## **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?* * *Are there sensitive work files?* * *Is it safe to store personal files with work files?*   *La unicad USB contiene PII tanto de la persona como de miembros de su equipo.*  *Contiene archivos de trabajo sensibles como horarios de trabajo y nueva contratación de personal.*  *No es seguro que mezclar información y/o documentación del trabajo con cosas personales, ya que como es el caso es vulnerable a extravios.* |
| **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?* * *Could the information be used against relatives?* * *Could the information provide access to the business?*   *La información de trabajo que contiene la USB, puede ser alterada modificando los turnos de trabajo para conveniencia de alguien afectando al equipo de trabajo.*  *Además la información familiar puede afectar a los parientes ya que pueden hacer uso indebido de las fotografías encontradas o publicarlas sin autorización en redes sociales.*  *La información puede altera el manejo de información de la institución.* |
| **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? What could have happened if the device were infected and discovered by another employee?* * *What sensitive information could a threat actor find on a device like this?* * *How might that information be used against an individual or an organization?*   *La USB podría haber estado infectada de virus malicioso como:*  *De haber estado infectado, cabe la posibilidad que el sistema de red se hubiera visto bloqueado, al verse afectado por ejemplo de solicitudes hacia el servidor, ya que este no tendría la capacidad de responder.*  *Un actor de amenazas podría haber encontrado información sensible como, nombres, direcciones, email, teléfonos, horarios de trabajo, entre otro.*  *La información puede ser usada de forma mal intencionada para manipular datos (eliminación, modificación, agregación) que puede afectar al funcionamiento de la organización y al ambiente laboral del personal.*  *Algunos controles a tener en cuenta:*  *Promover la conciencia de los empleados sobre este tipo de ataques y qué hacer cuando una unidad USB sospechosa es un control gerencial que puede reducir el riesgo de un incidente negativo.*  *Configurar escaneos antivirus de rutina es un control operativo que se puede implementar.*  *Otra línea de defensa podría ser un control técnico, como deshabilitar la reproducción automática en las computadoras de la empresa, lo que evitará que una computadora ejecute automáticamente código malicioso cuando se conecta una unidad USB.* |