Sociedad Andaluza para el Desarrollo de las Telecomunicaciones
CONSEJERÍA DE EMPLEO, EMPRESA Y COMERCIO

seguridad+ Y CONFIANZA DIGITAL | AndalucíaCERT CENTRO DE SEGURIDAD TIC

Informe de divulgación

Uso de autenticación multi-factor en sistemas y aplicaciones II

Tipo de documento:	*Informe*
Autor del documento:	*AndalucíaCERT*
Código del Documento:	*CERT-IF-10039-161116*
Edición:	*0*
Categoría	*Uso Interno*
Fecha de elaboración:	*16/11/2016*
N° de Páginas	*1 de 24*

1 Tabla DE CONTENIDOS

2 OBJETO

El objeto de este documento es explicar al lector cómo configurar un segundo factor de autenticación en ciertas aplicaciones y servicios.

3 ALCANCE

Este documento va dirigido tanto al personal de la Junta de Andalucía, como al público en general. Pretende continuar con el anterior informe divulgativo elaborado por AndalucíaCERT sobre el uso de los métodos de autenticación multifactor en sistemas y aplicaciones. En particular, en el presente documento se expondrán algunos ejemplos de configuración de un segundo factor de autenticación en diversas aplicaciones y servicios ampliamente extendidos.

4 INTRODUCCIÓN

En el anterior informe divulgativo elaborado por AndalucíaCERT se concienció al lector sobre la importancia de las identidades digitales que posee, centrándonos en el proceso de autenticación y cómo lograr securizarlo. Para ello, se explicó en qué consistían los sistemas de autenticación multifactor y se pusieron algunos ejemplos de uso.

En el presente informe vamos a continuar desde ese punto de partida y nos centraremos en explicar al lector cómo configurar un segundo factor de autenticación en algunas aplicaciones y servicios muy conocidos y usados. El informe abarca el uso de diversos servicios, que si bien no son de uso oficial a nivel corporativo, sí que son ampliamente utilizados para asuntos personales, en el ámbito no laboral.

Por ello, antes de continuar repasaremos algunos conceptos que el lector debería tener asimilados tras la lectura de nuestro anterior informe.

4.1 Repaso de conceptos

Se entiende por identidad al conjunto de atributos que describen de forma unívoca a una persona en un contexto determinado.

Cuando un usuario ingresa en alguna aplicación o sistema (es decir, hace *login*) lo que realmente está haciendo es probar su identidad frente a dicha aplicación o sistema. Este procedimiento se realiza mediante la autenticación.

El proceso de autenticación es de vital importancia, puesto que se encarga de verificar la identidad de un usuario antes de darle acceso a los sistemas y aplicaciones que protege. No obstante, suele ser uno de los eslabones más débiles, puesto que la mayor parte de las veces suele basarse en el uso de la tradicional dupla usuario/contraseña.

Los sistemas de autenticación múltiple o MFA (*Multi Factor Authentication*) suponen un intento de bastionar el proceso de autenticación. Para ello, se basan en la combinación de dos o más factores de autenticación: un factor de conocimiento (algo que sólo el usuario sabe), un factor de posesión (algo que sólo el usuario posee), y un factor inherente al usuario (algo que sólo el usuario es).

De entre todos los sistemas de autenticación por factores múltiples, el más usado suele ser el 2FA (*Second Factor Authentication*), que implica la combinación de dos de los factores de autenticación anteriormente mencionados (generalmente, un factor de conocimiento y otro de posesión). En la práctica implica que, tras haber introducido los ya tradicionales usuario/contraseña en alguna aplicación o sistema, se le solicite al usuario algún token generado por un dispositivo que sólo él debe poseer.

En el mercado existen diversas alternativas para implementar mecanismos de 2FA, siendo dos de las más usadas el envío de mensajes de texto SMS y el servicio *Google Authenticator*, que se basa en el RFC 6238 del IETF para generar códigos TOTP (*Time-based One Time Password*). Esto es, genera contraseñas de un sólo uso gracias a un algoritmo que toma como entradas el instante de tiempo actual y una clave secreta precompartida entre la aplicación o sistema frente a la que el usuario se quiere autenticar y el software de *Google*.

5 Ejemplos de uso

En los siguientes epígrafes de este informe se le indicará al lector cómo puede configurar un sistema 2FA en diversas aplicaciones y sistemas.

5.1 Correo electrónico

El correo electrónico es un servicio de red que permite a los usuarios enviar y recibir cartas digitales mediantes redes de comunicación electrónica. En Internet existen multitud de estos servicios que incluyen a empresas, proveedores de servicios de Internet y proveedores de correo tanto libres como de pago.

Dos de los proveedores gratuitos más usados a nivel mundial son *Gmail* de *Google* y *Outlook* de *Microsoft*.

5.1.1 Google

En realidad, lo que vamos a hacer no será añadir un segundo factor de autenticación a una cuenta de *Gmail*, sino a una de *Google*. Es decir, que también se añadirá un 2FA a todos los servicios a los que se puede acceder gracias a una cuenta de la empresa del buscador: almacenamiento en la nube, calendario, álbum de fotos...

Para configurar el uso de un segundo factor de autenticación en nuestra cuenta de *Google* se debe acceder a la dirección http://accounts.google.com/SmsAuthConfig, autenticarse y proporcionar un número de teléfono válido. Al hacerlo, le habremos indicado a la empresa *Google* una forma en la que

poder contactar con nosotros para el envío de códigos de verificación mediante mensajes de texto SMS o mensajes de voz (según nuestras preferencias).

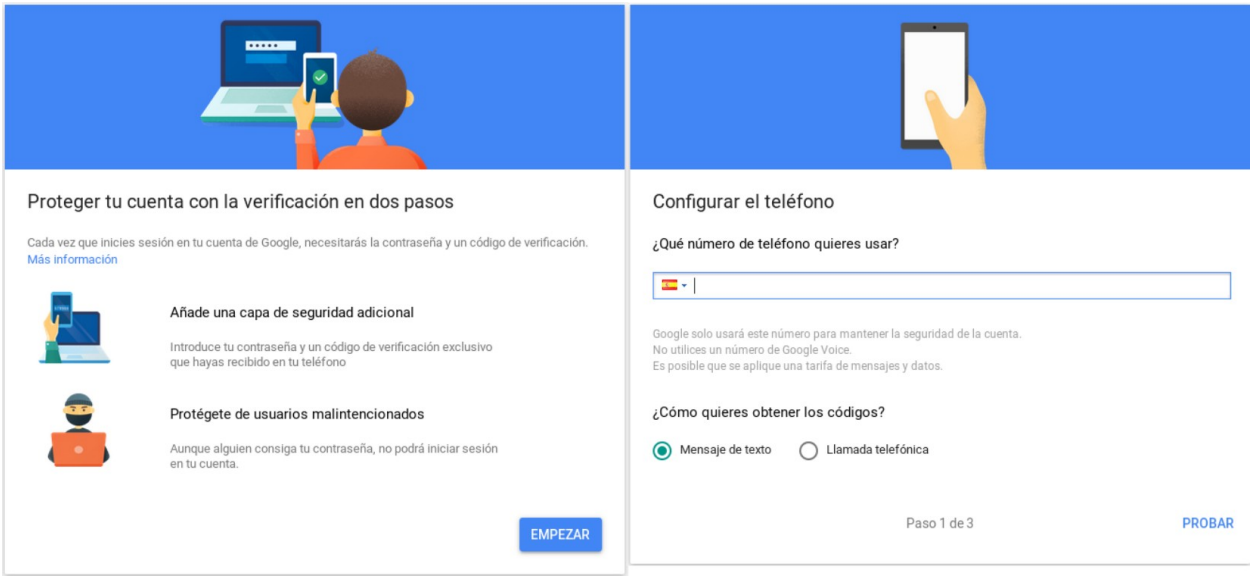

Figura 1. Configuración inicial de un 2FA para la cuenta de *Google*. Pantalla para proporcionar el número de teléfono y la forma de contacto preferida.

Una vez realizado este paso, *Google* se pondrá en contacto con nosotros para proporcionarnos una contraseña de un sólo uso consistente en un número de 6 cifras. Deberemos indicarle dicho código a la web para que el sistema lo verifique.

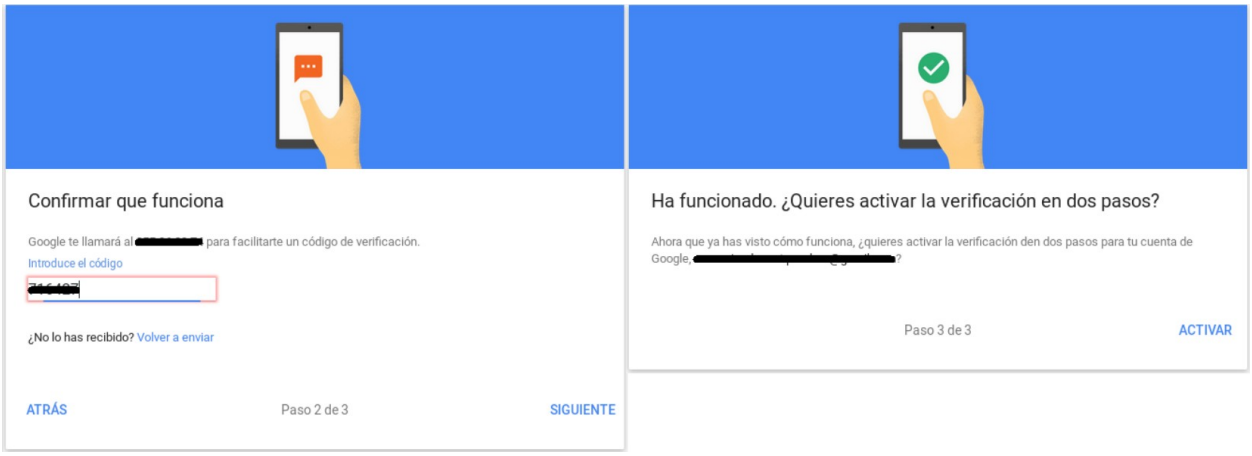

Figura 2. Configuración inicial de un 2FA para la cuenta de *Google*. Pantalla para proporcionar el código de verificación recibido.

Hay que indicar que una vez realizado este paso, a todos los efectos, ya tendremos configurado un sistema 2FA en nuestra cuenta de *Google*, puesto que a partir de ahora cada vez que queramos iniciar sesión se nos preguntará por un código de verificación que nos llegará en forma de SMS o llamada telefónica. De hecho, el gigante de *Mountain View* proporciona diversos métodos para el uso de sistemas de autenticación múltiple. Al acceder a la página de configuración de la verificación en dos pasos se observa la siguiente Figura:

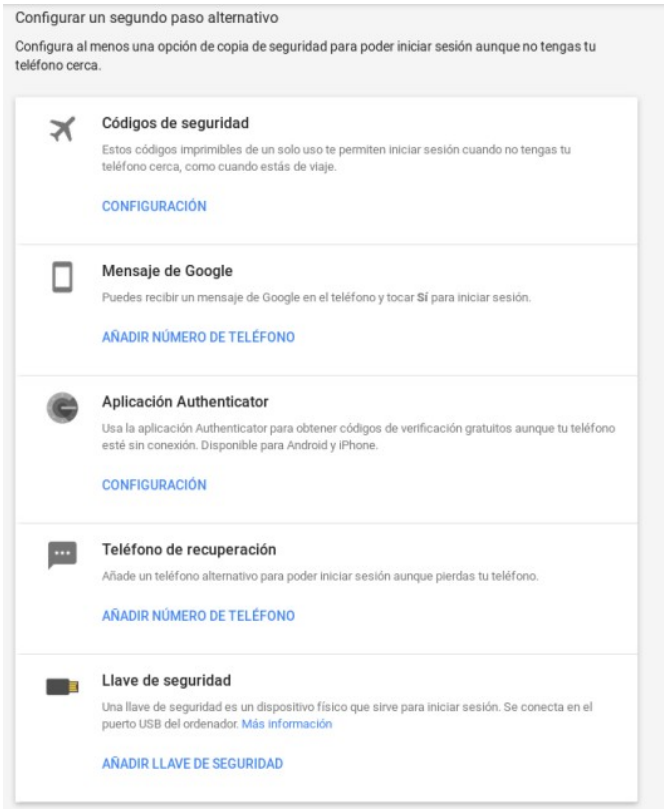

Figura 3. Opciones de configuración de un segundo factor de autenticación en *Google*.

Como se puede observar, además de mediante un SMS o una llamada telefónica, es posible configurar el uso de la aplicación *Google Authenticator* o incluso una llave USB tipo *Yibikey*.

Otra de las características a destacar son las opciones "Códigos de seguridad" y "Teléfono de recuperación". Hay que tener en cuenta que, al configurar un 2FA para nuestra cuenta de *Google*, lo que realmente estamos haciendo es añadir un factor de posesión, es decir, le estamos indicando a *Google* que tenemos en propiedad un dispositivo que puede recibir/generar códigos OTP pero, ¿qué sucede si perdemos dicho dispositivo? Para evitar que nuestra cuenta quede inaccesible es posible configurar algunas opciones de recuperación.

Mediante la opción "Códigos de seguridad" *Google* nos proporciona un total de 10 códigos únicos que deberemos guardar cautelosamente, puesto que serán la única forma de recuperar la cuenta en caso de pérdida o mal funcionamiento del dispositivo seleccionado para obtener los códigos OTP del 2FA.

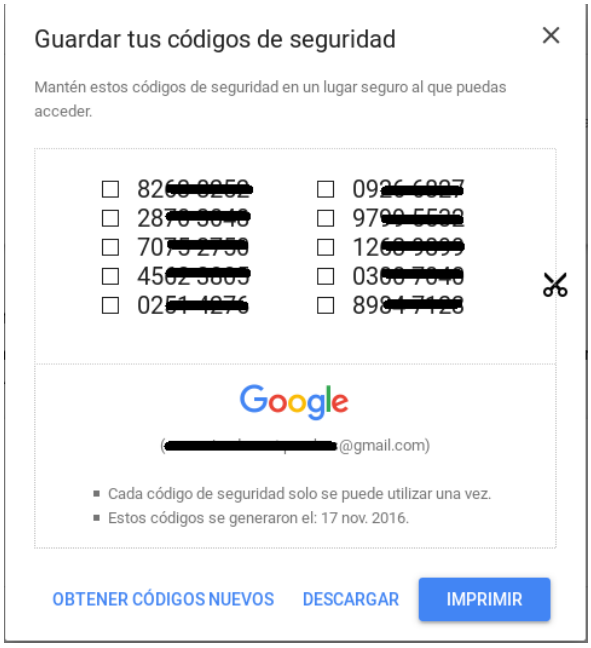

Figura 4. Códigos de recuperación para la cuenta de *Google*.

La opción "Teléfono de recuperación" es análoga a la anterior. Simplemente se debe proporcionar un número de teléfono (se entiende que distinto al configurado inicialmente) para que *Google* pueda ponerse en contacto con nosotros en caso de que necesitemos recuperar la cuenta.

Hay que tener en cuenta que, debido a la adición de un segundo factor de autenticación para el acceso a nuestra cuenta, es posible que algunas aplicaciones que dependan de ella dejen de funcionar (especialmente aquellas instaladas en nuestro *smartphone*). En tal caso será necesario generar una contraseña de aplicación siguiendo los pasos que se detallan en [9].

5.1.2 Microsoft Live

Al igual que en el epígrafe anterior, no sólo vamos a proteger nuestra cuenta de correo de *Outlook* con un segundo factor de autenticación, sino que se protegerán todos los servicios que la empresa *Microsoft* ofrece a través de *Microsoft Live*.

Para ello, el primer paso consiste en autenticarnos con nuestra cuenta en la siguiente dirección https://login.live.com

Una vez autenticados debemos acceder al menú "Seguridad y privacidad", donde deberemos seleccionar "Más opciones de configuración de seguridad". Y dentro de esta página deberemos acceder a la opción "Configurar la verificación en dos pasos".

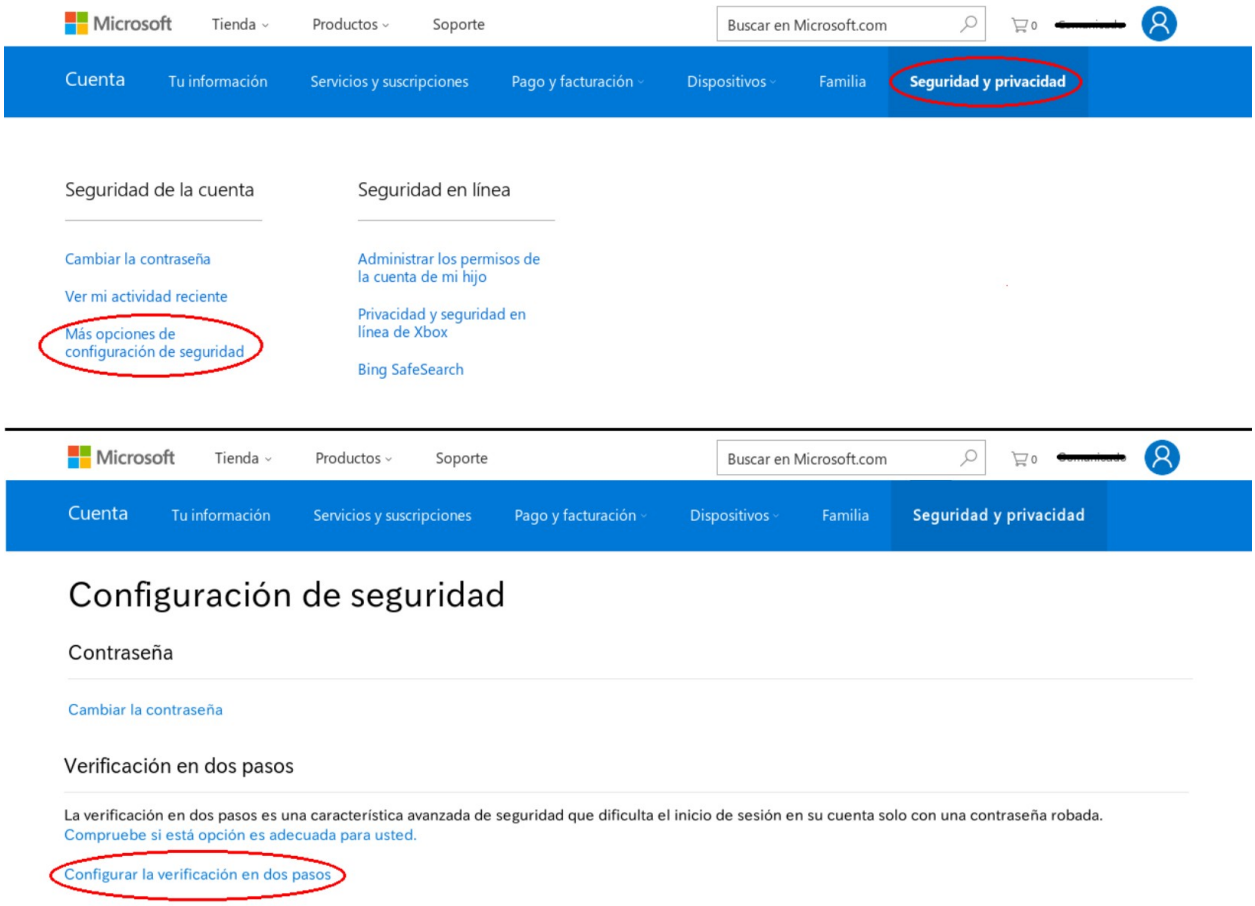

Figura 5. Acceso a la configuración de un 2FA en la web de *Microsoft Live*.

Llegados a este punto, desde Microsoft nos ofrecerán varios métodos para añadir un segundo factor de autenticación: el uso de una aplicación para generar códigos TOTP, un número de teléfono o una cuenta de correo distinta de la que estamos usando (y que puede ser de cualquier proveedor). En este ejemplo realizaremos la configuración del 2FA usando *Google Authenticator*, por lo que la opción que debemos seleccionar es "Una aplicación".

Respecto al tipo de dispositivo en el que instalar la aplicación debemos seleccionar "Otro" (el resto de opciones requieren la instalación de la app *Microsoft Authenticator*, que aunque es igual de válida que *Google Authenticator*, resulta menos flexible y su uso está menos extendido).

Al hacerlo, nos aparecerá una pantalla con todos los datos necesarios para configurar el 2FA en una aplicación como *Google Authenticator*, que previamente hemos debido instalar en nuestro terminal móvil desde un *market* oficial.

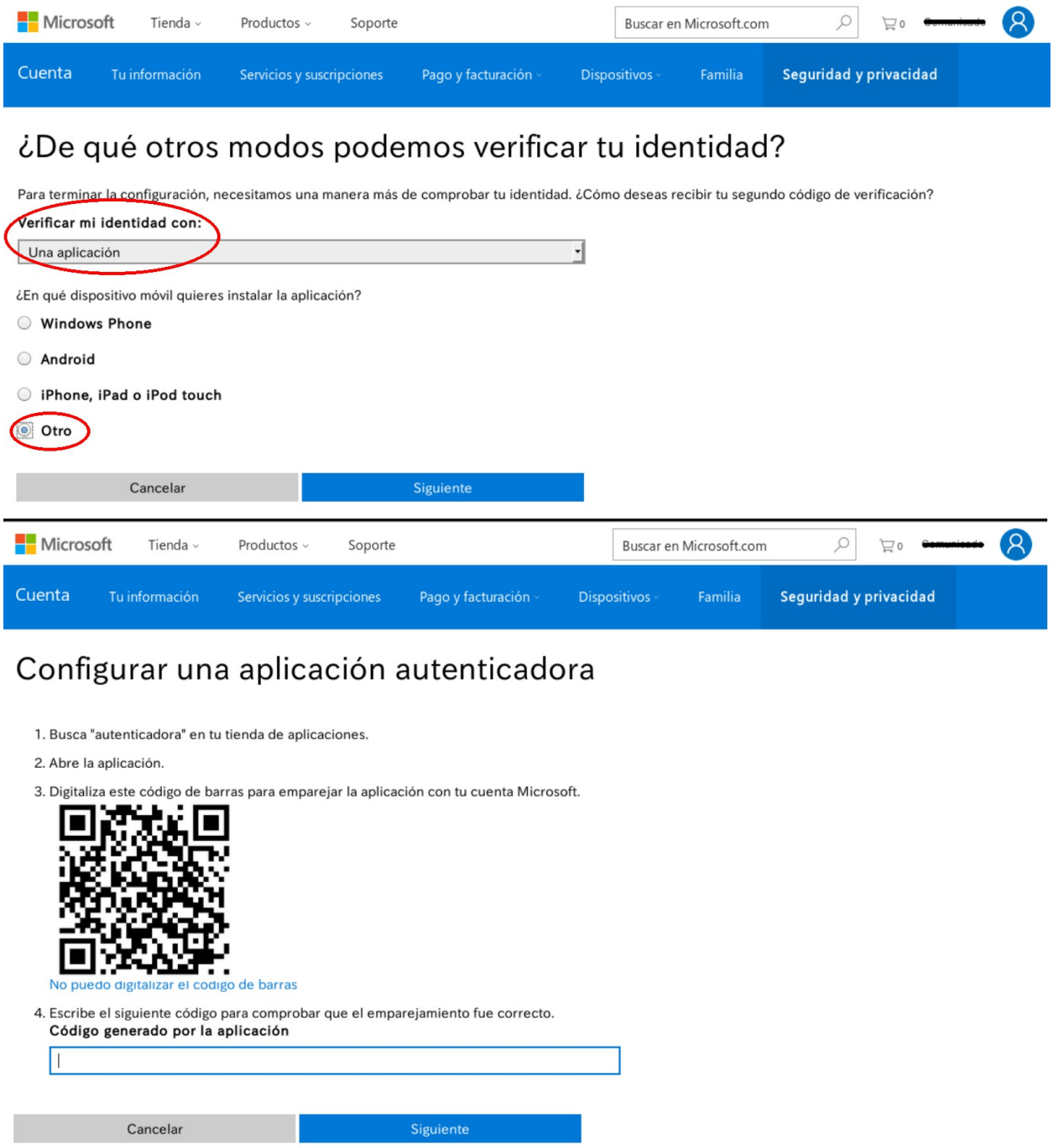

Figura 6. Datos para la configuración de un 2FA mediante *Google Authenticator* en *Microsoft Live*.

Como se puede observar, se nos muestra por pantalla un código QR. Lo que debemos hacer es abrir la aplicación de nuestro *smartphone*, seleccionar la opción de añadir una nueva cuenta y escanear el código QR proporcionado. Si todo ha ido correctamente deberemos tener la cuenta configurada en la *app* y se estarán generando códigos de tipo OTP en nuestro dispositivo cada 30 segundos.

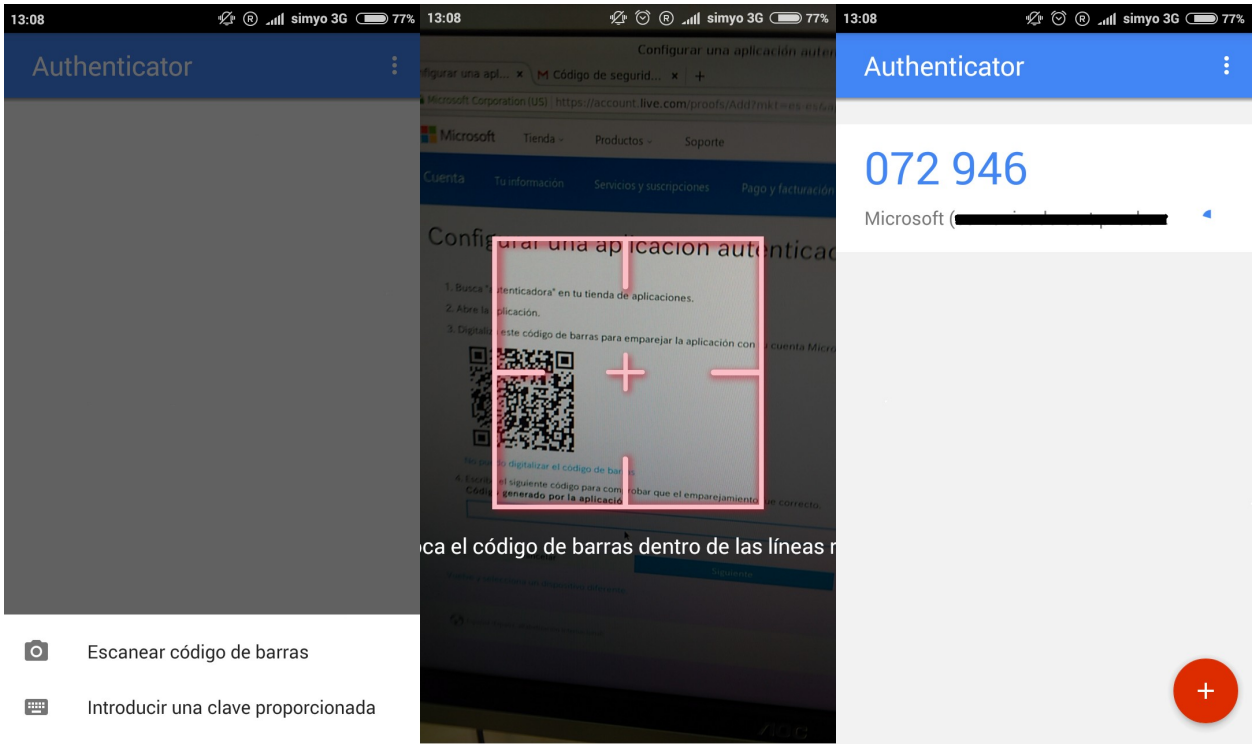

Figura 7. Proceso de lectura de un código QR para configurar una cuenta en *Google Authenticator*.

Si no se dispone de una cámara con la que realizar la lectura del código QR, existe la opción de introducir de forma manual una cadena de texto al pulsar sobre "No puedo digitalizar el código de barras". Dicho cadena es la clave secreta precompartida que se usará en la generación de los códigos TOTP.

Para comprobar que la configuración se ha realizado de forma correcta debemos introducir un código de verificación en el recuadro correspondiente y, si no se detecta ningún problema, ya podremos guardar los cambios realizados. En el momento de hacerlo se nos mostrará un código de recuperación para poder acceder a la cuenta en el supuesto de pérdida o mal funcionamiento del dispositivo móvil encargado de obtener/generar los códigos OTP. De igual forma, también podremos configurar alguna contraseña de aplicación si fuese necesario.

A partir de este instante, nuestra cuenta de *Microsoft Live* quedará configurada para el uso de un segundo factor de autenticación mediante la aplicación *Google Authenticator*, por lo que la próxima vez que

se inicie sesión, tras proporcionar el clásico usuario/contraseña, se nos solicitará un código que deberemos leer desde la *app* instalada en nuestro terminal móvil.

5.2 Redes sociales

Actualmente, el uso de redes sociales está ampliamente extendido, por lo que no queremos dejar pasar la oportunidad de explicar cómo configurar un 2FA en dos de las redes sociales más usadas: *Facebook* y *Twitter*.

5.2.1 Twitter

Para configurar un segundo factor de autenticación en la red social Twitter, primero debemos acceder a la web https://twitter.com/?lang=es e iniciar sesión. A continuación debemos acceder al menú "Perfil y configuración" de la parte superior y, dentro de las opciones disponibles, seleccionar "Configuración".

Figura 8. Acceso a las opciones de configuración de una cuenta *Twitter*.

El siguiente paso será asociar un número de teléfono móvil con nuestra cuenta de Twitter, si es que no se ha hecho ya. Para ello debemos acceder a la opción "Móvil" del menú lateral y seguir las instrucciones.

A continuación debemos acceder a la sección "Seguridad y privacidad" del menú lateral y marcar la casilla "Verificación de inicio de sesión", tras lo cual se abrirá una ventana emergente que nos indicará los pasos necesarios para configurar el envío de códigos de verificación a nuestro teléfono móvil mediante mensajes SMS.

Básicamente, se nos enviará un mensaje de texto con un código de verificación que debemos introducir en la web y, si todo funciona correctamente y el sistema lo valida, la configuración de un 2FA quedará establecida.

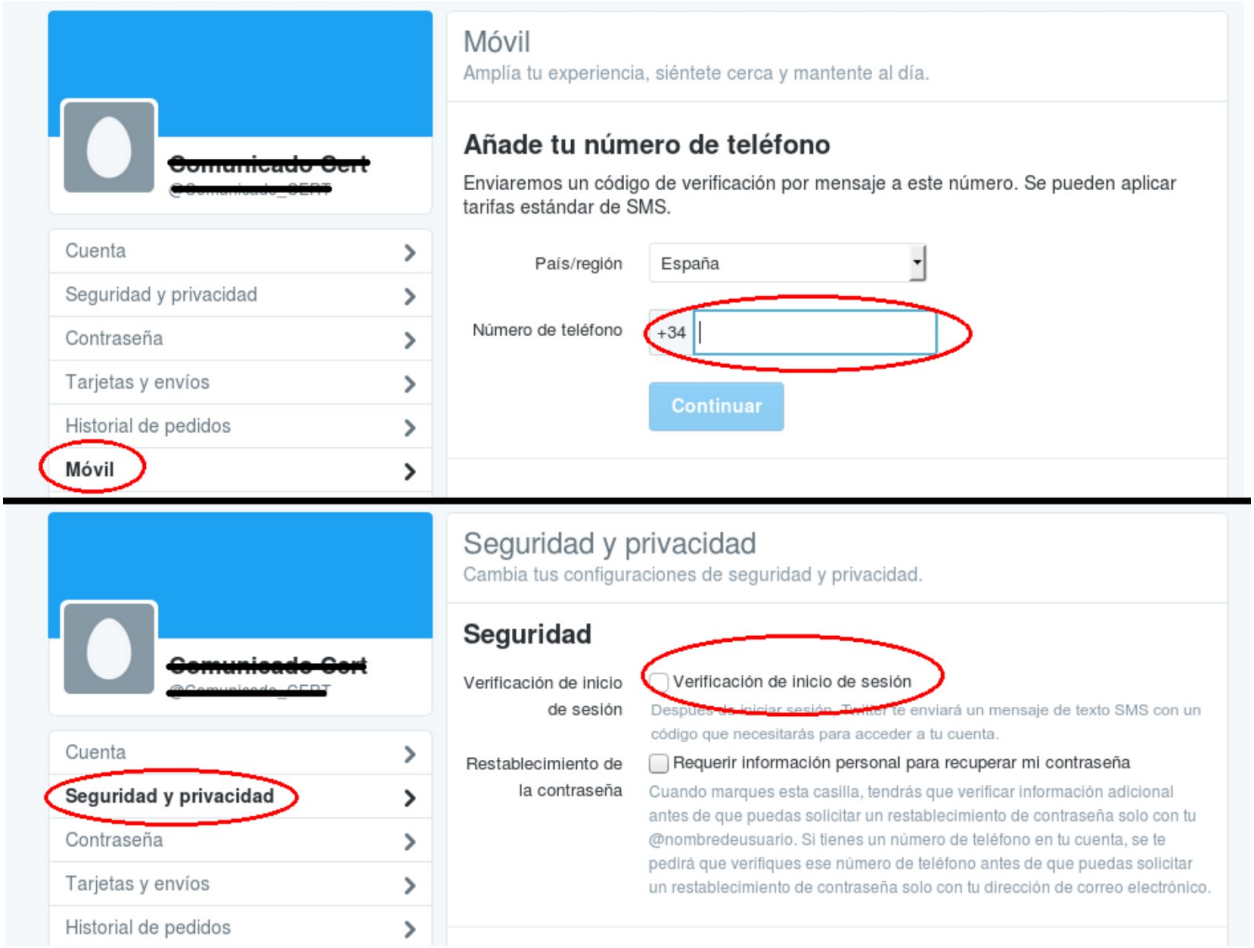

Figura 9. Opciones para vincular un número de teléfono y habilitar un 2FA en *Twitter*.

Figura 10. Validación del código de verificación recibido por SMS en *Twitter*.

Tras estos pasos, y como viene siendo habitual, se nos ofrecerá posibilidad de obtener un código de recuperación de nuestra cuenta para que lo usemos si perdemos el terminal móvil o deja de funcionar correctamente. Y de igual forma, se nos ofrece la posibilidad de generar una contraseña de aplicación para poder configurar el servicio en un *smartphone* o *tablet* sin la necesidad del 2FA.

Figura 11. Opciones para la generación de un código de recuperación y una contraseña de aplicación en *Twitter*.

5.2.2 Facebook

Para poder configurar un segundo factor de autenticación en nuestra cuenta de *Facebook*, el primer paso consiste en acceder a la siguiente URL https://www.facebook.com/ e iniciar sesión. Posteriormente debemos acceder al menú de la parte superior y seleccionar "Configuración".

Figura 12. Menú configuración de una cuenta de *Facebook*.

Ahora debemos acceder a la opción "Seguridad" del menú lateral y, dentro de las opciones disponibles, seleccionar "Aprobaciones de inicio de sesión", donde deberemos marcar la casilla "Requerir un código de inicio de sesión para acceder a mi cuenta desde navegadores desconocidos".

Figura 13. Opción para que *Facebook* nos solicite un código de verificación al iniciar sesión.

Al hacerlo, deberemos indicar un número de teléfono móvil al que nos hagan llegar los códigos de verificación mediante el envío de SMS.

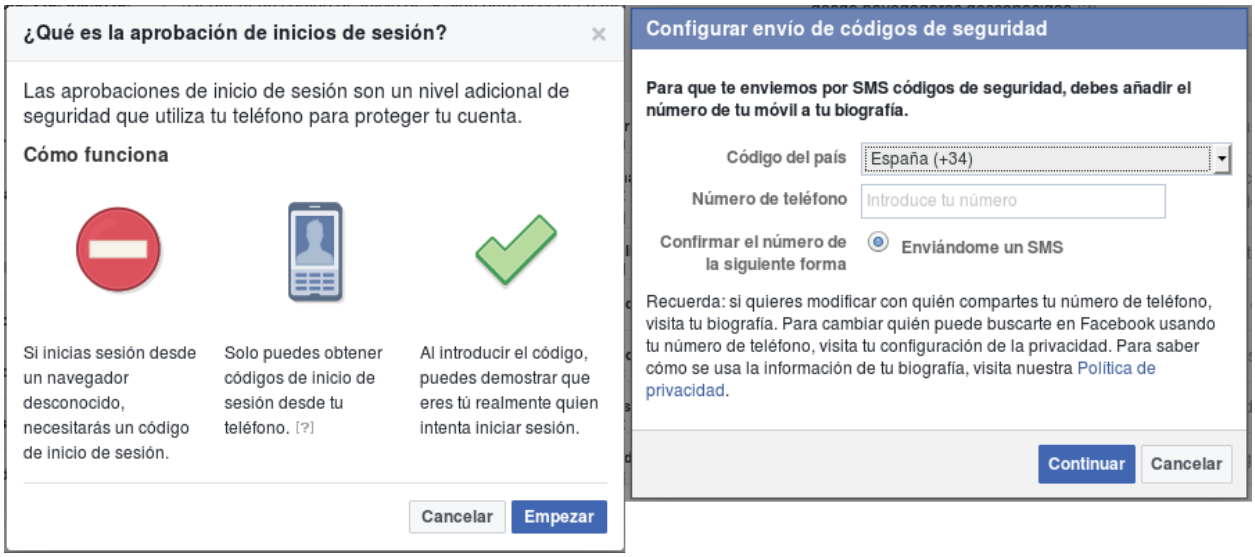

Figura 14. Proceso de verificación del teléfono móvil en *Facebook*.

Igual que en ocasiones anteriores, una vez validado el código de verificación que llegue a nuestro *smartphone* mediante SMS, el 2FA quedará configurado.

Hay que destacar que una vez realizado este proceso, desde *Facebook* nos permiten seleccionar el uso de una *app* generadora de códigos TOTP para obtener los códigos de verificación. Tan sólo hay que acceder a la opción "Generador de códigos" y seguir las instrucciones.

Figura 15. Opción para configurar una aplicación generadora de códigos de verificación en *Facebook*.

Como no podía ser de otra manera, para configurar dicha *app* nos ofrecen la posibilidad de escanear un código QR o introducir una clave de forma manual en la aplicación *Google Authenticator*.

Figura 16. Configuración de una aplicación generadora de códigos de verificación en *Facebook*.

5.3 Servicios de almacenamiento en la nube

Los servicios de almacenamiento en la nube (del inglés *cloud storage*), suponen un modelo de almacenamiento de datos en el que éstos se alojan en espacios de almacenamiento lógicos ubicados en Internet y, por lo general, aportados por un tercero.

Aunque en el presente informe ya hemos indicado cómo configurar un 2FA en nuestras cuentas de *Google* y *Microsoft Live*, y por lo tanto ya habremos configurado un segundo factor de autenticación en servicios de almacenamiento en la nube como *Google Drive* y *OneDrive*, no queremos dejar pasar la oportunidad de explicar cómo configurarlo también en *Dropbox*.

5.3.1 Dropbox

Para configurar un 2FA en *Dropbox* el primer paso consiste en acceder a la URL https://www.dropbox.com/es_ES/ e iniciar sesión con nuestra cuenta. A continuación debemos acceder a la sección "Configuración" del menú desplegable superior y, en la página que se nos presenta, seleccionar la pestaña "Seguridad", donde se nos proporciona una opción para habilitar la verificación en dos pasos:

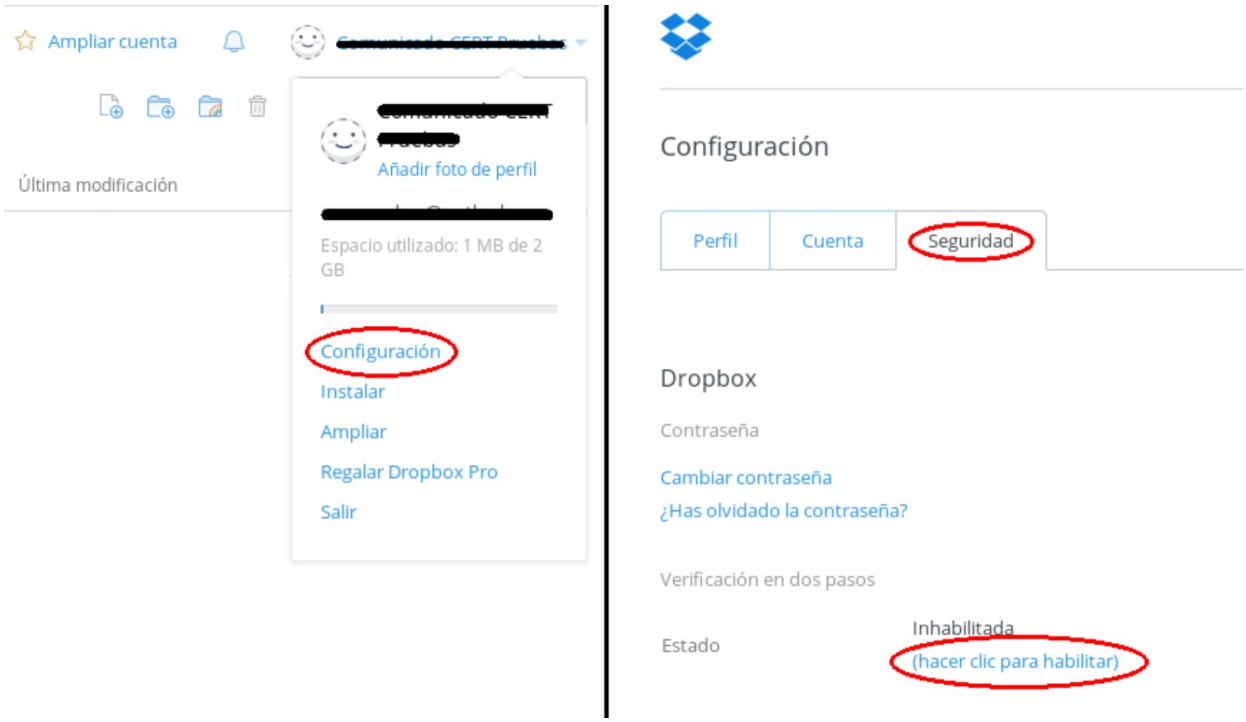

Figura 17. Opciones de configuración de un 2FA en *Dropbox*.

Al seguir los pasos anteriormente detallados, se abrirá una ventana emergente que nos permitirá escoger el método que deseemos para usar un segundo factor de autenticación: mediante el envío de SMS (para lo

cual deberemos aportar nuestro número de teléfono móvil) o mediante el uso de una aplicación generadora de código TOTP (como por ejemplo *Google Authenticator*).

Figura 18. Proceso de configuración de un 2FA en *Dropbox* mediante el uso de *Google Authenticator*.

Al finalizar, se nos mostrarán una serie de códigos de recuperación que son los que debemos usar en caso de extravío o mal funcionamiento del dispositivo encargado de recibir/generar los códigos de verificación. Y como viene siendo habitual, también podremos revisar a qué aplicaciones/dispositivos de confianza les hemos facilitado el acceso sin necesidad de usar el 2FA (mediante una contraseña de aplicación).

5.4 SSH

Hasta ahora hemos detallado cómo configurar el uso de un 2FA en algunas aplicaciones y servicios web ampliamente usados. Como punto final de este comunicado nos gustaría poner un ejemplo sobre cómo configurar el uso de un 2FA en un servicio no relacionado con la web. Dicho ejemplo sería SSH.

SSH (*Secure Shell*, en español: intérprete de órdenes seguro) es un protocolo de comunicaciones que permite acceder a máquinas remotas a través de una red. Para ello, el usuario puede manejar por completo la computadora mediante el intérprete de comandos.

Una correcta configuración del servicio SSH supone la modificación de su fichero de configuración bastionando ciertos aspectos esenciales. Para ello se podrían seguir las recomendaciones reflejadas en la Guía de Seguridad de las TIC "Configuración segura de SSH" del CCN-CERT [16]. De hecho, las indicaciones aquí expuestas simplemente suponen una de las secciones de dicho documento y se recomienda al lector que profundice en el mismo para comprender el funcionamiento de otros aspectos de seguridad relacionados con SSH.

En este ejemplo mostraremos cómo configurar un segundo factor de autenticación en SSH mediante el uso de la aplicación *Google Authenticator*. La empresa de *Mountain View* desarrolló un módulo PAM para implementar este mecanismo de autenticación utilizando el estándar abierto OATH, por lo que su implementación es relativamente sencilla.

El primer paso consiste en la instalación del módulo PAM anteriormente mencionado en nuestro servidor SSH. En las distribuciones Ubuntu es tan simple como instalar un paquete:

```
sudo apt-get install libpam-google-authenticator
```

Una vez finalizada la instalación de la paquetería necesaria, debemos ejecutar el siguiente comando:

```
google-authenticator
```

Al hacerlo, se nos realizarán una serie de preguntas respecto a la configuración de dicho método de autenticación y se nos mostrará por pantalla un código QR para que lo escaneemos con nuestro terminal móvil, así como una serie de códigos de recuperación (*emergency scratch codes*):

Figura 19. Proceso de configuración de un 2FA en el servicio SSH.

El siguiente paso consiste en la modificación de los ficheros de configuración del servidor SSH para activar el uso del 2FA. Para ello, debemos editar el fichero `/etc/pam.d/sshd` y añadir la siguiente línea:

```
auth required pam_google_authenticator.so
```

A continuación, editar el fichero `/etc/ssh/sshd_config`, localizar la opción `ChallengeResponseAuthentication` y establecerla a sí:

```
ChallengeResponseAuthentication yes
```

También es necesario reiniciar el servicio SSH y una vez hecho ya tendremos configurado correctamente el uso de un 2FA para nuestra cuenta en el servidor SSH.

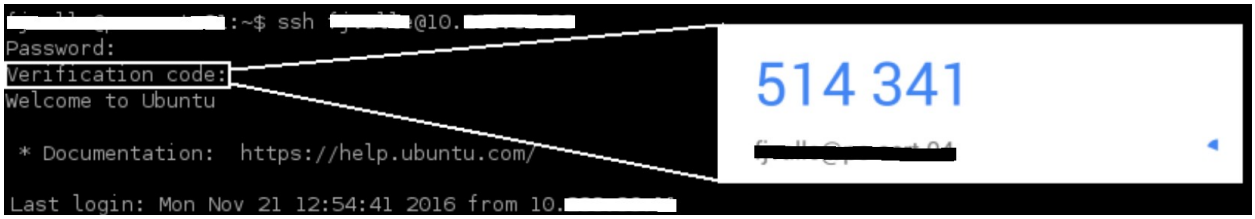

Figura 20. autenticación en un servidor SSH con 2FA habilitado.

Se debe tener en cuenta que esta configuración fuerza el uso de un 2FA para todas las cuentas del sistema, por lo que antes de activarla se debería estar seguro de que todos los usuarios han configurado el uso de *Google Authenticator* en sus dispositivos móviles o bien, establecer la opción `auth required pam_google_authenticator.so nullok` de forma temporal (para permitir códigos de verificación vacíos durante un tiempo hasta que todos los usuarios hayan configurado el 2FA) y/o aplicarlo sólo a un grupo de usuarios concreto (`auth [default=1 success=ignore] pam_succeed_if.so user ingroup <group>; auth required pam_google_authenticator.so`)[1].

6 RECOMENDACIONES DE SEGURIDAD SOBRE EL PROCESO DE AUTENTICACIÓN

Para concluir este pequeño informe divulgativo, desde AndalucíaCERT nos gustaría realizar algunos comentarios y recomendaciones de seguridad al lector:

- El proceso de autenticación es de vital importancia, por lo que es necesario disponer de diversos métodos para verificar la identidad de los usuarios. Si alguno de dichos métodos involucra el uso

1 Ambas opciones deberían especificarse en el fichero de configuración /etc/pam.d/sshd

de un esquema usuario/contraseña, es recomendable usar siempre contraseñas robustas y tener una diferente para cada aplicación o servicio. En este sentido será de gran utilidad el uso de gestores de contraseñas como LastPass, 1Password o KeePass.

- Por supuesto, el usuario deberá ser consciente de ante qué aplicación o sistema se está autenticando. Uno de los métodos más habituales para el robo de credenciales consiste en presentar una aplicación falsa al usuario para que éste proporcione sus datos, por lo que se insta al lector a realizar pequeñas comprobaciones de seguridad, como verificar la URL o el Error: No se encuentra la fuente de referencia del sitio web contra el que se autentica.

- Si el sistema o aplicación lo permiten, configurar siempre el uso de un segundo factor de autenticación. Cuál de ellos usar dependerá de los métodos ofertados y las preferencias personales de cada usuario.

- Desde el punto de vista de los desarrolladores, nos gustaría recordar que la seguridad debe ser tenida en cuanta en todas las fases del desarrollo del proyecto, por lo que sería interesante plantearse ya desde el comienzo qué mecanismos de autenticación se ofertarán al usuario y contemplar el uso de un sistema de autenticación MFA.

7 GLOSARIO

2FA: Acrónimo de la expresión inglesa *Two-Factor Authentication*. Hace referencia al uso de un Segundo Factor de autenticación, esto es, utilizar de forma conjunta dos de los tres factores descritos en un sistema de autenticación multifactor.

app: Contracción de *application* (aplicación en inglés). Suele hacer referencia a las aplicaciones especialmente diseñadas para teléfonos móviles.

autenticación: Proceso por el que un cliente prueba su identidad frente a una entidad (normalmente una aplicación o sistema).

código QR: Se trata de una imagen que almacena información en una matriz de puntos o en un código de barras bidimensional.

hash: Función resumen o *digest*. Hace uso de funciones matemáticas para generar un resumen o huella de tamaño fijo, de un recurso de tamaño arbitrario. Su bondad reside en que un mismo recurso siempre generará la misma huella y una pequeña modificación del mismo resultará en una huella completamente distinta. Además, las funciones hash no son reversibles, esto es, partiendo de una huella digital, nunca será posible obtener el recurso del que se ha obtenido dicha huella.

identidad: Conjunto de atributos que describen de forma unívoca a una persona en un contexto determinado.

IETF: Acrónimo de *Internet Engineering Task Force*. Organización internacional abierta de normalización, que tiene como objetivos el contribuir a la ingeniería de Internet. Se encarga de regular las propuestas y los estándares de Internet.

market: Repositorio de aplicaciones para dispositivos móviles. Aunque existen diversos tipos, sólo se recomienda el uso de aquellos que sean oficiales, como Google Play y App Store.

MFA: Acrónimo de la expresión inglesa *Multi-Factor Authentication*. Un factor de autenticación múltiple consiste en una aproximación a la seguridad en el proceso de autenticación del usuario que requiere de la presentación de dos o más elementos de los siguientes tres elementos de autenticación: un factor de conocimiento (algo que sólo el usuario sabe), un factor de posesión (algo que sólo el usuario posee), y un factor inherente al usuario (algo que sólo el usuario es).

NIST: Acrónimo de la expresión *National Institute of Standards and Technology*. Es una agencia del Gobierno de USA cuya misión es promover la innovación y la competencia industrial en Estados Unidos mediante avances en metrología, normas y tecnología.

OATH: Acrónimo de *Initiative for Open Authentication*. Se trata de un consorcio que tiene por objetivo el desarrollo de una arquitectura de referencia usando estándares abiertos para promover la adopción de la autenticación fuerte.

OTP: Acrónimo de la expresión inglesa *One-Time Password*. Contraseña de un sólo uso, esto es, un secreto que sólo será válido en un instante de tiempo determinado, impidiendo que pueda ser reutilizado.

PAM: Acrónimo de la expresión inglesa *Pluggable Authentication Modules*. Se trata de un mecanismo de autenticación muy flexible de los sistemas GNU/Linux que permite abstraer las aplicaciones y otro software del proceso de identificación.

RFC: Acrónimo de la expresión *Request For Comments*. Consiste en una serie de publicaciones del grupo de trabajo de Internet (IETF) que describen diversos aspectos del funcionamiento de Internet y otras redes de computadoras, como protocolos, procedimientos, etc. y comentarios e ideas sobre estos.

smartphone: Teléfono móvil inteligente o de última generación.

SMS: Acrónimo de la expresión inglesa *Short Message Service*. Sistema de mensajes de texto para teléfonos móviles.

SSH: Acrónimo de la expresión inglesa *Secure Shell*. Se trata de un procolo de comunicaciones que permite acceder a máquinas remotas a través de una red y controlarlas gracias a un intérprete de comandos..

TOTP: Acrónimo de la expresión *Time-based One-Time Password*. Contraseña de un sólo uso que usa una clave secreta precompartida y el instante de tiempo actual para generar los códigos de verificación.

USB: Acrónimo de la expresión inglesa *Universal Serial Bus*. Se trata de un estándar desarrollado en los años '90 y que define un protocolo de comunicaciones ampliamente extendido.

8 DOCUMENTACION DE REFERENCIA

[1] Editores de Wikipedia. <<*Autenticación*>>. Wikipedia, la enciclopedia libre. Disponible en línea: https://es.wikipedia.org/wiki/Autenticaci%C3%B3n (Fecha de consulta, 16/11/2016).

[2] Editores de Wikipedia. <<*Multi-factor authentication*>>. Wikipedia, la enciclopedia libre. Disponible en línea: https://en.wikipedia.org/wiki/Multi-factor_authentication (Fecha de consulta, 16/11/2016).

[3] Juan Manuel Vozmediano Torres. <<*Introducción a la seguridad e identificación digital. Módulo 1 del Máster en Seguridad de la Información y las Comunicaciones*>>. Universidad de Sevilla, 2014.

[4] Paul A. Grassi, James L. Fenton, Elaine M. Newton y otros. <<*DRAFT NIST Special Publication 800-63B- Digital Authentication Guideline*>>. National Institute of Standars and Technology (NIST). Disponible en línea: https://pages.nist.gov/800-63-3/sp800-63b.html (Fecha de consulta 16/11/2016).

[5] Editores de Wikipedia. <<*Token de seguridad*>>. Wikipedia, la enciclopedia libre. Disponible en línea: https://es.wikipedia.org/wiki/Token_de_seguridad (Fecha de consulta, 16/11/2016).

[6] Editores de Wikipedia. <<*Google Authenticator*>>. Wikipedia, la enciclopedia libre. Disponible en línea: https://en.wikipedia.org/wiki/Google_Authenticator (Fecha de consulta, 16/11/2016).

[7] Trabajadores de Google. <<*Instalar Google Authenticator*>>. Ayuda de Cuentas de Google, 2016. Disponible en línea: https://support.google.com/accounts/answer/1066447?rd=1 (Fecha de consulta, 16/11/2016).

[8] D. M'Raihi, Verisign Inc., S. Machani, Diversinet Corp., M. Pei, Symantec, J Rydell y Portwise Inc. <<*RFC 6238. TOTP: Time-Based One-Time Password Algorithm*>> Internet Engineering Task Force (IETF). Disponible en línea: https://tools.ietf.org/html/rfc6238 (Fecha de consulta: 16/11/2016).

[9] Trabajadores de Google. <<*Iniciar sesión mediante contraseñas de aplicación*>>. Ayuda de Cuentas de Google, 2016. Disponible en línea: https://support.google.com/accounts/answer/185833?hl=es (Fecha de consulta , 17/11/2016).

[10] Personal de Microsoft. <<*About two-step verification*>>. Microsoft Help Center, 2016. Disponible en línea: https://support.microsoft.com/en-us/help/12408/microsoft-account-about-two-step-verification (Fecha de consulta, 17/11//2016).

[11] Editores de Turn It On. <<*TURN IT ON. The Ultimate guide to two-factor authentication (2FA)*>>. TeleSign, 2016. Disponible en línea: https://www.turnon2fa.com/ (Fecha de consulta, 18/11/2016).

[12] jimio (@jimio) <<*Getting started with login verification*>>. Blog Oficial de Twitter, 2013. Disponible en línea: https://blog.twitter.com/2013/getting-started-with-login-verification (Fecha de consulta, 18/11/2016).

[13] Personal de Authy. <<*Setup Facebook Two Factor Authentication*>>. Twilio, 2015. Disponible en línea: https://www.authy.com/tutorials/add-2-factor-authentication-facebook/ (Fecha de consulta, 18/11/2016).

[14] Junal Chaudhari, Judie Green & otros. <<*How to enable 2-step verification? No login approval section under my security?*>>. Facebook Help Community. Disponible en línea: https://www.facebook.com/help/community/question/?id=10151548571887325 (Fecha de consulta, 18/11/2016).

[15] Editores de Wikipedia. <<*Secure Shell*>>. Wikipedia, la enciclopedia libre. Disponible en línea: https://es.wikipedia.org/wiki/Secure_Shell (Fecha de consulta, 21/11/2016).

[16] Personal del CCN-CERT. <<*CCN-STIC-665. Configuración Segura de SSH*>> CCN-CERT, 2014.

[17] Cris Hoffman. <<*How to Secure SSH with Google Authenticator's Two-Factor Authentication*>>. How-to Geek, 2012. Disponible en línea: http://www.howtogeek.com/121650/how-to-secure-ssh-with-google-authenticators-two-factor-authentication/ (Fecha de consulta, 21/11/2016).

[18] Colaboradores del proyecto GNU/Linux. <<*pam.d(5) - Linux man page*>>. Disponible en línea: https://linux.die.net/man/5/pam.d (Fecha de consulta, 21/11/2016).

[19] Imobach González Sosa & Manolo Padrón Martínez. <<*Pluggable Authentication Modules (PAM)*>>. Universidad de Las Palmas de Gran Canaria, 2004. Disponible en línea: http://sopa.dis.ulpgc.es/ii-aso/portal_aso/leclinux/seguridad/pam/pam_doc.pdf (Fecha de consulta, 21/11/2016).

[20] Personal y colaboradores del proyecto Ubuntu. <<*pam_google_authenticator - PAM module for two-step verification*>>. Ubuntu Manpage Repository. Ubuntu manuals, 2016. Disponible en línea: http://manpages.ubuntu.com/manpages/precise/man8/pam_google_authenticator.8.html (Fecha de consulta, 21/11/2016).

[21] Remi Bergsma. <<*Playing with two-factor authentication in Linux using Google Authenticator*>>. Blog de Remi Bergsma, 2013. Disponible en línea: https://blog.remibergsma.com/tag/google-authenticator/ (Fecha de consulta, 21/11/2016).