	INSTRUCCIÓN DETALLADA	Código KDBS_00_01_00	Versión 1.0
Universidad Autónoma de Madrid Configuración de Autenticación Multifactor	Configuración de Autortionsión Multifester	Fecha: 25/01/2023	
	Página 1	de 14	

Configuración de múltiple factor de autenticación (MFA)

Autores: Carlinho Amado Braga Márquez Miguel Ángel García Julio Álvarez Fecha de creación: 18/03/2022

Redacción y publicación: Fecha de revisión: 15/06/2022 Aprobado por: Jefatura de unidad Técnica de Soporte informático



Índice

1	Instrucciones de instalación	3
	Objetivo y requisitos:	3
	¿Como funciona el MFA?	. 3
2	Instrucciones de configuración	. 4
	Configuración de la cuenta	. 4
	Configuración de la aplicación móvil	5
	Probando el funcionamiento de la validación MFA	11
3	Enlaces de ayuda	14
4	Registro de cambios	14



1 Instrucciones de instalación

Objetivo y requisitos:

La autenticación multifactor (MFA), o autenticación fuerte, es más conocida por proporcionar una defensa adicional y dificultar el acceso de una persona no autorizada a una red, base de datos o servicio. La implementación de una solución MFA sólida puede proteger instantáneamente los datos y los recursos de TI contra el robo de identidad, la suplantación de cuentas y el phishing.

En lugar de pedir el tradicional "ID + contraseña", la autenticación fuerte MFA pide al usuario que proporcione información de verificación adicional, llamada "factores de autenticación", para garantizar que es quien dice ser.

Con esta implantación se pretende mejorar la seguridad en el acceso a los servicios online de la UAM. Esta autenticación multifactor se irá implantando progresivamente en aquellos servicios de la UAM en los que se pueda realizar la validación con el servicio de autenticación de Microsoft.

¿Como funciona el MFA?

El proceso de autenticación requiere la combinación de al menos dos factores de dos categorías diferentes entre las siguientes:

- Algo que conozco (factor de conocimiento), como una contraseña, frase de paso o PIN.
- Algo que tengo (factor de posesión), como un dispositivo (smartphone, ordenador, etc.), una tarjeta inteligente.
- Algo que soy (factor de inherencia), ya sea una huella dactilar, la voz o el reconocimiento facial, o cualquier otro tipo de biometría.



2 Instrucciones de configuración

Configuración de la cuenta

Para configurar la autenticación multifactor (MFA), previamente, es necesario proporcionar algunos datos. Para ello, acceder con las credenciales de la UAM a la página https://mysignins.microsoft.com/security-info:

Microsoft	UAM Universidad Autónoma de Madrid
Iniciar sesión	← direccion.correo@uam.es
direccion correo@uam es	Escribir contraseña
¿No puede acceder a su cuenta?	He olvídado mi contraseña
Sigu	ente
	En caso de problemas a la hora de iniciar sesión puedes ponerte en contacto con el Centro de
🔍 Opciones de inicio de sesión	Atención a Usuarios en cau@uam.es o al telefono 9 497 (40 29)

Desde Tecnologías de la Información, se recomienda instalar la aplicación **Microsoft Autenticator** para validar la autenticación. Esta aplicación está disponible para dispositivos Android y iOS. No obstante, es posible agregar otros métodos adicionales, como mensaje SMS, llamada telefónica o correo electrónico alternativo.

En el menú de la izquierda, acceda a la opción **Información de seguridad** y posteriormente **Agregar método**:

UAM Universidad Autónoma de Madrid	Nis inicios de sesión
A Información general Re Información de seguri	Información de seguridad Estos son los métodos que usa para iniciar sesión en su cuenta o restablecer su contraseña.
 Organizaciones 	+ Agregar método No hay elementos para mostrar.
 Dispositivos Privacidad 	¿Ha perdido el dispositivo? Cerrar todas las sesiones

IMPORTANTE: Además de la aplicación, es fundamental añadir, por ejemplo, un número de teléfono móvil o fijo como alternativas de acceso en caso de pérdida o cambio del terminal o número.



Seleccione **Agregar Aplicación de autenticación** y siga las indicaciones que aparecerán en las ventanas siguientes:

×
\sim
regar

En esta ventana, se recomienda descargar e instalar la aplicación **Microsoft Autenticator** para validar la autenticación.

Si dispone en su dispositivo de otra aplicación de autenticación (por ej. Google Authenticator), ésta podrá ser utilizada seleccionando la opción **Quiero usar otra aplicación de autenticación**, siguiendo los pasos que aparezcan en pantalla.

Desde Tecnologías de la Información, se recomienda el uso de **Microsoft Authenticator**, ya que permite realizar la validación con solo pulsar un botón en la aplicación.



A través del siguiente enlace, la descarga de la aplicación está disponible tanto para Google Play Store como para Apple Store:

Microsoft Mobile Phone Authenticator App | Microsoft Security

Configuración de la aplicación móvil

Una vez descargada la aplicación en el dispositivo, se configura añadiendo ID-UAM del usuario.

Las capturas de pantalla de este manual corresponden a la versión de iOS, pudiendo variar ligeramente en los dispositivos Android.



Al acceder por primera vez a la aplicación, se permite iniciar sesión con una cuenta Microsoft personal, una cuenta profesional o educativa o escanear un código QR. Pulse sobre **Agregar una cuenta profesional o educativa**:



A continuación acceda a la opción Agregar Cuenta:





Seleccione de nuevo Cuenta profesional o educativa:



Pulse sobre Escanear código QR:



La aplicación solicitará acceso a la cámara del dispositivo móvil para poder capturar el código QR que se muestra en la pantalla de su PC. Debe **Permitir** el acceso a la misma:





Una vez concedido el acceso, enfoque el dispositivo hacia la pantalla de su ordenador para capturar el código que se muestra en cada caso:

Microsoft Authenticator		×
Digitalización del código C	QR	
Use la aplicación Microsoft Authenticat Authenticator y la cuenta quedarán em	or para escanear el código QR. Así, la aplicación Microsoft parejadas.	
Después de escanear el código QR, elija	"Siguiente".	
¿No puede escanear la imagen?		
	Atrás Siguient	¢

Tras capturar el código y procesarlo correctamente, la aplicación solicitará permiso para enviar notificaciones. Pulse en **Permitir** para poder recibir los avisos de la misma:





Llegado este momento, la aplicación recibirá una primera notificación de solicitud de permiso de acceso:

Microsoft	t Authenticator	×
	Vamos a probarlo	
	Apruebe la notificación que le vamos a enviar a su aplicación.	
L-J		
	Atrás	Siguiente

Estás notificaciones aparecerán cada vez que se intente hacer un inicio de sesión con su cuenta. Pulse en **Permitir** sólo si se está seguro de que es Usted mismo el que está intentando iniciar sesión:

11:10	al 🗢 🗔
\equiv Authenticator	+
UAM direccion.correo@uam.es	>
¿Quiere aprobar el inic de sesión?	io
UAM direccion.correo@uam.es	
Denegar Aprob	ar
	0
Authenticator Contraseñas	Direcciones

Puede tener configuradas tantas cuentas que usen MFA como necesite, tanto a nivel personal como profesional.



Si ha seguido los pasos correctamente, habrá finalizado la configuracion:

A	Microsoft Authenticator	×
D pe	Notificación aprobada	
l	Atrás Siguiente	

Una vez finalizada la configuración, se mostrará un listado con las cuentas que tiene configuradas en la aplicación:





Si se hace clic sobre la una de las cuentas, se mostrará información acerca de ella, así como distintos parámetros de configuración, la posibilidad de revisar la actividad reciente u otros parámetros:



Con realización de estos pasos de configuración, se habrá agregado el método de validación:

Información de seguridad Estos son los métodos que usa para iniciar sesión en su cuenta o restablecer su contraseña.			
Establecer método predeterminado de inicio de sesión			
+ Agregar método			
Microsoft Authenticator	Eliminar		
¿Ha perdido el dispositivo? Cerrar todas las sesiones			

Probando el funcionamiento de la validación MFA

Para comprobar el correcto funcionamiento de la validación multifactor (MFA), acceda a cualquier servicio que utilice la autenticacion con Microsoft, como por elemplo Office 365 a través del siguente enlace: <u>https://portal.office.com</u>



Una vez que se acceda, es necesario introdur su usuario y contraseña UAM:



Al pulsar Iniciar Sesión, aparecerá una pantalla donde se ofrecerá elegir cualquiera de los distintos métodos de autenticación que tenga configurados. Para utilizar la aplicación MFA de Microsoft, seleccione Aprobar una solicitud en la aplicación Microsoft Authenticator:

direccion.correo@uam.es		
Û	Aprobar una solicitud en la aplicación Microsoft Authenticator	
123	Usar el código de comprobación de mi aplicación móvil	
	Enviar un mensaje de texto al +XX XXXXXXX33	
R	Llamar al +XX XXXXXXX33	
Más info	ormación	
¿Están a Compru	¿Están actualizados los métodos de verificación? Compruébelo en https://aka.ms/mfasetup	
	Cancelar	
En caso de problemas a la hora de iniciar sesión puedes ponerte en contacto con el Centro de Atención a Usuarios en cau@uam.es o al telefono 91 497 (40 29)		

En su PC se mostrará la siguiente información y un código aleatorio a la espera de la aprobación de sesión en el dispositivo móvil:





Llegado este momento, saltará una notificación en el dispositivo móvil que asoció a la cuenta, a la espera de la aprobación del acceso. Debe indicar el código mostrado anteriormente.

Crange uil 😤 💻	Android	iPhone
11.00	20:31 7,8KB/5 🗇 🕫 💷 💲 📶 🚛 🖗 🎟	13:45 .nl 후 🖿)
Miércoles, 30 de marzo	 ¿Está intentando iniciar sesión? UAM elena velasco@uam.es 	Authenticator + ¿Está intentando iniciar sesión?
¿Quiere aprobar el inicio de sesión? #7078	Aplicación Office 365 SharePoint Online Ubicación Comunidad de Madrid, España	@uam.as Escriba el número que se muestra para iniciar sesión.
		VPN TI - Acceso Remoto TI Ubicación Madrid, España
	Escriba el número que se muestra para iniciar sealón. Escriba el número aquí	No. no sory yo
	si	Ruames
	NO, NO SOY YO	1 2 3 ABC DEF
	1 2 ABC 3 DEF	4 5 6
	4 GHI 5 JKL 6 MINO	7 8 9 Pors Tuv Wxyz
Destilas hacis arriba para abriv	7 Polisis 8 TUV 9 WXTZ	■ 0

Una vez aprobada la sesión, accederá a su página personal de Office 365 (en este caso) o al servicio que haya elegido.



3 Enlaces de ayuda

https://support.microsoft.com/es-es/topic/qu%C3%A9-es-autenticaci%C3%B3nmultifactor-e5e39437-121c-be60-d123-eda06bddf661

4 Registro de cambios

Fecha	Versión	Motivo de cambio	Autor cambio
25/01/2023	1.1	Aplicación normativa seguridad Microsoft	