GESTIÓN RESPONSABLE · EDICIÓN 13

IA EN TODAS PARTES: COPILOTO, NO PILOTO

Acelera tareas; datos, decisiones y responsabilidad siguen bajo control humano.



4 HÁBITOS PARA USAR BIEN LA IA

01 PIDE CON INTENCIÓN
Define tarea, público y formato; añade solo el contexto necesario.

02 PROTEGE LOS DATOS
No compartas claves ni datos personales o internos en herramientas no autorizadas.

03 REVISA LO IMPORTANTE
Contrasta hechos, fuentes, cifras, fechas y tono: la IA puede inventar.

04 DECIDE Y RESPONDE
Edita, respeta derechos y asume responsabilidad; declara el apoyo cuando corresponda.

SEMÁFORO DE INFORMACIÓN

VERDE · PÚBLICA
Contenido público o datos ficticios: útiles para practicar, idear y crear borradores.

AMARILLO · INTERNA
Usala solo en herramienta aprobada y según las reglas de la empresa.

ROJO · SENSIBLE
Clientes, claves, salud, pagos, contratos o estrategia: nunca en IA pública; consulta a TI/privacidad.

ACELERA LO REPETITIVO

- Redactar o resumir contenido permitido.
- Ordenar ideas, agendas y listas.
- Explicar fórmulas con datos ficticios.
- Preparar un primer borrador.

REVISA ANTES DE USAR

- Cifras, fechas, citas, enlaces y fórmulas.
- Tono, sesgos, licencias y datos ajenos.
- No delegues contratación, evaluaciones ni decisiones sobre clientes.

PROMPT BASE · TAREA + CONTEXTO + FORMATO + LÍMITES

GENERAL: “Resume este texto público para [audiencia] en 5 puntos. No agregues hechos y señala qué no puedas comprobar.”

OFICINA: “Redacta un borrador para [audiencia] sobre [tema]. Tono claro; no inventes cifras ni compromisos y marca lo que deba verificar una persona.”

RETO RÁPIDO · TOCA A, B O C

Te piden resumir un archivo con datos de clientes. ¿Qué haces?

A Pegar el archivo en una IA pública.

B Minimizar datos y usar herramienta aprobada.

C Pedir a la IA que priorice clientes.

La explicación está en la página 2.

Fuentes: NIST · Perfil de riesgos de IA generativa | Microsoft · Privacidad y protecciones de Copilot Chat



PROMPT LAB · 5 ASISTENTES

CINCO HERRAMIENTAS. CINCO FORMAS DE PEDIR MEJOR.

Selección por visitas web globales estimadas (Similarweb, sep. 2026); no mide calidad.

UNA BUENA PETICIÓN TIENE CINCO PIEZAS

ROL › TAREA › CONTEXTO › FORMATO › LÍMITES

01	CHATGPT · OpenAI	“Actúa como tutor. Explícame [tema] para [nivel], con un ejemplo y 3 preguntas para practicar.”
02	GEMINI · Google	“Compara estas fuentes públicas sobre [tema]. Resume coincidencias, diferencias y dudas en una tabla.”
03	CLAUDE · Anthropic	“Revisa este borrador: señala afirmaciones que requieren fuente y propón una versión clara sin cambiar el sentido.”
04	DEEPSEEK	“Resuelve [problema] y comprueba el resultado con un caso de prueba. Explica brevemente qué supuestos usaste.”
05	GROK · xAI	“Resume la conversación pública sobre [tema] a fecha [día]. Separa hechos y opiniones; cita fuentes y marca lo no verificado.”

CUIDA LA INFORMACIÓN

No pegues datos personales o internos; pide que distinga hechos de supuestos y diga qué no sabe. Afina la indicación y revisa fuentes y políticas antes de compartir.

RESPUESTA AL RETO DE LA PÁG. 1 · B

Minimiza los datos y usa una herramienta aprobada. A expone información; C delega una decisión. Confirma la política y verifica el resultado antes de compartir.

VOLVER AL RETO

Fuentes: Tráfico · Visual Capitalist / Similarweb | OpenAI · prompts | Google · Gemini Anthropic · Claude | DeepSeek · guía | xAI · búsqueda

ALERTA · IA SEGURA · EDICIÓN 13

¿ES REALMENTE TU JEFE QUIEN TE HABLA POR VIDEOLLAMADA?

La IA es una gran aliada, pero también un riesgo: deepfakes que suplantan directivos y herramientas no autorizadas que exponen nuestros datos.



01 · EN LA MIRA

El doble filo de la IA: amenazas y uso no autorizado

La inteligencia artificial está transformando cómo trabajamos, pero también abre la puerta a riesgos críticos si no se gestiona adecuadamente:

RIESGO EXTERNO

Deepfakes

Ciberdelincuentes usan IA generativa para clonar voces o rostros y suplantar a directivos en videollamadas o llamadas de emergencia.

RIESGO INTERNO

Shadow AI

Usar herramientas públicas de IA no verificadas para redactar contratos, analizar datos financieros o procesar información confidencial de clientes.

¿POR QUÉ IMPORTA? El Shadow AI puede exponer propiedad intelectual o datos sensibles fuera de los controles corporativos.

02 · EL ABC DE LA DEFENSA

3 señales para detectar un ataque de IA

Cuando dudes de la autenticidad de una comunicación, busca estas alertas:

1

Urgencia y presión inusual

Te exigen actuar de inmediato, saltándote los canales habituales de aprobación: “hazlo ya, estoy en una reunión importante”.

2

Pequeñas fallas tecnológicas

En videollamadas: parpadeos extraños, labios desincronizados o movimientos robóticos. En audios: tonos metálicos o falta de modulación natural.

3

Solicitudes fuera de lo común

Peticiones de datos confidenciales, claves de acceso administrativo o transferencias de dinero a cuentas no habituales.

DESAFÍO INTERACTIVO · ELIGE A O B PARA VER LA RESPUESTA

Si mi jefe me pide por WhatsApp una transferencia urgente y me adjunta un audio de voz que suena exactamente como él, ¿es seguro proceder de inmediato?

A **Sí, porque su voz es inconfundible.**

B **No. Verifica por un canal oficial.**

Fuentes: NIST · Riesgos de IA generativa | FTC · Clonación de voz

03 · COMPROMISO DEL GRUPO

Diseñando políticas y controles para una IA segura

Para proteger la información del grupo empresarial y potenciar el talento de nuestros equipos de forma segura, estamos trabajando activamente en:



01

DIRECTRICES CLARAS DE USO

Definir qué herramientas de IA están aprobadas para el entorno corporativo y cuáles están prohibidas por motivos de privacidad y seguridad.

02

CONTROLES TÉCNICOS

Barreras en las redes y sistemas del grupo para evitar la filtración accidental de datos sensibles hacia plataformas de IA externas no autorizadas.

03

PRIVACIDAD POR DISEÑO

Asegurar que cualquier iniciativa o software de IA implementado internamente cumpla con la protección de datos y el secreto corporativo.

04 · GUÍA PRÁCTICA

¿Cómo debemos usar la IA en nuestro día a día?

Para mantener un entorno seguro, recuerda estas pautas clave:

✓ **Usa solo herramientas autorizadas**

Si necesitas apoyo de IA para tus tareas, consulta con el área de TI/Ciberseguridad cuáles son las plataformas oficiales aprobadas por el grupo.

× **Nunca compartas datos confidenciales en plataformas públicas**

No pegues contraseñas, código fuente de la empresa, datos financieros ni información personal de clientes o empleados en herramientas de IA abiertas o gratuitas.

◎ **La regla de la doble verificación ante fraudes**

Si recibes una solicitud inusual por audio o video de un superior pidiendo acciones urgentes, corta y comunícate por un canal oficial verificado.

¿DETECTASTE ALGO SOSPECHOSO?

No te lo guardes. Repórtalo al equipo de Ciberseguridad con el botón de reporte de correo o escribiendo a:

Reportar a
[Correo de Seguridad]

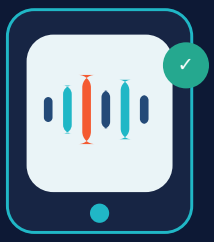
DESAFÍO · PÁG. 3

Fuentes: NIST · Riesgos de IA generativa | Microsoft · Protección y privacidad

05 · EL RINCÓN DEL DESAFÍO

Respuesta del desafío

Una voz conocida no confirma quién está al otro lado.



RESPUESTA REVELADA · CORRECTA: B

B

No. Debo llamarlo directamente por un canal oficial para confirmar la solicitud.

La respuesta aparece aquí al elegir una opción del desafío en la página 3.

RESPUESTA CORRECTA: B

La clonación de voz por IA es hoy económica y accesible para los ciberdelincuentes. Una voz conocida no es prueba de identidad.

IA SÍ, PERO SEGURA:

herramientas aprobadas · datos protegidos · doble verificación

EQUIPO DE CIBERSEGURIDAD

Boletín interno para colaboradores de las empresas del Grupo · Edición #13

No reenvíes este correo fuera de la organización.

VOLVER A LA PREGUNTA · PÁG. 3

Fuentes: FTC · Clonación de voz