1- Risco

Pergunta 1.1

Num PC doméstico temos que o nível de ameaça é baixo e que o grau de vulnerabilidade é alto, isto porque, num PC doméstico não há, em geral, nada de importante que leve a um ataque, mas no entanto os utilizadores também não se protegem muito. O impacto que um ataque possa ter nestes computadores é baixo, uma vez que não existe informação "sensível"a ser descoberta. Com isto, podemos concluir que o risco que existe para os PCs domésticos é baixo.

Por outro lado, num servidor de *homebanking* de um Banco o nível de ameaça já é elevado, isto porque existe muita informação "sensível", mas também temos que nestas situações o grau de vulnerabilidade já é mais baixo, porque, por norma, este tipo de servidores têm melhores proteções para proteger a informação confidencial. Tendo em conta, que se houver um ataque a estes servidores o impacto que este gera é muito grande, então podemos concluir que o risco é bastante elevado.

Em conclusão, temos que o servidor de *homebanking* de um Banco está sujeito a um risco de internet mais elevado.

Pergunta 1.2

O fator da fórmula do risco que seria afetado pela descoberta e encarceramento de cibercriminosos que ameçavam a aplicação é o nível de ameaça. Este iria diminuir, porque as pessoas que conheciam as vulnerabilidades não podiam usar o seu conhecimento.

Os fatores da fómula do risco que seriam afetados se uma empresa descobri-se e remove-se as diversas vulnerabilidades da aplicação são o grau de vulnerabilidade e a probabilidade de o ataque ter sucesso. Ambos iriam diminuir, o primeiro porque deixariam de haver vulnerabilidades por onde atacar e o segundo porque sem vulnerabilidades os ataques não têm sucesso.

2- Secure Software Development Lifecycle (S-SDLC)

Pergunta 2.1

No modelo em cascata, na fase de Requisitos devem ser levados em linha de conta o regulamento europeu RGPD, porque nesta fase é onde são definidos os requisitos de segurança.

Pergunta 2.2

No modelo Microsoft Security Development Lifecycle é na fase de Requisitos que deve ser levada em linha de conta o regulamento europeu RGPD, porque é aqui que definimos os requisitos mínimos de segurança que as fazes posteriores utilizarão.

Pergunta 2.3

No SAMM deve ser levada em linha de conta o regulamento europeu RGPD, na função do negócio **Governance**, na prática de segurança **Police & Compliance** e na atividade **Build policies and standarts for security and complience**.

O nível de maturidade dessa prática de segurança onde tem de estar a empresa é no nível 2 porque só neste nível é que se encontra a atividade que trata das questões de segurança seguindo o RGPD.