## **Ejercicio USB en estacionamiento**

| **Contenido** | Escriba **2 o 3 oraciones** sobre los tipos de información que se encuentran en este dispositivo.  *Algunos documentos parecen contener información personal que Jorge no querría que se hiciera pública. Los archivos de trabajo incluyen información personal identificable de otras personas. Además, los archivos de trabajo contienen información sobre las operaciones del hospital.* |
| --- | --- |
| **Mentalidad de atacante** | Escribe **2-3 oraciones** sobre cómo esta información podría usarse en contra de Jorge o del hospital.  *Las planillas de horas pueden proporcionar a un atacante información sobre otras personas con las que Jorge trabaja. Tanto la información personal como la laboral podrían utilizarse para engañar a Jorge. Por ejemplo, un correo electrónico malicioso puede diseñarse para que parezca que proviene de un compañero de trabajo o un familiar.* |
| **Análisis de riesgos** | Escriba **3 o 4 oraciones** que describan los controles técnicos, operativos o de gestión que podrían mitigar este tipo de ataques:  *Promover la concienciación de los empleados sobre este tipo de ataques y qué hacer cuando se detecta una unidad USB sospechosa es un control de gestión que puede reducir el riesgo de un incidente negativo. Establecer análisis antivirus de rutina es un control operativo que se puede implementar. Otra línea de defensa podría ser un control técnico, como desactivar la reproducción automática en las PC de la empresa que evitará que una computadora ejecute automáticamente un código malicioso cuando se conecte una unidad USB.* |