

LABORATORIO · SERIE 984

Del dato a la decisión

Manual breve y ejercicio integrador de ciberinteligencia

Ciclo de inteligencia · Requerimientos · Obtención · Valoración 6×6 · Hipótesis · Difusión

DOCUMENTO PARA DISTRIBUCIÓN ACADÉMICA. Los documentos del caso 984 son ficticios y están identificados como tales. Las fuentes doctrinarias, normativas y el caso KA-SAT se citan mediante enlaces públicos verificables.

Jornadas sobre Ciberseguridad | Neuquén, 14–16 de octubre de 2026

Pablo Gris Muniagurria · Material complementario de la conferencia de ciberinteligencia

Edición: 14 de octubre de 2026 · Versión 1.0 (docente)

01 / Cómo aprovechar este material

Este documento acompaña un laboratorio HTML autónomo. No pretende reemplazar doctrina institucional ni habilitar actividades de inteligencia. Enseña a producir y auditar un razonamiento a partir de información pública y de un escenario ficticio.

Resultado esperado

Al finalizar, el participante debería poder redactar una apreciación ejecutiva de una página que separe hechos, información de terceros, inferencias, nivel de confianza, vacíos y opciones de decisión.

Recorrido sugerido (25 a 35 minutos de trabajo personal)

Tramo	Tiempo	Resultado
Lectura inicial del caso	3 min	Definir qué decisión requiere apoyo
Hipótesis y EEI	6 min	No confundir coincidencia con autoría
Plan / orden de obtención	5 min	Definir fuentes abiertas y productos
Fuentes y valoración	6 min	Evaluar confiabilidad y corroboración
Apreciación y contraste	7 min	Distinguir juicio y sustento
Cierre / caso real	5 min	Comparar con KA-SAT

Regla del laboratorio

El problema no es acumular datos: es reducir incertidumbre de forma trazable para apoyar una decisión. Las conclusiones deben ser proporcionales a la calidad de las fuentes.

Todas las fichas INF-984, nombres de organizaciones, fechas de simulación y extractos de prensa de la práctica son construcciones docentes. No describen personas, hechos o investigaciones reales.

Marco metodológico: adaptación original para docencia, consistente con la estructura del ciclo de inteligencia presentada en la conferencia y con orientaciones públicas UNODC y ODNI [1, 2].

02 / La inteligencia no es una carpeta de datos

Dato: registro puntual sin interpretación suficiente para decidir. Información: dato o conjunto de datos contextualizados y relacionados. Inteligencia (producto): juicio analítico producido mediante un proceso sistemático, con fuentes valoradas, incertidumbre explícita y destinatario definido.

Ciclo de trabajo simplificado

Fase	Pregunta operativa	Producto
Dirección / planeamiento	¿Qué debe decidirse? ¿Qué se necesita conocer?	Requerimientos y prioridades
Obtención / reunión	¿Qué fuentes autorizadas podrían responder?	Informes de información
Elaboración y análisis	¿Qué hipótesis explican los datos?	Juicios, escenarios y confianza
Difusión / retroalimentación	¿Qué necesita saber el decisor, y cuándo?	Apreciación ejecutiva

Es un ciclo iterativo: la obtención adicional se ordena en función de vacíos relevantes y la utilidad temporal del producto. La difusión oportuna forma parte de su valor. [1, 2]

No son equivalentes

Inteligencia aplicada a riesgos	Investigación criminal
Pregunta: ¿qué podría ocurrir, con qué escenarios y bajo qué incertidumbre?	Pregunta: ¿qué ocurrió, quién intervino y cómo acreditar los hechos jurídicamente?
Producto: apreciación para decisión y prevención	Producto: información y evidencia sometidas a garantías y reglas procesales
Una inferencia puede ser útil si su incertidumbre está delimitada.	Una inferencia no reemplaza autenticidad, integridad ni admisibilidad de la prueba.

La frontera es de finalidad, competencia y garantías; en una misma situación pueden coexistir análisis preventivos e investigación de un hecho concreto. Para la Argentina, la norma aplicable debe consultarse en su texto actualizado [5].

03 / Dirección: requerimientos, EEI y obtención

De la misión a lo esencial

MISIÓN: apoyar una decisión concreta. RR.Icia.: aquello que debe conocerse para cumplir esa misión. EEI (elemento esencial de información): requerimiento cuya ausencia impide, compromete o modifica significativamente la decisión. ORI: otros requerimientos complementarios.

Los EEI no se eligen por curiosidad ni por facilidad de búsqueda. Se seleccionan por relevancia para el decisor y por la consecuencia práctica de desconocerlos.

PO-984: plan docente de obtención

EEI	Indicador	Fuente abierta	Plazo	Producto
01	¿Hay vínculo operativo verificable entre episodios?	Comunicados, cronologías y prensa con fuentes diferenciadas	48–72 h	Matriz de coincidencias y diferencias
02	¿Existe una atribución pública sustentada?	Autoridades competentes y reportes originales	72 h	Nota de atribución publicada y límites
ORI	¿Qué consecuencias sectoriales se describen?	Comunicados y estadísticas agregadas	5 días	Panorama de impacto

OO-984-01: orden simulada

OBJETO: reunir y comparar referencias públicas sobre incidentes ficticios. RESPONSABLE: equipo académico de fuentes abiertas. PRIORIDAD: alta. PLAZO: 72 h. LÍMITES: sin interacción con presuntos autores, sin acceso intrusivo, sin datos privados, sin individualizaciones. RESULTADO: parte con URL o procedencia, fecha, hechos, contradicciones y vacíos.

La tabla es una plantilla creada para docencia: no es una orden real, un modelo oficial ni una habilitación para realizar operaciones. La orden efectiva depende de las competencias y autorizaciones exigidas por el marco legal. [5]

04 / Reunión y valoración: sistema 6 × 6

La valoración de la confiabilidad de la fuente y de la validez de la información debe realizarse en dos dimensiones distintas. La escala 6×6, descrita por UNODC, se emplea aquí como referencia didáctica, no como sustituto del juicio analítico. [1]

Confiabilidad de la fuente (A–F)

Código	Descripción sintética
A	Completamente confiable
B	Habitualmente confiable
C	Relativamente confiable
D	Habitualmente poco confiable
E	No confiable
F	No es posible valorarla

Validez del dato o información (1–6)

Código	Descripción sintética
1	Confirmada por fuentes independientes
2	Probablemente verdadera; coherente, sin confirmación independiente
3	Posiblemente verdadera; plausible, sin corroboración
4	Dudosa, aunque posible
5	Improbable; contradicha por otra evidencia
6	No es posible valorarla

Una institución fiable (A o B) puede retransmitir un rumor no corroborado (3 o 6). A la inversa, una fuente poco conocida (F) puede aportar información luego confirmada independientemente (1). No se debe convertir la notación 6×6 en una probabilidad matemática.

Registro mínimo de cada pieza

ID · fecha de publicación · fecha de consulta · fuente primaria/secundaria · URL de origen · texto o dato relevante · independencia respecto de otras fuentes · valoración provisional · limitación conocida.

05 / Hipótesis alternativas e incertidumbre

Un distintivo, un nombre de grupo o una frase similar no demuestran coordinación ni identidad de autor. La coincidencia puede explicarse por acción conjunta, imitación o circulación de un mismo mensaje entre actores independientes.

CASO-984: tres explicaciones rivales

Clave	Hipótesis	Predicción discriminante
H1	Los episodios responden a coordinación operativa	Aparecen patrones adicionales verificables e independientes
H2	Al menos una reivindicación imita una identidad grupal	Inconsistencias cronológicas y ausencia de continuidad operativa
H3	Se trata de episodios separados con señales comunicacionales compartidas	Similitudes textuales pero contextos y secuencias no relacionados

Preguntas de control antes de atribuir

- ¿La segunda noticia repite la primera o obtiene confirmación independiente?
- ¿La fuente afirma haber visto un hecho o solo reproduce una declaración?
- ¿La evidencia también sería esperable si H2 o H3 fueran correctas?
- ¿Qué información concreta cambiaría nuestra conclusión?
- ¿Qué incertidumbre permanece incluso después de la búsqueda?

Los estándares ICD 203 recomiendan distinguir información subyacente, supuestos y juicios analíticos; explicar incertidumbres, evaluar alternativas y atender la utilidad para el destinatario. [2]

La falta de prueba de coordinación NO prueba que no existió coordinación. Pero tampoco autoriza a declarar una autoría o una estructura organizacional.

06 / GPT como asistente, no como fuente

Una herramienta generativa puede asistir en la formulación de hipótesis, la construcción de matrices o la revisión de contradicciones. Sus respuestas son borradores sujetos a cotejo con fuentes originales y evaluación humana.

Prompt 1: apertura de hipótesis

Sobre las siguientes tres fichas ficticias, proponé tres hipótesis alternativas que expliquen su posible relación. Para cada una, indicá: hechos compatibles, hechos que la debilitan, un indicador discriminante y qué NO puede concluirse. No atribuyas autoría. Separá la información de las inferencias.

Prompt 2: auditoría adversarial

Actuá como revisor crítico. Detectá fuentes dependientes entre sí, saltos lógicos, atribuciones no justificadas y lenguaje excesivamente categórico. Devolvé una tabla con hallazgo, gravedad, fundamento textual y propuesta de corrección. No inventes datos.

Prompt 3: apreciación ejecutiva

Redactá una apreciación de 180 palabras para un decisor sobre el caso simulado. Usá apartados: juicio principal; hechos que lo sostienen; hipótesis alternativas; confianza cualitativa; vacíos; y decisión prudente. No uses porcentajes sin base empírica.

Límites obligatorios

- No ingresar datos de expedientes, víctimas ni personas identificadas.
- No presentar como citas enlaces, documentos ni hechos que el modelo no haya recibido y que no hayan sido verificados.
- Registrar qué aporte realizó la IA y qué comprobó la persona responsable.
- No usar el asistente para proponer accesos, vigilancia o actividades sin habilitación.

El estándar de calidad de la apreciación sigue siendo humano: trazabilidad, proporcionalidad del juicio, contraste de alternativas y pertinencia decisoria. [2]

07 / La apreciación: utilidad, no acumulación

La pieza final debe responder una pregunta del decisor sin confundir confirmaciones y posibilidades. Una síntesis útil puede ser breve; una síntesis poco clara, aunque contenga muchos datos, puede resultar inservible.

Plantilla AP-984, una página

Campo	Contenido esperado
Destinatario y fecha	A quién va dirigida, momento de elaboración
Pregunta a resolver	¿Hay indicios suficientes de coordinación entre episodios?
Juicio principal	Conclusión condicionada y alcance exacto
Base verificable	Tres referencias numeradas como máximo
Hipótesis alternativas	Qué explicaciones continúan abiertas
Confianza	Alta, media o baja; explicar por qué, no solo etiquetar
Vacios prioritarios	Dato concreto que mejoraría la decisión
Implicación / decisión	Acción preventiva prudente, proporcional y legal

Criterio de revisión final

- ¿Puede el decisor distinguir en menos de un minuto qué se sabe y qué se estima?
- ¿Cada afirmación factual remite a una ficha rastreable?
- ¿La frase de conclusión sería distinta si una fuente duplicada se elimina?
- ¿Se describió la incertidumbre que realmente afecta la decisión?
- ¿El producto evita convertirse en una imputación criminal?

La publicación y el intercambio de inteligencia de amenazas requieren reglas de difusión y control del destinatario. FIRST TLP 2.0 y NIST SP 800-150 son referencias públicas útiles, sin reemplazar la normativa propia. [3, 4]

08 / Caso 984: paquete de documentos ficticios

Escenario: una organización necesita valorar si tres comunicaciones públicas con lenguaje semejante indican un episodio coordinado o simplemente una difusión imitativa. El fin del ejercicio es apoyar una decisión preventiva general, no identificar personas.

INF-984/01 · Medio regional simulado, 12/10/2026

Se publica una nota sobre un presunto incidente digital contra el servicio X. El medio reproduce una captura de un mensaje que usa la marca «984»; indica que no logró confirmación técnica independiente del supuesto incidente.

INF-984/02 · Comunicado institucional simulado, 13/10/2026

La entidad Y informa que recibió mensajes intimidantes con el mismo distintivo. Aclara que en su revisión preliminar no detectó afectación de sistemas y que no dispone de elementos para atribuir origen.

INF-984/03 · Segundo medio simulado, 13/10/2026

Una nota afirma que los hechos de X e Y «serían parte de una campaña». Su única referencia explícita para X es la publicación de INF-984/01 y para Y es el comunicado de INF-984/02.

INF-984/04 · Nota de cierre simulada, 14/10/2026

Una consulta académica a fuentes abiertas no localiza informes públicos independientes que conecten los episodios. La ausencia de esos informes se registra como «información no localizada», no como prueba de inexistencia.

Aviso: nada de lo expuesto en estas cuatro fichas corresponde a publicaciones reales. Los códigos son internos del ejercicio. La referencia «984» conserva continuidad pedagógica con la conferencia, no presupone vínculo fáctico con sujetos o grupos reales.

09 / Caso 984: resolución de referencia

Plan y orden

EEL-01: ¿existe evidencia independiente de coordinación operativa? Indicadores: cronología comprobable, artefactos técnicos coincidentes de procedencia verificable y comunicados originales. OO-984-01: obtener exclusivamente fuentes abiertas, registrar procedencia y elaborar matriz de corroboración.

Valoración orientativa, no automática

Ficha	Juicio didáctico	Por qué
INF-984/01	F/3 o F/6 para la reivindicación	Se desconoce historial de la fuente; la captura no corrobora el hecho ni la autoría
INF-984/02	B/2 provisional para el acto de publicar el comunicado	Se identifica el emisor; la afirmación técnica sigue siendo autodeclarada
INF-984/03	F/3 para la tesis de «campaña»	No aporta corroboración independiente y encadena citas
INF-984/04	No es prueba negativa concluyente	La no localización de información no demuestra inexistencia

Las valoraciones varían según la pregunta precisa: puede estar confirmada la existencia de un comunicado sin estar confirmado su contenido o la identidad del emisor original de una amenaza. No deben asignarse categorías por reputación del medio únicamente.

AP-984 · ejemplo de apreciación

Con la documentación ficticia disponible no se acredita una coordinación operativa entre los episodios X e Y. La semejanza de la etiqueta «984» admite hipótesis alternativas, especialmente imitación o repetición de un mismo mensaje. La tercera publicación no constituye corroboración independiente de la primera.

CONFIANZA: baja para cualquier atribución de coordinación, por ausencia de indicadores discriminantes.

RECOMENDACIÓN: mantener seguimiento de comunicados verificables y reforzar controles preventivos generales sin imputar autoría. Reevaluar si surgen registros técnicos o fuentes primarias independientes.

10 / Una prueba de realidad: KA-SAT (2022)

Para no confundir simulación con evidencia real, este caso adicional se apoya únicamente en fuentes públicas citadas. Su uso es comparativo: enseña a separar el relato del operador, el impacto observado y una atribución efectuada por un actor estatal.

Tres niveles que no deben fusionarse

Afirmación	Soporte público	Qué permite concluir
El 24/02/2022 hubo una interrupción parcial del servicio satelital KA-SAT	Informe del operador Viasat de 30/03/2022 [6]	Existencia, cronología y alcance reportado por el operador
El incidente afectó clientes en Ucrania y otras partes de Europa	Viasat [6]	Impacto descrito y límites de la investigación publicados
La Unión Europea atribuyó públicamente la actividad a la Federación de Rusia	Declaración institucional del Consejo de la UE, 10/05/2022 [7]	Que hubo una atribución oficial de la UE; no convierte al participante en perito de autoría

Preguntas para el análisis

- ¿Qué contenidos serían hechos documentados por el operador y cuáles son sus interpretaciones?
- ¿Quién formula la atribución estatal y cuál es el alcance de esa fuente?
- ¿Qué nueva información haría variar la recomendación de continuidad operativa?
- ¿Qué sería distinto en una investigación penal respecto de una apreciación estratégica?

No se reproducen informes íntegros: se incluyen referencias a sus ubicaciones originales. El material no afirma haber verificado de modo independiente los hechos técnicos descritos por el operador.

11 / Publicación, competencias y controles

Cinco condiciones de distribución

1. Revisión jurídica: cualquier referencia a facultades de organismos argentinos debe cotejarse con el texto vigente de la Ley 25.520 y normas aplicables [5].
2. Origen transparente: datos ficticios identificados; fuentes reales con autor, fecha y enlace; inferencias del autor etiquetadas como tales.
3. Derechos de autor: disponibilidad pública no equivale a permiso para reproducir documentos enteros; preferir síntesis propia y enlace al original.
4. Protección de datos: no agregar víctimas, identidades privadas, información de expedientes ni registros sensibles a ejemplos distribuidos.
5. Difusión: respetar los límites de compartición que correspondan a documentos de terceros. TLP 2.0 distingue distintos alcances de redistribución [4].

Uso académico / uso institucional

Las matrices PO-984 y OO-984 se publican únicamente para explicar un método. No son instrucciones operativas reales, no sustituyen autorizaciones, no justifican el tratamiento de datos privados y no pueden presentarse como instrumentos oficiales de ningún organismo.

Puente con la clase de cibercrimen

La próxima pregunta no es «¿qué sabemos del riesgo?», sino «¿qué hechos podríamos reconstruir y acreditar, con qué evidencias y garantías?». Separar los dos carriles permite aprovechar el valor anticipatorio de la inteligencia sin sobreextender las inferencias en sede penal.

12 / Bibliografía pública y trazabilidad

[1] UNODC (2011). Criminal Intelligence Manual for Managers. Capítulo sobre evaluación de fuentes y datos, matrices 4×4 y 6×6.

https://css.unodc.org/documents/organized-crime/Law-Enforcement/Criminal_Intelligence_for_Managers.pdf

[2] ODNI. Intelligence Community Directive 203: Analytic Standards.

<https://www.dni.gov/files/documents/ICD/ICD-203.pdf>

[3] NIST. SP 800-150, Guide to Cyber Threat Information Sharing.

<https://csrc.nist.gov/pubs/sp/800/150/final>

[4] FIRST (2022). Traffic Light Protocol, TLP 2.0.

<https://www.first.org/tlp/>

[5] Argentina. Ley 25.520, texto actualizado (consultar cambios normativos).

<https://www.argentina.gob.ar/normativa/nacional/ley-25520-70496/actualizacion>

[6] Viasat (30/03/2022). KA-SAT Network Cyber Attack Overview.

<https://www.viasat.com/perspectives/corporate/2022/ka-sat-network-cyber-attack-overview/>

[7] Consejo de la UE (10/05/2022). Operaciones cibernéticas de Rusia contra Ucrania: declaración sobre KA-SAT.

<https://www.consilium.europa.eu/es/press/press-releases/2022/05/10/russian-cyber-operations-against-ukraine-declaration-by-the-high-representative-on-behalf-of-the-european-union/>

Trazabilidad editorial

Parte docente original: modelo CASO-984, H-984, PO-984, OO-984, INF-984 y AP-984. Antecedente: estructura pedagógica del material de conferencia de ciberinteligencia Neuquén 2026. Los textos y situaciones de INF-984 son deliberadamente ficticios. Las equivalencias doctrinarias son resúmenes pedagógicos; para una cita formal debe consultarse siempre el documento original.

Fecha de consulta de las fuentes digitales: 14/10/2026. Este material es una síntesis original, no traducción oficial de ninguna referencia.