## **Parking lot USB exercise**

|  |  |
| --- | --- |
| **Contents** | Write **2-3 sentences** about the types of information found on this device.   * *There are sensitive information like PII in this USB that can compromise users and the organization* * *Sensitive documentation that are part of the organization that can affect the confidentiality, integrity and availability of the company.* * *No encryption in this files which can be compromised by a threat actor if they plan to penetrate.* * *Internal Operations file are part of this device* |
| **Attacker mindset** | Write **2-3 sentences** about how this information could be used against Jorge or the hospital.   * *The information or data in this device can compromise not only the user, relative but also the company itself since compromise and sensitive information is saved. It could create a huge leak to compromise the confidentiality and integrity of the data. This information can be used against anyone and the organization included in which the only beneficiary is the threat actor.* |
| **Risk analysis** | Write **3 or 4 sentences** describing technical, operational, or managerial controls that could mitigate these types of attacks:  In this particular case, the released of USB worms can be hidden in the device. Once is plugged then the attack starts. This would affect the organization in case the USB baiting were found by another employee who do not have enough training awareness about the security posture of the company or even for themselves. PII information could been leaked where it can be used against the company and also all the users could have been compromised by the leak of information.  *To avoid this situation, it is important to train employees about these attacks. A technical control is also implemented in this training where the provision of tools for the employees like antivirus scan before opening.* |