Parking lot USB exercise

Contents	Write **2-3 sentences** about the types of information found on this device. *The device contains personal documents that Jorge would prefer to keep private, along with work-related files that include sensitive personal information about others. Additionally, the work files reveal confidential details about the hospital's operations and activities.*
Attacker mindset	Write **2-3 sentences** about how this information could be used against Jorge or the hospital. *This information could be used by attackers to gather insights about Jorge's colleagues, which could make it easier to target them in an attack. Whether the data is personal or professional, it can be exploited for social engineering. For example, an attacker might craft a fake email that appears to come from one of Jorge's coworkers or family members, tricking him into clicking on a malicious link.*
Risk analysis	Write **3 or 4 sentences** describing technical, operational, or managerial controls that could mitigate these types of attacks: *To minimize these risks, it's important to focus on employee training regarding the dangers of suspicious USB drives and the actions to take if one is found. Routine antivirus scans should be scheduled to help detect and prevent malware. Additionally, a technical control like disabling AutoPlay on workplace computers can stop malicious software from running automatically when a USB device is plugged in. These combined controls offer multiple layers of protection against potential threats.*

Italo B.