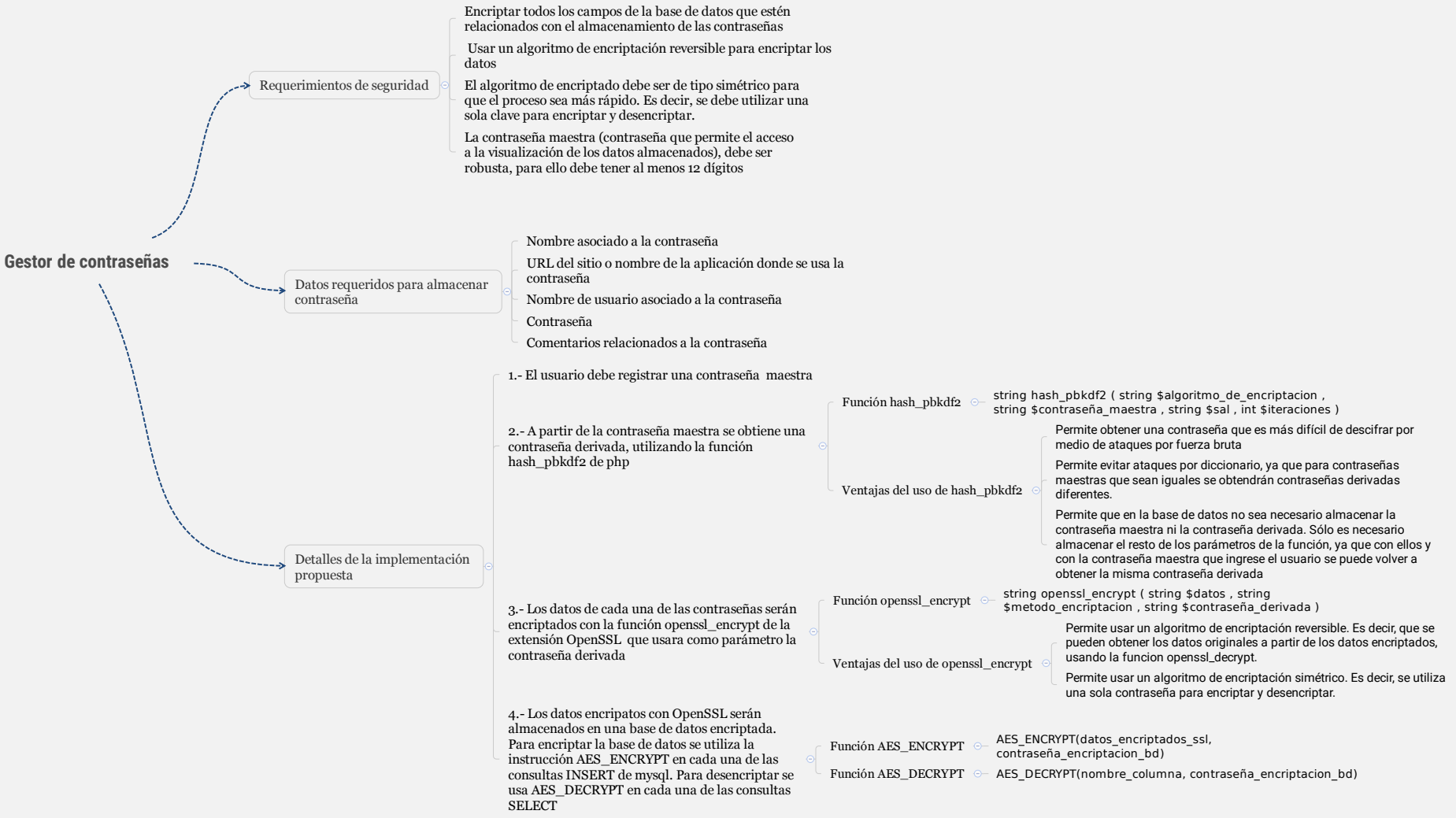
Gestor de contraseñas
Requerimientos de seguridad
Encriptar todos los campos de la base de datos que estén relacionados con el almacenamiento de las contraseñas
Usar un algoritmo de encriptación reversible para encriptar los datos
El algoritmo de encriptado debe ser de tipo simétrico para que el proceso sea más rápido. Es decir, se debe utilizar una sola clave para encriptar y desencriptar.
La contraseña maestra (contraseña que permite el acceso a la visualización de los datos almacenados), debe ser robusta, para ello debe tener al menos 12 dígitos
Datos requeridos para almacenar contraseña
Nombre asociado a la contraseña
URL del sitio o nombre de la aplicación donde se usa la contraseña
Nombre de usuario asociado a la contraseña
Contraseña
Comentarios relacionados a la contraseña
Detalles de la implementación propuesta
1.- El usuario debe registrar una contraseña maestra
2.- A partir de la contraseña maestra se obtiene una contraseña derivada, utilizando la función hash_pbkdf2 de php
Función hash_pbkdf2
string hash_pbkdf2 ( string $algoritmo_de_encriptacion , string $contraseña_maestra , string $sal , int $iteraciones )
Ventajas del uso de hash_pbkdf2
Permite obtener una contraseña que es más difícil de descifrar por medio de ataques por fuerza bruta
Permite evitar ataques por diccionario, ya que para contraseñas maestras que sean iguales se obtendrán contraseñas derivadas diferentes.
Permite que en la base de datos no sea necesario almacenar la contraseña maestra ni la contraseña derivada. Sólo es necesario almacenar el resto de los parámetros de la función, ya que con ellos y con la contraseña maestra que ingrese el usuario se puede volver a obtener la misma contraseña derivada
3.- Los datos de cada una de las contraseñas serán encriptados con la función openssl_encrypt de la extensión OpenSSL que usara como parámetro la contraseña derivada
Función openssl_encrypt
string openssl_encrypt ( string $datos , string $metodo_encriptacion , string $contraseña_derivada )
Ventajas del uso de openssl_encrypt
Permite usar un algoritmo de encriptación reversible. Es decir, que se pueden obtener los datos originales a partir de los datos encriptados, usando la funcion openssl_decrypt.
Permite usar un algoritmo de encriptación simétrico. Es decir, se utiliza una sola contraseña para encriptar y desencriptar.
4.- Los datos encripatos con OpenSSL serán almacenados en una base de datos encriptada. Para encriptar la base de datos se utiliza la instrucción AES_ENCRYPT en cada una de las consultas INSERT de mysql. Para desencriptar se usa AES_DECRYPT en cada una de las consultas SELECT
Función AES_ENCRYPT
AES_ENCRYPT(datos_encriptados_ssl, contraseña_encriptacion_bd)
Función AES_DECRYPT
AES_DECRYPT(nombre_columna, contraseña_encriptacion_bd)