Ejercicio encriptación (Video relacionado: 8.4, 8.5. Contenido: Encriptación)

Eres nuevo en la empresa de ciberseguridad que te ha contratado como Data Engineer, recientemente el gerente ha decidido que toda la infraestructura de la empresa debe migrar a Python ya que es el lenguaje más demandado y sus clientes se lo están pidiendo. Una de las cuestiones más importantes a tener en cuenta es que sin importar el lenguaje de programación la empresa debe tener mucho cuidado con la información sensible (PII) por esto necesita que analices distintas librerías en Python para poder encriptar datos de este tipo. Te sugiero que compares cuatro librerías: Faker, anonympy y Pseudonymization por el momento.

Deberías comentarle luego de tu análisis cuál sería la mejor opción para la implementación.

- ❖ **Solución**

En este código encontrarás una solución propuesta

Cada una de estas librerías tiene sus ventajas y es más adecuada para diferentes situaciones. Si necesitas generar datos ficticios para reemplazar información real, Faker podría ser una buena opción. Si buscas una solución más personalizada y orientada a la anonimización de datos, AnonymPy podría ser más adecuada. Por otro lado, si estás interesado en pseudonimizar datos para mantener relaciones entre registros sin exponer datos sensibles, puedes considerar el uso de funciones de hash de la librería hashlib.