GUÍA DE SEGURIDAD

Boletín Nro.: 2015-06
Fecha de publicación: 15/04/2015
Tema: Autenticación de Doble Factor

Descripción:

Para realizar la mayoría de las transacciones en Internet, tales como revisar nuestro correo, publicar información, editar un documento, enviar un mensaje a través de una red social, etc., necesitamos autenticarnos en las diversas plataformas.

El método de autenticación más utilizado en las plataformas en internet es, por lejos, el sistema basado en usuario y contraseña.

Desde hace varios años que los ataques a los sistemas de autenticación se han popularizado drásticamente: se han vuelto más frecuentes, más sofisticados, más fáciles de realizar. Hoy en día, un atacante con herramientas de nivel intermedio es capaz de procesar 350 mil millones de contraseñas por segundo.

	Números	**Minúsculas**	**Minúsculas + números**	**Minúsculas + Mayúsculas + números**
6 caracteres	<0,003 milisegundos	< 1 milisegundos	6 milisegundos	0,16 segundos
8 caracteres	0,3 milisegundos	0,6 segundos	8 segundos	10 minutos
10 caracteres	0,3 segundos	6,7 minutos	3 horas	1 mes
12 caracteres	3 segundos	3 días	5 meses	296 años

Además, pueden ser combinados varios tipos de ataque que pueden comprometer todo tipo de contraseñas en tiempos cada vez menores.
Es por eso que deben tomarse una serie de medidas de seguridad adicionales de modo a reducir el riesgo de que un atacante logre obtener acceso a nuestras cuentas, algunas de las cuales pueden ser:

- Utilizar contraseñas robustas
- No utilizar la misma contraseña para todo.

- Cambiar las contraseñas con regularidad. Establezca un recordatorio automático para cambiar las contraseñas de sus sitios web de correo electrónico, banca y tarjetas de crédito cada tres meses aproximadamente.
- No escribir ni reflejar la contraseña en un papel o en documentos donde puedan quedar expuestas.
- Nunca introducir una contraseña en un sitio o programa del cual no tengamos la certeza absoluta de que es legítimo.
- No utilizar herramientas online para crear contraseñas ni para encriptarlas.

Autenticación de Doble Factor

Debido a que han aumentado considerablemente las técnicas para romper o comprometer contraseñas, de diversas formas, las cuales son cada día más sofisticadas, las buenas prácticas muchas veces no son suficientes y nos encontramos con la realidad de que, aún habiendo tomado todas las precauciones, nuestra contraseña se vio expuesta debido a factores que escapan de nuestro control.

Es por eso que surgió el concepto de autenticación de doble factor.

¿Qué es la Autenticación de doble Factor?

Un sistema de doble autenticación es aquel que utiliza dos de los tres factores de autenticación que existen para validar al usuario. Estos factores pueden ser:

- Algo que el usuario sabe (conocimiento), como una contraseña.
- Algo que el usuario tiene (posesión), como un teléfono o *token* que le permite recibir un código de seguridad.
- Algo que el usuario es (inherencia), o sea, una característica intrínseca del ser humano como huellas dactilares, iris, etc.

Por lo general, los sistemas de doble autenticación suelen utilizar los factores conocimiento (nombre de usuario y contraseña) y posesión (teléfono o *token* para recibir código de seguridad

Se trata de una medida de seguridad adicional que complementa la autenticación tradicional en los servicios. En otras palabras, además de requerir un nombre de usuario y contraseña, solicita el ingreso de un segundo factor de autenticación, como puede ser por ejemplo, un código de seguridad. Generalmente, este código se genera en un dispositivo del usuario como un teléfono celular o token. Luego, la persona debe ingresarlo para poder validarse en el sistema.

Con este modelo de autenticación, si un atacante ha logrado obtener el usuario y contraseña de alguna manera, aún así no podrá iniciar sesión debido a que no tendrá forma de obtener el código de seguridad ya que no posee el dispositivo del usuario.

¿Cómo podemos comenzar a usarla?

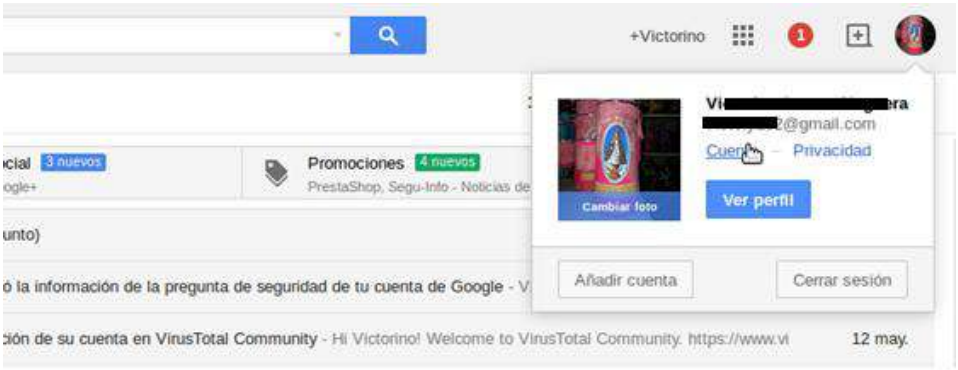
La mayoría de los servicios como Google, Twitter, Outlook, Dropbox, etc. ofrecen esta característica de forma opcional para que cada usuario pueda activarlo. Es importante destacar que este tipo de protección no viene configurada por defecto, por lo tanto, el usuario deberá modificar algunos parámetros para activarla.

Si además, administramos un sitio web o blog basado en CMS como Wordpress, Joomla u otros CMS populares, existen *plugins* que pueden ser integrados fácilmente para brindar una capa adicional a nuestro sitio web.

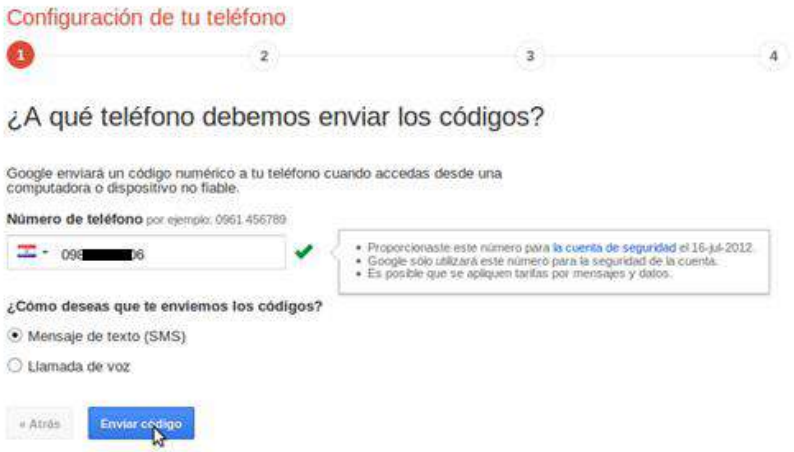
A continuación mostramos cómo activarla en las plataformas más utilizadas.

Google:

1. Iniciamos sesión ingresando a https://accounts.google.com
2. En la esquina superior derecha, hacemos click sobre nuestra imagen de perfil y seleccionamos "Cuenta".

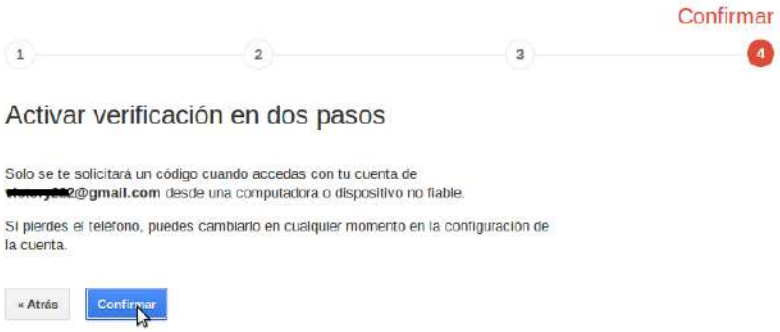


3. Vamos hasta la sección Acceso y veremos que hay una opción "Verificación de dos pasos", que nos dirá si está activada o desactivada. En caso de que esté desactivada, hacer click sobre la opción.
4. En la siguiente pantalla, selecciona "Iniciar configuración", lo que nos abrirá el asistente de configuración.
5. En el primer paso, completar el número de teléfono con el cual deseamos vincular la cuenta, y elegir si queremos recibir el código a través de un SMS o llamada de voz.

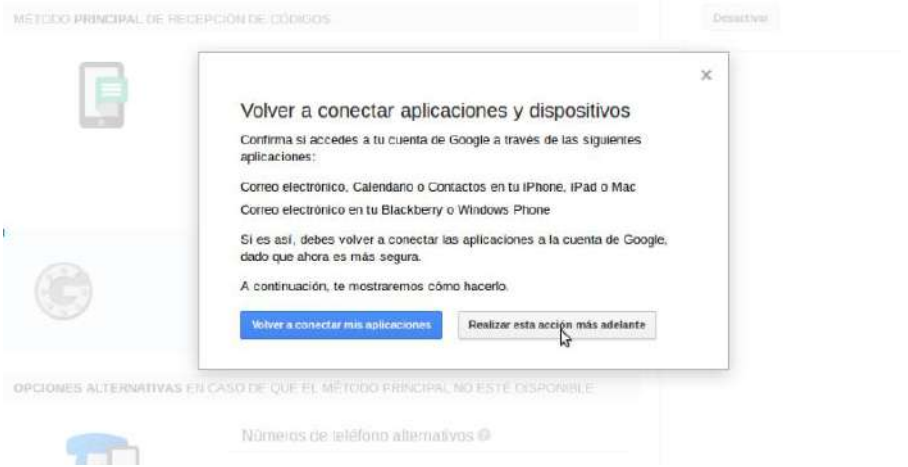


6. A continuación recibiremos un SMS (o una llamada) con un código de 6 dígitos, el cual debemos ingresar en la pantalla.

7. A continuación, se puede elegir si el navegador actual en el que estamos configurando la autenticación será un navegador de confianza o no. Al marcar un navegador como “confiable”, no nos solicitará un código cuando iniciemos sesión en éste. No es recomendable marcar un navegador como “confiable” en caso de que el equipo sea compartido con otras personas.
8. En el último paso hacemos click sobre “Confirmar”, con lo que se ha activado la autenticación de doble factor.



Obs.: Como hemos activado la autenticación de doble factor por primera vez, Google nos desautenticará de sus servicios como Gmail, Calendario, Google+ o Contactos. Nos preguntará si deseamos volver a conectarlas. Podemos elegir “Volver a conectar mis aplicaciones” y seguir las instrucciones, o “Realizar esta acción más adelante”.

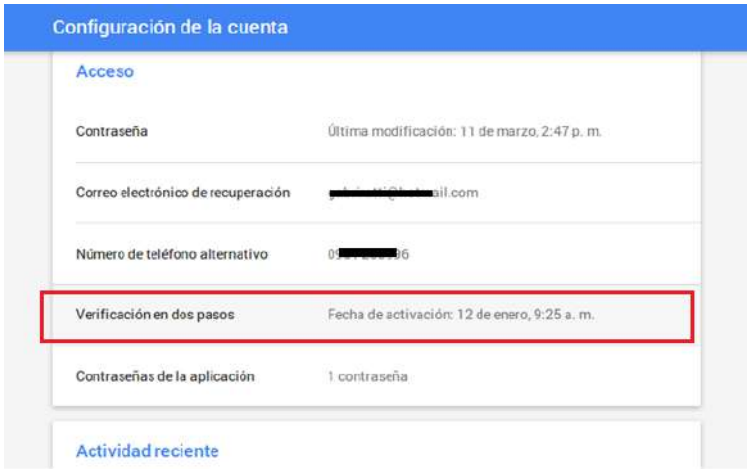


Opcional:

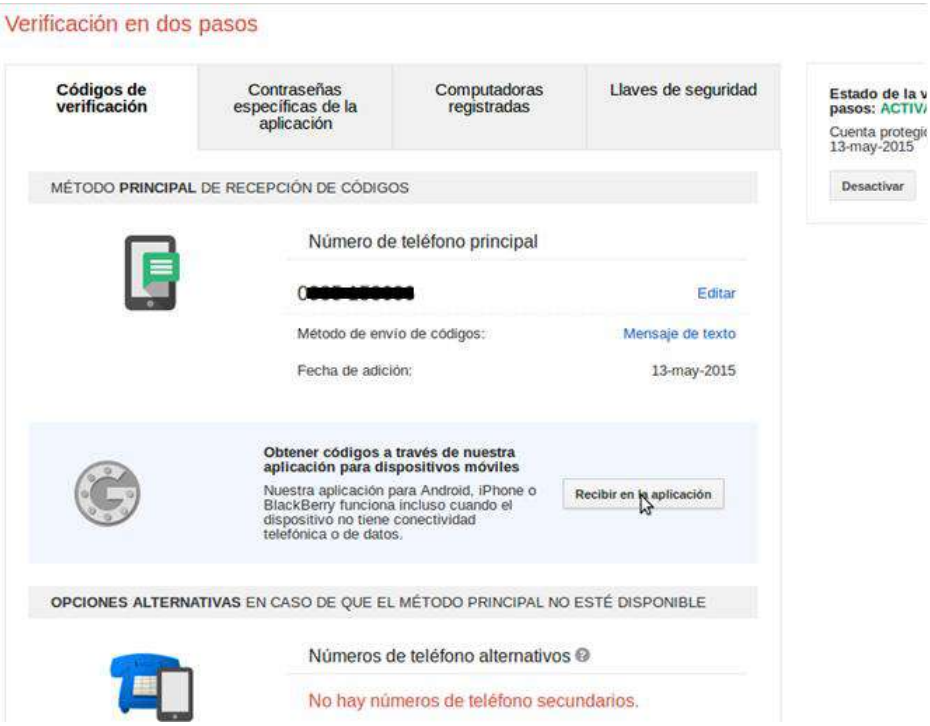
La autenticación de doble factor de Google requiere el envío de un SMS o una llamada, por lo que si no estamos conectados a una red telefónica, la autenticación no será posible. Es por eso que Google además ofrece otro método de recibir el código, a través de una aplicación para el teléfono, Google Authenticator. Este método funcionará incluso cuando no tengamos conectividad telefónica o de datos.

Para que este método funcione, es necesario que la hora del dispositivo móvil esté correctamente sincronizada, por lo que antes de iniciar debemos verificar esto.

1. Para configurarlo, debemos iniciar sesión, entrar a la configuración de la cuenta y hacer click sobre “Verificación de dos pasos”, la cual ahora indicará que fue activada en la fecha en la que lo hicimos.



2. Dentro de la pestaña “Códigos de Verificación”, en la sección “Método principal de recepción de códigos” hacemos click sobre “Recibir en la aplicación”

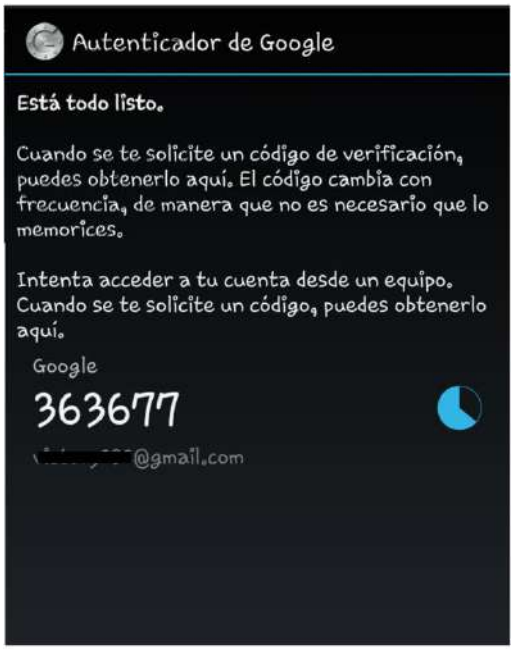


3. A continuación, debemos elegir la opción de acuerdo al sistema operativo que tengamos en nuestro teléfono móvil o en el dispositivo en el cual deseamos recibir el código de verificación. A modo demostrativo, en este manual hemos elegido “Android”. El proceso puede variar ligeramente de acuerdo al sistema operativo y al modelo del teléfono utilizado.
4. Nos aparecerá una guía de configuración con las instrucciones que debemos seguir, paso por paso.

5. Primero debemos instalar la aplicación Authenticator de Google en nuestro teléfono, desde el Google Play Store. Una vez instalada, abrimos la aplicación.

6. En la aplicación, hacemos click en “Comenzar la instalación” y seleccionamos “Escanear código de barras”. Dependiendo del modelo del teléfono, nos podrá pedir que instalemos un lector de códigos adicional, Zxing. En otros modelos, funcionará con el lector de códigos nativos del teléfono.

7. En la aplicación Authenticator seleccionamos “Escanear código” y escaneamos el código QR que aparece en la pantalla del navegador en el que estamos realizando la configuración. Una vez que la aplicación haya reconocido correctamente el código, aparecerá un código de 6 dígitos en la aplicación de nuestro teléfono. Debemos introducir este código en el navegador.



Obs.: Los códigos generados en esta aplicación son dinámicos y tienen un tiempo de vida de 30 segundos, es decir, este código será válido únicamente durante 30 segundos. Transcurrido ese tiempo, el código ya no será válido, por lo que si lo ingresamos para autenticarnos nos dará un error. Siempre debemos asegurarnos de introducir el código antes de que transcurra su tiempo de vida.

Métodos alternativos:

Google permite elegir métodos alternativos de autenticación para los casos en que no tengamos acceso al teléfono que habíamos configurado, por ejemplo en el caso de extravío, daños u otros imprevistos.

En la sección de configuración de la autenticación de dos pasos, en la pestaña “Códigos de verificación”, en “Opciones alternativas” podemos elegir:

1. Números de teléfono alternativos: podemos elegir recibir los códigos a través de un mensaje SMS o una llamada.
2. Códigos de Seguridad: podemos generar 10 códigos de seguridad, cada uno de los cuales será válido por una única vez. Estos códigos pueden ser impresos y/o guardados en un archivo.

Los métodos alternativos se utilizarán solamente cuando, al tratar de iniciar sesión y no poder acceder al método principal, voluntariamente elegimos usarlo. Para ello, ingresamos nuestra contraseña, y cuando nos pida el código de verificación, seleccionamos “Problemas con el código”. Se desplegará un menú donde podemos seleccionar el método alternativo que deseamos usar.

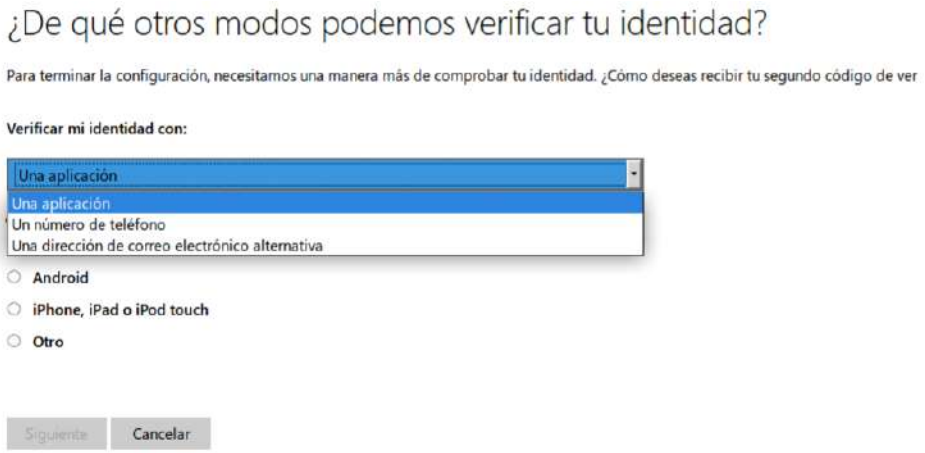
Outlook:

1. Iniciamos sesión ingresando en https://login.live.com/ o en https://outlook.com.
2. Ingresamos a la pestaña “Seguridad y Privacidad” y elegimos “Administrar seguridad avanzada”

Obs.: En caso de que hayamos iniciado sesión desde Outlook, vamos a la esquina superior derecha seleccionamos nuestro perfil y entramos a “Configuración de cuenta”.

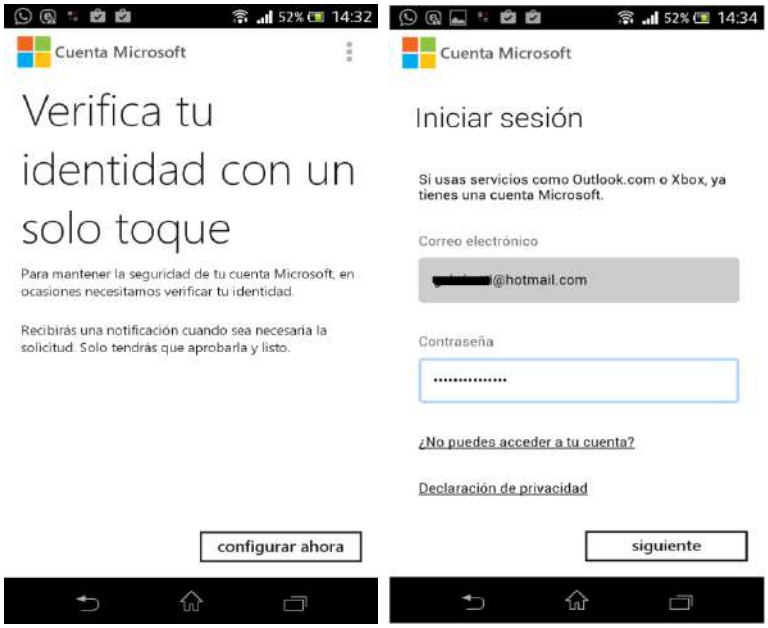
3. A continuación, en la sección “Verificación de dos pasos”, seleccionamos “Configurar la verificación de dos pasos”.

4. Debemos seleccionar el método que queremos utilizar para recibir el código; puede ser a través de:
   - la aplicación para dispositivos móviles
   - un SMS o una llamada a un número telefónico ó
   - un correo a una dirección de correo alternativa.



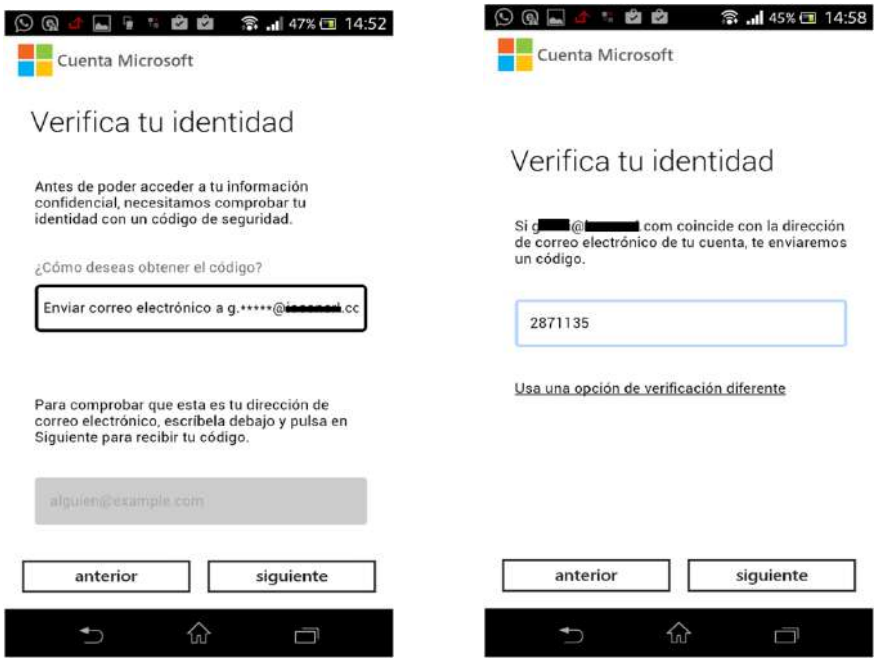
Luego de elegir el método, nos aparecerán instrucciones que deben ser seguidas. A modo de demostración, se elegirá la opción “Una aplicación”, en un dispositivo “Android”. El proceso puede variar ligeramente dependiendo del tipo de dispositivo.

5. En el teléfono, instalamos la aplicación “Cuenta Microsoft” desde el Play Store. Luego de instalar la abrimos y seleccionamos “Configurar ahora”.



6. Completamos la información solicitada (nombre de la cuenta y contraseña) y seleccionamos “Siguiente”.

7. A continuación nos pedirá verificar nuestra identidad, enviando un código de seguridad a nuestra información de verificación que tenemos vinculada ya con anterioridad a nuestra cuenta: un SMS a nuestro número de teléfono o un correo a un correo alternativo. Seguimos las instrucciones, ingresando el código recibido, con lo cual habremos finalizado de configurar la aplicación.

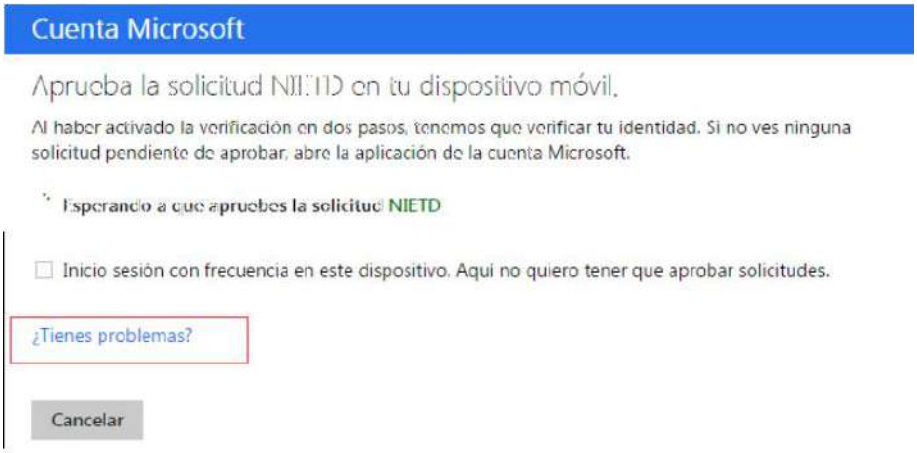


8. En el navegador donde habíamos iniciado la configuración de la autenticación de doble factor, seleccionamos “Siguiente”, con lo cual ha quedado activa la autenticación de doble factor.

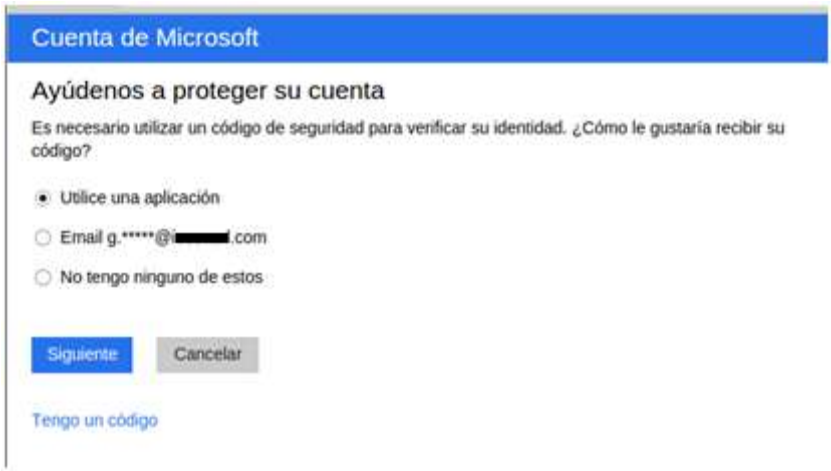
Cada vez que ingresemos nuestro usuario y contraseña, en el dispositivo móvil que hemos configurado nos aparecerá una notificación de inicio de sesión, la cual debemos aprobar. Luego, en unos segundos, el navegador o la aplicación desde donde estamos intentando acceder nos redirigirá a nuestro correo.

Obs.: Es importante configurar correctamente la información de recuperación de la cuenta, tales como números de teléfono alternativos, cuentas de correo alternativas y/o códigos de recuperación. Esto es de suma importancia para poder acceder a nuestra cuenta cuando no podamos utilizar el método de autenticación primario (en el caso de robo del dispositivo móvil, falta de conectividad a redes telefónicas o datos u otros inconvenientes).

En caso de no poder acceder a través del método de autenticación primario, luego de ingresar nuestro usuario y contraseña, cuando nos pide el código de verificación, seleccionamos “Tienes problemas?” o “Si no puedes usar una aplicación en este momento, obtén un código de otra manera” (el mensaje puede variar dependiendo del tipo de dispositivo).



A continuación podemos seleccionar un método alternativo para recibir un código de verificación.



Facebook:

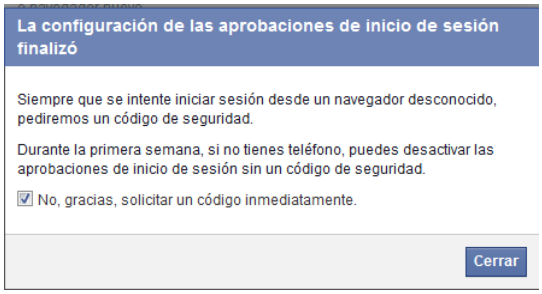
1. Luego de iniciar sesión, vamos al menú de la esquina superior derecha y seleccionamos "Configuración".

2. En la sección "Seguridad", seleccionamos "Aprobación de inicio de sección". Tildamos la opción "Solicitar un código de seguridad para acceder a mi cuenta desde navegadores desconocidos". Seguimos las instrucciones en pantalla.

3. Ingresamos el número de teléfono que deseamos vincular.

4. Recibiremos un mensaje de texto con el código de verificación, el cual debemos ingresar en el campo indicado.

5. Nos solicitará nuestra contraseña antes de continuar.
6. Durante la primera semana posterior a la activación de la autenticación de doble factor, Facebook nos da la posibilidad de iniciar sesión sin código de verificación. Sin embargo, si deseamos activarla de forma inmediata, tildamos la opción “No, gracias, solicitar un código inmediatamente”. Con esto, la autenticación de doble factor quedará activa.



7. En caso de que, cuando se requiera el código de verificación tuvieramos problemas para recibirlo, seleccionamos “¿No encuentras tu código?” y elegimos una opción.

Opcional:

Facebook ofrece métodos alternativos para obtener los códigos de verificación. Para revisar las opciones disponibles entramos a “Configuración” > “Seguridad” > “Aprobación de inicio de sesión”.

Se puede elegir configurar la aplicación de Facebook en el móvil como generador de códigos. Este método funciona cuando no tenemos conectividad a la red telefónica o de datos.

Si esta opción está activa, los códigos no llegarán a través de mensajes de texto.

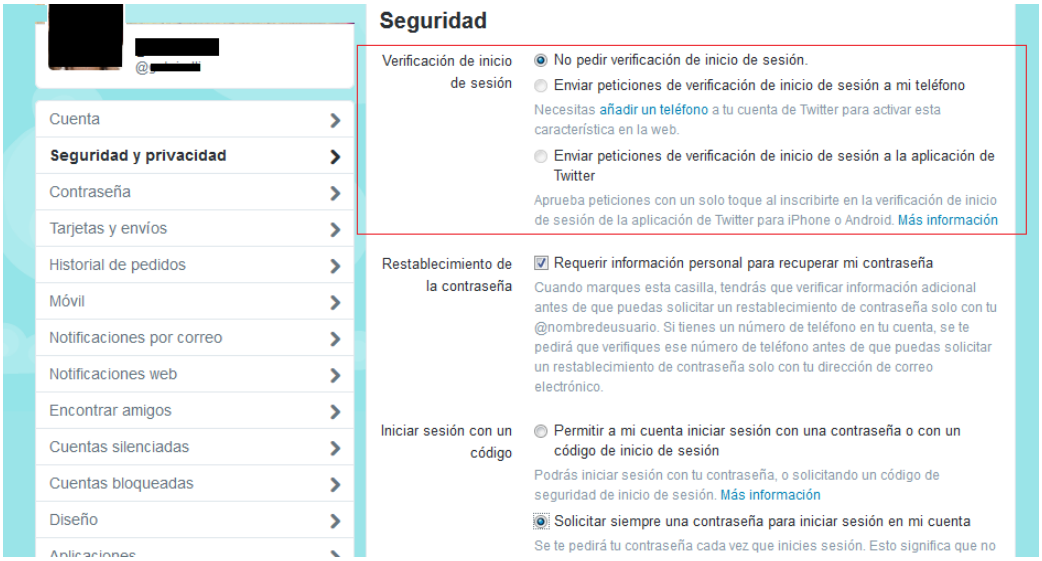
También se puede obtener 10 códigos para utilizarlos cuando no tengamos acceso al teléfono vinculado, como en casos de robo, extravío, daño, etc. Estos códigos servirán una sola vez. Podemos volver a generarlos en el panel de Configuración. Se recomienda imprimir estos códigos y/o guardarlos en un archivo en un lugar seguro.

Obs.: Es importante revisar y completar las configuraciones de seguridad y privacidad disponibles, tales como “Dónde iniciaste sesión”, “Tus navegadores y aplicaciones”, “Alertas de inicio de sesión”, etc. Esto aumentará la efectividad de las medidas de seguridad tales como la autenticación de doble factor.

Twitter:

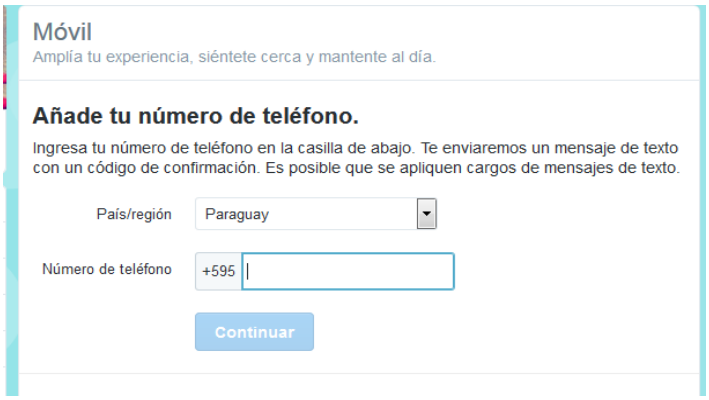
1. Iniciamos sesión y en la esquina superior derecha entramos a la Configuración de nuestra cuenta.

2. En la sección "Seguridad y Privacidad", en la opción de "Verificación de inicio de sesión" tenemos dos posibles métodos que podemos elegir para recibir los códigos de verificación:
   - A través de un mensaje de texto en un teléfono
   - A través de la aplicación de Twitter

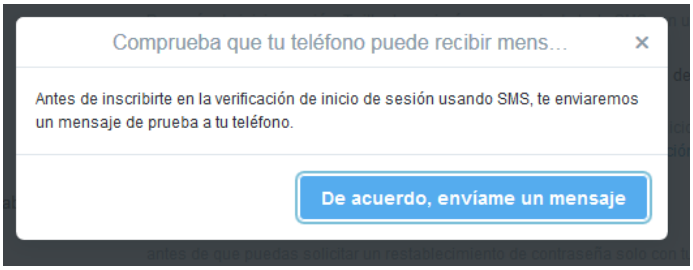


   A modo de demostración, elegiremos el método "Enviar petición de verificación de inicio de sesión a mi teléfono".

3. Hacemos click en el enlace "añadir un teléfono" e ingresamos el número de teléfono que deseamos vincular.



4. Recibiremos un código de confirmación que debemos ingresar antes de continuar.
5. Recién ahora podemos activar la verificación de inicio de sesión en el teléfono. Regresamos a la sección de Seguridad y privacidad y seleccionamos la opción.
6. Nos pedirá una comprobación de que el teléfono vinculado puede recibir mensajes, para lo cual debemos seleccionar "De acuerdo, envíame un mensaje". En caso de recibir un mensaje, lo confirmamos en la siguiente pantalla eligiendo "SI".



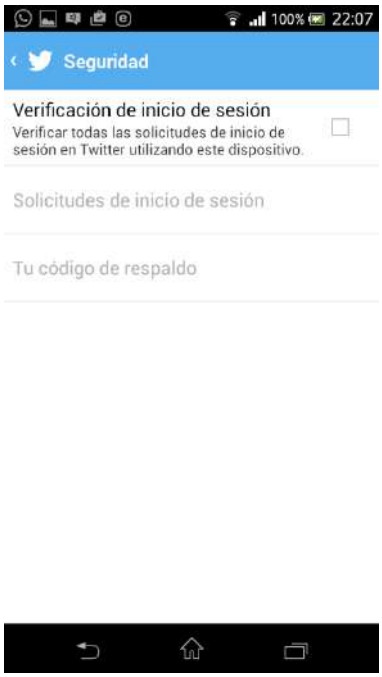
7. Antes de finalizar nos solicitará nuevamente nuestra contraseña, con lo que la autenticación de doble factor quedará activa.

Opcional:

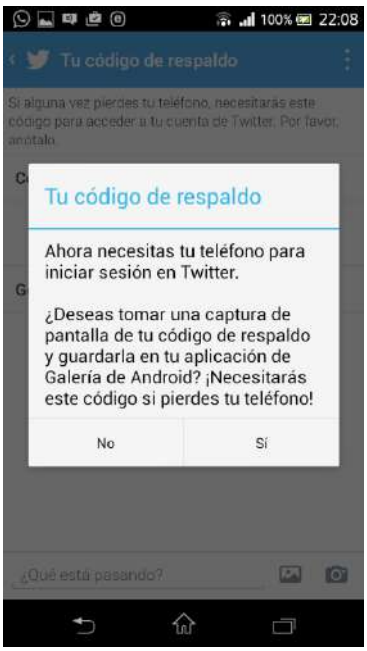
Twitter ofrece un segundo método de autenticación en el cual las solicitudes de inicios de sesión deben ser autorizadas a través de la aplicación de Twitter de un dispositivo móvil determinado. A modo de mostración, mostramos la configuración en un dispositivo Android. En otros sistemas operativos el proceso puede ser ligeramente diferente.

1. Iniciamos sesión en la aplicación de Twitter para Android con nuestro usuario y contraseña. En caso de haber activada la verificación de inicio de sesión a través de un teléfono, debemos introducir además el código de verificación que nos llegará a través de SMS.

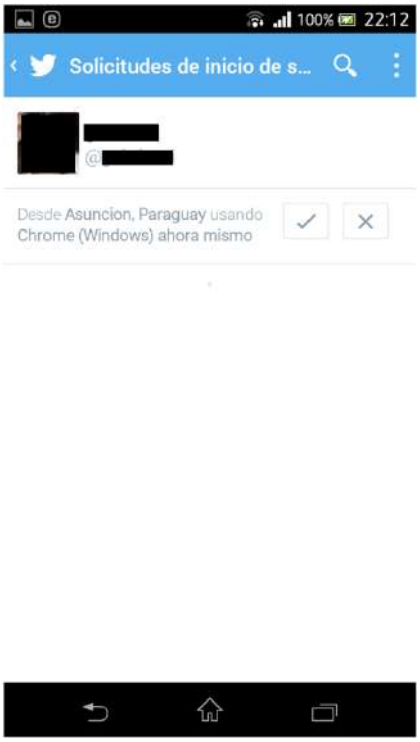
2. En la aplicación, hacemos click sobre los tres puntos en la esquina superior derecha, seleccionamos “Configuración” y elegimos el usuario de la cuenta que deseamos configurar.
3. Entramos en la sección “Seguridad” y tildamos la opción “Verificación de inicio de sesión”. Nos advertirá que necesitaremos iniciar sesión con el dispositivo actual.



4. A continuación se nos solicitará que hagamos una captura de pantalla y/o que guardemos el código de respaldo en caso de que no tengamos acceso al dispositivo, como en caso de robo, extravío, daño u otros imprevistos. Seleccionamos “Si” para resguardar el código de respaldo.



Cuando deseamos iniciar una sesión en otro dispositivo o a través de un navegador, luego de ingresar el usuario y contraseña, recibiremos una notificación en la aplicación que hemos configurado. Debemos aprobar dicha solicitud de modo a que se pueda completar el inicio de sesión desde el otro dispositivo o navegador, que será redirigido luego de la aprobación.

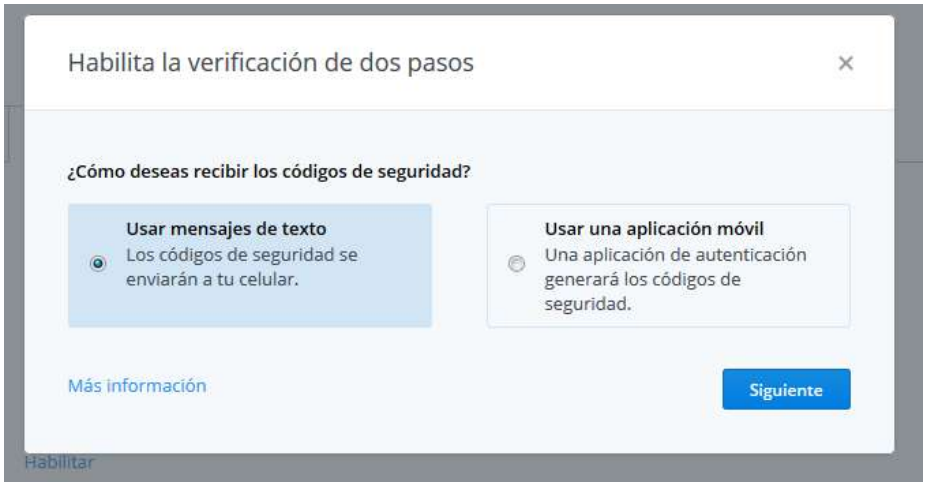


Obs.: Al activar este método, éste pasará a ser el método de verificación principal, por lo que ya no recibiremos mensajes de texto con códigos de verificación. Todas las solicitudes de aprobación de inicio de sesión se recibirán en la aplicación del dispositivo vinculado.

Dropbox:

1. Iniciamos sesión con nuestra cuenta y en la esquina superior derecha seleccionamos "Configuración".
2. Seleccionamos la pestaña "Seguridad", y en la opción Verificación de dos pasos, elegimos "Habilitar".

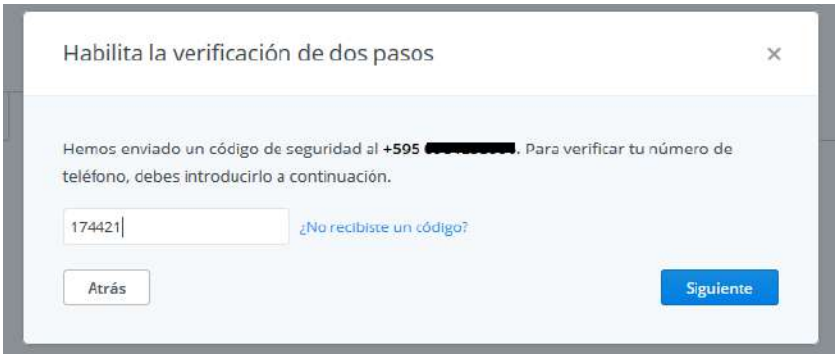
3. Se abrirá un asistente de configuraciones cuyas instrucciones debemos seguir.
4. Introducimos nuestra contraseña para continuar.
5. Dropbox ofrece dos métodos para recibir los códigos de verificación:
   - A través de un mensaje de texto a un número de teléfono
   - A través de una aplicación de autenticación.



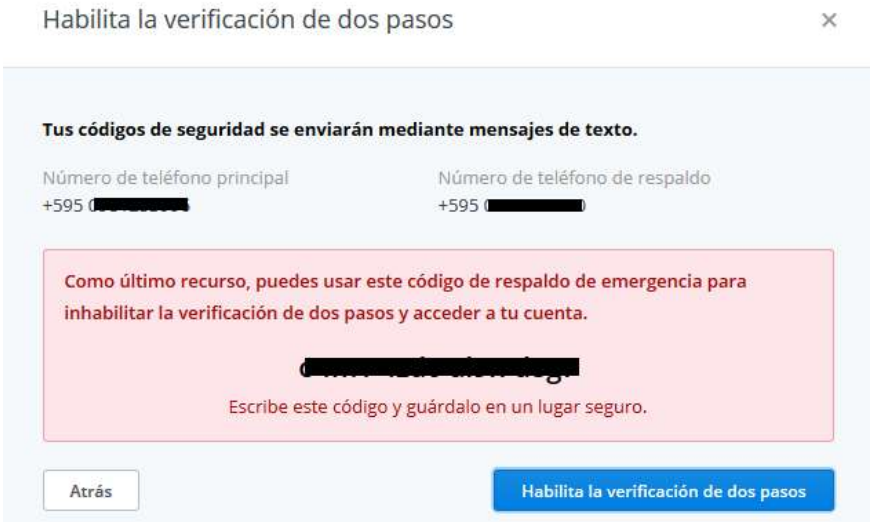
A modo de demostración elegiremos el primer método.

6. Introducimos el número de teléfono que deseamos vincular.

7. A continuación recibiremos un mensaje de texto con el código de verificación, que debemos introducir antes de continuar.



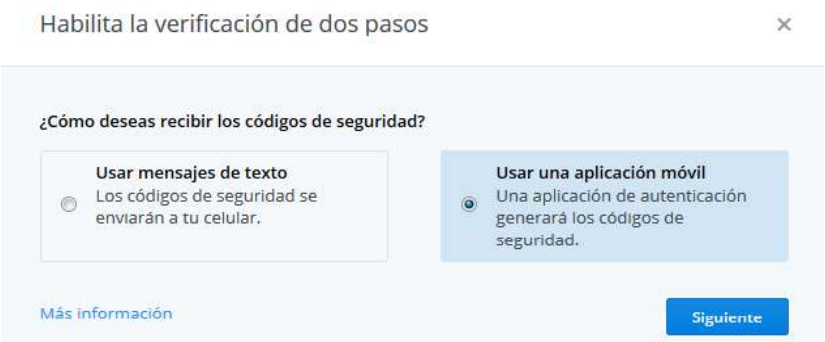
8. Si deseamos, podemos introducir un número de teléfono alternativo en el que podemos recibir el código en caso de que no tengamos acceso al número que vinculamos.
9. Dropbox generará un código de respaldo único que podrá ser utilizado para acceder a la cuenta en caso de que no podamos recibir el código de verificación en ninguno de los números vinculados. Dicho código debe ser guardado en un lugar seguro. Con esto quedará habilitada la autenticación de doble factor.



Opcional:

El método de mensaje de texto a un número celular funcionará únicamente si tenemos conectividad a la red telefónica o de datos. El segundo método, con el cual recibimos el código a través de una aplicación, no requiere que esté disponible ninguna conectividad.

1. En la configuración de la autenticación de doble factor, elegimos el segundo método “Usar una aplicación móvil”.



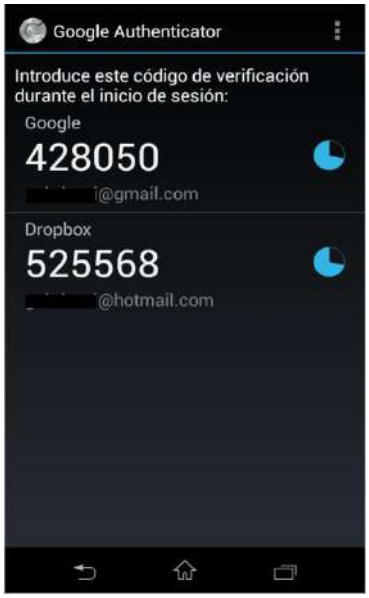
2. Podemos elegir entre varias aplicaciones de autenticación, tales como Authenticator de Google, Duo Mobile, Amazon AWS MFA, etc. A modo de demostración, utilizaremos Authenticator de Google (disponible para iOS, Android y Blackberry desde los app store).

3. Una vez instalada la aplicación Authenticator de Google, la abrimos y hacemos click sobre los tres puntos verticales en la esquina superior derecha y elegimos “Configurar cuenta”.

4. Para añadir la cuenta, seleccionamos “Escanear código de barras”. Luego de que el código QR sea reconocido, la cuenta quedará añadida a la aplicación y se empezarán a generar los códigos.

Obs.: alternativamente, se puede seleccionar la opción de introducir una clave proporcionada, para lo cual debemos hacer click sobre el enlace de “especifica manualmente tu clave secreta”, que se encuentra en el asistente de configuración de Dropbox. Obtendremos una clave que es la que debemos introducir en la aplicación del teléfono.

5. A continuación ingresamos el código de 6 dígitos generado para la cuenta de Dropbox en la aplicación, atendiendo de introducirlo antes de que expire su tiempo de vida.

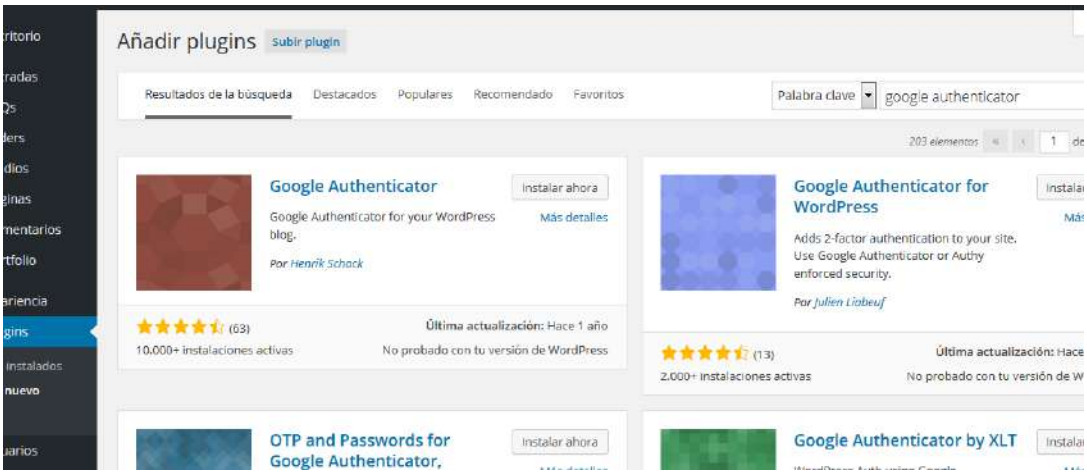


6. Se nos solicita un número de teléfono de respaldo, como método alternativo para recibir el código de verificación si es que no tenemos acceso a la aplicación. Se genera además un código de respaldo de emergencia el cual debe ser guardado en un lugar seguro, en caso de que los demás métodos fallaran o no estuvieran disponibles. Con esto, la autenticación de doble factor quedará habilitada.

Wordpress:

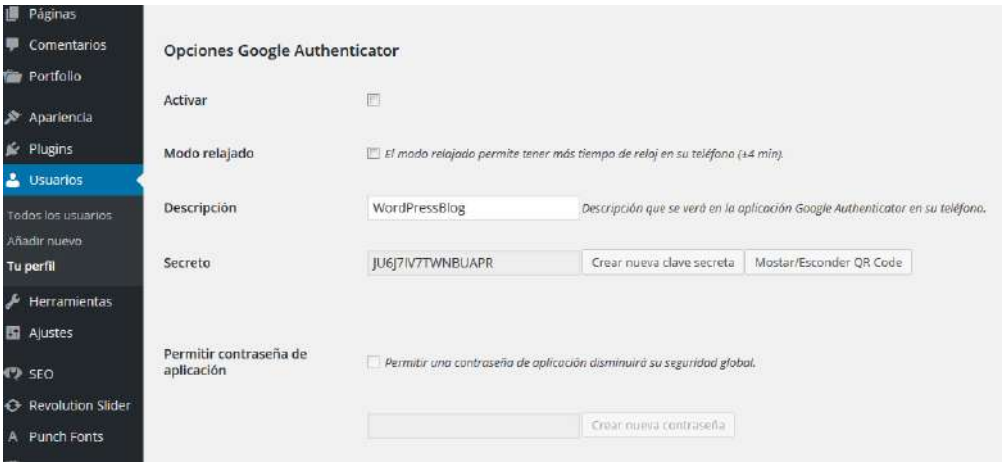
Existen múltiples *plugins* para Wordpress que integran la autenticación de doble factor al sitio web. Muchos de estos *plugins* se basan en el esquema de autenticación de Google, a través de su aplicación Google Authenticator. Veremos cómo implementar uno de estos *plugins* a Wordpress.

1. Iniciamos sesión como Administrador en nuestro sitio web.
2. Vamos a la pestaña "Plugins" y elegimos "Añadir nuevo". Buscando "Google Authenticator", vemos que aparecen varios *plugins*. A modo de demostración elegiremos "Google Authenticator" de Henrik Schack. Seleccionamos "Instalar ahora" y lo activamos.



Obs.: El plugin podría ser descargado de https://wordpress.org/plugins/google-authenticator/ e instalado de forma manual.

3. Para configurarlo, una vez instalado y activado el *plugin*, vamos al perfil del usuario en el que aparecerán unas opciones extras.



4. Tildamos la opción “Activar”.
5. En caso de que lo deseemos, tildamos la opción “Modo relajado”, el cual aumentará el tiempo de vida del código generado por la aplicación. Si no lo tildamos, el tiempo de vida por defecto es de 30 segundos.
6. Editamos la descripción que veremos en la aplicación.
7. Para configurar la cuenta en la aplicación Authenticator de Google (instalada previamente en el teléfono móvil, ver instrucciones en la sección de Google), podemos optar por introducir la clave secreta de forma manual o a través de un código QR. En caso de que deseemos utilizar el código QR, seleccionamos “Mostrar/Esconder QR Code”.

8. Para añadir la cuenta, abrimos la aplicación Authenticator en nuestro dispositivo móvil y seleccionamos “Escanear código de barras”. Luego de que el código QR sea reconocido, la cuenta quedará añadida a la aplicación y se empezarán a generar los códigos.

Obs.: alternativamente, se puede seleccionar la opción “Introducir clave proporcionada”, para lo cual debemos copiar manualmente la clave “Secret” generada en Wordpress.

9. Para finalizar, seleccionamos “Actualizar perfil” en nuestro sitio de Wordpress, con lo que quedará activada la autenticación de doble factor para dicho usuario. La configuración debe realizarse para cada usuario.

Cuando deseamos iniciar sesión en nuestro sitio, nos aparecerá un campo adicional en el cual nos solicitará el código de verificación generado en la aplicación Authenticator.

Información adicional:

http://www.welivesecurity.com/la-es/2014/02/19/doble-factor-autenticacion-que-es-porque-lo-necesito/
https://twofactorauth.org/
https://support.google.com/accounts/answer/180744?hl=es
https://www.google.com/landing/2step/
https://www.facebook.com/help/148233965247823
https://support.twitter.com/articles/20170388
http://windows.microsoft.com/es-xl/windows/two-step-verification-faq
http://answers.microsoft.com/es-es/winphone/wiki/wp8-wppersonal/c%C3%B3mo-instalar-y-utilizar-la-aplicaci%C3%B3n/68db90ff-1e1c-4a62-917a-3f159037f9f9
https://support.apple.com/es-la/HT204152
https://www.dropbox.com/es/help/363
https://en.support.wordpress.com/security/two-step-authentication/