Desinformación e inteligencia artificial

Riesgos y herramientas para verificar antes de compartir.

¿Qué es la desinformación?

Es información falsa o engañosa que se crea o se difunde a propósito para engañar o manipular. Puede incluir datos inventados, contenidos reales alterados o información verdadera presentada fuera de contexto.

La **información errónea**, en cambio, también es falsa o inexacta, pero se comparte sin intención de dañar. Distinguir una de otra ayuda a entender cómo circulan los contenidos y cómo actuar.

¿Para qué se usa?

- Generar confusión, miedo o desconfianza.
- Influir en opiniones o decisiones.
- Dañar la reputación de personas u organizaciones.
- Conseguir visitas, interacciones o dinero con títulos engañosos.
- Facilitar fraudes o suplantaciones de identidad.

El impacto de la inteligencia artificial

La **IA generativa** permite crear o modificar textos, imágenes, audios y videos muy rápido. Entre esos contenidos están los **deepfakes**: piezas sintéticas o manipuladas que muestran, de forma convincente, a personas diciendo o haciendo algo que nunca pasó.

Estas tecnologías también pueden ayudar a analizar y detectar contenidos falsos. Pero ninguna herramienta automática es una prueba definitiva: verificar requiere revisar el origen, el contexto y otras fuentes confiables.

Riesgos de los contenidos sintéticos

Los deepfakes y otros contenidos manipulados pueden usarse para desinformar, imitar voces, hacerse pasar por autoridades o referentes, dañar la reputación de una organización o facilitar estafas. Por eso, que una imagen, un audio o un video parezca real no alcanza para darlo por auténtico.

Cómo verificar antes de compartir

- **Frená antes de reaccionar:** los mensajes que buscan provocar miedo, enojo o urgencia merecen una revisión extra.
- **Leé más allá del título:** fijate si el contenido completo sostiene lo que dice el título y si aporta datos comprobables.
- **Buscá la fuente original:** revisá autoría, fecha, dirección del sitio y la primera publicación, no solo la cuenta que lo compartió.
- **Contrastá con otras fuentes:** consultá organismos oficiales, medios confiables, especialistas o verificadores reconocidos.

- **Revisá el contexto:** comprobá si la imagen, la frase o el video corresponden al lugar, la fecha y el hecho que se les atribuyen.
- **Verificá imágenes y videos:** hacé una búsqueda inversa de imágenes o de fotogramas para detectar reutilizaciones, ediciones o contenidos fuera de contexto.
- **Confirmá los pedidos sensibles por otro canal:** si un audio o video te pide dinero, contraseñas, información reservada o una acción urgente, contactá a esa persona u organización por un medio que conozcas.
- **No te guíes solo por errores visuales:** las fallas pueden ser una señal de alerta, pero que no las haya no prueba que el contenido sea real.

En resumen

Pausá	No compartas un contenido solo por su impacto o urgencia.
Verificá	Revisá la fuente, la fecha, el contexto y la evidencia.
Contrastá	Buscá confirmación en fuentes confiables e independientes.
Protegé	No entregues datos, dinero ni contraseñas a partir de un mensaje sin verificar.

Ante la duda, no compartas. La pausa y el pensamiento crítico son las mejores defensas frente a la desinformación. Desde **BA-CSIRT** promovemos una ciudadanía digital informada.