

Defensa de la Integridad Democrática: Desinformación e Infodemia

Estrategias de análisis y respuesta operativa para el Instituto Nacional Electoral

Identificación:

Diferenciar tipologías y patrones narrativos.

Comprensión:

Analizar mecanismos técnicos (algoritmos) y psicológicos (sesgos).

Respuesta:

Diseñar criterios de intervención proporcional, oportuna y estratégica.

El Mandato Operativo: De la Observación a la Defensa Estratégica

El objetivo no es solo desmentir noticias falsas, sino fortalecer la capacidad analítica y operativa del INE para proteger la integridad institucional.

“La confianza pública es el activo más valioso en un contexto de infodemia.”

Precisión Conceptual: La Taxonomía del Caos Informativo

Desinformación (Disinformation)



Información falsa creada deliberadamente con intención de dañar (instituciones, personas o procesos).

Misinformation



Información falsa compartida sin intención de daño (error, confusión).

Infodemia



La sobreabundancia de información (precisa y falsa) que dificulta que las personas encuentren fuentes y orientación fidedigna.

El factor crítico para la respuesta institucional es la intención y la coordinación, no solo la falsedad del contenido.

Tipologías de la Decepción en Contextos Políticos



Contenido Fabricado

Nuevo contenido es 100% falso, diseñado para engañar y dañar.



Contenido Manipulado

Información o imágenes genuinas alteradas para cambiar la narrativa.



Contexto Falso

Contenido genuino compartido con información contextual falsa (ej. foto antigua presentada como actual).



Contenido Impostor

Suplantación de fuentes genuinas (ej. logos del INE en comunicados falsos).



Sátira o Parodia

Sin intención de daño inicial, pero con potencial de engañar.



Conexión Falsa

Titulares que no respaldan el contenido del artículo (clickbait).

La Nueva Frontera: Inteligencia Artificial y Contenido Sintético

Deepfakes

Definición: Uso de IA para reemplazar rostros o voces con alto realismo.

Riesgo Electoral: Videos de funcionarios o candidatos diciendo cosas que nunca dijeron.

Generación Automatizada

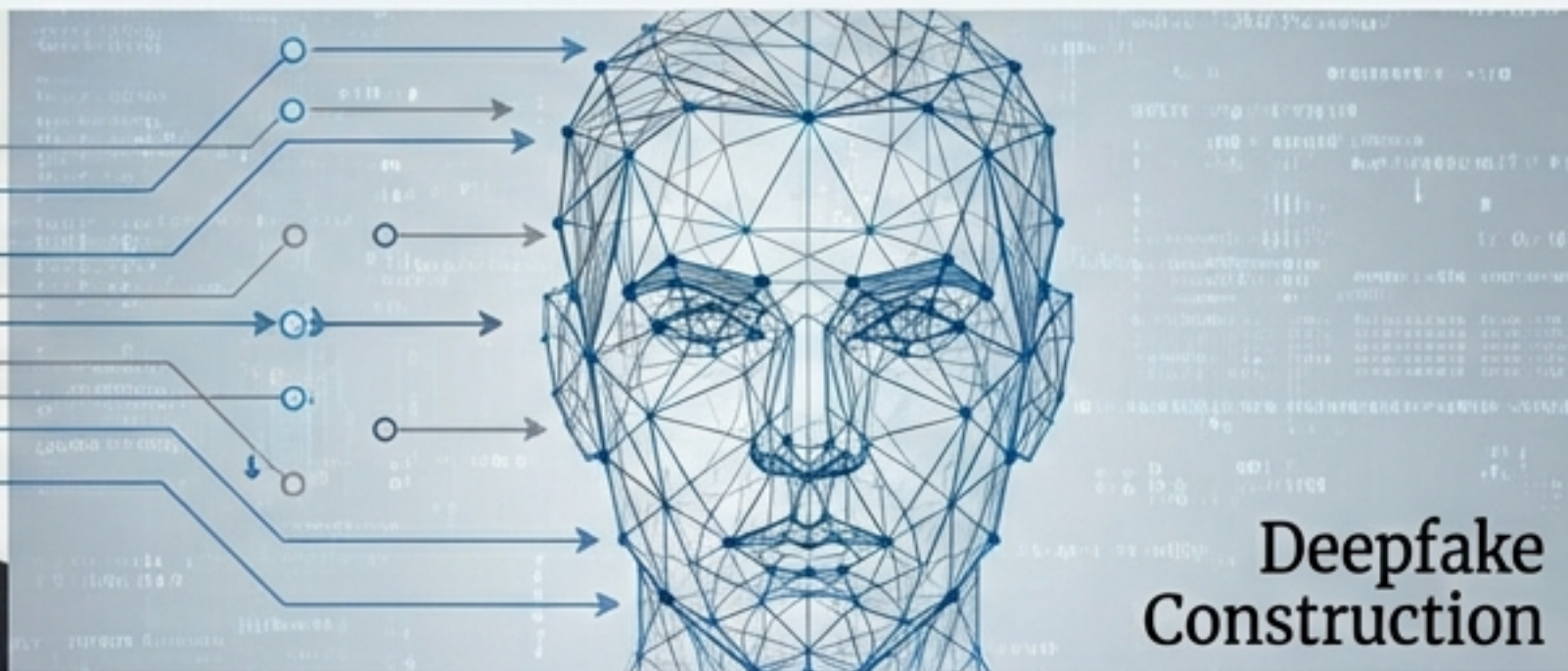
Creación masiva de textos y narrativas mediante LLMs para saturar el discurso público.

Microsegmentación

Uso de IA para adaptar mensajes falsos a perfiles psicológicos específicos de votantes.

Wireframe Analysis

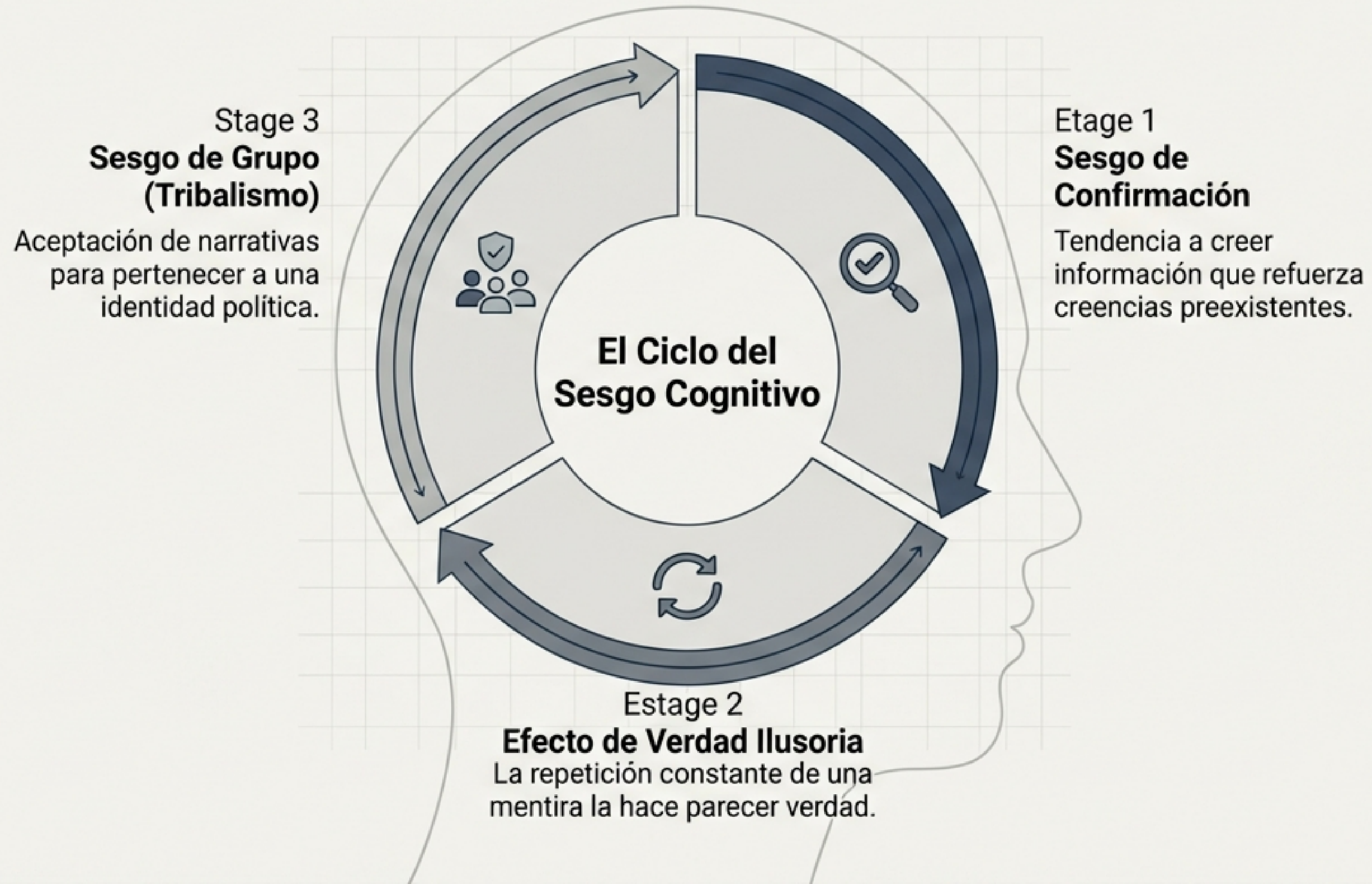
Original



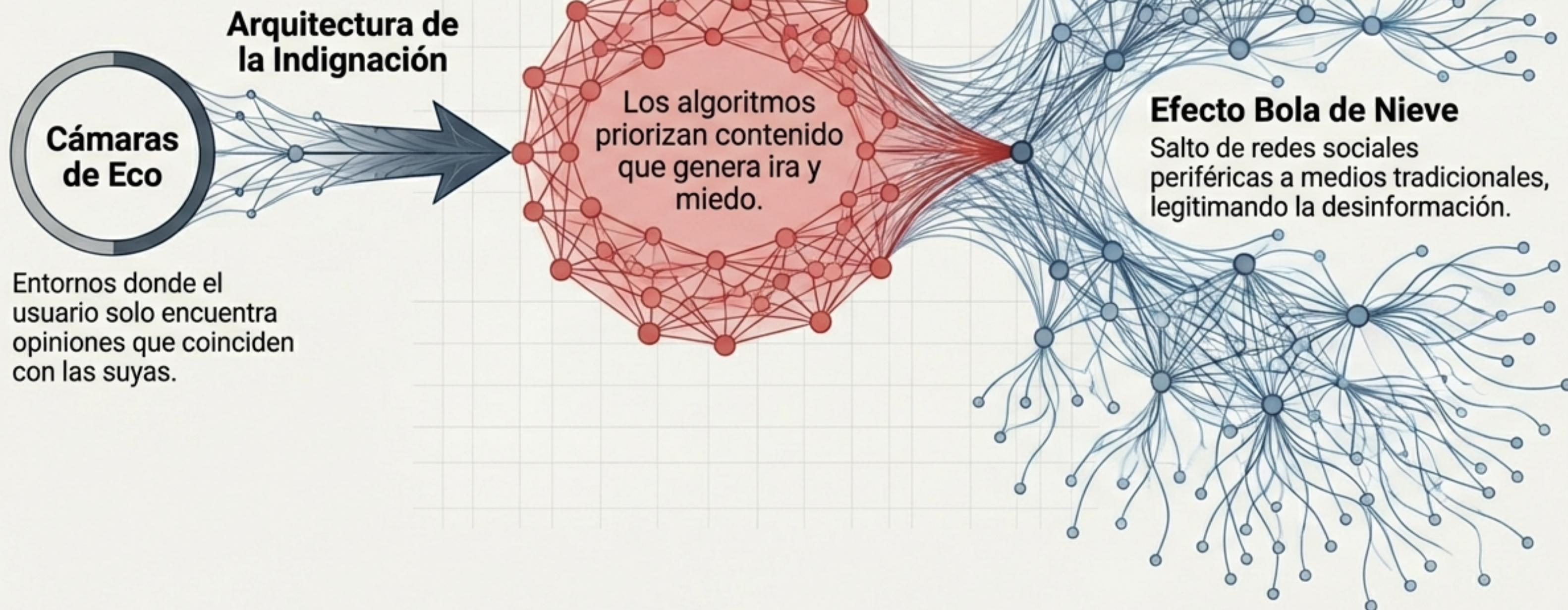
Deepfake Construction

Mecanismos Psicológicos de la Credulidad

La viralización no depende solo de los algoritmos, sino de cómo el contenido apela a las emociones y prejuicios del electorado.



Arquitectura de la Viralización: El Motor Algorítmico



Actores de la Desinformación: Orgánico vs. Inorgánico

Comportamiento Inorgánico (Coordinado)



Bots

Cuentas automatizadas para inflar métricas y simular apoyo popular.



Granjas de Contenido

Operaciones humanas pagadas para generar y difundir noticias falsas masivamente.



Astroturfing

Simulación de movimientos ciudadanos espontáneos.

Amplificadores



Influencers Políticos

Nodos clave para la diseminación de narrativas.



Redes de “Tontos Útiles”

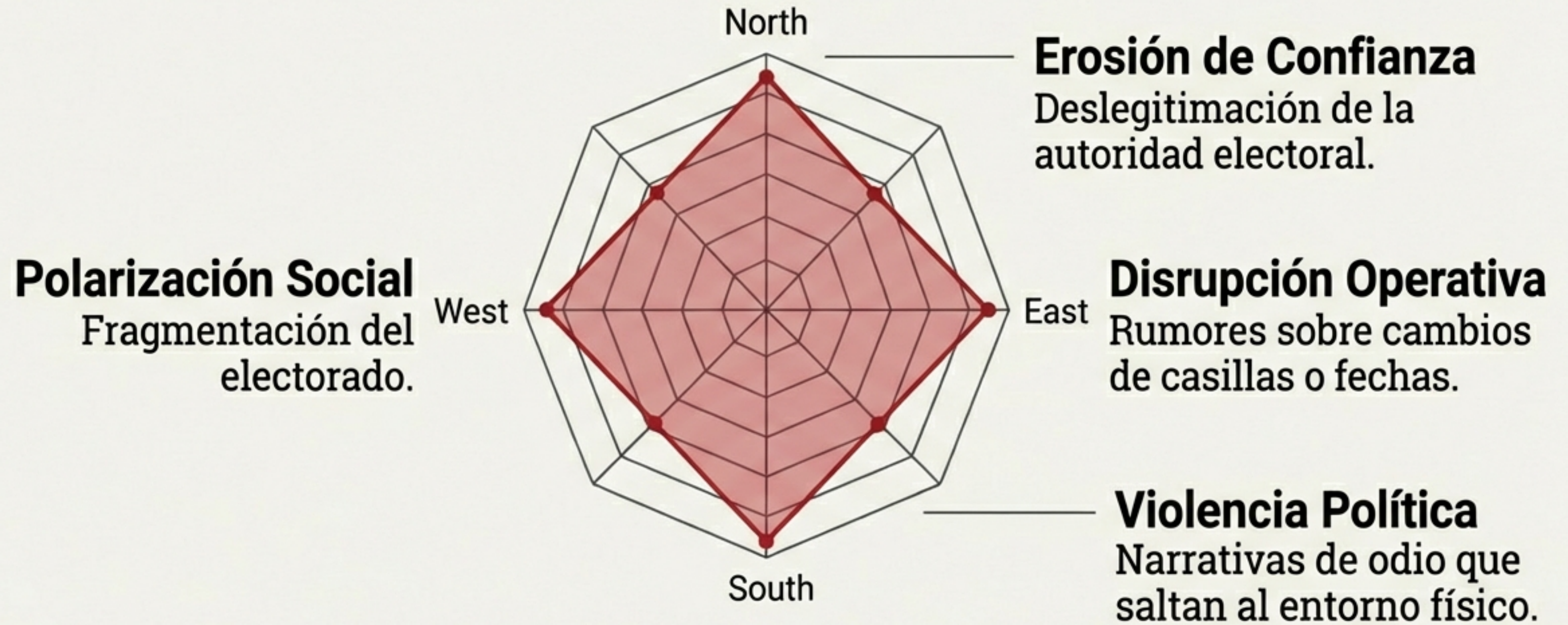
Usuarios reales que comparten desinformación sin saberlo.

El Campo de Batalla: Ecosistemas Abiertos vs. Cerrados

Redes Abiertas (X, Facebook, TikTok)	Dark Social (WhatsApp, Telegram)
● Visibilidad pública. ● Posibilidad de monitoreo y “fact-checking” directo. ● Viralidad rápida y masiva.	● Alta opacidad (encriptado). ● Dificultad de monitoreo y medición. ● Confianza alta (el mensaje viene de un familiar).

Strategic Note: En América Latina, WhatsApp es el vector primario de desinformación indetectable.

Evaluación del Daño: Riesgos Institucionales y Reputacionales



El objetivo final de las campañas de desinformación es la parálisis institucional.

Estrategia de Defensa I: Monitoreo y Escucha Estratégica



1. Detección

Uso de herramientas de social listening para identificar picos de conversación inusuales.



2. Análisis de Sentimiento

Evaluar la carga emocional (negativa/positiva) hacia el INE.



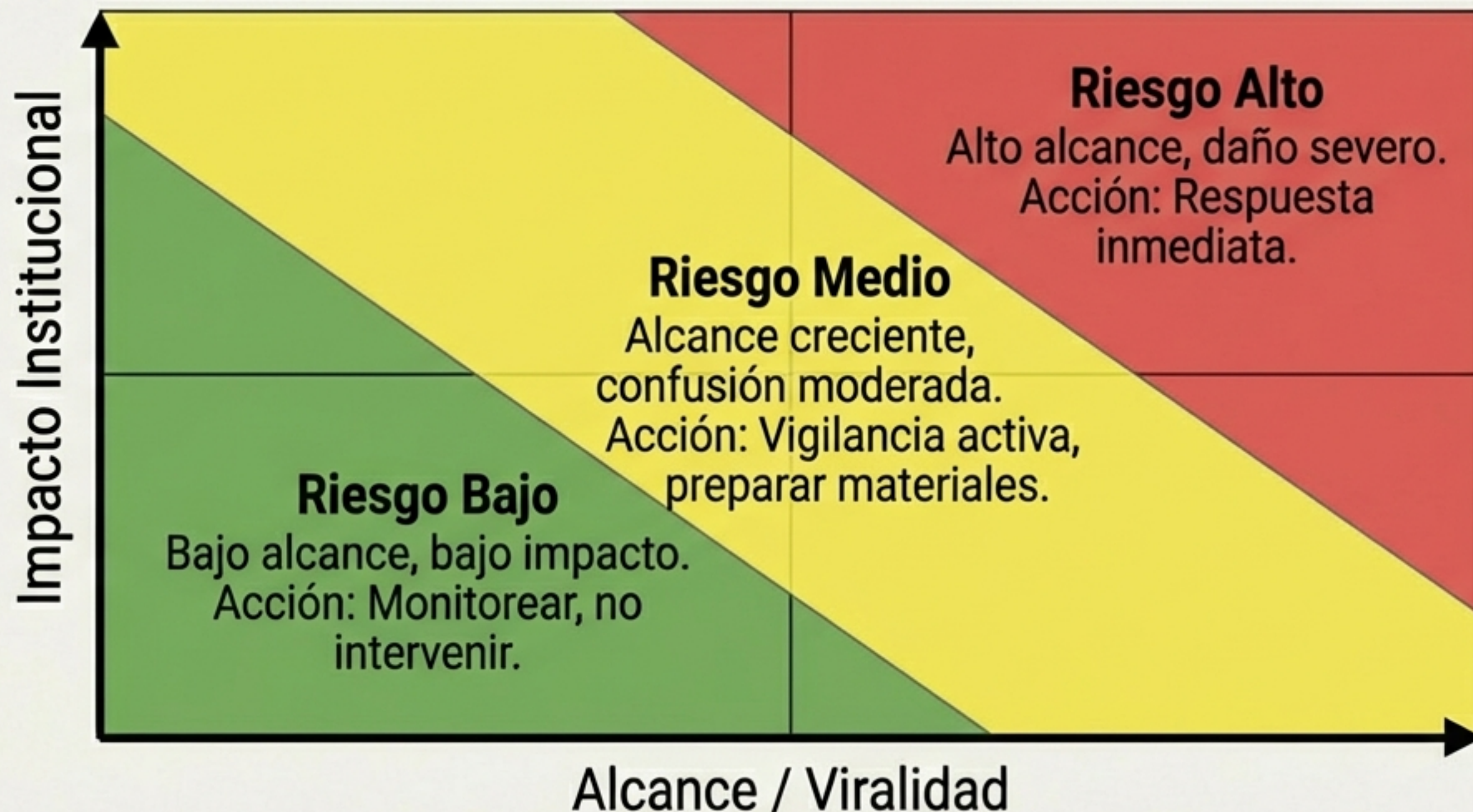
3. Mapeo de Nodos

Identificar quién inicia y quién amplifica la narrativa.

Action Item: Establecer alertas tempranas sobre palabras clave críticas (fraude, casillas, caída del sistema).

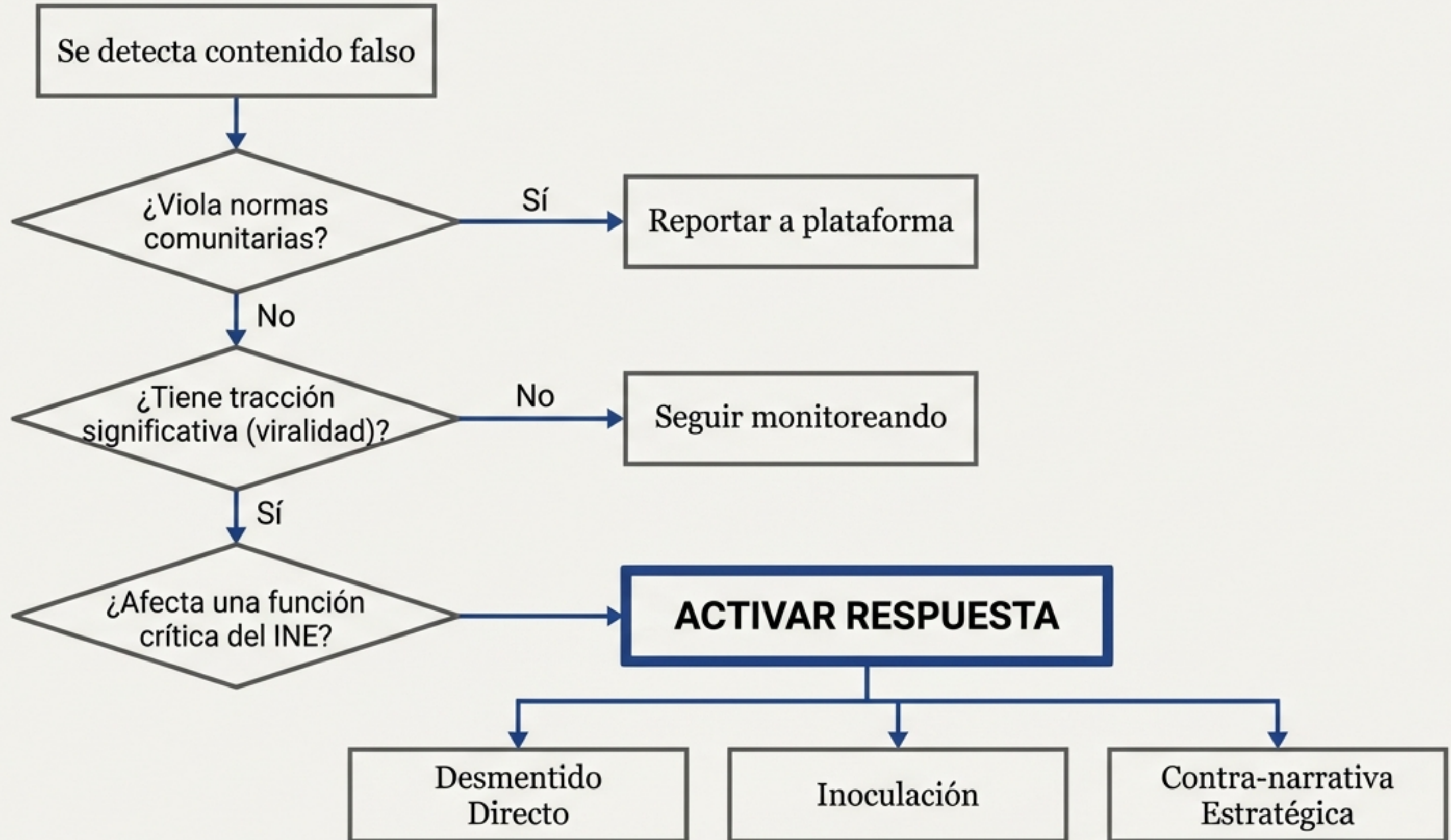
Estrategia de Defensa II: Clasificación y Triage del Riesgo

Impacto vs. Viralidad



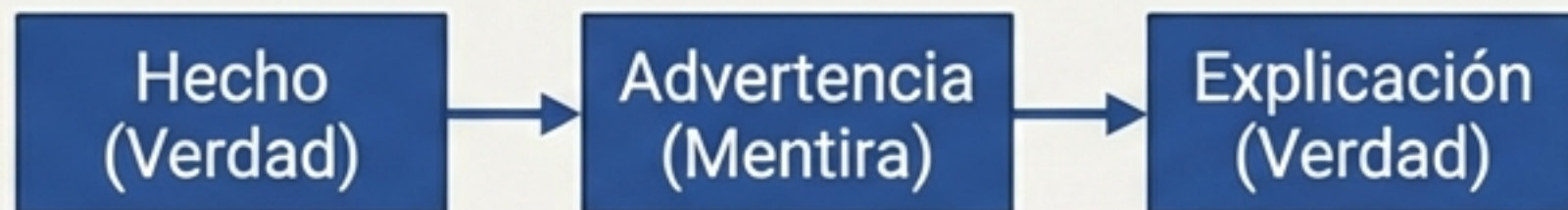
El “Efecto Streisand”:
Responder a una mentira irrelevante puede darle la visibilidad que no tenía.

Protocolo de Respuesta Proporcional



Comunicación y Coordinación Interinstitucional

Sandwich de la Verdad



Evitar repetir la mentira sin contexto.

Narrativa Preventiva (Pre-bunking)

Educar a la ciudadanía sobre posibles tácticas antes de que ocurran.

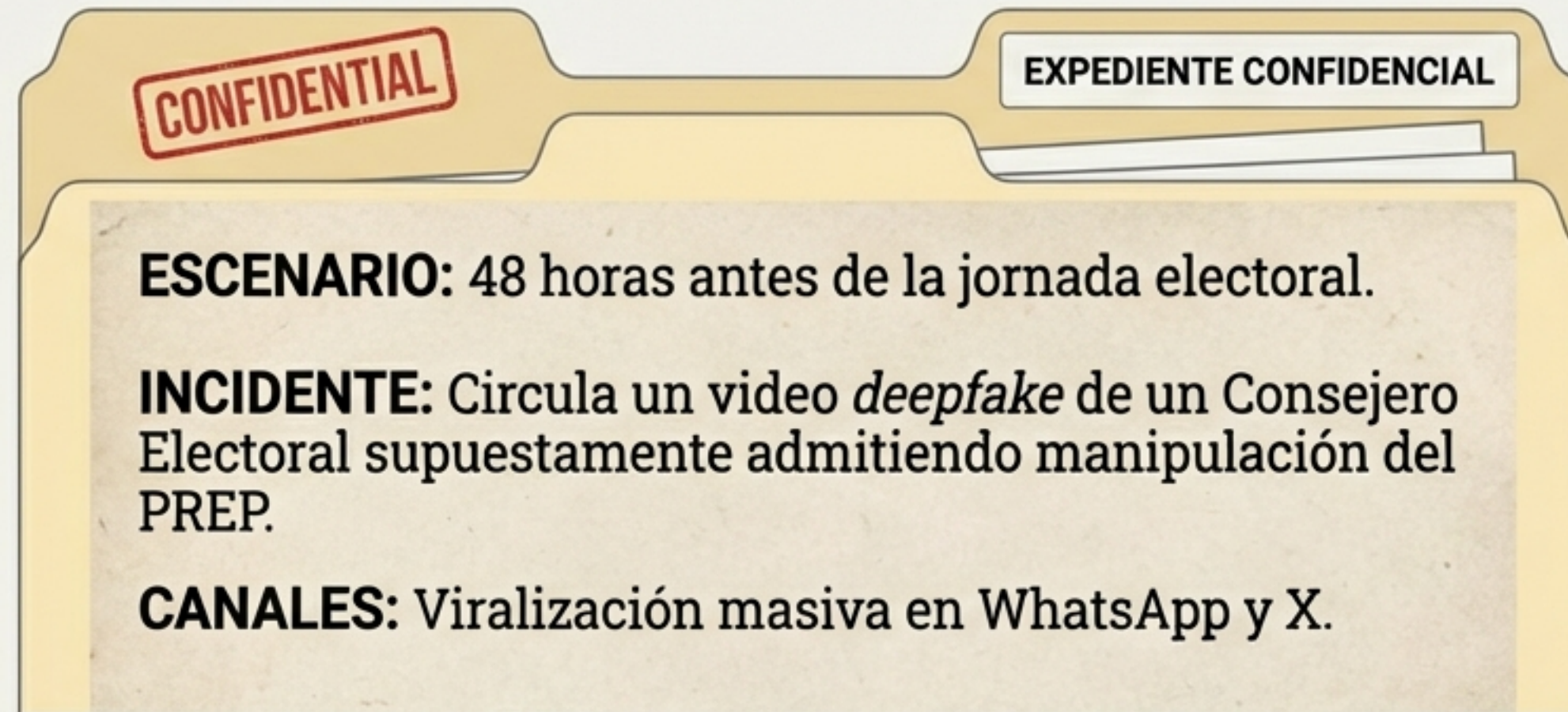
Alianzas

Coordinación con plataformas digitales, medios y organizaciones de verificación.

Transparencia

La mejor defensa es la apertura radical de datos e información oficial.

Taller Aplicado: Simulación de Crisis



Asignación

1. Evaluar el nivel de riesgo en la matriz.
2. Diseñar la cadena de mando para la aprobación de la respuesta.
3. Redactar el mensaje clave para la ciudadanía y medios.

La preparación en tiempos de calma define la eficacia en tiempos de crisis.