



PROCEDIMIENTO DE AUTENTICACIÓN POR MULTI-FACTOR DESDE AZURE MFA

Fecha de publicación 05/06/2020
Versión 5.0

1.	INTRODUCCION	3
1.1.	OBJETIVO Y ALCANCE	3
2.	COMPROBACIONES PREVIAS DEL NAVEGADOR.....	4
3.	REGISTRO EN AZURE Y ESTABLECIMIENTO MÉTODO PREDETERMINADO.	5
4.	OTROS MÉTODOS.....	11
4.1.	MÉTODO “TELÉFONO ALTERNATIVO”	12
4.2.	MÉTODO “CORREO ELECTRONICO”	13
4.3.	MÉTODO “APLICACIÓN DE AUTENTICACIÓN” (VÁLIDO PARA SMARTPHONES)	14
4.4.	MODIFICACIONES POSTERIORES DE LOS DATOS PROPORCIONADOS EN EL PROCESO DE REGISTRO	16
5.	AUTENTICACIÓN.....	17
6.	MANTENIMIENTO PASSWORD.....	18
7.	FAQS	21

1. INTRODUCCION.

1.1. OBJETIVO Y ALCANCE

El presente documento tiene como objetivo explicar el procedimiento de autenticación por multi-factor desde la página de Azure MFA con los diferentes métodos que ofrece:

- Llamada de teléfono
- Mensaje de texto,
- Correo electrónico
- Aplicación móvil.

Se recomienda por lo menos tener siempre dos métodos habilitados para el doble factor de autenticación, por ejemplo con un teléfono y un correo electrónico. De tal forma que si cambia de número de teléfono, podrá seguir usando el método de correo electrónico, o si por el contrario cambia de correo electrónico, se seguirá pudiendo acceder con el número de teléfono... en este documento se explica cómo agregar, modificar o eliminar los diferentes métodos posibles.

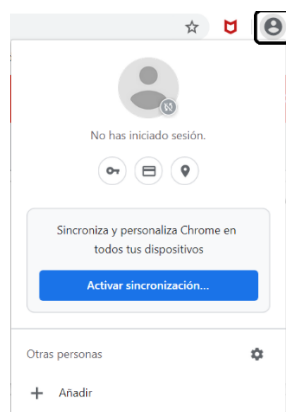
2. COMPROBACIONES PREVIAS DEL NAVEGADOR.

Para una mejor visualización, es recomendable hacer el registro o enrolamiento, a través de Chrome, Firefox o Microsoft Edge.

En el caso de disponer en su empresa ya un doble factor de autenticación con Microsoft hay muchas probabilidades que su navegador nada más iniciarlo inicie sesión automáticamente con el usuario de su empresa. Es necesario cerrar la sesión de su empresa para garantizar que accede con las credenciales de Santander Global Tecnología.

Se debe revisar que el navegador no tiene iniciada la sesión con el usuario de su empresa ya que provocará errores a la hora de identificarse con credenciales de Santander y a mayores se recomienda eliminar cookies y caché:

- Caso de Chrome: arriba a la derecha comprobar en el perfil si hay alguna sesión activa, en caso de estarlo basta con acceder como invitado o cerrar la sesión.



- Caso de Firefox: Para garantizar que no entra en conflicto basta con abrir una navegación privada: **Ctrl+Mayús+P**

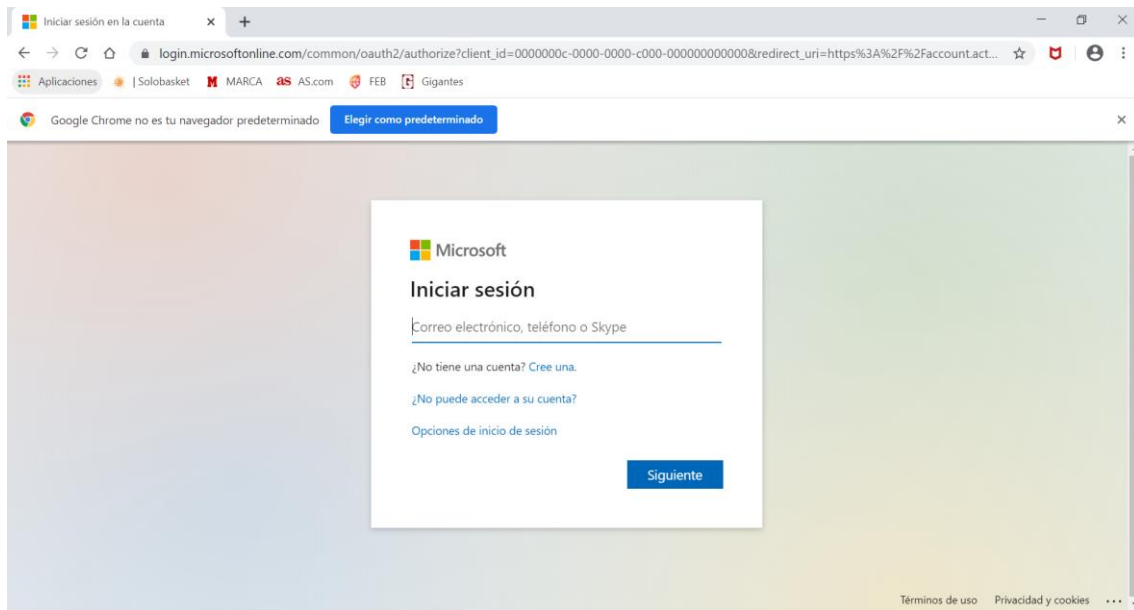
Archivo Editar Ver Historial Marcadores	
Nueva pestaña	Ctrl+T
Nueva ventana	Ctrl+N
Nueva ventana privada	Ctrl+Mayús.+P

- Caso de Microsoft Edge: Para garantizar que no entra en conflicto basta con confirmar en “Configuración del navegador” que no hay ninguna cuenta registrada de su empresa.

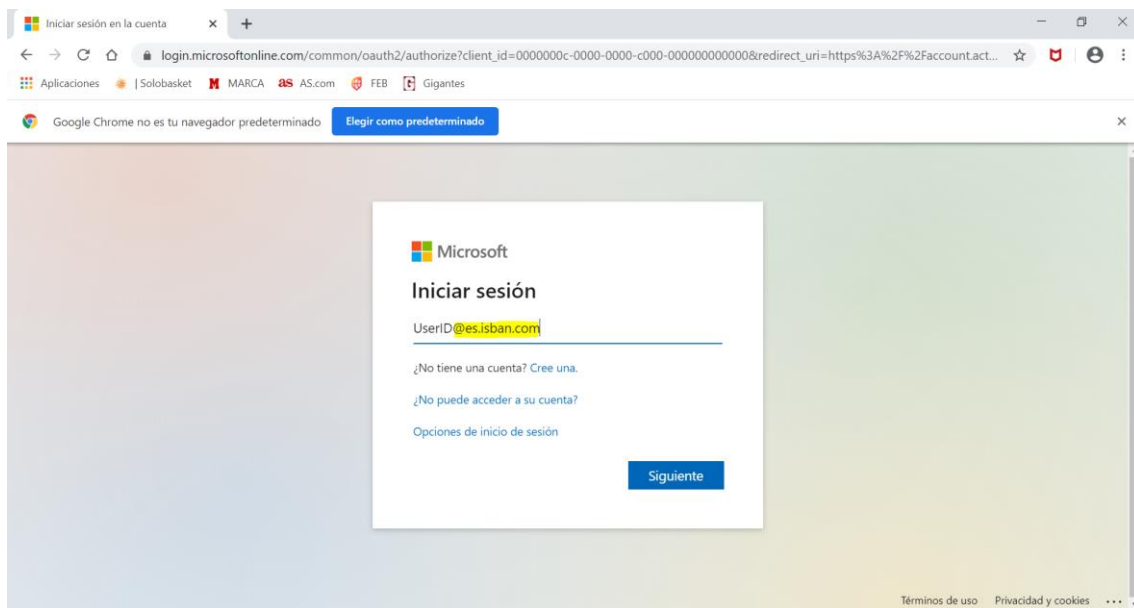
3. ENROLARSE EN AZURE Y ESTABLECIMIENTO MÉTODO PREDETERMINADO.

Tras realizar las verificaciones mencionadas anteriormente con el navegador que vayas a usar y de **comprobar que estás conectado a la VPN**, se procede a entrar en:

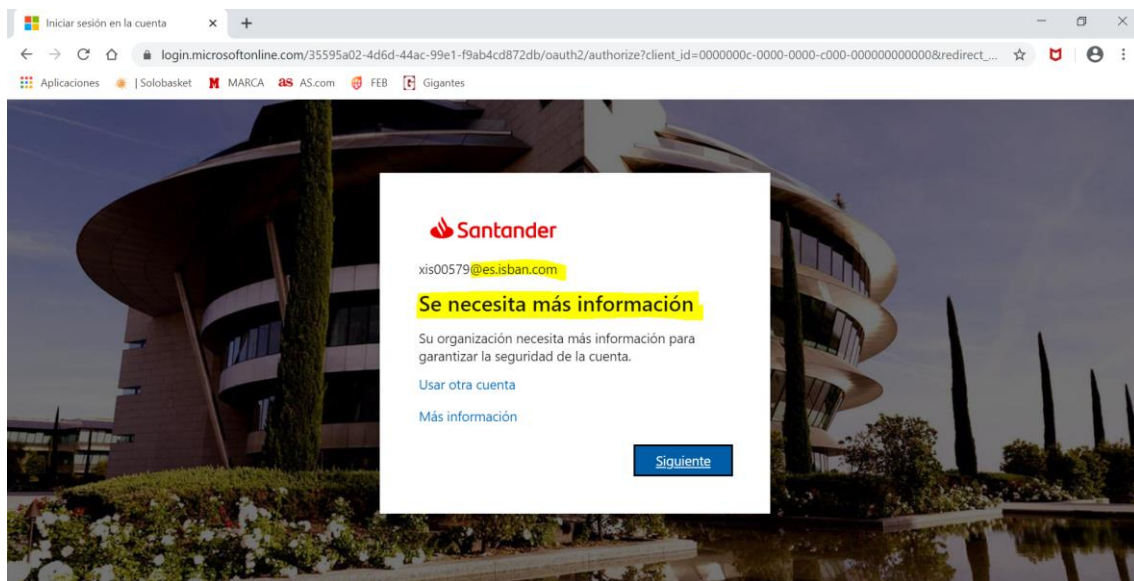
➤ <https://aka.ms/mfasetup>



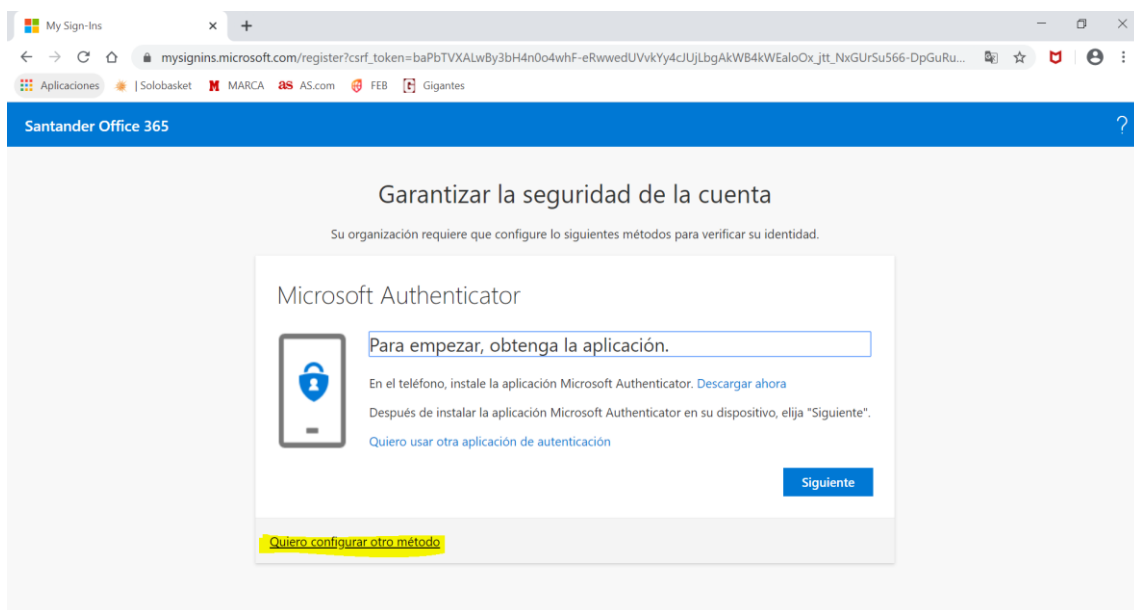
En esta primera página genérica de inicio de sesión de Microsoft, te identificarás con tu usuario UPN (el que lleva el @es.produban.com, @es.isban.com o @santanderglobaltech.com si tienes migrado tu equipo a Dominio SGT) tal y como se muestra a continuación:



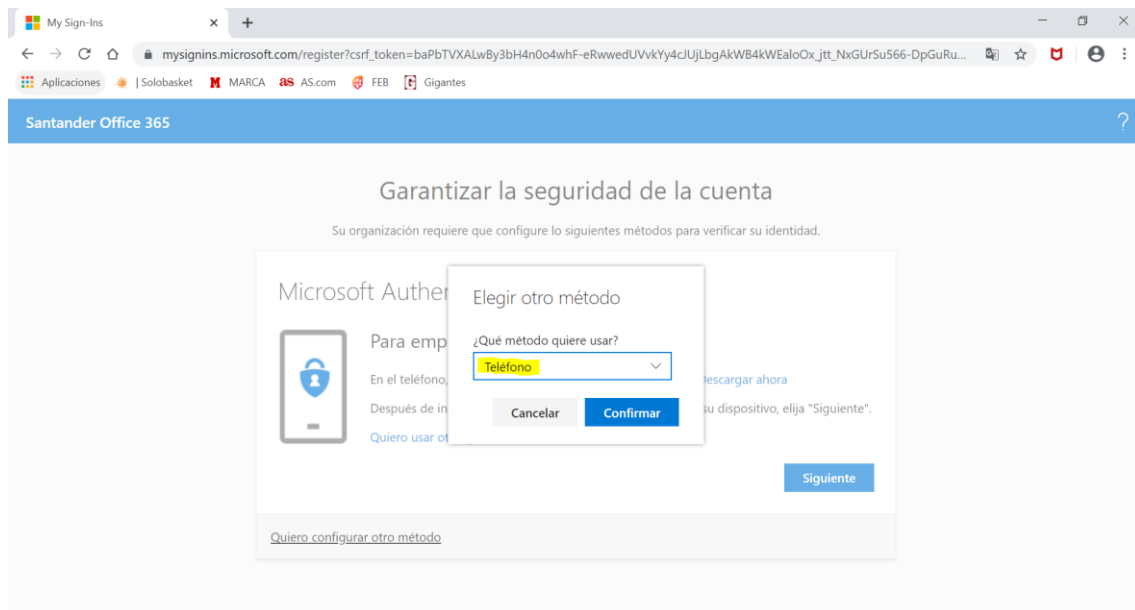
Tras pulsar siguiente te mostrará la pantalla en que te indica que Se necesita más información de la cuenta asociada al UPN indicado, hacemos clic en botón siguiente:



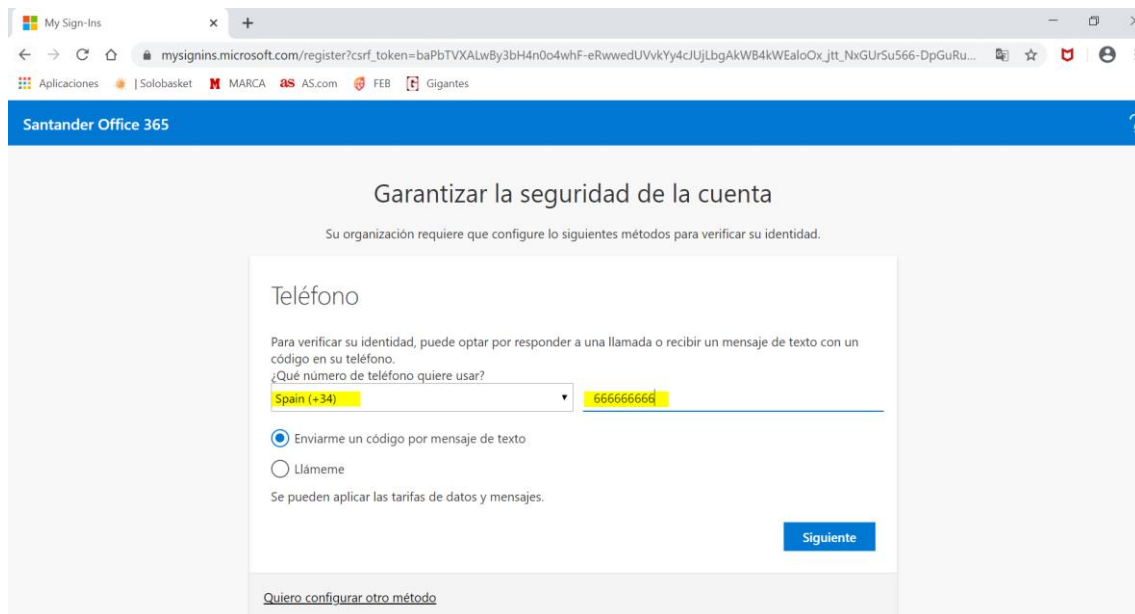
Y accedemos a la pantalla donde vamos a configurar el método por defecto. Inicialmente nos ofrece la opción de establecer nuestro 2º factor de autenticación a través de la aplicación “Microsoft Authenticator”. Y un enlace dónde podemos cambiar el método “Quiero configurar otro método”, seleccionamos éste enlace.



Y nos aparece una pantalla dónde elegir otro método. Seleccionamos “Teléfono” y pulsamos el botón “Confirmar”.



Introducimos el Nº de Teléfono, el país al que pertenece el número de teléfono y el método donde queremos recibir el mensaje de texto o la llamada, que servirá de 2º factor de autenticación para validar nuestra identidad.



Inmediatamente después de pulsar Siguiente, recibiremos un Mensaje de texto con un código que debemos introducir en la pantalla siguiente o si hemos elegido el método de la Llamada de teléfono, recibiremos una llamada, que debemos contestar y seguidamente pulsar “#” en el Nº de Teléfono que hayamos especificado:

Opción Mensaje de Texto:

My Sign-Ins

mysignins.microsoft.com/register?csrf_token=baPbTVXALwBy3bH4n0o4whF-eRwwedUVvkYy4cJlJLbgAkWB4kWEaloOx_jtt_NxGURsu566-DpGuRu...

Aplicaciones | Solobasket | MARCA | AS.com | FEB | Gigantes

Santander Office 365

Garantizar la seguridad de la cuenta

Su organización requiere que configure lo siguientes métodos para verificar su identidad.

Teléfono

Acabamos de enviar un código de 6 dígitos al número +34 666666666. Escriba el código a continuación.

Especificar el código

Reenviar código

Atrás Siguiente

[Quiero configurar otro método](#)

Opción Llamada de Teléfono:

My Sign-Ins

mysignins.microsoft.com/register?csrf_token=c8zVgX3XMQUhZj8BkSn0HrtOYfsPyg4iHWiyrDNg4bsOssHc83xn8tKeA-mWXcrrvXjXNefXSARggQk4...

Aplicaciones | Solobasket | MARCA | AS.com | FEB | Gigantes

Santander Office 365

Garantizar la seguridad de la cuenta

Su organización requiere que configure lo siguientes métodos para verificar su identidad.

Teléfono

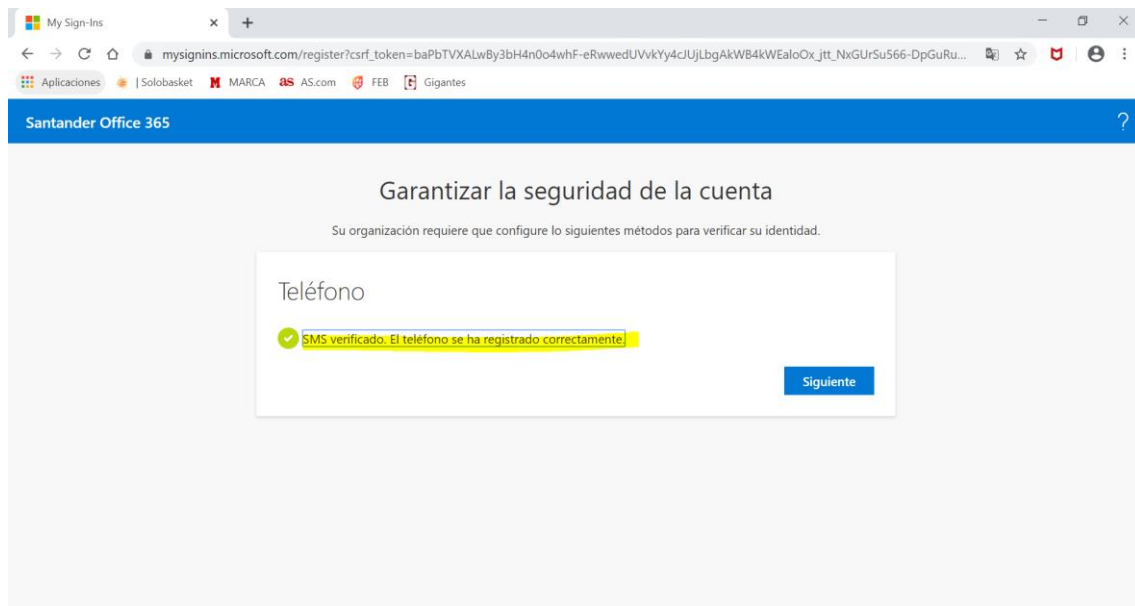
Estamos llamando al +34 666666666

Atrás

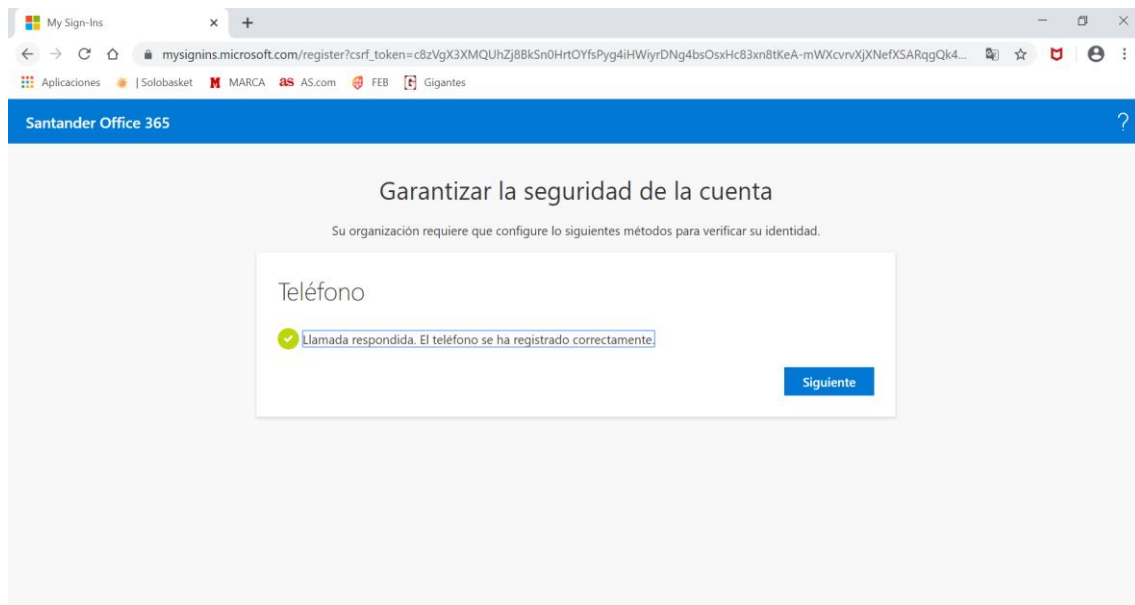
[Quiero configurar otro método](#)

Una vez hemos verificado nuestro 2º Factor de autenticación nos mostrará un mensaje indicando que el teléfono se ha quedado registrado correctamente.

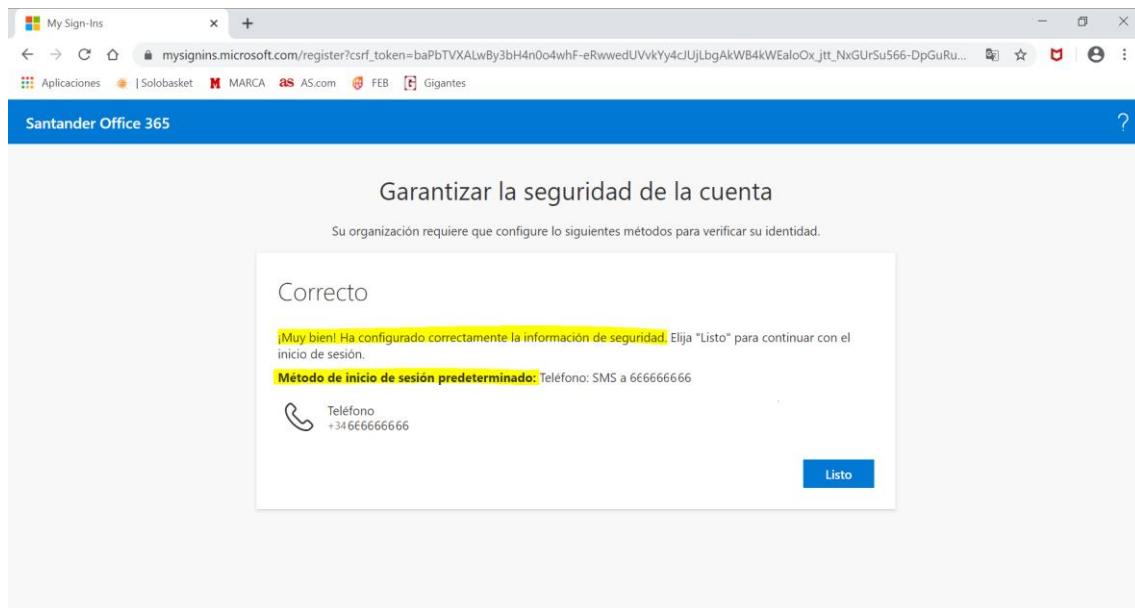
Opción Mensaje de Texto:



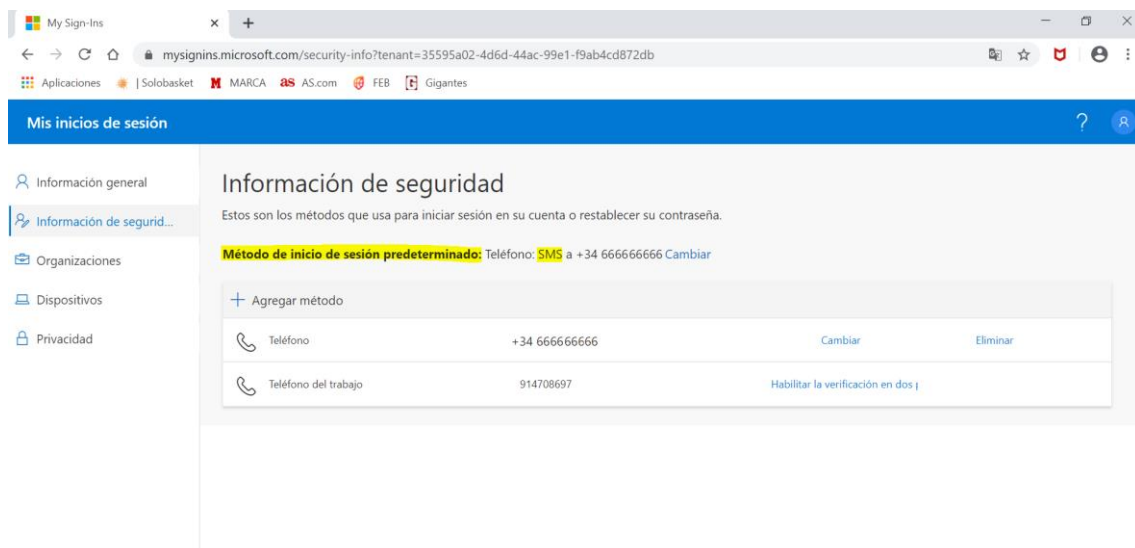
Opción Llamada de Teléfono:



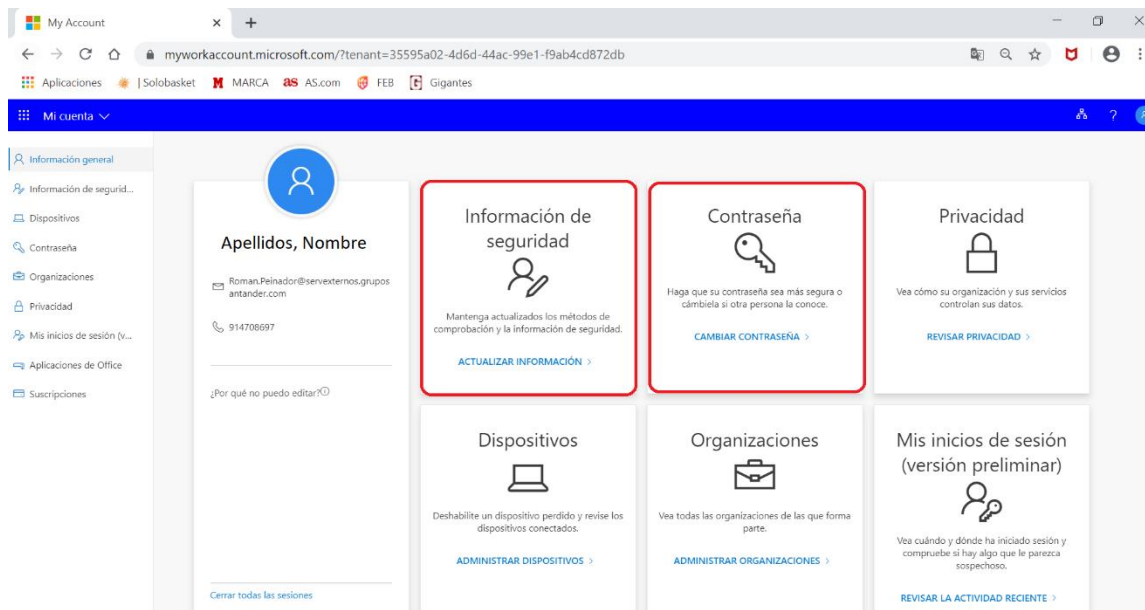
Una vez superada la autenticación, habremos configurado el 2º Factor de autenticación(Inicio de Sesión) predeterminado con el método que hayamos seleccionado y verificado:



Y accederemos a la pantalla de Administración de Mi Cuenta de Azure:



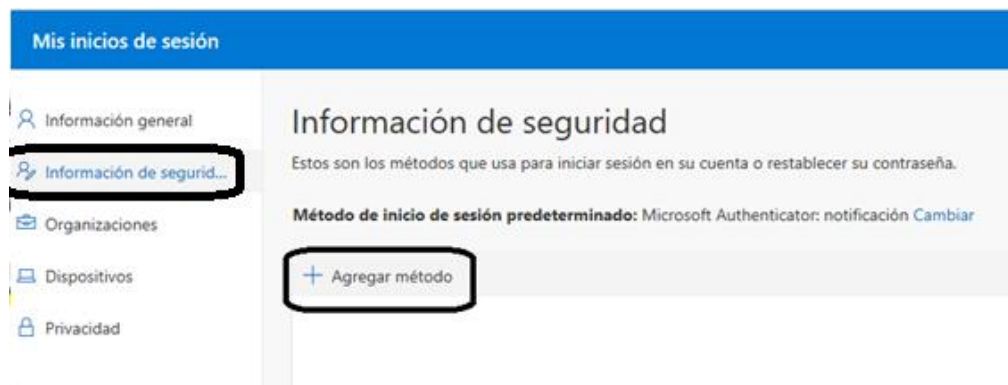
Este documento se centra en como habilitar los diferentes métodos posibles, para el segundo factor de autenticación, así como el mantenimiento de la contraseña. A continuación se muestra la ubicación de los enlaces de “Información de seguridad” y “Contraseña”.



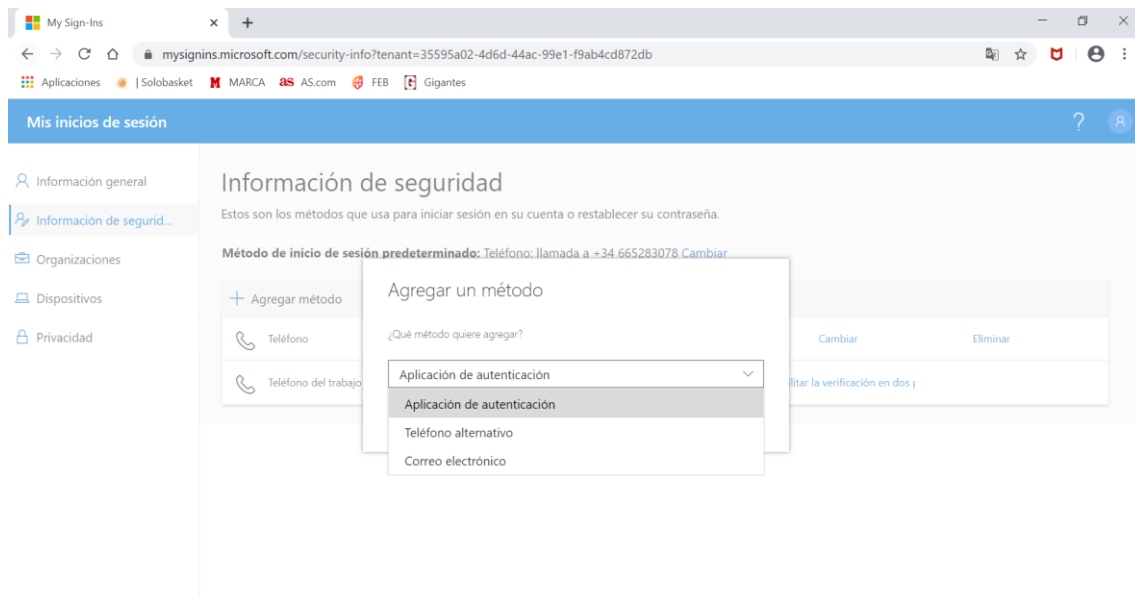
4. CÓMO ESTABLECER OTROS MÉTODOS DE AUTENTICACIÓN.

Seguidamente, se exponen las diferentes formas de agregar otros métodos de autenticación, ya que como hemos indicado al inicio de esta guía, recomendamos tener siempre dos métodos habilitados para el doble factor de autenticación.

Para ello pulsar en “Información de seguridad” y pulsar en “Agregar método” tal y como se indica a continuación:

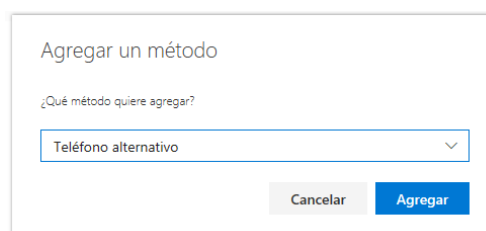


Los diferentes métodos de autenticación son:

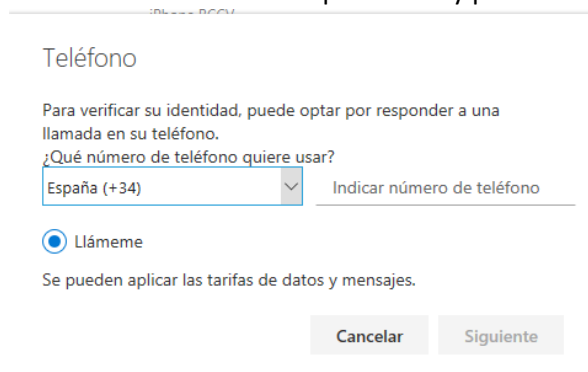


4.1. MÉTODO “TELÉFONO ALTERNATIVO”

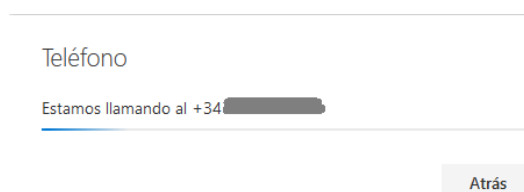
A continuación se evidencian los pasos a seguir para habilitar la opción de recibir llamada de teléfono, para ello pulsar en “Agregar método” y seleccionar “Teléfono alternativo” tal y como se muestra a continuación:



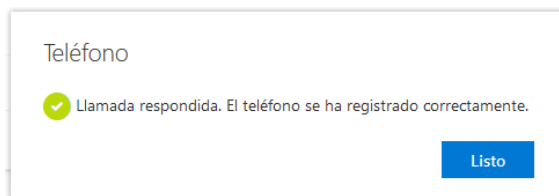
Debe introducirse el teléfono correspondiente y pulsar en “Siguiente”:



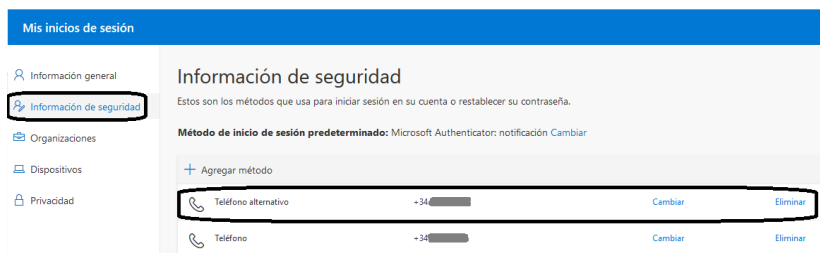
Tras pulsar “Siguiente” aparecerá el aviso de que le están llamando tal que así:



Una vez que se descuelga el teléfono se le indicará “pulse almohadilla” y tras pulsarlo en su teléfono se le mostrará el siguiente aviso de confirmación:

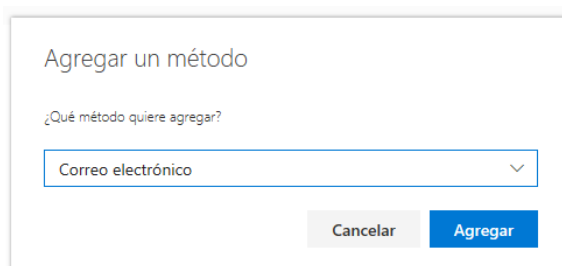


La confirmación final se muestra en la sección de “Información de seguridad” tal que así:



4.2. MÉTODO “CORREO ELECTRONICO”

Para agregar el método “Correo electrónico” hay que seguir los siguientes pasos:



Introducir un correo electrónico y pulsar en “Siguiente”

Correo electrónico

¿Qué correo electrónico quiere usar?

nombre@gruposantander.com

CancelarSiguiente

Hay que introducir el código recibido en el correo seleccionado y pulsar en “Siguiente”. A continuación se muestra un ejemplo real del mail recibido:

Comprobar la dirección de correo electrónico

Gracias por comprobar la cuenta de xIS00579@es.isban.com.

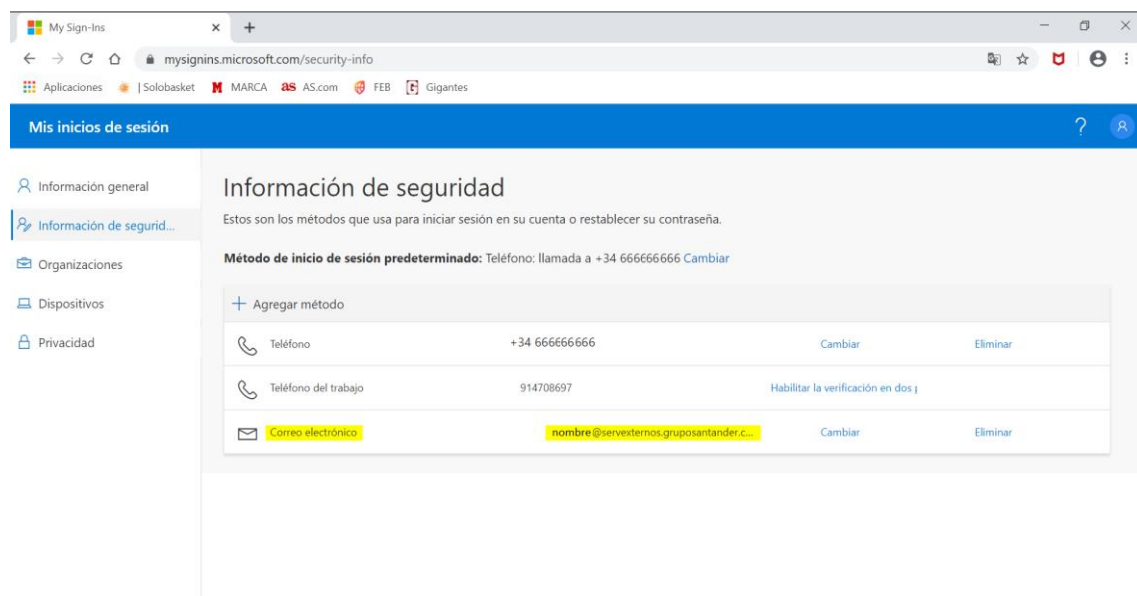
Su código es: 610892

Atentamente,
Santander Office 365

Este mensaje se envió desde una dirección de correo electrónico no supervisada. No responda a este mensaje.



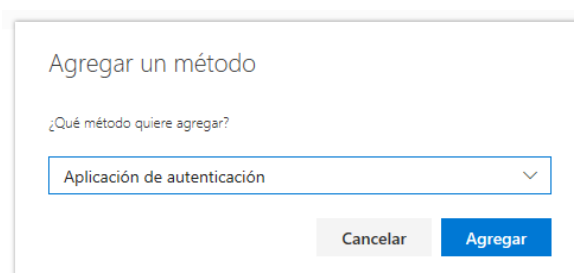
La confirmación final se muestra en la sección de “Información de seguridad” tal que así:



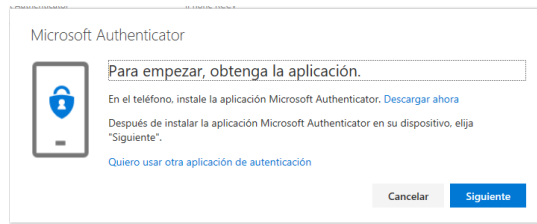
4.3. MÉTODO “APLICACIÓN DE AUTENTICACIÓN” (VÁLIDO PARA SMARTPHONES)

Para agregar el método “Aplicación de autenticación” hay que seguir los siguientes pasos:

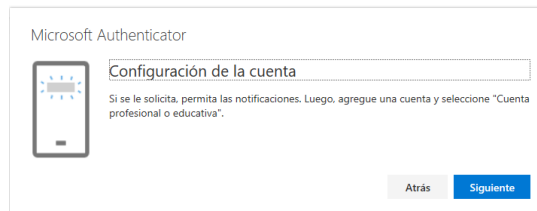
Seleccionar “Aplicación de autenticación” y pulsar en “Agregar”:



Seleccionar “Aplicación de autenticación” y pulsar en “Agregar”.



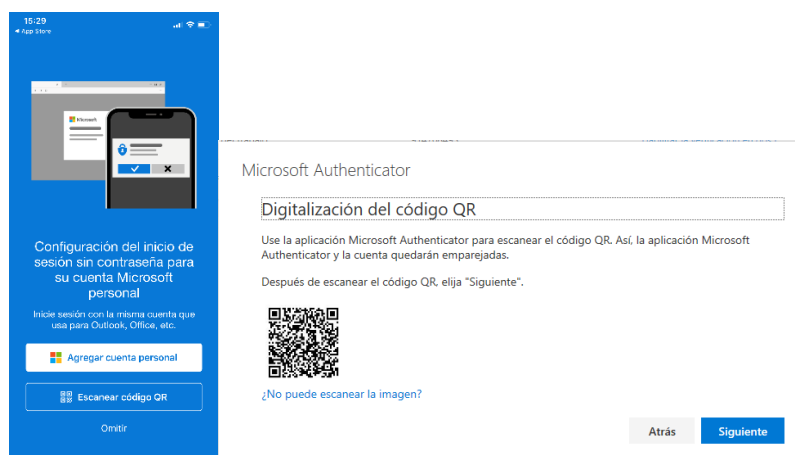
Se requiere instalar en el smart phone la app “Microsoft Authenticator” habilitando o dando permisos para las notificaciones. Pulsar en “Siguiente”:



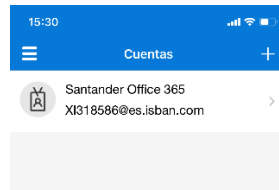
Se requiere abrir la app recién instalada, una vez abierta hay que pulsar “Agregar cuenta”:



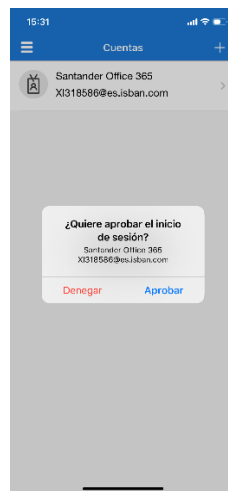
A continuación seleccionar “Escanear código QR” y proceder a escanear con el smart phone el código mostrado en pantalla:



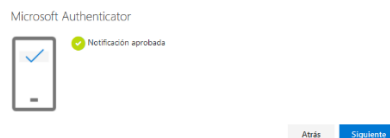
Tras pulsar “Siguiente” ya se tendrá habilitada la cuenta del Santander y se mostrará en la app tal que así:



Automáticamente se lanza una validación online donde se deberá “Aprobar” el inicio de sesión mediante la app, mostrándose la siguiente notificación en la que se requiere pulsar en “Aprobar”:



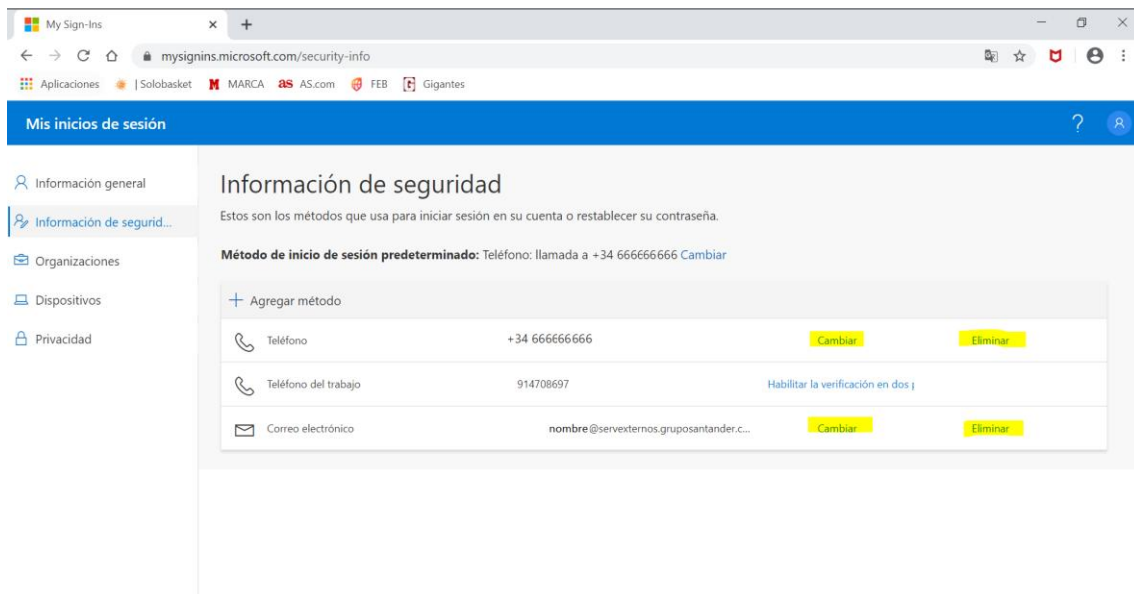
En el navegador saldrá la correspondiente aprobación en la que para acabar hay que pulsar en “Siguiente”



La confirmación final se muestra en la sección de “Información de seguridad”.

4.4. MODIFICACIONES POSTERIORES DE LOS DATOS PROPORCIONADOS EN EL PROCESO DE REGISTRO

Toda modificación de métodos configurados se realiza desde la sección “Información de seguridad”. En el caso de tener un nuevo teléfono por ejemplo, basta con eliminar el método correspondiente y volver a agregar el nuevo teléfono. En caso de cambiar de correo electrónico exactamente lo mismo, basta con eliminar el método correspondiente y volver a agregar el nuevo correo electrónico.



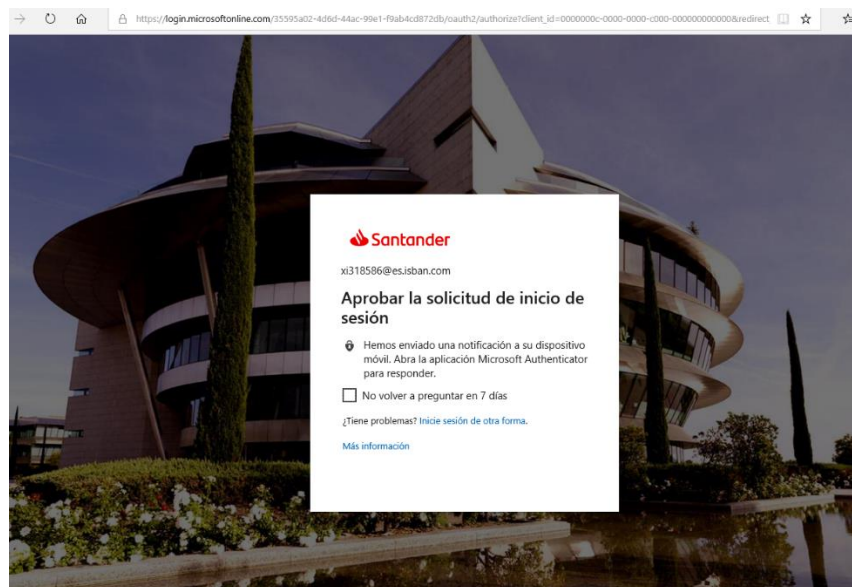
Se permite establecer un método predeterminado de inicio de sesión, para ello desde “Información de seguridad” se puede cambiar el “Método de inicio de sesión predeterminado” tal y como se muestra en la imagen.

5. ACCESO A APLICACIONES Y USO 2º FACTOR AUTENTICACIÓN.

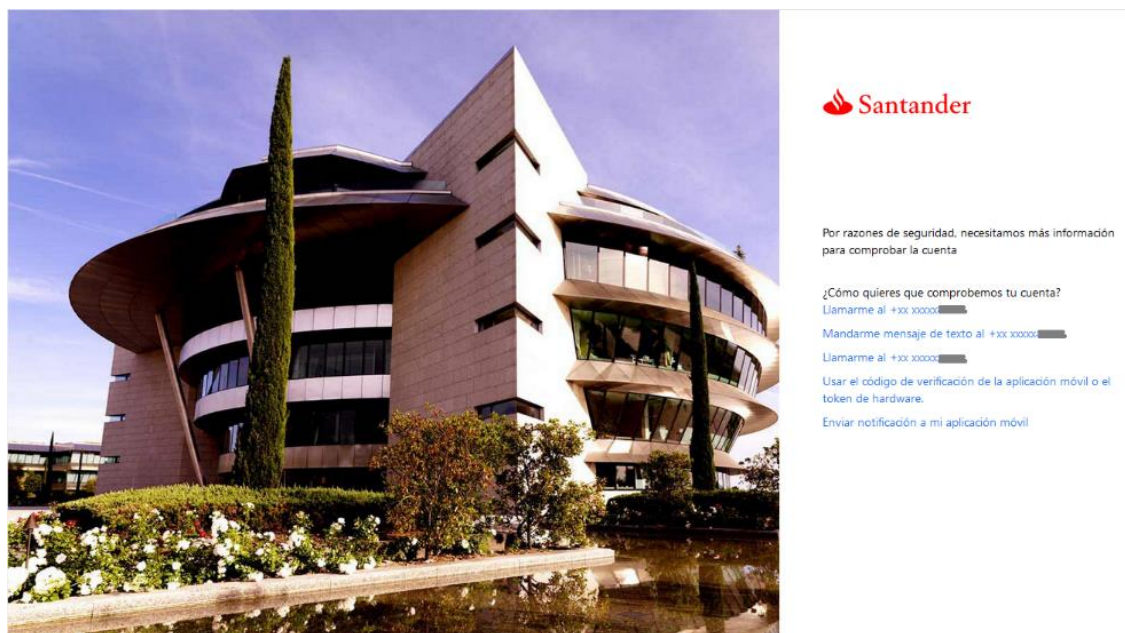
En el caso de tener como “Método de inicio de sesión predeterminado” el envío de SMS, cuando se acceda a una aplicación del Santander (solo para aquellas aplicaciones que requieren el doble factor de autenticación) y tras introducir el UPN correspondiente le saldrá por pantalla un aviso de que se le ha enviado un SMS a su teléfono y se requiere que introduzca en pantalla el código recibido:



En el caso de tener como “Método de inicio de sesión predeterminado” la app Microsoft Authenticator, cuando se acceda a una aplicación del Santander (solo para aquellas aplicaciones que requieren el doble factor de autenticación) y tras introducir el UPN correspondiente le saldrá por pantalla un aviso de que se necesita aprobar desde la app este inicio de sesión:



En el caso de tener varios métodos habilitados también se podrá escoger cual usar desde la ventana de login tal y como se muestra a continuación:



6. MANTENIMIENTO PASSWORD.

Desde esta web <https://aka.ms/mfasetup> y estando en la red de Santander se permite modificar el password del UPN, para ello en la ventana principal pulsar en la sección “Contraseña” tal y como se muestra a continuación:

My Account

myworkaccount.microsoft.com/?tenant=35595a02-4d6d-44ac-99e1-f9ab4cd872db

Aplicaciones | Solobasket | MARCA | AS.com | FEB | Gigantes

Mi cuenta

Información general

Información de seguridad...

Dispositivos

Contraseña

Organizaciones

Privacidad

Mis inicios de sesión (v...

Aplicaciones de Office

Suscripciones

Apellidos, Nombre

Roman.Peinador@servexternos.grupos-antander.com

914708697

¿Por qué no puedo editar?

Cerrar todas las sesiones

Información de seguridad

Mantenga actualizados los métodos de comprobación y la información de seguridad.

ACTUALIZAR INFORMACIÓN

Contraseña

Haga que su contraseña sea más segura o cámbiela si otra persona la conoce.

CAMBIAR CONTRASEÑA

Privacidad

Vea cómo su organización y sus servicios controlan sus datos.

REVISAR PRIVACIDAD

Dispositivos

Deshabilite un dispositivo perdido y revise los dispositivos conectados.

ADMINISTRAR DISPOSITIVOS

Organizaciones

Vea todas las organizaciones de las que forma parte.

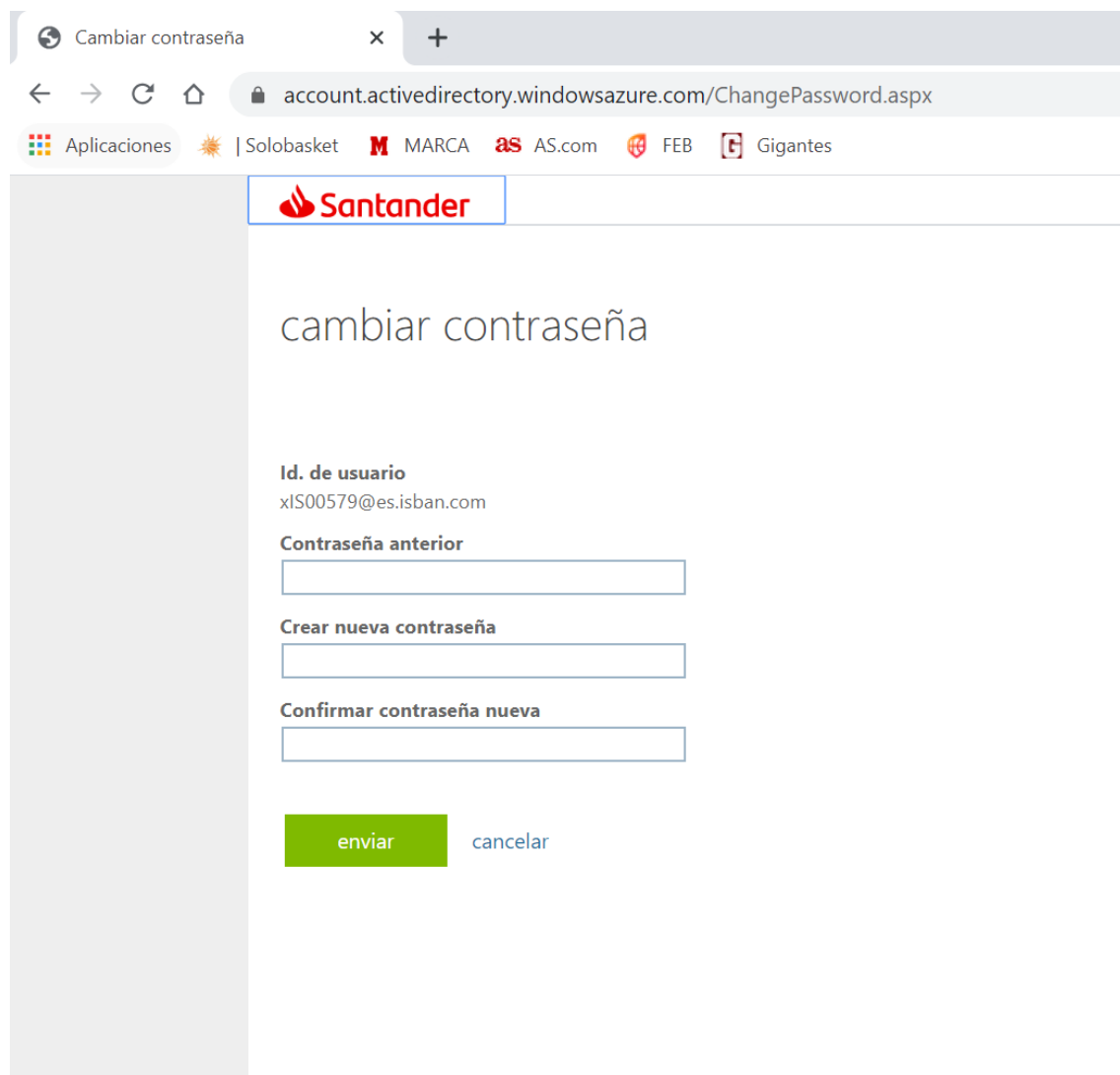
ADMINISTRAR ORGANIZACIONES

Mis inicios de sesión (versión preliminar)

Vea cuándo y dónde ha iniciado sesión y compruebe si hay algo que le parezca sospechoso.

REVISAR LA ACTIVIDAD RECIENTE

Para ello hay que introducir el password actual, dos veces el nuevo password y tras pulsar “enviar” se procederá a actualizar el password:



Cambiar contraseña

account.activedirectory.windowsazure.com/ChangePassword.aspx

Aplicaciones | Solobasket | MARCA | AS.com | FEB | Gigantes

Santander

cambiar contraseña

Id. de usuario
xIS00579@es.isban.com

Contraseña anterior

Crear nueva contraseña

Confirmar contraseña nueva

enviar cancelar

Se recuerda que en la “Intranet” en los accesos directos a herramientas, está disponible la aplicación “myPassword” desde dónde también se puede realizar el cambio de contraseña como lo hemos venido haciendo hasta ahora.

7. FAQs.

¿Qué necesito para acceder? Se requiere tanto del UPN y su contraseña así como un teléfono o correo electrónico.

¿Cuántos métodos se requieren habilitar o configurar? Se recomienda al menos tener 2 métodos habilitados.

He cambiado de teléfono, ¿qué hago? Desde la web de azure en la sección “Información de seguridad” podrá eliminar el método teléfono y volver a configurarlo tal y como se explica en el punto 3 de este documento.

He cambiado de correo electrónico ¿qué hago? Desde la web de azure en la sección “Información de seguridad” podrá eliminar el método correo electrónico y volver a configurarlo tal y como se explica en el punto 3 de este documento.

¿Cuántos teléfonos se pueden configurar? Se permite habilitar el método teléfono vía llamada en dos teléfonos distintos.

Tengo Mensaje de error contraseña incorrecta: En el caso de obtener el error de “Contraseña incorrecta” se deberá solicitar a través de ITSM un reset de password especificando en “Dominio SGT” en la siguiente ruta de ITSM:

CATALOGO DE USUARIO FINAL / Identity & Access Management / LDAP-Domain / Domain – User Reactivation

No carga la página “fs.gsnetcloud”: Se trata de una url pública y por lo tanto en caso de no llegar comprobar que en el fichero host del Windows de su PC no existe esa entrada “fs.gsnetcloud”, en caso de estar informada es necesario eliminarla.

Durante el login salta “error de certificados”: En el caso de obtener el “error de certificados” por favor enviad un Email al Buzon Soporte Intranet Sanglobaltech <soporteintranetsanglobaltech@gruposantander.com>:

Indicando el usuario, una evidencia del error y puntualizar si la prueba se está realizando desde la red del Santander o no.

Tras introducir la contraseña salta el error “No puede acceder a este recurso”: es probable que su navegador tenga iniciada sesión o lo cuenta activa de su empresa aunque no sea consciente. Para ello revisar la sección 2 de este documento.

Estoy bloqueado y ya no sé qué hacer o no puedo avanzar: Se deberá abrir un ticket, indicando el usuario y adjuntando una evidencia del error, a través de ITSM en la siguiente ruta:

- **Tipo:** INCIDENCIA
- **Categoría:** Aplicaciones
- **Subcategoría:** Sistemas de información
- **Entorno:** Producción
- **Aplicación:** Login y Acceso