****

**Universidad Politécnica Salesiana**

**Tema:**

GESTOR DE CONTRASEÑAS ENCRIPTADAS

**Integrantes:**

SR. WALTER ADALBERTO ISBES SANCHEZ (LIDER)

SR. ABDÓN JOEL CALDERÓN LIMONES

SR. CARLOS ARTURO FLOREZ MOLINA

SR. BYRON ANDRES CONFORME DEMERA

**Asignatura:**

CRIPTOGRAFÍA

**Docente:**

XAVIER MERINO MIÑO

**SEMESTRE:**

9NO

**Guayaquil – Ecuador**

2021 – 2022

**INDICE**

[ANTECEDENTES 3](#_Toc92048723)

[PROBLEMA 4](#_Toc92048724)

[OBJETIVO GENERAL 5](#_Toc92048725)

[OBJETIVOS ESPECIFICOS 5](#_Toc92048726)

[PROPUESTA DE SOLUCIÓN 6](#_Toc92048727)

[METODOLOGÍA 7](#_Toc92048728)

[Método de Cifrado 7](#_Toc92048729)

[Algoritmo AES (Advanced Encryption Standard) 7](#_Toc92048730)

[Front End 8](#_Toc92048731)

[Back End 8](#_Toc92048732)

[Base de Datos 8](#_Toc92048733)

[Diagrama de Bloques 9](#_Toc92048734)

[EQUIPO Y TAREAS 10](#_Toc92048735)

[BIBLIOGRAFÍA 11](#_Toc92048736)

# ANTECEDENTES

Los usuarios del internet se manejan bajo credenciales para acceder a varios servicios que están publicados en la red, lo cual nos lleva a crear varias credenciales digitales para acceder a ellas, la mayoría de usuarios prefieren utilizar los gestores nativos de los navegadores de internet, pero aquellos se muestran vulnerables debido a que cualquiera que tenga acceso a su computador puede visualizar las contraseña ya que en la mayoria de los casos la seguridad de los navegadores al proteger las contraseña es la misma clave que se usa al acceder al computador creando así una brecha para poder conocer hasta credenciales importantes como de las entidades financieras personales.

En otros casos existen personas que guardan la información de sus contraseñas en su e-mail como fue el caso de: “Javier Rodríguez, a quien le robaron USD 5 000 directamente de su cuenta bancaria en línea, luego de ‘hackearle’ su correo electrónico, en donde a manera de respaldo tenía guardado un e-mail con las claves de acceso a sus redes sociales, a sus dos cuentas bancarias e incluso la clave de la alarma de su domicilio.” (Gómez, 2012). Buscando una facilidad y seguridad para el usuario se piensa crear un servicio para poder ayudar a tener de una manera más ordenada y segura las credenciales digitales con la ayuda de encriptación a las contraseñas e implementaciones de seguridad informática.

# PROBLEMA

Dada la gran cantidad de servicios que en la actualidad requieren del uso de credenciales, es bastante común que los usuarios utilicen contraseñas sencillas o reutilicen las mismas en diferentes plataformas, también es fácil identificar que gran parte de estas personas opten por armar contraseñas empleando sus datos personales. El uso de estas prácticas los convierte en un objetivo sencillo para los hackers que utilizan la fuerza bruta para obtener las contraseñas, “Un ataque de fuerza bruta es un intento por descifrar una contraseña o un nombre de usuario. Mediante prueba y error, los atacantestratan de dar con la combinación correcta.” (Rodríguez, 2020)

Debido a la alta capacidad de procesamiento con la que cuentan los computadores actuales, es posible descifrar una contraseña corta que solo contenga números y letras en cuestión de horas o incluso menos, las contraseñas que están constituidas por datos personales del usuario son igual de vulnerables que las anteriores porque los atacantes emplean diccionarios de datos armados con la información del objetivo, la cual suele encontrarse fácilmente en las redes sociales de la víctima, esta brecha de seguridad se agiganta en los casos en los que la contraseña obtenida ilegalmente es usada en distintas cuentas del mismo usuario.

OBJETIVO GENERAL

Desarrollar un gestor web de credenciales que utilice un algoritmo de encriptación simétrica para la protección de los datos registrados en él mismo.

# OBJETIVOS ESPECIFICOS

1. Implementar una interfaz web para un manejo apropiado de la aplicación.
2. Diseñar la base de datos donde se almacenarán las credenciales.
3. Investigar un algoritmo simétrico de encriptación para su uso en las credenciales registradas.

# 

# PROPUESTA DE SOLUCIÓN

Con base en las problemáticas evidenciadas de múltiples credenciales para diferentes sitios o aplicaciones se propone crear un sistema web en el cual se pueda crear y administrar cuentas, que se pueda acceder mediante cualquier navegador web usando una única contraseña máster con la cual se pueda desbloquear, visualizar y usar las credenciales guardadas.

El sistema web contará con certificado de seguridad SSL (conexiones HTTPS) protegiendo las conexiones que el usuario establezca para acceder al gestor web de credenciales.

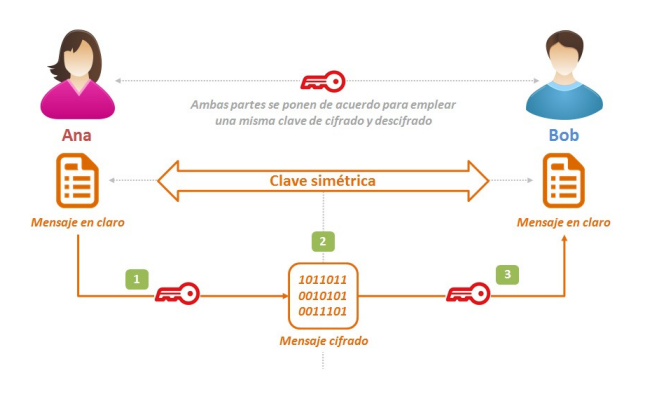
El sistema almacenará las credenciales de forma encriptada usando encriptación simétrica.

# METODOLOGÍA

En esta sección se detallará los aspectos a desarrollar tanto como conceptos y funciones del algoritmo de encriptación a implementar en nuestro proyecto de gestor de contraseñas encriptadas para el usuario.

## Método de Cifrado

El método para implementar en nuestro sistema será con un algoritmo de encriptación simétrica que consiste en que la información que se necesita cifrar se hará por medio de una única clave secreta que se encargará de cifrar o descifrar la información.



## Algoritmo AES (Advanced Encryption Standard)

Este es un algoritmo de cifrado por bloques el cual es utilizado en varios canales de protocolos seguros. El tamaño fijo del bloque es de 128 bit, su clave puede ser como de 128 hasta 256 bits, es usado como dominio público de rápida y sencilla implementación.

Ya que es un algoritmo importante que es usado hoy en día y que las probabilidades son casi imposibles esto nos lleva a que si una persona mal intencionada desea realizar un ataque de fuerza bruta le tomaría varios años dando como resultado una alta posibilidad de protección con este algoritmo de simétrico.

Además, es un sistema de clave simétrica, lo cual le otorga una mayor seguridad, ya que la clave usada debe ser conocida para el cifrado como para el descifrado y tanto emisor como receptor necesitan una copia de la llave maestra correspondiente.

## Front End

Para el desarrollo de las interfaces de diseño usaremos HTML y CSS para un desarrollo amigable y entendible para el usuario sin utilizar demás tecnologías para su complejidad ya que la parte importante de este proyecto está en la funcionabilidad del algoritmo de encriptación.

## Back End

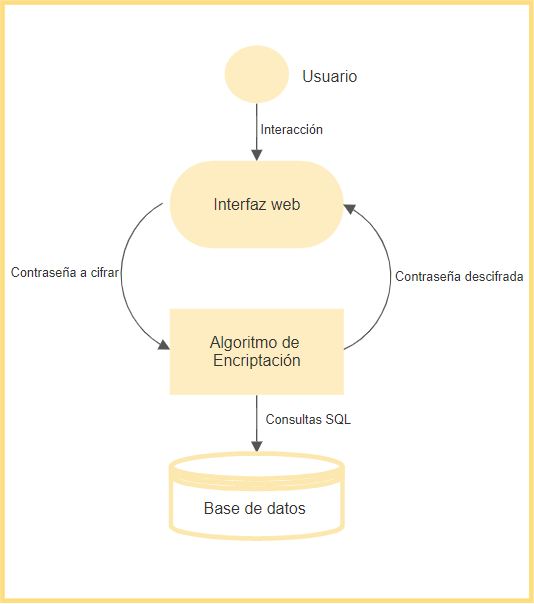
Para el desarrollo del código del sistema se trabajará con el algoritmo de encriptación AES descrito anteriormente para su correcto funcionamiento interno teniendo las consideraciones necesarias para que la información guardada se encuentre bajo las medidas de seguridad altas.

## Base de Datos

La base de datos que se usará para el desarrollo del sistema será MySQL para que nos permita guardar la información que ingrese el usuario en el sistema concentrando los datos en un solo fichero para facilitarnos el respaldo de los datos.

## Diagrama de Bloques

En este diagrama presentamos como estaría estructurado el funcionamiento del sistema. El usuario hace uso de la aplicación web desde su ordenador donde ingresa la clave a cifrar, el sistema hace uso del algoritmo de encriptación y esta a su vez la guarda a una base de datos para luego poder hacer uso de ella cuando se requiera.



# EQUIPO Y TAREAS

|  |  |
| --- | --- |
| INTEGRANTES | TAREA |
| Abdón Calderon | Antecedentes |
| Byron Conforme | Problema  Objetivo general  Objetivos especificos |
| Walter Isbes | Metodología |
| Carlos Florez | Propuesta de solución |

# BIBLIOGRAFÍA

Gómez, L. (2012). Ciudadanos con el robo de sus contraseñas. Diario El Comercio, 1-2.

Rodríguez, A. (15 de Noviembre de 2020). Diario El Comercio. Obtenido de https://www.elcomercio.com/tendencias/hackers-ciberataques-fuerza-bruta-usuarios.html

López, A. (2021, 4 abril). Todo sobre criptografía: Algoritmos de clave simétrica y asimétrica. RedesZone. https://www.redeszone.net/tutoriales/seguridad/criptografia-algoritmos-clave-simetrica-asimetrica/