CONFIGURACIONES SEGURAS PARA **PROTEGER** TU CORREO ELECTRÓNICO

Refuerza la seguridad de tus cuentas en línea para evitar accesos no autorizados y **proteger tu información.**

Financiado por la Unión Europea
NextGenerationEU

GOBIERNO DE ESPAÑA
MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES

Plan de Recuperación, Transformación y Resiliencia

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

Índice

Analizando el uso del correo electrónico

¿Utilizas tu correo para registrarte en páginas web o contratar algún servicio?

Piensa en cuántas veces has usado tu dirección de correo electrónico para acceder a una aplicación o plataforma. También es muy frecuente que diferentes entidades soliciten tu correo para fines publicitarios, enviarte notificaciones, información de servicios, etc.

¿Conoces los diferentes proveedores de correo más conocidos que existen?

Gmail

Es el servicio de correo de **Google,** una de las empresas tecnológicas más grandes del mundo.

Outlook (Hotmail)

Pertenece a **Microsoft,** la compañía detrás de los sistemas **Windows.**

Apple Mail

Dispone de un servicio de correo, y pertenece a **Apple,** empresa conocida por sus dispositivos como **iPhone, iPad y Mac.**

¿Sabías que tu cuenta de correo no solo sirve para enviar mensajes?

Tu cuenta de **correo electrónico** es como **tu carnet de identidad en Internet.** Antes solo servía para enviar mensajes, pero ahora es una **herramienta clave para acceder a servicios** como redes sociales, bancos y tiendas en línea. Además, **te ayuda a recuperar contraseñas** si las olvidas. Por eso, es muy importante cuidarla bien, porque quien tenga acceso a tu correo podría entrar a tus otras cuentas.

¿Te has preguntado qué ocurriría si alguien accediera a tu correo sin autorización?

Si alguien accede a alguna de tus cuentas, **puede acceder a tus datos privados** (nombre completo, DNI, teléfono, datos bancarios, etc.), **suplantar tu identidad, robarte la cuenta** o incluso cometer fraudes en tu nombre.

Medidas básicas **para proteger** tu cuenta **de correo electrónico**

Contraseñas robustas y únicas

Utiliza una **contraseña de al menos 10 caracteres que incluya mayúsculas, minúsculas, números y símbolos especiales,** como, por ejemplo, Mi@casa#72 o Sol&Verano25. Cámbiala regularmente y **no la reutilices para otros servicios *online*.**

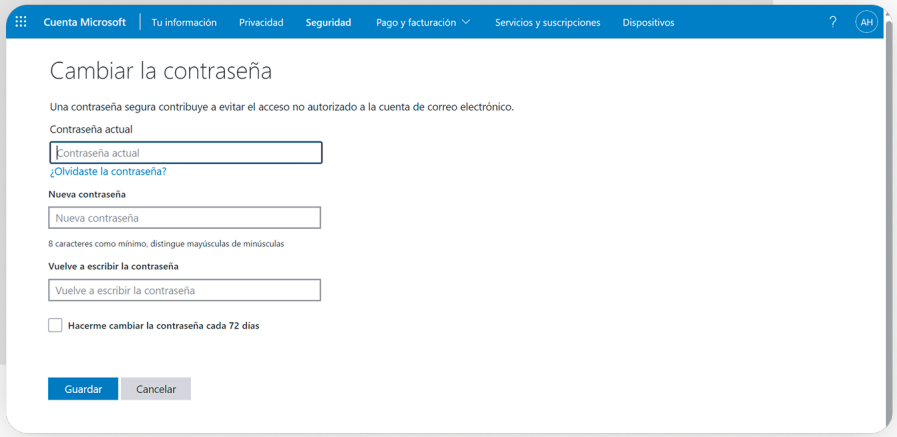
¿Cómo puedes cambiar tu contraseña?

Gmail:

1. Accede a https://mail.google.com y **pulsa sobre tu perfil** en la esquina superior derecha.
2. Selecciona **Gestionar tu cuenta de Google > Seguridad > Contraseña**

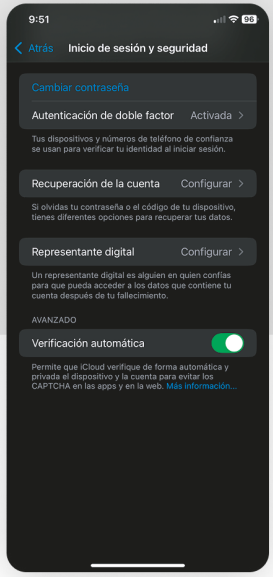
Outlook:

1. Accede a https://outlook.live.com y **pulsa sobre el icono de tu perfil** en la esquina superior derecha.
2. Selecciona **Mi cuenta de Microsoft > Seguridad > Cambiar contraseña.**

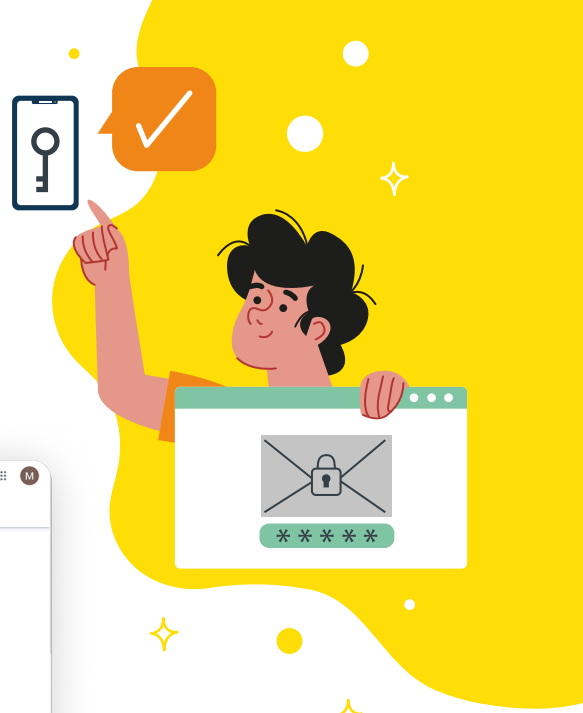


Apple Mail:

1. Desde icloud.com accede a **Gestionar cuenta de iCloud > Inicio de sesión y seguridad.**
2. También puedes dirigirte a los ajustes de **tu dispositivo iCloud** y pulsar sobre **tu perfil de iCloud > Inicio de sesión y seguridad > Cambiar contraseña.**



Autenticación de dos factores



La autenticación en dos pasos es una forma de hacer **tu cuenta más segura.** Funciona así: además de tu contraseña, necesitarás un **código especial** para entrar. Este código cambia cada vez y solo tú puedes recibirlo en tu teléfono o en una aplicación. Así, aunque alguien descubra tu contraseña, no podrá acceder a tu cuenta sin ese código adicional. Esto añade una protección extra y te ayuda a mantener tu **información segura.**

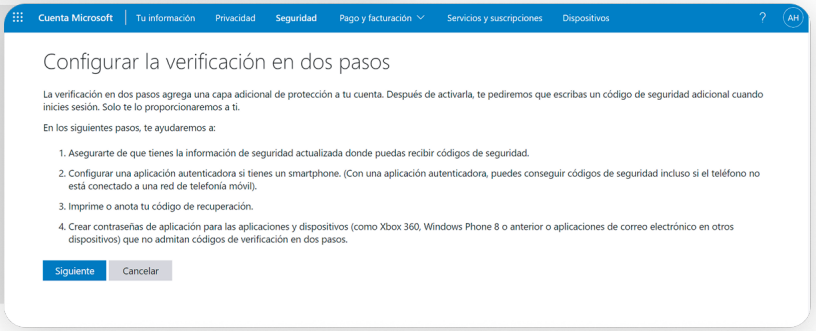
¿Cómo puedes configurar este mecanismo de seguridad adicional a la contraseña?

Gmail:

1. Dirígete a **tu perfil** en la esquina superior derecha.
2. Elige **Gestionar tu cuenta de Google > Seguridad > Verificación en dos pasos > Activar verificación en dos pasos.**

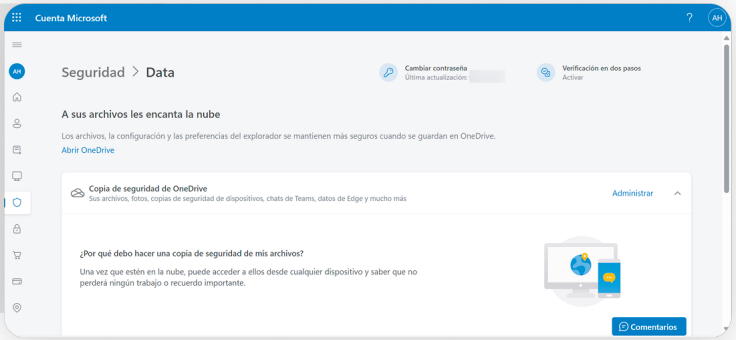
Outlook:

1. Sitúate en la página principal de Outlook y pulsa en el icono de tu perfil que está en la esquina superior derecha de la pantalla.
2. Selecciona **Mi cuenta de Microsoft > Seguridad > Verificación en dos pasos > Administrar.**



Apple Mail:

1. Ve a "**Ajustes" en tu dispositivo y selecciona tu nombre.**
2. Elige "**Inicio de sesión y seguridad" y activa Autenticación de doble factor,** para ello deberás asignar un número de teléfono a donde quieres que lleguen las notificaciones de segundo factor.



Alertas de inicio de sesión

Activa las **notificaciones de inicio de sesión** para recibir **alertas** de cualquier acceso a tu cuenta desde un dispositivo no reconocido. Esto te permitirá detectar y actuar rápidamente ante **intentos de acceso no autorizados.**

¿Cómo puedes activar las alertas?

Gmail:

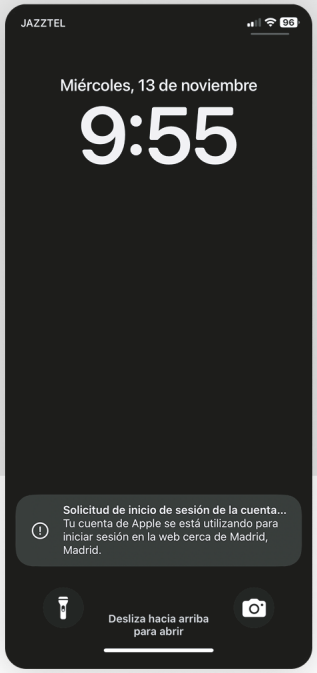
1. Dirígete a **Seguridad > Actividad reciente,** y comprueba las notificaciones de inicio de sesión no reconocido.

Outlook:

1. Ya tiene activado por defecto la detección de intentos de inicio de sesión si se producen desde otro dispositivo distinto al habitual, solicitando **un código que se envía a otro correo electrónico** distinto **asociado a tu cuenta.**
2. Si deseas ver la actividad que ha habido en tu cuenta puedes hacerlo clicando sobre el icono de tu perfil en la **esquina superior derecha > Mi cuenta de Microsoft > Seguridad > Ver mi actividad de inicio de sesión.**

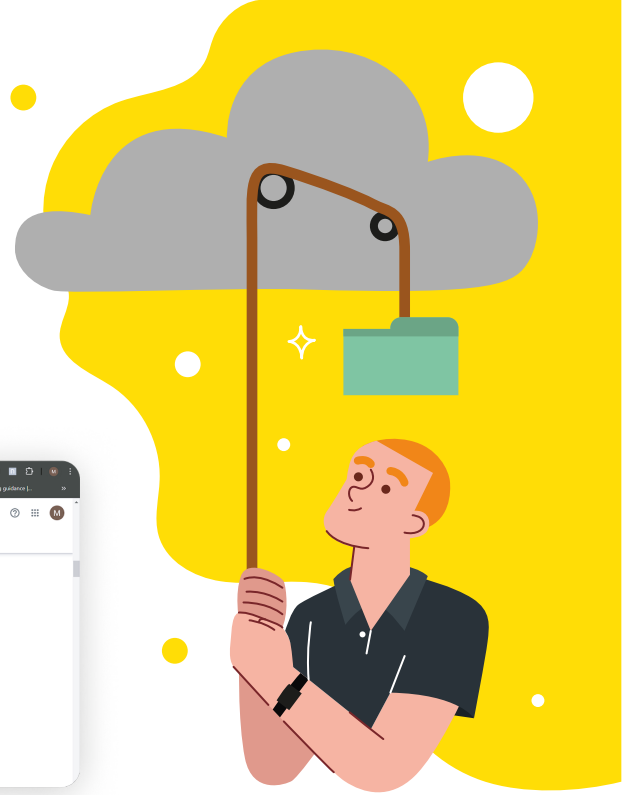
Apple Mail:

1. Apple **envía automáticamente alertas** de inicio de sesión cuando se detecta el acceso desde un dispositivo nuevo.



Realizar copias de seguridad

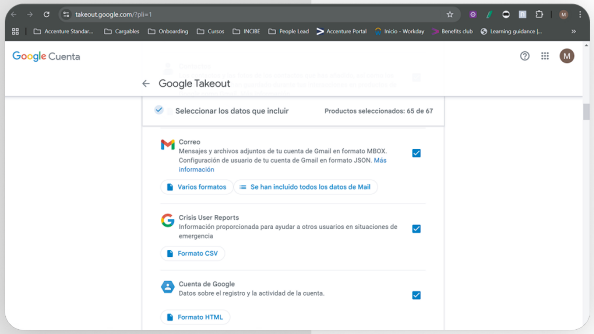
Te recomendamos **hacer copias de seguridad** periódicas de **tus correos electrónicos y contactos.** Esto es útil en caso de que desees cambiar de cuenta o para mantener un respaldo seguro de tu información.



¿Cómo puedes hacer una copia de seguridad de tus correos y contactos?

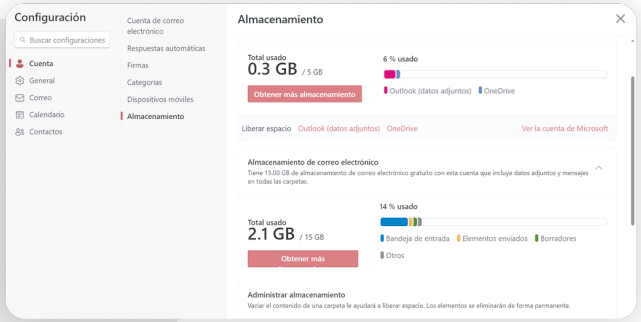
Gmail:

1. Entra en la página de Google Takeout escribiendo **"takeout.google.com" en el navegador.**
2. Una vez dentro, selecciona los datos que deseas guardar para hacer una **copia de seguridad,** elige con qué frecuencia.
3. Por último, selecciona el formato de archivo "Zip" y define el tamaño máximo para cada archivo de la copia.



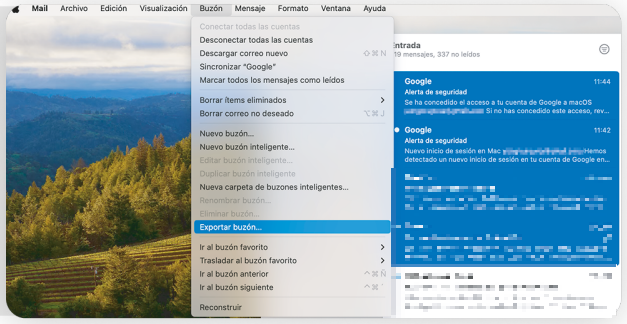
Outlook:

1. En este caso no se puede hacer una copia de seguridad como tal, ya que los datos se sincronizan con **One Drive automáticamente.**
2. Por otra parte, puedes administrar los datos guardados clicando en el icono de engranaje en la **esquina superior derecha > Cuenta > Almacenamiento.**



Apple Mail:

1. En tu dispositivo Mac, abre la **aplicación Mail.**
2. Selecciona los correos que deseas respaldar y utiliza **la opción Buzón > Exportar buzón para guardar una copia de seguridad.**



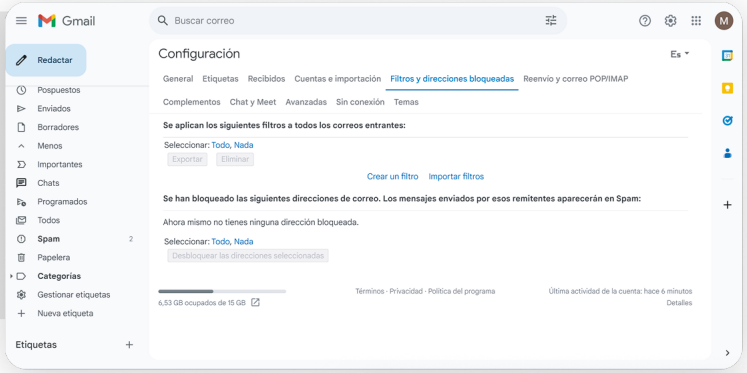
Aplicar filtros anti-spam

Configura filtros anti-spam en tu cuenta de correo para **bloquear correos no deseados y potencialmente peligrosos.**
Esto ayuda a mantener tu bandeja de entrada libre de mensajes fraudulentos, como **intentos de *phishing*** o correos publicitarios invasivos.

¿De qué manera puedes aplicar los filtros anti-spam en los principales *proveedores* de correo?

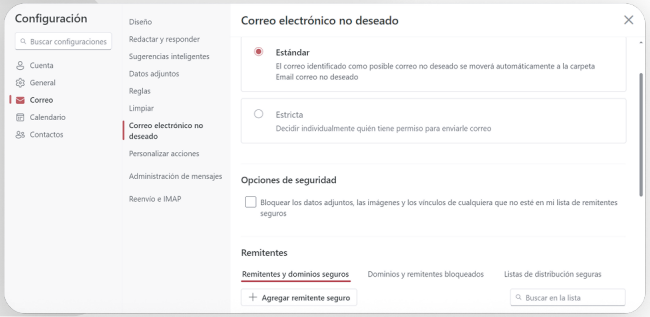
Gmail:

1. Puedes crear filtros adicionales yendo a **Configuración (icono de un engranaje) > Ver todos los ajustes > Filtros y direcciones bloqueadas > Crear un filtro.**
2. Aquí puedes especificar criterios adicionales para **marcar correos como spam.**



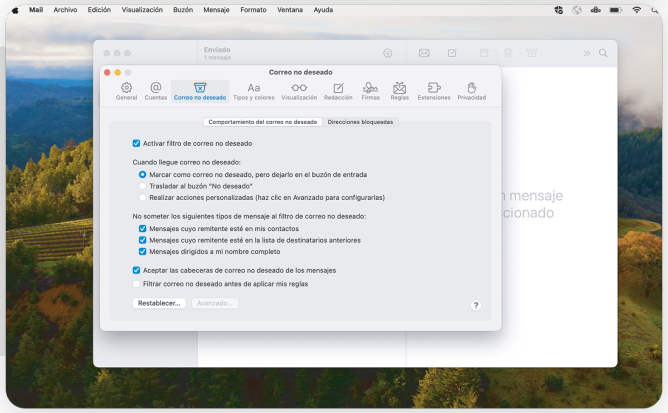
Outlook:

1. Si lo deseas, puedes **gestionar filtros** para administrar los correos recibidos en función del remitente.
2. Clica sobre el icono de **engranaje en la esquina superior derecha > Correo > Correo electrónico no deseado.**



Apple Mail:

1. Abre la aplicación Mail en tu Mac, ve **a Ajustes > Correo no deseado y selecciona las opciones de filtrado.**
2. Aquí puedes elegir cómo se gestionan los correos no deseados y marcarlos automáticamente para moverlos fuera de tu bandeja principal.

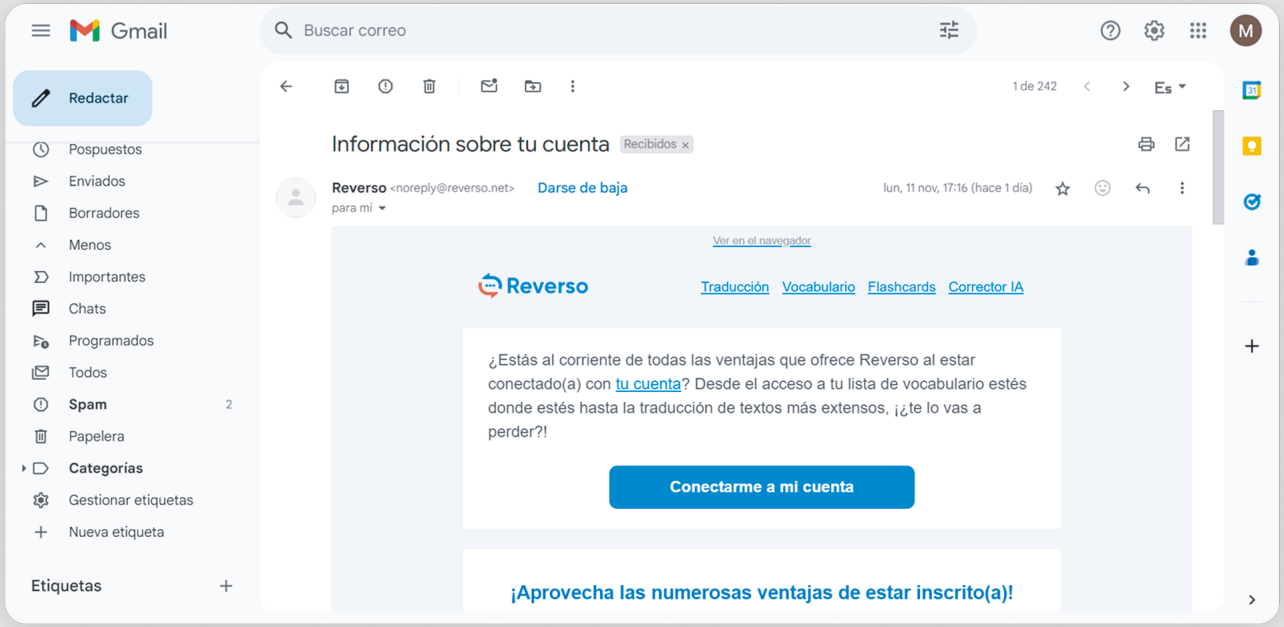


Dar de baja suscripciones innecesarias

Reduce la cantidad de **correos no deseados cancelando suscripciones** a boletines o servicios que **no te interesen.**

Puedes realizar esta acción tanto para Gmail, Outlook y Apple Mail de la misma manera:

1. Abre uno de los correos de los que quieras **darte de baja.**
2. Justo al lado del remitente encontrarás **"Darse de baja".** En caso contrario, al final del correo encontrarás un mensaje tipo: **"Cancelar la suscripción", "Baja" o "Unsubscribe".**



Recomendaciones adicionales para **la protección en línea**

Existen pautas generales que debes seguir para reforzar la seguridad de tus cuentas:

No compartas tu contraseña: evita compartir tu contraseña y no utilices la misma clave en otros servicios. Cada cuenta debe tener su contraseña única para dificultar el acceso en caso de que una de ellas se vea comprometida. Los siguientes consejos te pueden ser de ayuda:

- **Crea contraseñas únicas pero que sean complejas,** utilizando al menos 10 caracteres, entre los que debes utilizar, letras mayúsculas, minúsculas, números y caracteres especiales, como las siguientes: Rio!Verde5 y Sol#Mar45.

- **Utiliza gestores de contraseñas,** estos son una herramienta que te ayuda a guardar y organizar todas tus contraseñas de forma segura. En lugar de tratar de recordar muchas claves diferentes, solo necesitas recordar una única contraseña maestra para acceder a todas las demás, de esta manera no tienes que recordar todas las contraseñas que hayas creado.

Ignora y elimina correos sospechosos: algunos correos intentan engañarte para que hagas clic en enlaces o descargues archivos maliciosos. Sé cauteloso con los correos que no esperabas y que solicitan información personal o acciones inusuales. Algunos de los ejemplos más comunes que puedes encontrarte son:

- **Suplantación de entidades conocidas,** como pueden ser bancarias, eléctricas, etc. Este tipo de correos lo que pretenden es:
  - Que utilices enlaces en su interior para redirigirte a sitios web falsos donde te solicitan a través de un formulario tus datos personales para evitar supuestamente alguna emergencia relacionada con los servicios de la entidad en cuestión.
  - También se utilizan para que descargues archivos adjuntos maliciosos y de esa manera infectar tu dispositivo.
- **Sorteos y promociones falsas con regalos gratuitos.** Estos engaños buscan que ingreses tus datos personales o bancarios con la promesa de recibir un premio, pero en realidad pueden usarlos para robarte dinero o suplantar tu identidad. Si algo parece demasiado bueno, consulta antes con otra persona de tu confianza.
- **Remitente desconocido.** Si observas que el remitente es desconocido, el asunto es urgente o intenta crear alarma y contiene errores ortográficos y/o gramaticales, tómate tu tiempo y desconfía.

- **Utilizar una cuenta de correo alternativa:** si necesitas registrarte en una página web que no conoces bien o en la que no tienes pensado quedarte mucho tiempo, es recomendable usar una cuenta de correo secundaria. Así podrás mantener tu cuenta principal libre de correos no deseados y protegerla de posibles riesgos.

Proteger tu cuenta de correo electrónico y otros servicios no es solo una cuestión de privacidad, sino también de seguridad personal y financiera. Con estas configuraciones y recomendaciones, podrás reducir los riesgos y disfrutar de una experiencia en línea más segura.