Parking lot USB exercise

Contents	Write **2-3 sentences** about the types of information found on this device. *Some documents appear to contain personal information that Jorge wouldn't want to be made public. The work files include the PII of other people. Also, the work files contain information about the hospital's operations.*
Attacker mindset	Write **2-3 sentences** about how this information could be used against Jorge or the hospital. *The timesheets can provide an attacker intel about other people that Jorge works with. Either work or personal information could be used to trick Jorge. For example, a malicious email can be designed to look as though it comes from a coworker or relative.*
Risk analysis	Write **3 or 4 sentences** describing technical, operational, or managerial controls that could mitigate these types of attacks: *Promoting employee awareness about these types of attacks and what to do when a suspicious USB drive is a managerial control that can reduce the risk of a negative incident. Setting up routine antivirus scans is an operational control that can be implemented. Another line of defense could be a technical control, like disabling AutoPlay on company PCs that will prevent a computer from automatically executing malicious code when a USB drive is plugged in.*

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?*
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?*
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?*