**Ejercicio sobre USB abandonado en estacionamiento**

|  |  |
| --- | --- |
| **Contenido** | Escribe **2 o 3 oraciones** sobre los tipos de información que se encuentran en este dispositivo.   * *¿Hay archivos que puedan contener PII?*   Existen archivos en formato de imagenes tanto fammiliares como de mascotas.   * *¿Hay archivos de trabajo confidenciales?*   Se encuentra datos de empleados y horarios de los mismos.   * *¿Es seguro almacenar archivos personales con archivos de trabajo?*   No, el contenido familiar deberia ir aparte, en este caso se extravio esta unidad USB y se esta revelando datos personales como laborales |
| **Mentalidad de atacante** | Escribe **2 o 3 oraciones** sobre cómo se podría usar esta información contra Jorge o el hospital.   * *¿Se puede usar la información contra otros empleados?*   Al conocer los horarios de los empleados se puede plantear una intrusion sin que el personal se de cuenta de la presencia de extraños. En los documentos de contratacion existe informacion que puede ser usada para infiltrar a una persona totalmente diferente o buscar y dañar al empleado que figure en el contrato.   * *¿Se puede usar la información contra familiares?*   Con solo tener imagenes se puede tener un indicio de saber la figura de la persona hasta dar con ella, existen herramientas que pueden buscar los rostros en miles de imagenes o inclusive usar ese rostro con fines no eticos.   * *¿Podría la información proporcionar acceso a la empresa?*   Con tener un contrato un agente malicioso puede hacer pasar a una persona y que se infiltre en la empresa robando la identidad de la persona que figura en el contrato, sabiendo los horarios del los empleados poder burlar la seguridad del sitio. |
| **Análisis de riesgos** | Escribe **3 o 4 oraciones** que describan los controles técnicos, operativos o gerenciales que podrían mitigar estos tipos de ataques:   * *¿Qué tipos de software malicioso podrían estar ocultos en estos dispositivos? ¿Qué podría haber sucedido si el dispositivo hubiera estado infectado y lo hubiera descubierto otro empleado?*   Una USB sospechasa puede almacenar varios riesgos como virus, worm, trojan horse, ransomware, spyware, adware, rootkits keyloggers, rogue software, etc.  Si el USB hubiera estado infectado se podria controlar el daño si se ejecutaba dentro de una maquina virtual la cual esta desconectada de la red para evitar que los daños se propaguen, tambien hubiera sido efectivo un antivirus,desactivar la autoejecucion, segmentacion de red, etc, un empleado si saber como gestionar esta amenaza y sin previa concentizacion sobre sus actos podria vulnerar a todo el sistema.   * *¿Qué información confidencial podría encontrar un agente de amenaza en un dispositivo como este?*   Archivos de la empresa, empleados, horarios, contratos, etc.   * *¿Cómo se podría utilizar esa información contra un individuo o una organización?*   Haciendo uso de esta informacion saber como operan, suponer el numero de empleados por departamentos, los horarios de los empleados, correo electronicos de los mismo, datos de acceso al sistema, etc. |