Exercício USB de estacionamento

Conteúdo	Escreva **2 a 3 frases** sobre os tipos de informação encontrados neste dispositivo. ● ***Existem arquivos que podem conter informações pessoais identificáveis?*** ***R.:*** *Sim, há arquivos pessoais, como por exemplo, um currículo, uma lista de casamento, fotos de família e do pet.* ● ***Existem arquivos de trabalho confidenciais?*** ***R.:*** *Sim, arquivos como o horário dos funcionários, um currículo com informações sobre um possível candidato e o orçamento dos funcionários.* ● ***É seguro armazenar arquivos pessoais junto com arquivos de trabalho?*** ***R.:*** *O pen-drive em questão deveria conter somente dados do trabalho, pois, a situação aparenta que o dispositivo é do próprio hospital.*
Mentalidade do atacante	Escreva **2 a 3 frases** sobre como essa informação poderia ser usada contra Jorge ou o hospital. ● ***As informações poderiam ser usadas contra outros funcionários?*** ***R.:*** *Sim, as informações poderiam ser utilizadas contra outros funcionários, pois contém informações sobre seus horários e possíveis orçamentos.* ● ***As informações poderiam ser usadas contra os familiares?*** ***R.:*** *Sim, pois, há informações pessoais, como as informações do casamento dos amigos Wendy e Jorge, além de fotos da família.* ● ***Será que essa informação poderia dar acesso à empresa?*** ***R.:*** *Se utilizada de forma indevida, sim, seria possível acessar a empresa com essas informações, podendo ser na forma digital, testando senhas com os nomes dos familiares, dos pets, etc ou de forma física, através de engenharia social com as informações que estão disponíveis sobre os funcionários.*

Análise de risco	Escreva **3 ou 4 frases** descrevendo os controles técnicos, operacionais ou gerenciais que poderiam mitigar esses tipos de ataques: ● ***Que tipos de software malicioso poderiam estar ocultos nesses dispositivos? O que poderia ter acontecido se o dispositivo estivesse infectado e a infecção tivesse sido descoberta por outro funcionário?*** ***R.:*** *O dispositivo em questão poderia possuir um malware do tipo worm, que no momento que ele fosse ligado em outro dispositivo, ele automáticamente iniciaria a contaminação em toda a rede, além de ser possível contaminar os arquivos que possuíssem a maior probabilidade de abertura, dessa forma iniciando mais uma infecção de dispositivo. Se o dispositivo em questão estivesse infectado e fosse utilizado por outro funcionário sem conhecimento, o dano poderia ser catastrófico, onde vários dados poderiam ser criptografados através de um ramsonware, ou diversas informações sobre pacientes e funcionários vazadas na internet.* ● ***Que informações sensíveis um agente malicioso poderia encontrar em um dispositivo como este?*** ***R.:*** *No momento, o dispositivo possuía informações sobre o horário e possíveis orçamentos dos funcionários, fora uma grande quantidade de informações pessoais do proprietário do dispositivo, como fotos da família, idéias para férias, informações sobre o casamento de amigos, etc, mas, com o uso de malwares um agente malicioso poderia invadir os sistemas da empresa e vazar ou roubar ou sequestrar os dados dos funcionários ou pacientes da empresa.* ● ***De que forma essa informação poderia ser usada contra um indivíduo ou uma organização?*** ***R.:*** *As informações pessoais presentes no dispositivo podem ser utilizadas por meio de engenharia social, dessa forma fazendo com que o proprietário seja influenciado a cair em golpes ou fraudes, já no meio profissional, as informações poderiam ser utilizadas para explorar brechas na segurança, por meio do controle de horário de funcionários.* *Para evitar que tal situação ocorresse por um UBS Bating, o ideal seria instruir os funcionários a não misturar arquivos pessoas com arquivos de trabalho, não ligar dispositivos desconhecidos nos dispositivos da empresa, além de aprimorar as defesas dos sistemas, com atualizações, um bom anti-vírus, etc.*