En cumplimiento con la ley 1581 del 2012 la cual establece;

Los datos personales que no sean públicos no pueden ser publicados en internet, salvo que el acceso a los mismos sea técnicamente controlable para brindar un conocimiento restringido sólo a las personas autorizadas conforme a la Ley 1581 de 2012, es decir: (i) a los Titulares, sus causahabientes o sus representantes legales; (ii) a las entidades públicas o administrativas en ejercicio de sus funciones legales o por orden judicial y (iii) a los terceros autorizados por el Titular o por la ley. Lo anterior, con el fin de garantizar que terceros no autorizados puedan acceder a ella. En todo caso, cuando se pretenda realizar tratamiento de la información pública publicada en internet deberá someterse al cumplimiento del principio de finalidad de la base de datos.

Cabe precisar que los datos personales que se encuentren en sitios de acceso público como internet por ese solo hecho no convierte a dichos datos personales en naturaleza pública y, por ello, el tratamiento de los mismos deberá realizarse garantizando el derecho de hábeas data y el derecho de la intimidad del titular dando aplicación a los principios de legalidad, finalidad, libertad, veracidad y calidad, transparencia, acceso y circulación restringida, seguridad, confidencialidad consagrados en el artículo 4 de la Ley 1581 de 2012.

Los datos personales que no sean públicos no pueden ser publicados en internet, salvo que el acceso a los mismos sea técnicamente controlable para brindar un conocimiento restringido sólo a las personas autorizadas conforme a la Ley 1581 de 2012, es decir: (i) a los Titulares, sus causahabientes o sus representantes legales; (ii) a las entidades públicas o administrativas en ejercicio de sus funciones legales o por orden judicial y (iii) a los terceros autorizados por el Titular o por la ley. Lo anterior, con el fin de garantizar que terceros no autorizados puedan acceder a ella. En todo caso, cuando se pretenda realizar tratamiento de la información pública publicada en internet deberá someterse al cumplimiento del principio de finalidad de la base de datos.

¿Qué son Datos Personales?

Cuando hablamos de datos personales nos referimos a toda aquella información asociada a una persona y que permite su identificación. Por ejemplo, su documento de identidad, el lugar de nacimiento, estado civil, edad, lugar de residencia, trayectoria académica, laboral, o profesional. Existe también información más sensible como su estado de salud, sus características físicas, ideología política, vida sexual, entre otros aspectos.

¿A qué datos personales no se aplica la ley?

A las bases de datos o archivos mantenidos en un ámbito exclusivamente personal o doméstico. Las que tengan por finalidad la seguridad y defensa nacional la prevención, detección, monitoreo y control del lavado de activos y el financiamiento del terrorismo. Las que tengan como fin y contengan información de inteligencia y contrainteligencia. Las que contengan información periodística y otros contenidos editoriales Las bases de datos con información financiera, crediticia, comercial y de servicios, y de los censos de población y vivienda.

Fuentes:

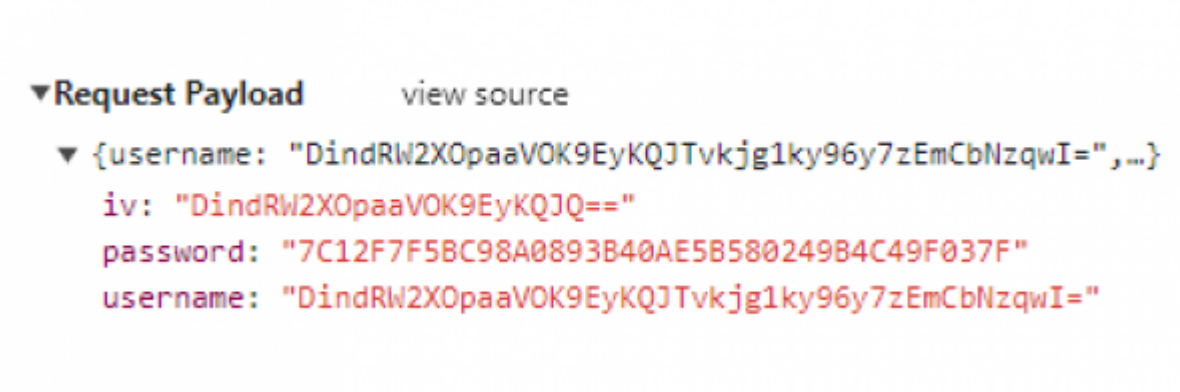
https://www.sic.gov.co/boletin-juridico-junio-2018/tratamiento-de-datos-personales-en-internet

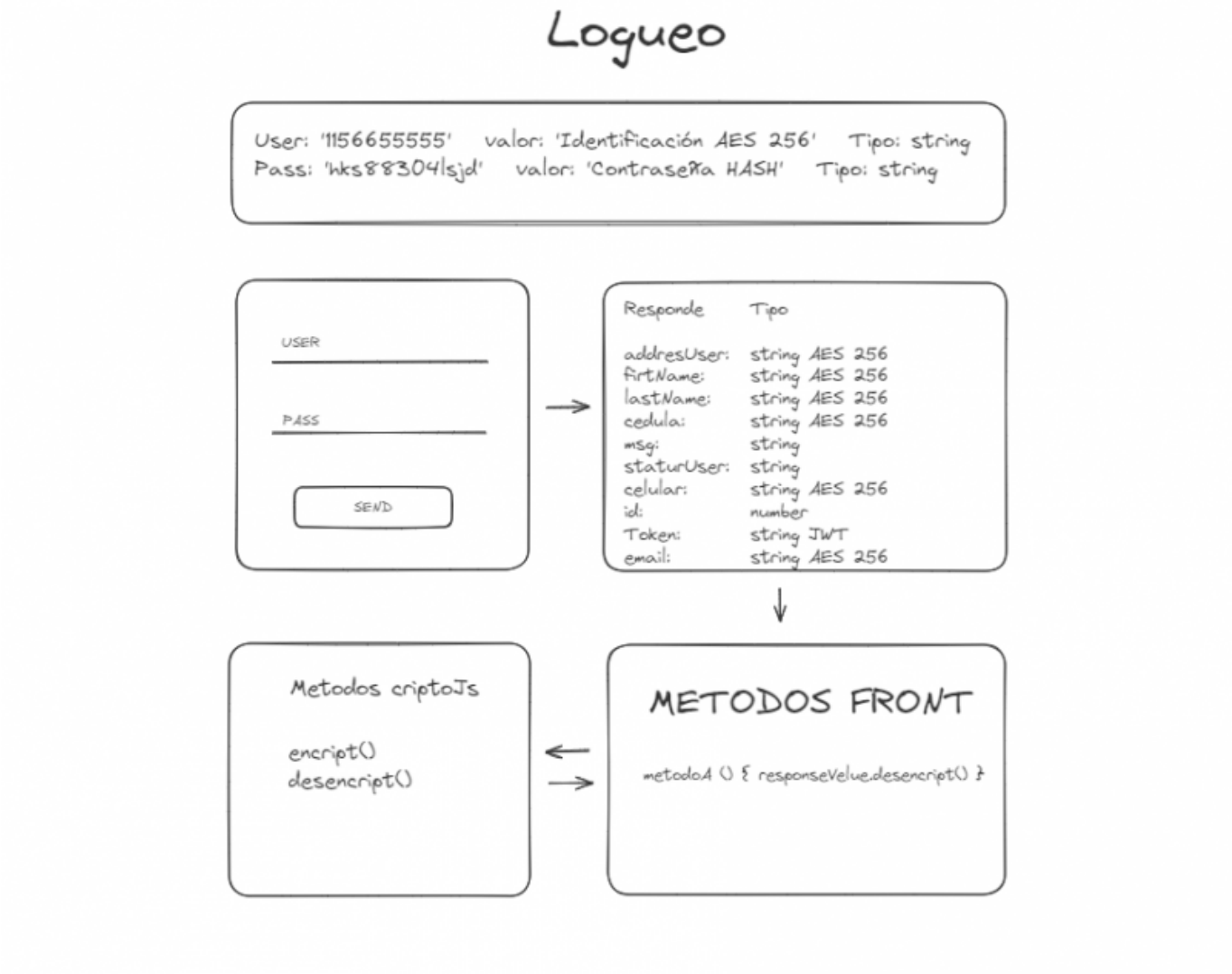
https://www.sic.gov.co/content/sobre-la-protecci%C3%B3n-de-datos-personales

Por tal motivo se establece que el esquema de seguridad personal los datos sensibles viajan encriptados entre back y el front, en ambas partes se encripta - desencripta para evitar la captura de información personal sensible por terceros. Por lo cual se utilizan algoritmo el AES 256 el cual se implementa con dos llaves una publica y una privada para todo el proceso, una de las llaves se genera aleatoriamente.

Para la contraseña se genera un HASH el cual es un valor único sin algoritmo de desencriptación, por tal motivo este valor no podrá descifrarse aún se tenga acceso al back o a la base de datos. La única persona que tendrá conocimiento del valor del Hash es el user, por tal motivo si este olvida su valor real al momento de loquearse deberá ingresar a olvidar contraseña y remplazará el valor actual por un nuevo valor, lo cual genera un nuevo Hash valido.

El siguiente ejemplo muestra los tres valores enviados del front al back; el User encriptado AES 256, el password encriptado con Hash y iv que corresponde a la llave aleatoria.





La información de usuario guardada en el Storage se encuentra encriptada, es necesario que los métodos que requiera dicha información utilicen el metodo desencryptbody de la libreria encryption-lib


```
▼ {msg: "WwPvzu3v8CIk5K2U+FWxBkxwHzOZFhVsjf7OwWVnyWL+q0HkCbAH3swEd0brNTnX9S+HEuHFJEJekCL1RD/oIA==",…}
    addressUser: "WwPvzu3v8CIk5K2U+FWxBtoyIuUJAVQYDmRFe9zs3rs="
    cedula: "WwPvzu3v8CIk5K2U+FWxBmrdYbPYG58BKeOKrkQ2ZuQ="
    cellularUser: "WwPvzu3v8CIk5K2U+FWxBoQk7bwjJRK/MLxVUGdGkuw="
    emailUser: "WwPvzu3v8CIk5K2U+FWxBg9JD2tCp4F/mIR1NAyKbjQh2QIMw3yfIKeLjhIFZM3w"
    firstname: "WwPvzu3v8CIk5K2U+FWxBtwFWTHfdg21VEkMSs3ZUrw="
    id: "WwPvzu3v8CIk5K2U+FWxBvW5nUaIHOU/swITubyAI14="
    iv: "WwPvzu3v8CIk5K2U+FWxBg=="
    lastname: "WwPvzu3v8CIk5K2U+FWxBilZDFG0m5/ARuboa+K/trg="
    login: null
    msg: "WwPvzu3v8CIk5K2U+FWxBkxwHzOZFhVsjf7OwWVnyWL+q0HkCbAH3swEd0brNTnX9S+HEuHFJEJekCL1RD/oIA=="
    password: null
    statusUser: "WwPvzu3v8CIk5K2U+FWxBjPIS6CAvJ5eR13rv+o+RCw="
    token: "WwPvzu3v8CIk5K2U+FWxBhbJzbCovu51tKGpPUcRiSVItilxJTh4FHKMwS0Upw1ILRWHuNxzg23QBYeAlFZ2bahb8D9bWgnlors4nToajVh
    typeUser: "WwPvzu3v8CIk5K2U+FWxBjPIS6CAvJ5eR13rv+o+RCw="
```


←Regresar