



Argentina Cibersegura®

una iniciativa de ESET®

Realizado por: 



**Guía de doble  
autenticación**

### 1. Introducción a la Doble Autenticación:

¿Qué es?	4
Ataques a las contraseñas	6
Fuerza bruta	6
Malware	6
Phishing	6
Ataques a servidores	6

### 2. Cómo configurar la Doble Autenticación en los siguientes servicios:

Facebook	10
Twitter	11
LinkedIn	12
Google (Gmail)	13
Apple	14

### 3. Conclusión

15

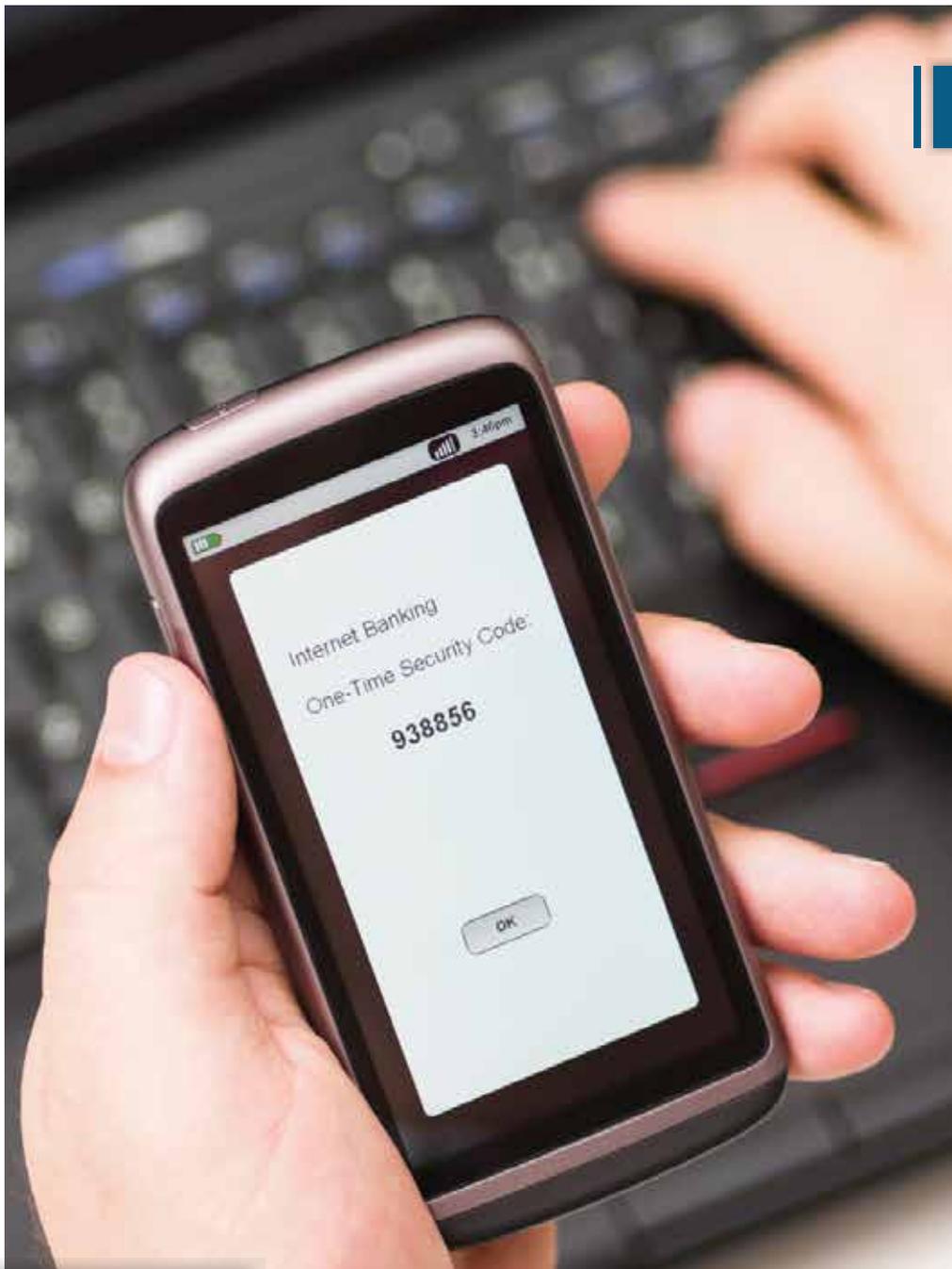


## INTRODUCCIÓN

En la actualidad, la mayoría de las personas utilizan servicios que requieren de credenciales de acceso, es decir, un nombre de usuario y contraseña para poder ingresar a sitios o servicios. En esta línea, la clave actúa como una llave digital que le permite a un usuario identificarse en el sistema para poder acceder a su información. De este modo, dicha contraseña protege los datos privados del acceso no autorizado por parte de terceros.

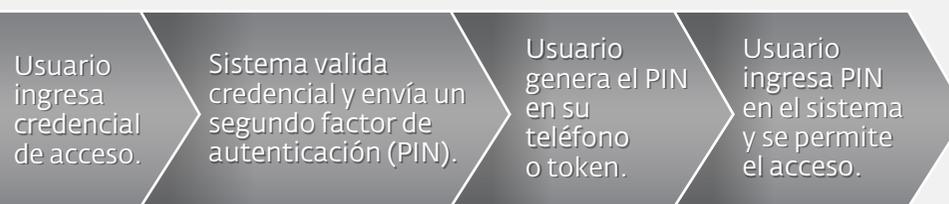
Sin embargo, el aumento de ataques informáticos sumado a las conductas inseguras de las personas, como el uso de contraseñas débiles e iguales en varios servicios, hacen necesario utilizar métodos de autenticación complementarios más robustos. A raíz de esto, muchas empresas están implementando la doble autenticación.

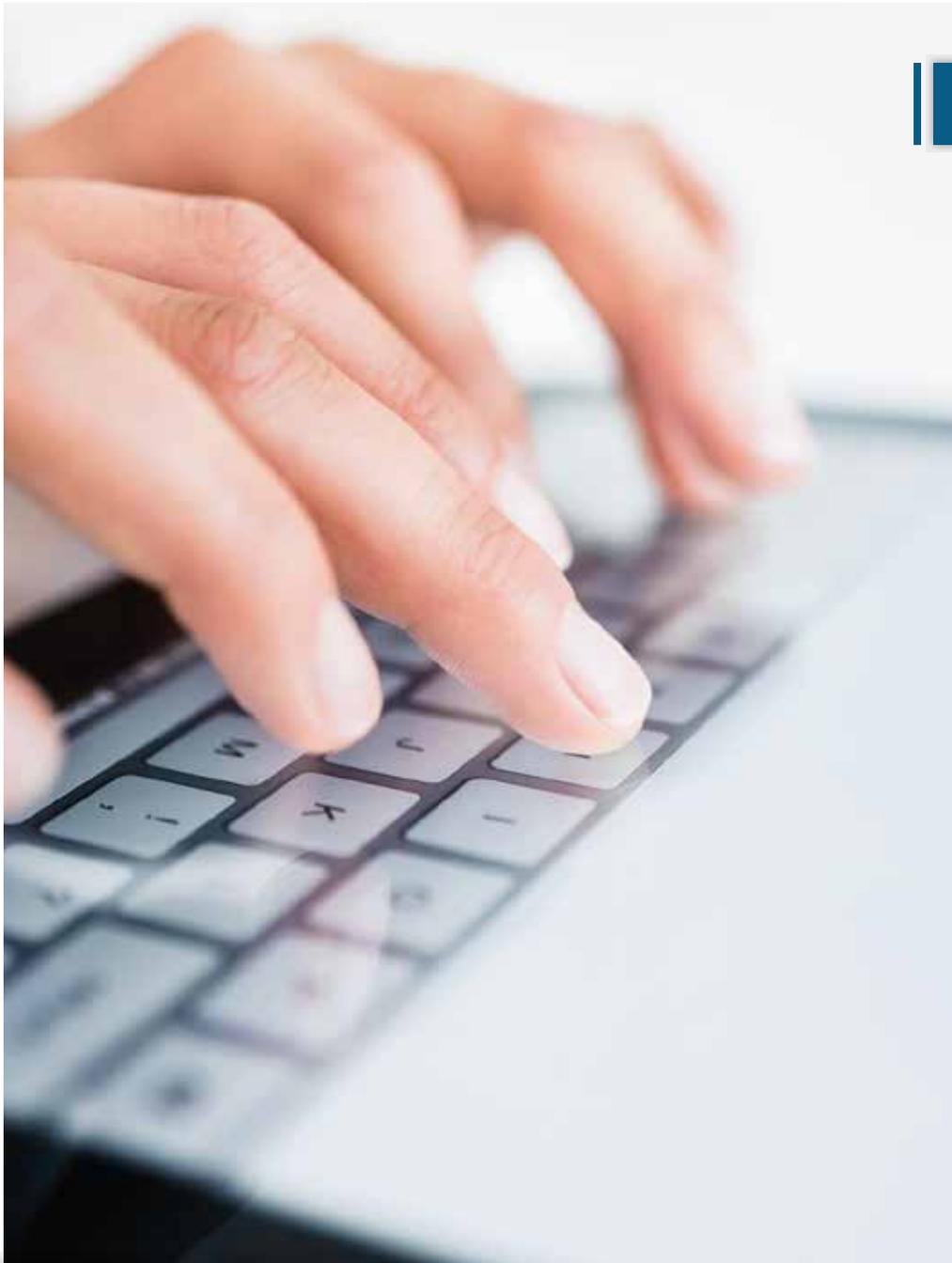
Esta guía tiene como objetivo, explicar qué es la doble autenticación y el modo de activarla en los servicios más populares como Gmail, Facebook, Twitter y otros.



## ¿QUÉ ES LA DOBLE AUTENTICACIÓN?

La doble autenticación se trata de un sistema que complementa la autenticación tradicional en los servicios. En otras palabras, además de requerir un nombre de usuario y contraseña, solicita el ingreso de un segundo factor de autenticación, como por ejemplo, un código de seguridad. Generalmente, este código se genera en un dispositivo del usuario como un teléfono celular o token. Luego, la persona debe ingresarlo para poder validarse en el sistema. El siguiente esquema muestra el funcionamiento de la doble autenticación:





## FACTORES DE AUTENTICACIÓN

Un sistema de doble autenticación es aquel que utiliza dos de los tres factores de autenticación que existen para validar al usuario. Estos factores pueden ser:

- Algo que el usuario sabe (conocimiento), como una contraseña.
- Algo que el usuario tiene (posesión), como un teléfono o token que le permite recibir un código de seguridad.
- Algo que el usuario es (inherencia), o sea, una característica intrínseca del ser humano como huellas dactilares, iris, etc.

Por lo general, los sistemas de doble autenticación suelen utilizar los factores conocimiento (nombre de usuario y contraseña) y posesión (teléfono o token para recibir código de seguridad).

## ATAQUES INFORMÁTICOS QUE ROBAN CONTRASEÑAS

A continuación, se explican los cuatro tipos de amenazas informáticas que utilizan los cibercriminales para vulnerar contraseñas:



### **FUERZA BRUTA:**

software que utiliza un "diccionario" cargado de contraseñas comúnmente utilizadas, con el objetivo de descifrar la clave de la víctima a través de comparaciones y pruebas sucesivas.



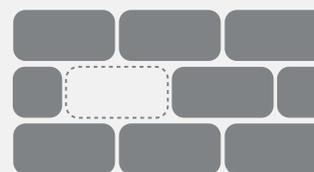
### **MALWARE (CÓDIGO MALICIOSO):**

programa diseñado para realizar diversas acciones maliciosas, como el robo de contraseñas y credenciales de acceso.



### **PHISHING:**

falsificación de una entidad de confianza, como bancos y redes sociales, por parte de un cibercriminal. De este modo, el atacante busca manipular a la víctima para que ingrese sus credenciales de acceso en un sitio falso pero que luce idéntico al original.

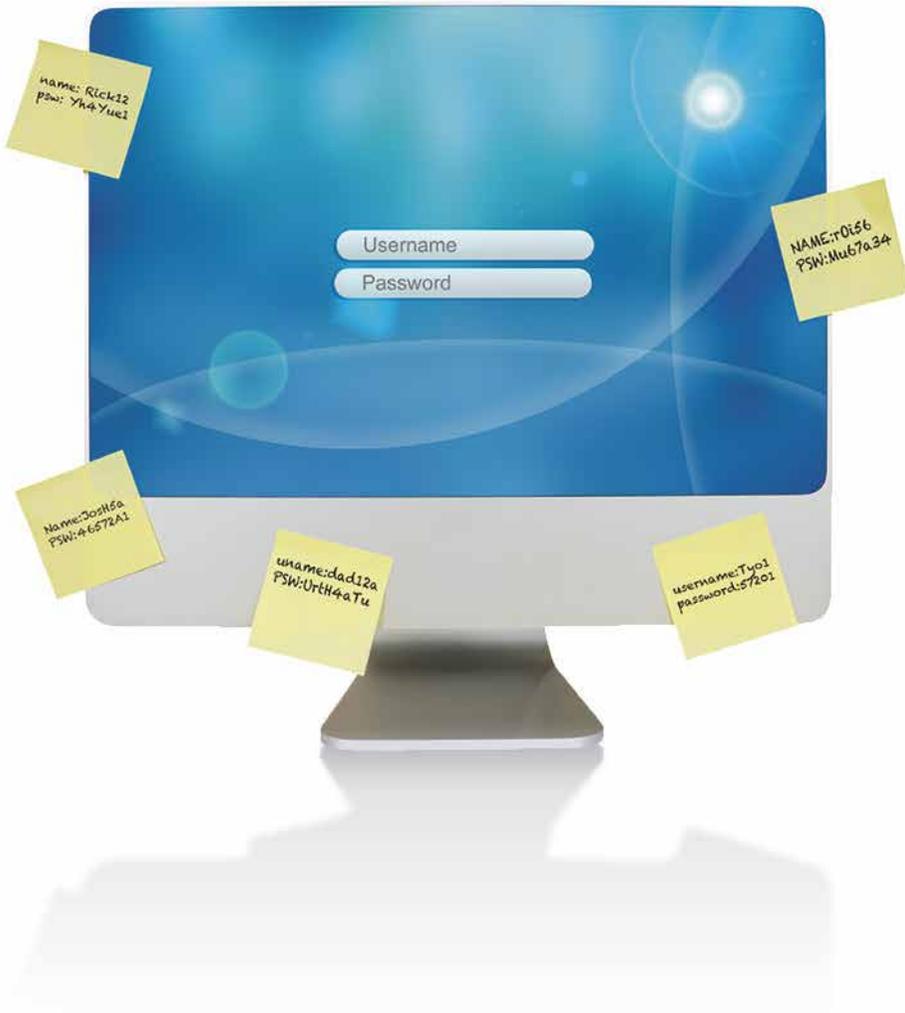


### **ATAQUES A SERVIDORES:**

vulneración de un sistema informático utilizado para almacenar la base de datos de credenciales de acceso de un determinado servicio.

## CONDUCTAS INSEGURAS DEL USUARIO CON LAS CONTRASEÑAS

Al igual que las amenazas explicadas anteriormente, una conducta insegura por parte del usuario también contribuye a que una contraseña pueda ser vulnerada. En este sentido, el uso de una clave única para varios servicios, que sea fácil de adivinar, que se encuentre escrita en documentos, que sea compartida, entre otras alternativas; facilita considerablemente que los cibercriminales puedan obtener acceso a la información del usuario.



## DOBLE AUTENTICACIÓN Y MITIGACIÓN DE ATAQUES

Como se pudo observar en las páginas anteriores, son diversas las amenazas y conductas que pueden contribuir a que un usuario se vea afectado por el robo de una o varias contraseñas, no obstante, la doble autenticación permite mitigar considerablemente tales amenazas. Por ejemplo, un cibercriminal podría robar una clave utilizando un código malicioso, y si bien dicha contraseña sería obtenida, el atacante no podría lograr el acceso al sistema debido a que desconocería el segundo factor de autenticación, es decir, el código que se envía al teléfono o token del usuario. El siguiente esquema expone cómo la doble autenticación logra mitigar ataques que roban contraseñas:

Cibercriminal roba contraseña utilizando alguna amenaza informática.

Luego, ingresa la credencial robada e intenta acceder al sistema.

Sistema solicita el segundo factor de autenticación.

Atacante no tiene acceso al segundo código. Sistema prohíbe el ingreso.





## ¿CÓMO ACTIVAR LA DOBLE AUTENTICACIÓN EN SERVICIOS WEB?

Debido a diversos ataques que involucran el robo de contraseñas, y que han afectado a importantes empresas, muchos servicios ofrecen la posibilidad de activar la doble autenticación de forma gratuita. Es importante destacar que este tipo de protección no viene configurada por defecto, por lo tanto, el usuario deberá modificar algunos parámetros para activarla. En las siguientes páginas se detallarán las instrucciones necesarias para configurar este sistema de protección en Facebook, Twitter, LinkedIn, Google y Apple.



Para activar la doble autenticación en Facebook se debe seguir este procedimiento:

- 1) Hacer clic sobre el icono en forma de rueda dentada ubicado en la parte superior derecha del sitio. Posteriormente hacer clic en “Configuración de la cuenta”.
- 2) Luego, hacer clic sobre la opción **Seguridad** que aparece en el costado izquierdo de la página.
- 3) Allí se debe activar la opción **Solicitar un código de seguridad para acceder a mi cuenta desde navegadores desconocidos**, tal como aparece en la siguiente captura:



En el caso de Facebook, el segundo código de seguridad será solicitado cada vez que el usuario ingrese al servicio utilizando un dispositivo desconocido, es decir, un equipo que no ha sido utilizado anteriormente para acceder a la red social.



Para activar la doble autenticación en Twitter se debe seguir este procedimiento:

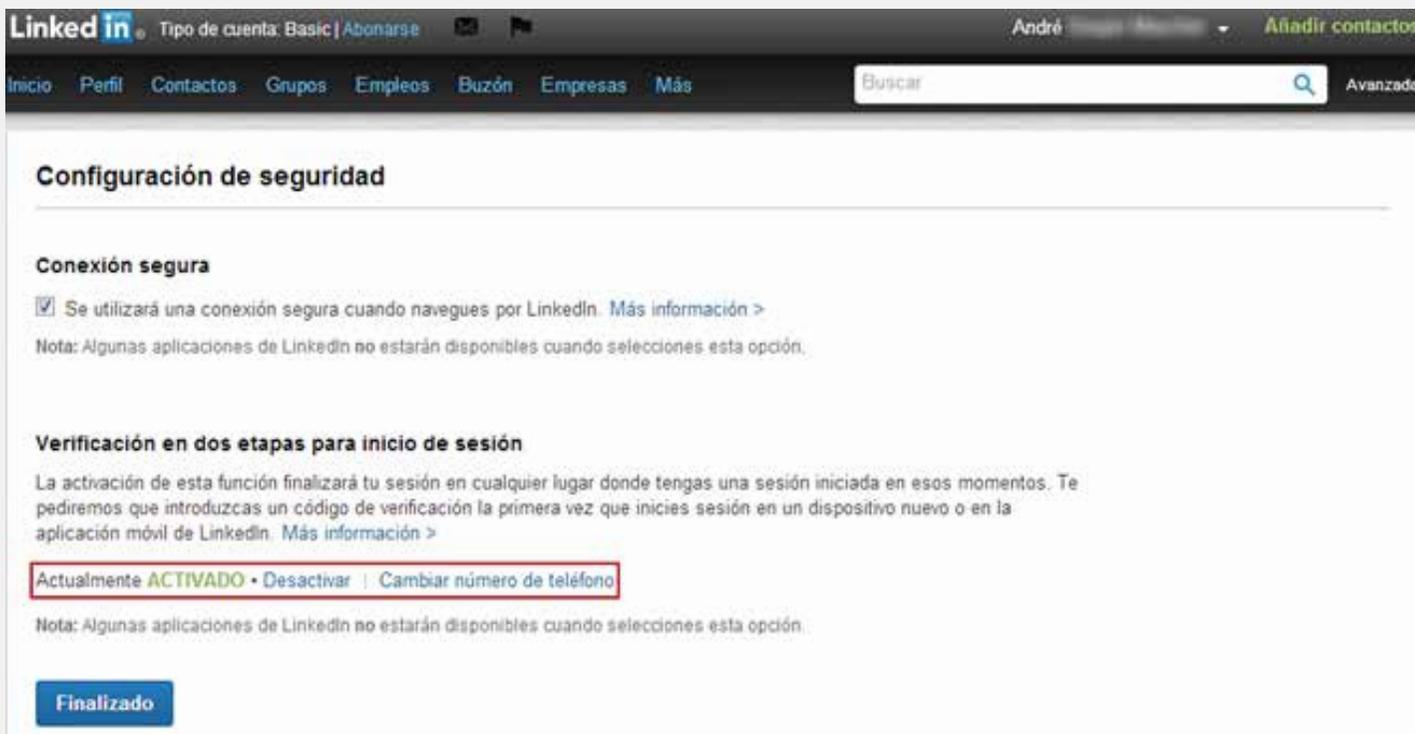
- 1) Hacer clic sobre el icono en forma de rueda dentada ubicado en la parte superior derecha del sitio. Posteriormente hacer clic en **Configuración**.
- 2) En la sección **Seguridad y privacidad** activar la opción **Enviar peticiones de verificación de inicio de sesión a mi teléfono**:



- 3) Para poder activar dicha opción el usuario deberá asociar un número de teléfono con la cuenta de Twitter. Esto puede realizarse haciendo clic en el enlace **añadir un teléfono**.

Para activar la doble autenticación en LinkedIn se debe seguir este procedimiento:

- 1) Acceder al menú de configuración haciendo clic en el nombre de usuario que aparece en el costado superior derecho de la página. En el menú, hacer clic sobre "Configuración".
- 2) En la sección de configuración se debe acceder a la pestaña "Cuenta" y luego hacer clic en "Gestionar configuración de seguridad".
- 3) Luego activar la opción "Verificación en dos etapas para inicio de sesión":



The screenshot shows the LinkedIn 'Configuración de seguridad' (Security Settings) page. At the top, the user's name 'André' and 'Añadir contactos' are visible. The navigation bar includes 'Inicio', 'Perfil', 'Contactos', 'Grupos', 'Empleos', 'Buzón', 'Empresas', and 'Más'. A search bar is present with the text 'Buscar' and a magnifying glass icon. The main content area is titled 'Configuración de seguridad' and contains two sections: 'Conexión segura' and 'Verificación en dos etapas para inicio de sesión'. The 'Conexión segura' section has a checked checkbox and the text 'Se utilizará una conexión segura cuando navegues por LinkedIn. Más información >'. Below it is a note: 'Nota: Algunas aplicaciones de LinkedIn no estarán disponibles cuando selecciones esta opción.' The 'Verificación en dos etapas para inicio de sesión' section has a description: 'La activación de esta función finalizará tu sesión en cualquier lugar donde tengas una sesión iniciada en esos momentos. Te pediremos que introduzcas un código de verificación la primera vez que inicies sesión en un dispositivo nuevo o en la aplicación móvil de LinkedIn. Más información >'. Below the description, the status is 'Actualmente ACTIVADO' with a red box around it, followed by 'Desactivar' and 'Cambiar número de teléfono'. A final note is present: 'Nota: Algunas aplicaciones de LinkedIn no estarán disponibles cuando selecciones esta opción.' At the bottom left of the page is a blue button labeled 'Finalizado'.



Para activar la doble autenticación en Gmail se debe seguir este procedimiento:

- 1) Ir al botón en forma de rueda dentada (ubicado en el costado superior derecho) y presionar sobre "Configuración".
- 2) Se debe hacer clic en la pestaña "Cuentas" y luego sobre el enlace "Otra configuración de la cuenta de Google":



- 3) Allí presionar sobre "Seguridad" y luego hacer clic en el botón "Configuración" o "Editar" que aparece en la sección Verificación en dos pasos que aparece casi al final de la página:





Para activar la doble autenticación en Apple se debe seguir este procedimiento:

- 1) Ingresar al portal Mi ID de Apple. Allí, presionar el botón "Administra tu ID de Apple" que aparece en la parte derecha del sitio.
- 2) Se deberá iniciar sesión utilizando las credenciales de acceso y presionando sobre el botón "Conectarse".
- 3) Una vez que el usuario se ha identificado en el sistema, deberá hacer clic en "Contraseña y seguridad" tal como aparece en la siguiente imagen:

**En esta sección debería aparecer la opción para activar la doble autenticación cuando esté disponible.**

Cabe destacar que, Apple está implementando la doble autenticación gradualmente, por lo tanto, aún no se encuentra disponible para usuarios de América Latina.

## CONCLUSIÓN

A lo largo de esta guía, se profundizó en la importancia de contar con un método de autenticación robusto. En esta línea y conscientes de esta problemática, muchas empresas han implementado sistemas de doble autenticación para contribuir a la seguridad y protección de la información de sus usuarios. Teniendo en cuenta que los usuarios manejan cada vez más información sensible en sus cuentas, resulta lógico que los cibercriminales destinen mayores recursos al robo de las contraseñas que la protegen. Desde el punto de vista técnico, **es posible reducir este tipo de ataques**, sin embargo, la participación del usuario es primordial en todo el proceso de protección para poder evitar una amenaza que involucre el robo de contraseñas.

Varias empresas y bancos ofrecen sistemas de doble autenticación, no obstante, en la mayoría de los casos dicha opción se encuentra desactivada por defecto. Para solucionar este inconveniente **es necesario que el usuario comprenda la importancia de este método** de protección y aprenda a configurarlo en los distintos servicios disponibles en Internet. Asimismo, este aspecto cobra mayor relevancia, ya que de acuerdo a una encuesta realizada por ESET Latinoamérica, **el 64% de los usuarios de América Latina desconocen qué es la doble autenticación.**



Argentina Cibersegura®  
una iniciativa de ESET®

Realizado por: 

