IntelKIT

HERRAMIENTAS INTELIGENTES
PARA ANALISTAS DE INTELIGENCIA

METODOLOGÍA ACH

HIPÓTESIS COMPETIDORAS

ACH

MANUAL DE USO · PROFESSIONAL

Análisis de Hipótesis Competidoras
para el juicio entre explicaciones alternativas

Evidencia, diagnosticidad y refutación

VERSIÓN 1.0 | OCTUBRE DE 2026 | Manual de uso de ACH IntelKIT Professional v1.0.xlsx

Uso libre citando la fuente

Índice

1. Cómo utilizar este manual....3
2. Qué es ACH y qué problema resuelve....4
3. El principio de hipótesis competidoras....5
4. El recorrido y las tres capas....6
5. Preparar la pregunta analítica....8
6. Formular las hipótesis....9
7. Registrar la evidencia....11
8. La matriz: valorar cada cruce....12
9. Diagnosticidad....15
10. Intentar refutar....17
11. Los cálculos auxiliares de IntelKIT....20
12. Sensibilidad....22
13. La conclusión provisional....23
14. Indicadores y revisión futura....24
15. El panel y la lectura del analista....25
16. El caso Grupo Alventa, de principio a fin....27
17. Sesgos, límites y errores frecuentes....28
18. Checklist final....29

1. Cómo utilizar este manual

A QUIÉN SE DIRIGE Y CÓMO LEERLO

Este manual enseña a utilizar ACH IntelKIT Professional. No es un tratado sobre análisis de inteligencia: es la guía de una herramienta concreta, y está escrito para leerse con el Excel abierto al lado.

1.1 Para quién está escrito

Se presupone alguna familiaridad con el análisis estructurado, o al menos que la idea de confrontar hipótesis con evidencia no te resulta nueva. No se presupone que conozcas ACH: el método tiene exigencias que no se deducen de otras técnicas, y este manual las explica todas.

Situación	Qué encontrarás aquí
Es tu primera vez con ACH	El método explicado desde cero y un recorrido completo por el Excel
No sabes qué símbolo poner en una celda	La escala explicada con los noventa cruces reales del caso
No entiendes un número	Qué calcula Excel, de dónde sale y qué NO significa
Quieres saber qué puedes afirmar	Qué permite concluir ACH y, sobre todo, qué no

1.2 El caso que recorre todo el manual

Todas las explicaciones se apoyan en un mismo caso: **el incidente de ciberseguridad de Grupo Alventa**. Las capturas de este manual son reales y proceden del archivo `ACH IntelKIT v1.0 — Caso práctico Professional.xlsx`, que se entrega con la herramienta.

EL CASO DE GRUPO ALVENTA

Grupo Alventa es una distribuidora española ficticia de productos sanitarios, con sede en Valladolid y tres centros logísticos. Entre el 9 y el 14 de abril de 2026 detecta actividad anómala en varios equipos y una interrupción parcial del ERP y del sistema de preparación de pedidos.

El analista no sabe de entrada qué ocurrió. Compara **seis explicaciones alternativas** frente a **quince evidencias**. Ninguna cifra del caso debe citarse como dato real: la organización, el incidente y toda la evidencia son ficticios.

1.3 Las tres capas, de principio a fin

La herramienta separa siempre tres cosas, y este manual mantiene esa separación en cada capítulo. Cada vez que veas uno de estos tres recuadros, sabes en cuál de las tres estás.

TÚ INTRODUCES

Lo que escribes tú: la pregunta, las hipótesis, la evidencia con su procedencia, la valoración de cada cruce, el examen de refutación, las evidencias críticas, la conclusión y los indicadores futuros.

EXCEL CALCULA

Lo que hace Excel solo: organizar la matriz, contar categorías, señalar lo que falta por valorar y calcular dos indicadores auxiliares. Nada más.

TÚ INTERPRETAS

Lo que significa el resultado. La herramienta no escribe ninguna conclusión: ordena lo que has introducido y se detiene ahí.

2. Qué es ACH y qué problema resuelve

EL MÉTODO, EN UNA PÁGINA

ACH —*Analysis of Competing Hypotheses*, Análisis de Hipótesis Competidoras— es una técnica de análisis estructurado para juzgar cuestiones importantes cuando existen varias explicaciones alternativas plausibles. Fue formulada por **Richards J. Heuer Jr.** y publicada por la CIA en 1999.

2.1 El principio

Su principio central cabe en una frase: **no evaluar una hipótesis aislada para decidir si parece verdadera, sino enfrentar simultáneamente varias hipótesis alternativas con la misma evidencia.**

El propósito no es demostrar que una hipótesis es verdadera. El procedimiento busca identificar cuáles alternativas quedan peor explicadas por la evidencia disponible y cuáles permanecen compatibles con ella.

2.2 El problema que intenta resolver

Heuer sitúa ACH dentro de una preocupación más amplia: las limitaciones del razonamiento humano cuando trabaja con información incompleta, ambigua o contradictoria. Tres problemas importan especialmente.

Problema	En qué consiste
Anclaje en una primera explicación	El analista adopta demasiado pronto una explicación que encaja con los primeros datos. Cuando se convierte en la hipótesis favorita, la evaluación posterior tiende a buscar confirmación.
Generación incompleta de alternativas	Una conclusión solo puede competir con las hipótesis que hayan sido formuladas. Las personas no somos buenas generando por nuestra cuenta un conjunto completo de explicaciones plausibles.
Evidencia compatible con demasiadas hipótesis	Muchos datos parecen apoyar una explicación pero también son compatibles con otras. Ese tipo de evidencia tiene utilidad limitada para distinguir entre alternativas.

ACH intenta invertir el orden habitual del razonamiento:

REGLA

alternativas → evidencia → comparación → refutación → conclusión

y no: hipótesis favorita → evidencia confirmatoria → conclusión

2.3 Cuándo utilizarlo y cuándo no

ACH es apropiado cuando...	ACH no es la herramienta cuando...
La cuestión es importante y una conclusión precipitada sería costosa	Solo hay una explicación posible: no hay nada que comparar
Hay varias explicaciones plausibles y no está claro cuál se sostiene mejor	La respuesta es un dato comprobable, no un juicio entre alternativas
La información es incompleta, ambigua o contradictoria	Buscas priorizar factores del entorno: eso es PESTEL
Existe riesgo de que ya tengas una hipótesis favorita	Buscas analizar actores y relaciones de fuerza: eso es MACTOR
Cabe la posibilidad de ocultación, manipulación o engaño	Necesitas una probabilidad calculada: ACH no la produce

2.4 Qué NO garantiza

Esto debe quedar explícito desde el principio. Heuer reconoce que ninguna aplicación de ACH garantiza llegar a la respuesta correcta, porque el análisis sigue dependiendo de información incompleta y del juicio humano.

- No garantiza una respuesta correcta.
- No elimina la incertidumbre ni crea información que no existe.
- No compensa una mala selección de hipótesis.
- No demuestra que una hipótesis sea verdadera.
- No convierte el juicio analítico en una medición objetiva.
- No elimina la necesidad de interpretación.

Lo que sí proporciona es **un proceso sistemático y un registro auditable del razonamiento**. Es menos de lo que promete cualquier puntuación automática, y es mucho más útil.

3. El principio de hipótesis competidoras

POR QUÉ LAS HIPÓTESIS TIENEN QUE COMPETIR DE VERDAD

Este capítulo es corto y es el más importante del manual. Si las hipótesis no son alternativas reales, todo lo que viene después —la matriz, los recuentos, los índices— deja de significar nada.

3.1 Qué es una hipótesis en ACH

Heuer utiliza «hipótesis» en sentido amplio: **una explicación o conclusión potencial que puede ser evaluada mediante evidencia.** No tiene que ser una hipótesis científica formal. Puede ser una explicación sobre el comportamiento de un actor, sobre el origen de un hecho, una interpretación de una situación o una conclusión alternativa sobre una misma cuestión.

Las hipótesis deben ser plausibles, suficientemente distintas, comparables respecto de la misma pregunta y formuladas de manera que la evidencia pueda evaluarse frente a ellas.

3.2 Qué significa «competidoras»

Competidoras significa **excluyentes**: si una es cierta, las demás no lo son. No basta con que sean distintas.

> **INCISO**
>
> Si dos hipótesis pueden ser ciertas a la vez, una evidencia a favor de una lo es también de la otra. La matriz deja entonces de comparar: los recuentos se mueven en paralelo y el índice pierde sentido.
>
> La competencia es **analítica**, no de las hipótesis entre sí: se enfrentan simultáneamente por la evidencia disponible.

El caso de Grupo Alventa ilustra el problema y su corrección. Una primera versión formulaba dos hipótesis así:

Formulación que NO compite	Por qué falla
H1: el atacante entró por la VPN y se movió lateralmente	Las dos pueden ser ciertas a la vez: el compromiso del proveedor podría haber sido el origen de las credenciales. Compararlas por inconsistencias no mide nada.
H3: el compromiso llegó por el acceso del proveedor	

La versión definitiva obliga a cada una a afirmar **un vector inicial distinto**, y a la segunda a negar el de la primera:

Hipótesis	Formulación que sí compite
H1 · Credenciales	Un atacante externo obtuvo credenciales válidas de un empleado y utilizó esas credenciales como vector inicial de acceso.
H3 · Proveedor	El acceso inicial se produjo mediante el acceso remoto del proveedor del ERP como vector de entrada, sin que las credenciales del empleado fueran el vector inicial.

> **REGLA**
>
> Prueba rápida: si puedes imaginar un escenario en el que dos de tus hipótesis son ciertas simultáneamente, no están compitiendo. Reformúlalas o fúndelas en una.

3.3 Lo que no está formulado no se evalúa

La matriz solo compara las hipótesis que has escrito. En el caso de Alventa queda una explicación verosímil fuera del análisis: que el compromiso del proveedor hubiera sido el **origen** de las credenciales. No es ninguna de las seis, y evaluarla exigiría formularla como séptima hipótesis y rehacer la matriz.

> **ADVERTENCIA**
>
> ACH no evalúa hipótesis que no hayan sido formuladas. Esa limitación no la corrige ningún cálculo: solo la corrige volver al paso 1 y añadir la alternativa que falta.

4. El recorrido y las tres capas

LOS OCHO PASOS DE HEUER, HOJA POR HOJA

La herramienta implementa el núcleo de los ocho pasos de Heuer. La pregunta analítica se escribe antes del paso 1 porque en la práctica es lo primero que hay que fijar.

4.1 Los ocho pasos y dónde están

Paso de Heuer	Hoja de la herramienta
1 · Identificar las hipótesis posibles	02 Hipótesis
2 · Reunir la evidencia y los argumentos significativos	03 Evidencia
3 · Construir la matriz	04 Matriz ACH
4 · Refinar la matriz	04 Matriz ACH y los controles de Comprobación
5 · Extraer conclusiones provisionales intentando refutar	Refutación
6 · Analizar la sensibilidad	Sensibilidad
7 · Informar de las conclusiones	Conclusión
8 · Identificar indicadores para observación futura	Indicadores

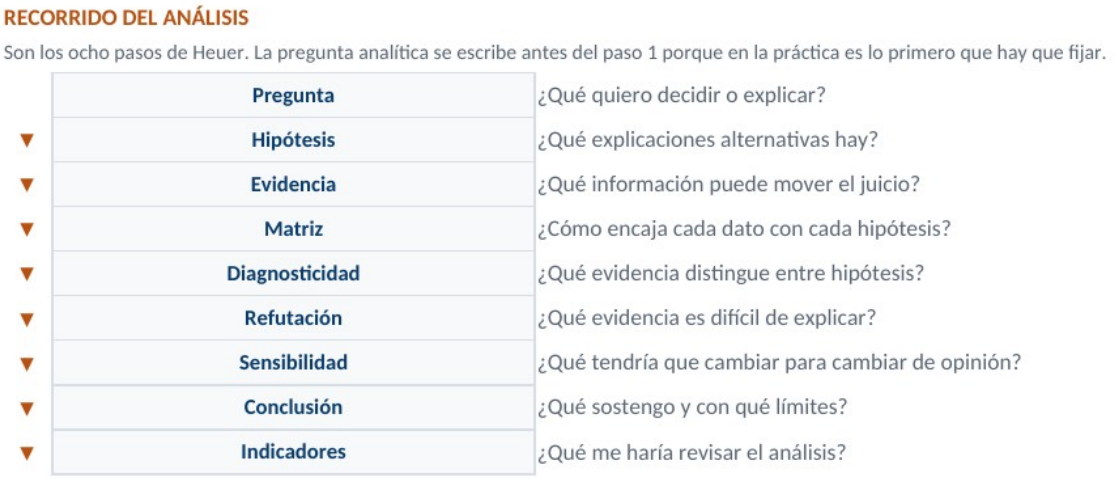


Figura 1. El recorrido, en la hoja 00 Inicio. Cada eslabón lleva la pregunta que responde esa fase.

4.2 Las tres capas

Cada hoja abre con una tarjeta que dice, en una línea por capa, qué ocurre **en esa hoja**. Es lo que permite saber en segundos qué parte del trabajo es tuya y qué parte es del libro.

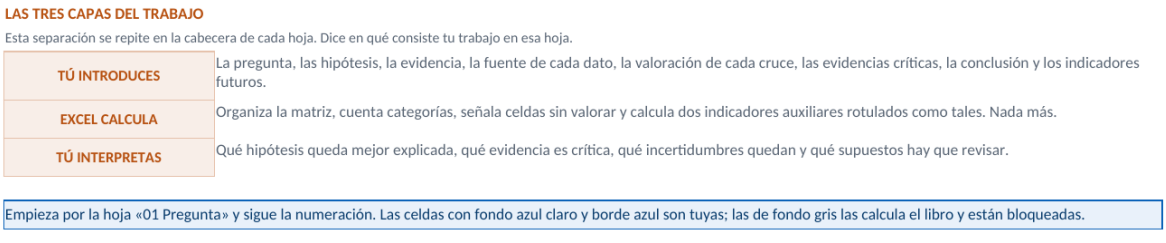


Figura 2. Las tres capas, explicadas en la hoja de inicio. La capa activa se marca con «▸» y en negrita, nunca solo con el color.

INCISO

No confundas cálculo con interpretación. Excel organiza, cuenta y ordena. Decidir qué hipótesis queda mejor explicada, qué evidencia es crítica y qué incertidumbres quedan es trabajo del analista, y la herramienta no lo hace por ti en ningún punto.

4.3 Capacidad de la herramienta

ACH IntelKIT admite hasta **8 hipótesis, 30 evidencias, 20 indicadores y 10 evidencias críticas**. Esta capacidad pertenece al diseño de IntelKIT; no constituye un límite metodológico de ACH. Heuer no fija un número correcto de hipótesis: depende de la complejidad del problema y del impacto de la conclusión, y advierte de que un número excesivo hace la comparación inmanejable.

5. Preparar la pregunta analítica

HOJA 01 · LO PRIMERO QUE HAY QUE FIJAR

Todo lo que sigue —hipótesis, evidencia, matriz— responde a esta pregunta. Si la pregunta cambia, el análisis se rehace.

TÚ INTRODUCES

La pregunta, por qué importa, el horizonte, el ámbito, los supuestos de partida, el analista y la fecha. Professional añade las perspectivas consultadas, las fuentes disponibles y las restricciones de información.

EXCEL CALCULA

Nada: esta hoja no calcula.

TÚ INTERPRETAS

Si la pregunta admite más de una respuesta razonable.

5.1 Cómo se formula

Una buena pregunta de ACH admite varias respuestas. La prueba rápida: **si no puedes escribir tres respuestas razonables y distintas, replantea la pregunta antes de seguir.**

No sirve	Sí sirve
¿Va a subir el precio?	¿Por qué está subiendo el precio?
Admite sí o no. No hay explicaciones que comparar.	Permite escribir varias explicaciones alternativas y confrontarlas con los mismos datos.

ADVERTENCIA

Evita formular la pregunta como «¿cuál es la causa más probable?». ACH no calcula probabilidades y no determina causas: compara el ajuste de explicaciones alternativas a la evidencia reunida. La pregunta del caso lo refleja: «¿qué hipótesis está mejor sustentada provisionalmente por la evidencia disponible?»

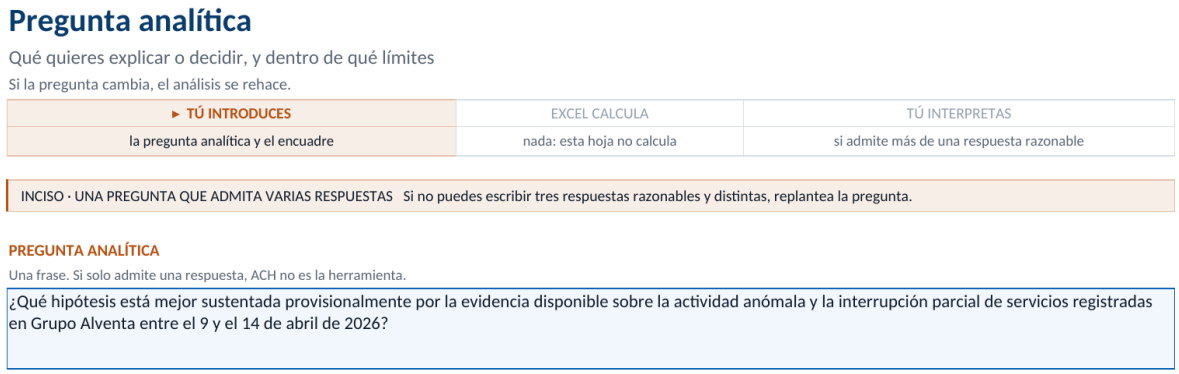


Figura 3. La hoja de pregunta analítica del caso. La tarjeta de capas dice que aquí no se calcula nada.

5.2 Los supuestos de partida

Hay un campo que suele rellenarse a la ligera y no debería: los supuestos. Son lo que estás dando por bueno sin haberlo comprobado, y pesan en el juicio precisamente porque no se ven.

EL CASO DE GRUPO ALVENTA

En Alventa se declaran dos: que los registros del concentrador VPN y del cortafuegos no han sido alterados —aunque sí consta borrado selectivo en los del servidor de aplicaciones— y que el inventario de software estaba al día antes del incidente. **Ninguno de los dos está verificado**, y los dos sostienen evidencia que después entra en la matriz.

BUENA PRÁCTICA

Los supuestos relevantes deben acabar siendo **filas de evidencia**. Si al rellenar la matriz notas que una valoración depende de algo que no has escrito, ese algo merece su propia fila.

6. Formular las hipótesis

HOJA 02 · PASO 1 DE HEUER

Escribe las explicaciones que merecen consideración, incluidas las que te resultan incómodas. Lo que no esté aquí no se evaluará.

TÚ INTRODUCES

Nombre corto, formulación completa, por qué es plausible, observaciones y estado de cada hipótesis.

EXCEL CALCULA

Activa la columna de la matriz en cuanto escribes el nombre corto.

TÚ INTERPRETAS

Si son alternativas reales o la misma explicación con otras palabras.

6.1 Los campos de la ficha

Campo	Qué se escribe
NOMBRE CORTO	Dos o tres palabras. Es lo que aparece en la matriz, en los gráficos y en los indicadores: cuanto más corto, mejor se lee la matriz.
FORMULACIÓN COMPLETA	Una frase afirmativa y comprobable. Debe responder a la misma pregunta que las demás y poder confrontarse con evidencia.
POR QUÉ ES PLAUSIBLE	Qué hace razonable esta explicación. Si no sabes responder, probablemente no sea una hipótesis sino una posibilidad remota.
OBSERVACIONES	Matices, discrepancias dentro del equipo, precisiones sobre el alcance.
ESTADO	Activa, en revisión, fusionada o descartada. Descartar no es borrar: deja constancia de que se consideró.

6.2 Las seis hipótesis del caso

REGISTRO — **TÚ INTRODUCES**

El NOMBRE CORTO activa la columna de la matriz.

ID	NOMBRE CORTO	FORMULACIÓN COMPLETA	POR QUÉ ES PLAUSIBLE	OBSERVACIONES	ESTADO
	¿Cómo la llamo?	*¿Qué afirma exactamente?*	*¿Por qué merece estar aquí?*	*¿Algo que deba recordar?*	*¿En qué situación está?*
H1	Credenciales	Un atacante externo obtuvo credenciales válidas de un empleado y utilizó esas credenciales como vector inicial de acceso a la organización.	Es la vía de entrada más frecuente en organizaciones de este tamaño y la campaña de concienciación de marzo registró un 23 % de clics.	Excluyente con H3: afirma que el vector inicial fueron las credenciales del empleado, no el canal del proveedor.	Activa
H2	Ransomware	Una campaña de ransomware oportunista entró por un servicio expuesto y la interrupción de servicios es el efecto del despliegue del cifrado.	La interrupción simultánea de varios servicios es el patrón típico, y el sector de distribución sanitaria es objetivo habitual.	Hipótesis de partida del primer parte interno, antes del inventario forense.	Activa
H3	Proveedor	El acceso inicial se produjo mediante el acceso remoto del proveedor del ERP como vector de entrada, sin que las credenciales del empleado fueran el vector inicial.	El proveedor tiene acceso permanente con cuenta de mantenimiento y hubo una sesión suya la noche en que empezó la interrupción.	Excluyente con H1: afirma un vector inicial distinto y niega el de aquella. El proveedor no ha aportado sus registros.	Activa
H4	Configuración	No hubo intrusión: un cambio mal planificado en la segunda fase de la migración del directorio activo provocó fallos de autenticación en cascada, y las alertas se interpretaron como un ataque.	La migración estaba en curso, afectaba a las políticas de autenticación y la interrupción coincide con la ventana de cambios.	Es la alternativa que explica el incidente sin atacante. Debe evaluarse con el mismo rigor que las demás.	Activa
	Interna	Una persona con acceso legítimo actuó	Hubo borrado selectivo de registros de	Hipótesis incómoda, incluida a	Activa

Figura 4. El registro de hipótesis del caso. Las seis afirman vectores iniciales distintos, y H3 niega expresamente el de H1.

H4 es deliberadamente la hipótesis **sin atacante**: sostiene que no hubo intrusión y que un cambio mal planificado provocó los fallos que se interpretaron como ataque. Un análisis que no la incluya está decidiendo por omisión que hubo intrusión antes de mirar la evidencia.

ERROR HABITUAL

Tres errores frecuentes al formular hipótesis:

Repetir la misma explicación con palabras distintas. **Formular una hipótesis tan amplia** que todo encaje en ella. **Escribir una predicción** («subirán los precios») en lugar de una explicación («los precios suben porque…»).

Si una hipótesis no puede quedar mal frente a ningún dato, no está compitiendo.

6.3 Generar las alternativas

Heuer recomienda utilizar distintas perspectivas para reducir el riesgo de omitir una explicación plausible. El beneficio no está en votar: está en **ampliar el conjunto de alternativas** y desafiar las relaciones entre evidencia e hipótesis.

EL CASO DE GRUPO ALVENTA

Las seis hipótesis de Alventa se generaron en una sesión con el responsable de sistemas, la responsable de cumplimiento, un técnico de redes y un analista externo que no conocía la organización. La hipótesis de error interno la aportó el analista externo; la de actuación interna deliberada, cumplimiento. Ninguna de las dos salió del equipo de sistemas.

7. Registrar la evidencia

HOJA 03 · PASO 2 DE HEUER

Anota cada elemento que esté haciendo que consideres una hipótesis más o menos plausible. No hace falta que sea un documento.

TÚ INTRODUCES

La etiqueta, la descripción, la fuente, la fecha, el tipo, tu interpretación, observaciones y estado.

EXCEL CALCULA

Activa la fila de la matriz en cuanto escribes la etiqueta.

TÚ INTERPRETAS

Qué información te falta todavía por reunir.

7.1 Evidencia en sentido amplio

Heuer habla de «evidencia y argumentos» en sentido amplio: documentos, observaciones, datos, indicios, razonamientos lógicos y también **los supuestos** que estás dando por buenos. La razón es práctica: un supuesto no declarado puede estar sosteniendo tu conclusión sin que nadie lo revise.

7.2 Tres cosas distintas en tres columnas

INCISO

La **EVIDENCIA** es el dato que vas a enfrentar a las hipótesis. La **FUENTE** es de dónde procede. La **INTERPRETACIÓN** es lo que tú deduces de él.

Se registran en columnas separadas a propósito: una fuente muy fiable no convierte una interpretación en un hecho, y un dato cierto puede admitir varias lecturas. Si en la descripción escribes «esto demuestra que…», lo que has anotado es una conclusión, no una evidencia.

REGISTRO — TÚ INTRODUCES

La ETIQUETA activa la fila de la matriz.

ID	ETIQUETA	DESCRIPCIÓN	FUENTE	FECHA	TIPO	INTERPRETACIÓN	OBSERVACIONES	ESTADO
	¿Cómo la llamo?	*¿Qué dice el dato?*	*¿De dónde procede?*	*¿De cuándo es?*	*¿Qué clase de elemento es?*	*¿Qué significa para mí?*	*¿Algo que deba recordar?*	*¿En qué situación está?*
E1	Fallos VPN 4.200	Entre el 9 y el 11 de abril se registran 4.200 intentos fallidos de autenticación contra el portal VPN desde 37 direcciones IP distintas.	Registros del concentrador VPN	09-11/04/2026	Hecho	Patrón compatible con un tanteo masivo de credenciales previo al acceso.	El pico cesa el 11 por la tarde, el día antes de la primera sesión exitosa anómala.	Activa
E2	Sesión 03:14	Sesión VPN exitosa con la cuenta de un técnico de almacén el 12 de abril a las 03:14, desde una dirección IP de un proveedor de alojamiento situado fuera de España.	Registros del concentrador VPN	12/04/2026	Hecho	El técnico declara no haber trabajado esa noche. La cuenta no tenía segundo factor habilitado.	Es la evidencia individual más citada en las tres hipótesis de intrusión externa.	Activa
E3	Sin nota de rescate	No se ha localizado ninguna nota de rescate ni comunicación de extorsión en los sistemas afectados ni en los buzones de dirección.	Revisión del equipo de respuesta	15/04/2026	Observación	Ausencia de evidencia: su peso depende de si cabría esperar la nota a estas alturas.	Se ha comprobado también el correo en cuarentena y los canales de atención al cliente.	Activa
E4	Borrado de auditoría	Se han eliminado selectivamente los registros de auditoría del servidor de aplicaciones correspondientes al 11 y al 12 de abril; los del resto del periodo están intactos.	Análisis forense	16/04/2026	Hecho	El borrado es selectivo y preciso, no un fallo de rotación de registros.	Impide reconstruir el movimiento lateral. Es la laguna más seria del análisis.	Activa

Figura 5. El registro de evidencia del caso. Descripción, fuente e interpretación ocupan columnas distintas.

7.3 La ausencia de evidencia

Antes de interpretar que «no hay nada» juega en contra de una hipótesis, hazte cuatro preguntas: ¿podríamos realmente observar ese dato? ¿Podría estar oculto? ¿Podría no estar disponible todavía? ¿Podría haber interés en manipularlo?

> **ADVERTENCIA**
>
> La ausencia de evidencia no equivale a evidencia de ausencia. Si la respuesta a alguna de esas cuatro preguntas es sí, la ausencia dice poco. Si es no en todas, entonces sí es un dato y merece entrar en la matriz como evidencia con su propia fila.

> **EL CASO DE GRUPO ALVENTA**
>
> En Alventa, «Sin indicios internos» —ni incidencias laborales ni accesos presenciales anómalos— se registra como inconsistente con la hipótesis de actuación interna, pero es ausencia de evidencia: una actuación remota no dejaría rastro ni en recursos humanos ni en el control de accesos físicos. El analista lo anota expresamente en el examen de refutación.

8. La matriz: valorar cada cruce

HOJA 04 · PASOS 3 Y 4 DE HEUER

Las hipótesis se colocan en las columnas y la evidencia en las filas. Cada intersección registra la relación entre una evidencia concreta y una hipótesis concreta.

> **TÚ INTRODUCES**
>
> La valoración de cada cruce, con la escala CC / C / N / I / II.

> **EXCEL CALCULA**
>
> Recuentos por fila y por columna, y lo que falta por valorar.

> **TÚ INTERPRETAS**
>
> Qué filas no separan nada y qué columnas acumulan inconsistencias.

8.1 La pregunta de cada celda

La pregunta es siempre la misma, y no es la que uno tiende a hacerse: **«Si esta hipótesis fuera cierta, ¿cómo encajaría este dato?»** No es «¿me gusta este dato?» ni «¿apoya mi conclusión?».

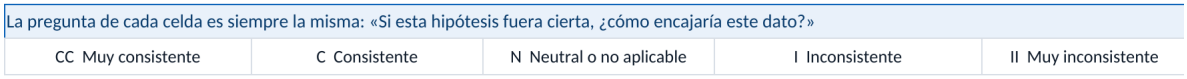


Figura 6. La pregunta de la celda y la tira con los cinco símbolos, encima de la matriz.

> **BUENA PRÁCTICA**
>
> Recorre la matriz **por filas**: toma un dato y mira cómo encaja con todas las hipótesis antes de pasar al siguiente. Si la recorres por columnas vuelves a evaluar una hipótesis cada vez, que es justo lo que ACH trata de evitar.

8.2 La escala

Heuer admite varias notaciones —letras C/I/N, signos más y menos, incluso probabilidades— y advierte de que **la notación no es el método**: es una abreviatura de un razonamiento más largo.

> **NOTA METODOLÓGICA**
>
> La escala de cinco categorías de IntelKIT es una **decisión de implementación**, no «la escala oficial de ACH». C, I y N proceden de Heuer; la graduación doble (CC, II) sigue la convención documentada en la implementación de referencia en software. Se eligió graduada porque distinguir «inconsistente» de «muy inconsistente» es el juicio que más influye en el paso 5.

	Significado	Cuándo marcarlo
CC	Muy consistente	Si la hipótesis fuera cierta, esperaría justo este dato.
C	Consistente	Encaja sin dificultad.
N	Neutral o no aplicable	No mueve el juicio sobre esta hipótesis, o no viene al caso.
I	Inconsistente	Difícil de explicar si la hipótesis fuera cierta.
II	Muy inconsistente	La contradice de forma difícil de salvar.

> **INCISO**
>
> **Una celda en blanco significa «sin valorar», no «neutral».** Para «no aplica» se usa N. La distinción es lo que permite medir si la matriz está completa.

8.3 Qué NO significa cada símbolo

INCISO

«Consistente» no significa «verdadero». Marcar C quiere decir que el dato encaja con la hipótesis, nada más. Encajar es fácil: una explicación suficientemente flexible encaja con casi todo, y eso es un defecto, no una virtud.

«Inconsistente» no significa «falso». Puede ocurrir que el dato esté mal, que la fuente se equivoque, que falte contexto o que exista una explicación razonable que todavía no has visto. Antes de dar una hipótesis por debilitada, mira la calidad del dato que la contradice.

8.4 La matriz del caso

EVIDENCIA	Credenciales	Ransomware	Proveedor	Configuración	Interna	Vulnerabilidad
Fallos VPN 4.200	CC	C	I	II	I	N
Sesión 03:14	CC	C	II	II	I	I
Sin nota de rescate	C	II	C	CC	C	C
Borrado de auditoría	C	I	C	II	CC	C
Sin cifrado	C	II	C	CC	C	C
Ventana de cambios	N	N	CC	CC	C	N
Sesión del proveedor	N	N	CC	C	N	N
Proveedor niega cambios	N	N	I	N	N	N
Migración AD en curso	C	C	C	CC	C	C
Perímetro parcheado	C	I	C	C	C	II
Herramienta remota	CC	C	I	II	C	C

Figura 7. La matriz del caso: 15 evidencias × 6 hipótesis, 90 cruces valorados. El color solo refuerza: el símbolo de la celda ya dice el valor.

Dos filas merecen mirarse de cerca antes de seguir.

Fila	Por qué importa
Sesión 03:14	CC para Credenciales y II para Proveedor. Es la contradicción directa entre las dos: esa sesión del día 12 es el primer acceso externo satisfactorio registrado, y la única sesión del proveedor es del día 13. Su capacidad discriminante, 0,87, es la segunda más alta del caso.
Cuenta de servicio	C en las seis. Es verdadera, es importante para la seguridad de la organización y **no sirve para elegir entre hipótesis**. Su capacidad discriminante es 0.

Celdas valoradas	15	15	15	15	15	15		
Sin valorar	0	0	0	0	0	0		
Inconsistencias (I + II)	0	4	4	5	3	2		

Figura 8. Los totales por columna, debajo de la matriz. Credenciales no acumula ninguna inconsistencia; Configuración acumula cinco muy inconsistentes.

8.5 Refinar la matriz

ACH es iterativo. Con la matriz delante se ven cosas que antes no: dos hipótesis que en realidad son la misma, una hipótesis tan amplia que conviene partirla, filas enteras de C que no separan nada y el hueco de la evidencia que falta. **Volver atrás y reescribir hipótesis o evidencia no es empezar de cero: es el paso 4.**

INCISO · UNA EVIDENCIA NO «DEMUESTRA» UNA HIPÓTESIS Si encaja con todas, puede ser cierta y no servir para elegir entre ellas.

INCISO · «CONSISTENTE» NO SIGNIFICA «VERDADERO» Encajar es fácil: una explicación flexible encaja con casi todo, y eso es un defecto.

INCISO · «INCONSISTENTE» NO SIGNIFICA «FALSO» Antes de dar una hipótesis por debilitada, mira la calidad del dato que la contradice.

INCISO · LA PRIMERA MATRIZ NO ES LA DEFINITIVA Volver y reescribir hipótesis o evidencia es el paso 4, no empezar de cero.

La escala es una decisión de implementación de IntelKIT, no «la escala oficial de ACH». La explicación completa del método, la escala, los cálculos auxiliares y sus límites está en la hoja Método.

Figura 9. Los incisos que la herramienta coloca junto a la matriz, donde surge cada confusión.

9. Diagnosticidad

QUÉ EVIDENCIA DISTINGUE Y QUÉ EVIDENCIA NO

Es uno de los conceptos más importantes de ACH y el que lo distingue de una lista de argumentos a favor de la explicación que ya preferías.

TÚ INTRODUCES

Nada: ya está todo en la matriz.

EXCEL CALCULA

Recuentos por evidencia y capacidad discriminante.

TÚ INTERPRETAS

Qué evidencia distingue entre hipótesis y cuál no.

9.1 Qué significa «diagnóstico»

No tiene nada que ver con el diagnóstico clínico. Significa **capacidad de una evidencia para diferenciar entre hipótesis competidoras**. Una evidencia es diagnóstica cuando no se comporta igual frente a todas: encaja con unas y choca con otras.

INCISO

Una misma evidencia puede ser consistente con varias hipótesis a la vez. Si E1 es consistente con H1, H2 y H3, E1 puede ser cierta y relevante **y no servir para elegir entre las tres**.

Lo que ACH pregunta no es «¿cuántos datos apoyan H1?», sino «¿qué dato permite distinguir H1 de H2 y de H3?». Por eso una fila entera de C no aporta nada a la comparación, aunque todo en ella sea verdad.

9.2 El recuento por evidencia

RECUENTO POR EVIDENCIA — *EXCEL CALCULA*

EVIDENCIA	CC	C	N	I	II	VALORADAS	CD	ORDEN
Fallos VPN 4.200	1	1	1	2	1	6	0.93	1
Sesión 03:14	1	1	0	2	2	6	0.87	2
Sin nota de rescate	1	4	0	0	1	6	0.60	7
Borrado de auditoría	1	3	0	1	1	6	0.80	3
Sin cifrado	1	4	0	0	1	6	0.60	7
Ventana de cambios	2	1	3	0	0	6	0.73	5
Sesión del proveedor	1	1	4	0	0	6	0.60	7
Proveedor niega cambios	0	0	5	1	0	6	0.33	12
Migración AD en curso	1	5	0	0	0	6	0.33	12
Perímetro parcheado	0	4	0	1	1	6	0.60	7
Herramienta remota	1	3	0	1	1	6	0.80	3
240 GB salientes	2	3	0	0	1	6	0.73	5
Cuenta de servicio	0	6	0	0	0	6	0.00	15
Phishing 23 %	0	2	4	0	0	6	0.53	11
Sin indicios internos	0	5	0	1	0	6	0.33	12

Figura 10. El recuento por evidencia del caso, con la capacidad discriminante y su orden.

9.3 La capacidad discriminante

El concepto de valor diagnóstico es de Heuer. **La fórmula concreta es una decisión de IntelKIT**, y la herramienta la rotula como tal cada vez que la muestra.

$CD(e) = (n^2 - \Sigma c^2) / (n^2 - n)$, siendo *n* el número de celdas valoradas de la fila y *c* cuántas de ellas han recibido cada categoría. El resultado es exactamente **la proporción de pares de hipótesis a los que esa evidencia asigna categorías distintas**, de modo que puede comprobarse a mano sobre la propia matriz contando pares.

Fila del caso	Reparto	CD	Lectura
Fallos VPN 4.200	1·CC 1·C 1·N 2·I 1·II	0,93	Separa casi todos los pares
Sesión 03:14	1·CC 1·C 2·I 2·II	0,87	Separa mucho
Ventana de cambios	2·CC 1·C 3·N	0,73	Separa dos bloques
Migración AD en curso	1·CC 5·C	0,33	Casi no separa
Cuenta de servicio	6·C	0,00	No separa nada

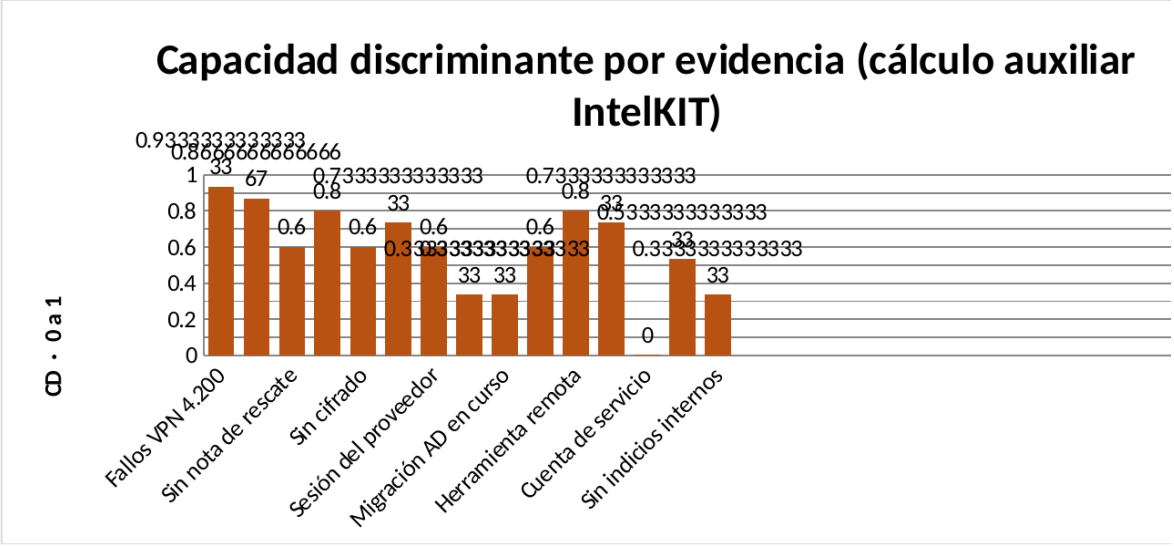
CÁLCULO AUXILIAR INTELKIT · CAPACIDAD DISCRIMINANTE Proporción de pares de hipótesis a los que la fila da categorías distintas. Mide separación. No mide importancia, fiabilidad ni verdad.

Figura 11. La ficha del cálculo auxiliar, tal como aparece bajo la matriz: qué es y qué no es, en una línea.

ADVERTENCIA

La diagnosticidad **no mide la calidad de una fuente**, ni la importancia, ni la fiabilidad, ni la verdad. Mide separación. Una evidencia con CD alta puede ser falsa; una con CD = 0 puede ser cierta y muy relevante para entender la situación.

CAPACIDAD DISCRIMINANTE DE CADA EVIDENCIA



La explicación completa del método, la escala, los cálculos auxiliares y sus límites está en la hoja Método.

Figura 12. La capacidad discriminante de cada evidencia del caso. El rango va de 0,00 a 0,93.

9.4 Lo que enseña el caso

Las dos evidencias que más pesan en la conclusión de Alventa **no son las de mayor CD**. «Sin nota de rescate» y «Perímetro parcheado» tienen CD 0,60 y son las que prácticamente cierran dos hipótesis, porque lo que importa no es solo cuánto separa una evidencia, sino **a quién** señala.

10. Intentar refutar

PASO 5 · EL GIRO DEL MÉTODO

Aquí cambia la pregunta. Hasta ahora has valorado cómo encaja cada dato; ahora se trata de buscar, hipótesis por hipótesis, qué dato NO encaja y si eso la debilita de verdad.

TÚ INTRODUCES

El examen de cada hipótesis y su situación.

EXCEL CALCULA

Nada: los recuentos están en la hoja anterior.

TÚ INTERPRETAS

Si la inconsistencia la debilita de verdad.

10.1 El principio de refutación

ACH pone deliberadamente el foco en buscar elementos que **desmientan** una hipótesis, no en acumular elementos que parezcan confirmarla. Heuer lo resume así: **la hipótesis más probable suele ser la que tiene menos evidencia en contra, no necesariamente la que tiene más evidencia a favor.**

ADVERTENCIA

Esa frase hay que leerla entera. «Menos evidencia en contra» **no** significa certeza, demostración, verdad absoluta ni probabilidad estadística calculada.

Es una comparación entre las alternativas que tú has escrito, con la evidencia que tú has reunido. Cambia la evidencia y cambia la comparación.

BUENA PRÁCTICA

El analista debe intentar refutar **su propia hipótesis preferida**, y es la que menos tiende a examinar. Empieza por ella.

10.2 El examen, hipótesis por hipótesis

La herramienta pide cuatro cosas de cada hipótesis. No se trata de resumir el recuento: se trata de intentar tumbar cada explicación.

Campo	Qué responde
¿Qué evidencia es difícil de explicar si fuera cierta?	La pregunta del paso 5. Cita evidencias concretas.
¿Cómo podría explicarse esa inconsistencia?	¿Hay otra lectura, un error de fuente, un dato que falta?
¿Qué dato buscarías para refutarla?	Qué tendrías que encontrar para descartarla.
Situación	Sigue en pie · Debilitada · No demostrada · Descartada. Es tu juicio, no un cálculo.

el examen de cada hipótesis y su situación	nada: los recuentos están en la hoja anterior	si la inconsistencia la debilita de verdad

INCISO · BUSCA QUÉ PODRÍA REFUTAR TU HIPÓTESIS La más probable suele ser la que tiene menos evidencia EN CONTRA, no más a favor.

EXAMEN DE CADA HIPÓTESIS — **TÚ INTRODUCES**

Una fila por hipótesis. Intenta tumbar cada una, incluida la que te parece más sólida.

HIPÓTESIS	¿QUÉ EVIDENCIA ES DIFÍCIL DE EXPLICAR SI FUERA CIERTA?	¿CÓMO PODRÍA EXPLICARSE ESA INCONSISTENCIA?	¿QUÉ DATO BUSCARÍAS PARA REFUTARLA?	SITUACIÓN
	Cita evidencias concretas.	*¿Otra lectura, un error de fuente, un dato que falta?*	*Qué tendrías que encontrar para descartarla.*	*¿Sigue en pie?*
	Ninguna evidencia registrada la contradice: su índice es 0. La única que incomoda es E6, la coincidencia de la interrupción con la ventana de mantenimiento, que se ha valorado N y no I. Conviene	Un índice 0 puede significar que la hipótesis es sólida o que todavía no se ha buscado evidencia capaz de contradecirla. Aquí es lo segundo en parte: faltan la imagen forense del equipo del	Imagen forense del equipo del técnico de almacén y registros del proveedor de identidad. Si no hay rastro de phishing ni de uso de la credencial antes del 12, la vía se debilita mucho.	

Figura 13. El examen de refutación del caso. Cuatro campos por hipótesis, todos de entrada.

Proveedor	La cronología. E2 sitúa el primer acceso externo satisfactorio el día 12, con credenciales de un empleado, y E11 fecha ese mismo día la instalación de la herramienta remota; la única sesión registrada del proveedor es del 13 (E7). E1 añade un tanteo masivo de la VPN que no haría falta si el acceso venía por el canal de mantenimiento, y E8 es la negativa del proveedor.	Podría haber habido accesos del proveedor anteriores al 13 que no quedaran registrados: el bastión guarda metadatos, y el proveedor no ha aportado sus propios registros. E8, además, es una declaración de parte sin respaldo, de modo que de las cuatro inconsistencias una es floja y tres proceden de la misma observación cronológica.	Los registros propios del proveedor, y no solo de la sesión del 13: cualquier acceso suyo anterior al 12 convertiría la cronología de inconsistencia en apoyo. Llevan tres días solicitados.	Sigue en pie
Configuración	Cinco evidencias muy inconsistentes: E1, E2, E4, E11 y E12. Un error de configuración no produce 4.200 intentos desde 37 IP, ni una sesión desde hosting extranjero, ni borrado selectivo de auditoría, ni software de administración remota, ni 240 GB salientes.	E9 y E6 sostienen que la migración pudo causar la interrupción del ERP, y eso sigue siendo posible. Lo que no explica es la actividad externa: como explicación del conjunto queda descartada; como explicación parcial de la caída del servicio, sigue viva.	Que la reversión del cambio de directorio activo restableciera el servicio por sí sola confirmaría la parte de la interrupción. No rehabilitaría la hipótesis como causa del incidente completo.	Debilitada

Figura 14. El examen del proveedor. Tres de sus cuatro inconsistencias proceden de una sola observación cronológica.

10.3 No demostrada no es refutada

INCISO

NO DEMOSTRADA significa que falta apoyo. **REFUTADA o DEBILITADA** significa que hay evidencia que choca con la hipótesis. No son lo mismo y la herramienta las distingue en el campo de situación.

«No hemos encontrado evidencia de H1» no permite concluir «H1 es falsa». La pregunta adicional es: si H1 fuera verdadera, ¿esperaríamos realmente encontrar esa evidencia?

EL CASO DE GRUPO ALVENTA

En Alventa, **Vulnerabilidad** queda registrada como *no demostrada*, no como refutada: el escaneo externo del 16 de abril no encuentra vulnerabilidades sin parchear, pero mira el presente, no la ventana del incidente. **Ransomware**, en cambio, queda *debilitada* por evidencia en contra: catorce días después no hay nota de rescate ni cifrado.

11. Los cálculos auxiliares de IntelKIT

QUÉ CALCULA EL LIBRO Y QUÉ NO SIGNIFICA

Este capítulo trata los únicos tres números que la herramienta produce por su cuenta. Ninguno es parte del método: los tres son decisiones de implementación de IntelKIT, y así están rotulados dentro del propio libro.

11.1 Por qué no hay una «fórmula oficial de ACH»

NOTA METODOLÓGICA

Heuer no establece ninguna escala numérica ni ninguna puntuación obligatorias. Presenta una notación cualitativa y señala que pueden emplearse otras convenciones. Permite una clasificación provisional atendiendo a las inconsistencias, pero advierte de que contar signos es solo una aproximación y de que no todas las inconsistencias pesan igual.

La literatura posterior tampoco converge en una fórmula única: la implementación de referencia en software documenta **dos algoritmos experimentales distintos** y los presenta como aportación propia del software, no de Heuer.

Por eso ACH IntelKIT no presenta ningún número como «la puntuación oficial de ACH».

11.2 Índice de inconsistencia por hipótesis

IIH(h) = Σ peso(e,h), con peso = máx(0, −valor): **2** en las celdas II, **1** en las I y **0** en todas las demás. Es la suma de la columna de pesos.

La graduación I = 1 / II = 2 sigue la convención documentada en el algoritmo de recuento de inconsistencias de la implementación de referencia. **IntelKIT no aplica los multiplicadores de peso por calidad de la evidencia** de esa implementación, porque no son trazables a Heuer y multiplicarían una decisión de implementación por otra.

ADVERTENCIA

Un índice bajo significa «se ha registrado poca evidencia en contra». Eso puede deberse a que la hipótesis sea sólida **o a que todavía no hayas buscado evidencia que la contradiga**. No es una probabilidad y no mide verdad.

RECUENTO POR HIPÓTESIS — *EXCEL CALCULA*

HIPÓTESIS	CC	C	N	I	II	VALORADAS	SIN VALORAR	ÍNDICE	I + II	ORDEN
Credenciales	4	8	3	0	0	15	0	**0**	0	1
Ransomware	0	8	3	2	2	15	0	**6**	4	5
Proveedor	2	8	1	3	1	15	0	**5**	4	4
Configuración	4	4	2	0	5	15	0	**10**	5	6
Interna	2	7	3	3	0	15	0	**3**	3	2
Vulnerabilidad	0	8	5	1	1	15	0	**3**	2	2

Figura 15. El recuento por hipótesis del caso, con el índice y el orden auxiliar.

11.3 El orden auxiliar

Es la posición del índice de menor a mayor. **Las hipótesis empatadas comparten posición**, y la herramienta cuenta cuántas lo están.

INCISO

La primera posición del orden **no es «la hipótesis ganadora»**. Es la que acumula menos inconsistencia registrada. La conclusión la escribes tú, y puedes perfectamente concluir algo distinto de lo que sugiere el orden, explicando por qué.

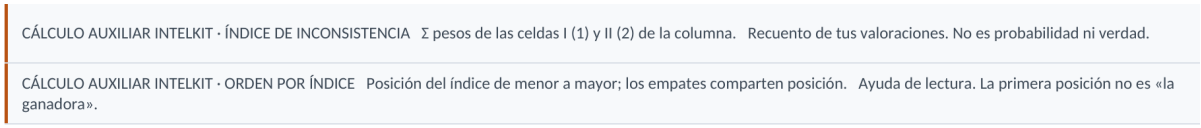


Figura 16. Las fichas de los dos cálculos auxiliares, tal como las muestra la herramienta junto a los números.

11.4 La trazabilidad del cálculo

Professional muestra las tres matrices internas con las que trabaja el libro, celda a celda, de modo que cualquier recuento puede comprobarse a mano.

Matriz interna	Qué contiene
Valor de la categoría	CC = 2 · C = 1 · N = 0 · I = −1 · II = −2. Son códigos de categorías, no magnitudes: la diferencia entre C y CC no son «dos unidades de algo». En blanco = sin valorar.
Peso de inconsistencia	peso = máx(0, −valor). La suma de cada columna es el índice de inconsistencia de esa hipótesis.
Celda valorada	1 si la celda tiene categoría reconocida y existen la evidencia y la hipótesis. Es la *n* de la capacidad discriminante.

EVIDENCIA	Credenciales	Ransomware	Proveedor	Configuración	Interna	Vulnerabilidad
Fallos VPN 4.200	2	1	-1	-2	-1	0
Sesión 03:14	2	1	-2	-2	-1	-1
Sin nota de rescate	1	-2	1	2	1	1
Borrado de auditoría	1	-1	1	-2	2	1
Sin cifrado	1	-2	1	2	1	1
Ventana de cambios	0	0	2	2	1	0
Sesión del proveedor	0	0	2	1	0	0
Proveedor niega cambios	0	0	-1	0	0	0
Migración AD en curso	1	1	1	2	1	1
Perímetro parcheado	1	-1	1	1	1	-2
Herramienta remota	2	1	-1	-2	1	1

Figura 17. La matriz de valores de la hoja de trazabilidad: la traducción de la matriz del analista a códigos numéricos.

11.5 El inciso que más importa

INCISO

Los cálculos auxiliares de IntelKIT no son una medida de verdad. Ordenan lo que tú has escrito: cambia una valoración y cambia el índice.

ACH no convierte automáticamente las valoraciones en probabilidades. Aquí no hay probabilidades a priori, ni verosimilitudes, ni actualización bayesiana. Llamar «probabilidad» a un orden por inconsistencia sería crear una precisión que no existe.

ACH no es una votación. La pregunta no es cuántas evidencias apoyan una hipótesis, sino qué evidencia permite discriminar entre ellas.

12. Sensibilidad

PASO 6 · DE QUÉ CUELGA TU CONCLUSIÓN

Una conclusión puede parecer muy sólida y depender en realidad de uno o dos datos. Este paso busca exactamente eso: identificar de qué cuelga el juicio.

TÚ INTRODUCES

Las evidencias críticas y qué pasaría si fallaran.

EXCEL CALCULA

Si la etiqueta existe en el registro de evidencia.

TÚ INTERPRETAS

De qué cuelga realmente tu conclusión.

12.1 La pregunta

«¿Qué tendría que cambiar para que mi conclusión cambiara?» Si al retirar una sola evidencia el orden se da la vuelta, esa evidencia es crítica, y verificarla es más urgente que añadir diez datos nuevos.

Campo	Qué responde
Evidencia crítica	La etiqueta, tal como está en el registro. La herramienta avisa si no la encuentra.
Por qué importa	Qué parte de tu razonamiento depende de este dato.
Si fuera incorrecta	Qué hipótesis cambiaría de posición y en qué sentido.
Qué habría que verificar	La comprobación concreta que resolvería la duda.
Prioridad	Alta, media o baja. Es tu criterio, no un cálculo.

ID	EVIDENCIA CRÍTICA	POR QUÉ IMPORTA	SI FUERA INCORRECTA	QUÉ HABRÍA QUE VERIFICAR	PRIORIDAD
	¿Qué dato es decisivo?	*¿Qué sostiene?*	*¿Qué se vendría abajo?*	*¿Cómo lo comprobaría?*	*¿Cuánto corre?*
S1	Sesión 03:14	Es el único acceso externo satisfactorio documentado y el primero de la cronología. Sostiene por sí sola la hipótesis de credenciales y es la contradicción principal de la del proveedor, que niega ese vector inicial.	Si la sesión resultara ser de un mantenimiento no documentado o de un proveedor de soporte, Credenciales perdería su único apoyo fuerte y Proveedor dejaría de tener su inconsistencia más grave: el orden auxiliar se daría la vuelta entre las dos.	Contrastar la IP de origen con los rangos de los proveedores de soporte contratados y entrevistar al técnico de almacén con el registro delante.	Alta
S2	Proveedor niega cambios	Es la única evidencia inconsistente específica de la hipótesis del proveedor, y su calidad es baja: declaración de parte sin registros.	Si el proveedor aporta registros que demuestren que sí aplicó cambios —o que accedió antes del 12—, esta evidencia se invierte y la cronología deja de jugar en contra: el índice de Proveedor caería de 5 a 1 y pasaría a disputar el primer lugar.	Reclamar formalmente los registros de la sesión del 13 de abril, con plazo. Si no los aporta, dejar constancia de que la hipótesis no se puede cerrar.	Alta

Figura 18. El análisis de sensibilidad del caso: seis evidencias críticas, cuatro de prioridad alta.

12.2 Lo que revela en el caso

El análisis de sensibilidad de Alventa muestra hasta qué punto el resultado es frágil, y lo muestra en dos direcciones distintas.

Evidencia crítica	Qué pasaría si fallara
Sesión 03:14	Credenciales pierde su único apoyo fuerte y Proveedor su inconsistencia más grave: el orden se daría la vuelta entre las dos.
Proveedor niega cambios	Si el proveedor aporta registros —o prueba que accedió antes del 12—, su índice caería de 5 a 1.
Perímetro parcheado	**Dos hipótesis dependen de un único escaneo.** Vulnerabilidad recuperaría posición y Ransomware volvería a tener vía de entrada.
Borrado de auditoría	Define lo que no se puede saber: es la razón por la que el índice de Credenciales es 0.

13. La conclusión provisional

PASO 7 · LA CONCLUSIÓN COMPARATIVA

El libro no escribe esta hoja. No declara hipótesis ganadora, no produce probabilidades y no redacta conclusión: ordena lo que has introducido y te deja el juicio.

TÚ INTRODUCES

La conclusión comparativa, en siete campos.

EXCEL CALCULA

Nada: el libro no redacta la conclusión.

TÚ INTERPRETAS

Por qué una alternativa queda por delante de las demás.

13.1 Qué debe contener

Heuer es explícito en el paso 7: no informar únicamente de la hipótesis considerada más favorecida, sino también de las alternativas descartadas o debilitadas, de las que permanecen plausibles, de las incertidumbres relevantes y de las evidencias críticas. **El lector debe poder entender por qué una alternativa quedó por delante de las demás.**

Campo	Qué se escribe
Hipótesis más favorecida por la evidencia	Puede no coincidir con la primera posición del orden auxiliar. Si no coincide, se explica en el razonamiento.
Hipótesis que permanecen plausibles	Qué alternativas siguen en pie y por qué no se descartan.
Hipótesis debilitadas o descartadas	Distinguiendo debilitada por evidencia en contra de no demostrada por falta de apoyo.
Evidencias críticas	Deben coincidir con lo registrado en sensibilidad.
Principales incertidumbres	Qué no se sabe, incluidos los supuestos dados por buenos.
Razonamiento del analista	El lector tiene que poder seguirlo sin volver a la matriz.
Limitaciones del análisis	Evidencia que no se pudo obtener, hipótesis que no se pudieron evaluar, sesgos reconocidos.

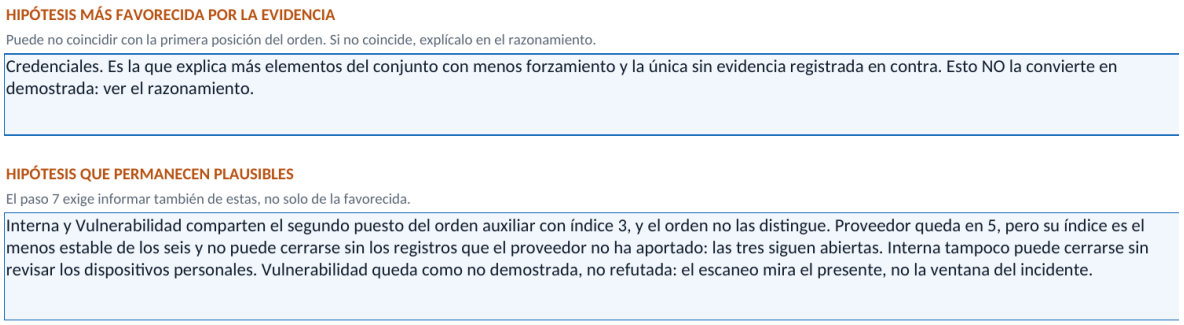


Figura 19. Los dos primeros campos de la conclusión del caso. El libro los deja vacíos: los escribe el analista.

13.2 Provisional quiere decir provisional

> **ADVERTENCIA**
>
> El resultado de ACH es provisional y depende de la evidencia disponible. No se escribe «la hipótesis ganadora» ni «la causa más probable»: se escribe cuál queda mejor sustentada **provisionalmente**, qué alternativas siguen abiertas y qué haría falta para cerrarlas.

14. Indicadores y revisión futura

PASO 8 · CUÁNDO VOLVER A ABRIR EL ANÁLISIS

El último paso de Heuer determina qué hechos futuros indicarían que la situación evoluciona de otra manera, para poder revisar el juicio cuando aparezca nueva información.

TÚ INTRODUCES

Los hitos que te harían revisar el análisis.

EXCEL CALCULA

Si la hipótesis relacionada existe en el registro.

TÚ INTERPRETAS

Qué indicador discrimina de verdad.

14.1 Qué es un buen indicador

INCISO

Un indicador no es una noticia futura cualquiera. Tiene que estar atado a una hipótesis concreta y tener capacidad para mover la valoración: si ocurriera, cambiaría algo en la matriz. **Un indicador compatible con todas tus hipótesis no te avisará de nada.**

Cada indicador registra qué hecho se observaría, a qué hipótesis afecta, qué esperaría observar, en qué horizonte, dónde se vería y —lo más importante— **la condición concreta que obligaría a rehacer el análisis**.

ID	INDICADOR	HIPÓTESIS RELACIONADA	QUÉ ESPERARÍA OBSERVAR	HORIZONTE	FUENTE POTENCIAL	CONDICIÓN DE REVISIÓN
	¿Qué hecho observaría?	*¿A cuál afecta?*	*¿En qué dirección?*	*¿Para cuándo?*	*¿Dónde lo vería?*	*¿Qué me haría rehacer el análisis?*
I1	El proveedor del ERP aporta los registros de su sesión del 13 de abril	Proveedor	Si muestran cambios aplicados o actividad no justificada, la hipótesis del proveedor se refuerza y E8 se invierte.	< 3 meses	Comunicación formal con el proveedor	Cualquier registro que contradiga la declaración escrita del 17 de abril obliga a revalorar E8 y a reabrir el paso 4.
I2	Aparece una nota de extorsión o una publicación de datos en un sitio de filtraciones	Ransomware	Si aparece, E3 deja de ser inconsistente y la hipótesis vuelve al primer plano.	3-6 meses	Vigilancia de sitios de filtración y buzones de dirección	La aparición de datos identificables de la organización obliga a rehacer la valoración de E3 y E5 y a notificar.
I3	El análisis forense del equipo del técnico encuentra rastro de phishing o de robo de credenciales	Credenciales	Convertiría el índice 0 de Credenciales en un resultado apoyado y no solo en una ausencia de contradicción.	< 3 meses	Imagen forense del puesto de trabajo	Tanto el hallazgo como su ausencia obligan a revisar: si no hay rastro, la vía de entrada queda sin explicar.

Figura 20. Los indicadores del caso. Cada uno apunta a una hipótesis concreta; la herramienta comprueba que existe.

14.2 El indicador que enseña más

EL CASO DE GRUPO ALVENTA

«El análisis forense del equipo del técnico encuentra rastro de phishing» está atado a Credenciales, la hipótesis mejor situada. Y su condición de revisión dice algo incómodo: **tanto el hallazgo como su ausencia obligan a revisar.** Si no hay rastro de phishing, la vía de entrada de la hipótesis mejor situada queda sin explicar.

15. El panel y la lectura del analista

LEER EL CONJUNTO SIN CONFUNDIR CÁLCULO CON JUICIO

El panel reúne recuentos y ecos de lo que has escrito. No hay ningún resultado nuevo: no busques aquí la respuesta.

15.1 El estado del análisis

ESTADO DEL ANÁLISIS

Hipótesis definidas	Evidencias definidas	Cruces valorados	Matriz completada
6	15	90	100 %

Figura 21. Las cifras de estado del caso: 6 hipótesis, 15 evidencias, 90 cruces, matriz completada al 100 %.

ADVERTENCIA

Completo no significa metodológicamente válido. Que no queden celdas sin valorar no dice nada sobre la calidad del análisis: esa depende de las hipótesis que escogiste, de la evidencia que reuniste y de tu juicio, y eso no lo comprueba ninguna fórmula.

15.2 Las hipótesis consideradas

HIPÓTESIS CONSIDERADAS — *EXCEL CALCULA*

HIPÓTESIS	ÍNDICE	I + II	VALORADAS	SIN VALORAR	ORDEN	SITUACIÓN
Credenciales	0	0	15	0	1	*Sigue en pie*
Ransomware	6	4	15	0	5	*Debilitada*
Proveedor	5	4	15	0	4	*Sigue en pie*
Configuración	10	5	15	0	6	*Debilitada*
Interna	3	3	15	0	2	*Sigue en pie*
Vulnerabilidad	3	2	15	0	2	*No demostrada*

Figura 22. La tabla del panel reúne el índice, el orden y la situación que el analista registró en la hoja de refutación.

La columna **SITUACIÓN** no la calcula el libro: es un eco del juicio que escribiste en el examen de refutación. Ponerla junto al índice es deliberado: permite ver de un vistazo si tu juicio coincide con el orden auxiliar, y si no coincide, que quede visible.

15.3 Las evidencias que más separan

EVIDENCIAS QUE MÁS SEPARAN LAS HIPÓTESIS — *EXCEL CALCULA*

EVIDENCIA	CD
Fallos VPN 4.200	*0.93*
Sesión 03:14	*0.87*
Borrado de auditoría	*0.80*
Herramienta remota	*0.80*
Ventana de cambios	*0.73*

Evidencias con capacidad discriminante 0: 1. No contribuyen a la comparación; pueden ser ciertas y relevantes.

Figura 23. Las cinco evidencias con mayor capacidad discriminante del caso, y el aviso de que una de ellas tiene CD 0.

15.4 La lectura del analista

ACH deja preguntas abiertas en cada fase, y la herramienta reserva un espacio para que la respuesta quede escrita y pueda auditarse después. Las cuatro columnas son siempre las mismas: **resultado observado, interpretación, evidencia en que me apoyo y limitación o duda.**

DIAGNOSTICIDAD — TÚ INTERPRETAS

RESULTADO	RESULTADO OBSERVADO	INTERPRETACIÓN	EVIDENCIA EN QUE ME APOYO	LIMITACIÓN O DUDA
	¿Qué muestra el recuento?	*¿Qué significa para mi análisis?*	*¿Por qué lo interpreto así?*	*¿Qué no sé o debo comprobar?*
¿Qué evidencias separan de verdad las hipótesis, y cuáles no?				
¿Hay evidencia con CD = 0? ¿Por qué no discrimina?				

Figura 24. La lectura del analista. El libro cuenta y ordena; interpretar es otra cosa.

16. El caso Grupo Alventa, de principio a fin

QUÉ SALIÓ Y QUÉ ENSEÑA

Este capítulo recorre el resultado completo. Los números son los verificados del caso: se han comprobado contra una reimplementación independiente y coinciden celda a celda en los dos niveles de la herramienta.

16.1 El resultado

Hipótesis	CC	C	N	I	II	Índice	I+II	Orden
Credenciales	4	8	3	0	0	0	0	1
Interna	2	7	3	3	0	3	3	2
Vulnerabilidad	0	8	5	1	1	3	2	2
Proveedor	2	8	1	3	1	5	4	4
Ransomware	0	8	3	2	2	6	4	5
Configuración	4	4	2	0	5	10	5	6

16.2 Una hipótesis con índice 0 no es la correcta

Credenciales no tiene ninguna evidencia registrada en contra. **Eso no la demuestra.** El propio libro lo pregunta en la hoja Comprobación: «¿has buscado de verdad evidencia que la contradiga?».

> EL CASO DE GRUPO ALVENTA
>
> Aquí la respuesta es que no se ha podido. La evidencia capaz de contradecirla estaría en los registros del servidor de aplicaciones del 11 y el 12 de abril, **que fueron borrados selectivamente**.
>
> Una hipótesis contra la que no se ha podido buscar no es lo mismo que una hipótesis que ha resistido la búsqueda.

Lo que sí la sostiene de forma positiva es una **secuencia temporal** que ninguna otra hipótesis explica completa: tanteo masivo de la VPN del 9 al 11 → primera sesión exitosa anómala el 12 a las 03:14 → instalación de la herramienta de administración remota ese mismo 12 → 240 GB salientes entre el 12 y el 13.

16.3 Un empate obliga a interpretar

Interna y Vulnerabilidad comparten índice 3 y el orden no las distingue. Son distintas por razones que el número no recoge: las inconsistencias de **Interna** son todas del tipo «no haría falta que lo hiciera así», que un

actor interno empeñado en parecer externo podría explicar; **Vulnerabilidad** es más débil, porque su única inconsistencia grave es sólida y no tiene ninguna evidencia que la apoye específicamente.

16.4 Un mismo argumento puede contarse varias veces

ADVERTENCIA

Proveedor queda en 5, pero ese número pide una corrección antes de usarlo. De sus cuatro inconsistencias, una es floja —una declaración de parte sin registros— y **tres proceden de una sola observación**: que el primer acceso externo satisfactorio y la instalación de la herramienta remota son del día 12, y la única sesión registrada del proveedor es del 13.

El índice cuenta esa observación tres veces porque aparece en tres filas. Es un efecto real del método —cada fila se evalúa de forma independiente— y es el tipo de cosa que el analista corrige al interpretar y que ningún cálculo corrige solo.

16.5 La calidad de la evidencia no entra en el índice

«Proveedor niega cambios» es una declaración de parte interesada sin registros que la respalden. Pesa en el índice exactamente lo mismo que una evidencia sólida, **y no debería**. El sitio para corregirlo es el razonamiento del analista, no la fórmula: IntelKIT registra fuente, fecha, tipo y observaciones como información cualitativa y no las mete en ningún cálculo.

16.6 Qué dicen los controles

Las doce comprobaciones de completitud salen «Correcto» y, aun así, el libro levanta **cinco avisos metodológicos**: hipótesis muy parecidas, una evidencia que no discrimina, dos consistentes con todas, una hipótesis sin ninguna inconsistencia y un empate en el orden auxiliar. Un análisis formalmente impecable que merece revisión.

17. Sesgos, límites y errores frecuentes

LO QUE ACH CONTIENE Y LO QUE NO

ACH está estrechamente vinculado a la preocupación de Heuer por las limitaciones cognitivas del análisis. Contiene algunos sesgos; no los elimina.

17.1 Qué sesgos ayuda a contener

Sesgo	Cómo lo contiene
Sesgo de confirmación	Obliga a evaluar todas las hipótesis con los mismos datos, no solo la preferida.
Cierre prematuro	El paso 5 exige intentar refutar antes de concluir.
Anclaje en la primera impresión	La matriz se recorre por filas, no por hipótesis.
Generación incompleta de alternativas	El paso 1 pide generar alternativas antes de evaluarlas, y preferiblemente desde perspectivas distintas.

ADVERTENCIA

ACH **no elimina** estos sesgos. Ayuda a reducir algunas formas de razonamiento confirmatorio al obligar a considerar alternativas y evidencia de manera explícita. La matriz la rellenas tú.

17.2 Errores frecuentes

Error	Por qué es un error
Tratar el índice como una probabilidad	Es un recuento ponderado de tus valoraciones. No hay probabilidades a priori ni actualización bayesiana.
Dar por ganadora la primera posición	Es la que acumula menos inconsistencia registrada, lo que puede deberse a que no se ha buscado en contra.
Contar evidencias a favor	ACH no es una votación. Una hipótesis puede tener muchas evidencias consistentes y seguir siendo poco diagnóstica.
Borrar la evidencia con CD = 0	Puede ser cierta y relevante para entender la situación. Simplemente no ayuda a elegir entre estas hipótesis.
Confundir completa con válida	Que no falten celdas no dice nada sobre la calidad de las hipótesis ni de la evidencia.
Leer la ausencia de evidencia como evidencia en contra	Solo cuenta si realmente cabría esperar observar ese dato.
Formular hipótesis que se solapan	Si dos pueden ser ciertas a la vez, la comparación no mide nada.
Cerrar el análisis sin indicadores	El paso 8 es lo que permite reabrirlo cuando llegue información nueva.

17.3 Qué pertenece al método y qué a IntelKIT

Marco ACH (Heuer · Heuer & Pherson · CIA)	Implementación IntelKIT
La matriz evidencia × hipótesis; la valoración como consistente, inconsistente o neutral; el valor diagnóstico; el foco en la refutación; la distinción entre no demostrada y refutada; la cautela con la ausencia de evidencia; el análisis de sensibilidad; la conclusión comparativa; los indicadores de observación futura; y que el juicio final es del analista.	La escala de cinco categorías CC / C / N / I / II; el índice de inconsistencia; la capacidad discriminante; el orden auxiliar; las capacidades 8 / 30 / 20 / 10; la estructura de campos de los registros; los controles de completitud; el panel, los colores y la navegación.

> **NOTA METODOLÓGICA**
>
> Ninguna métrica de IntelKIT debe atribuirse a Heuer ni presentarse como propiedad universal de ACH. La hoja Método del propio Excel mantiene esta separación campo por campo.

18. Checklist final

ANTES DE CERRAR EL ANÁLISIS

Las doce comprobaciones de completitud y los seis avisos metodológicos los hace la hoja Comprobación. Esta lista es lo que ninguna fórmula puede comprobar por ti.

18.1 Las hipótesis

- ¿Son alternativas **excluyentes**? ¿Puedo imaginar un escenario en que dos sean ciertas a la vez?
- ¿Responden todas a la misma pregunta?
- ¿He incluido la explicación incómoda y la que no implica a ningún adversario?
- ¿Hay alguna que no pueda quedar mal frente a ningún dato?
- ¿Falta alguna alternativa que la evidencia sugiera y no esté formulada?

18.2 La evidencia

- ¿He separado el dato, su procedencia y mi interpretación?
- ¿He incluido los supuestos que estoy dando por buenos?
- ¿He anotado qué información NO he podido obtener?
- ¿He valorado cada fila mirando todas las hipótesis antes de pasar a la siguiente?

18.3 La conclusión

- ¿He intentado refutar mi hipótesis preferida?
- ¿Distingo *debilitada por evidencia en contra* de *no demostrada por falta de apoyo*?
- ¿He explicado por qué una alternativa queda por delante, sin llamarla ganadora?
- ¿He informado también de las alternativas que siguen abiertas?
- ¿He escrito de qué evidencias depende la conclusión?
- ¿He definido indicadores que permitan reabrir el análisis?

18.4 Fuentes

Fuente primaria. Heuer, R. J. Jr. (1999). *Psychology of Intelligence Analysis*. Center for the Study of Intelligence, CIA. Capítulo 8, «Analysis of Competing Hypotheses».

Fuente complementaria. Heuer, R. J. Jr. & Pherson, R. H. (2014). *Structured Analytic Techniques for Intelligence Analysis* (2.ª ed.). CQ Press / SAGE.

Contraste institucional. Center for the Study of Intelligence (2009). *A Tradecraft Primer: Structured Analytic Techniques for Improving Intelligence Analysis*. CIA, sección ACH.

Documentación del proyecto. *ACH IntelKIT · Base académica y metodológica v1.0*, *Informe de construcción*, *Caso práctico* y *Auditoría del caso práctico*.