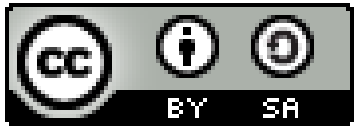
Tema 2. Sistema de Inteligencia Tecnológica: Norma UNE 166006:2018

Asignatura: Desarrollo con Tecnologías Emergentes (580011)
Curso 2020-21
Grado en Ingeniería en Sistemas de Información
Universidad de Alcalá
José Ramón Hilera González



Índice

1. Características de la norma UNE 166006:2018 (1)

- Permite realizar de **manera sistemática** la observación y búsqueda de señales de cambio y **novedades** enfocadas a la **captura de información**, la selección y el análisis, la difusión y comunicación para **convertirla en conocimiento** que permita la **toma de decisiones**, y el seguimiento de la explotación de sus resultados. (UNE, 2018)
- Facilita la **relación** entre los prestatarios de la Vigilancia Tecnológica, sean internos o externos, y sus clientes en la organización, proporcionando **una terminología común**, identificando las relaciones, posibles sinergias y complementariedad entre esta actividad y otras, precisando los elementos constitutivos de su oferta, ayudando a entender y clarificar los **roles** y compromisos respectivos
- Permite la **certificación** del sistema por parte de una Entidad de Certificación, y por tanto, demostrar ante terceros que se dispone de los recursos técnicos y humanos necesarios para realizar la vigilancia e inteligencia tecnológica dentro de la empresa o para otras empresas.

1. Características de la norma UNE 166006:2018 (2)

NORMAS RELACIONADAS

- UNE 166000:2006. Gestión de la I+D+i: Terminología y definiciones de las actividades de I+D+i.
- UNE 166001:2006. Gestión de la I+D+i: Requisitos de un proyecto de I+D+i.
- UNE 166002:2014. Gestión de la I+D+i: Requisitos del Sistema de Gestión de la I+D+i.
- UNE 166006:2018. Gestión de la I+D+i: Sistema de vigilancia e inteligencia.
- UNE 166008:2012. Gestión de la I+D+i: Transferencia de tecnología.

1. Características de la norma UNE 166006:2018 (3)

EVOLUCIÓN DE LA NORMA

1. Características de la norma UNE 166006:2018 (4)

APARTADOS

1. Objeto y campo de aplicación
2. Normas para consulta
3. Términos y definiciones
4. Contexto de la organización
5. Liderazgo
6. Planificación
7. Apoyo
8. Operación
9. Evaluación del desempeño
10. Mejora

1. Características de la norma UNE 166006:2018 (5)

OBJETO Y CAMPO DE APLICACIÓN

- Esta norma es aplicable a todas las organizaciones que establezcan un sistema de gestión de vigilancia e inteligencia, independientemente de su tamaño, actividad o ámbito geográfico.
- También puede utilizarse como especificación de compra para la contratación de servicios a terceros.

NORMAS PARA CONSULTA

- UNE 166000:2006 Gestión de la I+D+i: Terminología y definiciones de las actividades de I+D+i.

1. Características de la norma UNE 166006:2018 (6)

TÉRMINOS Y DEFINICIONES

- **Área**: Temática o tecnología delimitada y precisa, en la cual se centra la vigilancia e inteligencia, y que abarca un campo más reducido que los entornos de interés.
- **Entorno de interés**: Aspecto de la actividad de la organización en el que se presenta posibilidad de oportunidades.
- **Vigilancia e inteligencia**: Proceso ético y sistemático de recolección y análisis de información acerca del ambiente de negocios, de los competidores y de la propia organización, y comunicación de su significado e implicaciones destinada a la toma de decisiones

1. Características de la norma UNE 166006:2018 (7)

REQUISITOS A CUMPLIR POR EL SISTEMA DE VIGILANCIA E INTELIGENCIA

- Requisitos sobre la organización (Apartado 4)
- Requisitos sobre liderazgo (roles) (Apartado 5)
- Requisitos sobre planificación (Apartado 6)
- Requisitos sobre apoyo (Apartado 7)
- Requisitos sobre operación (etapas y resultados) (Apartado 8)
- Requisitos sobre evaluación del desempeño (Apartado 9)
- Requisitos sobre mejora (Apartado 10)

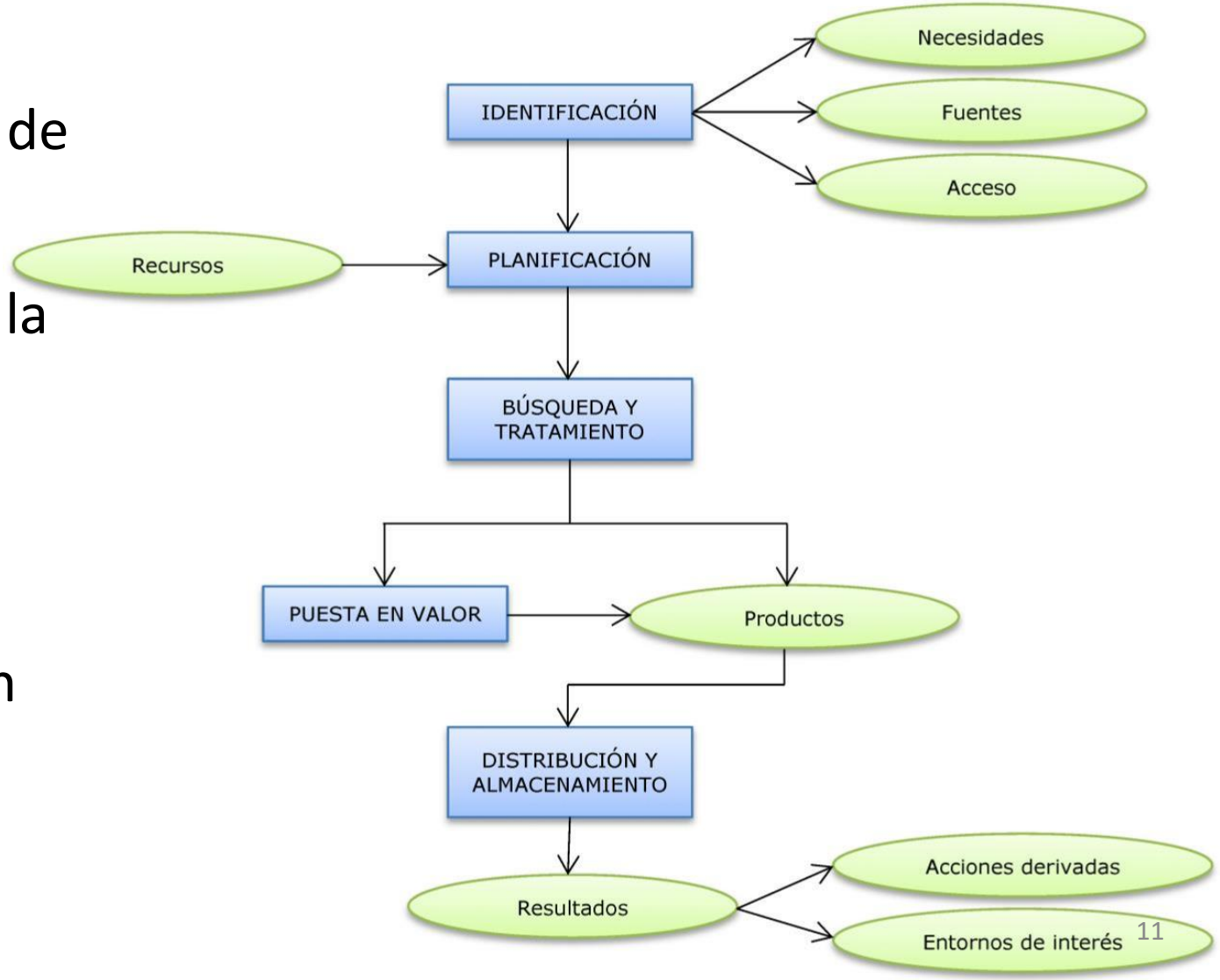
1. Características de la norma UNE 166006:2018 (8)

EJEMPLOS DE REQUISITOS

- *La organización debe determinar los límites y la aplicabilidad del sistema de gestión de vigilancia e inteligencia para establecer su alcance* (apdo. 4)
- *La alta dirección debe establecer una política de vigilancia e inteligencia…* (apdo. 5)
- *La organización debe planificar las acciones para abordar riesgos y oportunidades...* (apdo. 6)
- *La organización debe determinar y proporcionar los recursos necesarios para el establecimiento, mantenimiento y mejora continua del sistema de gestión de vigilancia e inteligencia* (apdo. 7)
- *Los productos de la vigilancia e inteligencia se deben distribuir a las partes interesadas de la organización según sus necesidades* (apdo. 8)
- *La organización debe conservar la información documentada adecuada como evidencia de los resultados* (apdo. 9)
- *La organización debe mejorar continuamente la idoneidad, adecuación y eficacia del sistema de gestión de vigilancia e inteligencia* (apdo. 10)

2. Etapas del proceso de vigilancia e inteligencia

1) **Identificación** de necesidades, fuentes de información y medios de acceso
2) **Planificación** de la realización de la vigilancia e inteligencia
3) **Búsqueda y tratamiento** de la información
4) **Puesta en valor** de la información
5) **Distribución y almacenamiento**

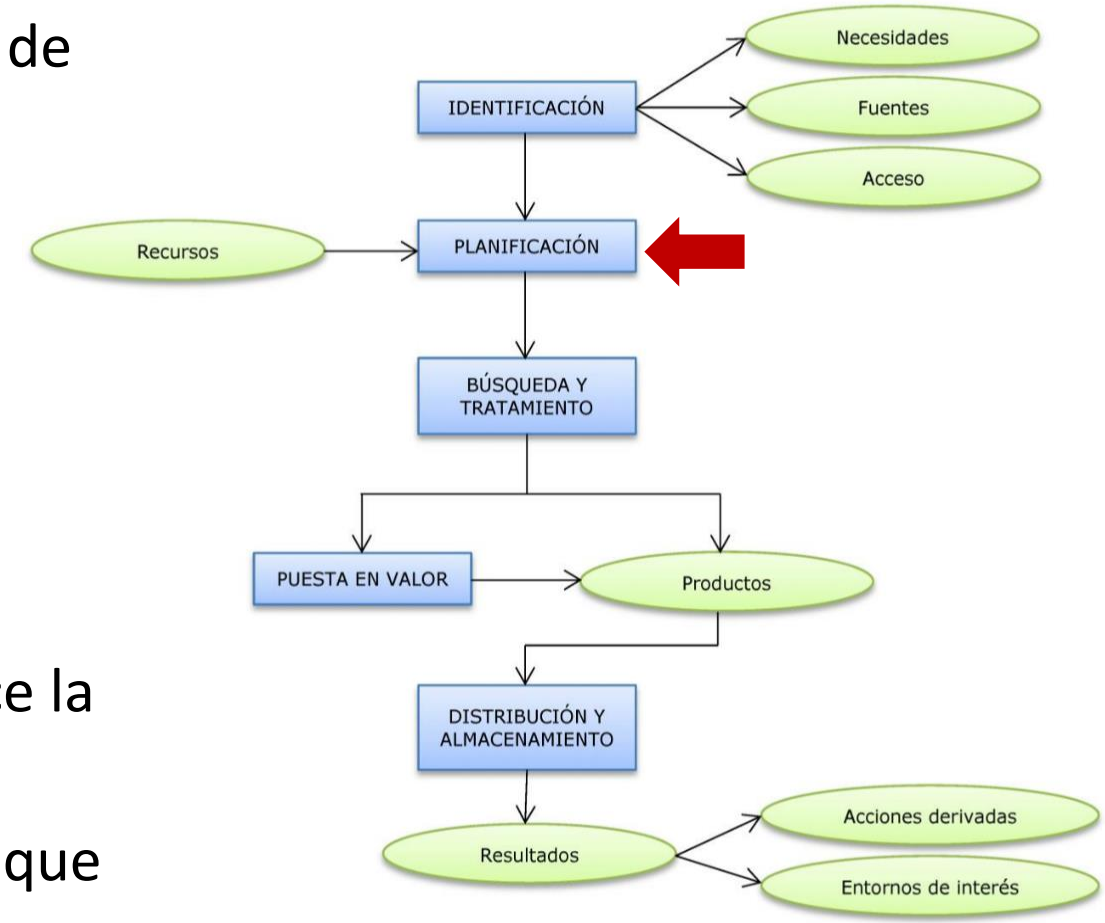


2. Etapas del proceso de vigilancia e inteligencia
1) Identificación de necesidades, fuentes y acceso

- **Necesidades**: La organización debe definir un proceso documentado para la identificación de necesidades de información, que incluya:
  a) Las áreas de vigilancia e inteligencia identificadas;
  b) Un primer avance sobre el conjunto de fuentes de información disponible para estas áreas;
  c) Un avance sobre palabras clave, operadores, criterios de selección etc.;
  d) Información sobre el tipo de producto que se entregará y sus contenidos.
- **Fuentes**: Tomando como base las necesidades de información, se deben identificar las fuentes de información y recursos internos disponibles en la organización, junto con aquéllas externas que pueden ser accesibles. La identificación de las fuentes de información externas debe estar basada en criterios de calidad, pertinencia, objetividad y fiabilidad de las mismas.
  - Ejemplos de fuentes: documentos, personas, organizaciones, congresos, normas, leyes, patentes.
- **Acceso**: Deben identificarse y valorarse los medios necesarios para el acceso al contenido completo de las fuentes de información.

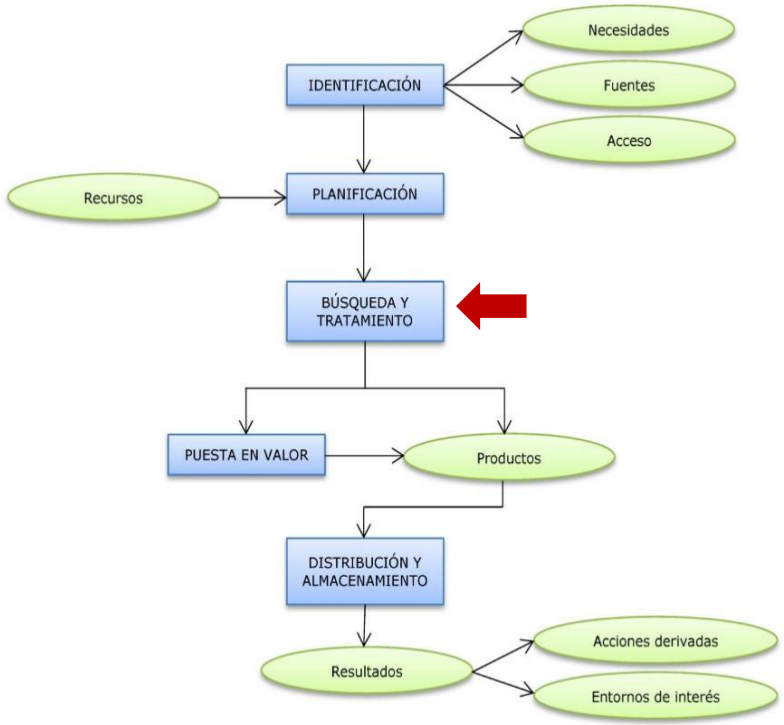
2. Etapas del proceso de vigilancia e inteligencia
2) Planificación

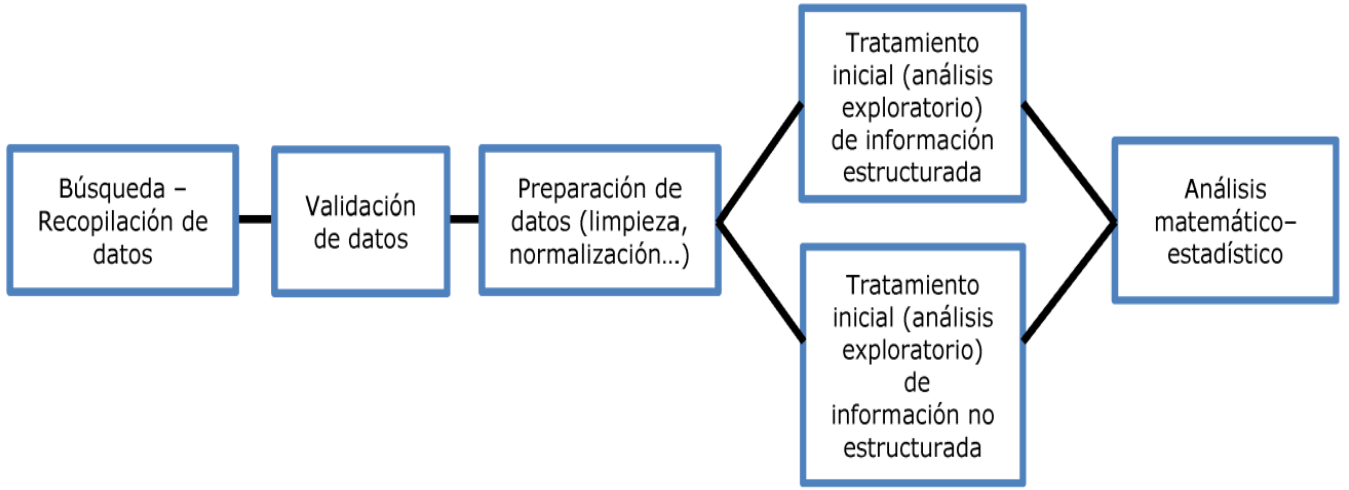
- En función de las necesidades de información detectadas, las fuentes de información y medios de acceso a las mismas, se deben planificar y dimensionar los **recursos** según datos de la experiencia y de acciones previsibles.
- Recursos: humanos, infraestructura, financieros, tecnológicos, permisos, licencias, etc.
- Como la vigilancia es un proceso continuo, la organización debe asegurarse de que se establece la estructura, la periodicidad y la actualización del **seguimiento** sistemático de novedades en áreas que ya estén previamente identificadas.



2. Etapas del proceso de vigilancia e inteligencia
3) Búsqueda y tratamiento de la información

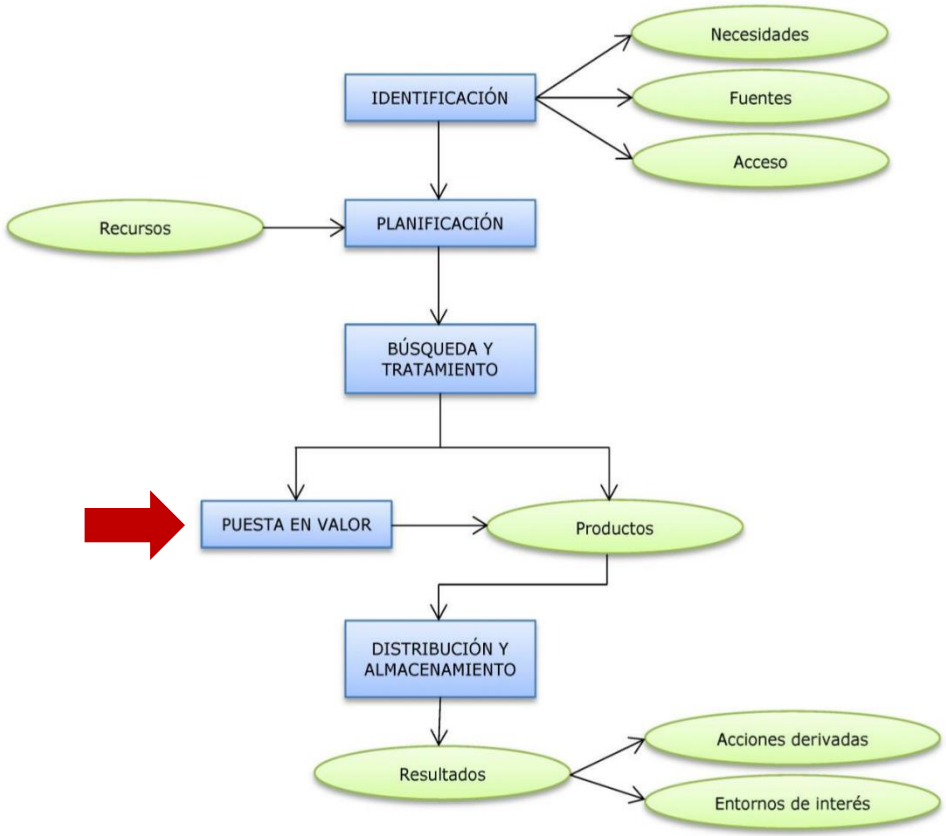
- **Búsqueda**: Se debe realizar estableciendo una estrategia y acciones de búsqueda en las fuentes seleccionadas, teniendo en cuenta, por ejemplo, los términos de búsqueda (palabras clave), operadores utilizados, la segmentación geográfica o temporal utilizada.
- **Tratamiento**: Puede incluir técnicas cualitativas, y otras cuantitativas como estudio estadístico sobre la frecuencia y distribución de los elementos identificados, extracción de términos frecuentes y relacionados, agrupación de términos, representaciones gráficas, análisis de la posición relativa de los términos, etc.





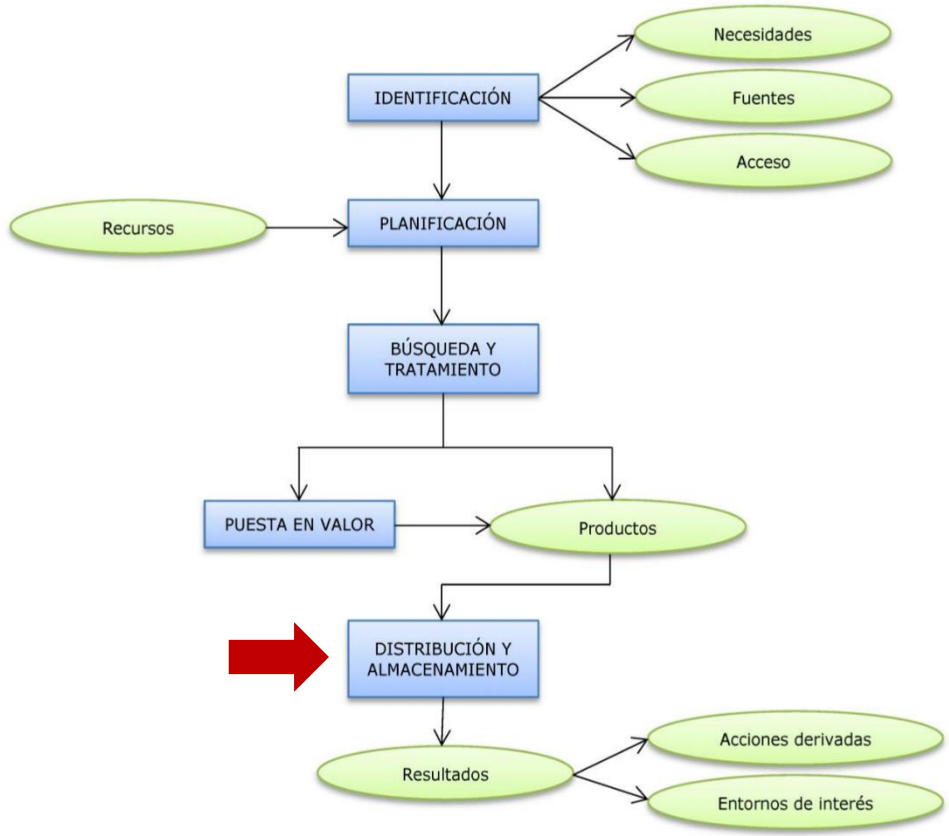
2. Etapas del proceso de vigilancia e inteligencia
4) Puesta en valor de la información

- Cuando el contenido de la información obtenida no sea suficiente para satisfacer las necesidades planteadas, será necesario una **mayor profundidad de análisis** para poner en valor la información obtenida de cara a la toma de decisiones.
- La puesta en valor puede incluir aspectos como:
  - **Integración** de datos de diversas procedencias, con objeto de conseguir sinergias donde la combinación de información procedente de los diferentes medios de obtención constituye un todo de mayor relevancia y alcance que cada una de las informaciones por separado.
  - **Interpretación** de la información, con el doble objetivo de determinar lo que es exacto y también lo que es relevante para la toma de decisiones, incluyendo por ejemplo la comprensión del fenómeno analizado o un pronóstico sobre sus consecuencias y previsible evolución.
  - Obtención del significado de los hechos analizados y de sus probables **implicaciones** y consecuencias para la organización.
  - **Recomendaciones** de actuación, aunque será el usuario final el que acabará de dar valor a la información



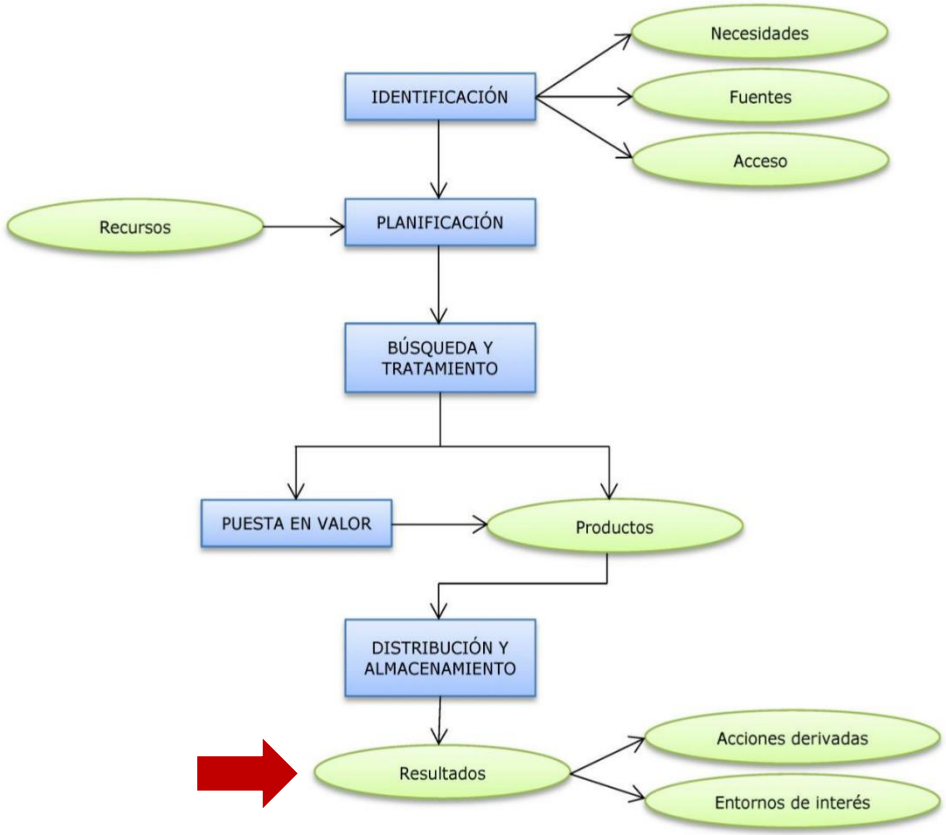
2. Etapas del proceso de vigilancia e inteligencia
5) Distribución y almacenamiento

- Los productos de la vigilancia e inteligencia obtenidos se deben distribuir a las partes interesadas de la organización según sus necesidades.
- Productos (ejemplos):
  a) Productos que incluyen un **nivel bajo de análisis**: Listados de noticias, que se difunden en formato RSS o mediante alertas personalizadas, boletines temáticos o sectoriales, etc., ya sean puntuales o periódicos.
  b) Productos que incluyen un **nivel medio de análisis**: Informes, estado del arte o de la técnica, estudios bibliográficos, estudios de patentabilidad, etc.
  c) Productos que incluyen un **nivel profundo de análisis**: Estudios exhaustivos, análisis de tendencias, etc.



3. Resultados de la vigilancia e inteligencia

- El principal resultado de la vigilancia e inteligencia es el conocimiento adquirido por la organización para reducir la incertidumbre en la toma de decisiones.
- Este conocimiento puede aplicarse:
  - poniendo en marcha acciones derivadas
  - o identificando nuevos entornos de interés para la organización.



3. Resultados de la vigilancia e inteligencia Acciones derivadas (ejemplos)

a) **Anticipación**: Propuestas de acciones en función de la situación relativa detectada respecto a los cambios y expectativas de cambios del entorno analizado.

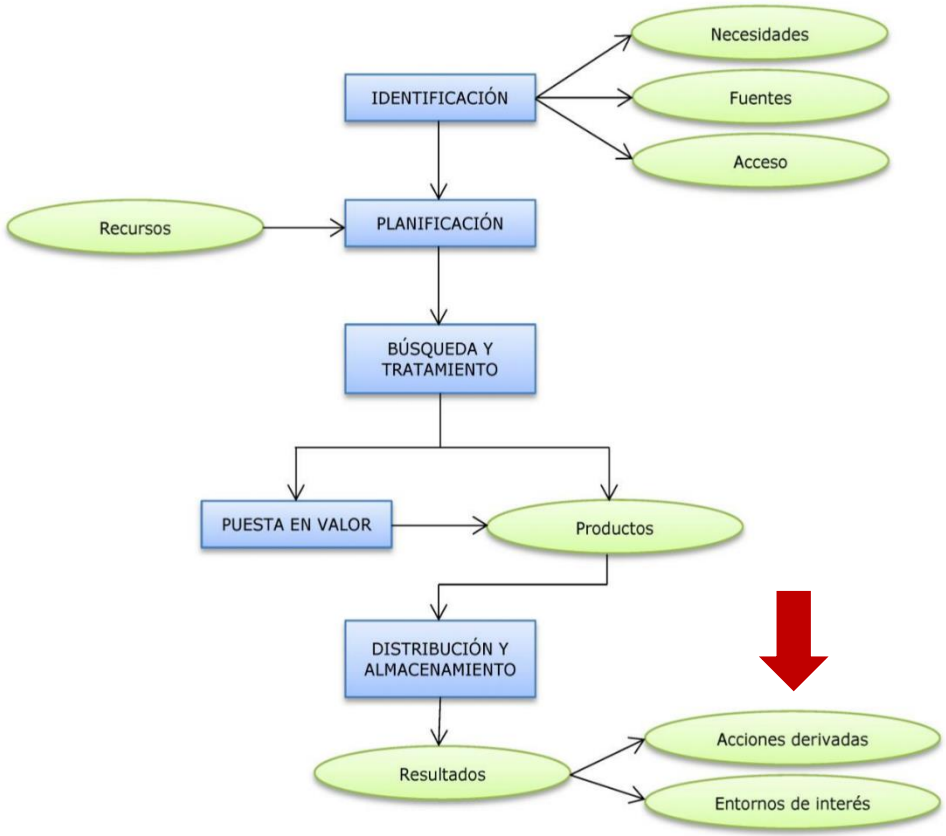
b) **Aprovechamiento de oportunidades**: Propuestas de acciones para explotar las ventajas identificadas.

c) **Reducción de riesgos**: Propuestas de acciones para disminuir las amenazas o superar las barreras de acceso a tecnologías y/o mercados.

d) **Líneas de mejora**: Propuestas de acciones necesarias para superar los desfases y minimizar las debilidades identificadas.

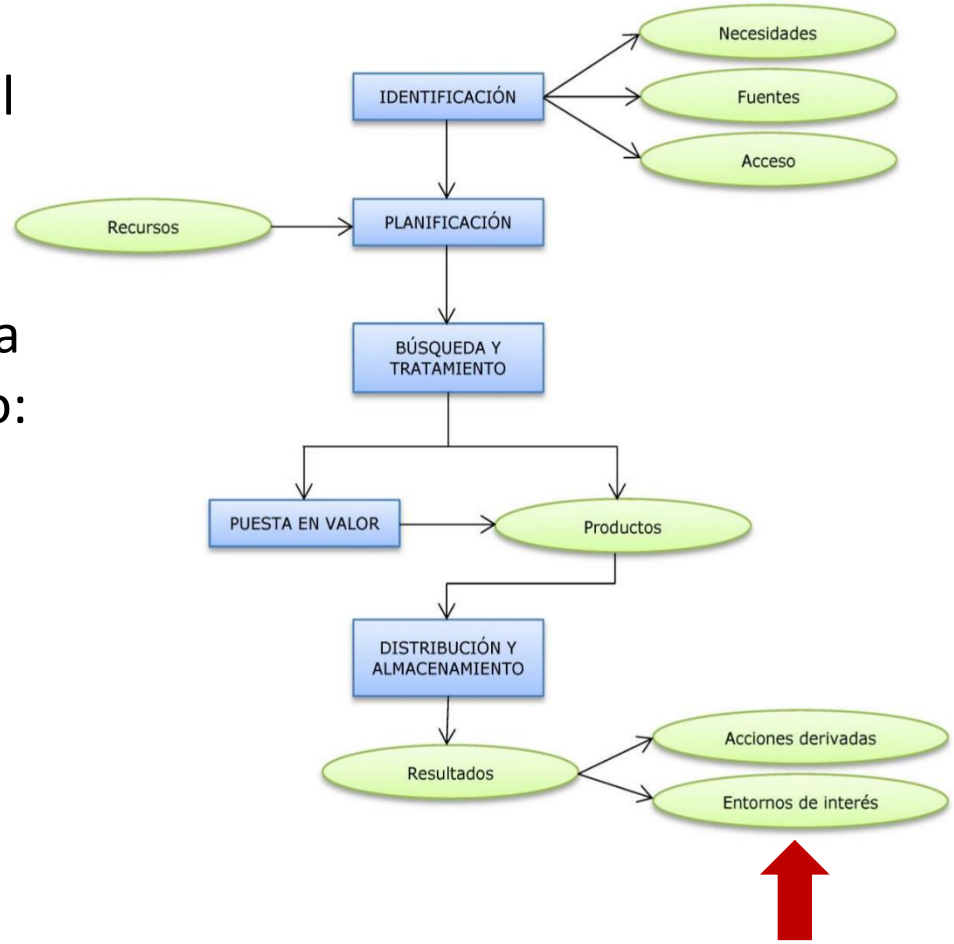
e) **Innovación**: Propuestas de nuevas ideas y/o proyectos de I+D+i.

f) **Cooperación**: Identificación de potenciales colaboradores.



3. Resultados de la vigilancia e inteligencia Entornos de interés para l organización

- Otro resultado de la vigilancia puede ser la identificación de **oportunidades** en nuevos entornos tecnológicos y/o mercados de interés para la organización, o bien propiciar el **abandono** por falta de interés de algunos los entornos actualmente considerados.
- La información sobre los entornos de interés es clave para la revisión por la Dirección, pudiendo contener aspectos como:
  a) La valoración de las opciones tecnológicas y/o de mercado.
  b) Los impactos e interacciones entre tecnologías, productos y procesos.
  c) Las expectativas de evolución de las tecnologías.
  d) Oportunidades de inversión y comercialización.
  e) Tendencias sociales.



4. Roles propuestos por la norma

- **Coordinador o Dinamizador**: se trata de la persona que se encarga del correcto funcionamiento del sistema de vigilancia e inteligencia, asegurando el proceso y organizando las tareas de los diferentes participantes.
- **Gestor de fuentes (documentalista)**: persona que conoce y gestiona las diferentes fuentes de información que existen, dando soporte a los analistas para sacar el máximo rendimiento de las mismas.
- **Analista (científico de datos)**: persona que se encarga de revisar, validar y compartir la información que se recibe, añadiendo valor a la misma con su conocimiento del sector.
- **Administrador**: persona que gestiona las tecnologías de la información para dar soporte al proceso. Normalmente, este rol no pertenece exclusivamente al sistema de vigilancia e inteligencia, pero tiene influencia sobre el mismo.
- **Lector o Consumidor**: destinatario de la información distribuida por los analistas, que la utiliza en la toma de decisiones a nivel operativo o estratégico, proporcionando también información de retorno a los analistas (sobre su pertinencia, relevancia, formato, etc.).

4. Roles propuestos por la norma Competencias por rol

- **Coordinador o Dinamizador**: Liderazgo. Capacidad de organización del trabajo. Capacidad de trabajo en equipo. Capacidad de comunicación. Iniciativa y proactividad.
- **Gestor de fuentes (documentalista)**: Manejo y explotación de bases de datos especializadas. Herramientas y recursos para la búsqueda de información. Técnicas y herramientas específicas de recuperación, análisis y tratamiento de datos. Minería de textos científico técnicos: Indicadores bibliométricos, índice de impacto, métrica de citaciones. Sistemas de clasificación de tecnologías y áreas tecnológicas. Conocimiento sobre propiedad industrial e intelectual. Conocimiento sobre herramientas de apoyo.
- **Analista (científico de datos)**: Proactividad, interés por las novedades más relevantes. Manejo de técnicas de análisis. Conocimiento sobre la información que aporta la propiedad industrial e intelectual, y sus mecanismos de funcionamiento. Análisis y gestión de las tecnologías, el entorno del negocio y los mercados. Competencia técnica en la materia a tratar.
- **Administrador**: Perfil técnico en tecnologías de la información. Instalación y administración de las herramientas tecnológicas utilizadas en el sistema.

5. Certificación (1)

- Es posible que una entidad acreditada certifique que un sistema de vigilancia e inteligencia tecnológica es conforme con la Norma UNE 166006.
- Las entidades que pueden certificar son las acreditadas para ello por ENAC.
- Proceso de certificación (Fuente: AENOR)
  1. Solicitud y contrato
  2. Recepción de la solicitud
  3. Auditoría inicial (Fase 1 y Fase 2)
  4. Evaluación y acuerdos
  5. Concesión del Certificado
  6. Mantenimiento de la Certificación
  7. Renovación del Certificado

5. Certificación (2)

1. **Solicitud y contrato**: Las organizaciones que soliciten la certificación tendrán implantado el sistema de vigilancia e inteligencia por un periodo mínimo de tres meses.
2. **Recepción de la solicitud**: La Entidad certificadora puede decidir la anulación de la solicitud si por alguna causa la certificación no se puede llevar a cabo en un año.
3. **Auditoría inicial (3 meses)**: Tiene como finalidad determinar si el sistema implantado por la organización cumple con los requisitos establecidos en la norma.
   - Fase 1: El equipo auditor se asegura de que el nivel de implantación del sistema garantiza que la organización está preparada para la auditoría de la fase 2.
   - Fase 2: El equipo auditor comprueba si el sistema, descrito en la documentación presentada por la organización y evidenciado en los registros, está efectivamente implantado y cumple con los requisitos.
   - Si existen no conformidades, la organización debe presentar en un plazo de 30 días un plan de acciones correctivas necesarias, indicando los plazos previstos para su puesta en marcha, así como cuantas evidencias sean necesarias para demostrar la eficacia de las mismas. Si éstas fuesen insuficientes, habrá un plazo extra de 15 días más.

5. Certificación (3)

4. **Evaluación y acuerdos**: Se evalúa la información recopilada en la auditoría inicial y, si existen no conformidades, el plan de acciones correctivas. Se adopta un acuerdo:
   - Conceder el Certificado
   - Conceder el Certificado y, tras ello, llevar a cabo una auditoría extraordinaria para verificar la resolución de las no conformidades detectadas.
   - No conceder el Certificado hasta la realización de una auditoría extraordinaria con resultados satisfactorios.

5. **Concesión del Certificado**: Se emite un certificado por un máximo de 3 años.
   - La organización se incluye en un registro público de organizaciones certificadas.

5. Certificación (4)

6. **Mantenimiento de la certificación**: Se realizarán auditorías anuales de seguimiento. Si existen no conformidades importantes, la organización deberá presentar en 30 días un plan de acciones correctivas.
   - Después de cada auditoría se decide si se mantiene la Certificación, si se hará una auditoría extraordinaria para comprobar la implantación de las acciones correctivas, o si se impone una sanción de Apercibimiento, de Suspensión temporal del Certificado, o de Retirada del Certificado.
7. **Renovación del Certificado**: Al menos 3 meses antes de finalizar el periodo de validez del Certificado, se efectuará una auditoría del sistema para verificar si procede su renovación.
   - La auditoría de renovación evaluará si el sistema es eficaz y contribuye al logro de la política y los objetivos de la organización. Se procede como en las auditorías de seguimiento (plazos, acuerdos).
   - Se emite un nuevo Certificado por una plazo máximo de tres años de vigencia. Las renovaciones se realizan por periodos consecutivos máximos de 3 años.
   - Si la organización no desea renovación, debe avisar al menos 4 meses antes de la caducidad.

6. Ejemplos de aplicación de la norma (1)

EMPRESAS CERTIFICADAS

- Buscar en los registros públicos de las entidades certificadoras (ej. AENOR)
- Buscar en Google: “UNE 166006”

KONIKER, una de las primeras empresas en certificarse en la norma UNE 166006

2019-01-30 Inteligencia Competitiva

En este año 2018 y después de más de un año de trabajo, la nueva norma 166006:2018 ha visto la luz y el sistema de Vigilancia e Inteligencia de KONIKER se ha certificado bajo la nueva revisión de norma de AENOR.

26

6. Ejemplos de aplicación de la norma (2)

EJEMPLOS DE APLICACIÓN

- Universidad Pontificia Bolivariana (Colombia)
- Universidad Politécnica de Valencia (TFG)
- Centro Tecnológico de Automoción (España)
- Observatorio de Tecnologías Nucleares (Chile)
- Industria alimentaria (España)
- Observatorio Tecnológico para la Atención Ciudadana (Cuba)
- Industrias biotecnológicas y farmacéuticas (Cuba)

7. Conclusiones

- La norma 166006:2018 es un buen marco de referencia para las organizaciones que quieren hacer vigilancia e inteligencia tecnológica
- Las organizaciones pueden adaptarla a sus propias necesidades porque no es de obligado cumplimiento, excepto si se quiere obtener la certificación

Preguntas de autoevaluación (1)

1. La norma UNE 166006:2018 permite la ___ del sistema de vigilancia e inteligencia y, por tanto, demostrar ante ___ que se dispone de los recursos necesarios para realizar la vigilancia e inteligencia tecnológica dentro de la empresa o para otras empresas. ¿Qué palabras faltan, en el orden indicado?

   a) certificación, la gerencia
   b) certificación, terceros
   c) implantación, la gerencia
   d) implantación, terceros

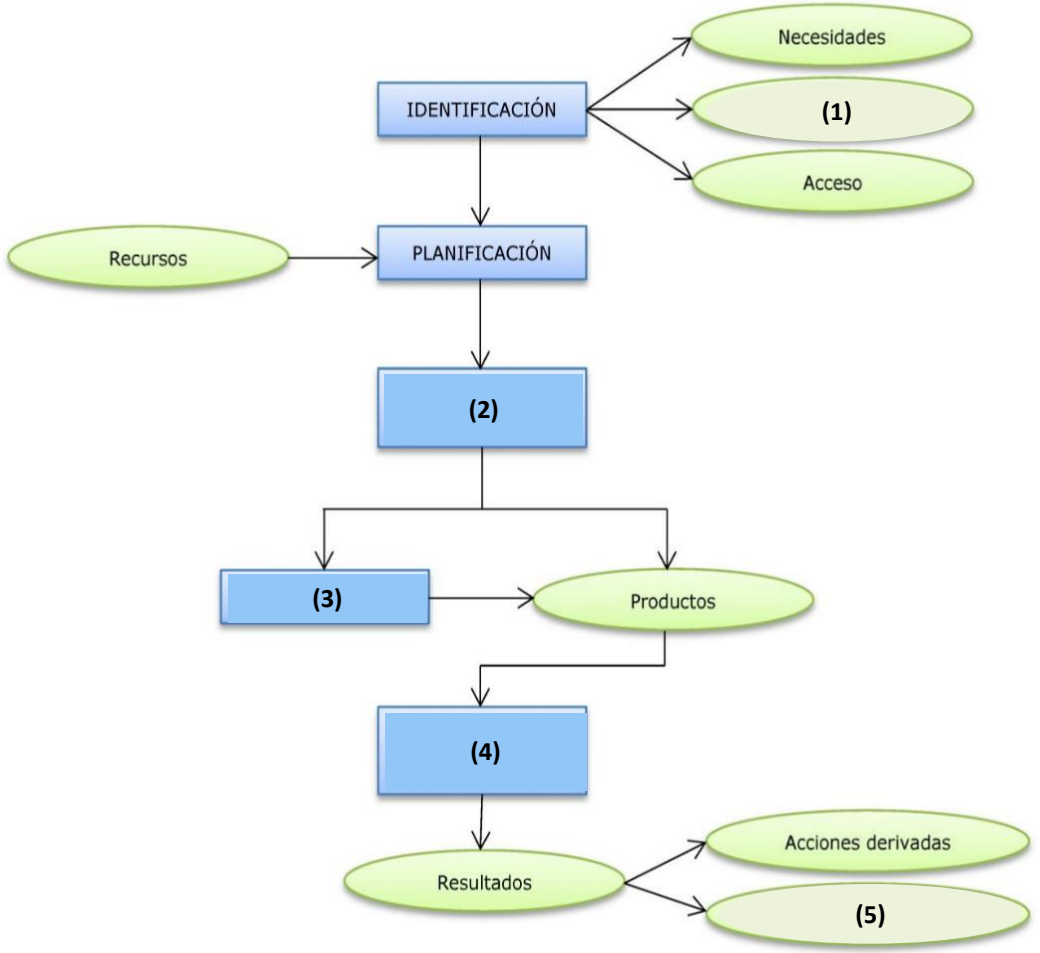
Preguntas de autoevaluación (2)

2. Según las definiciones de términos de la norma UNE 166006:2018, un aspecto de la actividad de una organización en el que se presenta posibilidad de oportunidades es:
   a) Un sistema de vigilancia e inteligencia
   b) Un entorno de interés
   c) Un ecosistema de inteligencia
   d) Una acción derivada

Preguntas de autoevaluación (3)

3. En la figura, que representa el proceso de Vigilancia e Inteligencia definido en la norma UNE 166006:2018, ¿qué texto falta en la caja indicada como (2)?

   a) Búsqueda y tratamiento
   b) Análisis de datos
   c) Distribución y almacenamiento
   d) Inteligencia competitiva



Preguntas de autoevaluación (4)

- Un listado de titulares de noticias obtenido en la etapa de distribución y almacenamiento en un sistema de vigilancia e inteligencia aplicando la norma UNE 166006:2018 es un producto que incluye un:
  a) Nivel bajo de análisis
  b) Nivel medio de análisis
  c) Nivel alto de análisis
  d) Nivel adecuado de análisis

Preguntas de autoevaluación (5)

- ¿Cuál de los siguientes no es una de las categorías (o roles) de participantes que propone la norma UNE 166006:2018 para un sistema de vigilancia e inteligencia?
  a) Dinamizador
  b) Analista
  c) Desarrollador
  d) Consumidor

Preguntas de autoevaluación (6)

4. ¿Durante cuanto tiempo es válido el certificado de cumplimiento de la norma UNE 166006:2018 por una organización?

   a) 1 año
   b) 2 años
   c) 3 años
   d) 4 años

Ejercicio propuesto

1. Localizar en la norma UNE 166006:2018 la información documentada que exige que quede registrada como evidencia de aplicación de la norma, y rellenar esta tabla:

Información documentada	Apartado de la norma

Ejercicio propuesto
Ejemplo

Información documentada	Apartado de la norma
La organización debe determinar los límites y la aplicabilidad del sistema de gestión de vigilancia e inteligencia para establecer su alcance. El alcance debe estar disponible como información documentada.	4.3 Determinación del alcance del sistema de gestión de vigilancia e inteligencia