

# Creación segura de cuentas en las plataformas del curso

## Datos de esta lección

|                                                     |                                                    |
|-----------------------------------------------------|----------------------------------------------------|
| <b>Fase</b>                                         | F2 — Capa de telefonía y generación de voz         |
| <b>Módulo</b>                                       | M2.1 — Gestión financiera y eliminación de riesgos |
| <b>Puntos de profesionalidad al superar el test</b> | 25                                                 |

## Objetivo práctico

---

Al terminar esta lección sabrás crear cuentas en ElevenLabs, Vapi o Retell, OpenAI y Twilio siguiendo un protocolo de seguridad consistente, evitando los errores más habituales al dar de alta cuentas de pago con capacidad de generar cargos económicos.

## Resultado que obtendrás

---

Un criterio de seguridad aplicado de forma sistemática a cada cuenta nueva que crees a partir de ahora en este curso.

## Dónde encaja dentro del sistema final

---

Esta lección precede a la creación de cualquier cuenta real en las plataformas técnicas del sistema (voz, telefonía, agente). Aplicarla correctamente reduce el riesgo de errores costosos más adelante.

## Conocimientos previos

---

- Gestor de contraseñas configurado (módulo 1.1).
- Correo profesional y perfil de navegador dedicado (módulo 1.1).

## Herramientas necesarias

---

- Tu gestor de contraseñas.
- Tu correo profesional.
- Tu perfil de navegador dedicado.

### **Posible coste**

Esta lección no requiere ningún gasto por sí misma: es el protocolo que aplicarás antes de dar de alta cuentas que sí pueden tener coste.

### **Advertencia de seguridad**

A partir de este módulo empezarás a crear cuentas en plataformas que pueden generar cargos reales si se configuran de forma incorrecta o si una clave de API se filtra. Sigue el protocolo de esta lección en cada cuenta nueva, sin excepciones.

## **Modelo mental**

---

Piensa en la apertura de una cuenta bancaria nueva para tu negocio: no usarías cualquier correo, no compartirías la clave de acceso por un canal inseguro, y activarías cualquier alerta de seguridad disponible desde el primer día. Cada cuenta de estas plataformas técnicas merece el mismo nivel de cuidado, porque igual que una cuenta bancaria, puede mover dinero.

## **Explicación**

---

El protocolo de seguridad de este curso para cualquier cuenta nueva de plataforma técnica consta de estos pasos, siempre en este orden:

1. Usa tu correo profesional (módulo 1.1), nunca el personal.
2. Genera la contraseña con tu gestor de contraseñas (módulo 1.1); nunca reutilices una contraseña de otra cuenta.
3. Guarda la entrada en tu bóveda inmediatamente, con un nombre identificable (por ejemplo, «ElevenLabs — Torus Academy»).
4. Activa la verificación en dos pasos si la plataforma la ofrece, antes de configurar nada más.
5. Antes de introducir cualquier dato de pago, localiza en la plataforma sus opciones de control de gasto (alertas, límites, saldo prepago) y actívalas si existen. Este paso se trata en profundidad en la siguiente lección de este módulo.

Este orden importa: activar la seguridad de la cuenta (2FA) antes de vincular un método de pago reduce la ventana de riesgo si algo sale mal durante el registro.

## Preparación

---

Ten abiertos tu gestor de contraseñas y tu perfil de navegador profesional antes de empezar a registrar ninguna cuenta.

## Procedimiento paso a paso

---

1. **Contexto:** Vas a registrar una cuenta nueva en cualquiera de las plataformas técnicas de este curso.

**Acción de teclado:** Antes de escribir nada en el formulario de registro, abre tu gestor de contraseñas y genera una contraseña nueva para esta cuenta concreta.

**Respuesta esperada de NVDA:** NVDA anunciará la nueva contraseña generada o confirmará que se ha copiado al portapapeles, según la interfaz de tu gestor.

**Qué significa:** Tienes ya preparada una contraseña única y segura antes de tocar el formulario de registro de la plataforma externa.

**Acción siguiente:** Vuelve al formulario de registro y pega la contraseña generada en el campo correspondiente.

2. **Contexto:** Has completado el registro y tienes acceso a la cuenta nueva.

**Acción de teclado:** Busca en el menú de configuración de la cuenta ("Settings", "Account", "Security") la opción de verificación en dos pasos y actívala siguiendo el asistente.

**Respuesta esperada de NVDA:** NVDA anunciará las opciones disponibles de verificación en dos pasos.

**Qué significa:** Con 2FA activo, el riesgo de que alguien acceda a la cuenta únicamente con la contraseña se reduce drásticamente.

**Acción siguiente:** Guarda la entrada completa (usuario, contraseña, y una nota indicando que 2FA está activo) en tu gestor de contraseñas.

## Errores frecuentes y diagnóstico

---

## **Registrar una cuenta de plataforma con el correo personal por prisa o distracción.**

**Cómo localizarlo:** Ocurre con facilidad si no se revisa el campo antes de enviar el formulario (ver módulo 1.1, lección de separación personal/profesional).

**Solución:** Revisar siempre el campo de correo antes de enviar cualquier formulario de registro en este módulo.

## **Comprobación final**

---

Revisa tu gestor de contraseñas y confirma que las últimas cuentas creadas siguen el protocolo completo: correo profesional, contraseña generada y guardada, y verificación en dos pasos activada cuando esté disponible. Si las tres condiciones se cumplen, la comprobación es positiva.

## **Qué acabas de conseguir**

---

Tienes un protocolo repetible de seguridad que aplicarás en cada cuenta nueva del resto del curso, reduciendo el riesgo de incidentes de seguridad o de facturación inesperada.

## **Ejercicio práctico**

---

Revisa cualquier cuenta que ya tengas creada de un curso o proyecto anterior y comprueba, contra este protocolo, si cumple los cinco pasos. Corrige lo que falte.

## **Resumen de lo imprescindible**

---

- Usa siempre tu correo profesional para registrar cuentas de plataformas técnicas.
- Genera y guarda la contraseña con tu gestor antes de escribir nada en el formulario de registro.
- Activa la verificación en dos pasos antes de vincular cualquier método de pago.
- Localiza y activa los controles de gasto disponibles antes de introducir datos de pago (siguiente lección).

## **Estoy preparado para continuar si puedo...**

---

- Aplicar el protocolo de cinco pasos al registrar una cuenta nueva.
- Explicar por qué activar 2FA antes de vincular un método de pago reduce el

riesgo.

## Test de comprobación

---

*Para registrar el resultado y obtener Puntos de profesionalidad, realiza este test desde la versión web de la lección. Las opciones se muestran aquí sin señalar la respuesta correcta.*

1. ¿Por qué el protocolo de esta lección recomienda activar la verificación en dos pasos ANTES de introducir un método de pago en una cuenta nueva, y no después?
  - a. Porque la mayoría de plataformas no permiten activar 2FA después de haber introducido un método de pago.
  - b. Porque reduce la ventana de tiempo en la que la cuenta está protegida sólo por una contraseña, antes de que exista capacidad real de generar cargos.
  - c. Porque el orden de los pasos no tiene ninguna importancia real.
2. Según la documentación oficial verificada en esta lección, Twilio exige 2FA de forma obligatoria en toda cuenta y no se puede desactivar, mientras que en ElevenLabs y OpenAI hay que activarlo tú mismo desde los ajustes de seguridad. Un compañero registra una cuenta de ElevenLabs siguiendo el protocolo pero no encuentra ninguna pantalla que le obligue a activar 2FA durante el registro. ¿Qué deberías concluir?
  - a. Que ElevenLabs no ofrece verificación en dos pasos y puede omitirse ese paso del protocolo sin más.
  - b. Que es un comportamiento esperado: a diferencia de Twilio, ElevenLabs no impone 2FA automáticamente, así que hay que activarlo manualmente desde los ajustes de cuenta tras el registro, tal como indica el protocolo de esta lección.
  - c. Que el registro ha fallado y hay que volver a crear la cuenta desde cero.
3. Has activado 2FA en una cuenta de OpenAI usando una aplicación autenticadora, y la plataforma te muestra un código de recuperación de un solo uso. Según el criterio de seguridad de esta lección, ¿qué deberías hacer con ese código?
  - a. Ignorarlo: si tienes la aplicación autenticadora instalada, el código de recuperación no sirve para nada.
  - b. Guardarlo de inmediato en tu gestor de contraseñas, igual que el resto de credenciales de la cuenta, porque es la única forma de recuperar el acceso si pierdes el dispositivo con la aplicación autenticadora.
  - c. Compartirlo por correo sin cifrar con tu equipo para que cualquiera pueda entrar si hace falta.

## Fuentes

---

- [How do I add two-factor authentication \(2FA\) to my account? — ElevenLabs \(centro de ayuda oficial\) \(consultado el 2026-08-30\)](#)
- [Enable Two-Factor Authentication on your Twilio Account — Twilio \(centro de ayuda oficial\) \(consultado el 2026-08-30\)](#)
- [Enabling or disabling multi-factor authentication \(MFA\) — OpenAI \(centro de ayuda oficial\) \(consultado el 2026-08-30\)](#)

Última actualización de este contenido: **2026-08-30**.