

¿Qué ofrece Autentia Real Business Solutions S.L?

Somos su empresa de **Soporte a Desarrollo Informático**.
Ese apoyo que siempre quiso tener...

1. Desarrollo de componentes y proyectos a medida



2. Auditoría de código y recomendaciones de mejora

3. Arranque de proyectos basados en nuevas tecnologías

1. Definición de frameworks corporativos.
2. Transferencia de conocimiento de nuevas arquitecturas.
3. Soporte al arranque de proyectos.
4. Auditoría preventiva periódica de calidad.
5. Revisión previa a la certificación de proyectos.
6. Extensión de capacidad de equipos de calidad.
7. Identificación de problemas en producción.



4. Cursos de formación (impartidos por desarrolladores en activo)

Spring MVC, JSF-PrimeFaces /RichFaces,
HTML5, CSS3, JavaScript-jQuery

Gestor portales (Liferay)
Gestor de contenidos (Alfresco)
Aplicaciones híbridas

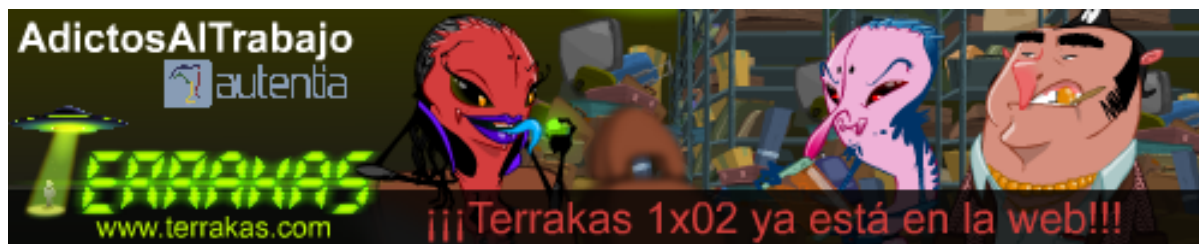
Tareas programadas (Quartz)
Gestor documental (Alfresco)
Inversión de control (Spring)

Control de autenticación y
acceso (Spring Security)
UDDI
Web Services
Rest Services
Social SSO
SSO (Cas)

JPA-Hibernate, MyBatis
Motor de búsqueda empresarial (Solr)
ETL (Talend)

Dirección de Proyectos Informáticos.
Metodologías ágiles
Patrones de diseño
TDD

BPM (jBPM o Bonita)
Generación de informes (JasperReport)
ESB (Open ESB)



[Inicio](#) [Quiénes somos](#) [Tutoriales](#) [Formación](#) [Comparador de salarios](#) [Nuestro libro](#)

» Estás en: **Inicio** **Tutoriales** Verificación en dos pasos de Google: Evitar accesos no autoriz



Director de Desarrollo de Negocio de Autentia

Ingeniero Superior de Telecomunicaciones (UPM) y Executive MBA por el Instituto de Empresa (2007). Perfil [LinkedIn](#) - [Xing](#)

Twitter: [@mmonede](#)

En [Autentia](#) ofrecemos servicios de soporte a desarrollo, factoría y formación. Si queréis saber más sobre nosotros, podéis contactarme en miguel.monedero@autentia.com. Estaré encantado de visitaros en vuestra empresa y contaros lo que hacemos y cómo podemos ayudaros... y además regalaros nuestro libro.

[Ver tutoriales de Miguel Monedero Rico](#)

DESARROLLADO POR:

Miguel Monedero Rico



Fecha de publicación del tutorial: 2012-01-25

Share |

0

[Reg](#)

Verificación en dos pasos de Google: Evitar accesos no autoriza

Índice de contenidos

- [1. Introducción](#)
- [2. La verificación en dos pasos](#)
- [3. Contraseñas específicas de aplicaciones](#)
- [4. Códigos de seguridad imprimibles](#)
- [5. Google Authenticator](#)
- [6. Conclusión](#)

Este tutorial está escrito usando el siguiente entorno:

- Hardware: Portátil MacBook Pro (Intel Core2 Duo 2,53 GHz, 8 GB RAM)
- Sistema Operativo: Mac OS X 10.6.8 Snow Leopard
- Mozilla Firefox 9.0.1
- iPhone 4 iOS 5.0.1
- Google Chrome 16.0.912.77

1. Introducción

Hace unos días me encontré con una desagradable sorpresa. De repente, no podía acceder a mi correo (ni desde el iPhone, ni desde el Mail de Apple) ya que daba error de contraseña incorrecta. Accediendo encuentro el siguiente mensaje de advertencia de Google:

Actividad en esta cuenta

Esta función informa sobre la última actividad que se ha producido en esta cuenta de correo electrónico y sobre

Esta cuenta no parece estar abierta en ninguna otra ubicación. Sin embargo, es posible que haya sesiones de las

Cerrar todas las demás sesiones


Actividad reciente:

Si crees que la actividad que se muestra a continuación no te pertenece, cambia la contraseña ahora mismo.

Tipo de acceso [?] (Navegador, móvil, POP3, etc.)
Desconocido
Desconocido
Navegador
IMAP
Navegador
IMAP
IMAP
IMAP
IMAP
IMAP
IMAP
IMAP
IMAP

Preferencia de alertas: Mostrar una alerta por actividad inusual. [cambiar](#)

* Indica que hay actividad en la sesión actual.

Este equipo utiliza la dirección IP  (España)

Oops, no suena muy bien. Menos mal que Google ha bloqueado mi cuenta para evitar un uso indebido.

Tras recuperar la normalidad de mi cuenta y cambiar la contraseña (si no lo habéis hecho aún, os recomiendo un teléfono o una dirección de mail alternativa en Gmail para recuperar estas situaciones), compruebo si he recibido contactos con spam. Parece que no, menos mal, pero... ¿y la próxima vez?

El problema además dista mucho de ser sólo el mail, sino todos los productos asociados a nuestra cuenta: YouTube, Google Docs, ...

Obviamente, todas las contraseñas son susceptibles de ser averiguadas, así que ¿qué podemos hacer para evitarlo?

En este tutorial voy a presentaros la solución propuesta por Google para evitar accesos no autorizados: la **verificación en dos pasos**. Yo ya lo he puesto en mis cuentas personales, y mucho me extrañaría que no lo hicierais vosotros también.

2. La verificación en dos pasos

La verificación en dos pasos aporta una capa extra de seguridad a nuestra cuenta de Google. Además de introducir la contraseña, debes introducir un código que Google te envía a través de un mensaje de texto (al teléfono o al correo electrónico) cada vez iniciada la sesión.

Esto reduce drásticamente las posibilidades de que otra persona acceda a nuestra cuenta de forma no autorizada en nuestro ordenador o a nuestro teléfono. Por otra parte, podemos autorizar nuestro ordenador durante 30 días en el que no necesitamos la verificación en dos pasos para acceder a la comodidad de la forma de acceso tradicional.

Vamos a ver cómo configurarla.

Entramos en nuestra cuenta de Google, y pulsamos en *Configuración de cuenta*:



Y después en *Uso de la verificación en dos pasos*:

Configuración personal

Seguridad

[Modificación de contraseña](#)[Recuperación de contraseña](#)[Uso de la verificación en dos pasos](#)[Autorización de aplicaciones y de sitios](#)

Panel de control

[Ver datos almacenados de esta cuenta](#)

Direcciones de correo electrónico

miguel.monede@gmail.com (Dirección de correo electrónico)
[Editar](#)

Inicio de sesión múltiple

Desactivado - [Editar](#)

Cuentas conectadas

[Consulta y administra tus cuentas desde otros servicios.](#)

Introducimos nuestro número de teléfono (por defecto nos presentará el empleado para la seguridad d código recibido por SMS:



Configuración de la verificación en dos pasos para miguel.m

[Configura el teléfono](#)[Recordar ordenador](#)[Activar](#)

Añade un número de teléfono móvil o fijo al que Google pueda enviar los códigos [?](#)

Cuando accedas desde un ordenador que no utilices normalmente, te pediremos tu contraseña y código que recibirás en tu teléfono. Esto ayudará a evitar que un desconocido acceda a tu cuenta simplemente con una contraseña robada. [Más información](#)

España

810 12 34 56



Proporcionaste este número para garantizar la [seguridad](#). Google solo utilizará este número para garantizar

por ejemplo: 810 12 34 56

Enviar códigos mediante:

☒ Mensaje de texto SMS

☐ Llamada de voz

Probemos el teléfono

1. Haz clic en Enviar código y comprueba si has recibido el código de verificación en tu teléfono.

Enviar código



Se ha enviado el código.

2. Introduce el código que se envíe a tu teléfono.

Código: 361828

Verificar



Tu número de teléfono está configurado.

Haz clic en Siguiente para continuar.

« Atrás

Siguiente »

[Cancelar](#)

Marcamos la casilla de recordar ordenador:

Configuración de la verificación en dos pasos para miguel.mc

[Configura el teléfono](#)[Recordar ordenador](#)[Activar](#)

Recordar este ordenador

Debes desactivar la casilla que aparece a continuación si estás utilizando un ordenador público o un

☒ Recordar este ordenador durante 30 días

[« Atrás](#)[Siguiente »](#)[Cancelar](#)

y activamos la verificación en dos pasos:

Configuración de la verificación en dos pasos para miguel.mo

[Configura el teléfono](#)[Recordar ordenador](#)[Activar](#)

Activar verificación en dos pasos

Se te pedirá un código cada vez que accedas desde un dispositivo u ordenador desconocidos.

[« Atrás](#)[ACTIVAR VERIFICACIÓN EN DOS PASOS](#)[Cancelar](#)

A partir de ahora, cada vez que intentemos acceder en un ordenador nuevo, nos pedirá, además del usuario, el código que habrá enviado al teléfono configurado.:



Introduce el código de verificación que hemos enviado a tu número de teléfono acabado en 72.

Introduce el código:

[Verificar](#)

☒ Recordar este ordenador durante 30 días

¿No has recibido el mensaje de texto?

[Obtener un código de verificación con una llamada de voz](#)

[Otras formas de obtener un código de verificación »](#)

[Cancelar](#)



NOTA: La gestión de los accesos en nuestro propio ordenador se realiza a través de las c estemos usando. La primera vez podéis probar si funciona correctamente:

- No marcando la casilla en la primera configuración,
- Accediendo con otro navegador,
- Borrando las *cookies* de vuestro navegador o
- Accediendo desde otro equipo.

En cada acceso inicial, os dará la opción de recordar la dupla ordenador/navegador empl

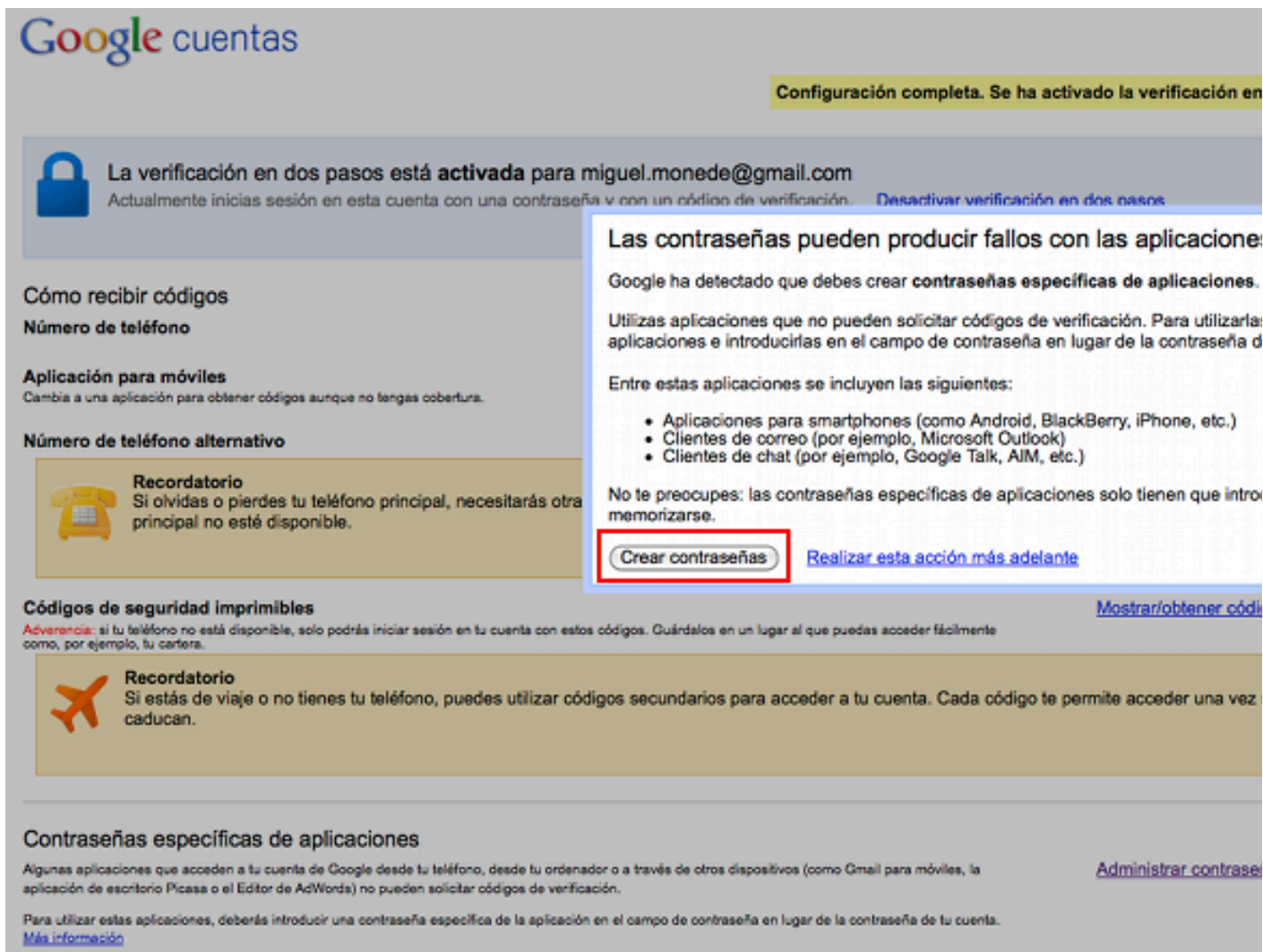
3. Contraseñas específicas de aplicaciones

Si accedéis a vuestra cuenta de Google desde una aplicación externa (en el caso de Gmail, vía POP/IMA dicha aplicación no admita aún la verificación en dos pasos y no pueda solicitar los códigos. Esto incluye

- Aplicaciones para smartphones (iPhone, Android, BlackBerry, ...)
- Clientes de correo (Apple Mail, Microsoft Outlook, ...)
- Clientes de chat (Google Talk, AIM, ...)

Para utilizar estas aplicaciones necesitaremos generar una contraseña específica de la aplicación, y em aplicación externa en lugar de la contraseña de Google.

Una vez activada la verificación en dos pasos, Google (que para eso es muy listo) nos avisará de la circ en este punto podéis comprobar como vuestro mail por POP/IMAP habrá dejado de funcionar):



Google cuentas

Configuración completa. Se ha activado la verificación en dos pasos.

La verificación en dos pasos está activada para miguel.monede@gmail.com
Actualmente inicias sesión en esta cuenta con una contraseña y con un código de verificación. [Desactivar verificación en dos pasos](#)

Cómo recibir códigos
Número de teléfono
Aplicación para móviles
Cambia a una aplicación para obtener códigos aunque no tengas cobertura.
Número de teléfono alternativo

Recordatorio
Si olvidas o pierdes tu teléfono principal, necesitarás otra principal no esté disponible.

Códigos de seguridad imprimibles
Recordatorio
Si estás de viaje o no tienes tu teléfono, puedes utilizar códigos secundarios para acceder a tu cuenta. Cada código te permite acceder una vez caducan.

Contraseñas específicas de aplicaciones
Algunas aplicaciones que acceden a tu cuenta de Google desde tu teléfono, desde tu ordenador o a través de otros dispositivos (como Gmail para móviles, la aplicación de escritorio Picasa o el Editor de AdWords) no pueden solicitar códigos de verificación.
Para utilizar estas aplicaciones, deberás introducir una contraseña específica de la aplicación en el campo de contraseña en lugar de la contraseña de tu cuenta. [Más información](#)

Las contraseñas pueden producir fallos con las aplicaciones:
Google ha detectado que debes crear **contraseñas específicas de aplicaciones**.
Utilizas aplicaciones que no pueden solicitar códigos de verificación. Para utilizarlas: aplicaciones e introducir las en el campo de contraseña en lugar de la contraseña de tu cuenta.
Entre estas aplicaciones se incluyen las siguientes:
• Aplicaciones para smartphones (como Android, BlackBerry, iPhone, etc.)
• Clientes de correo (por ejemplo, Microsoft Outlook)
• Clientes de chat (por ejemplo, Google Talk, AIM, etc.)
No te preocupes: las contraseñas específicas de aplicaciones solo tienen que introducirse una vez.
[Crear contraseñas](#) [Realizar esta acción más adelante](#)

[Mostrar/obtener códigos](#)

[Administrar contraseñas específicas de aplicaciones](#)

Pulsando en *Crear contraseñas*, accedemos a la página específica de administración de contraseñas de

Paso 1 de 2: obtén una nueva contraseña específica de la aplicación

Introduce un nombre que te ayude a recordar la aplicación correspondiente:

Nombre: [Generar contraseña](#)

ejemplos: "Android de Paco", "Gmail en mi iPhone", "GoogleTalk", "Outlook - ordenador de casa" o "Thunderbird"

NOTA: Si queréis acceder posteriormente a esta página de administración, podéis hacerla configuración: *Autorización de aplicaciones y de sitios*, o desde el menú de verificación en *contraseñas específicas de aplicaciones*.

Identificamos el servicio:

Paso 1 de 2: obtén una nueva contraseña específica de la aplicación

Introduce un nombre que te ayude a recordar la aplicación correspondiente:

Nombre:

Generar contraseña

ejemplos: "Android de Paco", "Gmail en mi iPhone", "GoogleTalk", "Outlook - ordenador de casa" o "Thunderbird"

Y obtenemos la contraseña, que simplemente copiaremos en la aplicación (sin espacios). Además, no h motivo que sea la perdemos no tenemos más que generar una nueva (os aconsejo que en ese caso re

Contraseñas específicas de aplicaciones**Paso 2 de 2: introduce la contraseña específica de la aplicación obtenida**

Ya puedes introducir la nueva contraseña específica de la aplicación para acceder a la aplicación.

Note that this password grants complete access to your Google Account. For security reasons, it v displayed again:

zmsu baji erli kaff

No es necesario que recuerdes esta contraseña.
Solo debes introducirla una vez. No se tienen en cuenta los espacios.

Listo

Tus contraseñas específicas de aplicaciones	Fecha de creación	Fecha de último uso
Apple mail Miguel	20-ene-2012	No disponible

NOTA: Podríais sin problema emplear la misma contraseña de aplicación para todas las a identificador no es más que un recordatorio personal). Sin embargo, os aconsejo que gei aplicación externa, para poder revocar el acceso a la misma sin afectar al resto:

Tus contraseñas específicas de aplicaciones	Fecha de creación	Fecha de ú
Apple mail Miguel	20-ene-2012	20-ene-201
iPhone Miguel	20-ene-2012	20-ene-201

Y con esto habríamos terminado. Podéis desactivar cuando queráis la verificación en dos pasos desde e



Configuración completa. Se ha activado

**La verificación en dos pasos está activada para miguel.monede@gmail.com**

Actualmente inicias sesión en esta cuenta con una contraseña y con un código de verificación.

[Desactivar verificación en dos p...](#)[¿Tienes dificultades para iniciar sesión c...](#)

Cómo recibir códigos

Número de teléfono



Aplicación para móviles

Cambia a una aplicación para obtener códigos aunque no tengas cobertura.

Número de teléfono alternativo

[Añ...](#)

Recordatorio

Si olvidas o pierdes tu teléfono principal, necesitarás otra forma de obtener los códigos. Al añadir un teléfono secundario, podr principal no esté disponible.

Códigos de seguridad imprimibles

[Mo...](#)**Advertencia:** si tu teléfono no está disponible, solo podrás iniciar sesión en tu cuenta con estos códigos. Guárdalos en un lugar al que puedas acceder fácilmente como, por ejemplo, tu cartera.

Recordatorio

Si estás de viaje o no tienes tu teléfono, puedes utilizar códigos secundarios para acceder a tu cuenta. Cada código te permite caducan.

Contraseñas específicas de aplicaciones

Algunas aplicaciones que acceden a tu cuenta de Google desde tu teléfono, desde tu ordenador o a través de otros dispositivos (como Gmail para móviles, la aplicación de escritorio Picasa o el Editor de AdWords) no pueden solicitar códigos de verificación.

[Ad...](#)

Para utilizar estas aplicaciones, deberás introducir una contraseña específica de la aplicación en el campo de contraseña en lugar de la contraseña de tu cuenta.

[Más información](#)

NOTA: Si desactiváis la verificación, podréis seguir funcionando con las contraseñas específicas de las aplicaciones. Google guardará la configuración realizada (salvo que la borréis explícitamente) por si queréis volver a activarla en el futuro. Tanto en activación como en desactivación, Google os enviará un mail a vuestra cuenta avisando de la configuración realizada.

Sin embargo, vamos a ver un par de detalles más, para el caso de que no tengamos nuestro teléfono disponible o sin cobertura (en el extranjero sin *roaming*, por ejemplo).

4. Códigos de seguridad imprimibles

Para el caso de que necesitéis acceder al correo y no tengáis disponible vuestro teléfono, conviene generar códigos de seguridad imprimibles (que podéis guardar protegidos en el ordenador, llevar en la cartera, ...), que os permitirán acceder a la cuenta sin necesidad de un teléfono.

Para generarlos, desde la página de configuración de la verificación:

Cómo recibir códigos

Número de teléfono

Aplicación para móviles

Cambia a una aplicación para obtener códigos aunque no tengas cobertura.

Número de teléfono alternativo

Códigos de seguridad imprimibles

Advertencia: si tu teléfono no está disponible, solo podrás iniciar sesión en tu cuenta con estos códigos. Guárdalos en un lugar al que puedas acceder fácilmente como, por ejemplo, tu cartera.

Los códigos se generan en bloques de diez, y cada código será válido únicamente para un acceso. Una revoca los anteriores, aunque no hubieran sido empleados:

Impresión de los códigos de verificación de seguridad

[Imprimir](#) - [Guardar como archivo de te](#)

Códigos de verificación de seguridad

- | | |
|---------------|----------------|
| 1. 138 07 378 | 6. 418 41 084 |
| 2. 802 53 357 | 7. 131 76 777 |
| 3. 856 48 781 | 8. 822 18 044 |
| 4. 853 18 781 | 9. 181 80 413 |
| 5. 858 61 234 | 10. 302 12 044 |

Hora de impresión: 20 de enero de 2012 3:16:28 PST

Guarda los códigos en un lugar seguro (por ejemplo, en tu cartera) y al que puedas acceder fácilmente cada vez que utilices tu equipo o tu teléfono móvil. Cada código se puede utilizar una vez.

Si vuelves a generar códigos de seguridad posteriormente, asegúrate de eliminar las versiones anteriores, ya que solo será válido el conjunto de códigos más reciente.

[Generar códigos nuevos](#)

Y ahora el último detalle, probablemente el más espectacular.

5. Google Authenticator

No deja de ser pesado recibir mensajes cortos cada vez que queremos acceder en un ordenador nuevo donde estemos o no tengamos cobertura o servicio. Si tenemos un smartphone, disponemos de una aplicación para generar los códigos de acceso: **Google Authenticator**.

Para acceder a la misma, en la página de configuración:

Cómo recibir códigos

Número de teléfono

Aplicación para móviles

Cambia a una aplicación para obtener códigos aunque no tengas cobertura.

Número de teléfono alternativo

Códigos de seguridad imprimibles

Advertencia: si tu teléfono no está disponible, solo podrás iniciar sesión en tu cuenta con estos códigos. Guárdalos en un lugar al que puedas acceder fácilmente como, por ejemplo, tu cartera.

Pulsando en nuestro modelo de smartphone (iPhone en mi caso), accedemos a la página de configuración para la aplicación y, oh sorpresa, un código QR para que la configuración de la misma sea instantánea:

Instala la aplicación de verificación para iPhone

1. En tu iPhone, toca el icono App Store.
2. Busca **Google Authenticator**. ([URL de iTunes](#))
3. Toca la aplicación y, a continuación, toca la opción de descarga gratuita para descargarla e instalarla.

Abre y configura Google Authenticator

1. En Google Authenticator, toca + y, a continuación, la opción Escanear código de barras.
2. Utiliza la cámara del teléfono para escanear el código de barras.



[+ ¿No puedes escanear el código de barras?](#)

Una vez configurada la aplicación, introduce el código obtenido y haz clic en Verificar.

Código:

[Cancelar](#)

Instalamos la aplicación (gratuita, por supuesto):

App Store > Utilidades > Google



Google Authenticator

Descripción

Google Authenticator works with 2-step verification for your Google Account to provide secure signing in. Use Google Authenticator to generate verification codes directly on your phone, without the need for a computer.

[Soporte técnico de Google Authenticator >](#)

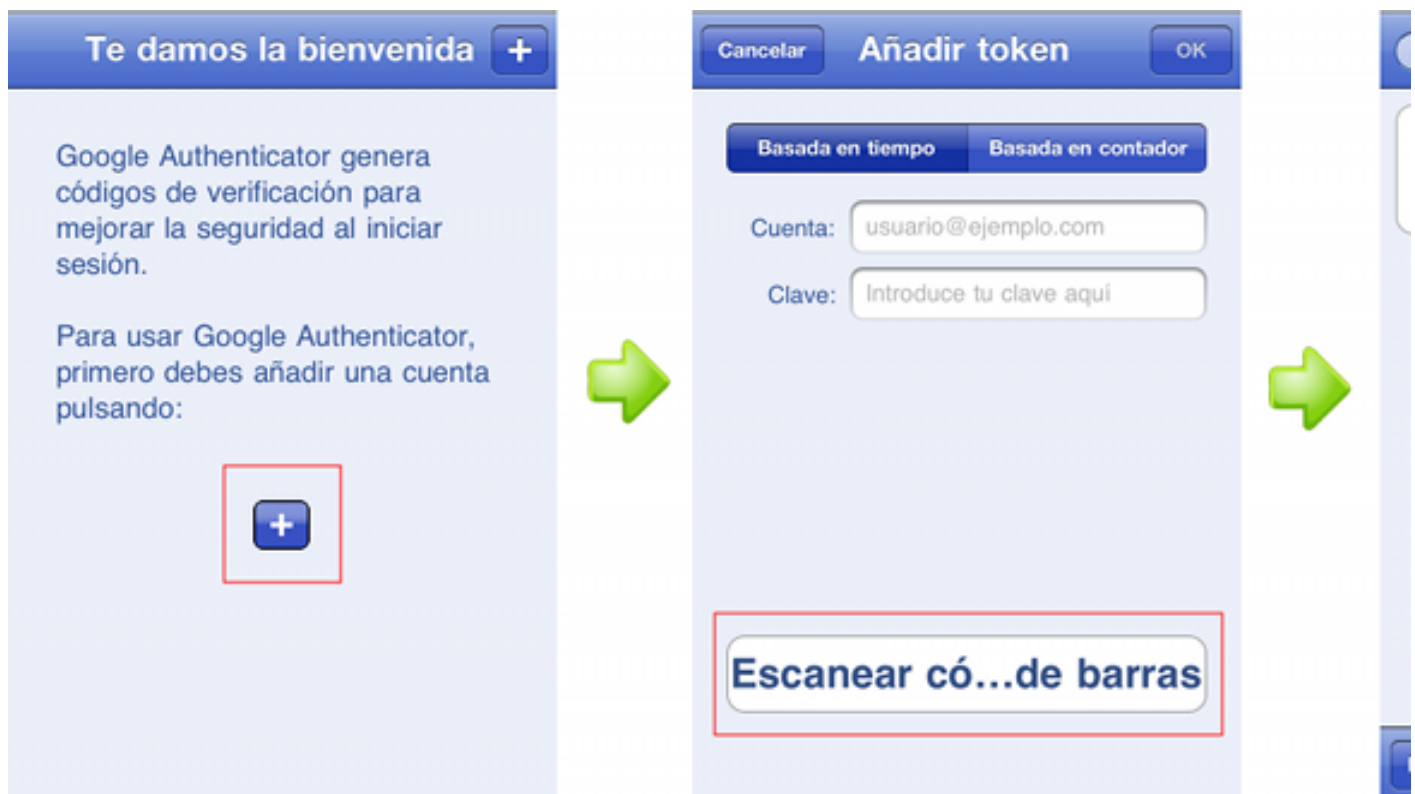
Lo nuevo en la versión 1.1.4.755

- Support for multiple languages
- Dropped minimum required iOS version to 3.1.3

App gratuita

Categoría: Utilidades
Actualizado: 19/07/2011
Versión: 1.1.4.755
Tamaño: 0.6 MB
Idiomas: Español, Árabe, Búlgaro,

Y la configuramos usando el código QR, que tan amablemente nos ofrece Google (la propia aplicación a



The image shows a sequence of three screenshots from the Google Authenticator app, connected by green arrows indicating the flow of the setup process.

- First Screenshot:** A welcome screen titled "Te damos la bienvenida" with a plus icon. It explains that Google Authenticator generates verification codes to improve security. It instructs the user to add an account by tapping a plus icon, which is highlighted with a red box.
- Second Screenshot:** A screen titled "Añadir token" with "Cancelar" and "OK" buttons. It has two tabs: "Basada en tiempo" (selected) and "Basada en contador". It contains input fields for "Cuenta:" (with the example "usuario@ejemplo.com") and "Clave:" (with the placeholder "Introduce tu clave aquí"). At the bottom, a button labeled "Escanear código de barras" is highlighted with a red box.
- Third Screenshot:** A partial view of the next screen, showing a QR code being scanned by the app's camera.

Por último, introducimos el código obtenido en la página de configuración:

Abre y configura Google Authenticator

1. En Google Authenticator, toca + y, a continuación, la opción Escanear código de barras.
2. Utiliza la cámara del teléfono para escanear el código de barras.



[+ ¿No puedes escanear el código de barras?](#)

Una vez configurada la aplicación, introduce el código obtenido y haz clic en Verificar.

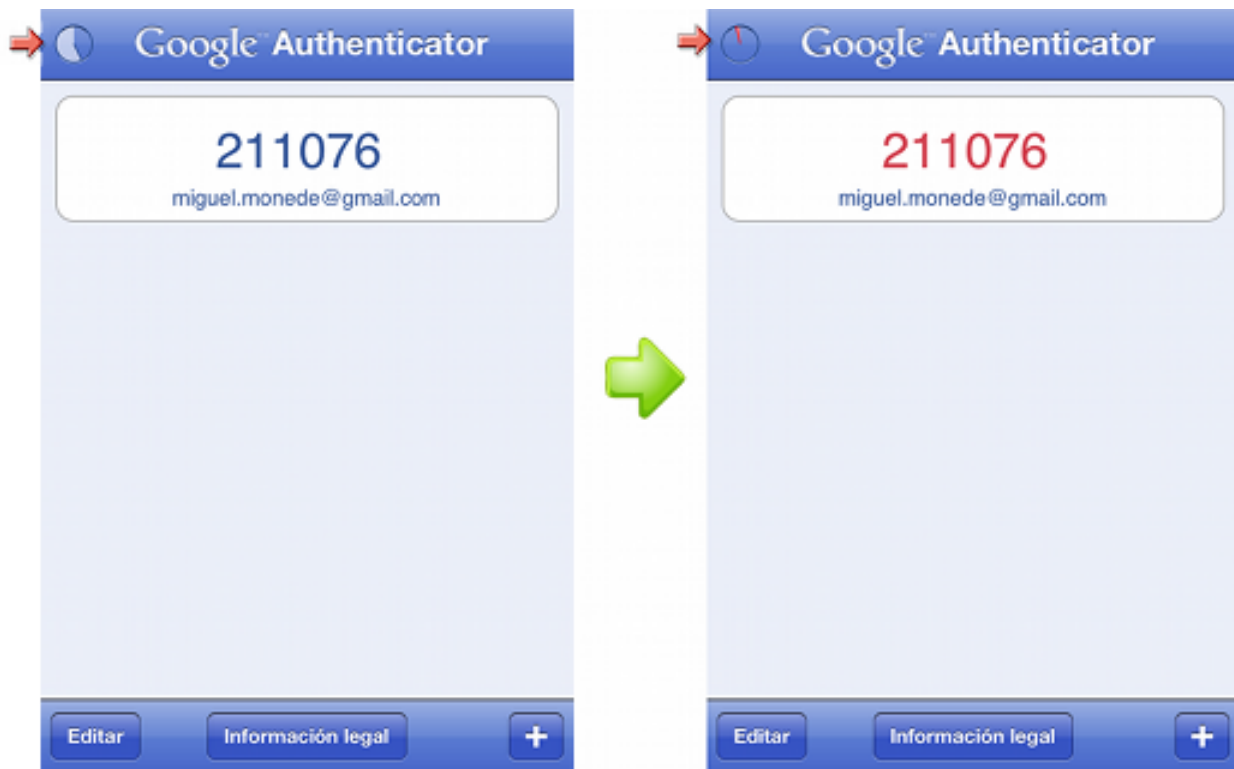
Código:

✓ El dispositivo iPhone está configurado.

y ya estamos listos.

Ya tenemos una aplicación para realizar la verificación en dos pasos sin necesidad de mensaje corto ni

Los códigos son válidos solamente durante medio minuto:



y la misma aplicación vale para todas vuestras cuentas de Google:



Al acceder desde un nuevo ordenador o navegador, ya no enviará automáticamente el mensaje corto, introduzcamos el código generado por Google Authenticator:



Introduce el código de verificación generado por tu aplicación para móviles.

Introduce el código:

☒ Recordar este ordenador durante 30 días

[Otras formas de obtener un código de verificación »](#)

[Cancelar](#)

NOTA: Google automáticamente modifica la configuración de nuestra cuenta para que el antes, aparezca ahora como método alternativo de acceso:

Cómo recibir códigos

Aplicación para móviles

✓ iPhon

Número de teléfono alternativo

✓ 8427

Códigos de seguridad imprimibles

[Mostrar](#)

Adverencia: si tu teléfono no está disponible, solo podrás iniciar sesión en tu cuenta con estos códigos. Guárdalos en un lugar al que puedas acceder fácilmente como, por ejemplo, tu cartera.

y nos permite, en cualquier nuevo acceso, elegir que método vamos a emplear:



6. Conclusión

Seguro, fácil, cómodo, versátil y simple de configurar, incluso con el detalle de ofrecer un código QR (y aplicación) para que ni siquiera tengas que introducir la cuenta en el móvil para Google Authenticator.

En mi opinión, un gran acierto de Google para ofrecernos una capa extra de seguridad para nuestras cuentas, yo ya lo he configurado en mis cuentas personales (y en breve en la de la oficina, ya que tengo Google Apps). Ya estáis tardando en hacer lo mismo ;-)

Como siempre, espero que os haya resultado útil. Para cualquier comentario, ya sabéis dónde estoy.

Actualización

Y ya está puesto en la cuenta de Autentia con Google Apps ;-)



Sólo necesitáis que vuestro administrador de dominio active la posibilidad (luego es elección de cada uno).

Por favor, vota +1 o compártelo si te pareció interesante

Share |

También puedes seguirnos a través de:



Anímate y coméntanos lo que pienses sobre este **TUTORIAL**:

Puedes opinar o comentar cualquier sugerencia que quieras comunicarnos sobre este tutorial; con tu mejor servicio.

Enviar comentario

(Sólo para usuarios registrados)

» **Registrate** y accede a esta y otras ventajas «



Esta obra está licenciada bajo [licencia Creative Commons de Reconocimiento-No com](#)

IMPULSA

Impulsores

Comunidad

[¿Ayuda?](#)

sin clicks

0 personas han traído clicks a esta página

+ + + + + + + +

powered by [karma](#)

Copyright 2003-2012 © All Rights Reserved | [Texto legal y condiciones de](#)

W3C XHTML 1.0

W3C CSS

XML RSS