
- ☐ c) propagación de eventos
- ☐ d) redes de pares (peer to peer)

**12** [1p] ¿Por qué los middlewares RPC suelen proporcionar por defecto invocaciones bloqueantes?

- ☐ a) Es más simple.
- ☐ b) Es más eficiente.
- ☐ c) Se parece más a una invocación convencional.
- ☐ d) No requiere la validación de la invocación por parte del servidor.

**13** [1p] ¿Qué proporcionan RRA que no proporcionan los otros estilos de intercambio?

- ☐ a) Fiabilidad
- ☐ b) Transparencia
- ☐ c) Retransmisión de resultados.
- ☐ d) Concurrencia a nivel de procesador

**14** [1p] ¿Cuál es la consecuencia principal de la semántica *at-least-once* en caso de error?

- ☐ a) La invocación no se realiza.
- ☐ b) Se re-ejecuta el procedimiento.
- ☐ c) Se almacena la historia de peticiones.
- ☐ d) El mensaje de respuesta indica un error.

**15** [1p] ¿A qué se refiere el concepto *binding* al realizar una invocación RPC?

- ☐ a) Al proceso que el cliente utiliza para localizar el servidor RPC.
- ☐ b) Al protocolo de bajo nivel que utiliza el cliente para codificar la petición.
- ☐ c) A la necesidad de almacenar en memoria del servidor los parámetros recibidos.
- ☐ d) Al proceso que convierte los datos que maneja la aplicación en secuencias de bytes serializables.