 <b>TÉCNICO LISBOA</b>	<b>81115 – Rodrigo Lousada</b>
<b>FT4 – Criminalidade Informática</b>	


**1. Questão:** *Indique o que faria se estivesse na situação abaixo descrita. Sistematize a justificação da posição tomada com base no processo de decisão em 5 passos apresentado (na aula e no Capítulo 1 do livro de CS).*

O Joaquim é engenheiro informático numa *start-up* que desenvolve um novo *software* de prescrição eletrónica online para consultórios médicos. Ao chegar ao trabalho deduziu estar na presença de **malware** uma vez que ao tentar aceder à pasta com o código dos programas da versão de desenvolvimento aparece uma mensagem a pedir para transferir **2 Bitcoin** (equivalente a 1767€ <http://preev.com/btc/eur>) para um endereço. O problema consiste em perceber se o Joaquim **deve ou não alertar o seu supervisor** e se **deve fazer a transferência** tendo em conta a possibilidade da “infecção” se ter espalhado e que provavelmente descarregou inadvertidamente o malware de um site de streaming de jogos.

Deparando-nos com este problema, o Joaquim possui as seguintes alternativas:

- **Pagar** a transferência e esperar que fique tudo bem
- Ir ao último **backup** que fez do software (há 2 semanas), **reformatar o disco** do computador, repor o software e **refazer o trabalho perdido**, prometendo a si próprio que vai trabalhar horas extras para compensar
- Falar com a **equipa de segurança** da empresa e pedir que tratem do assunto discretamente
- **Contar ao supervisor** e explicar que o facto de ter ido ao site de streaming de jogos pode ter sido a causa.
- **Contar ao supervisor** e referir que não sabe como foi infetado

Ao avaliar estas alternativas lembramo-nos que a possibilidade de outros computadores estarem também afetados é igualmente grande à **probabilidade de ele ter sido infetado por outro colega** e não por algo que tenha feito. Por outro lado, pagar os 2 Bitcoins **não nos garante que termine a chantagem** feita ao Joaquim, podendo não só nunca receber o acesso à pasta como ser novamente chantageado, mais tarde, de outra forma (exs: <https://goo.gl/sNg9ti>, <https://goo.gl/BM8ODX>). Diversos especialistas recomendam não pagar nestas situações (<https://goo.gl/dgbzpz8>). Falar “às escondidas” do seu supervisor pode fazer com que o mesmo descubra por terceiros, não favorecendo a posição do Joaquim.


 <b>TÉCNICO LISBOA</b>	<b>81115 – Rodrigo Lousada</b>
<b>FT4 – Criminalidade Informática</b>	

Para as alternativas ponderadas pelo Joaquim, o seguinte quadro ilustra uma avaliação das mesmas:

	Contar ao supervisor	Reformatar disco e refazer trabalho perdido	Pagar a transferência
<b>Ética da Virtude</b>	+	+	+
<b>Utilitária</b>	Permite que toda a equipa esteja ciente da ameaça e que a mesma seja tratada por uma equipa especializada em segurança	Embora se perca algum trabalho, temos a garantia de que a máquina não está infetada. No entanto nada nos garante a segurança por parte dos restantes colegas	Nada nos garante que o problema estará resolvido, não tendo garantia da remoção do malware nem da não repetição deste acontecimento
<b>Imparcialidade</b>	+	-	-
<b>Bem Comum</b>	Trabalhar em conjunto com toda a equipa de forma a resolver o problema	Se o computador do Joaquim for único afetado. No entanto este tem de refazer o trabalho perdido	Se após o pagamento for libertado do malware e não se repetir a situação

Após a avaliação das alternativas, chegamos à conclusão que deve **ser do conhecimento do supervisor** a existência do malware e que a análise à origem do mesmo deve ser feita por parte de uma **equipa de segurança especializada**. Deve ser feita referência à utilização do site de streaming de jogos no entanto apenas como uma possibilidade a analisar por esta equipa. As **medidas a tomar devem ser decididas pelo supervisor**, incluído se pagam ou não, e se recorrem ao backup. O Joaquim deve ainda mostrar-se 100% disponível para ajudar no que for necessário e recomendar que apenas se pague a transferência mesmo em última opção.

De forma a avaliar os resultados desta decisão devemos ter em conta a **reação do supervisor** (despedimento, penalização e/ou repreensão do Joaquim) e se a **origem do malware** era de facto culpa dele. Para além disso, ter em conta as **consequências e impacto na empresa** que o malware possa ter tido, incluindo então a **rapidez da resolução da situação** (ou a existência de resolução).

 <b>TÉCNICO LISBOA</b>	<b>81115 – Rodrigo Lousada</b>
<b>FT4 – Criminalidade Informática</b>	


**2. Questão:** *Indique o que faria se estivesse na situação abaixo descrita. Sistematize a justificação da posição tomada com base no processo de decisão em 5 passos apresentado (na aula e no Capítulo 1 do livro de CS).*

Sou o novo engenheiro informático numa *start-up* que desenvolve um novo *software* de prescrição eletrónica online para consultórios médicos. Ao desenvolver a 1ª versão do *software* do que será o único produto lançado no mercado descobri que existe um “bug” conhecido da equipa que poderá afetar os utilizadores. Embora a probabilidade de o “bug” ser descoberto seja baixa, o impacto potencial nos cerca de 50 clientes que já encomendaram o produto pode ser considerável, devido à vulnerabilidade da informação sensível dos mesmos. O problema consiste em saber o que dizer ao meu supervisor sobre o problema, sabendo que:

- O problema será corrigido na próxima versão que será lançada daqui a 6 meses,
- A empresa está a negociar um financiamento de 3 milhões de euros para garantir a operação do negócio até começar a haver lucro
- O esforço necessário para desenvolver e instalar a atualização, explicar as alterações às especificações já anunciadas aos clientes e eventuais saídas da equipa poderá ser excessiva para uma equipa tão pequena, atrasando ainda a publicação da 1ª versão em pelo menos mais 3 meses

Tenhamos então as seguintes alternativas em perspetiva:

	Vantagens	Desvantagens
Pedir para <u>atrasar o lançamento</u> do produto de forma a <u>corrigir o bug</u> antes que tenha consequências para os doentes	Contenção da ameaça, garantindo a segurança dos dados dos doentes	Atraso pode ser prejudicial na negociação do financiamento
Deixar seguir e <u>corrigir o bug numa atualização posterior</u> , sendo que este tem uma baixa possibilidade de ser descoberto	Permite o início da atividade impedindo que o bug afete o negócio do financiamento	Risco de ataque informático comprometendo a informação dos doentes

 <b>TÉCNICO LISBOA</b>	<b>81115 – Rodrigo Lousada</b>
<b>FT4 – Criminalidade Informática</b>	

<u>Não contar</u> nada ao supervisor e <u>ignorar o bug</u>	Lançamento do produto não é atrasado, e pode não vir a ser descoberto o bug	Risco de outro membro da equipa contar ao supervisor no seu lugar
Propor uma <u>versão Beta</u> apenas disponibilizada para quem esteja <u>ciente do bug</u> e que esteja disposto a correr o risco.	Permite que os doentes sejam alertados da possibilidade de alguém ter acesso às suas informações, e que estes apenas se coloquem nessa situação por vontade própria.	Consciência do bug pode promover afetar a imagem do produto, afetar o financiamento

Podemos então basear a nossa decisão nesta tabela e chegar à conclusão de que a melhor solução será então **falar com o chefe** explicando a existência do bug, e considerar ou o **atraso da versão** ou o lançamento da **versão Beta**, no entanto a decisão entre as duas opções apenas afeta o financiamento a negociar, algo que **não passa pelas nossas responsabilidades**, sendo então algo a deixar para o supervisor comunicar com as entidades da empresa que sejam responsáveis por essas decisão estratégica. Assim, a segurança dos doentes é tida em conta em primeiro lugar, havendo então um esforço por parte da equipa de desenvolvimento para corrigir o bug o mais rápido possível. Sabendo que praticamente todos os produtos têm algum bug deve ser criada uma **escala que avalie (de 0-5 por exemplo) a gravidade de cada bug**, sendo então apurado duma forma científica quais os bugs que podem e quais não podem ser lançados.

De forma a avaliar o resultado da decisão tomada, deve ser tido em conta o **impacto no financiamento** pretendido, o **tempo de atraso** da versão com o bug corrigido e o número de **doentes afetados** por este atraso. Para que situações destas não se voltem a repetir deve ainda haver uma avaliação do impacto do **bug nos doentes** de forma a reavaliar os sistema de classificação na escala.

**Fontes de Informação (Não incluídas nas hiperligações anteriores):**

- <http://www.bbc.com/news/technology-35091714>
- <https://goo.gl/fG2xCV>
- <https://www.staysmartonline.gov.au/alert-service/new-malware-blackmailing-companies-and-stealing-ip>
- <https://ual-pt.academia.edu/RogérioBravo>