

LA CUEVA  
BLUE TEAM

CUADERNO DE CAMPO

# Qué hace realmente un analista

N0 · Preparación informática / Clase + laboratorio práctico / GRATUITA

Una ficha premium, editable y orientada al trabajo: explica lo esencial, enseña los comandos y termina en una evidencia verificable.

**5 páginas:** mapa TKS · comandos · demostración · práctica · entregable



# 01 / Contrato de aprendizaje

Diferenciar observación, hipótesis y decisión dentro de una investigación defensiva.

| Campo              | Compromiso verificable                                                                                                                          |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|
| Pregunta operativa | ¿Qué necesito observar primero para investigar qué hace realmente un analista sin adelantar una conclusión?                                     |
| Objetivo           | Redactar una nota inicial que otra persona pueda verificar.                                                                                     |
| Producto           | Inventario técnico                                                                                                                              |
| Aplicación laboral | En un entorno profesional, esta competencia permite producir activo, usuario, síntoma, fuente y hora sin ocultar las limitaciones de la fuente. |

## Mapa TKS

| T - Tarea                                                   | K - Conocimiento                        | S - Habilidad               |
|-------------------------------------------------------------|-----------------------------------------|-----------------------------|
| Redactar una nota inicial que otra persona pueda verificar. | Activo, usuario, síntoma, fuente y hora | Producir inventario técnico |

## Roles NICE relacionados

- IO-WRL-007 · Technical Support
- IO-WRL-005 · Systems Administration

## Conceptos esenciales de esta clase

- Activo
- usuario
- síntoma
- fuente y hora

## Qué puede preguntarte una entrevista

En una entrevista: ¿cómo investigarías “Qué hace realmente un analista” sin confundir un indicio con una conclusión?

## Criterio de salida

La clase se considera dominada cuando podés producir la evidencia indicada, explicar su fuente y declarar qué limitación impide una conclusión más fuerte.

## 02 / Guía completa de comandos

Cada tarjeta responde una pregunta concreta: propósito, sintaxis, ejemplo, salida, parámetros, equivalencias, riesgos y errores. Empezá por consultas de solo lectura.

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>01 whoami</b><br>Confirmar la identidad efectiva de la sesión.<br><b>Sintaxis</b><br>whoami<br><b>Ejemplo</b><br>whoami<br><b>Salida esperada</b><br>analyst<br><b>Parámetros</b><br>sin parámetros obligatorios en el ejemplo base<br><b>Equivalencias</b><br>No existe una equivalencia exacta: compará la fuente y los campos disponibles en tu plataforma.<br><b>Riesgo / uso seguro</b><br>Registrá también host y hora. Empezá en modo lectura y conservá la salida original.<br><b>Error frecuente</b><br>Ejecutarlo sin registrar host, usuario, ruta y hora. · Interpretar una salida parcial como una conclusión definitiva. | <b>02 hostname</b><br>Identificar el equipo observado.<br><b>Sintaxis</b><br>hostname<br><b>Ejemplo</b><br>hostname<br><b>Salida esperada</b><br>Nombre único del laboratorio.<br><b>Parámetros</b><br>sin parámetros obligatorios en el ejemplo base<br><b>Equivalencias</b><br>No existe una equivalencia exacta: compará la fuente y los campos disponibles en tu plataforma.<br><b>Riesgo / uso seguro</b><br>No confundas hostname con identidad de usuario. Empezá en modo lectura y conservá la salida original.<br><b>Error frecuente</b><br>Ejecutarlo sin registrar host, usuario, ruta y hora. · Interpretar una salida parcial como una conclusión definitiva. |
| <b>03 ps aux</b><br>Listar procesos con usuario y consumo.<br><b>Sintaxis</b><br>ps aux<br><b>Ejemplo</b><br>ps aux<br><b>Salida esperada</b><br>PID, usuario, CPU, memoria y comando.<br><b>Parámetros</b><br>sin parámetros obligatorios en el ejemplo base<br><b>Equivalencias</b><br>PowerShell: Get-Process · CMD: tasklist<br><b>Riesgo / uso seguro</b><br>Un nombre raro necesita contexto adicional. Empezá en modo lectura y conservá la salida original.<br><b>Error frecuente</b><br>Ejecutarlo sin registrar host, usuario, ruta y hora. · Interpretar una salida parcial como una conclusión definitiva.                    | <b>04 grep</b><br>Buscar un patrón dentro de la evidencia.<br><b>Sintaxis</b><br>grep -i <patrón> <archivo><br><b>Ejemplo</b><br>grep -i 03:17 evidence.log<br><b>Salida esperada</b><br>Líneas coincidentes con su fuente.<br><b>Parámetros</b><br>-i · <patrón> · <archivo><br><b>Equivalencias</b><br>PowerShell: Select-String · CMD: findstr<br><b>Riesgo / uso seguro</b><br>Elegí el patrón a partir de una pregunta. Empezá en modo lectura y conservá la salida original.<br><b>Error frecuente</b><br>Ejecutarlo sin registrar host, usuario, ruta y hora. · Interpretar una salida parcial como una conclusión definitiva.                                      |

## 03 / Demostración y tres momentos prácticos

Ubicar cada señal en su capa antes de buscar una causa.

| Paso | Señal          | Pregunta             | Limitación                 |
|------|----------------|----------------------|----------------------------|
| 01   | Activo         | ¿Qué campo observar? | ¿Qué todavía no demuestra? |
| 02   | usuario        | ¿Qué campo observar? | ¿Qué todavía no demuestra? |
| 03   | síntoma        | ¿Qué campo observar? | ¿Qué todavía no demuestra? |
| 04   | fuentes y hora | ¿Qué campo observar? | ¿Qué todavía no demuestra? |

### 1. Demostración explicada

Comprendé qué problema resuelve un analista, cómo piensa y por qué su trabajo no consiste solamente en mirar alertas o escribir comandos.

### 2. Práctica guiada

Evitá que una señal se transforme en una acusación sin evidencia.

- Copiar el dato exacto
- Nombrar la fuente
- Explicar la interpretación
- Proponer una alternativa
- Declarar qué falta

### 3. Investigación independiente

Repetí el procedimiento con ruido, un dato faltante y una hipótesis alternativa. La respuesta debe incluir fuente y limitación, no solo un identificador.

## 04 / Hoja editable de aplicación

Completá desde tu lector de PDF o imprimí la ficha. Usá datos ficticios o sanitizados y separá claramente observación de interpretación.

### Evidencia observada - fuente, comando y timestamp

### Razonamiento - hipótesis principal, alternativa y confianza

### Decisión - preservación, limitación y próximo paso

### Checklist de salida

- Conservo la fuente
- Registro fecha y alcance
- Separo evidencia de interpretación
- Documento el próximo paso

### Revisión espaciada

- ¿Qué tres datos conservarías primero al trabajar qué hace realmente un analista?
- ¿Cómo cambiaría tu procedimiento si faltara fuente y hora?
- Aplicá qué hace realmente un analista dentro de un caso del módulo “Anatomía de un equipo” y defendé una hipótesis alternativa.

### Versión

Currículo 3.2.0 · NICE 2.2.0 · ATT&CK v19.2 · Actualizada 24 de agosto de 2026