Parking lot USB exercise

Contents	Write **2-3 sentences** about the types of information found on this device. ● *Are there files that can contain PII?* *Files contain PII of employee budget , work shift schedule, new hire document,* ● *Are there sensitive work files?* *Work File contain PII of employee budget , work shift schedule* ● *Is it safe to store personal files with work files?* *It is not safe to store the both files on the same place*
Attacker mindset	Write **2-3 sentences** about how this information could be used against Jorge or the hospital. ● *Could the information be used against other employees or relatives?* *Threat actors can easily find the other employee details who work with Jorge. Also a malicious email can be designed to look as if it comes from a coworker or relative.* ● *Could the information provide access to the business?*
Risk analysis	Write **3 or 4 sentences** describing technical, operational, or managerial controls that could mitigate these types of attacks: ● *What types of malicious software could be hidden on these devices? What could have happened if the device were infected and discovered by another employee?* *Operational control - Very often Antivirus scan that can be implemented. Technical control - disabling AutoPlay on company PCs that will prevent a computer from automatically executing malicious code when a USB drive is plugged in.*