



Manual de Usuario para el Registro de Datos en el Sistema Multifactor de Office365

	MANUAL DE USUARIO		Código: EPN-DGIP-MU-010
			Versión:001
			Elaborado: 16/05/2019
			Vigencia: 31/12/2023

Tabla de contenido

1	OBJETIVO	4
2	ALCANCE	4
3	DEFINICIONES	4
4	REQUERIMIENTOS TÉCNICOS	4
4.1	REQUERIMIENTOS DE SOFTWARE	4
4.2	CONDICIONES DE USO	4
5	GUIA DE USUARIO	5
5.1.	Administración de la plataforma multifactor de Office365	¡Error! Marcador no definido.

	MANUAL DE USUARIO		Código: EPN-DGIP-MU-010
			Versión:001
			Elaborado: 16/05/2019
			Vigencia: 31/12/2023

NIVELES DE RESPONSABILIDAD

Actividad	Nombre	Cargo	Firma
Elaboración	Ing. Edison Jiménez	Especialista en TICs 3	
Revisión	Ing: Liliana Cordova	Especialista en TICs 3	
Aprobación	Ing. Juan Pablo Ponce	Director de Gestión de la Información y Procesos	

	MANUAL DE USUARIO		Código: EPN-DGIP-MU-010
			Versión:001
			Elaborado: 16/05/2019
			Vigencia: 31/12/2023

CONTROL DE CAMBIOS

Versión	Razones del Cambio	Realizado por	Firma
1.0	Inicial	Ing. Edison Jiménez	

	MANUAL DE USUARIO		Código: EPN-DGIP-MU-010
			Versión:001
			Elaborado: 16/05/2019
			Vigencia: 31/12/2023

1 OBJETIVO

El objetivo del presente documento es presentar una guía al usuario para la inscripción de datos necesarios para el uso de Multifactor en la plataforma Office365.

2 ALCANCE

El presente documento se aplicará en la Escuela Politécnica Nacional, el servicio prestado es destinado para uso del doble factor de autenticación para los miembros de la Escuela Politécnica Nacional.

3 DEFINICIONES

Software: Programas de computadora (que se almacenan y se ejecutan en el hardware de la computadora) y datos asociados (que también se almacenan en el hardware) que se pueden escribir o modificar dinámicamente durante la ejecución.

DGIP: Dirección de Gestión de la Información y Procesos.

Multifactor: Capa de protección adicional a las credenciales tradicionales que permite tener un mayor control de acceso sobre las aplicaciones.

4 REQUERIMIENTOS TÉCNICOS

Los usuarios de la plataforma Office365 deben requerir tener un teléfono móvil para activar y utilizar el multifactor de autenticación.

4.1 REQUERIMIENTOS DE SOFTWARE

Acceso a la plataforma de Office365 mediante un navegador web.

4.2 CONDICIONES DE USO

El uso está limitado solamente a usuarios de la escuela Politécnica Nacional registrados en la plataforma de Office365.

	MANUAL DE USUARIO		Código: EPN-DGIP-MU-010
			Versión:001
			Elaborado: 16/05/2019
			Vigencia: 31/12/2023

5 GUÍA DE USUARIO

5.1. Acceso a la configuración de la plataforma multifactor de Office 365

Abra un navegador de internet e ingrese a la URL: <https://aka.ms/MFASetup>

El sistema le pedirá credenciales de acceso a la plataforma de Office365.

Figura 1. Ingreso en el Sistema

Una vez ingresadas las credenciales el sistema indicará que la organización requiere mas información para garantizar la seguridad de la cuenta, dar clic en “Siguiente”.

Figura 2. Ingreso en el Sistema

	MANUAL DE USUARIO		Código: EPN-DGIP-MU-010
			Versión:001
			Elaborado: 16/05/2019
			Vigencia: 31/12/2023

En la pantalla de “Comprobación de seguridad adicional” ingrese su número de teléfono celular y escoja el método “Llamarme”, dar clic en “Siguiente”.

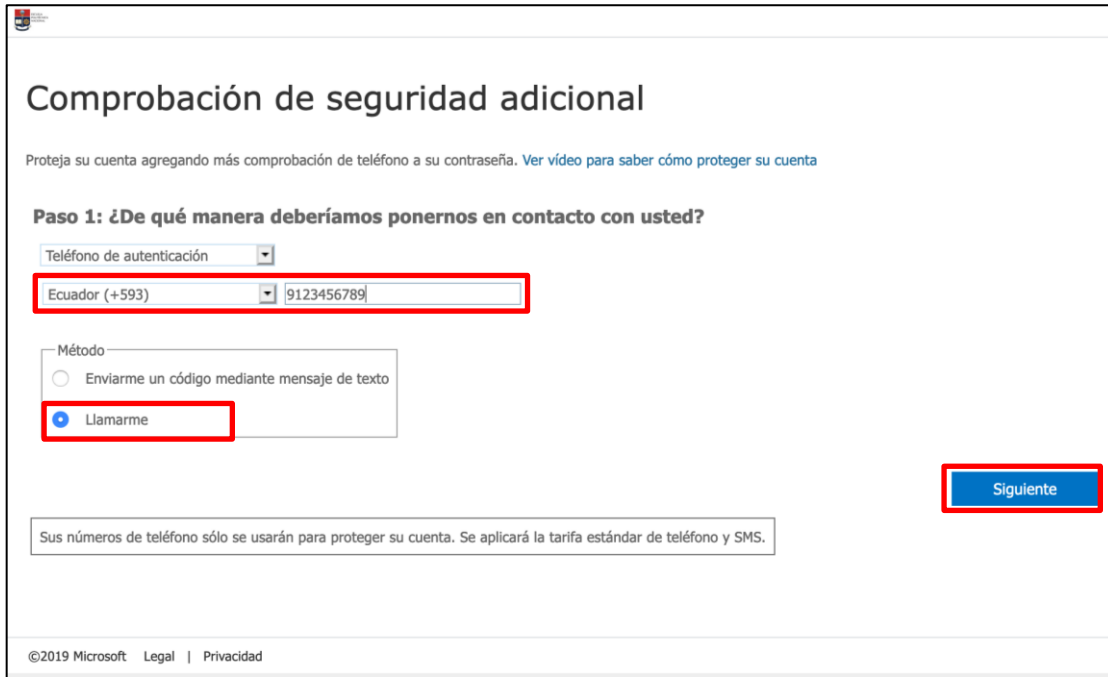


Figura 3. Comprobación de seguridad adicional

El sistema de Office365 llamará al número de teléfono inscrito en el paso anterior, una operadora automatizada se comunicará con Ud. y le solicitará que oprima la tecla almohadilla (#) de su teléfono para que confirme la comprobación de seguridad.



	MANUAL DE USUARIO		Código: EPN-DGIP-MU-010
			Versión:001
			Elaborado: 16/05/2019
			Vigencia: 31/12/2023

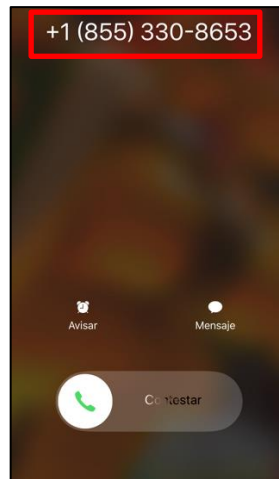


Figura 4. Llamada del sistema Office 365. Confirme la comprobación de seguridad con la tecla almohadilla (#)

Una vez que el sistema Office365 ha recibido la confirmación de la llamada y la acción de oprimir la tecla almohadilla (#), emitirá un mensaje de comprobación correcta. De clic en “Listo”

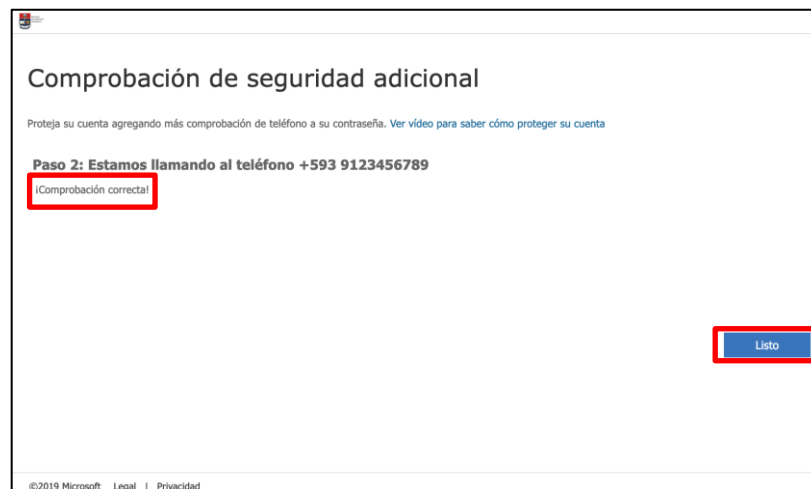


Figura 5. Comprobación de seguridad adicional confirmada.

La siguiente pantalla permite guardar esta configuración. Adicionalmente permite definir la configuración predeterminada para autorizar el acceso a la cuenta de Office365. Las opciones disponibles son: Llamada telefónica, Mensaje de Texto, Código de verificación provisto por la aplicación Microsoft Authenticator, y Aprobación directa con la aplicación Microsoft Authenticator.

	MANUAL DE USUARIO		Código: EPN-DGIP-MU-010
			Versión: 001
			Elaborado: 16/05/2019
			Vigencia: 31/12/2023

5.1.1 Configuración (opcional) de la aplicación Microsoft Authenticator

Importante: Al utilizar la opción de Microsoft Authenticator se requiere mantener una conexión estable de internet para que el aplicativo pueda autorizar el acceso a los aplicativos de Office 365. En caso de no cumplir con este requerimiento, se recomienda mantener la opción de llamada telefónica o SMS.

Microsoft Authenticator es una aplicación móvil disponible para Android y iOS que permite generar tokens, o autorizaciones de acceso multifactor de “un solo toque”. Se recomienda activar la autorización de “un solo toque” con el fin de facilitar el uso de la autenticación multifactor.

Una vez completado el paso de comprobación de seguridad adicional se despliega la pantalla donde se puede activar la aplicación Microsoft Authenticator. Active la opción “Aplicación autenticadora y de Clic sobre “Configurar aplicación autenticadora”.

Figura 5. Activación de configuración de aplicación autenticadora.

	MANUAL DE USUARIO		Código: EPN-DGIP-MU-010
			Versión:001
			Elaborado: 16/05/2019
			Vigencia: 31/12/2023

Siga los pasos indicados para configurar la aplicación móvil. Recuerde que esta aplicación puede ser descargada de la AppStore y de la PlayStore de forma gratuita y se identifica con el nombre “Microsoft Authenticator”



Configurar aplicación móvil

Complete los pasos siguientes para configurar su aplicación móvil.

1. Instale la aplicación Microsoft Authenticator para Windows Phone, Android o iOS.
2. En la aplicación, agregue una cuenta y seleccione "Cuenta profesional o educativa".
3. Examine la imagen siguiente.

 Configurar la aplicación sin notificaciones

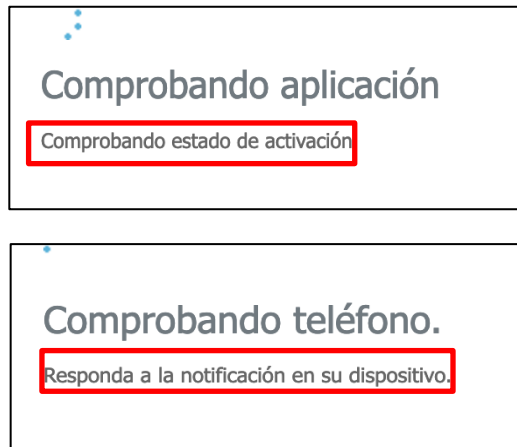
Si no puede examinar la imagen, especifique la información siguiente en la aplicación.
Código: 123 456 789
Dirección URL: <https://cys01pfpad16.phonefactor.net/pad/748634698>

Si la aplicación muestra un código de seis dígitos, elija "Siguiente".

Siguiente cancelar

Figura 6. Pasos para activar la aplicación Microsoft Authenticator.

Una vez que se ha configurado la aplicación de clic en “Siguiente” de la Figura 6. El sistema comprobará la activación, para ello le solicitará dar clic en el botón “Aprobar” de la aplicación móvil Microsoft Authenticator.



Comprobando aplicación

Comprobando estado de activación

Comprobando teléfono.

Responda a la notificación en su dispositivo.

Figura 7. Comprobación de teléfono a través de la aplicación Microsoft Authenticator.

	MANUAL DE USUARIO		Código: EPN-DGIP-MU-010
			Versión:001
			Elaborado: 16/05/2019
			Vigencia: 31/12/2023

Una vez que se haya confirmado la acción de “Aprobar” en la aplicación Microsoft Authenticator el sistema redireccionará a la pantalla donde podrá escoger la opción “Notificarme a través de la aplicación”, adicionalmente, podrá comprobar que ya se encuentre listado su dispositivo móvil, y finalmente deberá dar clic en el botón “Guardar”.



nombre.apellido@epn.edu.ec | ?

Comprobación de seguridad adicional

Al iniciar sesión con su contraseña, ahora también deberá responder desde un dispositivo registrado. De este modo, los hackers tendrán más dificultades para iniciar sesión solo con una contraseña robada. [Ver vídeo para saber cómo proteger su cuenta](#)

¿cuál es su opción preferida?

Se usará esta opción de configuración de forma predeterminada.

Notificarme a través de la aplicación

¿cómo desea responder?

Seleccione y configure una o más de estas opciones. [Más información](#)

☒ Teléfono de autenticación

☐ Teléfono del trabajo

☐ Teléfono de autenticación alternativo

☒ Aplicación autenticadora o token

Aplicación de autenticación - Dispositivo Nombre

Sus números de teléfono sólo se usarán para proteger su cuenta. Se aplicará la tarifa estándar de teléfono y SMS.

©2019 Microsoft Legal | Privacidad

Figura 8. Pantalla con resumen de cambios relacionados a la aplicación Microsoft Authenticator.

Los pasos anteriores le permitirán utilizar la aplicación móvil Microsoft Authenticator para autorizar el acceso a su cuenta de Office365. Sin embargo, el sistema de Multifactor no se habilitará hasta que un administrador de Office 365 de la EPN active esta opción en su cuenta.

	MANUAL DE USUARIO		Código: EPN-DGIP-MU-010
			Versión:001
			Elaborado: 16/05/2019
			Vigencia: 31/12/2023

5.2. Acceso a la cuenta de Office365 con Multifactor activado

Una vez que el administrador de Office 365 haya activado la opción de multifactor para su cuenta, Ud. podrá acceder a la misma ingresando su usuario y contraseña. Adicionalmente, Ud. deberá responder una llamada telefónica, o escribir un código que le llegue a su telefono mediante SMS, o escribir un código de la aplicación Microsoft Authenticator, o aprobar la autenticación directamente en la aplicación Microsoft Authenticator. La opción de respuesta por defecto configurada en los pasos anteriores será la primera en presentarse, pero Ud. puede utilizar las otras opciones disponibles en caso de requerirlo dando clic en la opción “Inicie sesión de otra forma”, se recomienda configurar y activar la aplicación Microsoft Authenticator.

	MANUAL DE USUARIO		Código: EPN-DGIP-MU-010
			Versión:001
			Elaborado: 16/05/2019
			Vigencia: 31/12/2023

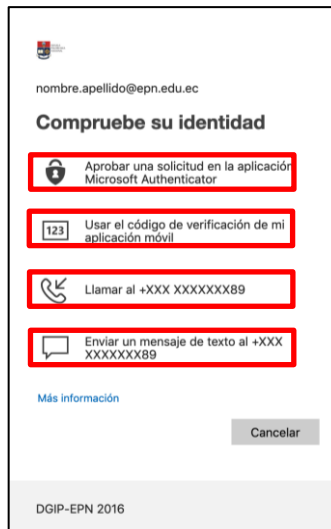


Figura 9. Pantallas de acceso a la cuenta de Office365 utilizando multifactor (Múltiples formas de autorizar el ingreso).

5.2.1 Configuración Outlook con la opción Exchange.

La siguiente configuración es válida para todos los clientes que soporten Exchange Sync.

Abra Outlook y añada una nueva cuenta.

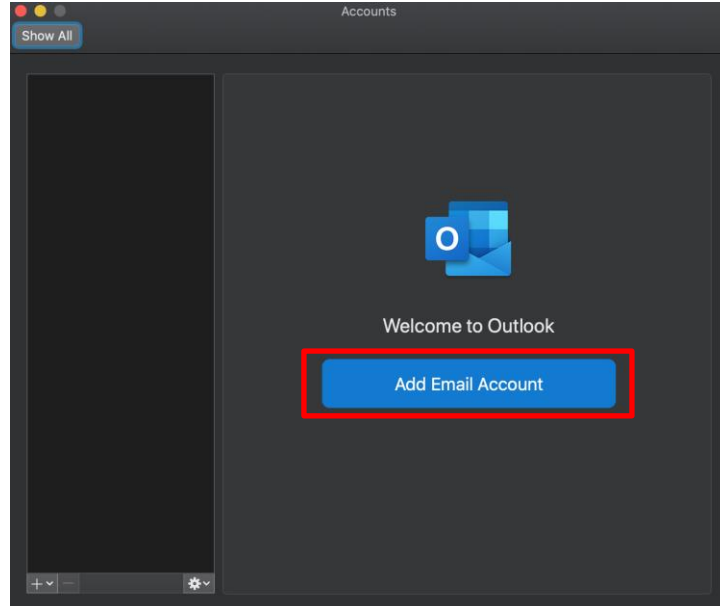


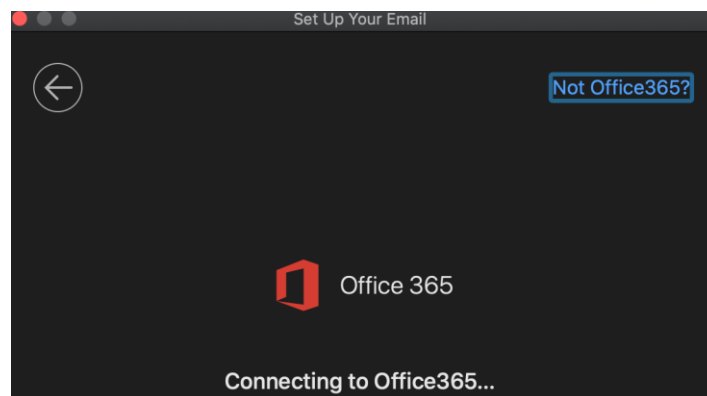
Figura 10. Pantalla de inicio de Outlook.

	MANUAL DE USUARIO		Código: EPN-DGIP-MU-010
			Versión:001
			Elaborado: 16/05/2019
			Vigencia: 31/12/2023

Ingrese la información solicitada.

Figura 11. Ingreso de información en Outlook.

El sistema reconocerá si la cuenta pertenece a Office365 y le mostrará la página de login de la organización. Ingrese sus datos de autenticación en esa pantalla.



	MANUAL DE USUARIO		Código: EPN-DGIP-MU-010
			Versión:001
			Elaborado: 16/05/2019
			Vigencia: 31/12/2023

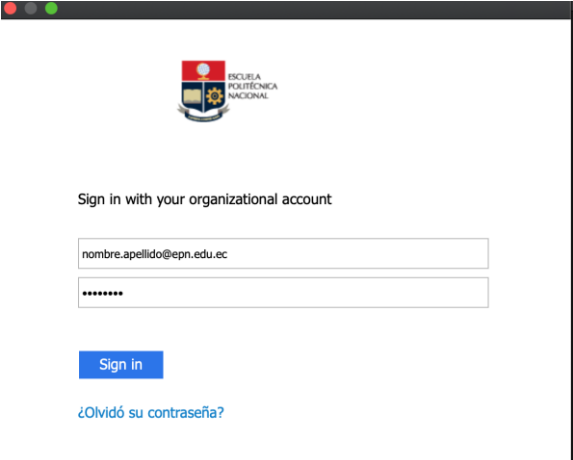


Figura 12. Página de login de la organización.

Para continuar, Office365 le solicitará validar su cuenta mediante el doble factor de autenticación que configuró al inicio de este documento.

Approve sign in request

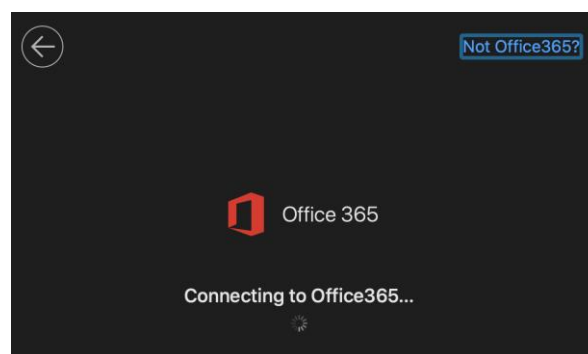
 We've sent a notification to your mobile device.
Please open the Microsoft Authenticator app to respond.

Having trouble? [Sign in another way](#)

DGIP-EPN 2016

Figura 13. Validación de acceso a través del doble factor de autenticación

Finalmente, el Outlook se conectará con Office365 y empezará a sincronizar sus correos, contactos, y calendarios.



	MANUAL DE USUARIO		Código: EPN-DGIP-MU-010
			Versión:001
			Elaborado: 16/05/2019
			Vigencia: 31/12/2023



Figura 14. Sincronización de buzones, contactos y calendarios de Office365 en Outlook

5.2.2 Configuración (opcional) de clave de una sola vida para clientes que no soportan doble factor de autenticación.

En clientes que no soportan la presentación de la pantalla de doble factor, es necesario crear una contraseña efímera de “una sola vida”. Estos clientes generalmente solo soportan el uso de protocolos IMAP(S) o POP(S).

Para este proceso debe ingresar al menú “Mi cuenta”, ubicado en el extremo superior derecho de la pantalla de Office365. Y después, dar clic sobre el menú “Mi cuenta”.

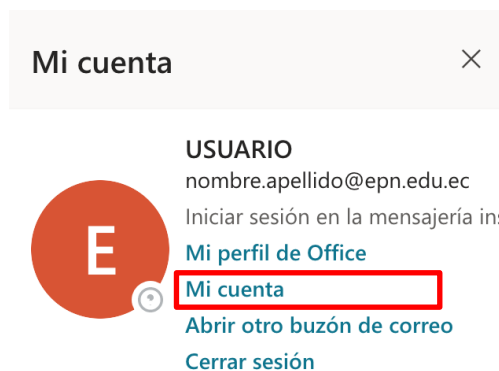


Figura 10. Acceso a menú “Mi cuenta”.

	MANUAL DE USUARIO		Código: EPN-DGIP-MU-010
			Versión:001
			Elaborado: 16/05/2019
			Vigencia: 31/12/2023

El paso anterior le permitirá ingresar al panel de gestión de su cuenta, en donde, Ud. deberá dirigirse al menú “Seguridad y privacidad > Crear y administrar las contraseñas de la aplicación”.

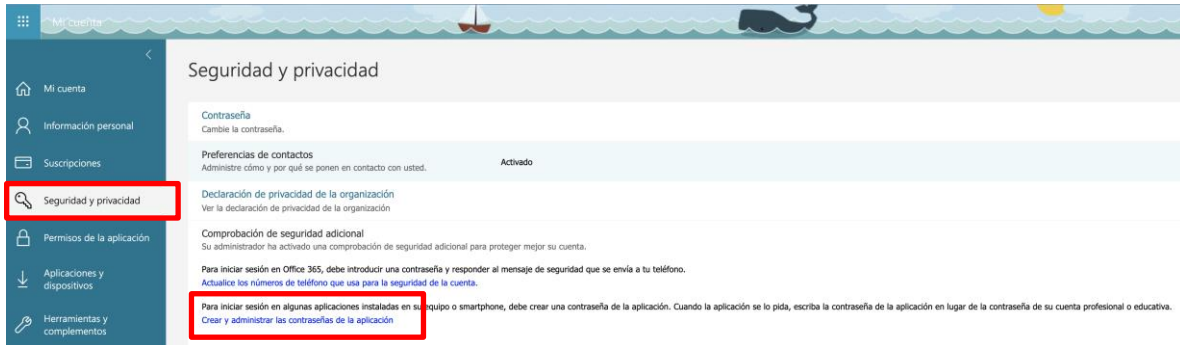


Figura 11. Panel de gestión de la cuenta.

En este paso Ud. podrá crear la contraseña efímera para configurar aquellos clientes de correo que no soporten doble factor de autenticación. Para ello, de clic sobre el botón “Crear”, ingrese un nombre descriptivo de donde va a usar esta clave, y finalmente úse la contraseña generada en el aplicativo de correo que no soporte el doble factor.

comprobación de seguridad adicional contraseñas de aplicación

Para iniciar sesión en Outlook, Lync u otras aplicaciones instaladas en el equipo o en el smartphone, necesitará crear una contraseña de aplicación. Cuando lo solicite la aplicación, escriba la contraseña de aplicación, en lugar de la contraseña de su cuenta profesional o educativa.

Puede usar la misma contraseña de aplicación en varias aplicaciones o crear una contraseña de aplicación nueva para cada aplicación. [¿Cómo consigo que mis aplicaciones funcionen con contraseñas de aplicación?](#)

Nota: si es el administrador de un servicio de Microsoft, le recomendamos no utilizar contraseñas de aplicación.

[Marcar esta página](#)





Crear contraseña de aplicación

Escriba un nombre que le ayude a recordar dónde usa esta contraseña.

Nombre:

	MANUAL DE USUARIO		Código: EPN-DGIP-MU-010
			Versión:001
			Elaborado: 16/05/2019
			Vigencia: 31/12/2023



Su contraseña de aplicación

Nombre: cliente correo telefono

Contraseña: hrlpkdbt86561msck

Nota: esta contraseña no se volverá a mostrar.

[copiar la contraseña en el portapapeles](#)

[cerrar](#)

Figura 12. Contraseña efímera creada.