

Instala y usa un gestor de contraseñas accesible

Datos de esta lección

Fase	F1 — Cimientos, seguridad y arquitectura del sistema
Módulo	M1.1 — Preparación del entorno de trabajo en Windows 11 con NVDA
Puntos de profesionalidad al superar el test	20

Objetivo práctico

Al terminar esta lección tendrás instalado y configurado un gestor de contraseñas accesible con NVDA, sabrás crear una bóveda protegida por una contraseña maestra, generar contraseñas seguras, guardar credenciales y notas seguras, y activar verificación en dos pasos (2FA) en tu propia cuenta del gestor.

Resultado que obtendrás

Una bóveda de contraseñas operativa, con al menos una entrada de prueba creada y recuperada correctamente, y 2FA activado en la cuenta del propio gestor.

Dónde encaja dentro del sistema final

A lo largo de este curso crearás decenas de cuentas y claves de API: ElevenLabs, Vapi o Retell, Twilio, n8n o Make, OpenAI, Cal.com, WordPress, y las de tus futuros clientes. Guardar cada credencial de forma segura y accesible es lo que te permitirá trabajar con velocidad y sin errores más adelante, en lugar de tener que recuperar contraseñas olvidadas en mitad de una sesión de trabajo con un cliente.

Conocimientos previos

- Estructura de carpetas creada en la lección anterior (útil, pero no obligatoria para ésta).
- Manejo básico del navegador con NVDA.

Herramientas necesarias

- Un navegador (Chrome, Edge o Firefox).
- Una cuenta de correo electrónico personal para registrar el gestor de contraseñas.

Posible coste

Esta lección usa Bitwarden, cuyo plan gratuito no tiene coste y es suficiente para todo lo que necesitas en este curso. Bitwarden también ofrece un plan Premium de pago (verificado el 30 de agosto de 2026: 1,65 USD al mes facturado anualmente) que añade autenticación de doble factor integrada (TOTP), adjuntos de archivo cifrados y acceso de emergencia; ninguna de esas funciones de pago es necesaria para seguir este curso.

Advertencia de seguridad

La contraseña maestra de tu gestor de contraseñas es la única contraseña que nunca debes guardar dentro del propio gestor (sería como guardar la llave de la caja fuerte dentro de la caja fuerte). Elige una frase larga, fácil de recordar y de teclear con NVDA, y no la compartas con nadie. Si la olvidas y no tienes activada ninguna opción de recuperación, la mayoría de gestores con cifrado de conocimiento cero no pueden recuperarla por ti: perderías el acceso a toda la bóveda.

Modelo mental

Piensa en una caja fuerte personal con una única llave maestra. Dentro de la caja fuerte guardas todas las demás llaves y notas confidenciales (contraseñas, claves de API, notas seguras). Sólo necesitas recordar una llave —la maestra— para acceder a todas las demás. Si alguien mira dentro del edificio sin esa llave, sólo ve una caja cerrada: no puede leer lo que hay dentro.

Explicación

Un gestor de contraseñas es una aplicación que almacena tus credenciales de forma cifrada, protegidas por una única contraseña maestra que sólo tú conoces. La mayoría de gestores serios usan «cifrado de conocimiento cero» (*zero-knowledge encryption*): ni siquiera la empresa que fabrica el gestor puede leer el contenido de tu bóveda, porque el cifrado y descifrado ocurren en tu propio dispositivo.

Para este curso se recomienda **Bitwarden** porque su plan gratuito es completo (contraseñas, notas seguras, identidades, tarjetas de pago, sincronización entre dispositivos ilimitados), su código es abierto y auditable, y la empresa mantiene una página pública dedicada a sus objetivos de accesibilidad, con el nivel AA de las pautas WCAG como referencia. Esto no significa que cada pantalla de Bitwarden sea perfecta —ninguna herramienta lo es al cien por cien— pero sí que la accesibilidad es un objetivo declarado y mantenido activamente, lo cual es relevante a la hora de elegir una herramienta que vas a usar a diario.

Vocabulario nuevo

Contraseña maestra

Piénsalo así: La única llave que abre la caja fuerte donde están todas las demás llaves.

La contraseña que protege el acceso a toda tu bóveda de contraseñas. Debe ser larga, única y no debe guardarse dentro del propio gestor.

Ejemplo: Una frase de varias palabras poco relacionadas entre sí suele ser más segura y más fácil de recordar y teclear que una combinación corta de símbolos.

Verificación en dos pasos (2FA)

Piénsalo así: Pedir, además de la llave, una segunda comprobación en la puerta: por ejemplo, un código temporal en tu teléfono.

Mecanismo de seguridad que exige, además de la contraseña, una segunda prueba de identidad (un código temporal, una aplicación autenticadora, una llave física) para iniciar sesión.

Ejemplo: Activar 2FA en tu cuenta de Bitwarden con una aplicación autenticadora en el móvil.

Bóveda

Piénsalo así: El interior de la caja fuerte, donde están ordenadas todas tus contraseñas y notas.

El conjunto cifrado de todas las credenciales, notas seguras, identidades y tarjetas que guardas en tu gestor de contraseñas.

Ejemplo: Tu bóveda de Bitwarden contendrá, a lo largo de este curso, las credenciales de ElevenLabs, Vapi, Twilio y muchas otras.

Preparación

Ten a mano tu correo electrónico personal (no el de un futuro cliente) y decide de antemano, antes de abrir la página de registro, cuál será tu contraseña maestra: una frase larga que no uses en ningún otro sitio.

Procedimiento paso a paso

1. **Contexto:** Vas a crear tu cuenta de Bitwarden desde cero.

Acción de teclado: Abre tu navegador y ve a la dirección oficial `bitwarden.com`. Navega por encabezados con `H` hasta encontrar un enlace o botón para crear una cuenta gratuita; suele llamarse «Get started» o «Crear cuenta gratis», según el idioma detectado.

Respuesta esperada de NVDA: NVDA debería anunciar un texto similar a «Crear cuenta gratis, enlace» o el nombre equivalente vigente en la página.

Qué significa: Ese enlace te llevará al formulario de registro de una cuenta nueva.

Acción siguiente: Pulsa Enter sobre ese enlace para abrir el formulario de registro.

2. **Contexto:** Estás en el formulario de registro.

Acción de teclado: Pulsa `Tab` para recorrer los campos: nombre, correo electrónico, contraseña maestra, confirmación de la contraseña maestra. Escribe tus datos en cada campo.

Respuesta esperada de NVDA: NVDA debería anunciar el nombre de cada campo al entrar en él, por ejemplo «Contraseña maestra, editar, contraseña».

Qué significa: El formulario suele incluir también un indicador de fortaleza de la contraseña; si NVDA lo anuncia, tenlo en cuenta, pero prioriza siempre la longitud de la frase sobre la complejidad de símbolos.

Acción siguiente: Recorre el formulario hasta el botón final de envío (normalmente «Submit» o «Enviar») y confírmalo con Enter.

3. **Contexto:** Ya tienes una cuenta creada. Ahora vas a guardar tu primera entrada de prueba en la bóveda.

Acción de teclado: Dentro de la aplicación web o de escritorio de Bitwarden, busca un botón para añadir un elemento nuevo (suele llamarse «Add item» o «Nuevo elemento», normalmente representado con un símbolo «+»). Recórrelo con la tecla **B** en modo exploración, o con Tab.

Respuesta esperada de NVDA: NVDA debería anunciar un texto similar a «Nuevo elemento, botón» o «Añadir elemento, botón».

Qué significa: Al activarlo se abrirá un formulario para crear una entrada de tipo Inicio de sesión, con campos como nombre, usuario, contraseña y URL.

Acción siguiente: Rellena una entrada de prueba (por ejemplo, «Prueba Torus Academy», usuario ficticio, contraseña generada) y guárdala.

4. **Contexto:** Quieres que Bitwarden genere una contraseña segura en lugar de inventarla tú mismo.

Acción de teclado: Dentro del formulario de la entrada, localiza el campo «Contraseña» y, junto a él, un botón de generar contraseña (icono de recarga o texto «Generate password»). Actívalo con Enter o la barra espaciadora.

Respuesta esperada de NVDA: NVDA debería anunciar que el campo de contraseña se ha actualizado con un nuevo valor, o anunciar directamente la nueva contraseña generada si el foco se sitúa sobre el campo.

Qué significa: Bitwarden ha generado una contraseña aleatoria y la ha colocado en el campo automáticamente; no necesitas inventarla ni memorizarla, porque quedará guardada en la bóveda.

Acción siguiente: Guarda la entrada y ciérrala.

5. **Contexto:** Quieres proteger tu propia cuenta de Bitwarden con verificación en dos pasos.

Acción de teclado: Ve a la configuración de la cuenta (busca «Settings» o «Configuración» recorriendo encabezados o el menú principal con Tab) y localiza la sección de verificación en dos pasos («Two-step Login»).

Respuesta esperada de NVDA: NVDA debería anunciar el nombre de la sección y las opciones disponibles (aplicación autenticadora, correo electrónico, llave de seguridad, entre otras según el plan).

Qué significa: La opción por aplicación autenticadora (código temporal de seis dígitos) suele ser la más accesible y no depende del plan de pago para activarse desde una app externa gratuita.

Acción siguiente: Sigue el asistente para vincular tu aplicación autenticadora y confirma con el primer código generado.

Posibles diferencias de interfaz

Bitwarden ofrece extensión de navegador, aplicación de escritorio, aplicación móvil y acceso web; cada una tiene una disposición ligeramente distinta, aunque los conceptos (bóveda, nuevo elemento, generador de contraseñas, configuración de dos pasos) son los mismos en todas. Si un nombre de botón cambia respecto a lo descrito aquí, busca por sinónimos («Add», «New», «Nuevo», «Crear») antes de asumir que la función ha desaparecido.

Errores frecuentes y diagnóstico

Olvidas la contraseña maestra.

Cómo localizarlo: Al usar cifrado de conocimiento cero, Bitwarden no puede leer ni recuperar tu contraseña maestra por ti.

Solución: Configura desde el principio un método de recuperación (frase de recuperación o email de recuperación, según lo que ofrezca la cuenta) y guarda esa información en un lugar físico seguro, fuera del propio gestor.

La extensión del navegador no rellena automáticamente un formulario de inicio de sesión.

Cómo localizarlo: Puede deberse a que la URL guardada en la entrada no coincide exactamente con la página actual, o a que la extensión no está habilitada en ese navegador.

Solución: Abre la bóveda directamente (icono de la extensión o aplicación web) y copia usuario y contraseña manualmente con Ctrl+C, sin depender del autorrelleno.

Comprobación final

Cierra sesión en Bitwarden y vuelve a iniciarla con tu contraseña maestra. Abre la entrada de prueba que creaste y confirma que NVDA lee correctamente el usuario y que puedes copiar la contraseña con el comando de copiar de la propia aplicación. Si

la entrada se recupera y el segundo factor te lo pide al iniciar sesión, la comprobación es positiva.

Qué acabas de conseguir

Tienes un lugar seguro y accesible donde guardar cada credencial que generes en este curso, protegido con contraseña maestra y verificación en dos pasos, en lugar de depender de la memoria o de notas sin cifrar.

Ejercicio práctico

Crea, además de la entrada de prueba, una nota segura (no un inicio de sesión) con el texto «Torus Academy — cuenta iniciada el [fecha de hoy]». Practica localizar y leer esa nota más adelante, cuando ya no la recuerdes de memoria.

Resumen de lo imprescindible

- Un gestor de contraseñas guarda tus credenciales cifradas detrás de una única contraseña maestra.
- La contraseña maestra nunca se guarda dentro del propio gestor.
- Bitwarden es la recomendación de este curso: plan gratuito completo y accesibilidad como objetivo declarado (WCAG AA).
- El generador de contraseñas evita tener que inventar y memorizar contraseñas complejas.
- La verificación en dos pasos añade una capa de protección adicional sobre la propia cuenta del gestor.

No necesitas aprender todavía

Todavía no necesitas configurar el acceso de emergencia ni compartir elementos con otras personas dentro de Bitwarden: son funciones útiles para cuando trabajes en equipo o con clientes, y se retoman en la Fase 5 del curso.

Estoy preparado para continuar si puedo...

- Crear una entrada de inicio de sesión nueva en mi bóveda.
- Generar una contraseña segura con el gestor en lugar de inventarla yo mismo.
- Explicar por qué la contraseña maestra nunca debe guardarse dentro del propio gestor.
- Activar y usar verificación en dos pasos al iniciar sesión.

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. Un compañero de curso te dice que ha guardado su contraseña maestra como una nota segura dentro de su propio gestor de contraseñas, «por si se le olvida». ¿Qué problema tiene esta decisión?
 - a. Ninguno: es una buena práctica de respaldo.
 - b. Es equivalente a guardar la llave de la caja fuerte dentro de la propia caja fuerte: si alguien accediera a la bóveda, ya no necesitaría la contraseña maestra para nada.
 - c. Bitwarden no permite guardar notas de texto, sólo contraseñas.
2. ¿Por qué esta lección recomienda usar el generador de contraseñas del gestor en lugar de inventar tus propias contraseñas para cada cuenta nueva?
 - a. Porque las contraseñas inventadas por una persona no son válidas técnicamente.
 - b. Porque el generador produce contraseñas aleatorias y distintas para cada cuenta, sin que tengas que memorizarlas ni reutilizarlas entre servicios.
 - c. Porque teclear una contraseña larga con NVDA es imposible.
3. Según lo verificado en la documentación oficial consultada en esta lección, ¿qué nivel de accesibilidad web declara Bitwarden como objetivo?
 - a. WCAG nivel AAA, el más exigente.
 - b. WCAG nivel AA.
 - c. Bitwarden no publica ningún objetivo de accesibilidad.

Fuentes

- [Bitwarden Pricing — Bitwarden Inc. \(consultado el 2026-08-30\)](#)
- [Accessibility on Bitwarden — Bitwarden Inc. \(consultado el 2026-08-30\)](#)

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