## **Parking lot USB exercise**

| **Contents** | Write **2-3 sentences** about the types of information found on this device.  *The USB drive contains a mixture of personal and work-related files. Personal files include family and pet photos, while work files comprise documents such as a new hire letter and an employee shift schedule. These files include PII and sensitive information related to the hospital's operations, posing a risk of data exposure.* |
| --- | --- |
| **Attacker mindset** | Write **2-3 sentences** about how this information could be used against Jorge or the hospital.  *An attacker could leverage the PII found in the work documents to target other employees at the hospital. Personal information on the drive could be used to craft convincing phishing attacks or social engineering schemes against Jorge. For example, an attacker could send a malicious email mimicking a coworker or relative to trick Jorge into disclosing more information or clicking on malicious links.* |
| **Risk analysis** | Write **3 or 4 sentences** describing technical, operational, or managerial controls that could mitigate these types of attacks:  *USB baiting attacks can conceal various types of malware, such as ransomware, spyware, or keyloggers, which could be activated when the device is connected to a computer. If another employee had discovered and used the USB drive, it could have compromised the hospital's network, leading to unauthorized access to sensitive patient information and disrupting hospital operations. Several controls should be implemented to mitigate these risks:*   1. ***Technical Controls:*** *Disable AutoPlay on company PCs to prevent the automatic execution of malicious code when a USB drive is connected. Employ endpoint security solutions to detect and neutralize threats from external devices.* 2. ***Operational Controls:*** *Conduct regular antivirus scans and use virtualization software to investigate safely unknown USB devices.* 3. ***Managerial Controls:*** *Promote employee awareness about the dangers of USB baiting and establish strict policies for handling found USB devices, including mandatory reporting and safe investigation protocols.* |