## **Parking lot USB exercise**

| **Contents** | Write **2-3 sentences** about the types of information found on this device.   * *There are several files that contain PI like his resume or his hire letter* * *He has some files like shift schedules and employee budgets that are company sensitive information* * *He shouldn’t be storing work files along with personal files, but he shouldn’t even be storing work files in a USB as he could lose it (like he did) or get easily stolen or copied.* |
| --- | --- |
| **Attacker mindset** | Write **2-3 sentences** about how this information could be used against Jorge or the hospital.  *Jorge stores information like vacation ideas that reveal where he could be going at all times, a wedding list that could aid in identifying all of his relatives which could lead to threats to get PII or money and his resume which has all of his PII and could lead to identity falsification.*  *His work is in danger as there is information of employees like their budgets and the times of leaving and entering of each one, along with PII of each one. All of this information may lead to kidnappings, threats to them to reveal information about the company, among other risks.*  *As well an attacker could falsify his identity to enter the company.* |
| **Risk analysis** | Write **3 or 4 sentences** describing technical, operational, or managerial controls that could mitigate these types of attacks:  *Lots of malicious software can be hidden inside the usb, files pretending to be regular files, scripts that run automatically after plugging in the usb. If someone that didn’t know about these dangers would’ve discovered the usb, they’d been in serious danger and would’ve placed the company in serious danger too.*  *Lots of information can be discovered in a personal USB, information like passwords, PII, relevant information about the company like salaries or other employees, future plans, amongst others that someone could’ve stolen.* |