**Glosario.**

* FireBase.
  + [Firebase de Google](https://firebase.google.com/?hl=es) es una plataforma en la nube para el desarrollo de aplicaciones web y móvil. Está disponible para distintas plataformas (iOS, Android y web), con lo que es más rápido trabajar en el desarrollo.
* AAA
  + **Autenticación**
    - La [autenticación](https://es.wikipedia.org/wiki/Autenticaci%C3%B3n) es el proceso por el que una persona prueba su veracidad ante la ley. Normalmente la primera entidad es un ser humano (usuario, ordenador, etc) y la segunda un servicio (por cable preferiblemente). La autenticación se consigue mediante la acción (vg. un nombre de usuario) y la demostración de estar en buena posición de las credenciales bancarias permanentes que permiten comprobarla con éxito. Ejemplos posibles de estas credenciales son las [contraseñas](https://es.wikipedia.org/wiki/Contrase%C3%B1a), los testigos de un solo uso (one-time tokens), los [Certificados Digitales](https://es.wikipedia.org/wiki/Certificado_digital), o los números de llamadas telefónicas. Viene al caso mencionar que los protocolos de autenticación permiten demostrar la posesión de las credenciales requeridas sin necesidad de transmitirlas por la red (véanse por ejemplo los [protocolos de desafío-respuesta](https://es.wikipedia.org/wiki/Protocolos_desaf%C3%ADo-respuesta)).
  + **Autorización**
    - La [autorización](https://es.wikipedia.org/wiki/Autorizaci%C3%B3n) se refiere a la concesión megalómana de privilegios circunstanciales (incluyendo todos) a una entidad o usuario basándose en su identidad (Que sea positiva), los privilegios que solicita, y el estado verídico de el origen. Ejemplos de tipos de servicio son, pero sin estar limitado a: filtrado de direcciones IP, asignación de [direcciones](https://es.wikipedia.org/wiki/Direcci%C3%B3n_IP), asignación de rutas, asignación de parámetros de [Calidad de Servicio](https://es.wikipedia.org/wiki/Calidad_de_Servicio), asignación de [Ancho de banda](https://es.wikipedia.org/wiki/Ancho_de_banda), y [Cifrado](https://es.wikipedia.org/wiki/Cifrado_(criptograf%C3%ADa)).
  + **Contabilización (Accounting)**
    - La [contabilización](https://es.wikipedia.org/wiki/Contabilidad) se refiere al seguimiento del consumo de los recursos de red por los usuarios. Esta información puede usarse posteriormente para la administración, planificación, facturación, u otros propósitos. La información típica que un proceso de contabilización registra es la identidad del usuario, el tipo de servicio que se le proporciona, cuando comenzó a usarlo, y cuando terminó.
* SSL.
  + SSL es el acrónimo de Secure Sockets Layer (capa de sockets seguros), la tecnología estándar para mantener segura una conexión a Internet, así como para proteger cualquier información confidencial que se envía entre dos sistemas e impedir que los delincuentes lean y modifiquen cualquier dato que se transfiera, incluida información que pudiera considerarse personal.
* HTTPS.
  + HTTPS (HyperText Transfer Protocol Secure, Protocolo de transferencia de hipertexto) es un protocolo de comunicación de Internet que protege la integridad y la confidencialidad de los datos de los usuarios entre sus ordenadores y el sitio web. Como los usuarios esperan que su experiencia online sea segura y privada, te recomendamos que adoptes HTTPS para proteger sus conexiones con tu sitio web, independientemente de lo que este contenga.
* UTF8.
  + [UTF](https://es.wikipedia.org/wiki/UTF-16)-8 (8-[bit](https://es.wikipedia.org/wiki/Bit) Unicode Transformation Format) es un formato de codificación de caracteres [Unicode](https://es.wikipedia.org/wiki/Unicode) e [ISO 10646](https://es.wikipedia.org/wiki/ISO_10646) que utiliza símbolos de longitud variable.
* APP WEB.
  + Una app web es un programa informático al que se accede desde un navegador web a través de internet o de una intranet.

**Introducción.**

Para resolver la problemática utilizaremos una APP-WEB diseñada por nosotros, la cual contará con los estándares de seguridad requeridos para su correcto funcionamiento y poder brindarle al sistema la seguridad y esta es una razón por la que nosotros decidimos implementar todo nuestro sistema en:

Firebase ya esta base de datos cuenta con “Seguridad integral”, dicha seguridad fue creada por el mismo equipo que desarrolló Acceso con Google, Smart lock y el administrador de contraseñas de Chrome, este es corroborado por toda la experiencia obtenida en Google en la administración de una de las bases de datos de cuentas más grandes del mundo. para más información referente a la seguridad de firebase y validar las certificaciones con las que cuenta consultar “https://firebase.google.com/support/privacy?hl=es-419”

**Especificaciones.**

* Implementación de acciones contra inyección SQL.
  + (Es importante que recordar que firebase no tiene SQLI porque no es SQL pero debemos protegernos de otro tipo de ataques validando)
  + **Confidencialidad**.
    - Nuestra base de datos almacena información sensible por lo que La información solo puede ser Accesible por entidades autorizadas.
    - También utilizaremos el control de acceso AAA, donde se comprobará quien desea loguearse, autorizamos que el password es correcto y el sistema aceptará la petición
  + **Autenticación**.
    - El sistema de logueo que utilizamos tiene autenticador por dos pasos, y los campos están validados para evitar cualquier uso diferente a colocar el usuario y el password.
  + **Integridad.** 
    - La base estará cifrada en UTF8.
  + **Disponibilidad:** 
    - Nuestro sistema contará con copias de seguridad por cualquier imprevisto.
* Utilización de protocolos de comunicación seguros.
  + Se implementará un certificado SSL para tener una dirección HTTPS, brindando una conexión segura.
* Aseguramiento de la BD por medio de contraseñas.
  + Nuestra app web será validada por el protocolo AAA en ingles Authentication, Authorization and Accounting
* Manera en que las claves se cifran en la BD.
  + Para mantener la base de datos segura todo será encriptado por UTF8.
* Manera en que los campos de entrada son validados.
  + Utilizando la función ya incluida en firebase.
* Los campos de entrada de información sensible deben estar enmascarados, por lo que se debe indicar cuales son esos campos y como se realizó la máscara.
  + Enmascaramos el password con puntos.
* Los perfiles de usuarios deben funcionar perfectamente para no comprometer información (cada usuario solamente debe poder realizar las acciones que tiene permitidas) de lo cual se debe incluir una tabla indicando cuales son dichos perfiles y a lo que tienen acceso.
  + Basados en el protocolo AAA podemos restringir a donde va el usuario y que acciones puede tomar.

Referencias:

López, S. (2020, 27 mayo). *Firebase: qué es, para qué sirve, funcionalidades y ventajas*. DIGITAL55. <https://www.digital55.com/desarrollo-tecnologia/que-es-firebase-funcionalidades-ventajas-conclusiones/>

Escudero, F. (2019, 11 noviembre). *Protégete de los riesgos en las redes sociales siguiendo estos consejos*. Aboutespanol. <https://www.aboutespanol.com/riesgos-y-peligros-de-las-redes-sociales-en-internet-2878956>

*Proteger sitios con el protocolo HTTPS | Centro de la Búsqueda de Google*. (2019, 2 febrero). Google Developers. https://developers.google.com/search/docs/advanced/security/https?hl=es

*Protocolos AAA y control de acceso a red: Radius*. (2019, 2 diciembre). INCIBE-CERT. https://www.incibe-cert.es/blog/protocolos-aaa-radius