

Manual de
configuración
segura

LinkedIn Pages



Desde el **Centro de Protección Digital SURA** queremos acompañarte para que tu experiencia en el entorno digital sea confiable y tranquila. Para ello es necesario que con cada paso que des, tu información se encuentre siempre protegida. Por eso, te invitamos a leer y a poner en práctica las siguientes recomendaciones.

Nota: *las instrucciones que encontrarás a continuación están diseñadas para realizarlas en los sitios web de las aplicaciones, es decir, desde un computador. Esto se debe a que la configuración de seguridad de las aplicaciones desde la versión móvil varía según el tipo de celular. Al realizar la configuración desde la web, esta quedará aplicada en tu cuenta para tus dispositivos personales.*

Contenido

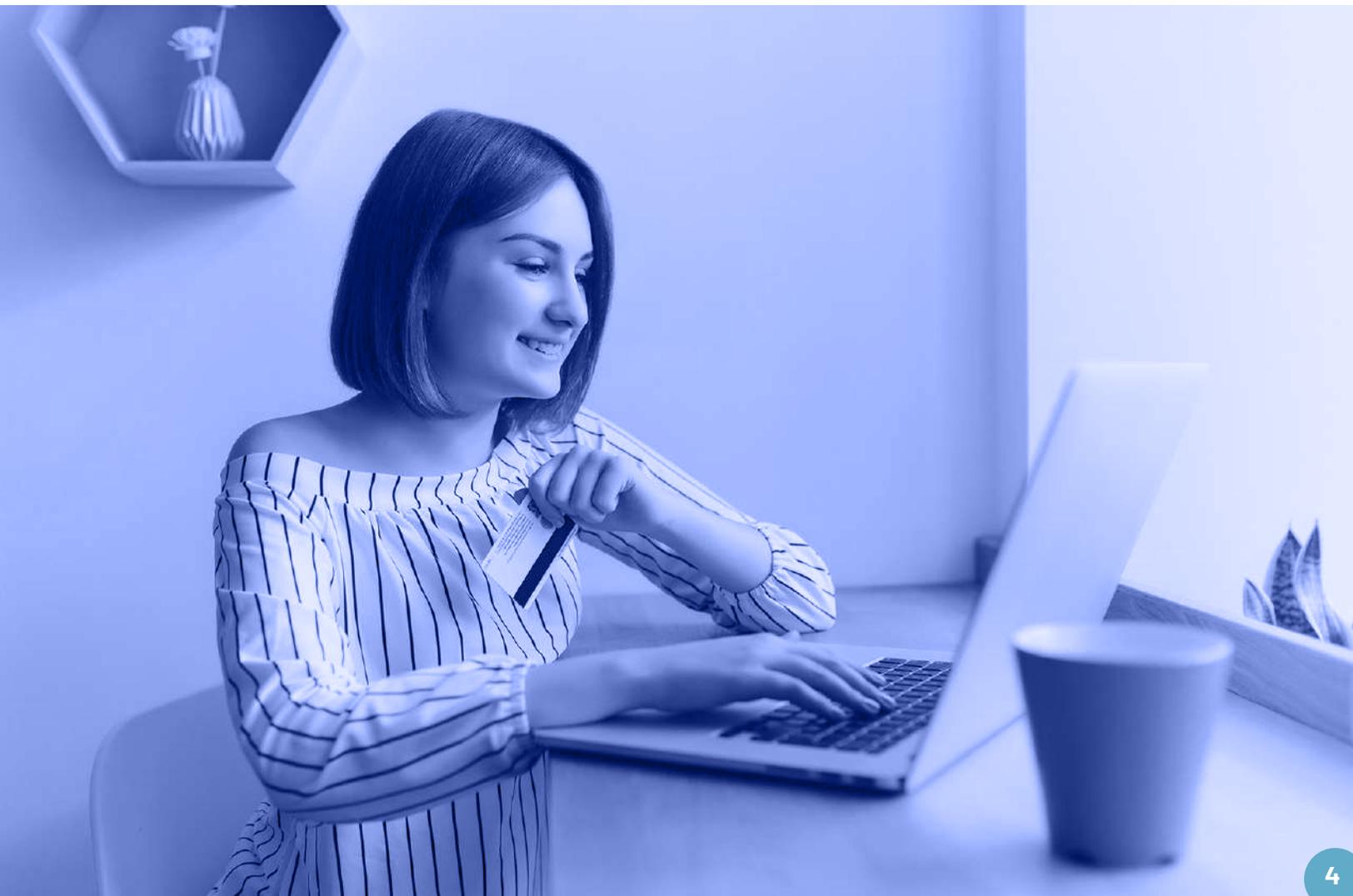
Riesgos asociados a la falta de configuración de seguridad.....	4
Configuración de seguridad.....	5
Configuración segura de cuentas.....	6
Gestión móvil.....	14



Riesgos asociados a la falta de configuración de seguridad

La importancia de configurar de forma segura tu cuenta de Instagram radica en que puedas estar más protegido frente a los siguientes riesgos:

- Cambio no autorizado de imagen o contenido de tu página, el cual podría generar un impacto en la reputación de tu negocio o impedir el adecuado funcionamiento del mismo.
- Robo de información asociada a tus tarjetas de débito/crédito registradas.
- Robo de información asociada a tus clientes que se encuentran en los chats y en tus sistemas de gestión de clientes asociados con LinkedIn.
- Robo de información de tus empleados asociados a LinkedIn.





Configuración de seguridad

A continuación, te presentamos las recomendaciones de seguridad que debes de tener en cuenta para configurar LinkedIn y que te ayudarán a estar más protegido frente a diversas amenazas digitales.

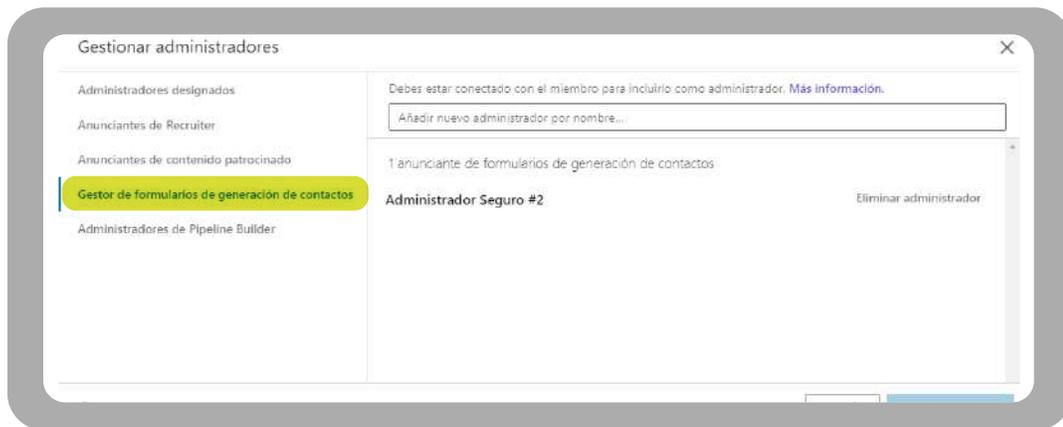
- 1 En tu perfil empresarial haz clic en el icono que muestra tu fotografía o avatar. Una vez allí, selecciona la opción **Empresa**.



- 2 En el panel derecho encontrarás la opción **Herramientas del administrador** para agregar a quienes tendrán acceso como administradores del perfil. Podrás hacerlo, específicamente, en la parte de **Configuración**, haciendo clic en **Gestionar administradores**.

- 3** Una vez allí, tendrás la posibilidad de segregar por roles las funciones que pueden desarrollar tus empleados al interior de la página, desde *Administradores designados*, *Anunciantes de Pipeline Builder* o de *Recruiter*, hasta *Anunciantes de contenido patrocinado* y *Gestor de formularios de generación de contactos*.

Si la configuras correctamente, esta segregación de funciones ayudará a que tu empresa tenga una presencia más segura en LinkedIn.



Configuración segura de cuentas

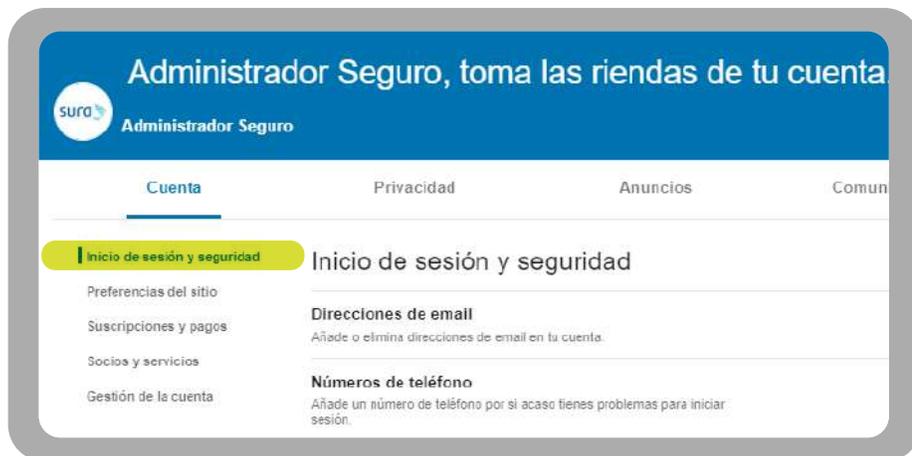
Para usar de forma segura **LinkedIn Pages**, también debes tener presente la configuración de tu cuenta de usuario, pues es con ella que gestionas dichas páginas en la red social. Compartimos contigo las siguientes recomendaciones para que puedas realizar la configuración de forma adecuada.

- 1** En tu perfil empresarial, haz clic en el icono que muestra tu fotografía o avatar. Una vez allí, selecciona la opción **Ajustes y privacidad**.



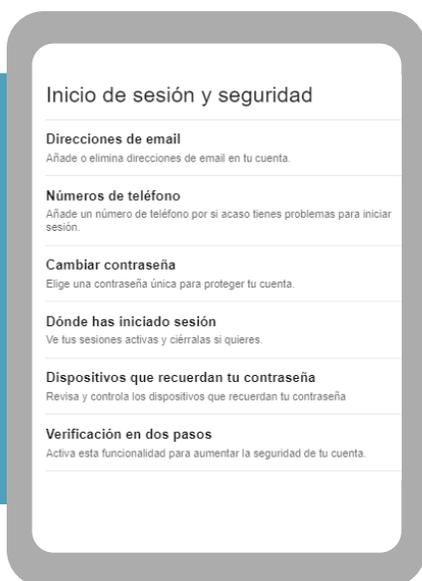
2 Haz clic en la opción **Cuenta**.

3 Navega el menú del costado izquierdo y dirígete a la opción **Inicio de sesión y seguridad**.



LinkedIn ofrece usabilidad y configuración de opciones seguras, guardando tu información con un solo correo electrónico y número celular. Nuestra recomendación es que evites ingresar información adicional de tu empresa para no exponerla en caso de que la red social sea objeto de un ataque cibernético. En ese orden de ideas, te sugerimos mantener un único correo electrónico registrado.

4 Ahora puedes configurar cada una de las opciones. Para comenzar, haz clic en **Direcciones de email**:



A. Si quieres agregar un nuevo correo electrónico corporativo, haz clic en **Añadir dirección de correo electrónico**.

B. Si quieres intercambiar el correo principal, ubícate sobre el que quieres asignar y haz clic en la opción **Seleccionar como principal**.

C. Si quieres eliminar un correo electrónico, haz clic en **Eliminar**.

En el caso del número celular, este es utilizado por LinkedIn como dato de búsqueda para que algún contacto pueda ubicarte. Además, con él se lleva a cabo la verificación en dos pasos. Te recomendamos realizar la siguiente configuración.

- 5** Agrega tu número telefónico corporativo, haciendo clic en **Números de teléfono**.
- A** Si quieres agregar un nuevo número de teléfono, selecciona la opción **Añadir número de teléfono**.
- B** Si quieres modificar el número de teléfono principal, ubícate sobre el que quieres asignar y haz clic en la opción **Hacer de el número principal**.
- C** Si quieres eliminar un número de teléfono, haz clic en **Eliminar**.

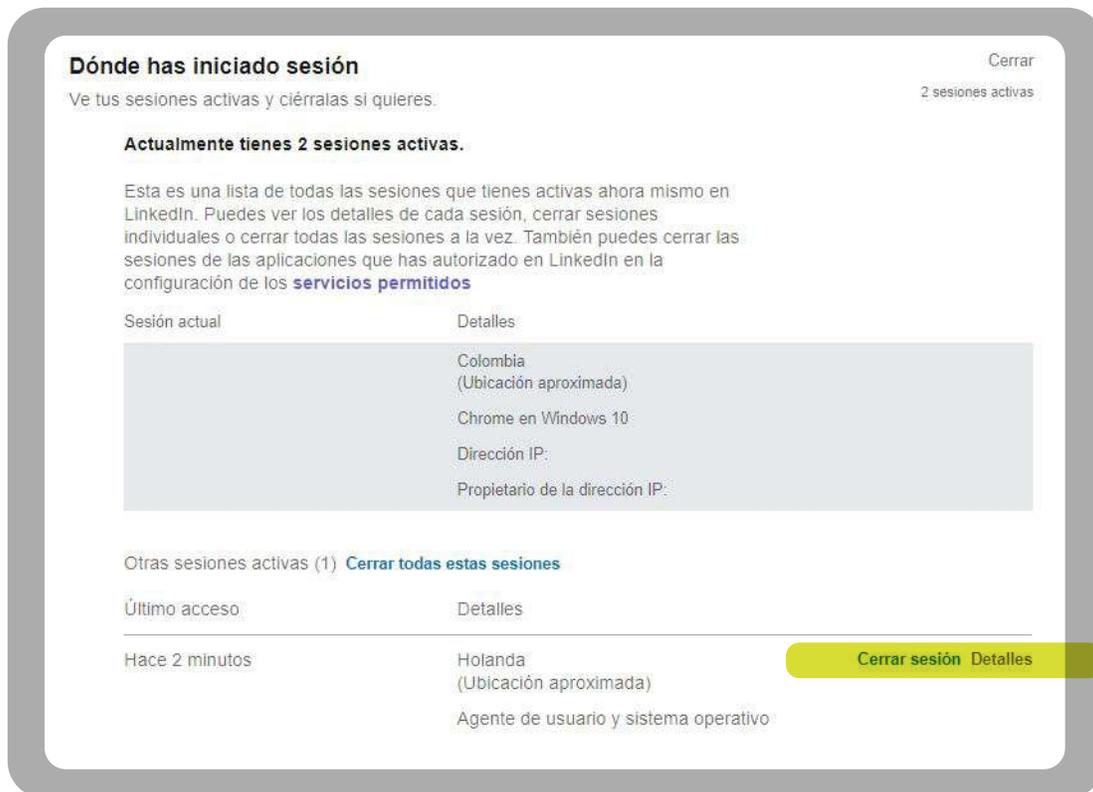
The screenshot shows a user interface for managing phone numbers. At the top left, there is a yellow header with the text "Números de teléfono". To the right of this header, there are two links: "Cerrar" and "1 número de teléfono". Below the header, there is a sub-header "Números de teléfono que has añadido". Underneath, there is a list of phone numbers. The first entry is "CO +57 NÚMERO DE TELÉFONO #1". To the right of this entry are two links: "Hacer de el número principal" and "Eliminar". Below the list, there is a checkbox labeled "Utilizar para restablecer la contraseña" which is checked. At the bottom of the interface, there is a link "Añadir número de teléfono".

Te recomendamos validar la calidad de tu contraseña actual y redefinirla en caso de que la encuentres inadecuada, teniendo en cuenta nuestras recomendaciones de seguridad. Para conocerlas, puedes consultar nuestra *Guía para construcción y administración segura de contraseñas*. [Clic aquí](#)

- 6** Para proceder con la actualización a tu contraseña, haz click en **Cambiar contraseña** y diligencia los campos introduciendo la contraseña actual y la nueva.

The screenshot shows a form for changing a password. The title is "Cambiar contraseña". Below the title, there is a sub-header "Elige una contraseña única para proteger tu cuenta." and a instruction "Escoge una contraseña que sea difícil de descifrar." There are three input fields: "Escribe tu contraseña actual.", "Escribe tu contraseña nueva.", and "Vuelve a escribir tu contraseña nueva." Below the input fields, there is a checkbox labeled "Solicita que todos los dispositivos inicien sesión con la nueva contraseña" which is checked. At the bottom of the form, there is a "Guardar" button.

- Una vez actualizada, es hora de validar en tiempo real en cuáles dispositivos está activa tu cuenta. ¡Recuerda monitorearla constantemente! Para hacerlo, selecciona la opción **Dónde has iniciado sesión**.
- Verifica allí los dispositivos y ciudades donde se encuentra activa tu sesión. Si alguna de estas resulta sospechosa, haz clic en **Cerrar sesión**.

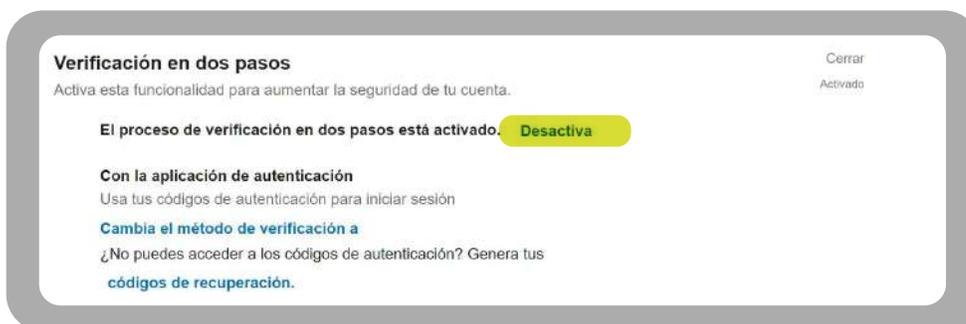


- Por último, haz clic en **Verificación en dos pasos**. Al activar la verificación en dos pasos o factor de doble autenticación, aumentarás el nivel de seguridad de tu cuenta. Esta se lleva cabo por medio de un SMS que llega al celular que ingresaste y que contiene un número de 6 dígitos.

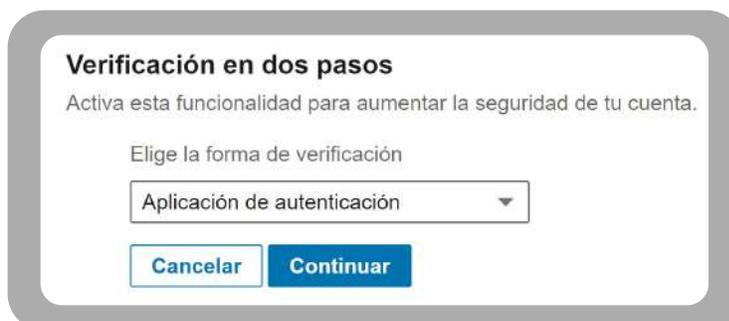
Cada vez que quieras entrar a tu cuenta de LinkedIn necesitarás tu contraseña y un código de verificación. No obstante, en la actualidad se han detectado vulnerabilidades asociadas a *SIM swapping* (duplicación de SIM), que permiten burlar este método. Por esta razón, te recomendamos utilizar un segundo paso alternativo, activando una aplicación de autenticación en tu teléfono celular como Google Authenticator o Microsoft Authenticator.

10

Haz clic en la opción **Activa**, para realizar el proceso de verificación en dos pasos y aumentar tu nivel de seguridad en LinkedIn.



Una vez selecciones esta opción, LinkedIn te pedirá seleccionar la forma de verificación. Haz clic en **Aplicación de autenticación** y después en **Continuar**. A continuación, se te solicitará ingresar nuevamente la contraseña para validar la actualización. Introdúcela y haz clic en el botón **Hecho**.

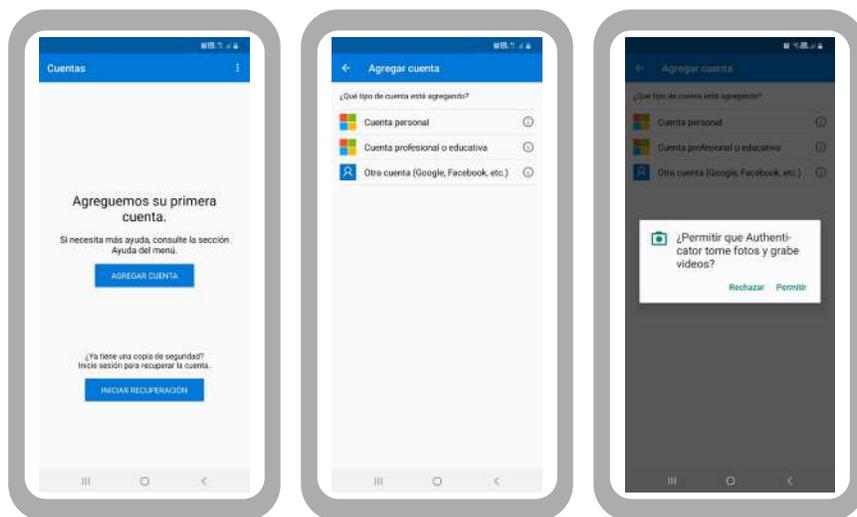


Se habilitará la siguiente pantalla:



En el mercado existen diferentes opciones gratuitas. Procura buscarlas en las tiendas oficiales como Play Store para Android, Apple Store para iOS y Microsoft Store para Windows. Descarga la aplicación seleccionada en tu celular, ábrela y completa los siguientes pasos (en este ejemplo usaremos Microsoft Authenticator):

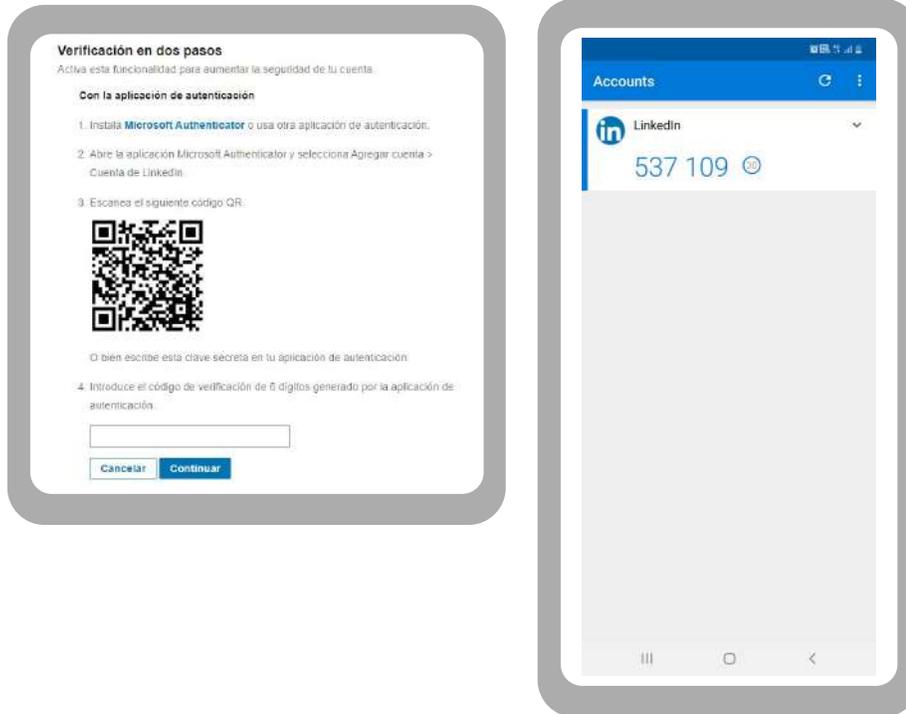
- A** Haz clic sobre el botón **Agregar cuenta**.
- B** Selecciona la opción **Otra cuenta** (Google, Facebook, etc.).
- C** Otorga los permisos a Microsoft Authenticator para la utilización de la cámara, esto con el fin de escanear el código QR (ver más adelante).



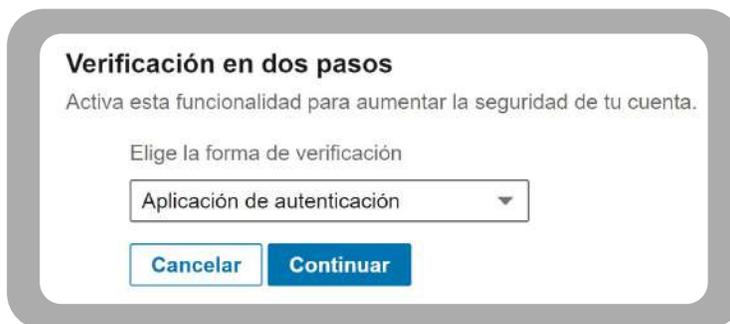
- D** Escanea el código QR que estás viendo en la pantalla de tu computador.



- E** Ingresa en los campos habilitados el código de confirmación que aparece directamente en la aplicación. Luego, haz clic en **Continuar**:



- 11** Una vez concluido el proceso, verás un mensaje indicando la correcta configuración del proceso de verificación en dos pasos.



A partir de este momento, cada vez que inicies sesión en tu cuenta de LinkedIn, se te solicitará la autenticación en dos pasos como se muestra a continuación:
Ingresa a tu cuenta de LinkedIn con tu usuario y contraseña actual: <https://www.linkedin.com/>



¡Te damos la bienvenida de nuevo!

¿Te vas a perder tu siguiente gran oportunidad? Inicia sesión para estar al día de tu entorno profesional.

Correo electrónico o teléfono

Contraseña Ver

Iniciar sesión

[¿Has olvidado tu contraseña?](#)

LinkedIn solicitará el código de autenticación generado por la aplicación previamente instalada y configurada en tu teléfono celular. Ingresa el código y haz clic en **Enviar** para iniciar sesión en tu cuenta.



Verificación en dos pasos
Activa esta funcionalidad para aumentar la seguridad de tu cuenta.

Con la aplicación de autenticación

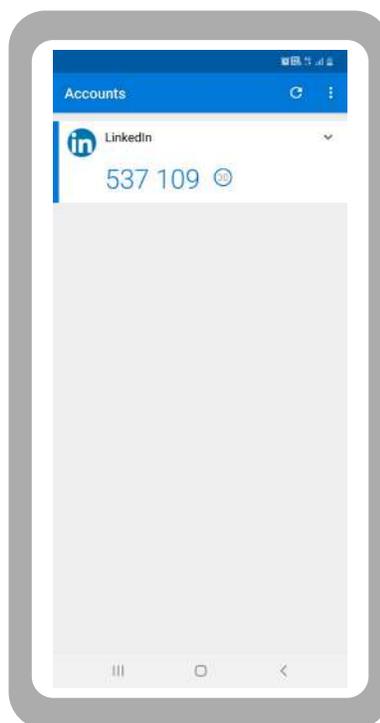
1. Instala **Microsoft Authenticator** o usa otra aplicación de autenticación.
2. Abre la aplicación Microsoft Authenticator y selecciona Agregar cuenta > Cuenta de LinkedIn.
3. Escanea el siguiente código QR:



O bien escribe esta clave secreta en tu aplicación de autenticación:

4. Introduce el código de verificación de 6 dígitos generado por la aplicación de autenticación:

Cancelar Continuar



Accounts

LinkedIn

537 109



Gestión móvil

Al momento de gestionar tu LinkedIn con tu celular, puedes hacerlo desde las apps que LinkedIn ha destinado para ello, como son: **LinkedIn, Recruiter, Sales Navigator y Elevate**. Al momento de descargarlas en tu móvil, hazlo desde tiendas oficiales como App Store, Google Play o Galaxy Store. Esto es de gran importancia para que evites descargar softwares maliciosos que desde otras tiendas pudieran agregarse a estas apps.

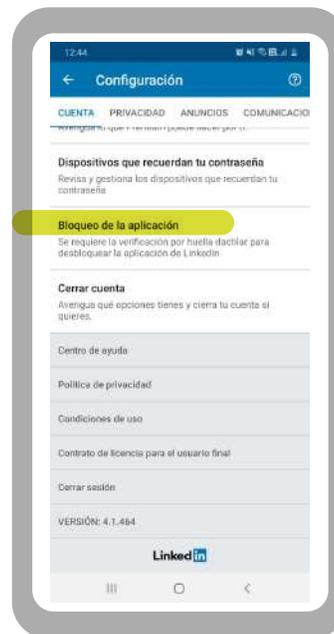
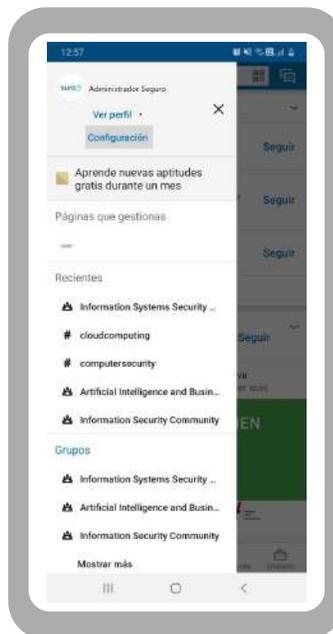
Algunas recomendaciones generales:

- Procura mantener tus credenciales sin compartir con algún empleado u otra persona.
- Cuando accedas a la gestión de tu cuenta de LinkedIn, hazlo desde redes de confianza como la de tu casa o la de tu celular. Evita el uso de redes públicas de centros comerciales o parques.
- Mantén actualizada la aplicación de LinkedIn, de manera que personas malintencionadas no puedan aprovecharse de las brechas de seguridad en versiones desactualizadas.

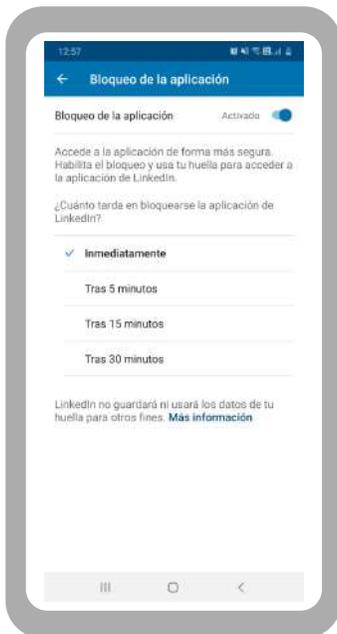


1 Al interior de tu aplicación móvil puedes aumentar el nivel de seguridad, habilitando el ingreso al aplicativo a través de huella dactilar. Para activarlo, sigue esta ruta:

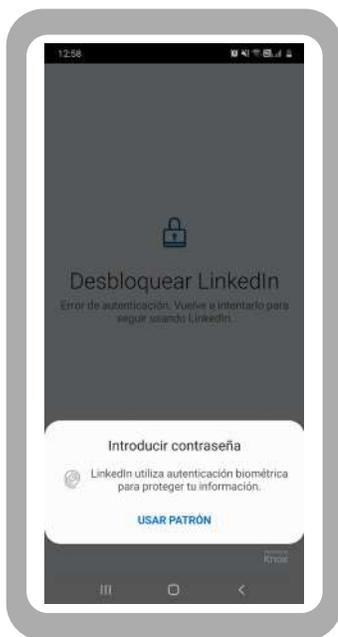
- > **Configuración**
- > **Cuenta**
- > **Bloqueo de la aplicación.**



2 Una vez allí, activa el bloqueo de la aplicación por medio de huella dactilar y especifica el tiempo en que dicho bloqueo funcionará luego de haber salido de la aplicación.



3 Con las configuraciones anteriores, ya deberías tener la protección habilitada. La próxima vez que inicies sesión desde el aplicativo, verás la siguiente pantalla:



Ya has finalizado la configuración segura de tu cuenta de LinkedIn. Gracias por atender nuestras recomendaciones para proteger tu identidad e información, y así evitar ser víctima de fraude digital.

Centro de Protección Digital SURA

SURA, conectado con tu seguridad para que no te desconectes.

[Conoce más aquí](#)

