## **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? Yes, there are.* * *Are there sensitive work files? Yes, there are.* * *Is it safe to store personal files with work files? Not at all.* |
| --- | --- |
| **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? Yes, the budget spreadsheet.* * *Could the information be used against relatives? Yes, the wedding list.* * *Could the information provide access to the business? Probably, through the new hire letter.* |
| **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?  Any kind of malware or spyware. What could have happened if the device were infected and discovered by another employee? PII & Sensitive info. related to the business leak* * *What sensitive information could a threat actor find on a device like this? Info. related to families, friends & relatives, work info, and more about the person to whom the pendrive belongs.* * *How might that information be used against an individual or an organization? Blackmailing people, morphing photos & videos, pretending to the person & hurting relatives, friends & workmates, and getting to know about the workplace & probably its vulnerabilities.* |