UNIVERSIDAD TÉCNICA DE MACHALA

Maestría en Software

Asignatura:

Gestión de la seguridad del software

Tema:

Documente el proceso de implementación de un mecanismo de autenticación de segunda fase utilizando Google Authenticator.

Docente: Ing. Félix Oscar Fernández Peña

Estudiantes:

Ing. Fernando Castillo

Ing. Carlos Quezada

Ing. Esteban Gonzabay

Ing. Jorge Miranda

Ing. Leonardo Caraguay

2021-2022

Proceso de autenticación de segunda fase utilizando Google Authenticator.

Para este caso práctico se utilizó el framework Laravel 8.

1) Descargar la librería que permitirá la interacción con Google autenticator, disponible en https://packagist.org/?query=sonatra%20google

Código de instalación: composer require sonata-project/google-authenticator

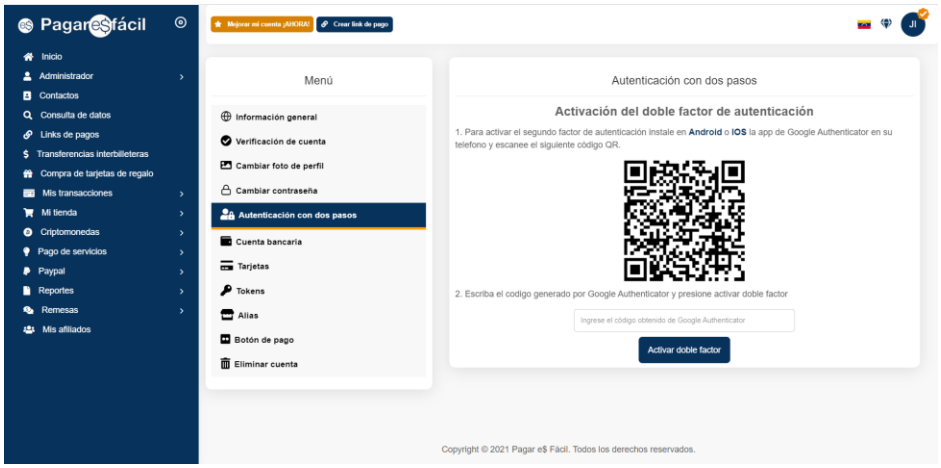
2) Aumentar una variable llamada “two_factor_verification” (opcional) a tu tabla de tu base de datos, para este caso práctico se utilizó Firebase.

```
two_factor_verification: ""
```

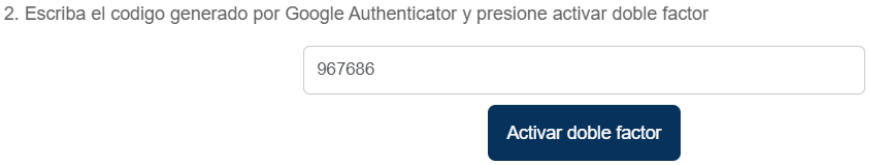
3) Diseñar la vista en donde se plasmará el código QR necesario para escanear con la aplicación de Google Authenticator y así establecer una conexión y obtener un código que posteriormente deberá ingresar.
4) El código fuente utilizado para diseñar el código QR y generar el código secreto necesario para posteriormente realizar una comparación con el código obtenido en el paso anterior es el siguiente:

```php
$g = new \Sonata\GoogleAuthenticator\GoogleAuthenticator();
$secret = $g->generateSecret();
$qrCode = \Sonata\GoogleAuthenticator\GoogleQrUrl::generate(session('displayName'), $secret, "PagarEsFacil");
```

5) El resultado del código anterior es el siguiente:



6) Colocar el código obtenido de la app de Google Authenticator y dar click en activar doble factor.



7) El código para comparar si el código ingresado es correcto es el siguiente:

```php
public function create_tfa(Request $request){
```

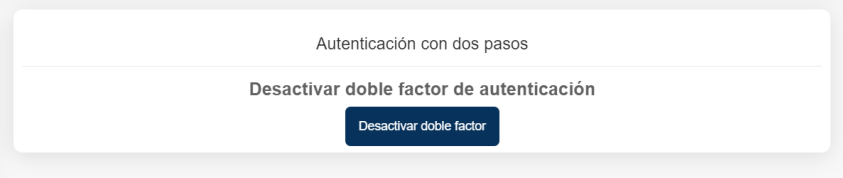
```
        if (session('userId')){

            $userId= session('userId');
            $secretKey= $request->secretKey;
            $code= $request->code;
            $pinSecurityEncriptado= $request->pinSecurityEncriptadoTFA;

            $g = new \Sonata\GoogleAuthenticator\GoogleAuthenticator();
            if ($g->checkCode($secretKey, $code)) {
                $client = new Client(
                    [
                        'base_uri' => 'mi_endpoint_es_secreto',
                        'verify' => false
                    ]
                );


                    $response = $client-
>request('POST', 'updateTokenTwoAutentication', [
                        'form_params'=> [
                            "userId" => $userId,
                            "secretKey" => $secretKey,
                            "pinSecurityEncriptado" => $pinSecurityEncrip
tado

                            ]
                    ])->getBody()->getContents();

                    $respuesta= json_decode($response, true);



                    if($respuesta['code'] == 200){

                        session(['two_factor_verification' => "Si"]);

                        return redirect(url('dashboard/profile').'/#auten
ticacion')->with('mensaje-
exito', 'Código correcto, autenticación de dos pasos activada correctamen
te!');

                    }else{

                        return redirect(url('dashboard/profile').'/#auten
ticacion')->with('mensaje-error', $respuesta['message']);



                    }
            }else{
```

```
                return redirect(url('dashboard/profile').'/#autenticacion
')->with('mensaje-error', 'El código ingresado es incorrecto');

            }


        }else{

            return redirect('/');

        }



    }
```

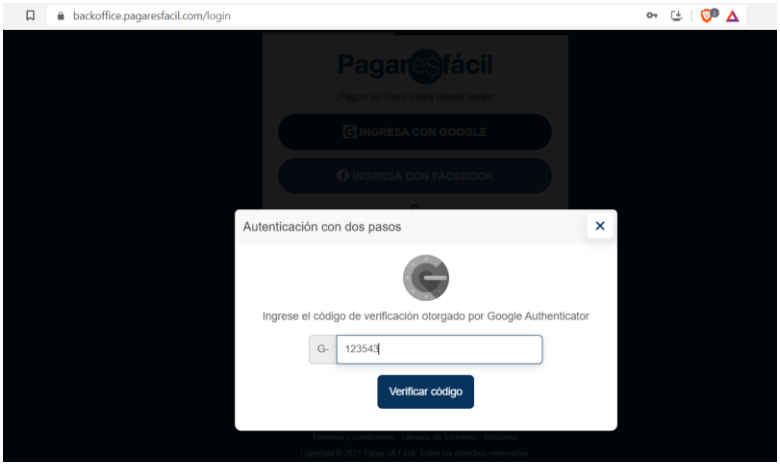
8) El código anterior deberá actualizar la variable two_factor_verification una vez que el código dado por Google es el correcto.

```
two_factor_verification: "Z5VT6CI37ZYG3PUA"
```

9) Si desea desactivar el doble factor de autenticación, se pude diseñar un botón que cuando se de click elimine la variable two_factor_verification de la base de datos.



10) Para probar, se inicia sesión normalmente pero esta vez le solicitará el código de Google.



11) El código para la comprobación del código de Google es el siguiente:

```
    public function checkCodeGoogleAutenticator(Request $request){

        try{

            $secretKey= $request->secretKey;

            $code_google= $request->code_google;

            $g = new \Sonata\GoogleAuthenticator\GoogleAuthenticator();
            if ($g->checkCode($secretKey, $code_google)) {
                return response()-
>json(["code"=>200,"message"=> 'Códigos iguales']);
            }else{

                return response()-
>json(["code"=>400,"message"=> 'Código ingresado incorrecto o caducó, por
 favor intentelo de nuevo']);

            }


        } catch (Exception $e) {

            return response()-
>json(["code"=>400,"message"=> 'Ocurrió un error inesperado, intente de n
uevo']);

        }

    }
```