IEI2016/2017 – ASO&COM

Reporte de horas de trabalho nesta entrega (preenchimento obrigatório):

Grupo: 4				
Nº Aluno	**Nome Aluno**	**Pesquisa na Web**	**Reuniões Grupo**	**Elaboração Relatório**
87664	Inês Albano	01h30	03h30	03h30
87709	Viviana Bernardo	01h30	03h30	03h30

1. Questão: Com base no artigo "The Tail at Scale" identifique outro fim para a qual a redundância esteja ser utilizada na infraestrutura da Google. Justifique a resposta (mais detalhado do que é dito no artigo) sobre a forma como a Google poderá estar a utilizar a redundância para lidar com padrões diurnos (i.e., a utilização típica e repetitiva de dia para dia) das procuras que são enviadas ao serviço da Google.

A **Google** em vez de tentar eliminar toda e qualquer tipo de redundância desenvolveu técnicas que permitem "contornar" patologias informáticas relacionadas com a mesma. A empresa está a utilizar a redundância de forma a **evitar o sobrecarregamento** e a existência de **falhas no seu sistema**. Uma das técnicas aplicadas para diminuir o tempo de resposta (*latency*) é a criação de várias cópias, de documentos importantes ou que são frequentemente acedidos, em diferentes servidores espalhados pelo mundo. Isto irá permitir que os pedidos de acesso a determinados conteúdos sejam processados mais rapidamente, tornando os sistemas mais fluidos e naturais para o utilizador. Este processo permite evitar a carga computacional recebida e o sobrecarregamento dos servidores.

Através da monitorização do comportamento dos utilizadores, é possível perceber quais são os servidores mais acedidos e melhorar o seu desempenho. Como a redundância consiste na criação de dados não necessários, criam-se também réplicas de conteúdos acedidos frequentemente por parte dos utilizadores, permitindo evitar o "*overload*" dos servidores, e um grande do tempo de latência.

2. Questão: Indique dois desafios científicos e/ou tecnológicos na área de ASO relacionados com as recentes preocupações de privacidade e segurança da informação na Web.

A ASO pretende **combater as ameaças** aos bens digitais que estão ligados à internet e são utilizados diariamente e que contém informações confidenciais ou de elevada importância. Estes bens estão sujeitos a vários tipos de ameaças, como de **confidencialidade** (os dados serem acedidos por terceiros) ou de **integrabilidade** (quando ocorre a alteração dos dados).

Esta área tem como desafios proteger, através do gerenciamento seguro do *software* utilizado, os serviços disponibilizados pela ***Cloud***. Esta proteção consiste na manutenção da confidencialidade, disponibilidade e integridade dos dados. Assim, é necessário ter em consideração o desenvolvimento de um bom *software* em harmonia com um bom *hardware*. Este, tem, ainda, de estar alojado num local onde as condições ambientais não o possam afetar, pois poderia haver comprometimento dos dados (afetando, não só, mas também, a disponibilidade e integridade do servidor), ou num local onde seja promovido o arrefecimento dos sistemas - "*Power Usage Effectiveness*".

Outro desafio, é a confidencialidade dos dados fornecidos no acesso bancário via *online* – ***homebanking***. O Banco de Portugal afirma que, «(...) procura garantir, (...), a atualidade e rigor da informação e minimizar os inconvenientes causados por eventuais falhas técnicas.», tais falhas técnicas que podem ocorrer e pôr assim em risco toda a informação partilhada. Com o desenvolvimento de *softwares* cada vez mais complexos, ocorrem bugs mais difíceis de detetar e, por conseguinte, de eliminar, o que fomenta a vulnerabilidade do sistema. Tal como anteriormente, essas vulnerabilidades estão suscetíveis a serem exploradas levando à existência de falhas no sistema que podem levar ao vazamento de informação (*leaks*).

Assim, esta área científica tem como objetivos o desenvolvimento de **código seguro**, para que a informação não seja intercetada por terceiros. Para além de ter que desenvolver técnicas de programação defensivas, como a utilização de **mecanismos de criptografia**.

Fonte: http://ai.stanford.edu/users/sahami/CS2013/final-draft/CS2013-final-report.pdf

https://pt.wikipedia.org/wiki/Confidencialidade

http://www.infoworld.com/article/3041078/security/the-dirty-dozen-12-cloud-security-threats.html

http://www.lusopt.pt/portugal/1257-privacidade-e-seguranca-na-internet#

3. Questão: Elabore um mapa conceptual que evidencie quais os aspetos a reter da área científica de Computadores.