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?* ● *Are there sensitive work files?* ● *Is it safe to store personal files with work files?* *The contents of the USB drive contains PII like family photos and personal files that he would not like if they were made public. Work files are present that pertain to company confidential information and its operations.*
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?* ● *Could the information be used against relatives?* ● *Could the information provide access to the business?* *The shift schedule documents can provide details to an attacker regarding the names of the people who work with Jorge at the hospital. Since both work and personal files exist, either work or personal information can be a threat to Jorge. For example, with the data I am after, I can easily impersonate one of Jorge's coworkers or relatives.*
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?* ● *What sensitive information could a threat actor find on a device like this?* ● *How might that information be used against an individual or an organization?* *Promoting employee awareness to prevent such attacks from happening can be linked to operational controls. Configuring workstations to have intrusion protection to scan any device plugged into a machine as a safety measure and can be considered a managerial control. For technical control, we can implement intrusion protection like previously stated or disabling simple features like AutoPlay to prevent the USB drive from*

	executing any malicious programs stored on the USB device.