Soluciones 2FA y passwordless

Luis Hong Wu Wang

Seguridad empresarial

Nombre Tutor/a de TF
Víctor Garcia Font
Profesor/a responsable de la asignatura
Pau Del Canto

13/03/2023

Universitat Oberta
de Catalunya

FICHA DEL TRABAJO FINAL

Título del trabajo:	*Soluciones de 2FA y passwordless*
Nombre del autor:	*Luis Hong Wu Wang*
Nombre del consultor/a:	*Pau Del Canto*
Nombre del PRA:	*Victor Garcia Font*
Fecha de entrega (mm/aaaa):	*06/2023*
Titulación o programa:	*Máster en Ciberseguridad y Privacidad*
Área del Trabajo Final:	*Seguridad empresarial*
Idioma del trabajo:	*Castellano*
Palabras clave	*Passwordless, 2FA, Contraseñas*

Resumen del Trabajo

Las contraseñas son una forma común de autenticación y se utilizan para proteger el acceso a información privada en línea. Sin embargo, a pesar de su importancia, las contraseñas son vulnerables a diversos tipos de ataques, como el robo o la adivinanza de contraseñas. El propósito del trabajo es explicar esas vulnerabilidades y como mejorar la seguridad con la implementación de autenticación de segundo factor y/o métodos de passwordless.

Abstract

Passwords are a common form of authentication and are used to protect access to private information online. However, despite their importance, passwords are vulnerable to various types of attacks, such as theft or password guessing. The purpose of the work is to explain these vulnerabilities and how to improve security with the implementation of second factor authentication and/or passwordless methods.

Índice

Lista de figuras

1. Introducción

El uso de contraseñas para la protección de información ha sido una práctica común en la era digital. Sin embargo, el aumento del número de contraseñas necesarias para acceder a diferentes servicios ha generado una carga adicional para los usuarios y, además, ha llevado a la creación de contraseñas débiles y reutilizadas. Estos factores han resultado en un aumento en los problemas de seguridad de las contraseñas.

En la actualidad, uno de los principales problemas de seguridad de las contraseñas es la facilidad con la que pueden ser descifradas por los hackers. Los ataques de fuerza bruta y de diccionario son dos de las técnicas más utilizadas por los ciberdelincuentes para descifrar contraseñas. Estas técnicas se basan en la generación sistemática de combinaciones de caracteres hasta encontrar la contraseña correcta. Además, el uso de contraseñas débiles y comunes, como "123456" o "contraseña", aumenta significativamente la probabilidad de que los hackers puedan descifrarlas.

Otro problema de seguridad de las contraseñas es la reutilización de contraseñas. Muchos usuarios utilizan la misma contraseña para diferentes servicios, lo que significa que si un hacker descubre la contraseña de uno de estos servicios, tendría acceso a todos los servicios donde se utiliza esa misma contraseña. Esta práctica aumenta el riesgo de pérdida de información y la vulnerabilidad a ataques malintencionados.

Por otro lado, el robo de contraseñas también es una preocupación importante. El phishing y la ingeniería social son técnicas utilizadas por los ciberdelincuentes para engañar a los usuarios y obtener sus contraseñas. En muchos casos, los usuarios proporcionan sus contraseñas sin saber que están siendo engañados, lo que permite a los hackers acceder a la información protegida por la contraseña.

En respuesta a estos problemas de seguridad, se han desarrollado diferentes soluciones. Una de ellas es la autenticación de dos factores, que requiere que los usuarios proporcionen una segunda forma de autenticación, como un código enviado a su teléfono móvil, además de la contraseña. Otra solución es el uso de contraseñas más largas y complejas, que incluyen caracteres especiales y números. También existen herramientas de gestión de contraseñas, que permiten a los usuarios generar contraseñas aleatorias y únicas para cada servicio, y almacenarlas de forma segura.

En conclusión, los problemas de seguridad de las contraseñas son una preocupación importante en la era digital. La reutilización de contraseñas, el descifrado de contraseñas y el robo de contraseñas son algunos de los riesgos a los que se enfrentan los usuarios. Es importante que los usuarios adopten

prácticas seguras al elegir y gestionar sus contraseñas y que se utilicen soluciones tecnológicas para mejorar la seguridad de las contraseñas.

1.1. Contexto y justificación del Trabajo

Hoy en día, la importancia que tiene el tema de la seguridad en el entorno digital, especialmente en un momento en el que la mayoría de la información se almacena y se comparte de manera remota, y la creciente utilización de servicios y aplicaciones en la nube hace que las contraseñas sean una pieza fundamental de la seguridad en internet, pero su vulnerabilidad es un problema que ha sido objeto de diversas investigaciones y estudios. Por tanto, entender las vulnerabilidades más comunes de las contraseñas y cómo mitigar o minimizar el riesgo protegiendo las contraseñas e investigando las posibles soluciones para mejorar su seguridad es de primerísima necesidad, sobre todo en los entornos empresariales.

La autenticación es un proceso vital en la seguridad de cualquier sistema informático, ya que se encarga de verificar la identidad del usuario que intenta acceder a un recurso. Sin embargo, el uso de contraseñas como único factor de autenticación ha demostrado ser cada vez más vulnerable a ataques de phishing, fuerza bruta y otros métodos de intrusión.

Es por eso que se han desarrollado diferentes métodos de autenticación de segundo factor, que agregan una capa adicional de seguridad al requerir que el usuario proporcione una segunda forma de identificación después de la contraseña. Estas formas pueden incluir un código generado por una aplicación móvil, un token físico o un mensaje de texto.

Por otro lado, el uso de autenticación sin contraseña (passwordless) se está convirtiendo en una opción popular para aquellos que buscan una forma más fácil y segura de autenticarse. La autenticación sin contraseña utiliza otras formas de autenticación, como la biometría o los mensajes de texto, para identificar al usuario en lugar de una contraseña tradicional.

La justificación de este trabajo es explorar los beneficios y desafíos de la autenticación de segundo factor y la autenticación sin contraseña, así como proporcionar una comparación entre los dos métodos. Además, también se discutirán las mejores prácticas y consideraciones de seguridad para implementar estos métodos en diferentes entornos, como en empresas o servicios en línea. Con esto, se espera proporcionar información valiosa para ayudar a las organizaciones a tomar decisiones informadas sobre la implementación de estos métodos de autenticación en sus sistemas.

1.2. Objetivos del Trabajo

El objetivo de este trabajo es entender mejor el problema de las contraseñas y exponer las ventajas e inconvenientes de las soluciones que existen para mitigar estos problemas. En concreto las soluciones de autenticación de dos factores y passwordless.

Una vez entendido y explicado el problema se realizará un estudio de las soluciones actuales en el mercado de para la autenticación de segundo factor y passwordless que ayudan a mitigar los riesgos dentro de las contraseñas.

Como parte final se propondrá un caso práctico creando un entorno empresarial simulado e implementando una solución para mejorar la seguridad en las contraseñas. A lo largo del trabajo se explicará paso a paso de todo el proceso de creación e implementación de la solución.

1.3. Impacto en sostenibilidad, ético-social y de diversidad

En cuanto a la sostenibilidad, se puede explorar cómo el uso de contraseñas débiles o la necesidad de cambiarlas con frecuencia puede afectar al medio ambiente a través del consumo energético de los servidores que almacenan información. Además, es importante considerar la seguridad de los datos personales y cómo la vulnerabilidad de las contraseñas puede impactar en la privacidad y la seguridad de las personas. En este sentido, se pueden estudiar aspectos ético-sociales de la seguridad de la información y cómo afecta a la confianza y transparencia en la relación entre empresas y usuarios. También es relevante analizar la diversidad en la seguridad de las contraseñas, como la necesidad de evitar prejuicios en los algoritmos de autenticación, y cómo la inclusión de diferentes grupos en el diseño de sistemas de seguridad puede mejorar la seguridad y la experiencia de usuario.

La implementación de soluciones de autenticación de segundo factor tiene un impacto en sostenibilidad, ético-social y de diversidad que debe ser considerado. En términos de sostenibilidad, la implementación de soluciones de autenticación de segundo factor puede generar una reducción en el consumo de energía y recursos, ya que se reduce la necesidad de reiniciar contraseñas olvidadas o recuperar cuentas hackeadas, lo que puede generar una disminución en la emisión de gases de efecto invernadero.

En cuanto al impacto ético-social, es importante tener en cuenta que no todas las soluciones de autenticación de segundo factor son iguales en términos de privacidad y seguridad. Algunas soluciones pueden recopilar y almacenar información personal, lo que puede ser preocupante desde una perspectiva de privacidad. Además, es importante considerar si el uso de una solución de autenticación de segundo factor es obligatorio para todos los usuarios, ya que esto puede excluir a aquellos que no tienen acceso a la tecnología necesaria.

En términos de diversidad, es importante tener en cuenta que no todas las personas tienen la misma capacidad o acceso a los dispositivos necesarios para utilizar ciertas soluciones de autenticación de segundo factor. Algunas personas pueden tener discapacidades físicas o cognitivas que les impiden usar ciertas soluciones, mientras que otras pueden no tener acceso a la tecnología necesaria debido a barreras financieras o geográficas. Por lo tanto, es importante considerar la accesibilidad y la inclusión al seleccionar una solución de autenticación de segundo factor.

1.4. Enfoque y método seguido

El trabajo se dividirá en dos partes claramente separadas, una parte teórica y otra práctica.

En la parte teórica se incluye:

- Explicación e investigación de los problemas de las contraseñas para entender el riesgo de seguridad.
- Investigar las diferentes soluciones actuales que existen para aumentar la seguridad en torno a las contraseñas.
- Entender y explicar las soluciones de autenticación de segundo factor.
- Entender y explicar las soluciones de passwordless.
- Investigar sobre las posibles herramientas actuales para la implementación de dichas soluciones.

Para realizar esta parte y abordar la problemática y analizarla, se deben aplicar los métodos lógicos y empíricos correspondientes, además de utilizar los tipos de fuentes que sean adecuados para el enfoque de la investigación.

Se consultará diferentes Fuentes actualizadas sobre las vulnerabilidades de las contraseñas y qué soluciones hay para mejorar la seguridad. También se hará un estudio de mercado para conocer las herramientas que hay hoy en día que ayudan a mitigar el riesgo que hay con el uso de contraseñas.

La segunda parte del trabajo consistirá en una parte práctica implementando una solución en un entorno empresarial simulado en la plataforma Azure (en la nube).

- Crear desde 0 un entorno empresarial en Azure, con su directorio activo. Se utilizará la cuenta de estudiante de la UOC.
- Configurar las políticas de seguridad de contraseñas para la organización empresarial.
- Implementar una solución de autenticación de segundo factor para los empleados/miembros de la empresa creada.
- Combinar otras posibles soluciones para mejorar la seguridad.
- Demostrar que la implementación ha sido exitosa.

Para realizar esta parte se necesitará investigación para entender la mejor manera de implementar las soluciones más adecuadas en la plataforma. Asegurarse que se siguen las buenas prácticas a la hora de la implementación de la o las posibles soluciones es igual de importante.

La manera de validar si la implementación ha sido exitosa será la simulación de un usuario que pertenece a la empresa simulada tendrá que acceder a su cuenta empresarial con los métodos de autenticación seguros implementados en el entorno empresarial.

1.5. Planificación del Trabajo

Como está previsto para realizar el trabajo final de máster varias entregas de seguimiento antes de la entrega final, se ha decidido la siguiente planificación:

1. Para la PEC 1
    a. Primera reunión con el profesor para alineamiento de las ideas para el trabajo.
    b. Primer borrador de la introducción y estado del arte.
    c. Planificación y metodología del trabajo.

2. PEC 2

    a. Refinar los objetivos parciales definidos en la actividad anterior.
    b. Índice de la memoria definiendo los apartados.
    c. Lectura e investigación de la parte teórica.
    d. Organizar la información de manera coherente en la memoria.

3. PEC 3
    a. Implementar los cambios después de la corrección de la PEC 2.
    b. Investigar y planificar como implementar la parte práctica.
    c. Crear el entorno práctico con las soluciones propuestas.
    d. Documentar todo el proceso.

4. Entrega Final
    a. Correcciones sobre la PEC 3, con los comentarios del profesor.
    b. Finalizar la memoria con la parte teórica y práctica.

5. Vídeo presentación.
    a. Realizar un vídeo explicando detalladamente el trabajo realizado.
    b. Crear herramientas de apoyo para la presentación (PPT, ejemplos, demos…)

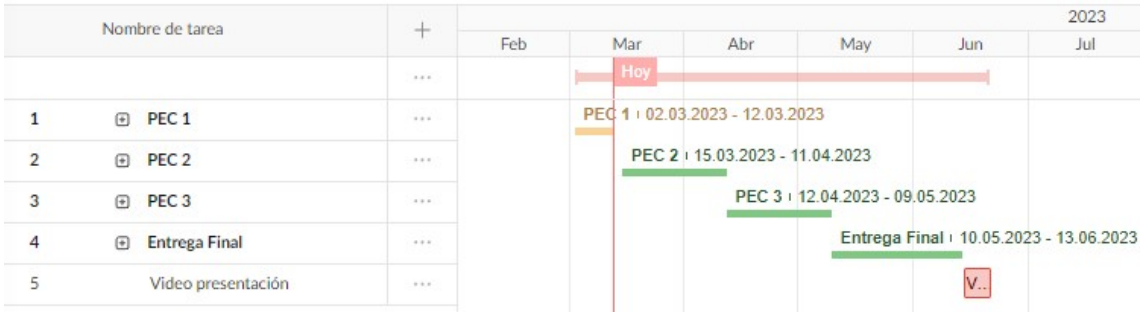

Figura 1: Planificación en Gantt [1].

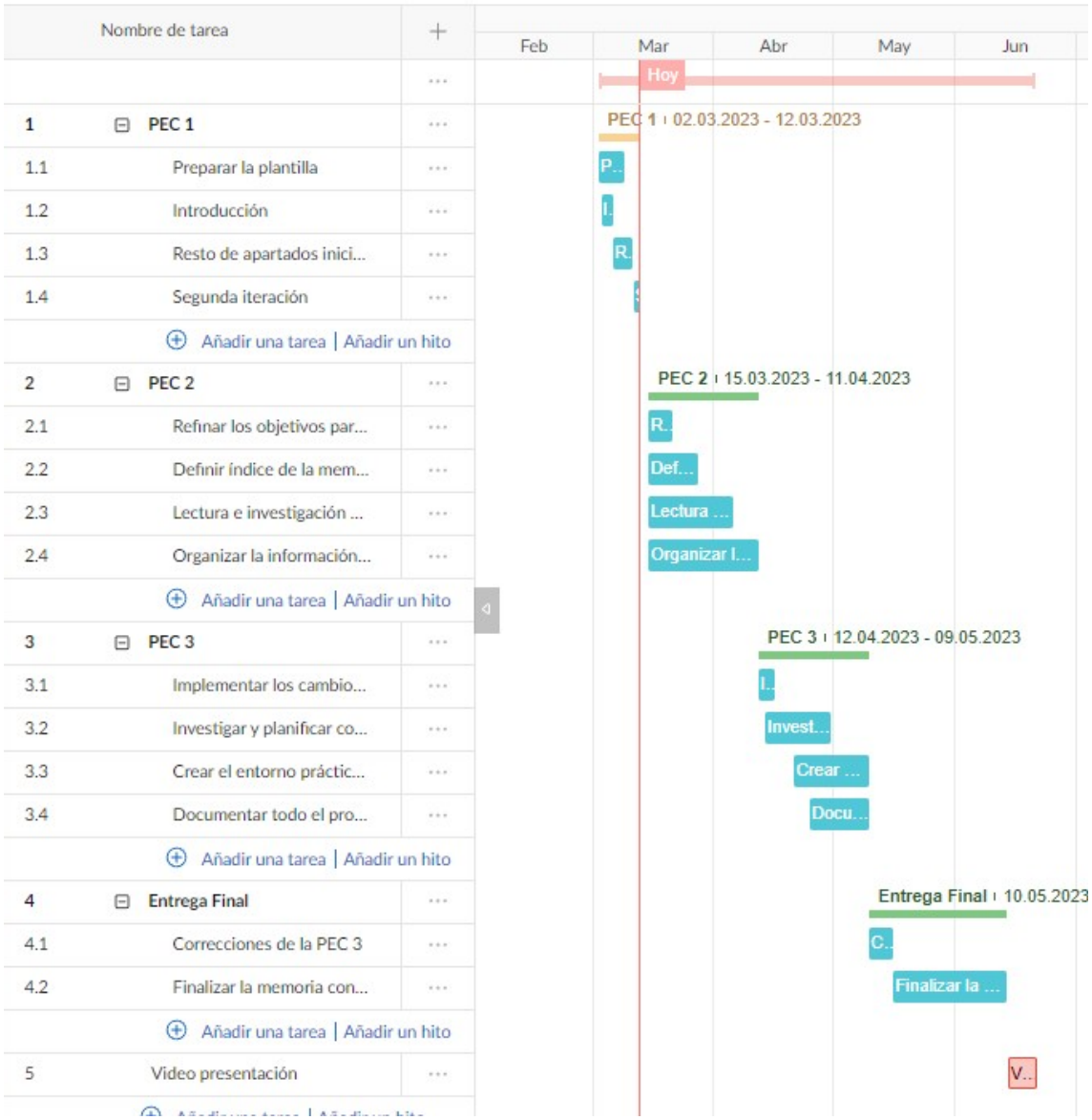

Figura 2: Planificación en Gantt detallada.

1.6. Breve sumario de productos obtenidos

En el marco teórico se detallarían los conceptos básicos relacionados con la autenticación y las contraseñas, los diferentes tipos de autenticación y los protocolos utilizados en la autenticación de segundo factor y sin contraseña.

En la parte práctica se va a desarrollar un entorno empresarial en la nube con usuarios y cuentas ficticias perteneciente a dicha empresa. Luego se implementarán las mejoras de seguridad en las contraseñas sobre las cuentas.

1.7. Breve descripción de los otros capítulos de la memoria

En los próximos capítulos se entrará en detalle sobre los métodos de autenticación de segundo factor y sin contraseña o passwordless. Empezando por un poco de historia sobre los métodos de autenticación de segundo factor y passwordless y los sus beneficios.

Hay que tener em cuenta los desafíos y riesgos de la autenticación de segundo factor y sin contraseña y las técnicas y tecnologías para implementarlas y tener en cuenta las consideraciones legales y de privacidad.

También se evaluará la efectividad de la autenticación de segundo factor y sin contraseña analizando las diferentes soluciones que hay en el mercado.

Para la parte más práctica se implementará diferentes soluciones de autenticación de segundo factor o sin contraseña en un entorno empresarial simulado. Se explicará paso a paso todo lo realizado de manera detallada explicando las decisiones tomadas.

2. Autenticación de segundo factor y passwordless

2.1. Historia sobre los métodos de autenticación de segundo factor y passwordless.

La autenticación de segundo factor sin contraseña es un avance sobre las técnicas de autenticación que se han utilizado desde los primeros días de la informática. Los primeros tipos de autenticación se basaban en contraseñas, que por lo general eran cortas y fáciles de adivinar. A medida que las amenazas en línea se volvieron más sofisticadas, se desarrollaron nuevas técnicas para la protección de la identidad del usuario.

La autenticación de segundo factor se usó por primera vez en la década de 1980 cuando los bancos comenzaron a usar tokens físicos para brindar una capa adicional de seguridad. Estos tokens generaban un código único que el usuario debía proporcionar junto con su contraseña para iniciar una sesión en su cuenta.

En la década de los 90, se desarrollaron las tarjetas inteligentes, que permitían almacenar información de autenticación y realizar la autenticación en el propio dispositivo. Con la llegada de los teléfonos móviles, se comenzaron a utilizar códigos de un solo uso enviados por SMS o por aplicaciones móviles para la autenticación de segundo factor.

La autenticación sin contraseña, por otro lado, se ha desarrollado en los últimos años con el objetivo de hacer que el proceso de autenticación sea más fácil y seguro para los usuarios. Las técnicas de autenticación basadas en biometría, como la identificación de huellas dactilares, reconocimiento facial y de iris, se han vuelto cada vez más comunes en los dispositivos móviles y computadoras portátiles.

En resumen, no hay una fecha u hora específica que se pueda usar para identificar el origen de la autenticación sin contraseña y de segundo factor. Sin embargo, debido a la necesidad de una mayor seguridad en línea, su uso se ha generalizado cada vez más en los últimos años. Desde el acceso a cuentas de correo electrónico hasta el acceso a sistemas corporativos, la autenticación de segundo factor se ha utilizado en una variedad de entornos. La idea sin contraseña, por otro lado, es una tendencia más reciente que ha ganado popularidad como resultado de los problemas de seguridad que se han revelado con el uso de contraseñas convencionales.

2.2. Beneficios e inconvenientes

Uno de los beneficios principales es que aumenta la seguridad del inicio de sesión [5] al requerir no solo una contraseña, sino también un segundo factor de autenticación, como un código generado por una aplicación de autenticación.

A continuación, podemos detallar los beneficios del uso de la autenticación de segundo factor:

- Activar la autenticación de segundo factor puede mejorar la seguridad de las cuentas de los usuarios, dificultando a los atacantes el acceso no autorizado y, a su vez, reduciendo las posibilidades de que se produzcan actividades fraudulentas e incidentes de usurpación de identidad.

- Aumento de la confianza del cliente: Al proporcionar una capa adicional de seguridad, la autenticación de segundo factor puede aumentar la confianza del cliente en la plataforma o servicio que utiliza.

- Cumplimiento de las normativas: La autenticación de segundo factor puede ayudar a las empresas a cumplir con las normativas y requisitos de seguridad, como el Reglamento General de Protección de Datos (RGPD) de la UE.

- Reducción de los costos operativos: Al reducir el riesgo de fraude y robo de identidad, la autenticación de segundo factor puede ahorrar a las empresas costos adicionales asociados con la recuperación de cuentas y la resolución de problemas de seguridad.

- Optimización de las transacciones móviles seguras: La autenticación de segundo factor puede ayudar a las empresas a proteger mejor las transacciones móviles, lo que es especialmente importante en un mundo cada vez más impulsado por dispositivos móviles.

- Combate la fatiga de las contraseñas: La autenticación de segundo factor puede reducir la fatiga de las contraseñas al permitir que los usuarios utilicen otros medios de identificación, como un lector de huellas digitales o una aplicación de autenticación.

- Simplificación del proceso de inicio de sesión: Aunque la autenticación de segundo factor agrega una capa adicional de seguridad, puede simplificar el proceso de inicio de sesión, ya que los usuarios pueden utilizar su segundo factor de identificación preferido, como una aplicación de autenticación en lugar de una contraseña compleja.

Aunque la autenticación de segundo factor y sin contraseña presenta varios beneficios, también existen algunos inconvenientes que se deben tener en cuenta. A continuación, se presentan algunos de ellos:

- Necesidad de hardware adicional: Algunas formas de autenticación de segundo factor, como el uso de llaves físicas o tokens, requieren que se tenga un hardware adicional. Esto puede resultar en un costo adicional y en la necesidad de llevar consigo el hardware en todo momento.

- Fallos en la integración: El uso de métodos de autenticación de segundo factor y sin contraseña puede no estar disponible en todas las aplicaciones o sistemas, lo que puede resultar en una experiencia de autenticación inconsistente.

- Problemas de privacidad: Algunas formas de autenticación de segundo factor pueden requerir el uso de datos biométricos, como huellas dactilares o reconocimiento facial, lo que plantea preocupaciones en cuanto a la privacidad y el almacenamiento de estos datos.

- Pérdida de acceso: Si se pierde el dispositivo utilizado para el segundo factor de autenticación, como un teléfono móvil o una llave física, se puede perder el acceso a la cuenta. Además, recuperar el acceso a la cuenta puede ser un proceso complicado y llevar mucho tiempo.

- Complejidad: Algunos usuarios pueden encontrar la autenticación de segundo factor y sin contraseña más complicada y engorrosa que simplemente ingresar un nombre de usuario y contraseña. Esto puede resultar en una resistencia al uso y un aumento en la probabilidad de errores al ingresar la información de autenticación.

En conclusión, hay que tener en cuentas los inconvenientes y saber cómo minimizarlos ya que, los beneficios que pueden aportar son más notorios. En este caso los inconvenientes se pueden solventar de manera relativamente sencilla.

2.3. Desafíos y riesgos

Uno de los principales desafíos es la forma en que se implementa la autenticación de segundo factor. Según, la opción más común es a través de SMS, pero esto puede no ser la opción más segura, ya que los ciberdelincuentes pueden interceptar los mensajes de texto o incluso simular la identidad del usuario para recibir los mensajes en su propio dispositivo.

Otro desafío es la complejidad que puede representar para los usuarios tener que usar diferentes métodos de autenticación, especialmente si se utilizan diferentes dispositivos o servicios que tienen diferentes opciones de autenticación.

Además, aunque la autenticación de segundo factor puede reducir el riesgo de ataques, no es una solución infalible. Los hackers o atacantes pueden utilizar técnicas como el phishing para engañar a los usuarios y obtener información de autenticación, incluyendo los códigos de segundo factor.

Por esta razón, los riesgos que hay con la autenticación de segundo factor puede ser la falsa seguridad que proporciona ya que no es infalible y se requiere también conocimientos para evitar los otros ataques de los malhechores.

Por otro lado, en el caso de la autenticación sin contraseña, uno de los principales riesgos es la posibilidad de que un atacante pueda acceder a la información biométrica del usuario, como huellas dactilares o reconocimiento facial. Además, existe la posibilidad de que la información biométrica del usuario sea almacenada de manera insegura y pueda ser robada por un atacante.

En resumen, aunque la autenticación de segundo factor y la autenticación sin contraseña son medidas de seguridad útiles, es importante tener en cuenta los riesgos asociados con estas formas de autenticación y tomar medidas para mitigarlos. Por ejemplo, es recomendable utilizar métodos de autenticación alternativos y más seguros, como aplicaciones de autenticación o tokens FIDO U2F.

2.4. Consideraciones legales y de privacidad

En cuanto a las consideraciones legales, es importante cumplir con la regulación y disposiciones aplicables en cada país, incluyendo el Reglamento General de Protección de Datos (RGPD) en la Unión Europea. El RGPD establece que las medidas de seguridad deben garantizar un nivel adecuado de seguridad y confidencialidad de los datos personales, teniendo en cuenta el estado de la técnica y el coste de su aplicación con respecto a los riesgos y la naturaleza de los datos personales que deban protegerse [2]. Además, las administraciones públicas deben aprobar la disposición de regulación pertinente de sus bases de datos y publicar en un Diario Oficial el fichero previamente al inicio de la recogida de datos y del uso de este.

En cuanto a las consideraciones de privacidad, es importante garantizar que la medida de autenticación elegida sea necesaria y adecuada para alcanzar el objetivo de vigilancia y control. Además, es importante que la medida elegida no comprometa la privacidad de los usuarios, por lo que se debe evaluar cuidadosamente el riesgo de exposición de datos personales o información confidencial.

3. Metodologías de autenticación de segundo factor

Existen diferentes metodologías para la autenticación de segundo factor, cada una con sus propias ventajas y desventajas [3]. Las más usadas son:

- OTP (One Time Password) o Código de un solo uso.
- Autenticación mediante aplicación móvil.
- Notificación push.
- Clave de seguridad física.

3.1. OTP (One Time Password) o Código de un solo uso

Como su nombre indica OTP son las siglas de "one-time password" o contraseña de un solo uso en español. Se trata de un código que se genera en el momento y que solo puede ser utilizado una vez para reforzar la seguridad en los procesos de autenticación.

Es el sistema más extendido y aceptado por los usuarios. Sobre todo, el envío por SMS de dichas contraseñas de un solo uso. La mayoría de sistemas bancarios utilizan esta tecnología de seguridad para que los usuarios puedan realizar transacciones en banca online.

Sin embargo, existen otras herramientas que usan este principio para securizar la identidad del usuario como la generación de contraseñas dinámicas por dispositivos físicos. Estos dispositivos son pequeños dispositivos electrónicos que generan códigos OTP en lugar de utilizar una aplicación. A menudo se les llama "tokens" y pueden ser más seguros que los métodos basados en software. Sin embargo, pueden ser menos convenientes para los usuarios que los métodos basados en aplicaciones debido a la necesidad de llevar el token físico consigo.

Figura 3: Dispositivo físico de generación de código de un solo uso.

No hay un estándar oficial para OTP, existe un algoritmo de código abierto conocido como "HOTP" o "HMAC-based One-Time Password Algorithm" que ha sido adoptado por muchas empresas y organizaciones como una alternativa segura para la autenticación de dos factores. Este algoritmo utiliza una clave compartida entre el usuario y el servidor, así como un contador que se incrementa cada vez que se genera un nuevo código OTP.

Además del algoritmo HOTP, existe otro algoritmo de código abierto llamado "TOTP" o "Time-based One-Time Password Algorithm", que utiliza un contador de tiempo en lugar de un contador de eventos para generar códigos OTP. Este algoritmo está estandarizado por el IETF (Internet Engineering Task Force) en el RFC 6238.

3.2. Autenticación mediante aplicación móvil

La autenticación mediante aplicación móvil consiste en descargar una aplicación de autenticación en un dispositivo móvil, como Google Authenticator o Microsoft Authenticator, que genera códigos de acceso únicos y temporales que se utilizan junto con la contraseña para confirmar la identidad del usuario al iniciar sesión en una cuenta en línea. Estos códigos se generan cada cierto tiempo y se pueden usar incluso sin conexión a Internet. Además, la autenticación mediante aplicación móvil puede ser utilizada como una forma de recuperar la cuenta en caso de que se olvide la contraseña, ya que la aplicación puede realizar una copia de seguridad y restaurar todas las credenciales de la cuenta. Este método de autenticación es cada vez más común en el entorno empresarial y en la protección de datos sensibles debido a su alta seguridad.

El funcionamiento de esta técnica es simple: una vez activada, cada vez que se inicia sesión en una cuenta se solicita un código adicional, además de la contraseña, para verificar la identidad del usuario. Este código puede ser generado por una aplicación de autenticación.

Para utilizar la autenticación mediante aplicación móvil, primero debemos instalar la aplicación de autenticación en nuestro dispositivo móvil y luego vincularla con nuestras cuentas de usuario en los sitios web o aplicaciones que lo permitan. Una vez activada, la autenticación de dos factores generará un código único que deberá ser ingresado para completar el proceso de inicio de sesión.

La principal ventaja es que es una técnica fácil de utilizar y que no requiere de grandes conocimientos técnicos para su configuración. El único inconveniente es en el caso de que el usuario pierda el dispositivo móvil no podría hacer uso de su cuenta o acceso y necesitaría de la ayuda de un administrador para vincular un nuevo dispositivo.

3.3. Notificación Push

Esta metodología es la evolución de la anterior ya que también suele requerir una aplicación móvil. Sin embargo, en este caso el usuario recibe una notificación push después de introducir sus credenciales y solo necesita aprobar o denegar la acción de autenticación que está realizando el usuario.

La ventaja de este método es la comodidad para el usuario, ya que no necesita introducir ningún código y los posibles errores humanos derivados. Otra ventaja es que no se guarda ningún código por lo que no hay posibilidad de que haya una mínima sospecha de que alguien pueda copiarlo.

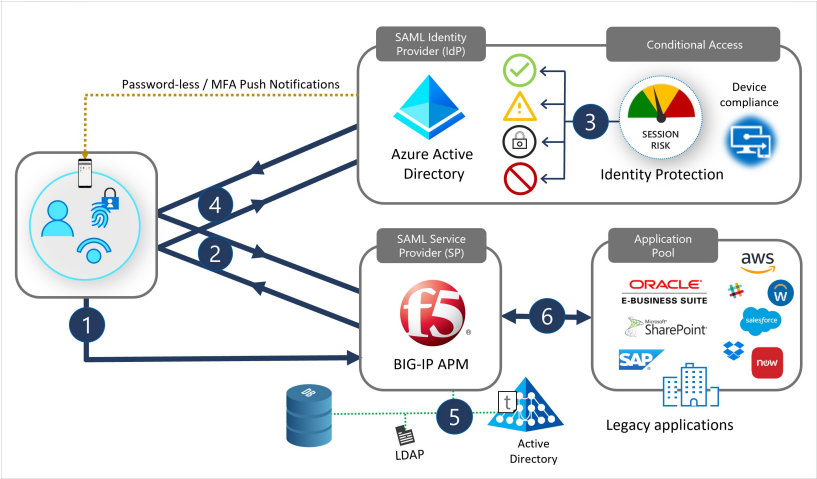

Figura 4: Ejemplo arquitectura notificación push.

Actualmente, cuando el usuario recibe la notificación push, tiene que desbloquear el dispositivo para aceptar la autenticación. Por lo tanto se suele combinar con la seguridad biométrica del dispositivo móvil (reconocimiento facial o huella dactilar) o el PIN de desbloqueo.

3.4. Clave de seguridad física

Este caso es sin duda el más desconocido y menos usado por las empresas que implementen seguridad en sus autenticaciones. Se requiere una "llave" física que se conecta a través del puerto USB para activar el dispositivo cuando la autenticación de segundo factor requiera la clave.

Es un método muy seguro ya que el usuario registra una clave pública en el servidor de autenticación y que se guarda en la llave USB. De esta manera solo el usuario con la llave podrá verificar su identidad incluso si has sido víctima de cualquier otro ciberataque o tu dispositivo móvil haya sido comprometido.

Figura 5: Llave de seguridad física.

4. Metodologías de autenticación passwordless

El uso de las contraseñas puede ser tedioso muchas veces, tener que recordad todas las contraseñas en todos los sitios registrados puede ser una odisea, o repetir contraseñas en diferentes sitios puede ser muy peligroso.

La autenticación passwordless [6] o sin contraseña puede ayudar a solventar esta problemática. Hoy en día hay diferentes metodologías para conseguirlo:

- Enlace de un solo uso enviado al correo.
- Cookie persistente.
- Uso de terceros (redes sociales).
- Biométrica a través del dispositivo móvil.

4.1. Enlace de un solo uso enviado al correo

Durante la autenticación, el usuario introduce su correo con el que está registrado y recibe un enlace en su correo y solo tiene que seguir el enlace. Este método es relativamente barato y fácil de implementar, sin embargo, toda la responsabilidad de seguridad recae sobre la cuenta de correo y en el caso de que estuviera comprometida la autenticación también lo estaría.

4.2. Cookie persistente

Es una de las metodologías más usadas, el usuario solo tiene que introducir correctamente una vez las credenciales, entonces se guardan en las cookies del navegador que se usan cada vez que accede al sitio. Esto es muy cómodo para el usuario, pero solo funciona en el dispositivo y navegador que el usuario se ha autenticado.

Uno de los grandes problemas es que los ciberdelincuentes y hackers saben esto e intentan robarte las cookies para suplantar la identidad y es uno de los ataques más comunes. Otra desventaja es que las cookies se caducan y entonces el usuario tiene que volver a introducir las credenciales.

4.3. Uso de terceros (redes sociales)

Muchas veces a la hora de la autenticación el usuario puede usar una cuenta existente de un proveedor de terceros como Google, Facebook o Linkedin. El usuario suele tener cuenta en esas aplicaciones y no tiene que recordar las credenciales ya que usa una cuenta ya registrada en la plataforma de terceros.

Es muy fácil de usar y simple de implementar. Sin embargo, si el usuario de alguna manera pierde el acceso a la cuenta de terceros también perdería acceso al servicio en el que quiere acceder.

4.4. Biométrica a través del dispositivo móvil.

Cuando el usuario se va a autenticar recibe una notificación en su dispositivo para confirmar la identidad a través de la huella dactilar del teléfono o del reconocimiento facial.

En este caso la seguridad de este método es muy eficiente ya que la seguridad recae en los fabricantes de los dispositivos y la efectividad en su tecnología biométrica que es muy alta.

5. Soluciones 2FA y Passwordless en el mercado

Hoy en día estamos viviendo en un mundo totalmente digital dónde las empresas están muy concienciadas sobre la seguridad de sus sistemas y tener bien controlado el acceso a sus redes e información. Existen muchos proveedores de soluciones de autenticación de doble factor en el mercado.

Según un estudio de tendencias el mercado de autenticación de dos factores [7] se valoró en USD 12 500 millones en 2021. Se prevé que la industria del mercado de autenticación de dos factores crezca de USD 14 650 millones en 2022 a USD 44 670 millones para 2030, mostrando una tasa de crecimiento anual compuesto (CAGR) de 17,26 % durante el período de pronóstico (2022 - 2030). Se espera que el creciente número de transacciones en línea, el aumento de las violaciones de seguridad y el cumplimiento de las normas regulatorias impulsen el crecimiento del mercado del segmento de autenticación de dos factores.

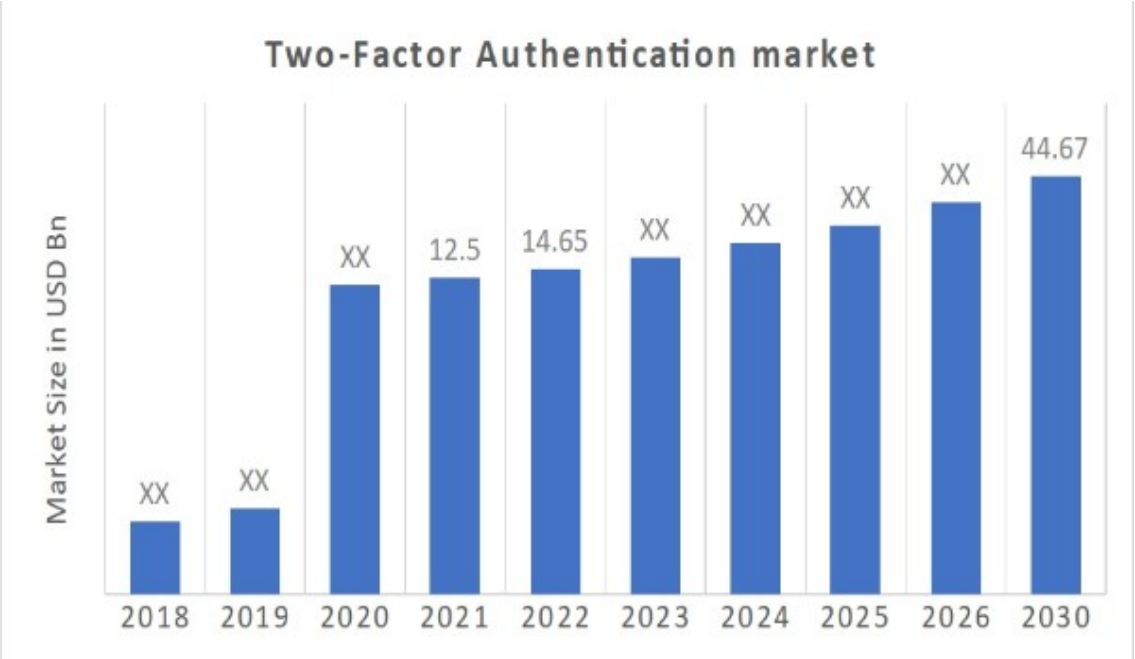

Figura 6: Tendencia de mercado

Como se ha podeido leer, es un mercado en exapansión y crecimiento. Existen varias solucione o empresas que ofrecen a otras empresas (B2B) servicios de seguirdad en autenticación. Cada empresa elige la solución que se adapta mejor a su entorno, siempre teniendo en cuenta ciertos factores importantes.

- Autenticación en remoto. Con el auge de teletrabajo es necesario proveer seguridad extra que soporte conexiones en remoto hacia la red interna de la empresa.

- Políticas y controles flexibles. Las necesidades de cada empresa son diferentes y la solución implementada tiene que integrarse con el entorno que actualmente está implementado.
- Analíticas. Una buena herramienta o solución tiene que poseer datos para poder analizarlos y que sean de relevancia para la empresa que ha implementado la solución.
- Sistema de login y reportes. Las soluciones de autenticación de segundo factor deben generar logs para poder investigar en el caso de que ocurra algún error. También deben tener la capacidad de generar reportes y opciones a ser monitorizados.

Las soluciones más conocidas o extendidas serían para grandes empresas varían mucho dependiendo de las necesidades descritas anteriormente. Sin embargo según un estudio de tendencias descrita en [4].

- Microsoft Authenticator
- Google Authenticator
- Duo security
- IBM Security Veirfy
- SecurID by RSA
- OKTA

Sabiendo que es un mercado en expansión [11] y la penetración del dispositivo móvil, también han surgido varias empresas que ofrecen aplicaciones para la autenticación de segundo factor como son LastPass, Authy, OneLogin o Ping Identity.

5.1. Microsoft Authenticator

Creado por la propia compañía Microsoft, Microsoft Authenticator es una aplicación que permite utilizar la autenticación en dos pasos para incrementar la seguridad en el inicio de sesión en las cuentas de Microsoft y en otras cuentas online. Esta aplicación permite iniciar sesión en cuentas Microsoft sin necesidad de ingresar una contraseña, utilizando huella digital, reconocimiento facial o PIN. Además, también permite autenticación multifactor y autorrelleno de contraseñas.

La aplicación Microsoft Authenticator se encuentra disponible para su descarga gratuita en dispositivos móviles Android y iOS.

Es una de las soluciones más extendidas ya que cuenta con la integración con sus sistemas y entornos del propio proveedor ya sea en local o en la nube. A través del directorio activo se integra la solución para que sus usuarios tengan un método de autenticación de segundo factor.

5.2. Google Authenticator

El gigante Google no ha querido quedarse atrás en temas de seguridad y por eso ha creado Google Authenticator [9].

Google Authenticator es una aplicación de autenticación en dos pasos creada para proporcionar códigos de seguridad que se pueden usar para verificar la identidad del usuario al iniciar sesión en una cuenta. Los códigos generados por Google Authenticator son de seis dígitos que cambian cada 30 segundos, lo que aumenta la seguridad de la cuenta del usuario.

La aplicación está disponible tanto para Android como para iOS, y puede ser configurada para varias cuentas del mismo dispositivo móvil, siendo necesario para cada cuenta una clave secreta diferente.

Para usar Google Authenticator, el usuario debe primero configurar la verificación en dos pasos en su cuenta de Google, lo que implica un proceso de configuración que puede variar según el dispositivo y el sistema operativo utilizado. Una vez que se configura la verificación en dos pasos, la aplicación se puede utilizar para recibir códigos de autenticación en cualquier momento y en cualquier lugar, incluso sin conexión a Internet o servicio telefónico.

Como podemos ver está usando la tecnología OTP (One time password) descrita anteriormente y añadiendo la dificultad que cambia cada 30s.

5.3. Duo Security

Duo Security [12] es una plataforma de seguridad cibernética que proporciona autenticación multifactorial para proteger el acceso a aplicaciones y dispositivos. Es una solución de seguridad Zero Trust fácil de usar y escalable para organizaciones de todos los tamaños y para todos los usuarios, dispositivos y aplicaciones.

La plataforma Duo Security es propiedad de Cisco y se conoce como "Duo: Secure Access de Cisco". Ofrece autenticación multifactorial potente y visibilidad avanzada de endpoints para proteger la fuerza laboral de una organización. Además, se establece como líder en Zero Trust.

Duo Security protege el inicio de sesión de los usuarios en aplicaciones y dispositivos desde cualquier dispositivo utilizado, mediante la implementación de MFA, lo que añade una capa adicional de seguridad en la identidad digital.

5.4. IBM Security Verify

IBM Security Verify [13] es una plataforma de seguridad cibernética que ofrece soluciones para el acceso seguro y la gestión de contraseñas de usuarios con privilegios en entornos híbridos multicloud o en local. Como su nombre indica ha sido desarrollada por la multinacional IBM.

IBM Security Verify Access, anteriormente conocido como IBM Security Access Manager o ISAM, es una aplicación que ayuda a simplificar el acceso de usuario adoptando tecnologías web, móvil, IoT y cloud de forma más segura. Puede ser desplegada en local, en un dispositivo de hardware o virtual o en contenedores con Docker.

Por otro lado, IBM Security Verify Privilege Vault, anteriormente denominado IBM Security Secret Server, ofrece una solución completa de blindaje de contraseñas, auditoría y control de acceso con privilegios. Permite identificar y proteger todas las cuentas de servicio, aplicación, administrador y raíz en toda la empresa.

5.5. SecurID by RSA

SecurID [14] es una solución de autenticación, administración de acceso y control de identidad desarrollada por RSA Security, una empresa de ciberseguridad propiedad de Dell Technologies. Esta solución permite a las organizaciones proteger sus recursos y datos mediante la autenticación de usuarios a través de un sistema de doble factor o multifactor, en el que se combinan contraseñas y tokens generados por un dispositivo. Además, SecurID permite la gestión centralizada de identidades y el control de acceso a recursos tanto en entornos locales como en la nube.

Es importante destacar que SecurID es una solución de seguridad que utiliza diferentes tecnologías, incluyendo RSA, pero no es un sistema criptográfico en sí mismo como el cifrado RSA, que resuelve el problema de enviar mensajes codificados sin compartir previamente el código con el destinatario.

5.6. OKTA

OKTA [10] es una empresa estadounidense de administración de acceso e identidad, fundada en San Francisco en el año 2009. Desde entonces, se ha posicionado como líder en gestión de acceso e identidades a nivel mundial.

La empresa proporciona software en la nube que ayuda a las empresas a administrar y asegurar la autenticación de usuarios en aplicaciones y servicios web de sitios web. El objetivo principal de OKTA es ofrecer una capa de seguridad y control alrededor de la identidad digital, permitiendo a las empresas administrar y asegurar el acceso de usuarios y proveedores a las herramientas corporativas, ubicadas tanto on-premise como en cloud.

OKTA es una solución de gestión de acceso e identidad digital, que permite a las empresas controlar y gestionar el acceso de usuarios y proveedores a las herramientas corporativas tanto en la nube como en las instalaciones locales (on-premise).

El sistema OKTA se basa en la nube, lo que significa que todas las funcionalidades se ofrecen de forma remota. OKTA está diseñado para simplificar y homogeneizar el proceso de gestión de acceso a sistemas informáticos, aplicaciones y páginas web, ofreciendo una capa de seguridad y control alrededor de la identidad digital. Además, OKTA es una solución comercial para manejar la autenticación en sitios web, lo que permite a las empresas asegurarse de que los visitantes puedan comprobar su identidad.

6. Ciclo de vida de la autenticación de segundo factor.

El ciclo de vida en caso de una autenticación de segundo factor está bien definido y afecta directamente al funcionamiento [8].

6.1. Configuración y Vinculación

En esta primera etapa del ciclo, se concreta qué método de autenticación se va a adoptar para el entorno empresarial que se adapte mejor a las necesidades. Una vez escogido, implementado y configurado todo el ecosistema, hay que registrar o vincular la cuenta del usuario al sistema de autenticación de segundo factor.

Al menos se debe vincular un autenticador a un usuario, se recomienda que se vinculen dos [4], ya que eso puede mitigar el riesgo en el caso de pérdida, extravío o robo de uno de los dispositivos o autenticadores. Por ejemplo, vincular un dispositivo físico de generación de códigos de un solo uso (figura 3) y un teléfono móvil.

6.2. Administración

Una vez que el entorno está listo y configurado con los usuarios vinculados correctamente para el uso de la autenticación, siempre existe necesidades que van surgiendo a medida que pasa el tiempo. Puede existir también la necesidad de ajustar parámetros o políticas que se actualicen para cumplir nuevas normas que se deben reflejar en el sistema.

En esta etapa se incluye las modificaciones o actualizaciones ya sean de los sistemas o de las políticas de la propia empresa o nuevas normas gubernamentales. También es muy importante el monitorizado de los problemas y del uso de la implementación de la autenticación de segundo factor.

Generar archivo de logs para el estudio y resolución de problemas es una de las buenas prácticas recomendadas a la hora de detectar y resolver cualquier error o problema.

6.3. Pérdida, robo, deterioro o duplicado no autorizado

Cuando el usuario ha perdido el autenticador, se lo hayan robado, se ha estropeado o tenga sospechas de que ha podido ser duplicado de alguna manera, debe reportarlo inmediatamente. Es importante que la empresa tenga una manera de contactar con el administrador para revocar o desvincular el autenticador de la configuración del usuario.

Al no tener el autenticador disponible, el entorno empresarial debe estar preparado para que un usuario contacte con ellos sin necesidad de acceder a la cuenta. También debe haber unas medidas de verificación de que el usuario

que reporta es realmente un usuario válido dentro del entorno. Para confirmar esto, cuando el usuario reporta debe aportar información que se ha guardado previamente en el perfil del usuario como, por ejemplo, preguntas, código postal, dirección de email secundaria, etc.…

6.4. Expiración

Algunas veces, a la hora de vincular un autenticador se pone fecha de validez a ese autenticador ya sea por temas contractuales o políticas de seguridad de la empresa. Una vez que haya caducado o expirado el autenticador, el usuario deberá contactar con el administrador para renovar o vincular un autenticador nuevo.

6.5. Eliminación o revocación

En esta etapa el administrador deniega al usuario el acceso o la autenticación eliminando la autenticación de segundo factor y desvinculando el o los posibles autenticadores que tenga el usuario.

7. Caso práctico

Para el primer caso práctico, vamos emular un entorno empresarial en la nube con entorno Microsoft Azure. Usaremos la cuenta de estudiante de la UOC (lwu@uoc.edu) para crear una estancia nueva para crear todo el entorno.

Una vez configurado el entorno, crearemos un usuario con el servicio de directorio activo de Azure [15]. Finalmente, configuraremos las políticas de autenticación para el usuario y vinculamos la autenticación de segundo factor.

Para el segundo caso práctico, se realizará una prueba en un entorno de Keycloak que es un gestor de identidades de código abierto y lo configuraremos para el uso de usuarios sin contraseña. Para el uso sin contraseña, simularemos una llave virtual (Figura 5) en vez de una llave física.

7.1 Primer caso práctico

7.1.1. Creación del entorno empresarial.

Para empezar a crear el entorno empresarial, tenemos que acceder a Microsoft Azure con la cuenta de la UOC y crear un directorio nuevo. En nuestro caso lo llamaremos “luiswu”.

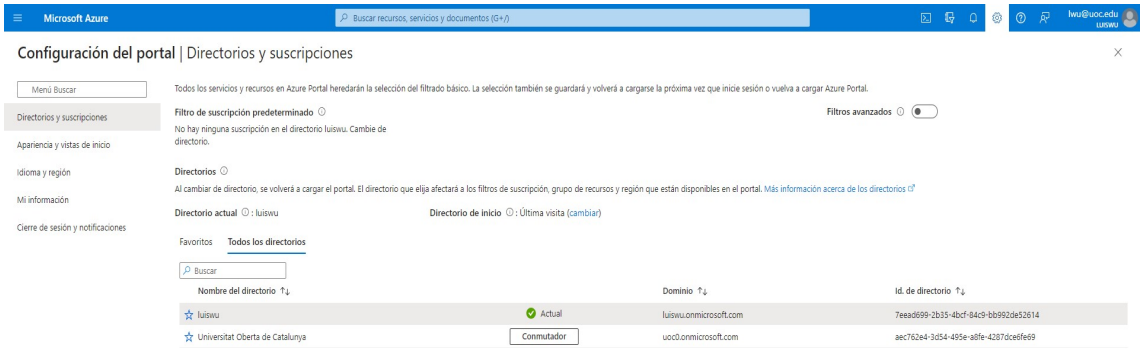

Figura 7: Configuración del portal

7.1.2. Configuración de seguridad

Una vez creado la instancia, hay que comprobar la seguridad predeterminada hay que estar activada.

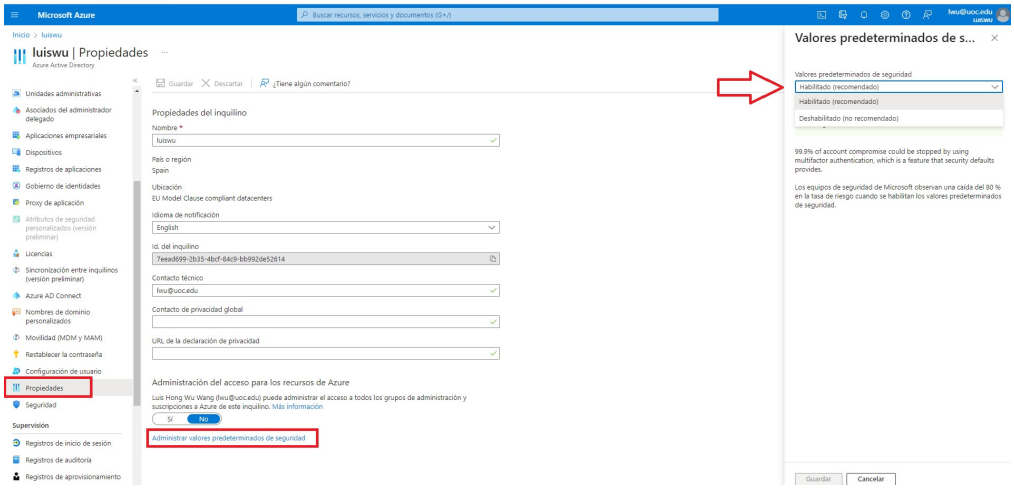

Figura 8: Configuración del portal

Con la seguridad predeterminada nos aseguramos que varias características de seguridad de Azure se aplique de manera predeterminada como es la autenticación de doble factor en los usuarios del entorno.

Sin embargo, en organizaciones donde hay muchos usuarios y departamentos se puede configurar el acceso condicional donde se puede aplicar políticas de seguridad para diferentes grupos y/o usuarios.

7.1.3. Creación de la cuenta de usuario

Una vez creado y configurado la instancia de la empresa “luiswu” con dominio “luiswu.onmicrosoft.com”, procederemos a crear un usuario en el directorio activo del entorno empresarial.

Para hacer eso es necesario entrar al servicio de directorio activo en la página principal del portal de Azure.

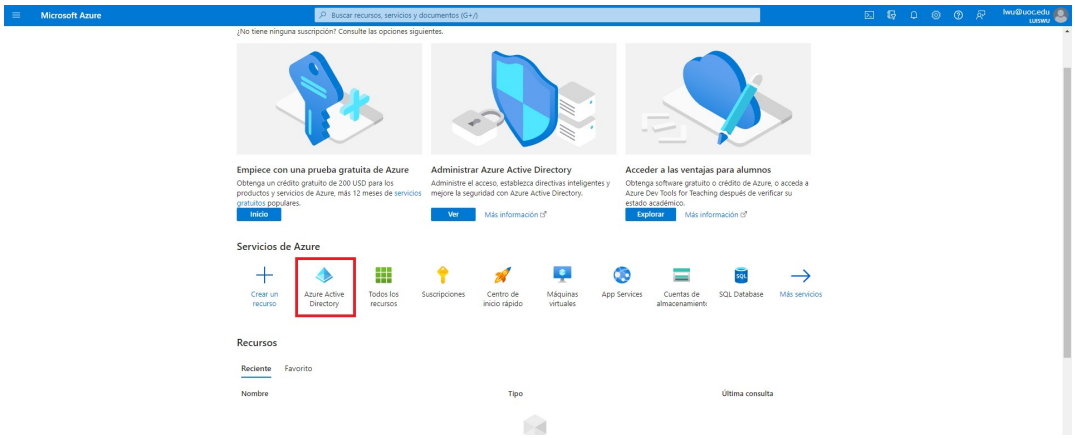

Figura 9: Panel principal de Microsoft Azure

Dentro del servicio del directorio activo, en el menú lateral en la sección de “Administrar” accedemos a la opción de “Usuarios”.

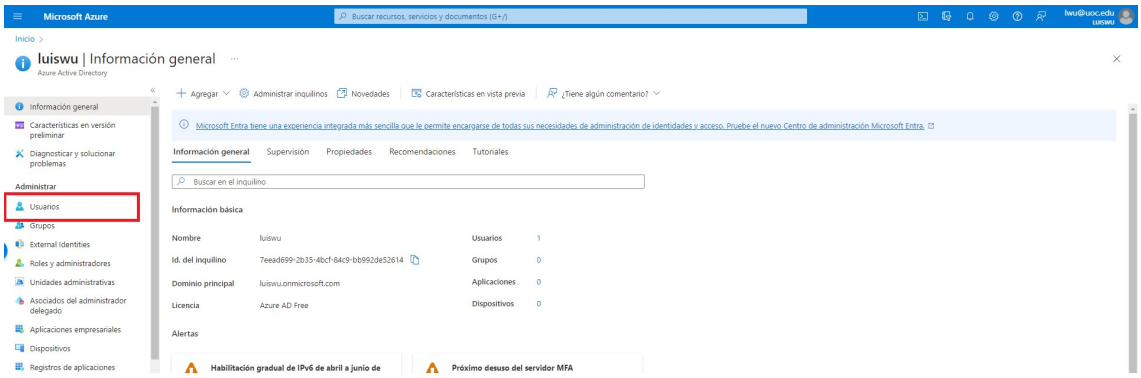

Figura 10: Página principal del servicio de Directorio activo de Azure

Una vez dentro de la administración de usuarios, tendremos la opción de crear nuevos usuarios. En la parte superior, accedemos al formulario para crear usuarios nuevos

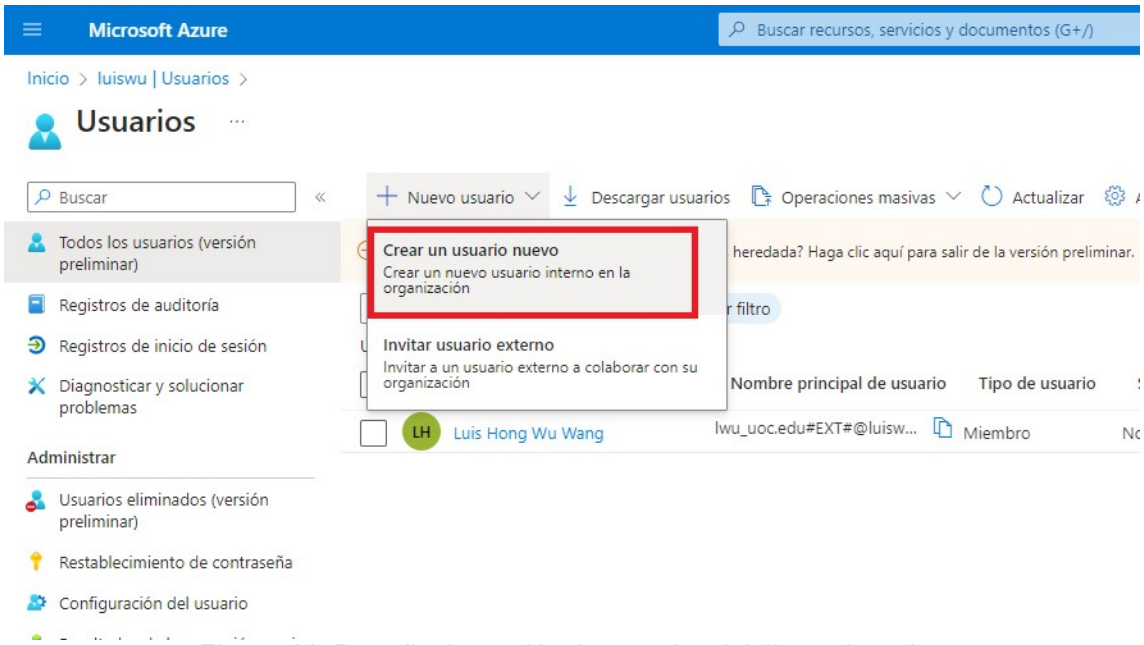

Figura 11: Pantalla de gestión de usuarios del directorio activo

En el formulario, rellenamos el nombre principal el usuario y nombre para mostrar. Luego procedemos a configurar las propiedades.

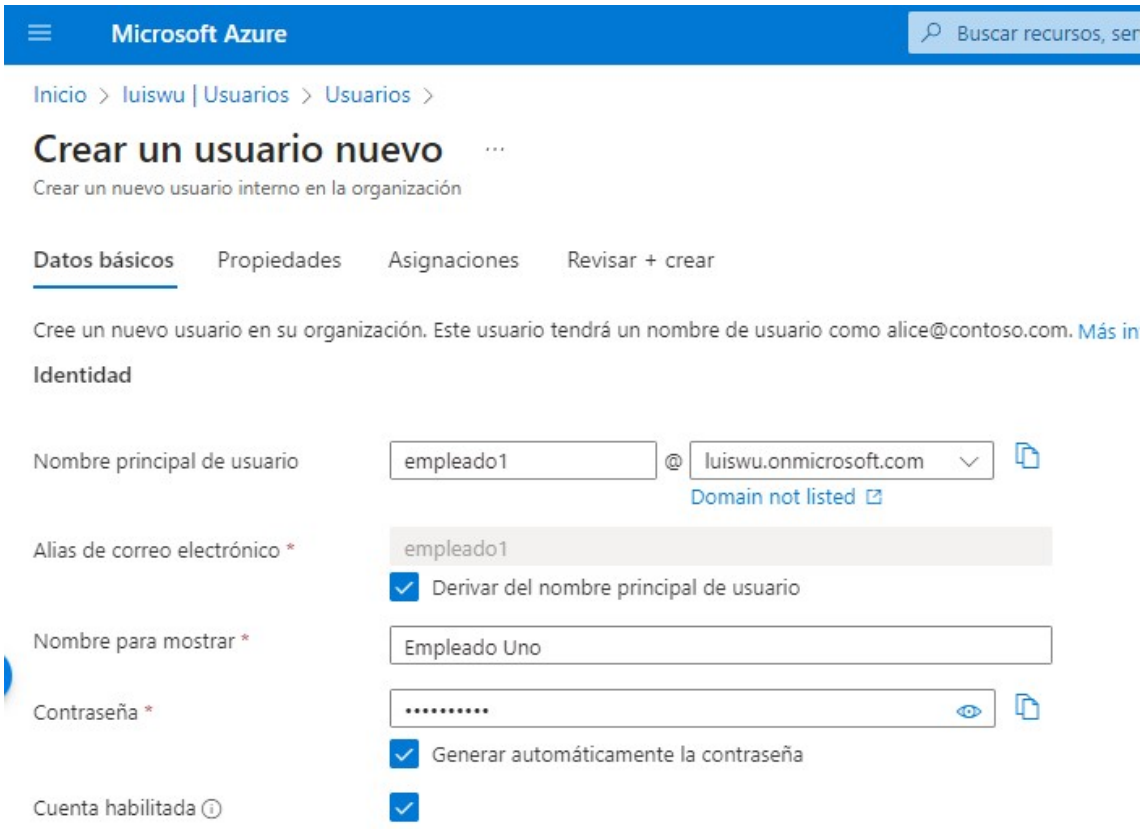

Figura 12: Formulario para crear un nuevo usuario

En la siguiente pantalla ya nos muestra un formulario más extenso donde podremos rellenar todo tipo de propiedades importante para el usuario para completar su perfil. Destacar que todas las propiedades son opcionales. En nuestro caso rellenaremos el nombre y apellidos del usuario que vamos a crear.

En el siguiente paso, podremos asignar al usuario los grupos y los roles necesarios. En este caso, no vamos a asignar nada, ya que no se han creado roles ni grupos aún en el directorio activo. Si en un futuro, se quiere añadir algún grupo se podría hacer sin problemas.

Como último paso, revisamos que toda la información de los formularios anteriores sea correcta antes de proceder a crear el usuario. Para finalizar el proceso y crear el usuario hacemos clic en “Crear”.

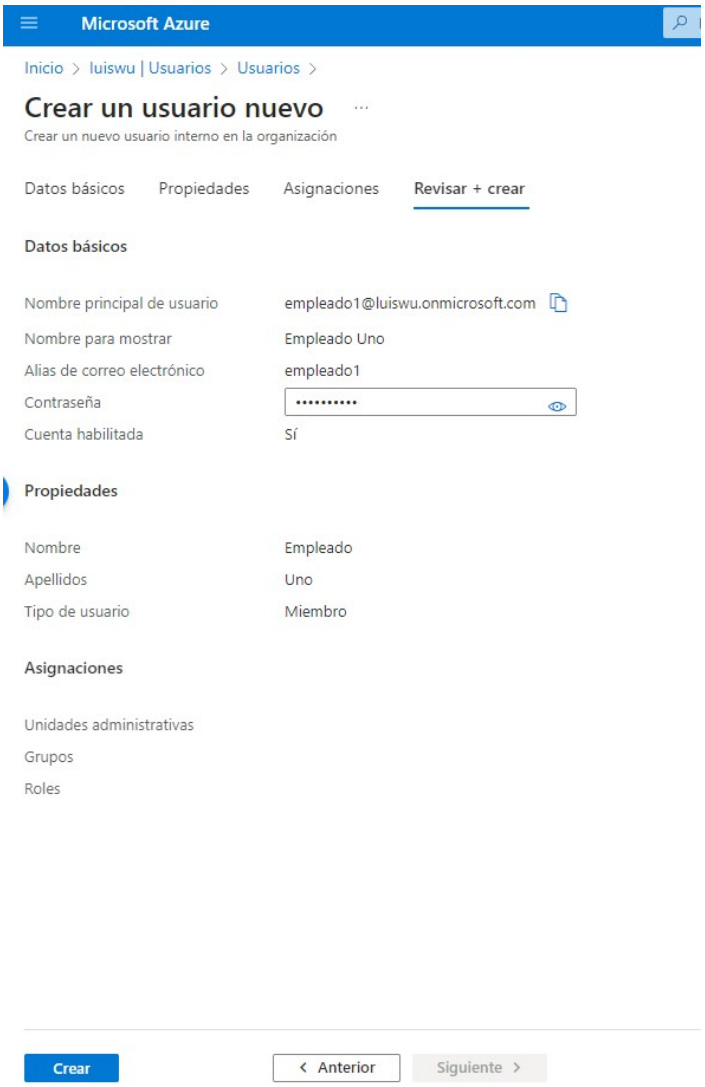

Figura 13: Resumen de las propiedades del usuario que se va a crear

Después de un par de minutos el directorio activo crea el usuario, hay que destacar que no es inmediato.

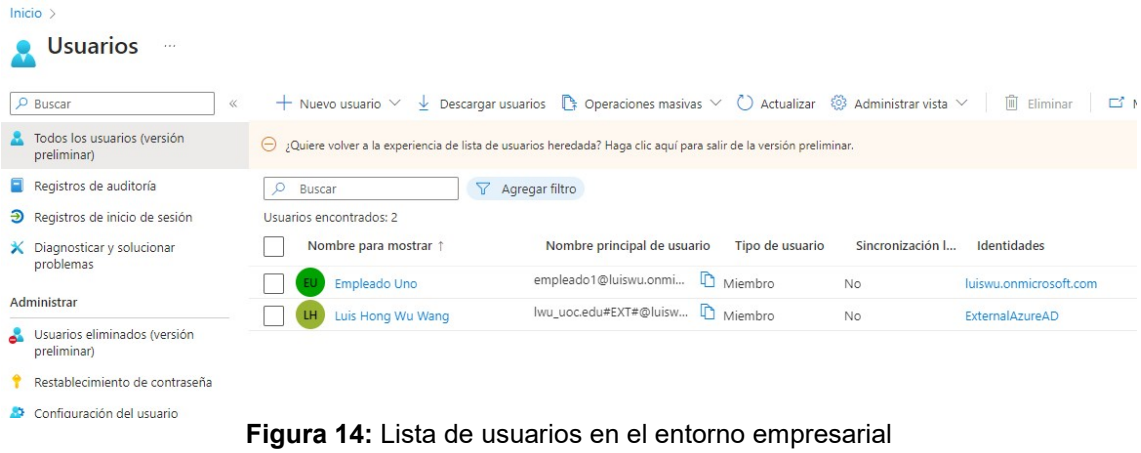

Figura 14: Lista de usuarios en el entorno empresarial

7.1.4. Vincular dispositivo con el usuario

Una vez creado el usuario y la seguridad activada en el entorno para una autenticación de segundo factor, el usuario debe registrar su dispositvo con la cuenta de empleado que se ha creado.

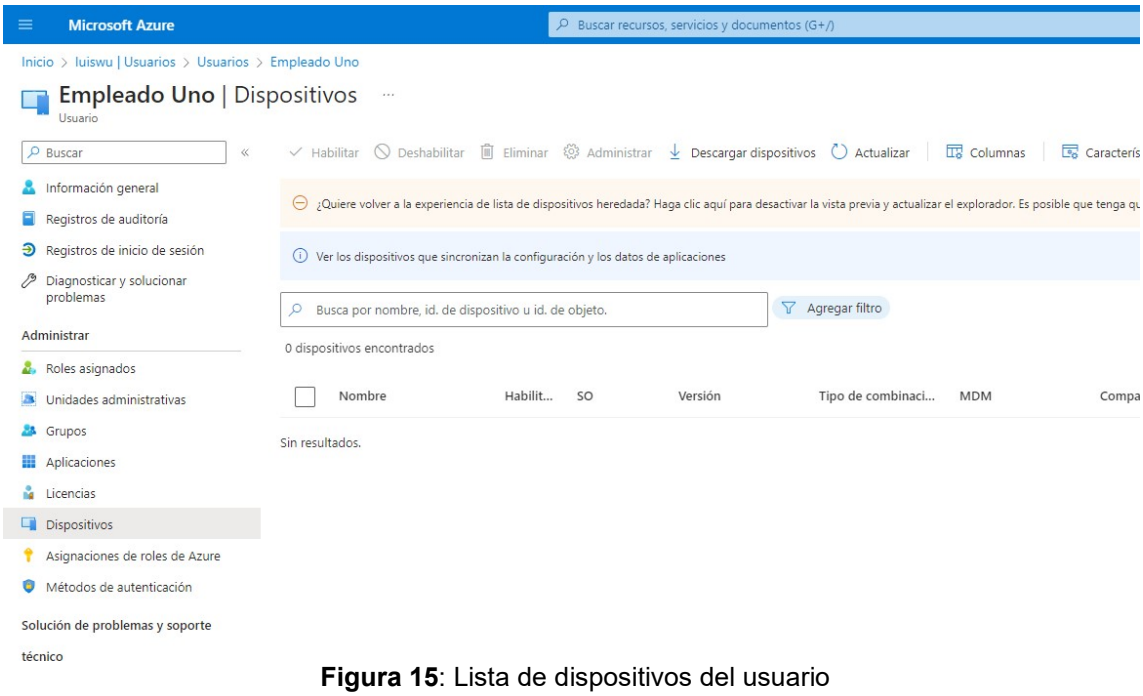

Figura 15: Lista de dispositivos del usuario

Como podemos ver en la figura anterior, el usuario “Empleado Uno”, no tiene dispositvos registrados aún. Para empezar el proceso, el usuario debe inciar sesión con la cuenta y seguir con el proceso.

Antes de todo le restablecemos la contraseña para que pueda activar la cuenta y luego en la primera sesión deberá cambiar esa contraseña por una más segura.

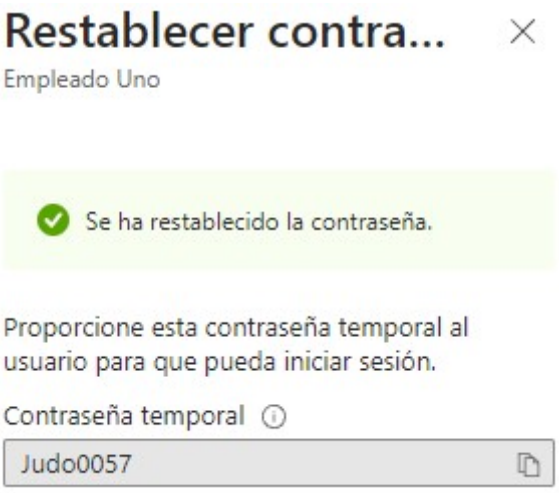

Figura 16: Contraseña inicial del usuario creado

Para iniciar sesión, deberemos ir a la página de inicio de sesión de Office 365, https://login.microsoftonline.com.

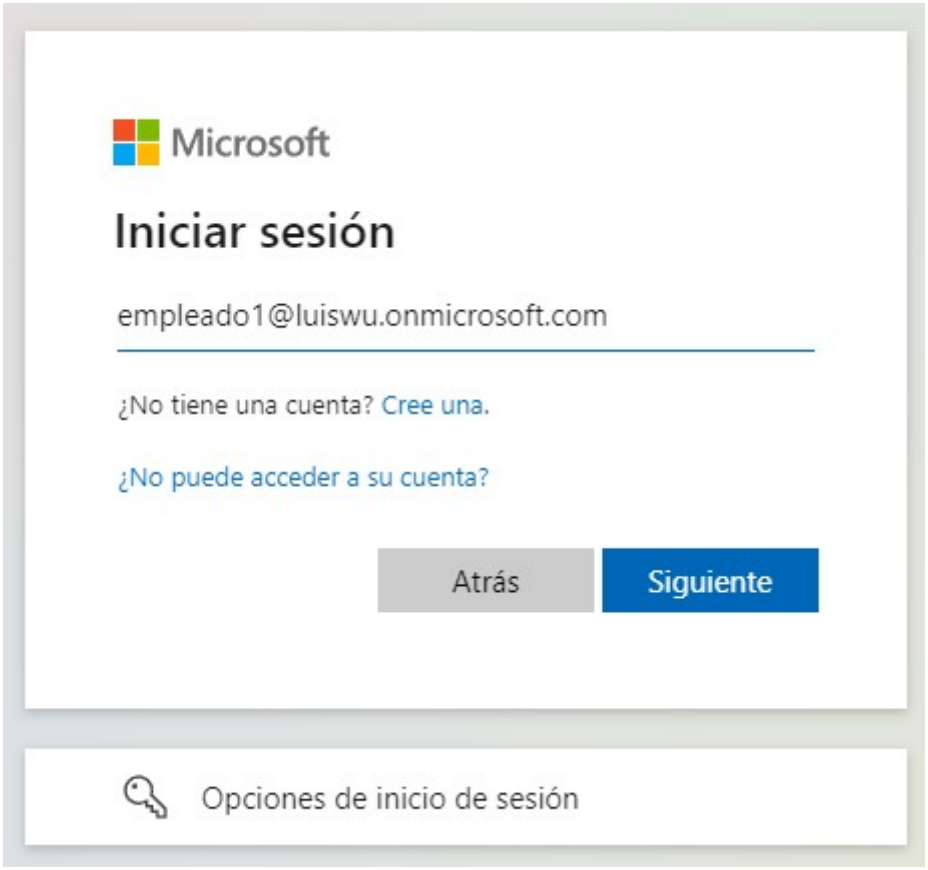

Figura 17: Pantalla de inicio de sesión en Office 365

Introducimos la cuenta empleado1@luiswu.onmicrosoft.com con la contraseña proporcionada. Ahora el sistema nos pide cambiar la contraseña por una contraseña nueva y que cumpla los requisitos de las políticas de contraseña del entorno empresarial.

Una vez cambiado la contraseña, al ser la primera vez que accede al sistema debe cumplir los requisitos del entorno para poder acceder.

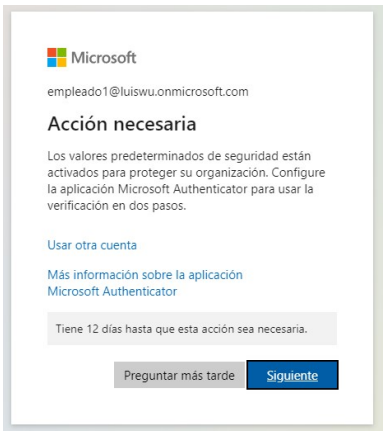

Figura 18: Mensaje de acción de seguridad necesaria

Aunque el usuario tiene 14 días para poder cumplir con los requisitos, en nuestro caso vamos a proceder a configurar la seguridad de la autenticación de doble factor. Haciendo clic en “Siguiente” iniciamos el proceso de vinculación.

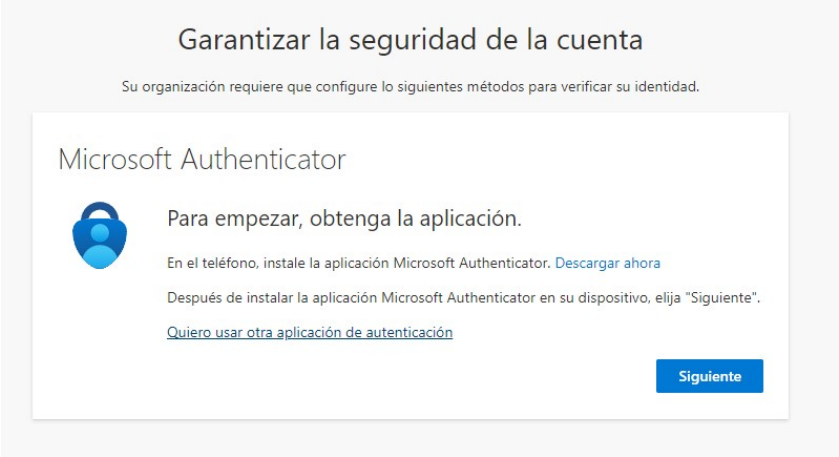

Figura 19: Mensaje de instrucción de Microsoft Authenticator

En nuestro entorno empresarial, ya se ha configurado la autenticación de segundo factor con “Microsoft Authenticator” que el usuario deberá instalar en su dispositivo móvil.

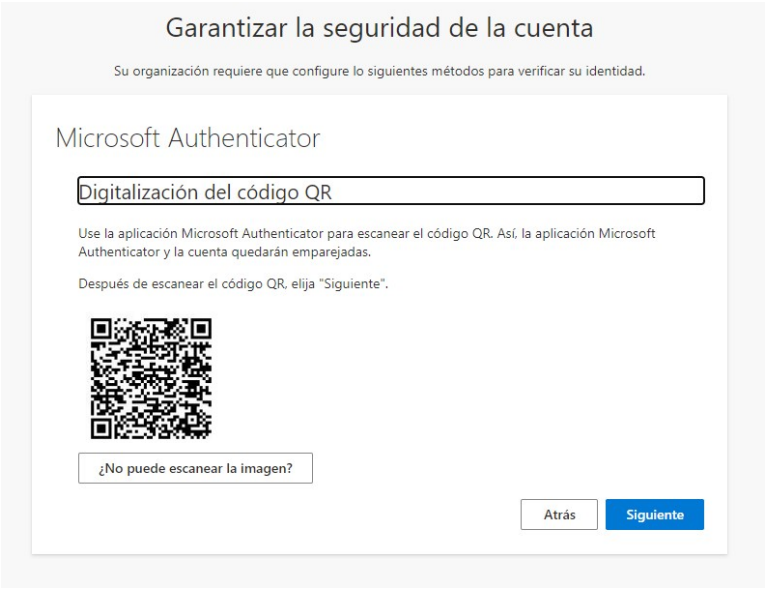

Figura 20: Código QR para vincular el dispositivo

La manera de vincular el dispositivo con la cuenta es mediante un código QR, donde el empleado o usuario debe escanear desde la aplicación. Dentro de la aplicación para añadir una cuenta ya nos deja la opción de escanear un código QR.

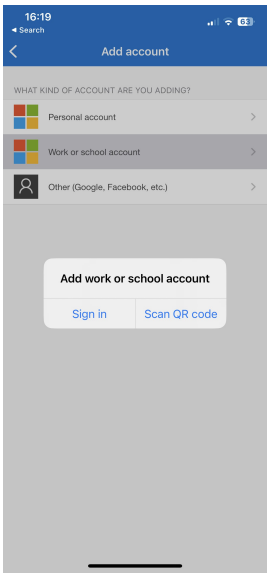

Figura 21: Añadir cuenta en la aplicación de Microsoft Authenticator

Escaneada con éxito el código QR, se añadirá automáticamente la cuenta en la aplicación "Microsoft Authenticator". Acto seguido para verificar el funcionamiento te envía una notificación push para poder finalizar el proceso.

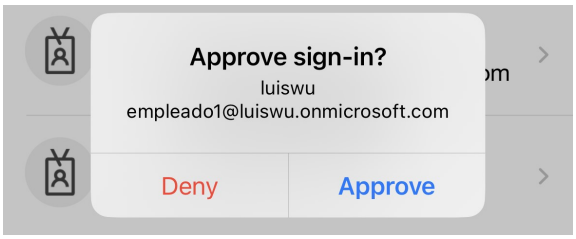

Figura 22: Notificación push para aprobar el inicio de sesión

Una vez que el usuario apruebe el inicio de sesión, entonces finalizará el proceso.

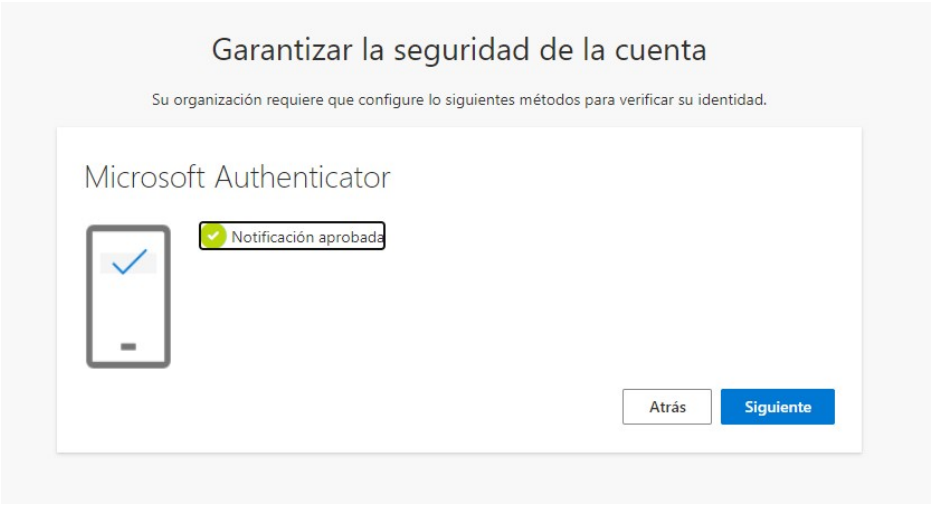

Figura 23: Notificación push aprobada por el usuario

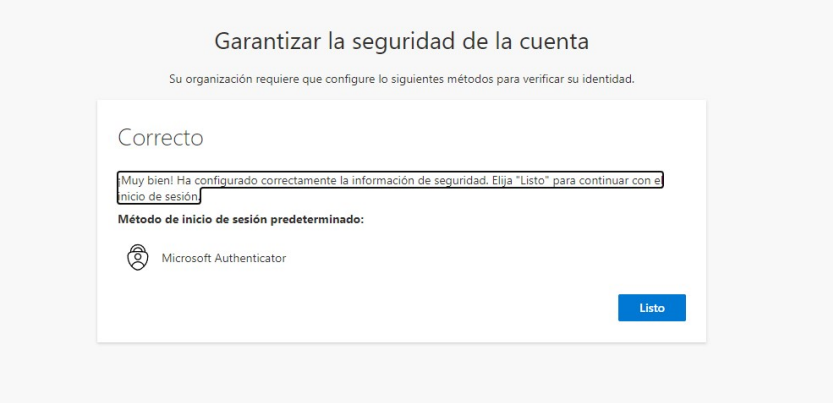

Figura 24: Vinculación del dispositivo correcta

7.1.5. Inicios de sesión

Una vez configurado con éxito el dispositivo, a partir de ahora cada vez que el usuario inicie sesión (si no la mantiene abierta) le pedirá la autenticación de segundo factor.

Si el usuario va a usar si cuenta en el mismo dispositivo durante un largo período de tiempo puede mantener la sesión iniciada para reducir el número de veces que tiene que iniciar sesión.

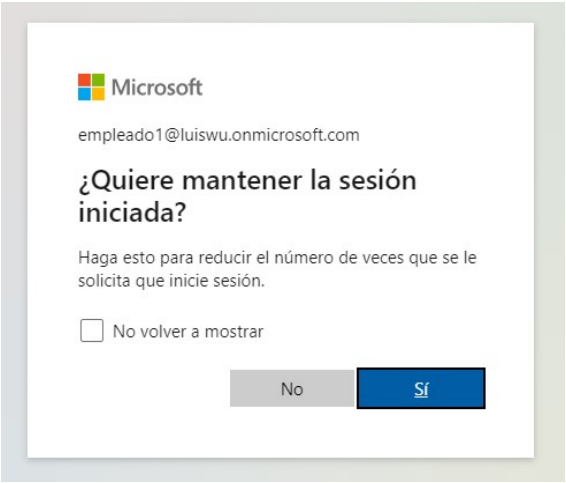

Figura 25: Mantener la sesión iniciada

Sin embargo, cada vez que el sistema detecte un dispositivo nuevo en el que quiere iniciar sesión le pedirá por seguridad la autenticación de segundo factor.

7.1.6. Extravío o sustitución de dispositivo

Uno de los mayores problemas de la autenticación de doble factor es cuando perdemos el dispositivo con que realizamos la autenticación. Sobre todo, aquellos métodos que requieren un dispositivo físico externo al sistema.

En nuestro caso, al utilizar la aplicación Microsoft Autheticator, el usuario se ha registrado su cuenta con la aplicación en su dispositivo. Entonces, en el caso que ese dispositivo haya sido robado, extraviado o estropeado se tendrá que volver a registrar a un nuevo dispositivo.

Para revocar el acceso y el uso de ese dispositivo si ha sido robado o puede haber estado comprometido, tendremos que hacer a través del perfil del usuario en el Azure AD Cloud.

Primero de todo buscamos al usuario en cuestión.

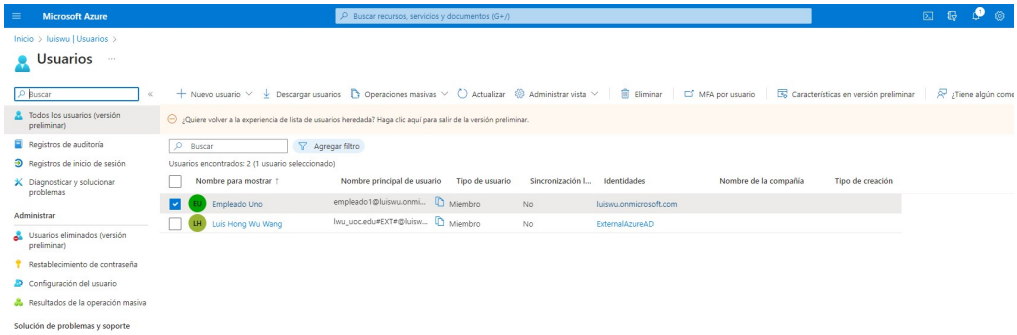

Figura 26: Lista de usuarios en el directorio activo

Dentro de la configuración del usuario podremos encontrar la configuración de los métodos de autenticación para el usuario en cuestión.

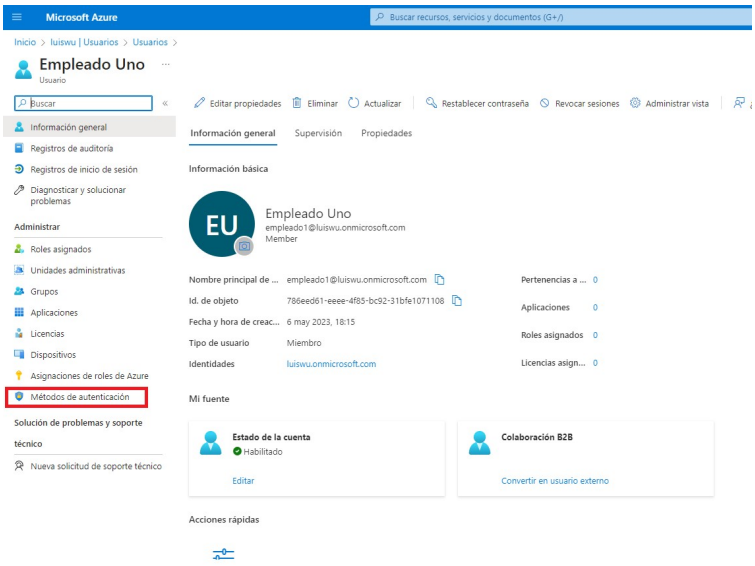

Figura 27: Perfil usuario en Directorio activo

Dentro de la configuración de métodos de autenticación, podemos forzar al usuario a requerir volver a registrar la autenticación multifactor o revocar sesiones de autenticación multifactor.

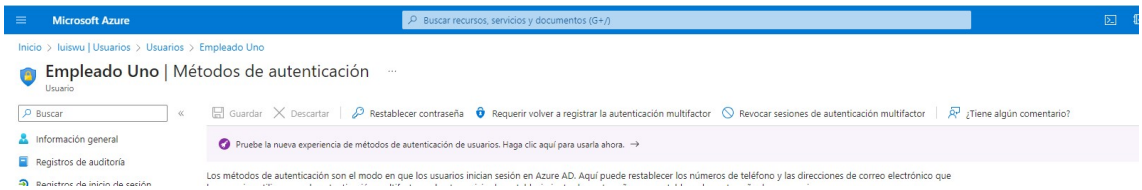

Figura 28: Configuración de métodos de autenticación

La primera opción sirve para que el usuario pueda volver a registrar otro dispositivo para la autenticación de segundo factor en el caso de que haya extraviado su dispositivo actual. Una vez requiramos a al usuario volver a registrar un dispositivo sería como volver a iniciar el proceso de vinculación de un dispositivo.

En cambio, la segunda es para revocar todas las sesiones que haya iniciado el usuario y tenga guardada y así obligar al usuario a tener que volver a iniciar sesión en todos los dispositivos y así requerir el uso de la autenticación de segundo factor.

7.1.7. Eliminar/Deshabilitar de usuario

Cuando un empleado se va de la empresa, se deberá revocar el acceso total al entorno empresarial. Dependiendo de las políticas de retención se podría deshabilitar el usuario en vez de eliminarlo directamente.

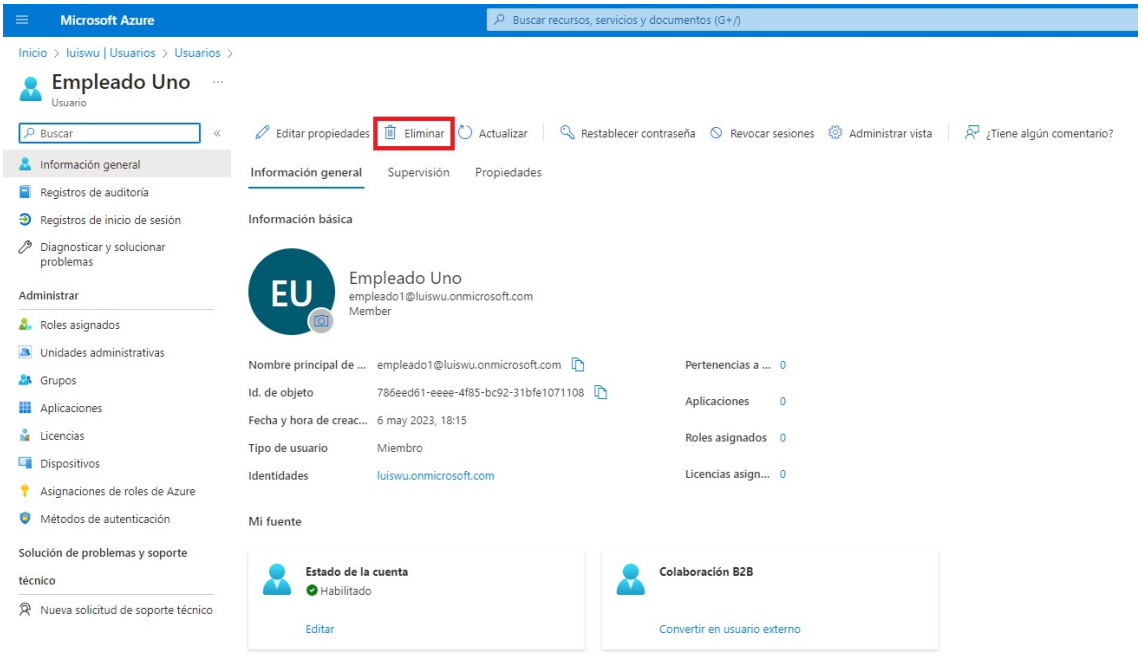

Figura 29: Eliminar un usuario

Eliminando al usuario haría que toda su información se eliminase también. Algo menos agresivo sería deshabilitarlo, en el caso de que no se quiera perder la información y tener guardado el registro de ese usuario o empleado.

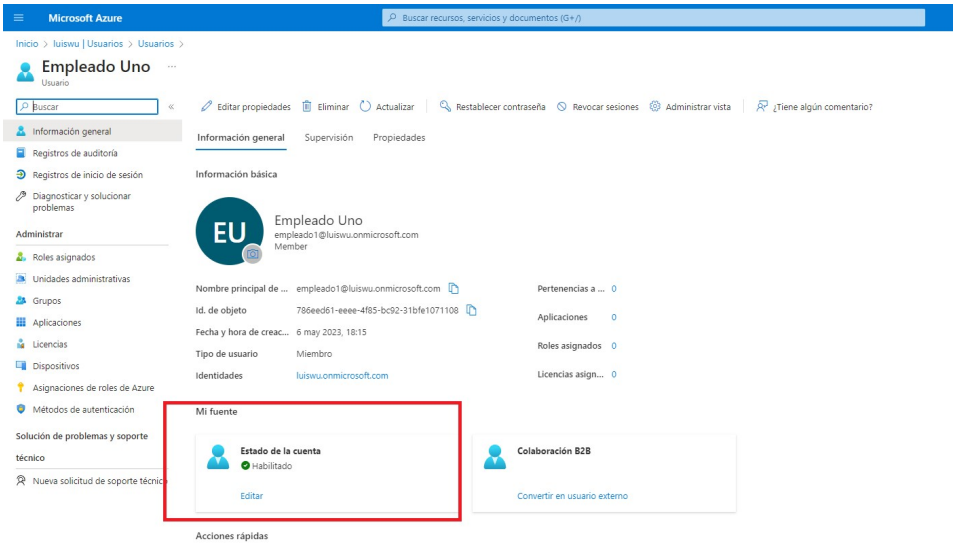

Figura 30: Deshabilitar un usuario

Para hacer eso, simplemente editamos el estado de la cuenta a una cuenta deshabilitada para poder denegar el inicio de sesión.

7.2. Segundo caso práctico

En este segundo caso práctico, intentaremos desplegar un contenedor Docker [16] con una imagen de Keycloak [17] y configurarlo para el uso de usuarios con autenticación sin contraseña a través de una llave USB (simulada virtualmente).

7.2.1. Configuración entorno

Antes de empezar a configurar el entorno, tendremos que instalar todo lo necesario. Primero hay que instalar Docker para poder crear contenedores aislados donde desplegar el Keycloak.

Una instalado el Docker, montamos un contenedor con la imagen de Keycloak con el siguiente comando:

```
docker run -p 8080:8080 -e KEYCLOAK_ADMIN=admin -e
KEYCLOAK_ADMIN_PASSWORD=admin quay.io/keycloak/keycloak:21.1.1 start-dev
```

Una vez descargada la imagen y montando el contenedor tendremos ya listo el servidor en el puerto 8080.

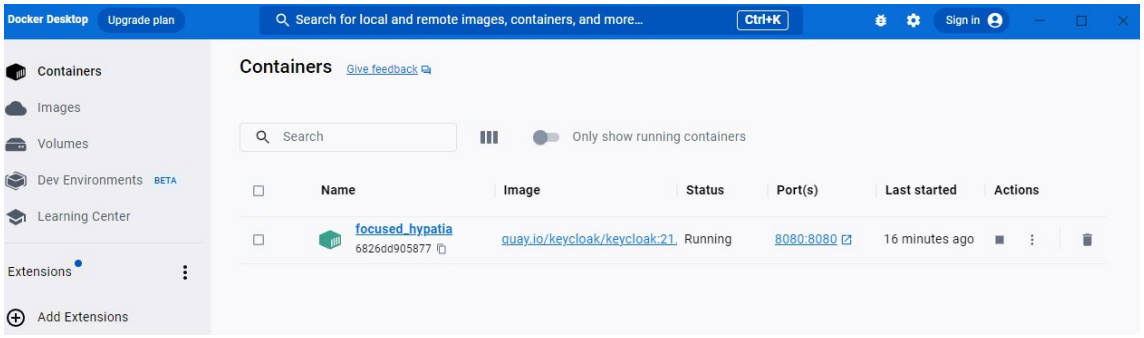

Figura 31: Docker, lista de contenedores creados

Entramos a la dirección localhost:8080 en el navegador y ya podremos entrar en la configuración de Keycloak con las credenciales de administrador definidas en el comando de instalación.

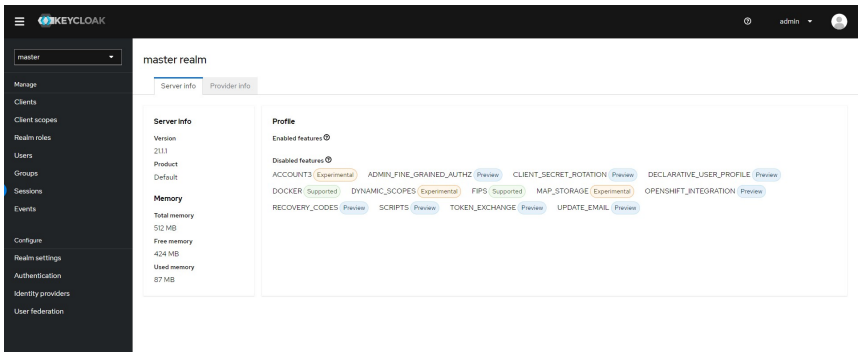

Figura 32: Panel de configuración de Keycloack

Una vez dentro del panel de configuración de Keycloak, crearemos un nuevo dominio o reino (realm). Lo llamaremos “myrealm”. Una vez creado el reino tenemos que cambiar el flujo de autenticación y las políticas del entorno.

Para el flujo de autenticación desde navegador, modificamos e introducimos la autenticación sin contraseña y quedaría de la siguiente manera:

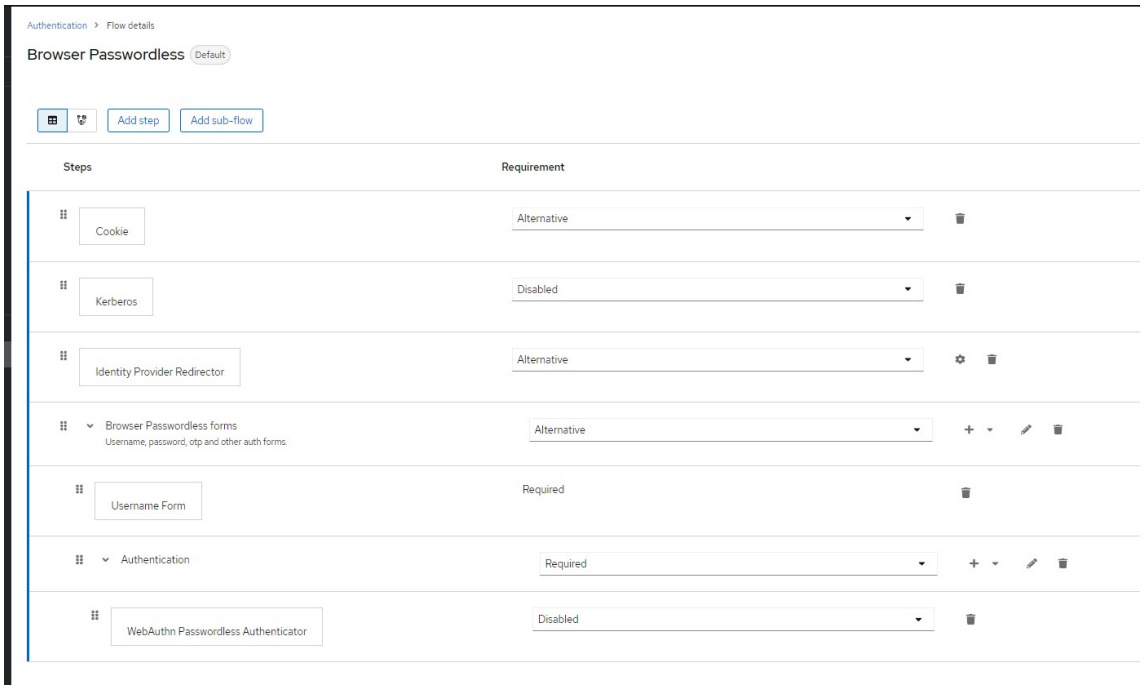

Figura 33: Flujo de inicio de sesión

Permitimos el registro de nuevos usuarios en nuestro entorno.

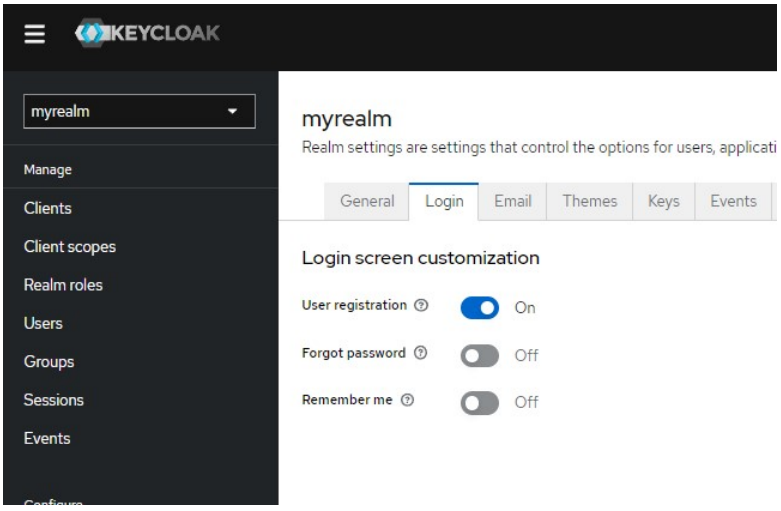

Figura 34: Activación de posibilidad de registro de usuario

Con esto ya tendremos listo el entorno, y usamos una aplicación para comprobar si todo ha ido bien. Accediendo a la aplicación de prueba que te ofrece Keycloak podemos ver que responde perfectamente.

https://www.keycloak.org/app/#url=http://localhost:8080&realm=myrealm&client=myclient

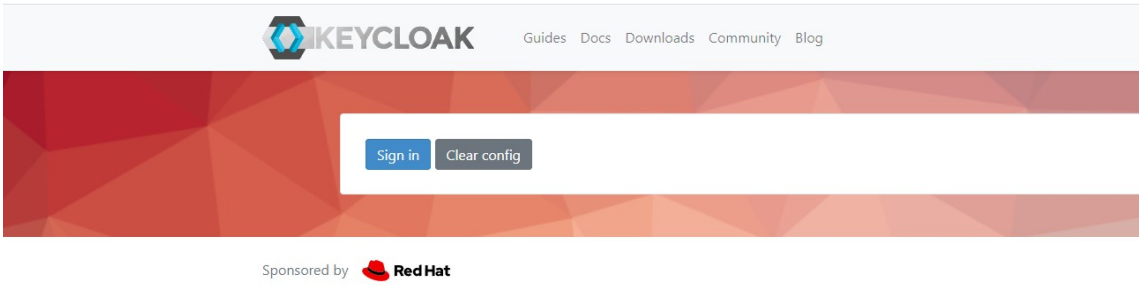

Figura 35: Aplicación de prueba de Keycloack

7.2.2. Creación de llave virtual

Para el uso de una autenticación sin contraseña por llave usb, el usuario debería tener una llave física única. Para esta prueba, se va a simular una llave a través de las herramientas de desarrollo de Google Chrome.

Abrimos la consolola de desarrollo de Chrome y accediendo al menú a través del icono de los tres puntitos, seleccionamos “More tools” y luego en la lista “WebAuthn”.

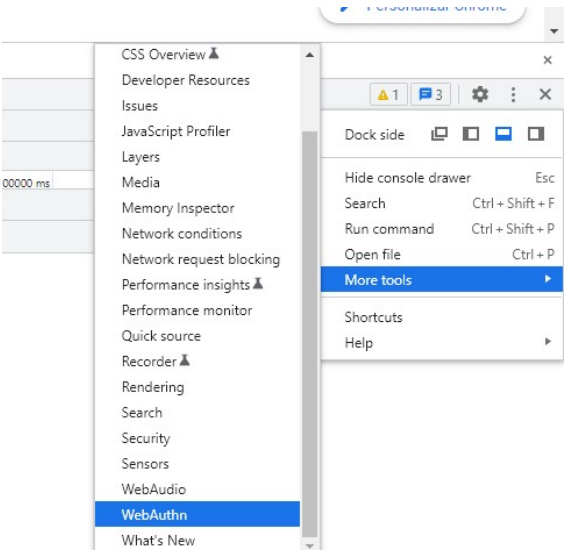

Figura 36: Herramienta de desarrolladores de Google Chrome

Una vez activado la opción, podremos crear una llave virtual para poder usarla en nuestra autenticación.

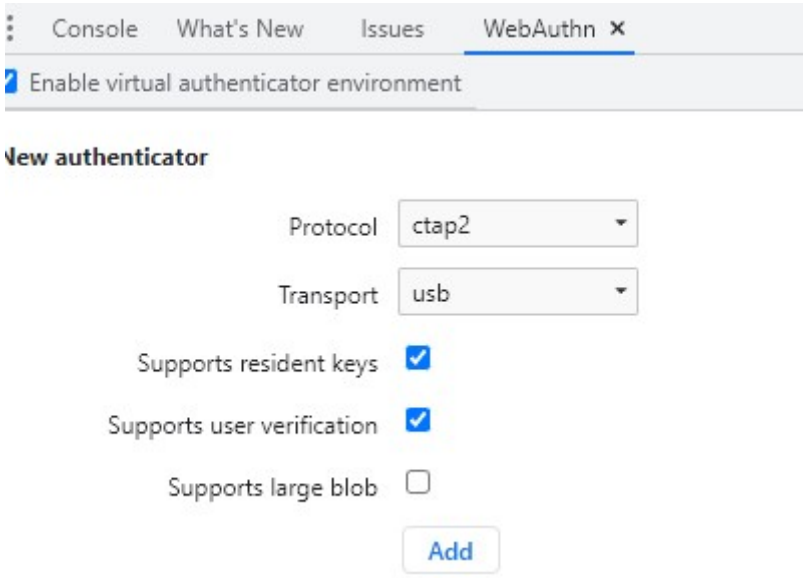

Figura 37: Creación de llave virtual en Google Chrome

Seleccionamos las dos primeras opciones y hacemos clic en “Add” para añadir nuestra nueva llave virtual.

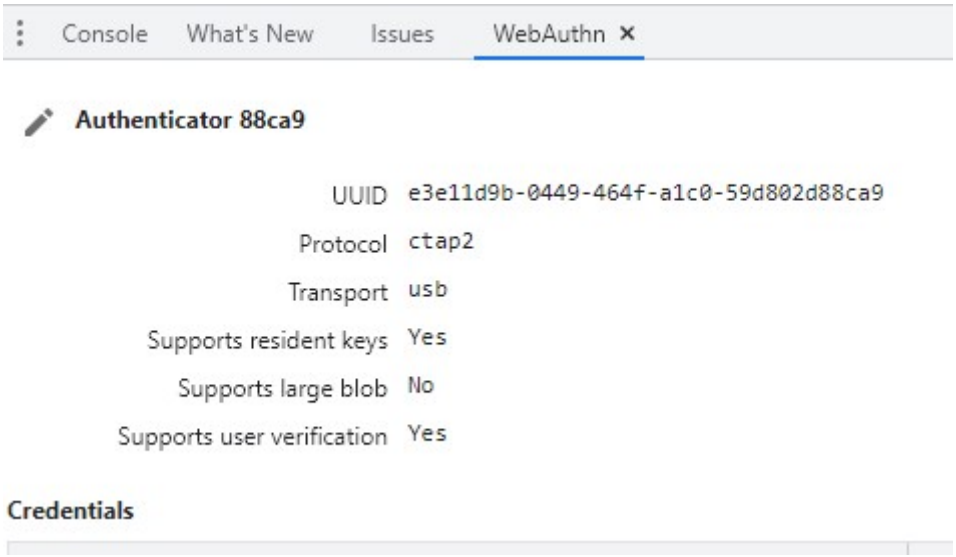

Figura 38: Detalle de la llave virtual

7.2.3. Creación de usuario y registro de llave

Ahora que tenemos la llave virtual lista, procedemos a registrarnos y crear el usuario y vincular la llave a nuestro usuario.

Accedemos a la página autenticación que nos habilita la opción de crear un usuario. Normalemente, en un entorno empresarial el administrador es el que crearía el usuario.

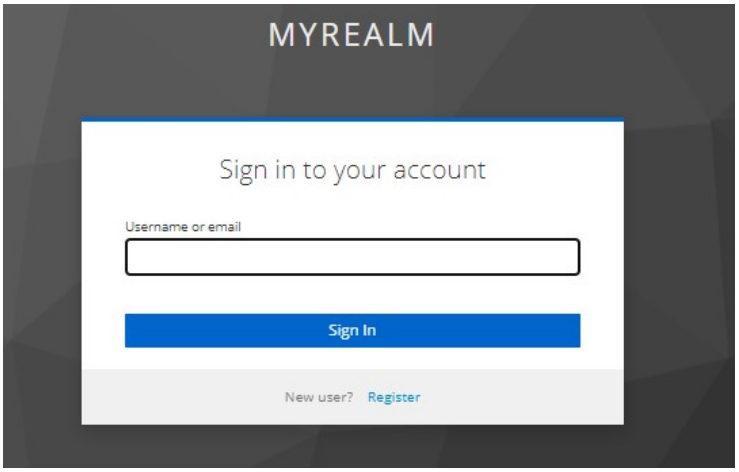

Figura 39: Página de inicio de sesión de la aplicación de pueba

Seleccionando la opción “Register” en la parte inferior del cuadro, accedemos al formulario de registro.

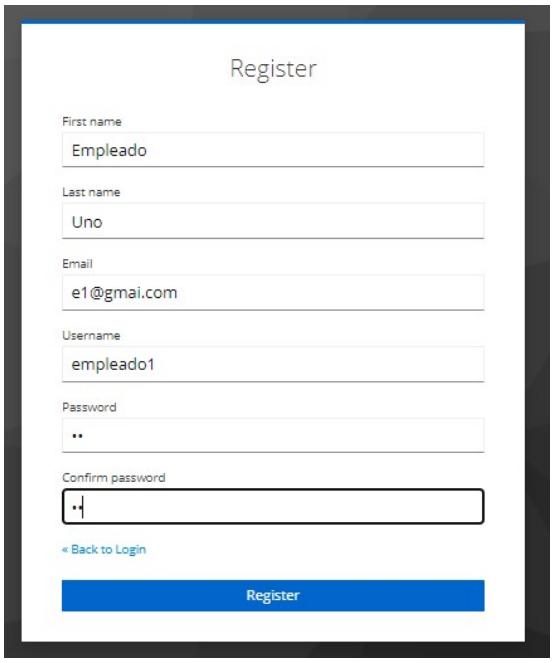

Figura 40: Formulario de registro de usuarios

Rellenamos el formulario y registramos el usuario.

El siguiente paso que nos pide el sistema es registrar la llave para vincularla con el usuario creado.

Figura 41: Registro de una llave de seguridad

Con la consola abierta y la llave virtual activa, estamos simulando que tenemos la llave conectada en nuestro ordenador. Seleccionamos registrar y automáticamente nos detecta la interfaz de la llave virtual.

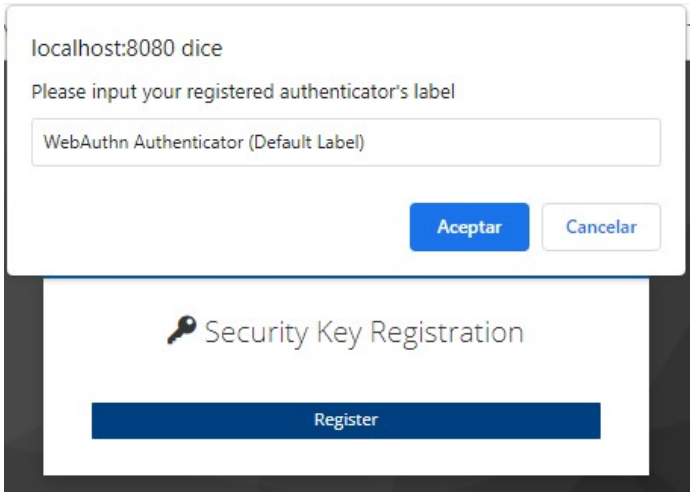

Figura 42: Detección de la llave virtual

Aceptamos, y ya tendremos el usuario credo con nuestra llave.

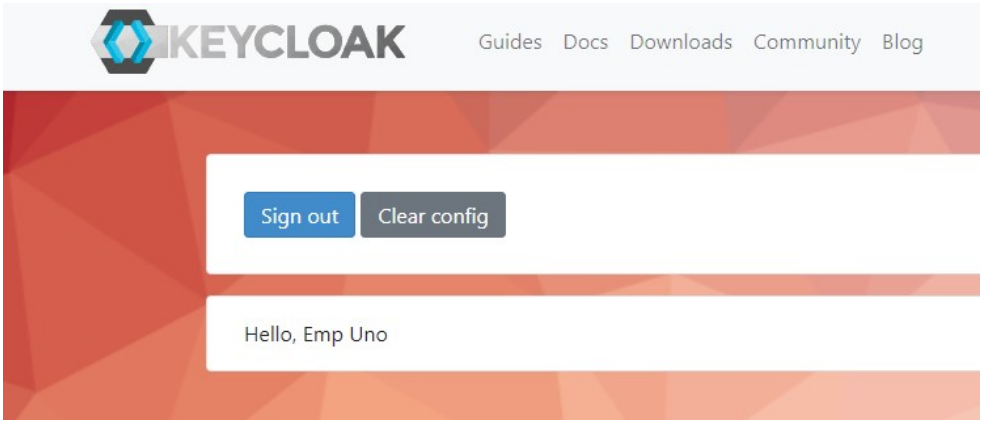

Figura 43: Página de inicio cuando el usuario ha entrado al sistema

7.2.4. Proceso de autenticación

En este punto que el usuario existe y ya tiene la llave registrada, vamos a intentar a hacer el proceso de autenticación sin contraseña usando la llave virtual.

Primero de todo, se tendrá que indicar al formulario de inicio de sesión el nombre de usuario. En nuestro caso es “empleado1”.

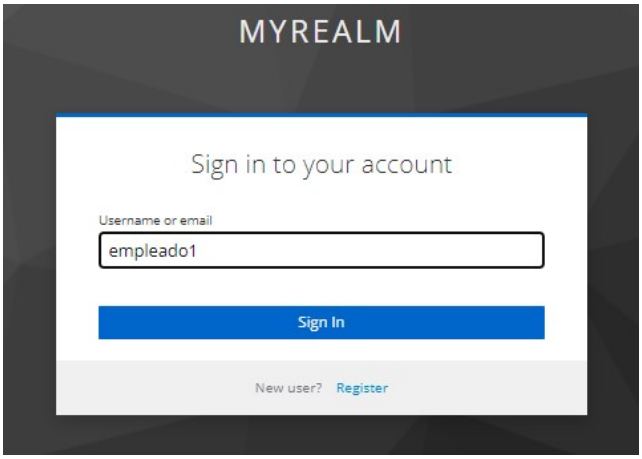

Figura 44: Iniciando sesión con el usuario

Como en la configuración del sistema hemos habilitado la autenticación sin contraseña, ahora en vez de poner la contraseña nos pide que introduzcamos la llave.

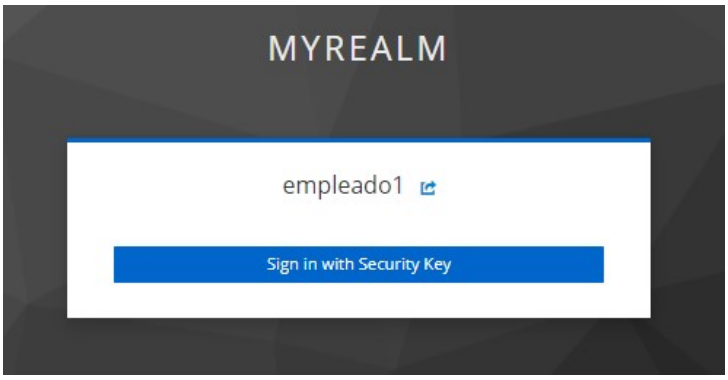

Figura 45: Inicio de sesión con la llave de seguridad

Con la ventana de la llave virtual abierta, seleccionamos la opción de iniciar sesión con la llave de seguridad y automáticamente entramos al sistema sin necesidad de usar ninguna contraseña.

7.2.5. Pérdida o extravío de llave.

En el caso de que el usuario pierda la llave, se estropee o haya sido sustraído, inmediatamente tiene que avisar al administrador para revocar el uso de esa llave y poder registrar una nueva.

Para eso, el administrador tiene que entrar al panel de control de Keycloak y entrar en la configuración del usuario.

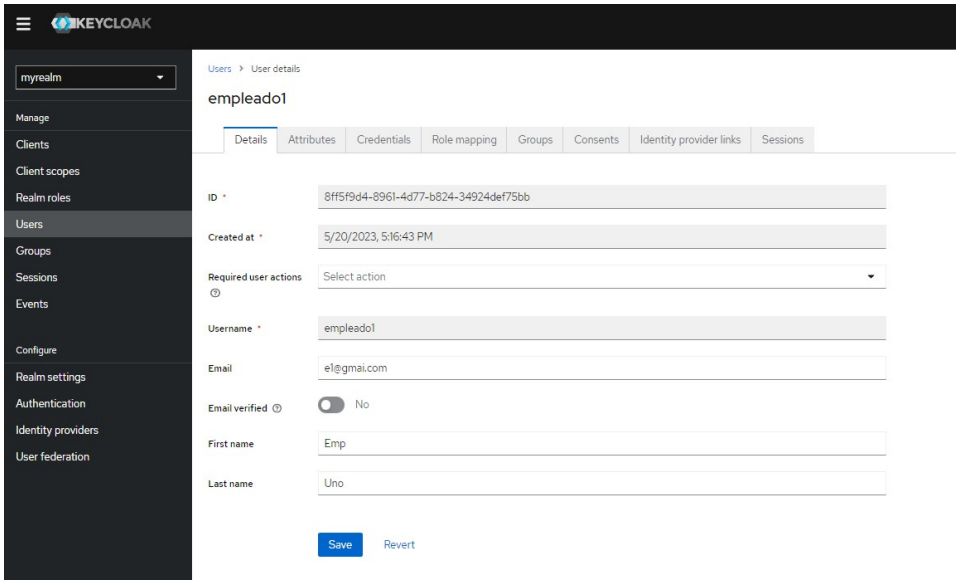

Figura 46:

En la pestaña de “Credentials”, tendremos que borrar la llave que autentica al usuario y así que pueda registrar una nueva.

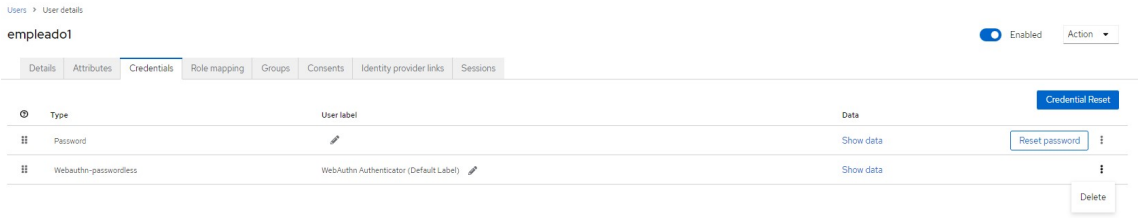

Figura 47:

Para que el usuario pueda registrar una nueva llave, accediendo a la opción de “Credential Reset” podremos enviar al usuario un email para que inicie el proceso de registro de una nueva llave.

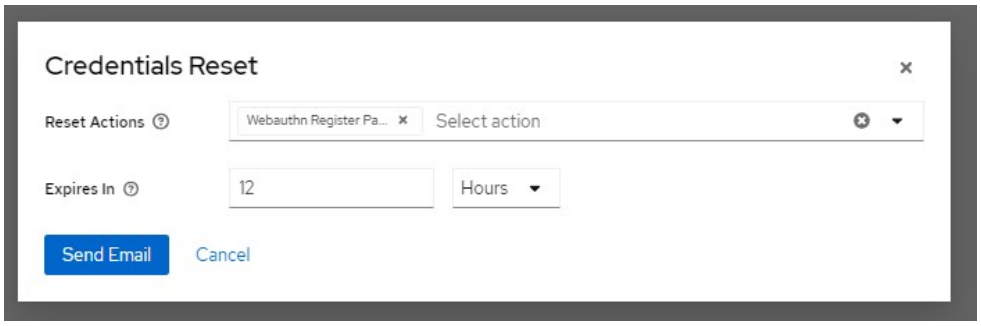

Figura 48:

7.2.5. Borrado o desactivación del usuario.

Para finalizar, si el empleado o usuario abandona el entorno se tendrá que desactivar o borrar el usuario. Comentado anteriormente, dependiendo de las políticas de retención de la empresa se hará una cosa o la otra.

Para desactivar el usuario, en el perfil del usuario hay una opción para desactivarlo.

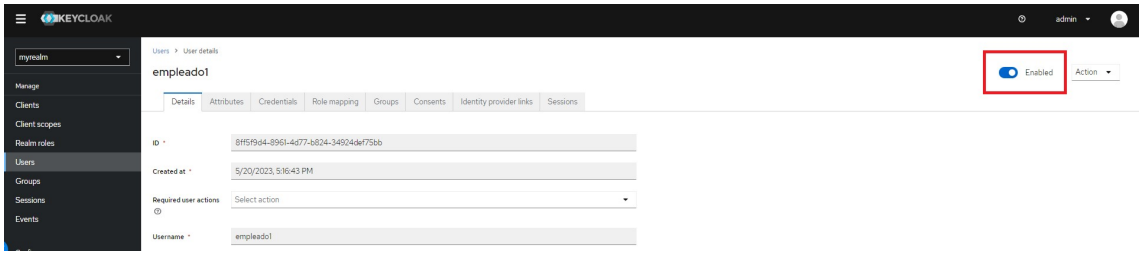

Figura 49: Desactivar un usuario

Con esta opción, se guardan todos los datos del usuario, pero éste ya no podrá acceder al sistema. En el caso de que el usuario volviese, volviendo a activar al usuario podría entrar en el sistema con su llave de siempre sin necesidad de pasar por todo el proceso de registro.

En cambio, para eliminar el usuario por completo, deberemos ir a la lista de usuarios y seleccionar eliminar de manera manual.

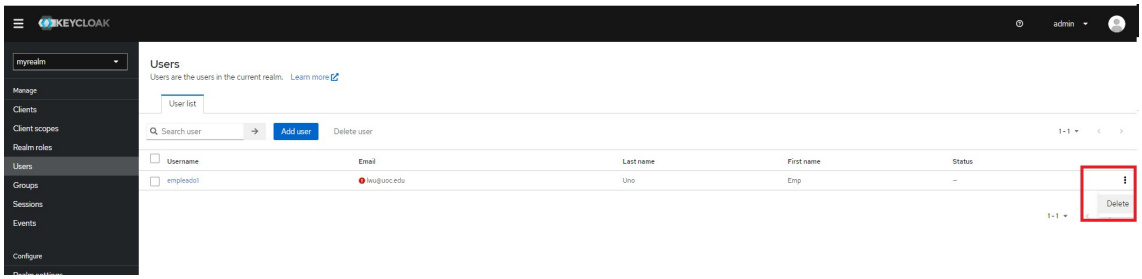

Figura 50: Eliminar un usuario

7.3. Unión de los casos prácticos

Una vez que tenemos nuestros entornos de los casos anteriores configurados, podemos unirlos de manea que nuestro directorio activo provea usuarios federados al gestor de identidades Keycloak.

Con este caso, si la empresa dispone sus usuarios en un directorio activo, podrá federar los usuarios en el gestor de identidades sin necesidad de crear los usuarios de nuevo en éste.

Para conectar los dos entornos, primero tendremos que indicar a Keycloak que habrá un proveedor de identidades federado externo. Para hacer eso, vamos a nuestra consola de administración en Keycloak y seleccionamos “Identity Providers”.

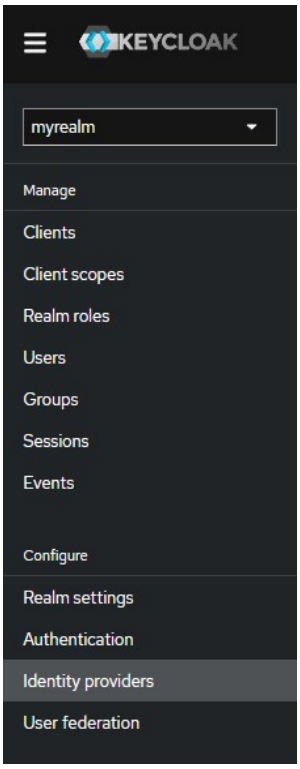

Figura 51: Menú lateral de Keycloak

Dentro de la sección de proveedor de identidades añadimos uno nuevo seleccionando la opción de “OpenID Connect v1.0”.

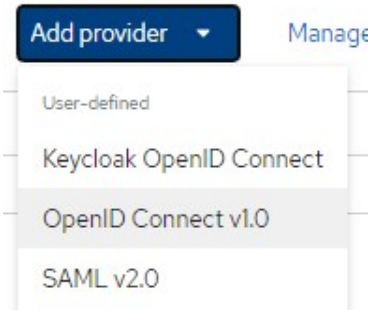

Figura 52: Añadir nuevo proveedor de identidades

Ahora, se abrirá un formulario para crear la conexión al proveedor de identidades. Rellenamos un Alias y copiamos la URL de redirección que nos da.

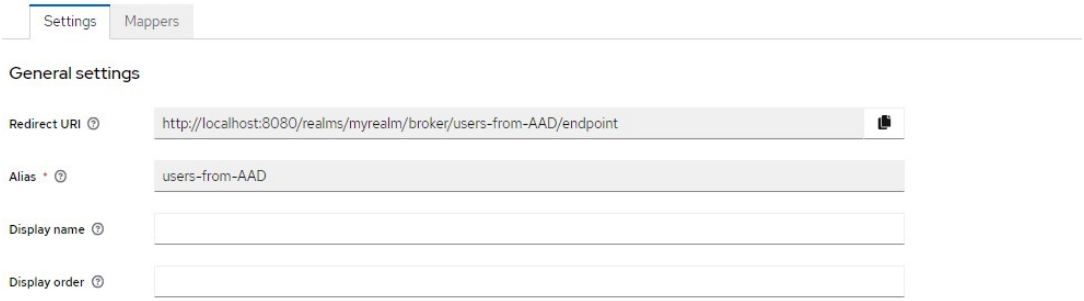

Figura 53: Configuración del nuevo proveedor

Con la “Redirect URI” copiada, en Azure AD tendremos que registrar una nueva aplicación con la que vamos a conectar nuestro directorio activo.

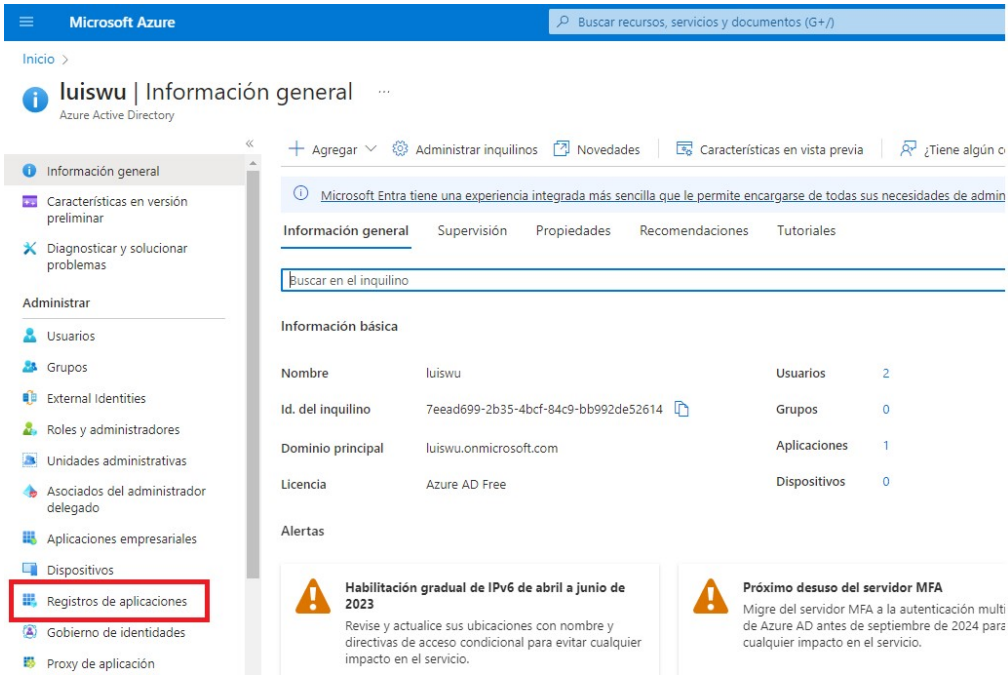

Figura 54: Panel de control de Azure AD

Ya dentro de la sección de registro de aplicaciones del portal de Azure, seleccionamos en la parte superior “+Nuevo Registro” para añadir una nueva aplicación. Entonces, se nos abre un formulario para crear la aplicación de conexión. Le indicamos un nombre descriptivo y en la URI de redirección pegamos el valor obtenido desde Keycloack (Redirect URI), seleccionado “Web” en el desplegable.

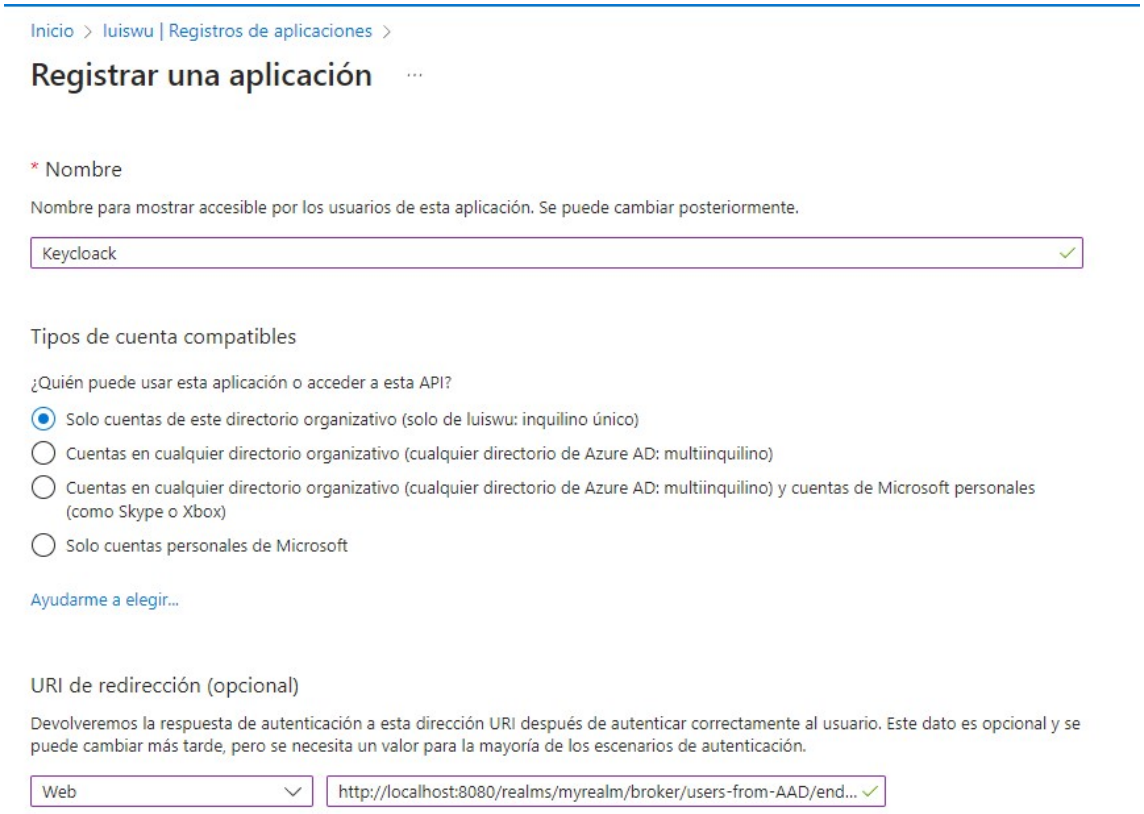

Figura 55: Registro de una nueva aplicación

Una vez creada la aplicación, ya nos aparece en el listado de aplicaciones registradas.

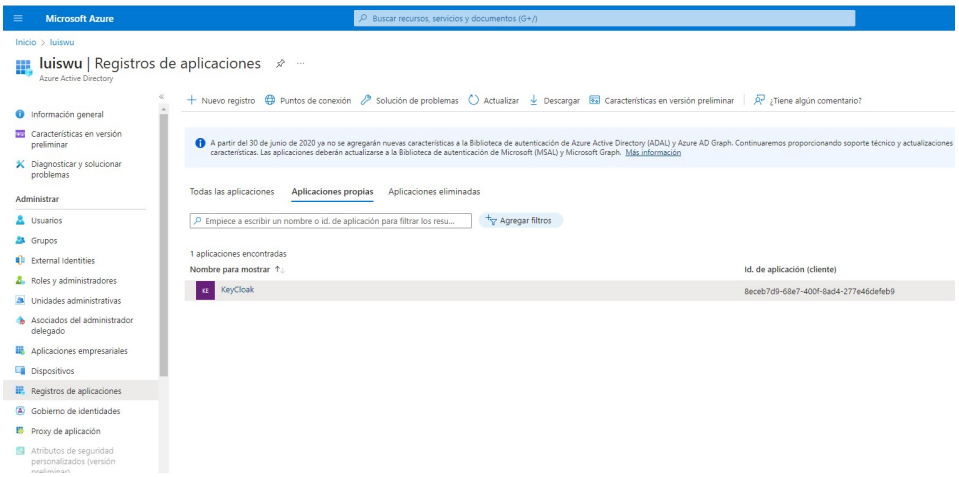

Figura 56: Listado de aplicaciones en Azure AD

En este punto, con la aplicación registrada en Azure, entramos en la aplicación y miramos los detalles y los puntos de conexión.

Figura 57: Detalle de la aplicación registrada

Lo que realmente nos interesa es el id de la aplicación, el punto de conexión y el token. Con esa información que introduciremos en Keycloak. Pero antes de volver a Keycloak, necesitaremos crear un secreto o código de conexión para que Keycloak y Azure AD puedan comunicarse. Para eso, dentro de la aplicación registrada seleccionamos “Certificados y secretos”.

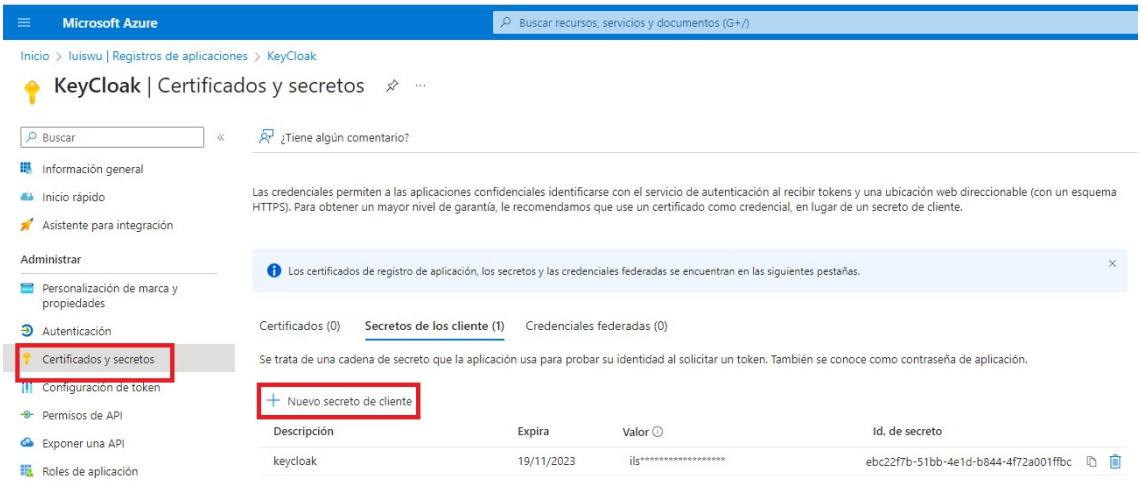

Figura 58: Creación de secretos en Azure AD

Creamos un nuevo secreto con validez de 6 meses (predeterminado) y guardaremos el valor para indicarlo en Keycloak.

Volviendo a la consola de administración de Keycloak, donde habíamos dejado a medias la creación del gestor de indentidades, introduciremos los valores que hemos obtenido a la hora de registrar la aplicación en Azure.

Para empezar, hay que especificar el punto de conexión y el token obtenidos en la aplicación de Azure (Figura 57).

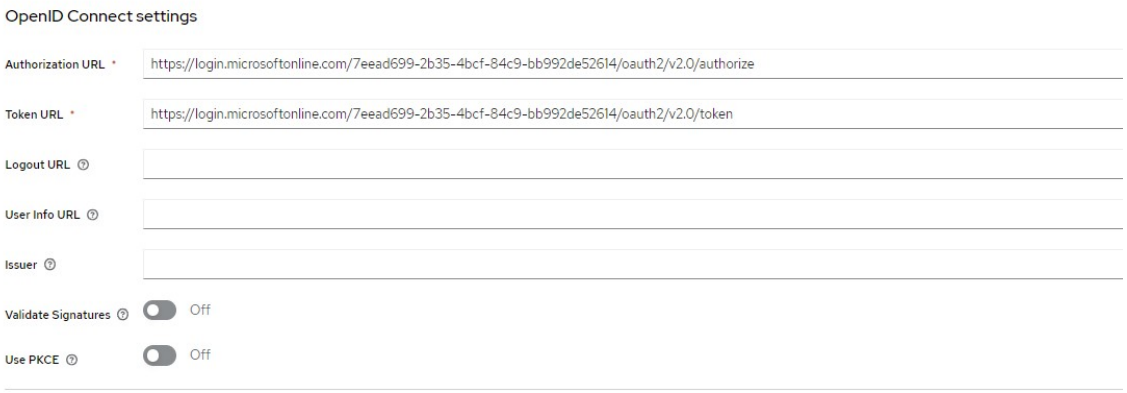

Figura 59: Formulario de creación de un proveedor de identidades

Como se puede ver, el resto de los valores los dejamos en blanco ya que no son estrictamente necesarios.

Ahora hace falta indicar el id del cliente y el secreto que hemos generado en Azure.

Figura 60: Detalle del id del cliente y el secreto

Y para finalizar indicamos qué flujo queremos usar y también marcamos la opción de que los emails de los usuarios han sido ya verificados y son de confianza.

Figura 61: Configuración avanzada del proveedor de identidades

Guardamos la configuración y debería estar listo. Ahora, entrando a la pantalla de inicio de sesión, encontraremos una nueva opción para iniciar sesión:

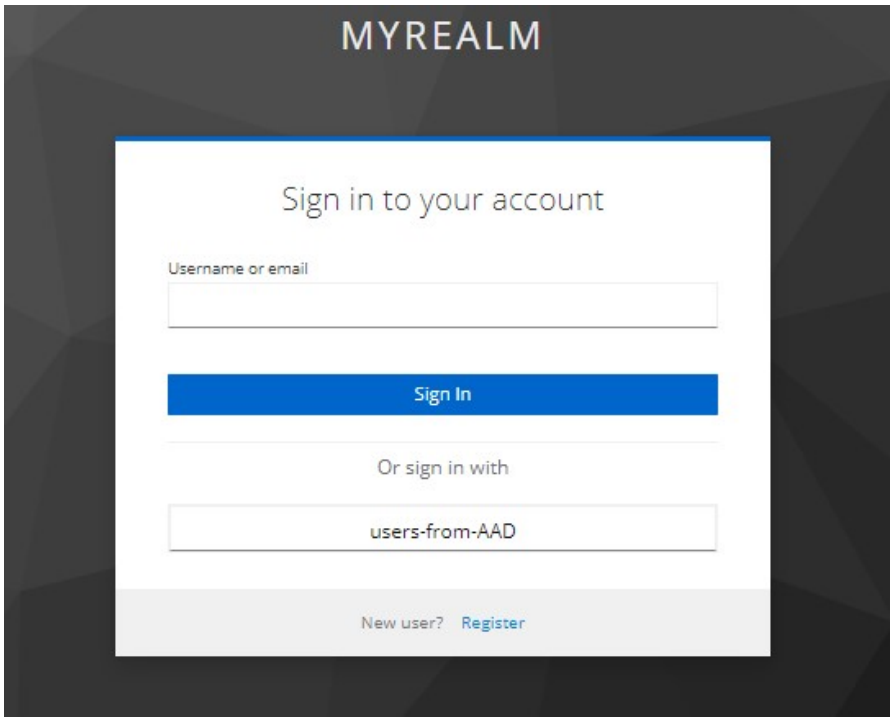

Figura 62: Nuevo formulario de inicio de sesión

Ahora podremos iniciar sesión con los usuarios federados desde Azure AD, al seleccionar la nueva opción de “users-from-AAD”, la aplicación nos redirigirá al inicio de sesión de Azure.

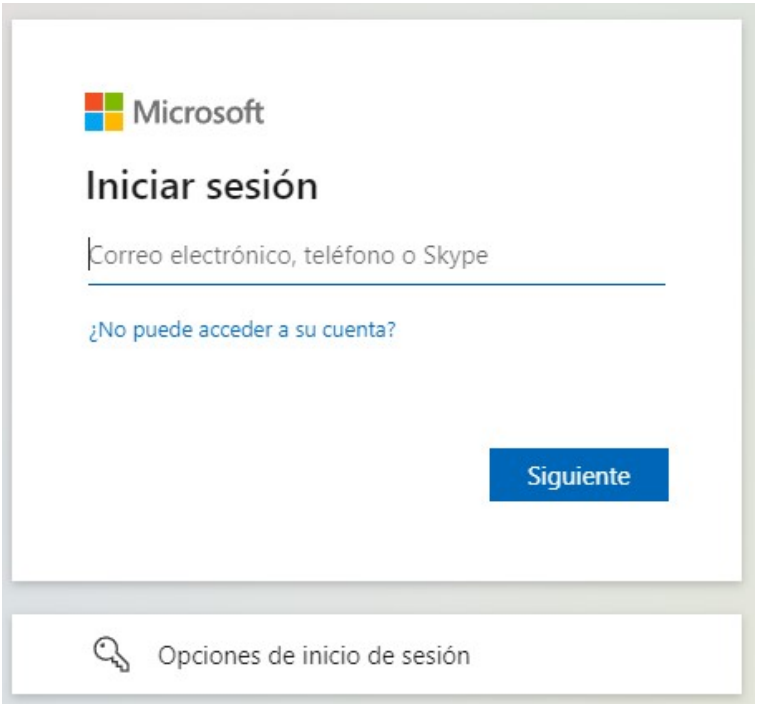

Figura 63: Inicio de sesión en Office 365

Iniciando sesión con nuestras credenciales de “empleado1”, accedemos de forma correcta al perfil con los datos que han venido de Azure AD.

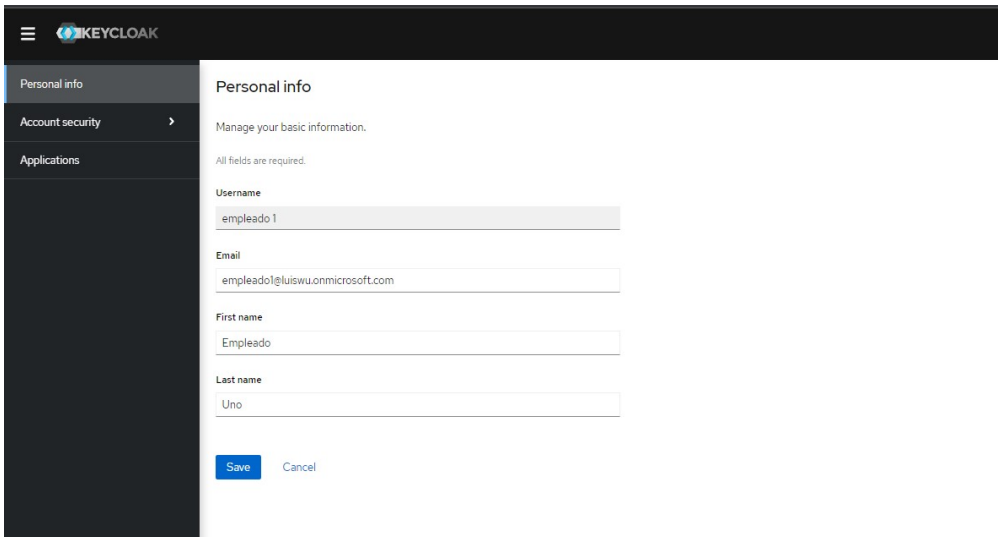

Figura 64: Detalle del usuario en Keycloak

Ahora que tenemos el perfil listo también en Keycloak, podremos desarrollar cualquier aplicación que lo use con usuarios federados desde Azure AD.

Ahora incluso podemos añadir una llave de seguridad para uso de autenticación sin contraseña a este usuario y así beneficiarse del entorno configurado en Kyecloak, ya que es de código abierto sin necesidad de pagar licencias.

Para registrar una llave, hacemos login en la aplicación con el email del empleado.

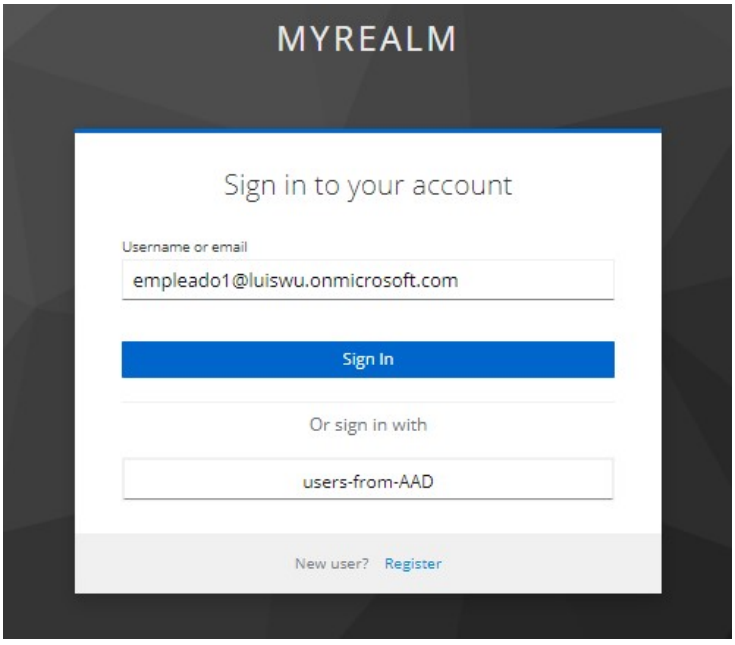

Figura 65: Inicio de sesión con usuario federado

El sistema detecta que no tiene registro de llave y automáticamente le salta el flujo para registrar una llave:

Figura 66: Registro de llave de seguridad

Usando la misma metodología anterior, simulamos la llave virtualmente para poder seguir el proceso. Una vez registrada la llave de seguridad podremos ver en el perfil que como metodología de autenticación solo tiene la llave de seguridad.

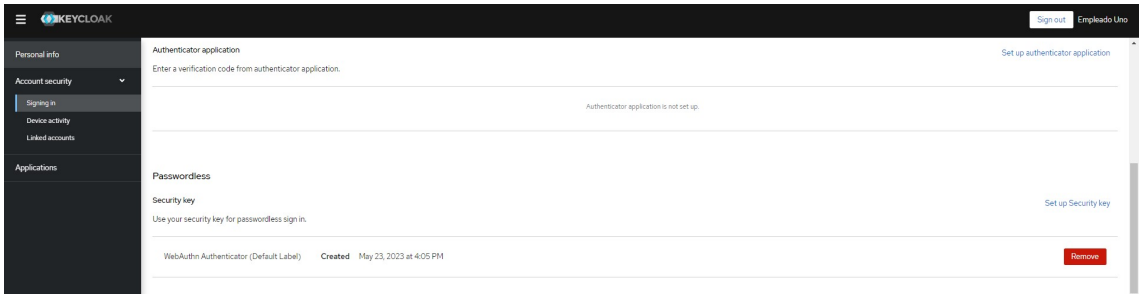

Figura 67: Información de las posibilidades de inicio de sesión del usuario

A partir de ahora, siempre que se quiera iniciar sesión, podremos usar nuestro usuario de Azure AD con nuestra llave de seguridad vinculada.

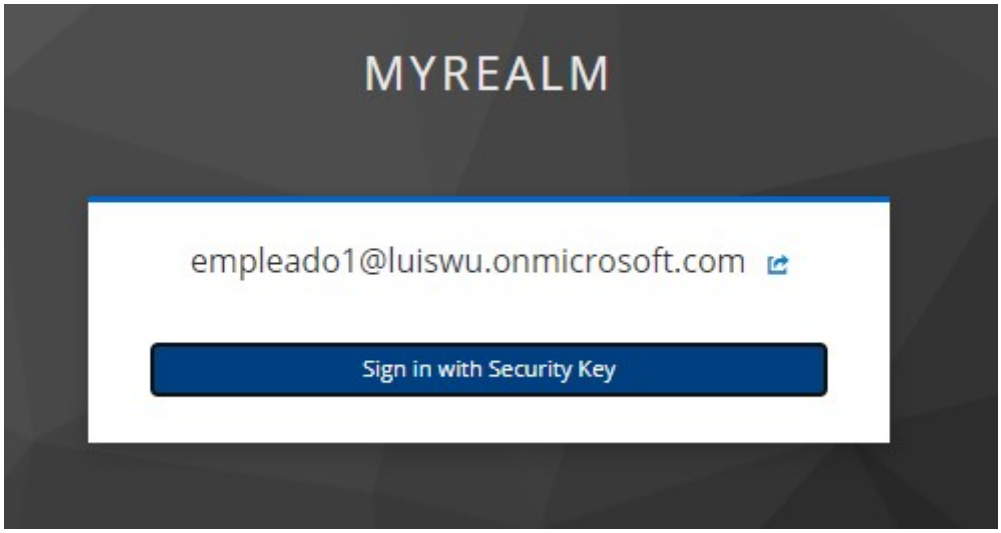

Figura 68: Inicio de sesión con llave de seguridad sin contraseña

Y de esta manera se ha obtenido un inicio de sesión con un usuario federado de directorio activo de Azure en una instancia de Keycloak.

8. Conclusiones y trabajos futuros

En conclusión, la autenticación de segundo factor es una técnica de seguridad esencial para proteger las cuentas de usuario contra el acceso no autorizado. Aunque la autenticación basada en contraseñas sigue siendo la forma más común de autenticación, su debilidad inherente significa que se necesita una capa adicional de protección.

Existen varios métodos de autenticación de segundo factor, como los códigos de un solo uso (OTP), los tokens físicos o las notificaciones push. Cada uno de ellos tiene sus propias ventajas y desventajas, y la elección del método adecuado dependerá de las necesidades y limitaciones específicas de cada sistema.

La autenticación sin contraseña ofrece una solución prometedora para mejorar la seguridad de la autenticación en línea, al mismo tiempo que mejora la experiencia del usuario. Utilizando diferentes métodos de autenticación, como biometría o autenticación basada en dispositivos. Estos métodos son más seguros y cómodos para los usuarios, ya que no tienen que recordar o escribir contraseñas complejas.

Aunque la implementación de autenticación de segundo factor o sin contraseña puede añadir complejidad al proceso de inicio de sesión y requerir un esfuerzo adicional por parte del usuario, los beneficios en términos de seguridad son significativos.

El seguimiento y planificación del trabajado ha sido bastante acertada siguiendo la metodología impuesta y el enfoque definido inicialmente. Se han ido cumpliendo las etapas marcadas, aunque se ha tenido algunas dificultades en ciertos aspectos del trabajo.

Uno de los objetivos principales era explicar qué opciones son las mejores a la hora de aplicar una metodología de autenticación de segundo factor y cuáles son las que más se usan en un entorno empresarial. Creo, que se ha conseguido reflejar de manera correcta, sin embargo, la parte de autenticación sin contraseña aún se podría desarrollar más.

Por la parte práctica, la simulación del entorno empresarial en Azure Cloud con la cuenta estudiante ha salido como esperaba. Se ha podido crear un usuario y añadir la autenticación de segundo factor a través de la aplicación de Microsoft Authenticator demostrando el funcionamiento principal del ejercicio.

En la segunda parte de la práctica ha sido más interesante, ya que Keycloak es software de código abierto sin necesidad de obtener licencia para acceder a todas las funcionalidades. Se ha hecho una prueba muy atractiva de un entorno para autenticación sin contraseña. Además, se ha tenido que desplegar a un contenedor Docker y configurarlo desde cero.

Se ha demostrado que añadiendo una capa de seguridad en la contraseña se mitiga bastante al hackeo de contraseñas por parte de los atacantes así

ayudando a proteger el sistema de posibles ataques y sobrecargas al sistema. Esto puede ayudar a ahorrar en energía evitando sobrecargas y reinicios de contraseña constantes, impactando así de manera positiva en la sostenibilidad.

En términos ético-sociales se ha demostrado que implementando una autenticación de doble factor no es tan compleja y no se requiere un extra recurso para el usuario tendiendo en cuenta que cualquier usuario medio dispone de un dispositivo móvil.

En cuanto a la diversidad, entendemos que no todas las personas pueden configurar un dispositivo para la autenticación de segundo factor pero las instrucciones que el propio sistema te proporciona paso a paso debería ayudar a mitigar ese problema.

Como trabajo futuro, una de las cosas interesantes sería explorar otras opciones de autenticación de segundo factor o poder combinar varias en un mismo entorno.

En la prueba en Azure, sería interesante poder configurar el acceso condicional para requerir autenticación de segundo factor solo cuando se accede a ciertos recursos importantes.

9. Glosario

2FA: Autenticación de segundo factor.

Passwordless: Autenticación sin contraseña

Phishing: Estafa que tiene como objetivo obtener a través de internet datos privados de los usuarios, especialmente para acceder a sus cuentas o datos bancarios.

FIDO2: Fast Identity Online y es un estándar permite que los usuarios puedan utilizar sus propios dispositivos para realizar la autenticación en servicios online, tanto en entornos móviles como de escritorio.

U2F: es un estándar de autenticación abierto que utiliza una clave para múltiples servicios.

USB: Bus de conexión universal.

NFC: Comunicación de campo cercano es una tecnología de comunicación inalámbrica, de corto alcance y alta frecuencia que permite el intercambio de datos entre dispositivos.

MFA: Autenticación multifactor.

Keycloak: Software de código abierto para identificar usuarios en un entorno (Identity Manager).

Docker: Proyecto de código abierto para despliegue de contenedores.

10. Bibliografía

[1] GanttPro. Disponible en: https://app.ganttpro.com/ (Consultado el 11/03/2023)

[2]. Agencia Española Protección de datos. Disponible en: https://www.aepd.es/es/prensa-y-comunicacion/blog/cifrado-y-privacidad-cifrado-en-el-rgpd (Consultado el 17/03/2023)

[3]. Reese et. al. (2019) *A Usability Study of Five Two-Factor Authentication Methods*, Usenix (The advanced computing systems association).

[4] '7 Ventajas de usar la autenticación de varios factores' (2021) *cm.com Blog*, 3 de diciembre. Disponible en: https://www.cm.com/es-es/blog/7-ventajas-de-usar-la-autenticacion-de-varios-factores/ (Consultado el 22/03/2023).

[5] '¿Qué es la autenticación de doble factor (2FA)?' (2020) *avg.com Blog,* 19 de noviembre. Disponible en: https://www.avg.com/es/signal/what-is-two-factor-authentication (Consultado el 22/03/2023).

[6] Passwordless Authenticaion Methods. Disponible en: https://github.com/OpenIdentityPlatform/OpenAM/wiki/Passwordless-Authenticaion-Methods (Consulatado el 23/03/2023).

[7] Best Multi-Factor Authentication (MFA) Software for Enterprise Businesses. Disponible en: https://www.g2.com/categories/multi-factor-authentication-mfa/enterprise (Consultado el 01/05/2023).

[8] NIST (2017), *Digital Identity Guidelines. Authentication and Lifecycle Management.* Disponible en: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf

[9] Acemyan et. al., 2fa might be secure, but it's not usable: A summative usability assessment of google's two-factor authentication (2fa) methods, 2018.

[10] OKTA. Disponible en: https://www.okta.com/ (Consultado el 09/04/2023)

[11] 'Top 10 Two-Factor Authentication Vendors in 2021' (2022*) spiceworks Blog*, 5 de Agosto. Disponible en: https://www.spiceworks.com/it-security/identity-access-management/articles/two-factor-authentication-vendors/ (Consultado el 28/04/2023).

[12] Duo.com. Disponible en: https://duo.com/es/duo-overview (Consultado el 02/05/2023)

[13] IBM España. Disponible en: https://www.ibm.com/es-es/verify (Consultado el 02/05/2023)

[14] RSA SecurID. Disponible en: https://www.rsa.com/resources/webinars/conozca-securid/ (Consultado el 02/05/2023)

[15] Azure Portal. Disponible en: https://portal.azure.com/?Microsoft_Azure_Education_correlationId=26a38f7df5164c7693d5fb6c85bb1dbd#home (Consultado el 05/05/2023)

[16] Docker. Disponible en: https://docs.docker.com/ (Consulatdo el 20/05/2023)

[17] Keycloak. Disponible en: https://www.keycloak.org/ (Consultado el 20/05/2023)