



## Manual de Capacitación

# Introducción al Sistema de Vigilancia e Inteligencia Une 166006

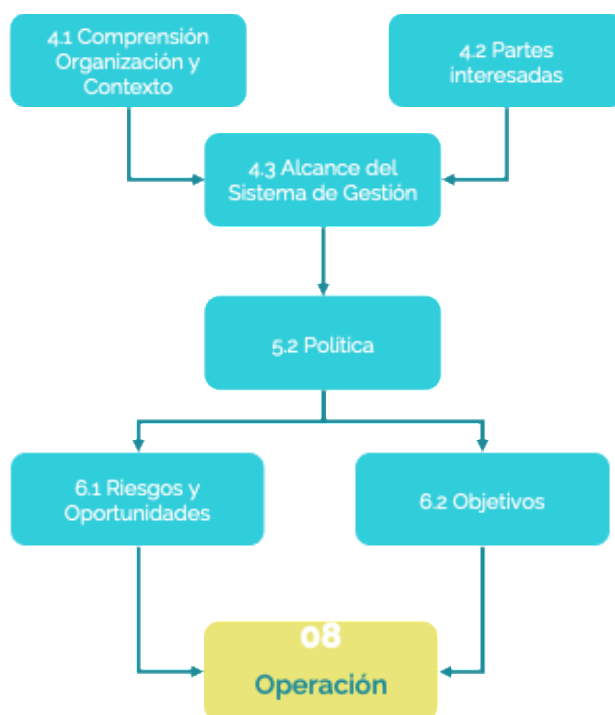
## MÓDULO 5: Diseño del Sistema

## Objetivo del módulo

Diseñar el sistema de vigilancia e inteligencia tecnológica a partir de la identificación de entornos y áreas de interés, formulando políticas, objetivos y procesos operativos en coherencia con el contexto organizacional, los riesgos y las partes interesadas.

## Enfoque de diseño y columna vertebral

A diferencia de una implementación puramente normativa basada en el seguimiento secuencial de los requisitos (4.1, 4.2, 4.3, etc.), el diseño de un sistema de vigilancia debe seguir una lógica funcional. Esta lógica parte desde la comprensión del contexto y partes interesadas, que permite identificar los entornos y áreas de interés, para luego traducirse en política, objetivos, planificación y operación.

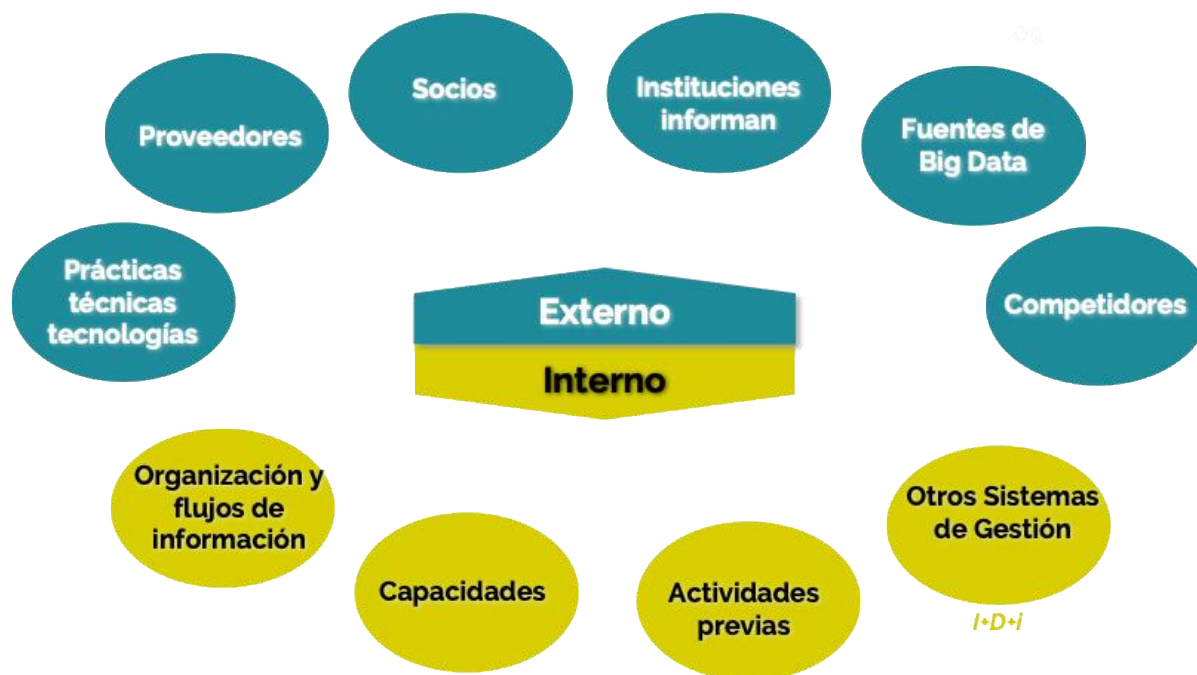


Esta estructura, que puede considerarse la columna vertebral del diseño, integra los siguientes requisitos clave:

- 4.1 Comprensión del contexto
- 4.2 Comprensión de las partes interesadas
- 4.3 Determinación del alcance
- 5.2 Política
- 6.1 y 6.2 Planificación: riesgos, oportunidades y objetivos
- 8. Operación (especificada en el siguiente módulo)

## Análisis del contexto (Requisito 4.1)

El análisis del contexto en vigilancia debe centrarse en aspectos técnicos, tecnológicos y estratégicos, más allá de diagnósticos genéricos como FODA o PESTEL.



Se deben considerar:

Contexto externo:

- Prácticas y modelos de vigilancia (e.g. francés, norteamericano)
- Técnicas de extracción y análisis de datos (booleanos, semánticos)
- Proveedores (software, analistas externos)
- Socios e instituciones que informan
- Fuentes de Big Data (ej. sensores, tráfico, internet)
- Competidores en vigilancia (no solo en mercado)

Contexto interno:

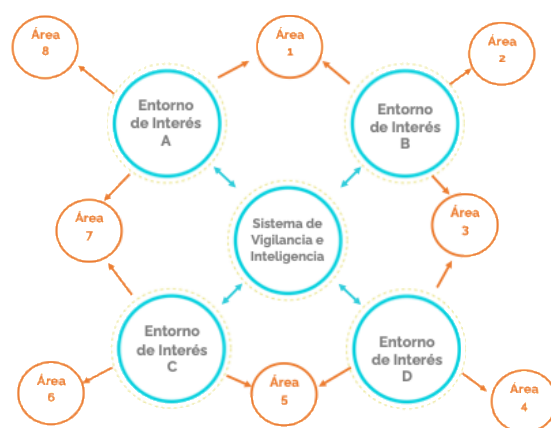
- Flujo de información y documentación
- Capacidades del equipo humano (uso de software, metodologías)
- Infraestructura tecnológica (mínimo: conexión, hojas de cálculo)
- Experiencias previas en vigilancia
- Integración con otros sistemas (innovación, calidad)

## Partes interesadas y entornos de interés (Requisito 4.2)

Las partes interesadas no solo deben identificarse como actores pasivos, sino como generadores de necesidades y expectativas de información. Este análisis permite definir los entornos de interés, es decir, dominios estratégicos donde la vigilancia aporta valor (clientes, socios, sector público, universidades, etc.).

Externas	Necesidades	Expectativas
Socios		
Proveedores		
Distribuidores		
Organizaciones Investigación		
Clientes y usuarios		
Autoridades		
...		

Internas	Necesidades	Expectativas
Empleados		
Dirección		
Departamentos		
Accionistas		
...		



Cada entorno de interés se traduce luego en una o varias áreas científicas o tecnológicas, que serán el núcleo del alcance del sistema. La relación entre entorno y área permite alinear vigilancia con la estrategia de innovación.

## Alcance del sistema de vigilancia (Requisito 4.3)

El alcance no se define por procesos organizacionales, como en calidad, sino por áreas científicas y tecnológicas, usualmente clasificadas según los códigos UNESCO.



01 Lógica  
12 Matemáticas  
21 Astronomía Y Astrofísica  
22 Física  
23 Química  
24 Ciencias De La Vida  
25 Ciencias De La Tierra Y Del Espacio  
31 Ciencias Agrarias  
32 Ciencias Médicas  
33 Ciencias Tecnológicas  
51 Antropología  
52 Demografía  
53 Ciencias Económicas  
54 Geografía  
55 Historia  
56 Ciencias Jurídicas Y Derecho  
57 Lingüística  
58 Pedagogía  
59 Ciencia Política  
61 Psicología  
62 Ciencias De Las Artes Y Las Letras  
63 Sociología  
71 Ética  
72 Filosofía

Estas áreas pueden pertenecer a:

- Ciencias básicas (códigos 01 al 25)
- Ciencias aplicadas y tecnológicas (31, 32, 33)
- Ámbitos sectoriales específicos (agrarias, médicas, económicas)

Es esencial actualizar estos códigos y vincularlos con las necesidades organizacionales.

## Política de vigilancia (Requisito 5.2)

La política debe ser coherente con el propósito de la organización y estar alineada con el contexto, partes interesadas y alcance definido. Aunque su redacción es formalmente similar a otras normas, su contenido debe ser específico a la vigilancia y, preferiblemente, estar integrada a la política de innovación si esta existe.

## Riesgos y oportunidades (Requisito 6.1)

La norma exige gestionar los riesgos y oportunidades asociados al sistema. Se recomienda usar la metodología de la ISO 31000 para estructurar la matriz.

Identificación (6.4.2)	Análisis (6.4.3)	Evaluación (6.4.4)	Tratamiento (6.5)
<b>A partir de objetivos</b> <ul style="list-style-type: none"> <li>Estratégicos</li> <li>Procesos</li> <li>Productos</li> <li>vigilancia</li> <li>Proyectos I+D+i</li> </ul>	<b>A partir de datos:</b> <ul style="list-style-type: none"> <li>Históricos</li> <li>Expertos</li> <li>Pronósticos</li> </ul> <b>Elementos</b> <p>a. Causas</p> <ul style="list-style-type: none"> <li>Fuentes de riesgos</li> <li>Eventos</li> <li>Amenazas</li> </ul> <p>b. Consecuencias</p>	<b>Nivel de riesgo</b> <p>Probabilidad x Consecuencia</p>	<b>Jerarquía de controles</b> <ol style="list-style-type: none"> <li>1. Eliminar fuente de riesgos</li> <li>2. Cambiar evento</li> <li>3. Cambiar consecuencia</li> <li>4. Evitar, mantener, financiar, aceptar, aumentar, compartir, etc.</li> </ol> <b>Evaluar eficacia de acciones</b> <b>Planes y procedimientos</b> <b>Riesgo residual</b>

Ejemplos de riesgos:

- Informes no entregados a tiempo
- Datos no validados o sin contexto
- Necesidades de información mal definidas
- Falta de claridad en las acciones derivadas

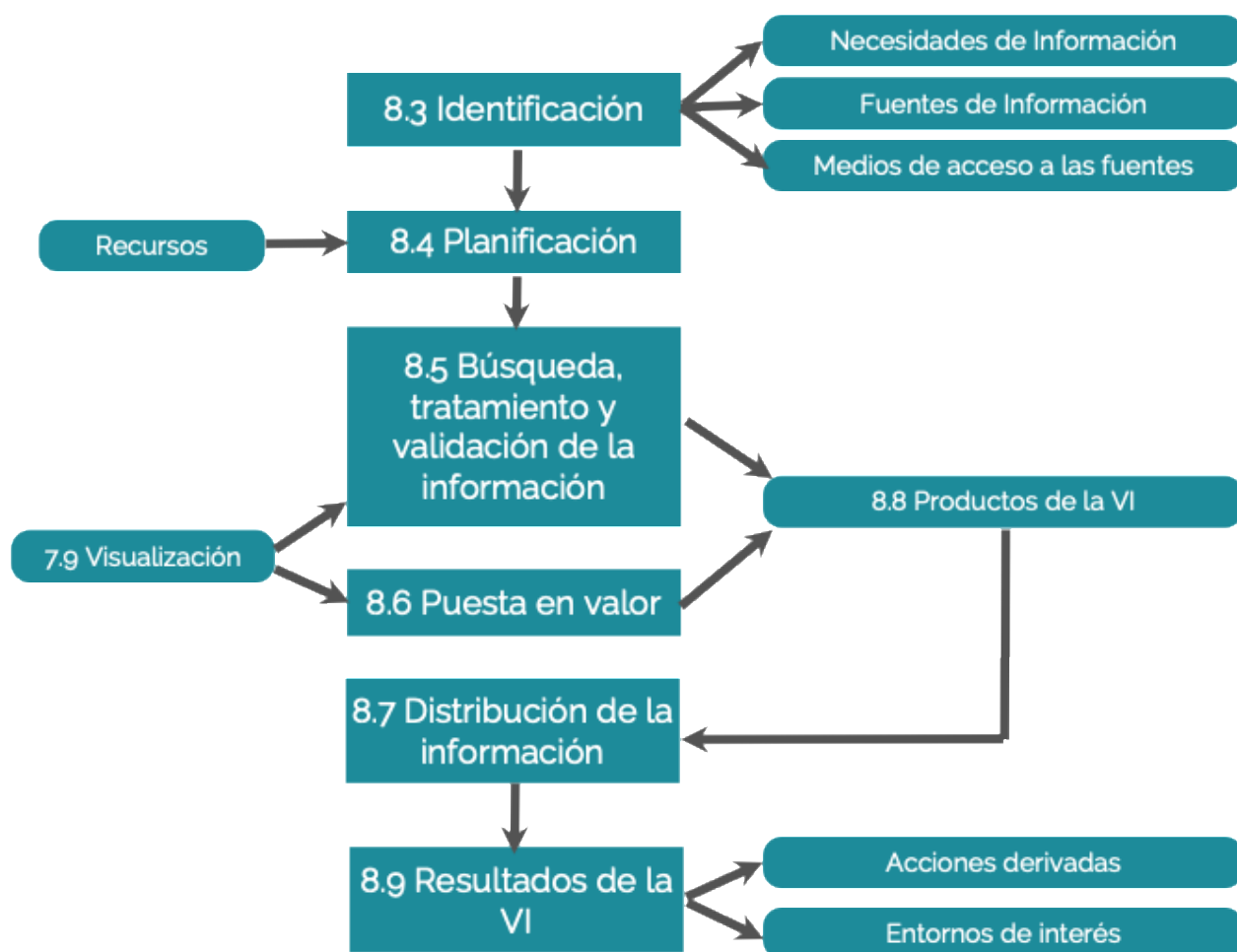
El tratamiento de estos riesgos debe quedar documentado con acciones concretas.

## Objetivos del sistema (Requisito 6.2)

Los objetivos deben derivarse de la política y estar alineados con el contexto y alcance. La norma exige que estén documentados (información documentada) y orientados a resultados verificables. Es decir, deben reflejar cómo el sistema contribuye a la toma de decisiones estratégicas.

## Operación del sistema (Requisito 8)

El diseño del sistema de vigilancia debe culminar en la definición del proceso operativo. Este se encuentra descrito en el capítulo 8 de la norma y comprende desde la identificación de necesidades de información hasta la generación de productos de vigilancia. Aunque el desarrollo detallado del proceso será tratado en el siguiente módulo, es fundamental en esta etapa del diseño prever los recursos, roles y flujos necesarios para su funcionamiento.



Una planificación del sistema sin su componente operativo no está completa. Por tanto, el diseño debe considerar que los objetivos y políticas establecidos se traduzcan en prácticas concretas de recolección, tratamiento, análisis, validación y entrega de información estratégica.