ENTIENDE. COMPRUEBA. MEJORA.

¿Qué es la autenticación multifactor y cuál conviene usar?

La autenticación multifactor (MFA) pide algo más que la contraseña para entrar en una cuenta, como un código o una llave de seguridad. Si puedes elegir, usa un método resistente al phishing basado en FIDO/WebAuthn, como las llaves de seguridad o las passkeys. Si aún no es posible, CISA sugiere una aplicación con comparación de números.



Una guía para pasar a la acción

Explicaciones claras, un ejemplo ficticio y una hoja para organizar tus próximas tres acciones.

Consulta la versión web y sus actualizaciones ↗

¿Qué es la autenticación multifactor y cuál conviene usar?

01 / COMPRENDER

Por qué no basta una contraseña

Una contraseña se puede robar con un correo falso, o reutilizar si se filtró en otro servicio. La MFA añade una segunda comprobación, de modo que la contraseña por sí sola ya no abre la cuenta.

02 / COMPRENDER

Los tipos, de más a menos resistente

- Llaves de seguridad y passkeys (FIDO/WebAuthn): según CISA, la única autenticación resistente al phishing ampliamente disponible.
- Aplicación con comparación de números: escribes en el móvil el número que ves en la pantalla, lo que dificulta aceptar por error una solicitud ajena.
- Aplicación con notificación o código temporal: protege más que la contraseña sola, pero alguien puede engañarte para que aceptes o le des el código.
- Código por SMS: mejor que nada, pero es de las opciones más débiles.

03 / COMPRENDER

Por dónde empezar

- El correo electrónico de toda la plantilla.
- Las cuentas de administrador.
- El acceso remoto y la VPN.
- La banca y las herramientas de pago.

04 / COMPRENDER

Si te llega una solicitud que no has pedido

Recházala y avisa por el canal de tu empresa: alguien podría tener tu contraseña. Si llegan varias seguidas, quizá intentan cansarte para que aceptes. Cambia la contraseña y revisa la cuenta con tu equipo de soporte.

DEL CONOCIMIENTO A LA PRÁCTICA

Llévalo a tu empresa

EJEMPLO FICTICIO

La excepción que deja una puerta abierta

Una empresa ficticia activa un segundo factor en el correo. Sin embargo, una cuenta antigua de administración conserva una excepción. La configuración general parece correcta, pero la cuenta con más permisos no está protegida igual.

La revisión debe incluir las excepciones y las formas de recuperar una cuenta. Activar una opción para la mayoría no prueba que todas las cuentas sensibles la cumplan.

01

Hoy

Localiza las cuentas críticas

Empieza por administradores, correo y acceso remoto. Comprueba si existen cuentas compartidas, antiguas o de proveedores que deban revisarse.

02

Esta semana

Prueba antes de extender

Usa un grupo pequeño y métodos resistentes al phishing cuando el servicio lo permita. Verifica el acceso normal y la recuperación si se pierde el dispositivo.

03

Después

Revisa las excepciones

Documenta cada excepción, su motivo y quién la aprueba. Revisa periódicamente que las cuentas y las políticas sigan siendo las esperadas.

Qué conviene conservar

Una relación de cuentas protegidas, método utilizado y excepciones justificadas. Conserva los códigos de recuperación de forma segura; no los incluyas en un informe compartido.

TU HOJA DE TRABAJO

Tres acciones. Un siguiente paso.

Completa esta hoja con tu equipo. Define cómo comprobaréis cada mejora. No anotes contraseñas, claves ni información confidencial.

01 / Acción

Responsable: _____ Fecha: _____

Cómo comprobarla: _____

02 / Acción

Responsable: _____ Fecha: _____

Cómo comprobarla: _____

03 / Acción

Responsable: _____ Fecha: _____

Cómo comprobarla: _____

Preguntas frecuentes

¿Puedo dar mi código a alguien de soporte que me llama?

No. Ese código sirve para entrar en tu cuenta. Termina la llamada y contacta con soporte por el canal habitual.

¿La MFA evita todos los ataques?

No. Hace que una contraseña robada no baste para entrar, pero no protege de todo. Es una medida entre otras, como las actualizaciones y las copias de seguridad.

Fuentes y siguiente paso

- CISA: More than a Password ↗
- NIST SP 800-63B: Authentication and Authenticator Management ↗

Comprueba en cinco minutos cómo están tus accesos y otras prácticas básicas. Hacer el análisis gratuito ↗

Información general. No es una auditoría, una certificación ni una garantía de seguridad. Ejemplos ficticios. Edición: 5 de noviembre de 2026.