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 USB contains personal files and work related files. The USB contains PII and also sensitive work files. Mixing or storing personal files and work related files is not a good practice. It contains work files such as a new hire letter and an employee shift schedule.
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 USB drive contains sensitive information that can be used against Jorge or even the employees by obtaining their shift schedule details and using it to blackmail them.
	There is a possibility that the attacker himself might have dropped the USB in the parking lot.
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?*
	The attacker could have injected the drive with malicious code to obtain control over the system and from there gain access to other systems in the network. Sensitive information such as employees working shift schedules could have been leaked and other details such as PII.
	This information could affect the organisation's reputation and

	asking for money in exchange of information. *The individual could be blackmailed to reveal sensitive information.*