**LEFRE WMS**

**PHP versión 7.4.32**

Ver más adelante información acerca de la configuración de PHP

**Mariadb versión 10.7.4**

Se debe instalar el motor CONNECT (Engine Connect) para hacer conexiones a la base de datos. Esto permite hacer SQL JOINS entre tablas de MariaDB y SQL Server.

Este motor ya viene incluido en la instalación. Al instalar MariaDB se debe ejecutar la siguiente instrucción en la línea de comandos de MariaDB.

INSTALL SONAME 'ha\_connect';

Al configurar la base de datos en el servidor se debe chequear estas recomendaciones:

https://mariadb.com/kb/en/configuring-mariadb-for-optimal-performance/

**VARIABLES DE ENTORNO DE SESSION**

|  |  |
| --- | --- |
| $\_VARIABLE | DESCRIPCION |
| username | Nombre de usuario. Por los momentos es único en toda la base de datos. No puede haber 2 usuarios con el mismo username indistintamente si pertenecen a distintas empresas. |
| empresa\_uuid | Como el id de la empresa no debe ser público. Se asigna un UUID para cada empresa y sea usado como variable de sesión global y parámetro GET. De esta manera filtramos los productos y los procesos a una única empresa. En la base de datos existe la función fget\_empresaid() que devuelve el ID de la empresa. El UUID y el ID de la empresa son valores distintos. No confundir. |
| user\_uuid | Cada usuario tiene un UUID() único. Se determina con una función de la base de datos de MariaDB. |

**PLUGGINS USADOS.**

1. **SweetAlert2**
2. **Bootstrap 5**
3. **Swift Mailer**

Una vez instalado el “Composer” procedemos a la instalación del pluggin con el siguiente comando.

composerrequiresymfony/Mailer

1. **MPDF** (https://mpdf.github.io/)

Una vez instalado el “Composer” procedemos a la instalación del pluggin con el siguiente comando.

Creamos la carpeta “mPDF” en la carpeta pluggins y una vez dentro ejecutamos el instalador

composerrequirempdf/mpdf

Nos ubicamos en la carpeta /wms/pluggins/mPDF

composerrequirempdf/qrcode

**Perfil de Usuarios de conexión a base de datos** (PROPUESTO O EN PLANIFICACION NADA OFICIAL AÚN)

Base de datos Godaddy: lefreintra

Usuario:lefre\_admin

Password: l3fr31ntr@

(Al importar datos eliminar todos los DEFINER=`root`@`localhost`del archivo SQL de importación de datos.

|  |  |  |
| --- | --- | --- |
| **Usuario** | **Password** | **Descripción** |
| Root | <sin password> | Sin password (durante desarrollo Alfa). |
| user\_lefre | Lefre | Para que vea solo datos de Lefre |
| user\_sm | Sm | Para que vea solo datos de SM |
| user\_web | Userweb | Usuario externo con acceso para ver datos en la web Acceso lectura a las siguientes tablas: tproductos, tgrupos\_productos, tproductos\_descuentos, |

GRANT EXECUTE ON function lefreintra1.fuser\_empresa TO 'user\_sm'@'%'

GRANT EXECUTE ON `lefreintra1`.\* TO 'user\_sm'@'%'

**CONTRASEÑAS**

* El método para ocultar la contraseña en la base de datos están descartados los métodos MD5 y SHA-1.
* Se usará el método Argon2ID (para PHP 7.3) o Argon2i (para PHP 7.2). Existe un programa en PHP que permite calcular el costo de procesamiento de CPU para generar el hash de un password y este tiempo no sea mayor a 1 milisegundo.

Valores x defecto Argon2i

PASSWORD\_ARGON2\_DEFAULT\_MEMORY\_COST=1024  
PASSWORD\_ARGON2\_DEFAULT\_TIME\_COST=2  
PASSWORD\_ARGON2\_DEFAULT\_THREADS=2

Valores a usar Argon2i

PASSWORD\_ARGON2\_DEFAULT\_MEMORY\_COST=2\*\*12 (2 elevado a 12 da 4096).

PASSWORD\_ARGON2\_DEFAULT\_TIME\_COST=10  
PASSWORD\_ARGON2\_DEFAULT\_THREADS=20

* No se debe diseñar un sistema de administración de contraseñas que permita revertir o desencriptar una contraseña. Prohibido totalmente.
* Prohibido recuperar contraseñas. Si el usuario olvida su contraseña debe generar una nueva.
* El manejo de generación de contraseña se efectuará a nivel de PHP.
* No desarrollar algoritmos de encriptación para manejar contraseñas.
* No desarrollar o generar una salt a través de propios algoritmos. PHP lo recomienda “encarecidamente”. Será evalúa convertirlo obsoleto en próximas entregas.
* Si 2 usuarios tienen la misma contraseña. Su hash o encriptación deben ser distintos.
* Ningún programador/desarrollador o administrador de base de datos debe tener la capacidad de conocer las contraseñas de los usuarios que sean almacenadas en la base de datos.

Fuentes:

<https://es.stackoverflow.com/questions/33420/almacenamiento-de-contrase%C3%B1as-php-y-mysql>

https://www.php.net/manual/es/faq.passwords.php

https://nakedsecurity.sophos.com/2013/11/20/serious-security-how-to-store-your-users-passwords-safely/

[**https://dev.to/anastasionico/good-practices-php-security-how-to-manage-password-18bm**](https://dev.to/anastasionico/good-practices-php-security-how-to-manage-password-18bm)

**https://dev.to/anastasionico/good-practices-how-to-sanitize-validate-and-escape-in-php-3-methods-139b**

**RECOMENDACIONES DE SEGURIDAD**

**(ALTA PRIORIDAD)**

**En el botón de buscar colocar**

**Código de riesgo (Cross-Site Scripting):**

1. URL: http://example.com/search.php?search=<script>alert('test')</script>
2. $search = $\_GET['search'] ?? null;
3. echo 'Search results for '.$search;

**Código Correcto**

1. $search = **htmlspecialchars**($search, ENT\_QUOTES, 'UTF-8');
2. echo 'Search results for '.$search;

**Código de riesgo (SQL Injection):**

**Colocar en el prepare los siguientes valores:**

1. $sql = "SELECT username, email FROM users WHERE id = :id";
2. $sth = $dbh->prepare($sql, [PDO::ATTR\_CURSOR => PDO::CURSOR\_FWDONLY]);
3. $sth->execute([':id' => $id]);
4. $users = $sth->fetchAll();

## SessionHijacking(INVESTIGAR SOBRE ESTO)

Session hijacking is a particular type of malicious web attack in which the attacker secretly steals the session ID of the user. That session ID is sent to the server where the associated $\_SESSION array validates its storage in the stack and grants access to the application. Session hijacking is possible through an XSS attack or when someone gains access to the folder on a server where the session data is stored.

To prevent session hijacking always bind sessions to your IP address to:

1. $IP = getenv("REMOTE\_ADDR");

Watch for it when working on localhost as it doesn’t provide you the exact IP but :::1 or :::127 type values. You should invalidate (unset cookie, unset session storage, remove traces) session quickly whenever a violation occurs and should always try not to expose IDs under any circumstances.

Fuentes:

https://www.cloudways.com/blog/php-security/

# Sending email using PhpMailer with Gmail XOAUTH2

Para crear o hacer mantenimiento se debe entrar al Google Cloud, a través de este link:

<https://console.developers.google.com/>

En el registro se tuvo que poner a Colombia como país de origen porque Venezuela no sale en la lista. La cuenta a usar para este servicio es [***lefre.sistemas@gmail.com***](mailto:lefre.sistemas@gmail.com)

* Nombre del Proyecto:

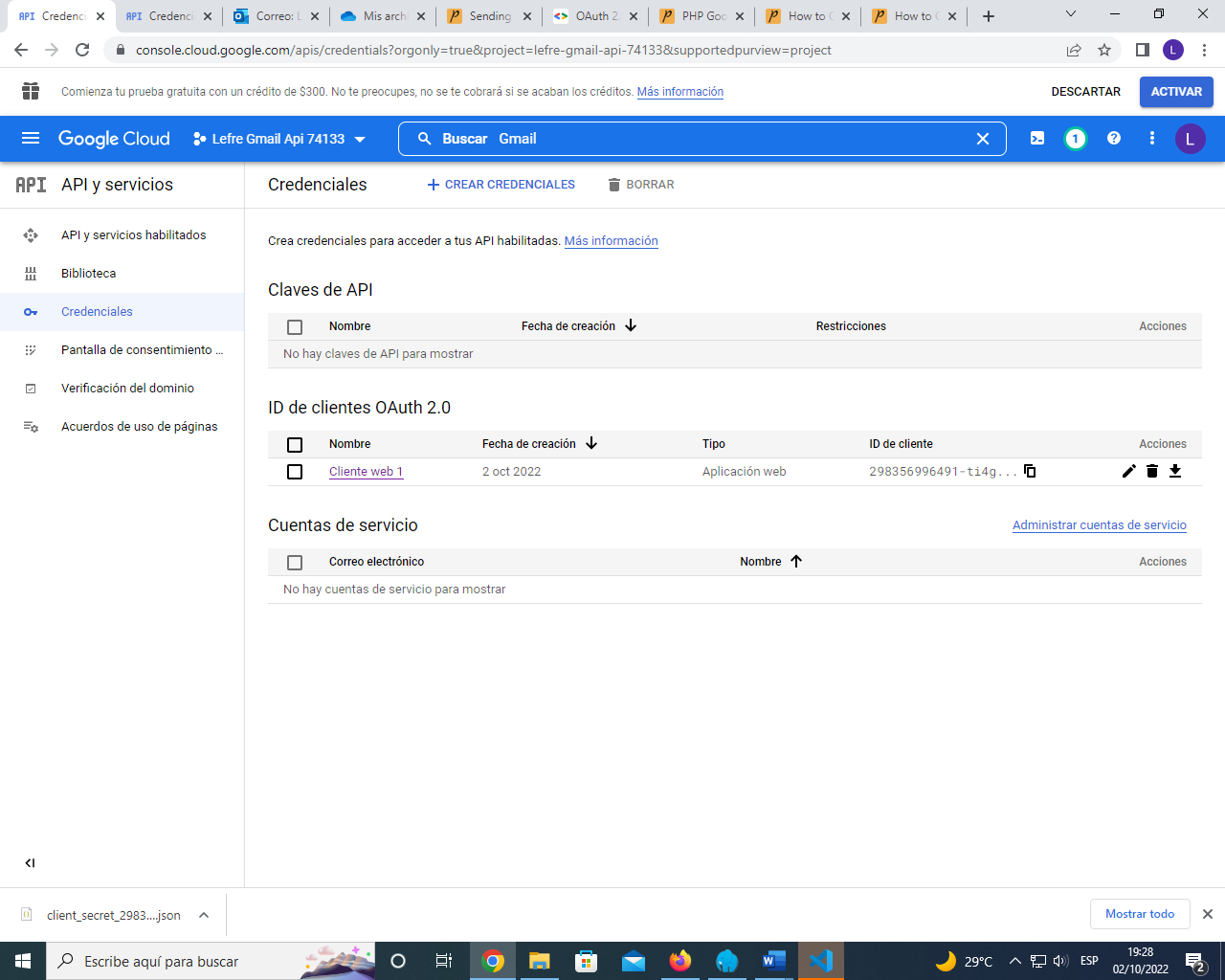
Lefre Gmail Api 74133 (ID: **lefre-gmail-api-74133).**

* **Credenciales:**

**ID. De Cliente:**

**298356996491-ti4gsau2i9jcug0kosqo55ehoqcmt7p1.apps.googleusercontent.com**

**Secreto de Cliente:**

**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**

**Este servicio falla si no se desactiva el servicio de firewall. No se ha investigado cuál es el puerto que usa el protocolo SMTP para comunicarse con los servicios de Google.**

**Es necesario ejecutar un programa llamado mail\_token2.php para refrescar o generar un nuevo Token para usar esta API.**

**Fuente:**

<https://phppot.com/php/sending-email-using-phpmailer-with-gmail-xoauth2/>

https://mailtrap.io/blog/send-emails-with-gmail-api/

**CONCEPTOS DE PRECIOS**

**Precio Bruto:** Es el precio del producto sin haber aplicado descuentos o impuestos. Las personas por lo general hacen referencia a él como Precio Lista o Precio Full. Se recomienda para efectos del sistema manejar el término Precio Bruto.

**Precio Neto:** Es el precio después de haber aplicado descuentos.

**Precio Total:** Es el precio después de haber aplicado Los impuestos.

**GUIA DE MANEJO DE IMÁGENES**

**GALERIAS DE FOTOS.**

Las fotos de los productos deben ser siempre cuadradas y con el background removido. SI la foto es formato webp se puede mantener la transparencia, si es .jpg se debe colocar el fondo en blanco (color por defecto).

A continuación link para ver que browsers aceptan el formato webp (año 2020), aunque siempre he creído que es cuestión de tiempo para que lo usen todos.

https://caniuse.com/#feat=webp

Dimensiones fotos:

1. 1000x1000 (Large)
2. 600x600 (Medium)
3. 300x300 (Small)
4. 100x100 (Thumbnail – no entra en los media queries y está en veremos)

Los thumbnails son imágenes muy especificas y el programador siempre sabrá como usarlos.

Cambiamos los thumbnails de 150x150 a 100 x 100.

Luego que se defina el tamaño máximo como punto de inicio se deben seleccionar tamaños para las distintas pantallas de dispositivos así como para las distintas pantallas del sistema.

* Tamaño grande (cuando se quiera ver en máximo detalle el producto).
* Tamaño regular (en detalle de producto, para ver en detalle del producto).
* Tamaño pequeño (en catálogo de producto, para identificar producto).
* Tamaño extra pequeño (en catálogos o listados, para identificar producto).

Ejemplo código para manejar Imágenes.

Falta incluir las webp en caso que las pueda usar el navegador. Usamos Imágenes PNG o JPG?.Inclimos las webp en los 3 formatos también?

<imgsrc="small.jpg"

srcset="large.jpg 1024w, medium.jpg 640w, small.jpg 320w"

sizes="100vw"

alt="A rad wolf" />

**Nombres de Imagenes**

Al usar la etiqueta <picture> la selección del tamaño de la foto debe estar basada en el ancho de la imagen y no de la relación de aspecto (aspect ratio).

|  |  |
| --- | --- |
| Uso imagen | Ancho de imagen |
| Background | 1980px |
| Desktop | 1660px |
| Tablet | 1440px |
| Mobile | 600px |
| Thumbnail | 150px |

(Las medidas anteriores no son definitivas)

**TAMAÑO DE SLIDERS**

*The Slider widget is normally used with larger sized images for dramatic effect. Sliders commonly stretch from end to end, so it is good to use images with more width to fit the slider. For square sliders, use an even aspect ratio such as 1:1.*

*It is best to choose images with good padding so that the main content of the image is not cut off when resized. The image ratios should be the same in the slider for design consistency.*

* *Commonaspect ratios: 16:9, 3:4*
* *Common resolution sizes (px): 1600x900, 1280x720, 1280x960*

**Tomado de la web:**

[**https://support.duda.co/hc/en-us/articles/360042436054-Image-Size-Guidelines**](https://support.duda.co/hc/en-us/articles/360042436054-Image-Size-Guidelines)

**TIPO DE ARCHIVOS.**

Las fotos de los productos deben estar primeramente en WEBP en sus diferentes dimensiones según el tamaño de la pantalla y su relación de aspecto (Aspect Ratio).

En caso que el navegador no acepte formatos webp, se debe seleccionar formato el formato JPEG (en sus diferentes dimensiones).

**OTROS TIPO DE ARCHIVOS.**

#### Icons

Icons are a very important part of any site. They are visual markers for information and can add a modern look to your site. You can use transparentPNGs, JPEGsorSVGs.

* Common aspect ratios: Generally 1:1, but any aspect ratio will work.
* Common resolution sizes (px): 200x200, 80x80 or any resolution. SVGs can be any resolution.

#### Favicons

Favicons are not used on your actual site, but rather displayed on the tab when users open your website.

* Requiredaspect ratio: 1:1
* Allowed resolution sizes (px): 24x24, 36x36, 48x48

**Tomado de la web:**

[**https://support.duda.co/hc/en-us/articles/360042436054-Image-Size-Guidelines**](https://support.duda.co/hc/en-us/articles/360042436054-Image-Size-Guidelines)

**CONFIGURACION DE PHP 7.4.19**

Esta configuración se propone para hacer el programa más seguro contra ataques o modificaciones de datos.

En el archivo INI de PHP se debe colocar lo siguiente:

* SESSION.USE\_STRICT\_MODE = ON (valor pordefecto OFF).
* SESSION.COOKIE\_HTTPONLY=ON (valor pordefecto OFF).
* SESSION.COOKIE\_SECURE=OFF

Allow access to the session ID cookie only when the protocol is HTTPS. If a website is only accessible via HTTPS, it should enable this setting.

HSTS should be considered for websites accessible only via HTTPS.

* SESSION.use\_trans\_sid=OFF(INVESTIGAR HAY CONTRADICCIÓN EN EL MANUAL DE PHP, contradicción con [session.referer\_check](https://www.php.net/manual/en/session.configuration.php#ini.session.referer-check)).

Disabling transparent session ID management improves the general session ID security by eliminating the possibility of a session ID injection and/or leak.

* SESSION.use\_trans\_sid=OFF
* SESSION.sid\_length=”48” (valor por defecto 26). Solamente a partir de PHP7.1.0
* SESSION.sid\_bits\_per\_character: 6
* SESSION.hash\_function=”sha256” (EN VEREMOS).

Tomado de la web el 09/03/2020.

<https://www.php.net/manual/en/session.security.ini.php>

Valores por defecto que se pueden cambiar en tiempo de ejecución.

<https://www.php.net/manual/es/session.configuration.php>

**OTRAS CONFIGURACIONES PHP**

Verificar que PHP.

File Uploads = ON

upload\_tmp\_dir = /tmp

(en localhost es “C:/laragon/www/tmp”

Upload\_max\_filesize = 3M

post\_max\_size = **150M**

**Si no se configure post\_max\_size podemos obtener este error:**

PHP Warning: POST Content-Length of 63023816 bytes exceeds the limit of 8388608 bytes in Unknown on line 0, referer: <https://my>website.com/upload

**PLUGGINS USADOS.**

1. **Bootstrap-select**:
   1. bootstrap-select.min.css
   2. bootstrap-select.min.js

<!-- Latest compiled and minified CSS -->

<link rel="stylesheet" href="https://cdn.jsdelivr.net/npm/bootstrap-select@1.13.9/dist/css/bootstrap-select.min.css">

<!-- Latest compiled and minified JavaScript -->

<script src="https://cdn.jsdelivr.net/npm/bootstrap-select@1.13.9/dist/js/bootstrap-select.min.js"></script>

<!-- (Optional) Latest compiled and minified JavaScript translation files -->

<script src="https://cdn.jsdelivr.net/npm/bootstrap-select@1.13.9/dist/js/i18n/defaults-\*.min.js"></script>

https://developer.snapappointments.com/bootstrap-select/

**hay un error en este pluggin. Investigando mandan a usar el de Silvio Moreto. Este es el link en Github.**

**https://github.com/silviomoreto/bootstrap-select**

**aparentemente son la misma vaina.**

1. **SweetAlert2**:
   1. datatables.min.css
   2. datatables.min.js

https://sweetalert2.github.io/