BASTIONADO DE REDES Y SISTEMAS

Tarea 3

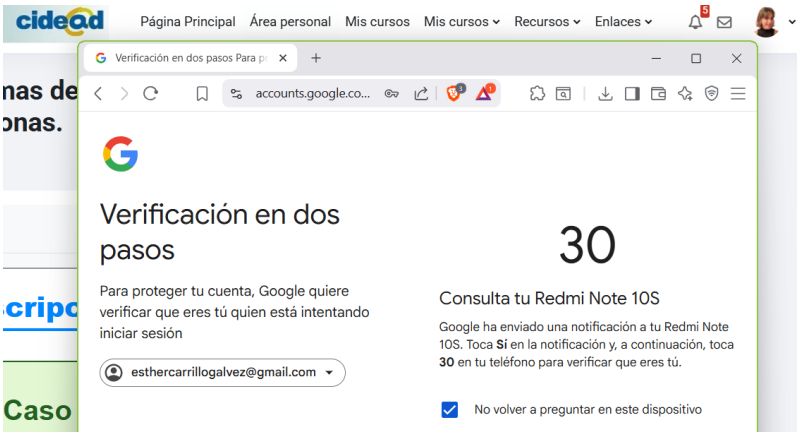
ESTHER CARRILLO GÁLVEZ

Índice

1. Apartado 1: Identificación de tres servicios reales

1.1. Gmail

Para activar la verificación en dos pasos para el correo electrónico, gmail ofrece distintas opciones como el autenticador de Google, las llaves de acceso y llaves de seguridad o la notificación de Google. A continuación, se muestra una captura durante el proceso de activación mediante el autenticador Google.



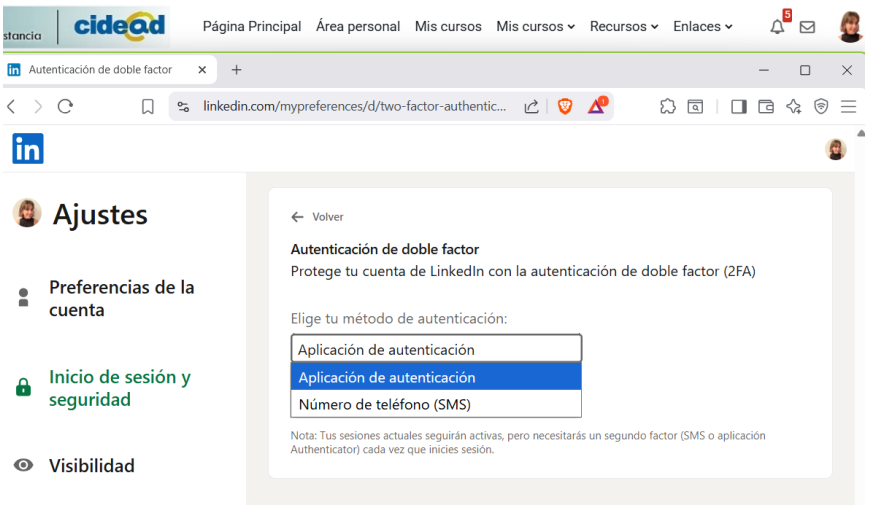
Para la recuperación de la cuenta en caso de olvidar la contraseña, se harán preguntas para confirmar que la cuenta es realmente de esa persona. Si en lugar de la contraseña, lo que se ha olvidado es la dirección de correo, se deben conocer los siguientes datos:

- El número de teléfono o la dirección de correo de recuperación de la cuenta.
- El nombre completo que se haya introducido en la cuenta.

Algunas de las ventajas que aporta frente a mecanismos convencionales es la gran variedad y flexibilidad que ofrece al usuario a la hora de elegir el nivel de seguridad. En el caso del autenticador de Google, los códigos se generan, incluso, sin necesidad de cobertura ni wifi. Sin embargo, el usuario podría perder el acceso permanente al dispositivo móvil si no guarda los códigos de *backup*.

1.2. Linkedin

Para activar la autenticación de doble factor, linkedin ofrece dos opciones: mediante la aplicación de autenticación y mediante número de teléfono (SMS).

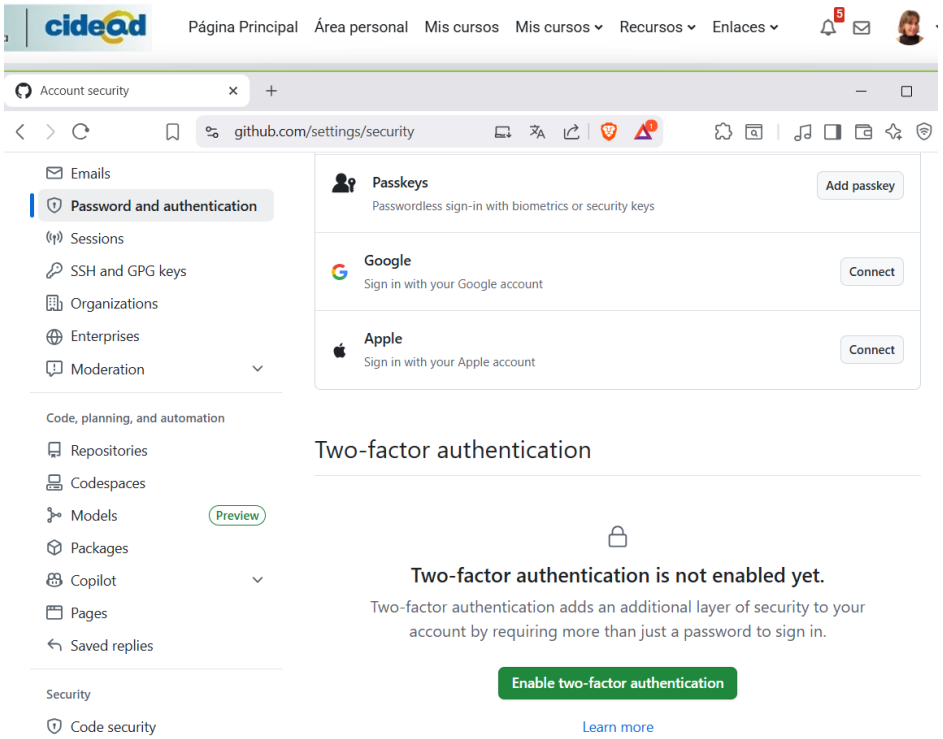


Para recuperar el acceso a la cuenta, se puede recuperar cargando una foto del DNI. En caso de que no se desee proporcionar un ID, se puede imprimir la Declaración jurada de identidad y firmarla ante notario. Una vez firmada, escanearla y adjuntarla en la incidencia. Asimismo también se puede hacer con una dirección de email asociada a esta empresa.

Las ventajas que proporciona el uso de SMS es la facilidad para configurarlo, ya que cualquier persona sin conocimientos técnicos podría activarlo sin problema. No obstante, la dependencia del SMS lo hace vulnerable al SIM Swapping.

1.3. Github

Los factores de autenticación que implementa Github son principalmente a través de una aplicación de autenticación (TOTP) como el autenticador de Google o mediante mensajes SMS. Otras opciones también incluyen las claves de seguridad física y la aplicación móvil de github.



Para recuperar la cuenta de Github, primero se debe restablecer la contraseña enviando un correo de restablecimiento a la dirección asociada a la cuenta. En caso de tener activada la autenticación en dos factores, se debe utilizar los códigos de recuperación. Del mismo modo, si se han perdido tanto el dispositivo 2FA como los códigos de recuperación, se deberá solicitar una recuperación de cuenta mediante la solicitud en el soporte de github.

Una de las ventajas frente a los mecanismos convencionales es la resistencia al phishing, ya que al ser obligatorio el 2FA y el uso para llaves físicas, se mitigan los ataques de phishing dirigidos al factor de contraseña. Por otro lado, existe la posibilidad al ataque *prompt bombing* porque el TOTP necesita una aplicación adicional, convirtiéndolo en un factor susceptible.

2. Análisis de un incidente documentado de seguridad

El caso real de incidente se basa en la noticia sobre la vulnerabilidad *AuthQuake* en Microsoft Azure. Según *Oasis Security*, el mecanismo que falló fue la validación del segundo factor de autenticación y la falta de un límite de frecuencia para la cantidad de veces que alguien podía intentar acceder a una cuenta.

La vulnerabilidad explotada fue que el sistema de verificación del código no tenía un límite estricto, con lo cual, esta vulnerabilidad permitió al atacante ejecutar un ataque de fuerza bruta. Por otro lado, la segunda vulnerabilidad explotada fue que

el código TOTP tenía una duración de 3 minutos, cuando lo recomendable es de 30 segundos, lo que permitió enviar 6 veces más intentos por cada código TOTP.

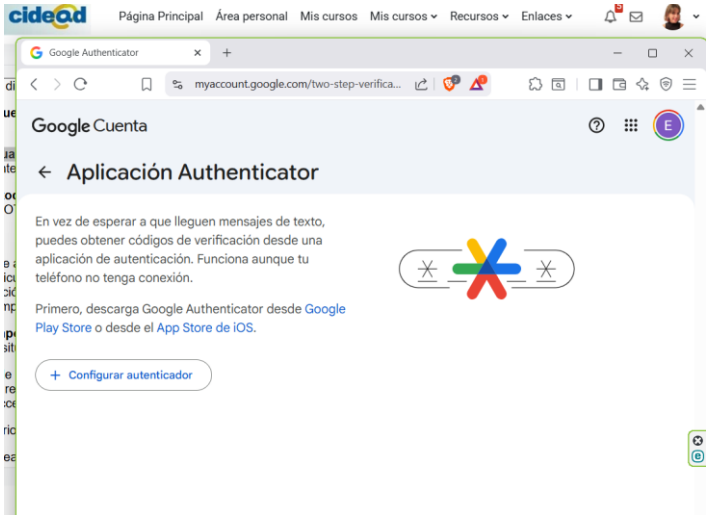
Puesto que la noticia es del pasado diciembre de 2024, considero que la vulnerabilidad podría volver a repetirse. Esta falla se ha encontrado en numerosos servicios, ya que cualquier aplicación que implemente un mecanismo MFA es susceptible si se ha ignorado la necesidad de aplicar límites en la validación de códigos.

Para evitar la repetición de este incidente habría establecido un límite de 3 fallos en el intento de sesión de modo que si se introducen más fallos de los permitidos no se genera ningún código MFA y, automáticamente, el sistema se bloquea. Asimismo, una buena práctica para mitigar esta vulnerabilidad sería que le llegara al usuario una notificación al correo con cada intento fallido de MFA.

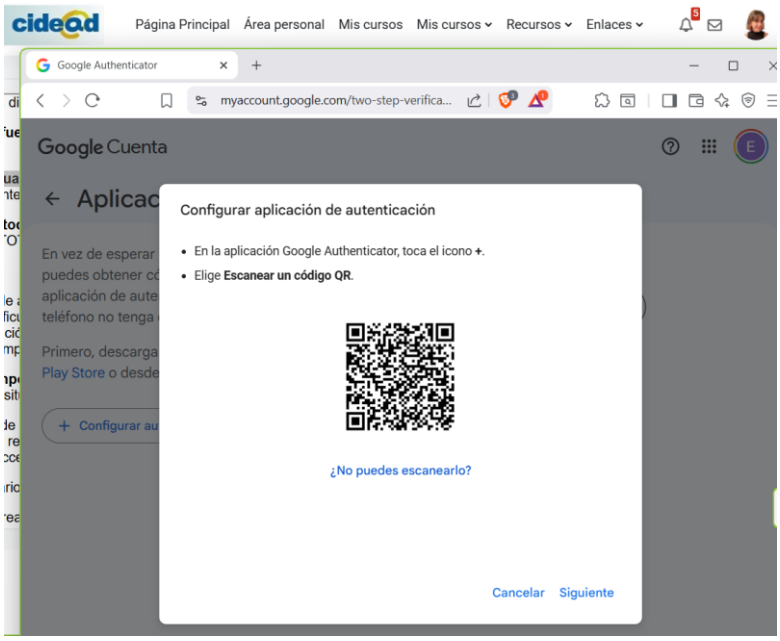
3. Apartado 2: Evaluación práctica

3.1. Activación verificación en dos pasos con Google Auhtenticator

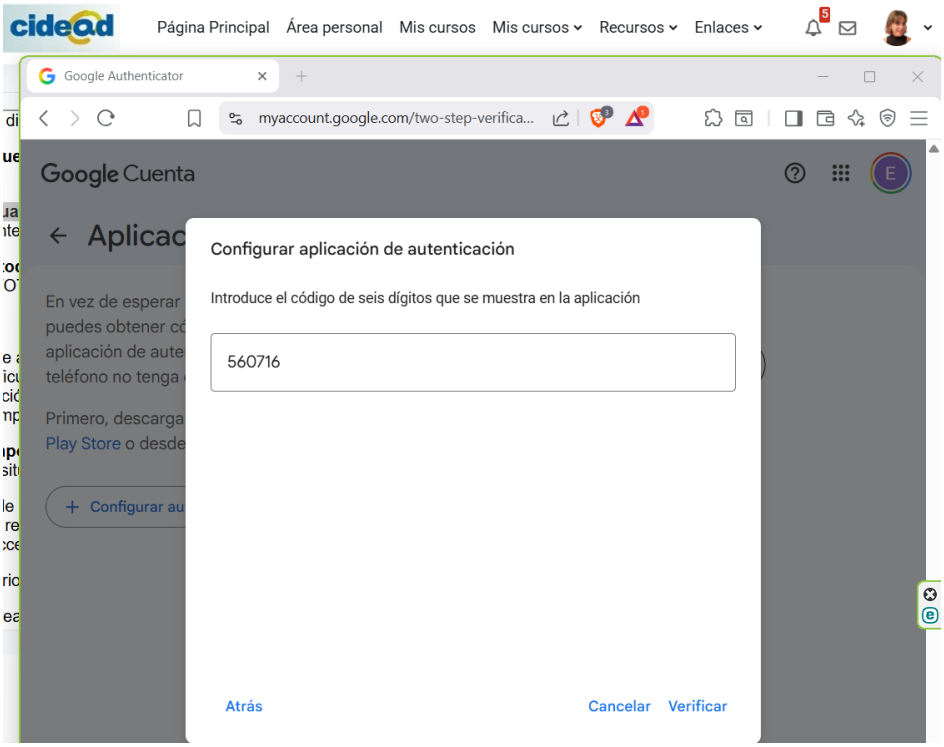
Para la activación de Google authenticator, se debe configurar el autenticador en la aplicación previamente instalada en el dispositivo móvil. A continuación, se debe configurar en el ordenador o en el dispositivo desde el que se vaya a acceder.



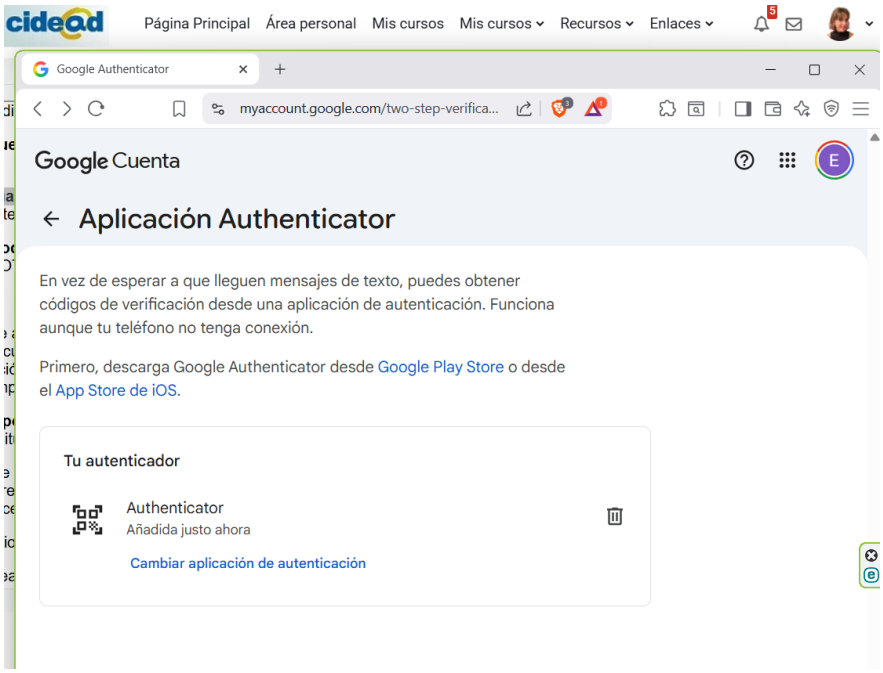
El siguiente paso es escanear con la aplicación móvil el código QR que se genera en la aplicación.



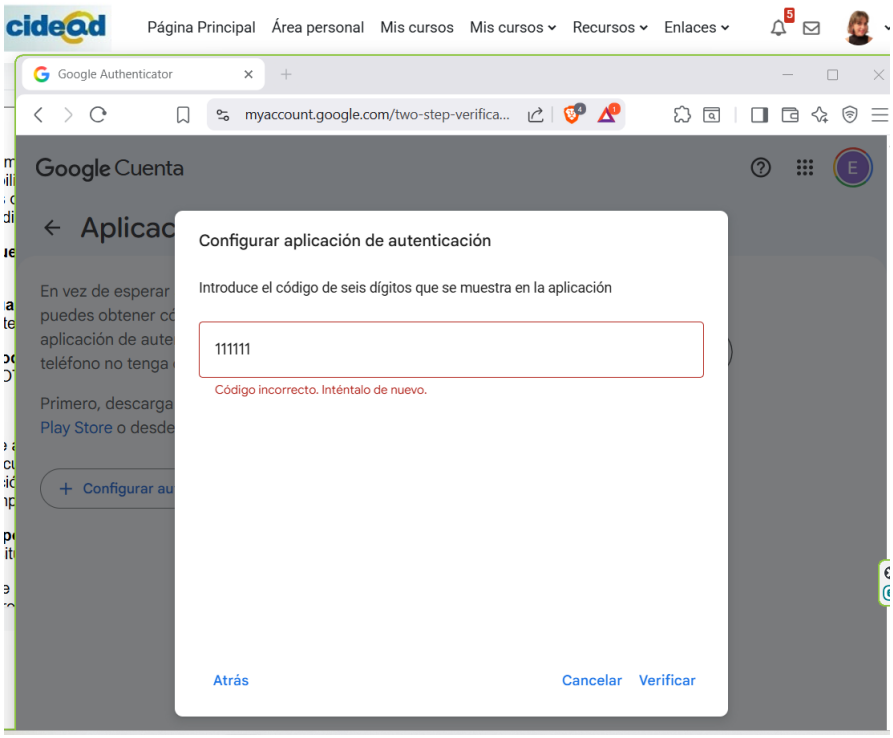
A continuación, se introduce el código que aparece en la aplicación y se verifica en el ordenador.



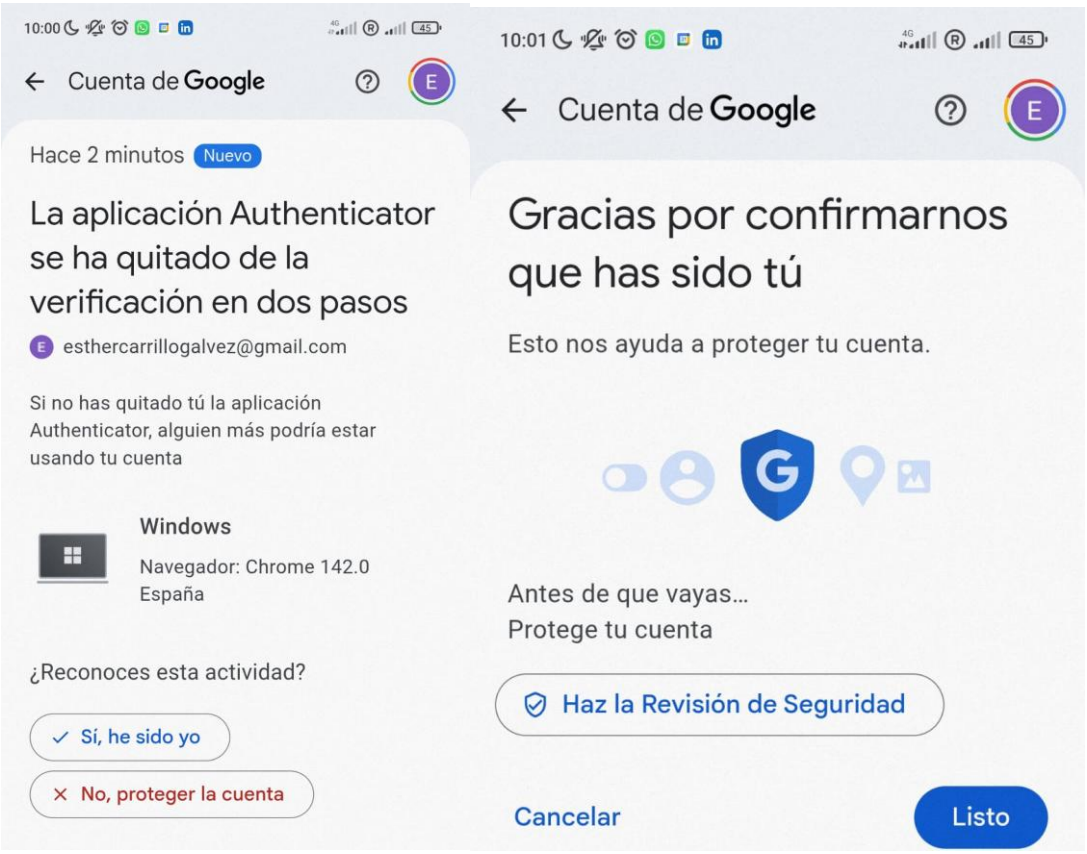
Finalmente, el autenticador se ha añadido correctamente en la cuenta de Google.



En caso de introducir un código erróneo, en este caso *111111*, la aplicación notifica con un mensaje de error “Código incorrecto. Inténtalo de nuevo”.

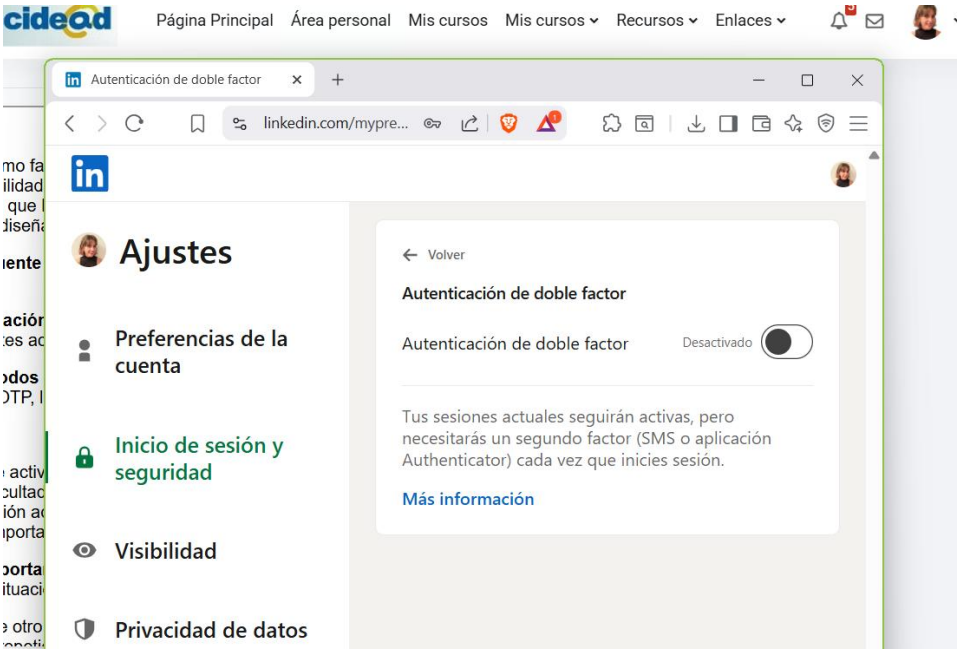


Como apunte relevante, en caso de quitar la verificación en dos pasos, el usuario recibirá una notificación al móvil indicando que se ha eliminado.

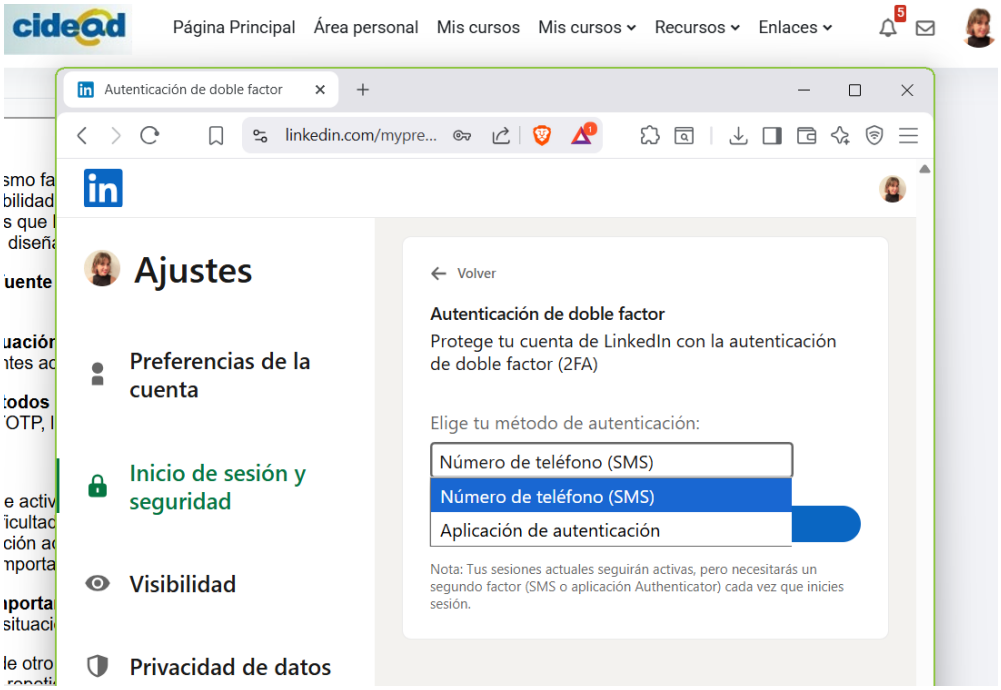


3.2. Activación doble factor en Linkedin

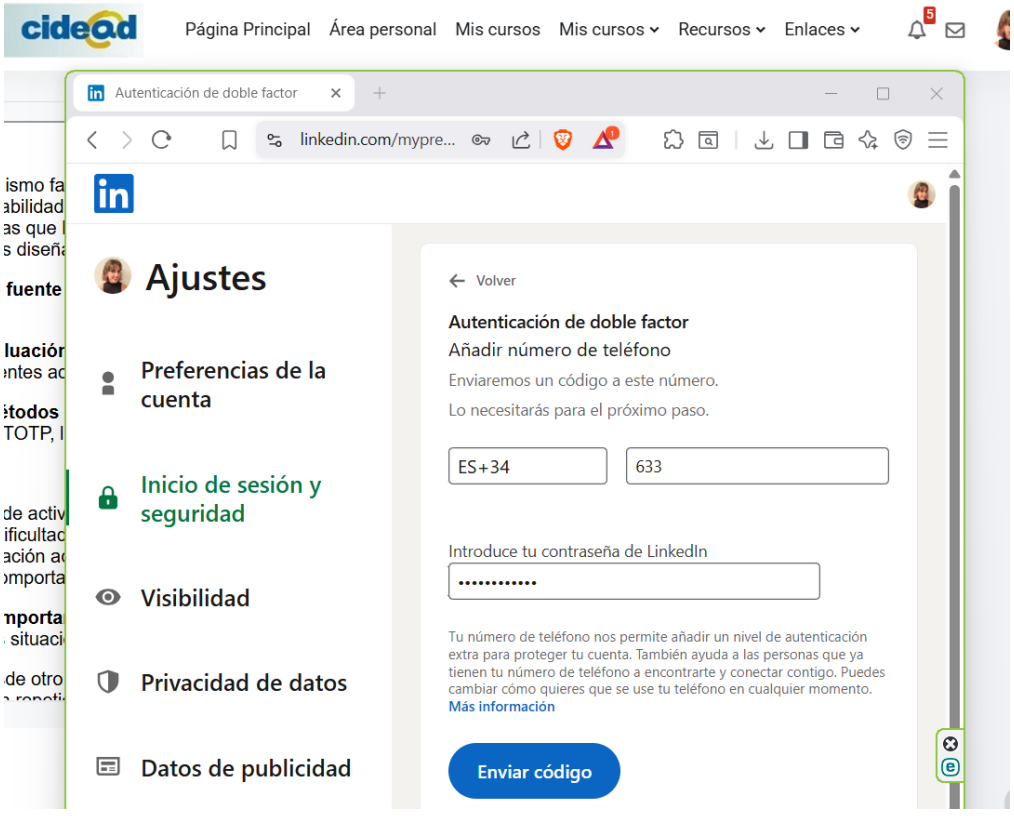
Para la autenticación de doble factor en linkedin, desde los ajustes, se debe acceder a “inicio de sesión y seguridad” y se debe deslizar la pestaña a *activado*.



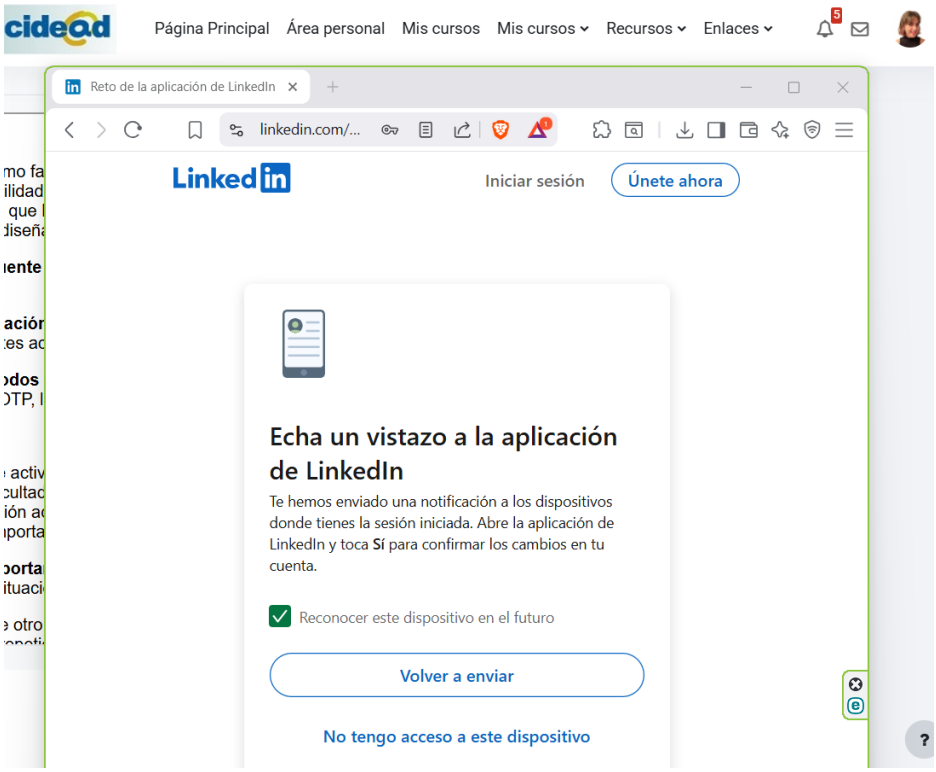
En el siguiente paso, se muestran las dos opciones disponibles. En este caso, se selecciona “número de teléfono (SMS)”.



Se rellenan los campos con los datos personales correspondientes y estaría listo para enviar el código al dispositivo móvil.



Se notifica que ha llegado un mensaje al dispositivo donde tenemos la sesión iniciada y se selecciona *sí* para confirmar los cambios en la cuenta.

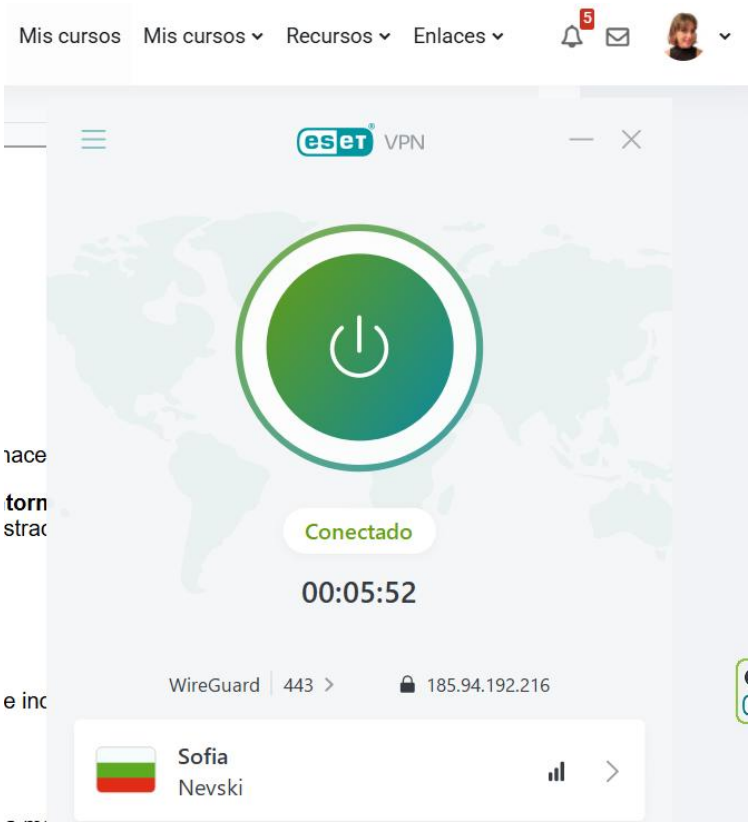


Se confirma la notificación que llega al dispositivo móvil, sin embargo la ubicación no es exacta.

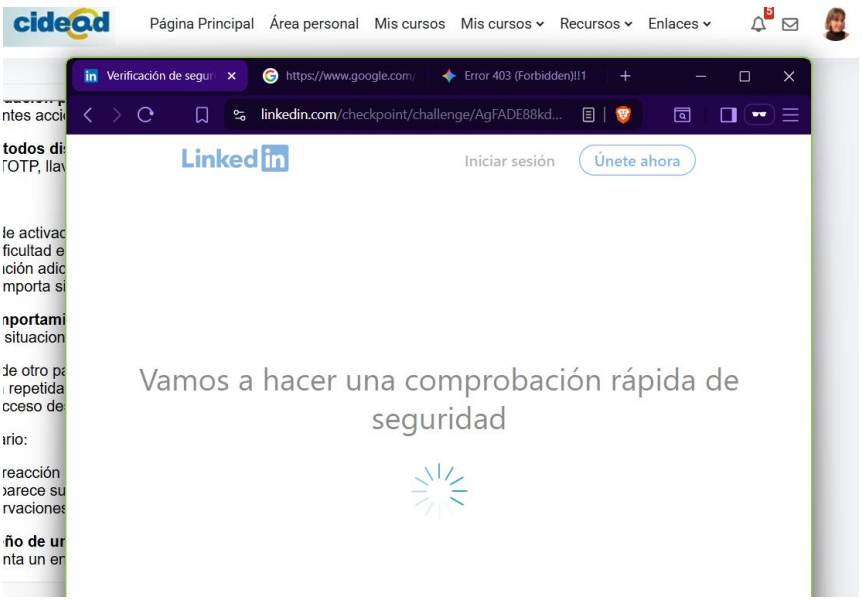
3.3. Prueba de comportamiento ante eventos poco comunes

Acceso desde otro país mediante VPN.

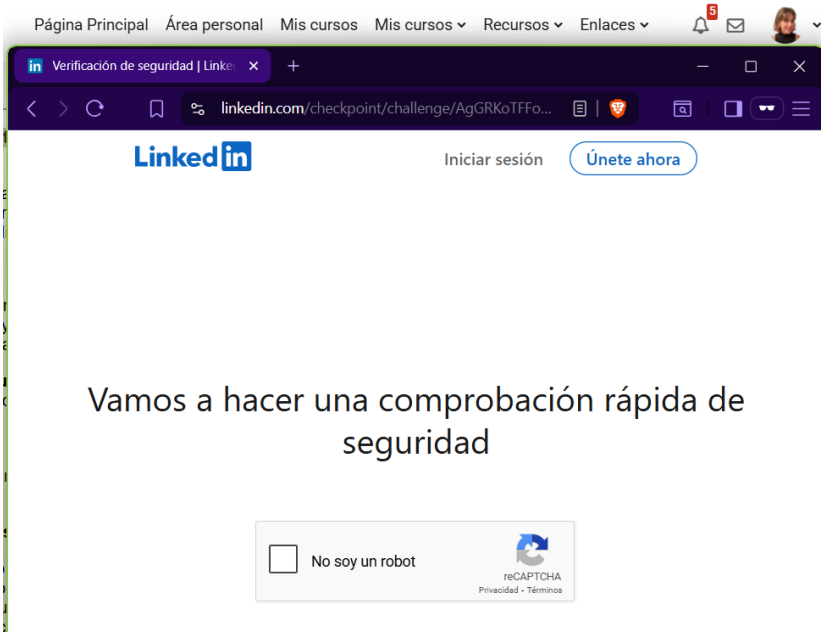
Se accede a linkedin desde una VPN establecida en Sofía, Bulgaria.

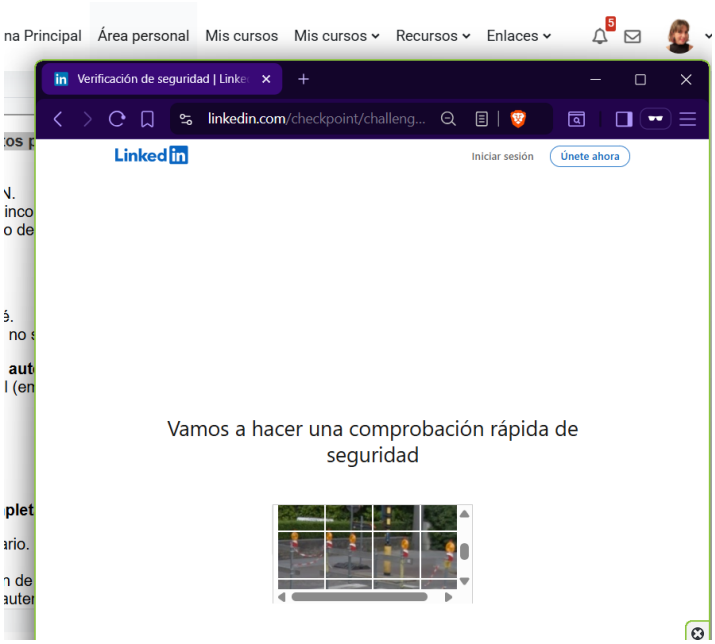


A continuación, se accede a la cuenta personal de linkedin y se notifica con una comprobación rápida de seguridad.

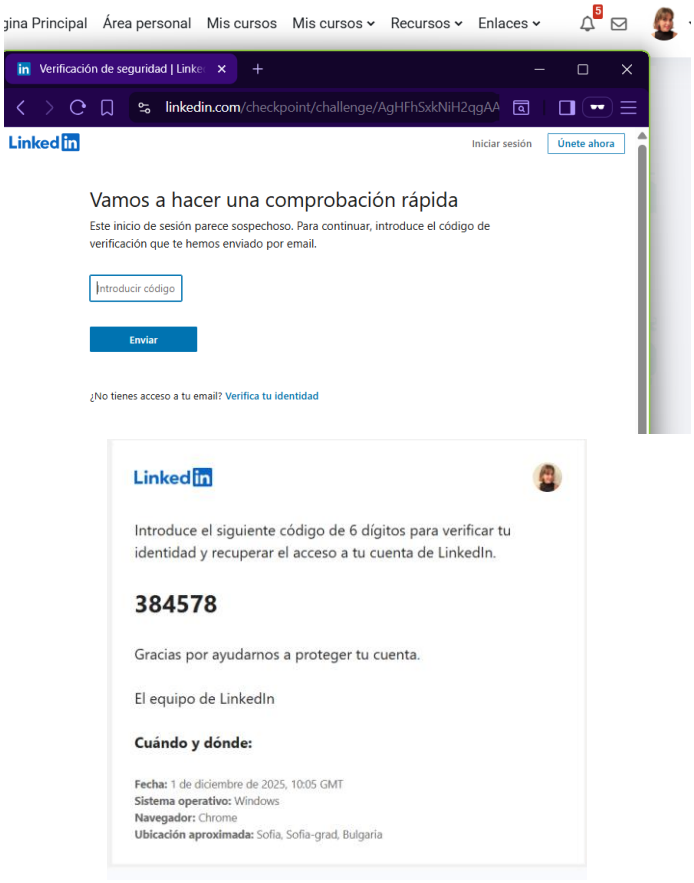


Se debe completar el recaptcha y seleccionar las imágenes que correspondan a un semáforo.



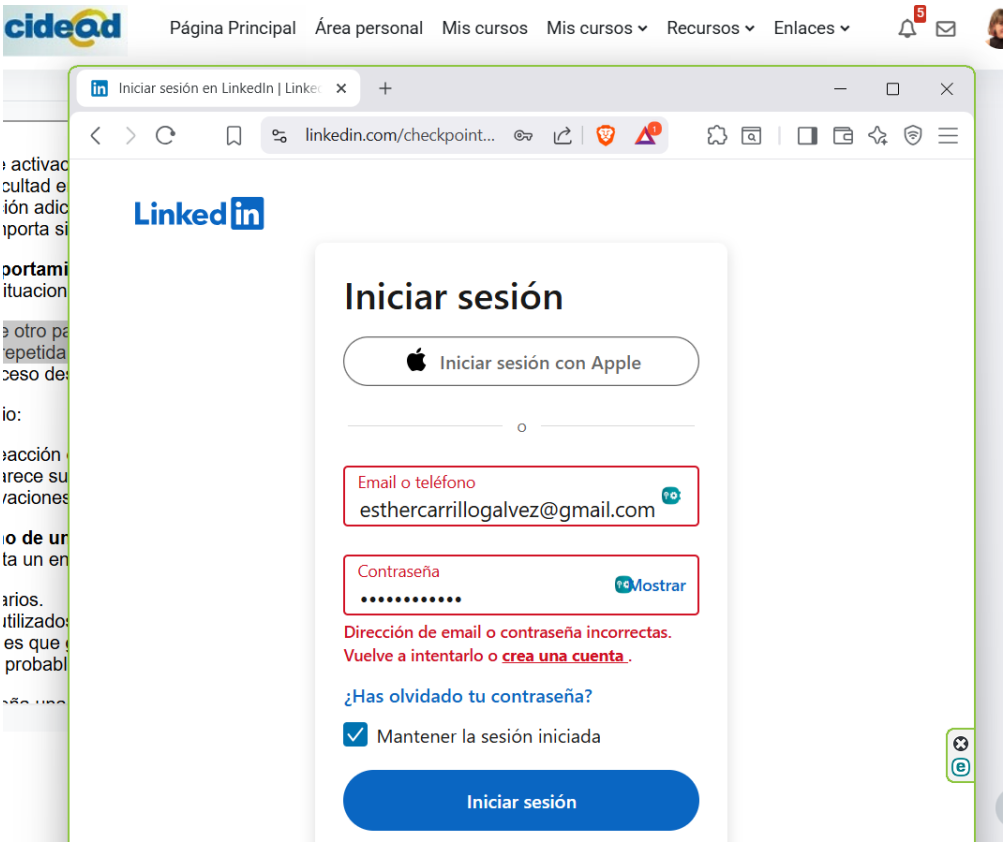


El siguiente paso es introducir el código que se ha enviado al dispositivo móvil. Finalmente se consigue el acceso a la cuenta de linkedin con una VPN en Sofía. Este proceso de verificación me ha parecido adecuado al enviar un código de comprobación al correo vinculado a la cuenta para evitar que el atacante tenga acceso sin medidas de seguridad.

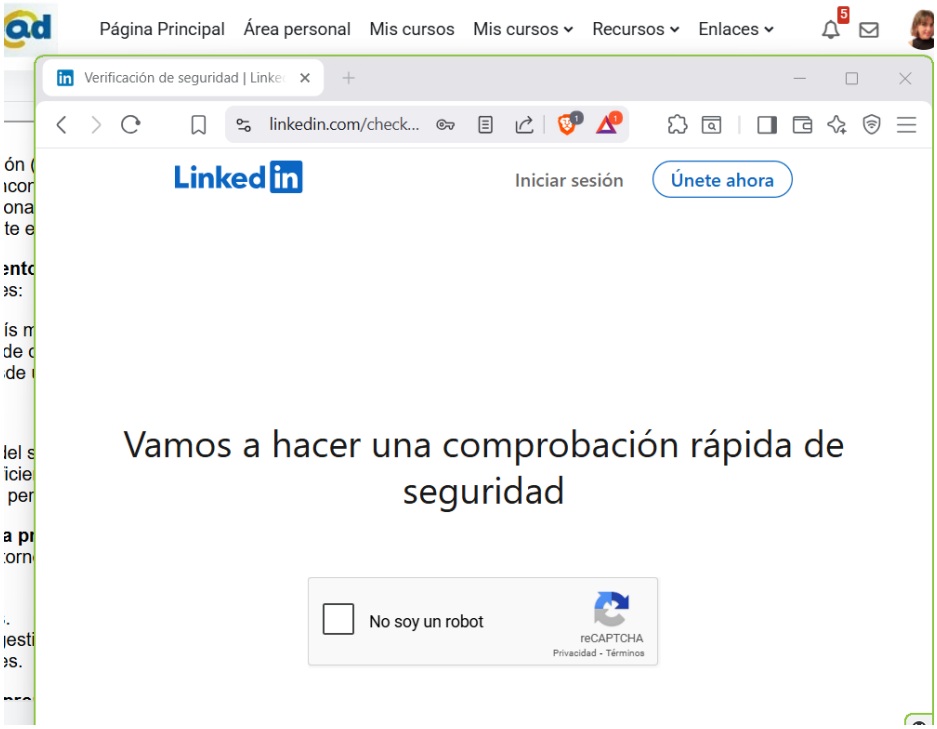


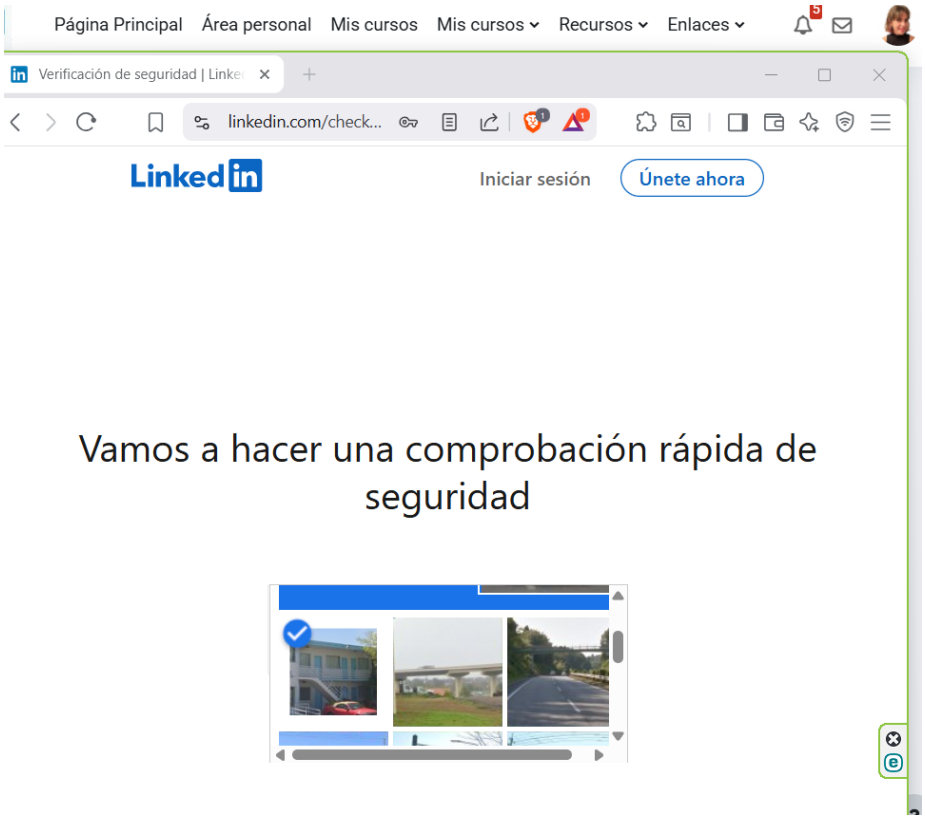
Introducción repetida de contraseñas incorrectas.

Se introduce la contraseña incorrecta *123456* en varias ocasiones.



Tras varios intentos con la contraseña incorrecta, la aplicación vuelve a solicitar la comprobación segura mediante el recaptcha. Es un método de comprobación de la persona que está accediendo, puesto que en todo momento hay una verificación en dos pasos, proporcionando un mayor nivel de robustez ante un posible ataque de fuerza bruta.





Intento de acceso desde un dispositivo desconocido.

Se accede a la cuenta de linkedin en un dispositivo desconocido, no obstante, no se recibe ningún aviso en el dispositivo de origen ni ninguna notificación *Popup*. Solamente se recibe este mensaje al correo vinculado con la cuenta, pero no indica en ningún momento que se ha accedido desde otro dispositivo diferente. Es una medida insuficiente porque en el caso de que el atacante consiga la contraseña de mi cuenta, no lo podré detectar y accederá sin ningún problema a mis datos. Además de que en ningún momento se ha solicitado la verificación de doble factor tal y como se solicitaba con una ubicación distinta mediante VPN.

Hola, Esther:

Has activado la funcionalidad «Recordar cuenta» en un nuevo dispositivo **LinkedIn, Android en Aguilas, Murcia, España**.
Obtén más información sobre cómo funciona «Recordar cuenta» en los dispositivos.

Si tienes más dudas,
contacta con el servicio de atención al cliente.

¡Gracias por confiar en LinkedIn!
El equipo de LinkedIn

Cuándo y dónde:

Fecha: 1 de diciembre de 2025, 10:38 (GMT)
Navegador: LinkedIn
Sistema operativo: Android
Ubicación aproximada: Aguilas, Murcia, España

4. Apartado 3: Diseño de una propuesta de autenticación para un entorno real

Diseño de propuesta de autenticación para colegio de secundaria y bachillerato

- Tipos de usuarios: profesorado, estudiantes y dirección.
- Dispositivos utilizados: pc, tablets y móviles.
- Datos sensibles que gestionan: información personal de menores, nombres, DNI, direcciones, historiales académicos, matrículas.
- Riesgos más probables: suplantación de identidad de alumnos

Tipo de usuario	Factores utilizados	Factores no recomendados	Política de recuperación de acceso
Profesorado	Autenticador de Google.	Llaves de seguridad físicas. Riesgo de pérdida masiva de los datos.	Validación mediante correo institucional del centro.
Estudiantes	Solo solicita verificación de acceso con más de 3 intentos erróneos seguidos.	Generar código vía SMS no es fiable para menores de edad y que puede que no dispongan de móvil.	Pueden usar un correo de un padre/madre o tutor/a para recibir el enlace de verificación.
Dirección	Reconocimiento biométrico mediante huella.	Preguntas de seguridad tradicionales porque son adivinables.	Validación mediante correo institucional del centro.

Diagrama proceso de autenticación para dirección.

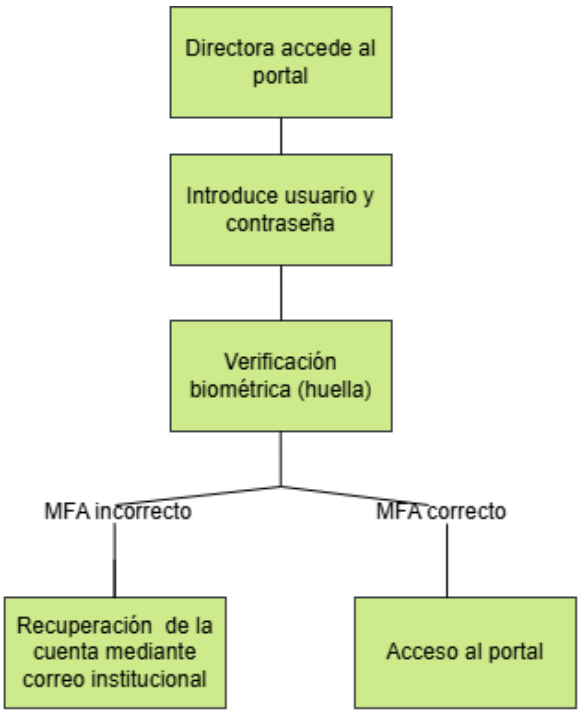


Diagrama proceso de autenticación para profesorado.

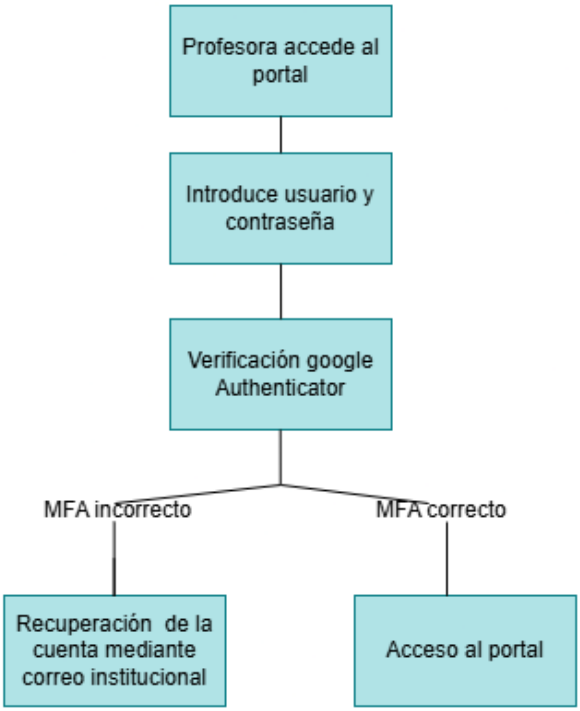
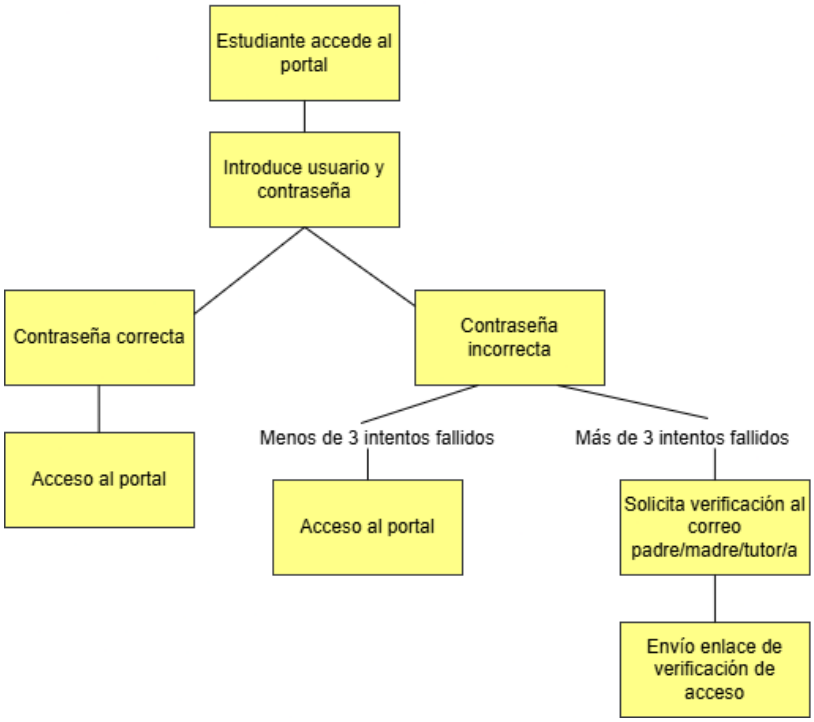


Diagrama proceso de autenticación para estudiantes.



5. Bibliografía

Darktrace. (s. f.). *MFA under attack: AiTM Phishing Kits abusing legitimate services*. Darktrace Blog. Recuperado el 1 de diciembre de 2025, de https://www.darktrace.com/blog/mfa-under-attack-aitm-phishing-kits-abusing-legitimate-services

EHC Group. (2024, 13 de diciembre). *Vulnerabilidad permitía saltear el 2FA de Microsoft Azure*. EHC Group Blog. Recuperado de https://blog.ehcgroup.io/2024/12/13/16/50/46/17854/vulnerabilidad-permitia-saltear-el-2fa-de-microsoft-azure/noticias-de-seguridad/ehacking/