Norma Española

UNE 166006

Abril 2018

Gestión de la I+D+i: Sistema de vigilancia e inteligencia

Esta norma ha sido elaborada por el comité técnico CTN 166 *Actividades de investigación, desarrollo tecnológico e innovación (I+D+i)*, cuya secretaría desempeña UNE.

Asociación Española
de Normalización
Génova, 6 - 28004 Madrid
915 294 900
info@une.org
www.une.org

UNE 166006

Gestión de la I+D+i: Sistema de vigilancia e inteligencia

R&D&i management: Monitoring and intelligence system.

Gestion de la R+D+i: Système de la veille et de l'intelligence.

Esta norma anula y sustituye a la Norma UNE 166006:2011.

Las observaciones a este documento han de dirigirse a:

Asociación Española de Normalización
Génova, 6
28004 MADRID-España
Tel.: 915 294 900
info@une.org
www.une.org
Depósito legal: M 12225:2018

Índice

Se llama la atención sobre la posibilidad de que algunos elementos de este documento puedan ser objeto de derechos de patente. UNE no es responsable de la identificación de dichos derechos de patente.

0 Introducción

Esta norma constituye una revisión de la Norma UNE 166006:2011 'Sistema de vigilancia tecnológica e inteligencia competitiva'. En esta revisión se ha profundizado en algunos contenidos, se han simplificado los requisitos y se han añadido aspectos nuevos, como por ejemplo la vigilancia e inteligencia en red. El título se ha generalizado a 'Sistema de vigilancia e inteligencia', sin que este hecho suponga un cambio de orientación en la norma. Simplemente da cuenta de que en la toma de decisiones en las organizaciones cada vez influyen más elementos no meramente tecnológicos que es necesario conocer, y que el concepto de inteligencia se enfoca a mejorar la competitividad, pero también está relacionada con otros aspectos ("inteligencia estratégica", "inteligencia de negocio", etc.), que básicamente no influyen en cómo ha de gestionarse el proceso, lo cual constituye el objetivo principal de esta norma.

En la Norma UNE 166002 se hace referencia a la vigilancia e inteligencia como herramientas fundamentales en el marco del sistema de gestión de la I+D+i. Por una parte, mejoran el acceso y gestión de los conocimientos científicos y técnicos, así como sobre legislación, normativa, economía, mercado, sociedad, etc. Por otra parte, permiten comprender a tiempo del significado e implicaciones de los cambios y novedades en el entorno. Ambos hechos las convierten en indispensables para la toma de decisiones, tanto en el ámbito estratégico (por ejemplo para ajustar el rumbo y marcar posibles caminos de evolución de interés para la organización), como en el ámbito operativo (por ejemplo para el desarrollo de un nuevo producto, servicio o proceso).

Actualmente en la literatura y en el mercado conviven diferentes versiones de sistemas de vigilancia e inteligencia, que comparten el núcleo del proceso y que ponen el acento en distintos puntos del mismo, por ejemplo:

Proceso de Vigilancia	**Proceso de Inteligencia**
Más centrado en captar información	Más centrado en analizar la información
Más centrado en explotar fuentes	Más centrado en recomendar acciones
Carácter más operativo	Carácter más estratégico
Aportación de valor más baja	Aportación de valor más alta
Más énfasis en la difusión rápida	Más énfasis en la comunicación efectiva
Más centrado en generar alertas	Más centrado en generar informes

En esta versión de la norma se considera el proceso de "vigilancia e inteligencia" como suma de los dos, sin marcar sus diferencias sino reforzando este enfoque basado en procesos (el proceso, su gestión y su impacto en la gestión de la innovación) tanto de carácter operativo como estratégico.

Este proceso, basado en información, tiene lógicamente cierta relación con la gestión de conocimiento. Sin embargo, esta última, como se explica por ejemplo en el Informe UNE 412001:2008 IN, es un concepto más general, que abarca la captura, identificación, generación, preservación y uso de información, pero también del *know-how* explícito o implícito de la organización, las competencias del personal, los activos intangibles, etc., con fines más amplios y variados.

Esta norma está alineada con la estructura de otros sistemas de gestión, como puede ser el de la Norma UNE-EN ISO 9001, con la finalidad de asegurar la compatibilidad con dichos sistemas y facilitar su implantación, en beneficio de la comunidad de usuarios.

En concreto, esta norma tiene una relación especial con la Norma UNE 166002 "Requisitos del sistema de gestión de la I+D+i". El apartado 7.9 de dicha norma especifica que "*el sistema de gestión de la I+D+i debe incluir un proceso de vigilancia tecnológica e inteligencia competitiva*". La presente norma proporciona información para establecer dicho proceso y, más allá, establecer un sistema propio para gestionar estas actividades de forma continua y efectiva. La Norma UNE 166002 también hace referencia al papel de la vigilancia e inteligencia para comprender el contexto de la organización (UNE 166002, capítulo 4), para generar ideas para nuevos proyectos de I+D+i (UNE 166002, 8.2) o para la revisión por la dirección del sistema de gestión de I+D+i (UNE 166002, 9.3). Además, incluye la vigilancia e inteligencia como actividades de soporte para el desarrollo de los proyectos concretos de I+D+i (UNE 166002, 8.3).

Esta norma contiene requisitos para la implantación y funcionamiento de un sistema de gestión de vigilancia e inteligencia (expresados en la forma "la organización *debe*…"), pero también información adicional y ejemplos para facilitar a las organizaciones la comprensión y aplicación de dichos requisitos. Estos ejemplos no deben entenderse en ningún caso como listas cerradas ni obligatorias. Cada organización tiene unas características distintas que serán las que den la forma concreta a su sistema de vigilancia e inteligencia.

1 Objeto y campo de aplicación

Esta norma tiene por objeto facilitar la formalización y estructuración del proceso de recogida, análisis y comunicación de información sobre el entorno de la organización, para apoyar la toma de decisiones a todos los niveles. Para ello propone la implantación de un sistema de gestión permanente de vigilancia e inteligencia, especialmente enfocadas a las actividades de I+D+i de la organización.

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.

2 Normas para consulta

Los documentos indicados a continuación, en su totalidad o en parte, son normas para consulta indispensables para la aplicación de este documento. Para las referencias con fecha, solo se aplica la edición citada. Para las referencias sin fecha se aplica la última edición (incluida cualquier modificación de esta).

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

3 Términos y definiciones

Para los fines de este documento, se aplican los términos y definiciones incluidos en la Norma UNE 166000:2006 además de los siguientes:

3.1 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.

3.2 dato:
Hecho discreto y objetivo sin contexto ni interpretación.

3.3 información:
Conjunto de datos estructurados con significado para el sujeto, en un momento concreto, y analizados en un contexto determinado.

3.4 entorno de interés:
Aspecto de la actividad de la organización en el que se presenta posibilidad de oportunidades.

3.5 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.

3.6 vigilancia e inteligencia en red:
Proceso de vigilancia e inteligencia compartida que se establece gracias a la interactuación de diferentes nodos pertenecientes a organizaciones distintas.

4 Contexto de la organización

4.1 Comprensión de la organización y de su contexto

La organización debe determinar las cuestiones externas e internas que son pertinentes para su propósito y que afectan a su capacidad para lograr los resultados previstos de su sistema de gestión de vigilancia e inteligencia.

Entre las cuestiones externas se pueden considerar, por ejemplo:

- prácticas, técnicas y tecnologías habituales y novedosas en vigilancia e inteligencia;
- posibles proveedores de este tipo de servicios;
- posibles colaboradores o socios;
- instituciones públicas o privadas que proporcionan información relevante para el sector;
- uso intensivo de datos (datos masivos –*big data*– provenientes de sensores, plataformas, etc.);
- actividades de los competidores en vigilancia e inteligencia, etc.

En cuanto a las cuestiones internas, se pueden considerar por ejemplo:

- la organización interna y los flujos de información definidos;

- las capacidades disponibles y necesarias;

- las actividades previas desarrolladas en este ámbito;

- la relación e interacción con otros sistemas de gestión de la organización (especialmente si se ha implantado un sistema de gestión de la I+D+i según la Norma UNE 166002), etc.

4.2 Comprensión de las necesidades y expectativas de las partes interesadas

La organización debe determinar:

- las partes interesadas que son pertinentes al sistema de gestión de vigilancia e inteligencia;

- los requisitos pertinentes de estas partes interesadas.

Las partes interesadas se dividen en aquellas externas a la organización (por ejemplo, socios, proveedores, distribuidores, organizaciones de investigación colaboradoras, clientes y usuarios, autoridades públicas, etc.) y aquellas internas a la misma (por ejemplo, empleados, dirección, departamentos, accionistas, etc.).

Las necesidades de estas partes interesadas en relación al sistema de gestión de vigilancia e inteligencia pueden referirse, por ejemplo, a rapidez en el tratamiento, pertinencia y utilidad de la información para la toma de decisiones, requisitos de confidencialidad, etc. Es importante consultar e implicar a las partes interesadas para poder identificar sus necesidades y expectativas, que pueden ser explícitas o implícitas.

NOTA Estas necesidades y expectativas en relación al sistema de gestión en su conjunto, son un concepto claramente diferente de las "necesidades de información" específicas que se identifican en el proceso de realización de cada acción de vigilancia e inteligencia (véase 8.3.1), y que están referidas a temáticas, palabras clave, objetivos de análisis, etc., con un objetivo concreto.

4.3 Determinación del alcance del sistema de gestión de vigilancia e inteligencia

La organización debe determinar los límites y la aplicabilidad del sistema de gestión de vigilancia e inteligencia para establecer su alcance.

Cuando se determina este alcance, la organización debe considerar:

- las cuestiones externas e internas indicadas en 4.1;

- los requisitos indicados en 4.2.

El alcance debe estar disponible como información documentada.

4.4 Sistema de gestión de vigilancia e inteligencia

La organización debe establecer, implementar, mantener y mejorar continuamente un sistema de gestión de vigilancia e inteligencia, incluidos los procesos necesarios y sus interacciones, de acuerdo con los requisitos de esta norma.

Se debe establecer un mapa de procesos que permita visualizar los principales elementos del sistema de vigilancia e inteligencia y las interrelaciones entre diferentes áreas de la organización. Se deben indicar también los recursos necesarios para cada área, la secuencia e interacción de las actividades y los indicadores para el adecuado seguimiento, medición y análisis del proceso.

En los casos en que la organización opte por contratar externamente cualquier actividad de vigilancia e inteligencia, la organización debe asegurarse de controlar tales actividades (véase también 7.10.3).

5 Liderazgo

5.1 Liderazgo y compromisos

La alta dirección debe demostrar liderazgo y compromiso con respecto al sistema de gestión de vigilancia e inteligencia:

- asegurándose de que se establezcan la política y los objetivos de vigilancia e inteligencia y que éstos sean compatibles con la dirección estratégica de la organización;
- asegurándose de la integración de los requisitos del sistema de gestión de vigilancia e inteligencia en los procesos de negocio de la organización;
- asegurándose de que los recursos necesarios para el sistema de gestión de vigilancia e inteligencia estén disponibles;
- comunicando la importancia de una gestión de vigilancia e inteligencia eficaz y conforme con los requisitos del sistema de gestión;
- asegurándose de que el sistema de gestión de vigilancia e inteligencia logre los resultados previstos;
- dirigiendo y apoyando a las personas, para contribuir a la eficacia del sistema de gestión de vigilancia e inteligencia;
- promoviendo la mejora continua;
- apoyando otros roles pertinentes de la dirección, para demostrar su liderazgo aplicado a sus áreas de responsabilidad.

NOTA En esta norma se puede interpretar el término “negocio” en su sentido más amplio para referirse a aquellas actividades que son esenciales para la existencia de la organización.

5.2 Política

La alta dirección debe establecer una política de vigilancia e inteligencia que:

a) sea apropiada al propósito de la organización;

b) proporcione un marco de referencia para el establecimiento de los objetivos de vigilancia e inteligencia;

c) incluya el compromiso de cumplir los requisitos aplicables;

d) incluya el compromiso de mejora continua del sistema de gestión de vigilancia e inteligencia.

La política de vigilancia e inteligencia debe:

– estar disponible como información documentada;

– comunicarse dentro de la organización;

– estar disponible para las partes interesadas, según corresponda.

5.3 Roles, responsabilidades y autoridades en la organización

La alta dirección debe asegurarse de que las responsabilidades y autoridades para los roles pertinentes se asignen y comuniquen dentro de la organización.

La alta dirección debe asignar la responsabilidad y autoridad para:

– asegurarse de que el sistema de gestión de vigilancia e inteligencia es conforme con los requisitos de esta norma;

– informar a la alta dirección sobre el desempeño del sistema de gestión de vigilancia e inteligencia.

De cara a una correcta gestión de los recursos humanos que dan soporte al sistema de gestión de vigilancia e inteligencia, se proponen varios posibles roles. Estos roles están divididos por responsabilidades y tareas dentro del proceso de vigilancia e inteligencia.

a) 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.

b) 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.

c) 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.

d) 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.).

e) 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.

Dependiendo del tamaño de la organización, del número de personas involucradas, del tipo de información manejada o por otras razones, una misma persona puede cumplir uno o varios roles.

6 Planificación

6.1 Acciones para abordar riesgos y oportunidades

Al planificar el sistema de gestión de vigilancia e inteligencia, la organización debe considerar las cuestiones referidas en el apartado 4.1 y los requisitos referidos en el apartado 4.2, y determinar los riesgos y oportunidades que es necesario abordar con el fin de:

– asegurar que el sistema de gestión de vigilancia e inteligencia pueda lograr sus resultados previstos;

– prevenir o reducir efectos no deseados;

– lograr la mejora continua.

La organización debe planificar:

a) las acciones para abordar estos riesgos y oportunidades;

b) la manera de:

  – integrar e implementar las acciones en sus procesos del sistema de gestión de vigilancia e inteligencia,

  – evaluar la eficacia de estas acciones.

6.2 Objetivos de vigilancia e inteligencia y planificación para lograrlos

La organización debe establecer objetivos de vigilancia e inteligencia para las funciones y niveles pertinentes.

Los objetivos de vigilancia e inteligencia deben:

a) ser coherentes con la política de vigilancia e inteligencia;

b) ser medibles y verificables;

c) tener en cuenta los requisitos aplicables;

d) ser objeto de seguimiento;

e) comunicarse;

f) actualizarse, según corresponda.

La organización debe conservar información documentada sobre los objetivos de vigilancia e inteligencia.

Al planificar cómo lograr sus objetivos de vigilancia e inteligencia, la organización debe determinar:

– qué se va a hacer;

- qué recursos se requerirán;
- quién será responsable;
- cuándo se finalizará;
- cómo se evaluarán los resultados.

7 Apoyo

7.1 Recursos

La organización debe determinar y proporcionar los recursos necesarios (humanos, infraestructura, financieros, tecnológicos, permisos o licencias, etc.) para el establecimiento, implementación, mantenimiento y mejora continua del sistema de gestión de vigilancia e inteligencia.

7.2 Competencia

La organización debe:

- determinar la competencia necesaria de las personas que realizan, bajo su control, un trabajo que afecta al sistema de vigilancia e inteligencia;
- asegurarse de que estas personas sean competentes, basándose en la educación, formación o experiencia apropiadas;
- cuando sea aplicable, tomar acciones para adquirir la competencia necesaria y evaluar la eficacia de las acciones tomadas;
- conservar la información documentada apropiada, como evidencia de la competencia.

NOTA 1 De acuerdo con los ejemplos de roles propuestos en el apartado 5.3, y teniendo en cuenta sus responsabilidades y tareas, ejemplos de las competencias necesarias pueden ser:

a) Coordinador o dinamizador:
   - Liderazgo.
   - Capacidad de organización del trabajo.
   - Capacidad de trabajo en equipo.
   - Capacidad de comunicación.
   - Iniciativa y proactividad.

b) Gestor de fuentes o documentalista:
   - Manejo y explotación de bases de datos especializadas.
   - Herramientas y recursos para la búsqueda de información disponibles en internet.
   - Técnicas y herramientas específicas de recuperación, análisis y tratamiento de datos, tecnologías de la información.

- Minería de textos científico técnicos: Indicadores bibliométricos, índice de impacto, métrica de citaciones y otras medidas de impactos de las publicaciones.
- Sistemas de clasificación de tecnologías y áreas tecnológicas.
- Conocimiento sobre la información que aporta la propiedad industrial e intelectual, y sus mecanismos de funcionamiento.
- Conocimiento sobre herramientas de apoyo.

c) Analista o 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.

d) Administrador: aunque este rol es externo al sistema, en lo que a él respecta se pueden considerar:

- Perfil técnico en tecnologías de la información.
- Instalación y administración de las herramientas tecnológicas utilizadas en el sistema.

Dependiendo del tamaño de la organización, del número de personas involucradas, del tipo de información u otras razones, una misma persona puede cumplir uno o varios roles, necesitando sumar las competencias correspondientes.

NOTA 2 Las acciones para adquirir la competencia necesaria pueden incluir, por ejemplo, la formación, la tutoría o la reasignación de las personas empleadas actualmente, o la contratación de personas competentes.

NOTA 3 La formación para el personal que realiza vigilancia e inteligencia debería satisfacer las necesidades tanto de adaptación a la rápida evolución de los entornos tecnológicos y competitivos a vigilar como al rápido ritmo de aparición de herramientas para la realización de la vigilancia e inteligencia.

7.3 Toma de conciencia

Las personas que realizan trabajos relacionados con la vigilancia e inteligencia bajo el control de la organización deben tomar conciencia de:

- la política de vigilancia e inteligencia;
- su contribución a la eficacia del sistema de gestión, incluidos los beneficios de una mejora del desempeño de la vigilancia e inteligencia;
- las implicaciones de no cumplir los requisitos del sistema de gestión de vigilancia e inteligencia.

7.4 Comunicación

La organización debe determinar las comunicaciones internas y externas pertinentes al sistema de gestión de vigilancia e inteligencia, que incluyan:

- qué comunicar;

– cuándo comunicar;

– a quién comunicar;

– cómo comunicar.

7.5 Información documentada

7.5.1 Generalidades

El sistema de gestión de vigilancia e inteligencia de la organización debe incluir:

a) la información documentada requerida por esta norma;

b) la información documentada que la organización determina como necesaria para la eficacia del sistema de gestión de vigilancia e inteligencia.

NOTA La extensión de la información documentada para un sistema de gestión de vigilancia e inteligencia puede variar de una organización a otra, debido a:

- el tamaño de la organización y su tipo de actividades, procesos, productos o servicios;
- la complejidad de los procesos y sus interacciones;
- la competencia de las personas.

7.5.2 Creación y actualización

Al crear y actualizar la información documentada, la organización debe asegurarse de que lo siguiente sea apropiado:

– la identificación y descripción (por ejemplo, título, fecha, autor o número de referencia);

– el formato (por ejemplo, idioma, versión del software, gráficos) y los medios de soporte (por ejemplo, papel, electrónico);

– la revisión y aprobación con respecto a la idoneidad y adecuación.

7.5.3 Control de la información documentada

La información documentada requerida por el sistema de gestión de vigilancia e inteligencia y por esta norma se debe controlar para asegurarse de que:

a) esté disponible y sea idónea para su uso, dónde y cuándo se necesite;

b) esté protegida adecuadamente (por ejemplo, contra pérdida de la confidencialidad, uso inadecuado, o pérdida de integridad).

Para el control de la información documentada, la organización debe abordar las siguientes actividades, según corresponda:

– distribución, acceso, recuperación y uso;

– almacenamiento y preservación, incluida la preservación de la legibilidad;

– control de cambios (por ejemplo, control de versión);

– conservación y disposición final.

La información documentada de origen externo que la organización determina como necesaria para la planificación y operación del sistema de gestión de vigilancia e inteligencia se debe identificar y controlar, según sea apropiado.

NOTA El acceso puede implicar una decisión en relación al permiso solamente para consultar la información documentada, o al permiso y a la autoridad para consultar y modificar la información documentada.

7.6 Confidencialidad, legalidad y aspectos éticos

Por la naturaleza de las actividades de vigilancia e inteligencia es importante considerar los aspectos de confidencialidad, legalidad y éticos desde la petición de información hasta la custodia de la información generada durante la realización de la vigilancia e inteligencia.

Se debe asegurar que se cumplen todos los aspectos legales y éticos aplicables.

Cuando proceda, se debe mantener la confidencialidad mediante el tratamiento adecuado de la información confidencial, la inclusión de cláusulas de confidencialidad con los trabajadores y la firma de compromisos de confidencialidad con los clientes y con los proveedores (véase también 7.5.3).

En el caso de proveedores externos de vigilancia e inteligencia, véase también 7.10.1.

7.7 Entornos de vigilancia e inteligencia en red

La globalización y digitalización de la economía favorecen cada vez más que las organizaciones planteen su sistema de innovación en un escenario en red, con distintos grados de intensidad en su apertura e interacción con el entorno. Así se generan diseños de sistemas de vigilancia e inteligencia en red, que pueden ser clasificados atendiendo a dos dimensiones: actuación en el escenario y modelo de gobernanza en red.

a) La actuación en el escenario, como dimensión externa, determina la relación del sistema de gestión de vigilancia e inteligencia con su entorno y su operatividad. Los sistemas pueden evolucionar desde sistemas aislados a sistemas íntegramente colaborativos, donde el proceso de vigilancia e inteligencia se gestiona en red (ver tabla 1).

Tabla 1 – Ejemplos de escenarios de vigilancia e inteligencia

Actuación	Escenario	Motivación	Estilo	Actores (ejemplos)
Sistemas aislados	Competitivo *Confidencial*	Maximización del beneficio individual.	Autónomo e integral.	Empresas comerciales.
	No competitivo *Público*	Proporcionar información abierta. Bien general.	Autónomo e integral.	Organismos públicos.
Sistemas en Red	Cooperativo-Competitivo (Coopetitivo) *Privado*	Reto específico. Beneficio de las partes implicadas en el consorcio.	Mixto, en función de las circunstancias o proyecto específico.	Consorcios de I+D+i. Asociaciones. Clústers.
	Colaborativo *Abierto y Público*	Bien común. Liderazgo. Excelencia. Reputación. Reconocimiento social. Altruismo.	Colaborativo y basado en el intercambio de experiencias y aprendizajes.	Universidades. Redes internacionales. Desarrollo regional. Instituciones públicas. Observatorios. Comunidades de práctica. Foros en Internet. Redes sociales.

b) El modelo de gobernanza, como dimensión interna, puede estar liderado por la organización o por un consorcio y determina el funcionamiento interno del sistema de vigilancia e inteligencia en red, que puede variar entre:

   - Centralizado: un nodo central articula la interacción entre el resto de nodos, controlando los flujos de información y trabajo.

   - Descentralizado: un grupo de nodos centrales articulan la interacción entre los demás, generando grupos y coordinando flujos.

   - Distribuido: todos los nodos interaccionan entre sí sin la existencia de un control central.

La operativa del sistema de gestión de vigilancia e inteligencia en red debe cumplir las especificaciones de esta norma. Adicionalmente, los responsables del sistema de gestión en red deben acordar los aspectos básicos de su interacción, como por ejemplo los siguientes:

- Organigrama del consorcio.

- Definición y alcance de la colaboración.

- Roles y responsabilidades de los participantes.

- Reglas de colaboración e interrelación.

- Productos o servicios generados.

- Reglas sobre la explotación y protección de estos productos.

- Tecnologías comunes usadas y/o especificaciones usadas para el intercambio de distintas informaciones.

NOTA Es una buena práctica el uso de especificaciones abiertas para el intercambio de información entre plataformas de vigilancia e inteligencia, automatizando las interacciones. Por ejemplo, [1]. En este caso se deberían definir las estructuras de datos (metadatos) que permitirán a estas plataformas interpretar correctamente las reglas de colaboración e interrelación.

7.8 Prospectiva y previsión

Según la OCDE, la **prospectiva** es un proceso sistemático que se ocupa de valorar las tendencias de futuro (concentrándose en el largo plazo), de la ciencia, la tecnología, la economía y la sociedad, con el propósito de identificar las áreas de investigación estratégicas y tecnologías genéricas emergentes que proporcionen mayores beneficios económicos y sociales. Desarrolla visiones de futuro analizando distintas posibilidades, dibujando escenarios alternativos basados en hipótesis plausibles sobre las tendencias de desarrollo y la evolución de variables de contexto (sociales, medioambientales, geopolíticas…). Como resultado construye descripciones de futuro consistentes, útiles para la toma de decisiones y que permitan posicionarse de la manera más favorable.

Los estudios de prospectiva son, en general, largos, complejos, requieren de la participación de expertos en distintos campos y están fuera del alcance de la mayoría de las organizaciones a causa de:

- la complejidad de su diseño;
- el número de agentes involucrados en su desarrollo;
- los conocimientos específicos necesarios, que suelen involucrar metodologías distintas a las empleadas en las actividades habituales de las organizaciones.

Por este motivo, los estudios de prospectiva suelen ser desarrollados por organismos públicos especializados en la materia o por grandes empresas, y se dirigen habitualmente a los responsables de la toma de decisiones.

Por otro lado, la **previsión** sí está al alcance de todas las organizaciones y es fundamental para orientar su actividad de cara al futuro. Al igual que en los casos de la vigilancia e inteligencia y de la prospectiva, se trata de un proceso sistemático consistente, en este caso, en la recogida y análisis de datos e información (que pueden incluir informes de prospectiva externos) sobre los cuales se realiza un ejercicio de proyección a futuro con diferentes horizontes temporales, en función de las necesidades de la organización. Estos horizontes pueden ser, por ejemplo, la duración estimada de un proyecto en curso, el alcance del punto de retorno de la inversión en la introducción de un nuevo producto, proceso o servicio en el mercado, etc.

Los análisis de previsión (internos), y los estudios de prospectiva (normalmente externos), suelen utilizar como punto de partida la vigilancia e inteligencia, pero sirven también para identificar nuevas áreas que vigilar en el futuro. Por ello, es conveniente tenerlos en cuenta como posible fuente de información en un sistema de vigilancia e inteligencia. En un futuro cercano, las aplicaciones dotadas de inteligencia cognitiva están, asimismo, llamadas a jugar un papel importante en la toma de decisiones.

7.9 Visualización

La visualización de información es un proceso interactivo de representar información dando sentido a grandes volúmenes de datos complejos, difíciles de entender de otras maneras. Las visualizaciones permiten resumir la información, centrándose en lo importante sin perder los detalles, manteniendo la información que en meros análisis estadísticos podría pasar desapercibida. Por tanto, facilitan la detección de tendencias, anomalías, agrupaciones y colaboraciones, etc., siempre relevantes en cualquier estudio de vigilancia e inteligencia.

Pero no cualquier visualización es válida para cualquier tipo de información, entorno, o caso de uso. Hay que tener en cuenta al destinatario del análisis, el medio en el que va a ser consumido, el tipo de dato y el objetivo de la tarea, antes de seleccionar la visualización más idónea a cada caso.

Lo primero que se debe determinar es qué es lo que se quiere mostrar, cual es el objetivo de la visualización, y aprovechar la semántica propia de los datos para tratar de representarlos del modo más idóneo posible, para que no haya información superflua, redundante o contradictoria, destacando la información objetivo de un modo sencillo y claro, sin perder el resto de información adicional.

La visualización consta de una visión principal, visiones auxiliares, y propiedades de interacción, que proporcionan distintas visiones sobre los mismos datos en función de los ejes, codificaciones y agrupaciones o segmentaciones que se utilicen.

Las visualizaciones están condicionadas por la tipología de los datos, por ejemplo:

- Datos geográficos/cartográficos/espaciales.
- Datos jerárquicos.
- Datos relacionales/correlaciones/redes.
- Datos secuenciales o de proceso.
- Series temporales.

Las visualizaciones adquieren mayores capacidades si, sobre estos conjuntos de datos, se identifican características claves de las visualizaciones:

- Capacidad de navegación (ir de lo general al detalle, por ejemplo, en gráficos jerárquicos).
- Opciones de filtrado y segmentación de los datos.
- Orden de datos (alfabéticamente, cuantitativamente…).
- Interactividad, pudiendo simular la evolución de los datos a lo largo del tiempo.
- Selección, mostrando atributos extra.
- Relacionando dos visualizaciones entre si y generando interactividad mutua.

En la aplicación de la vigilancia e inteligencia, la visualización de información es una herramienta de soporte a tener en cuenta en la fase de tratamiento y análisis o puesta en valor (véanse 8.5 y 8.6), y en la elaboración de productos de vigilancia e inteligencia (véase 8.8). Puede ser externalizada a especialistas en diseño gráfico, infografía, etc., por ejemplo para la elaboración de informes finales.

7.10 Externalización

7.10.1 Generalidades

En la medida en que cada organización lo considere conveniente, puede externalizar parte del proceso de la vigilancia e inteligencia (capítulo 8) a proveedores de estos servicios, asegurándose de que el servicio contratado cumple lo especificado en esta norma.

Toda información proporcionada por el cliente al proveedor del servicio debe considerarse confidencial y utilizarse solamente en este contexto, salvo que se acuerde lo contrario. No debe proporcionarse a terceros sin la autorización del cliente.

Conviene facilitar la labor de identificación de las informaciones de interés, de modo que el proveedor sea más eficaz en las tareas de búsqueda.

7.10.2 Información para la externalización

La organización solicitante debe especificar las necesidades objeto de la externalización al proveedor del servicio, que deben incluir al menos:

- Las partes del proceso a cubrir con la prestación.
- Los contenidos mínimos y extensión que deben tener los campos o temas a vigilar.
- La identificación de fuentes y tipos de información conocidos, si se dispone de ellos.
- La cobertura geográfica y temporal, y la periodicidad de seguimiento prevista.
- El soporte/formato de los resultados y nivel de análisis de la información.

La organización proveedora del servicio debe especificar en su oferta al menos la siguiente información:

- Las competencias del personal encargado de realizar el servicio (formación, años de experiencia, etc.).
- Los medios materiales que le permiten realizar la oferta (hardware, software, permisos, licencias, fuentes de información, etc.).
- Las condiciones de confidencialidad, salvaguarda y exclusividad de la información recibida.
- Las referencias y acreditaciones que pueda aportar el proveedor.
- La oferta económica y el plazo de validez de la oferta.

7.10.3 Control del servicio externalizado

La organización debe establecer e implantar la inspección u otras actividades necesarias para asegurarse de que el proveedor cumple los requisitos especificados en el acuerdo y en esta norma.

El control del proceso externalizado debe estar documentado dentro del sistema de gestión de vigilancia e inteligencia.

8 Operación

8.1 Planificación y control operacional

La organización debe planificar, implementar y controlar los procesos necesarios para cumplir los requisitos y para implementar las acciones determinadas en el apartado 6.1 mediante:

- el establecimiento de criterios para los procesos;
- la implementación del control de los procesos de acuerdo con los criterios;
- el almacenaje de información documentada en la medida necesaria para confiar en que los procesos se han llevado a cabo según lo planificado.

La organización debe controlar los cambios planificados y revisar las consecuencias de los cambios no previstos, tomando acciones para mitigar cualquier efecto adverso, según sea necesario.

La organización debe asegurarse de que los procesos contratados externamente estén controlados (véase 7.10.3).

8.2 Proceso de la vigilancia e inteligencia

La figura 1 resume el proceso genérico de realización de la vigilancia e inteligencia, mostrando el flujo de información, las etapas básicas que componen el proceso y los principales resultados obtenidos.

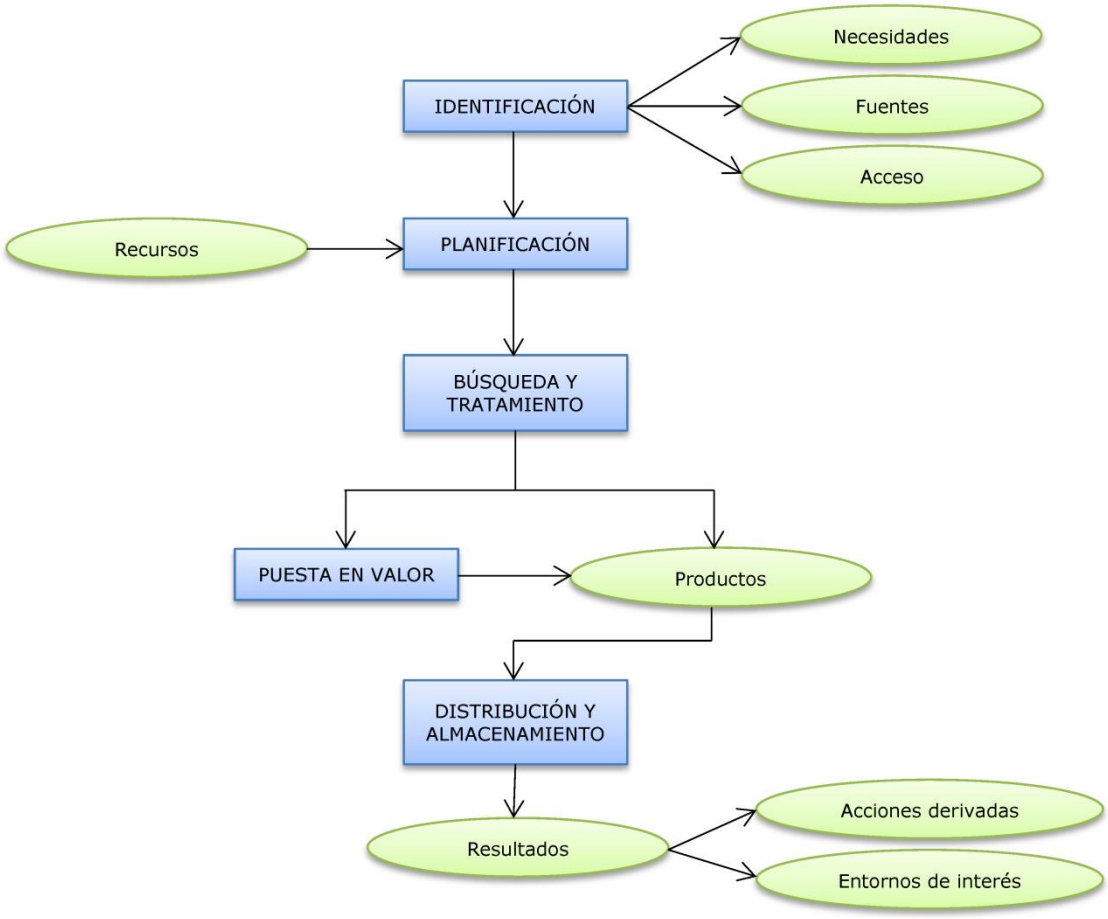

Figura 1 – Proceso de realización de la vigilancia e inteligencia

8.3 Identificación de necesidades, fuentes de información y medios de acceso

8.3.1 Identificación de necesidades de información

La identificación de necesidades de información puede realizarse partiendo de uno o varios factores, como por ejemplo:

- el análisis, la evolución o nuevas aplicaciones de los productos, procesos, materiales y tecnologías base de la organización;
- las demandas esperadas o manifestadas por las partes interesadas internas o externas;
- la evolución socioeconómica, legislativa o normativa;
- proyectos o actuaciones de la competencia.

La organización debe definir un proceso documentado para la identificación de necesidades de información, que incluya, al menos, los siguientes aspectos:

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., que serán empleados en la elaboración del informe.

d) Información sobre el tipo de producto que se entregará y sus contenidos.

8.3.2 Identificación de fuentes internas y externas de información

Tomando como base las principales necesidades de información, se deben identificar primeramente las fuentes de información y recursos disponibles en la organización, junto con aquellas que pueden ser accesibles, tales como por ejemplo:

a) Documentación propia o relacionada con la organización (carpetas locales, compartidas, repositorios documentales, bases de datos, intranet, etc.).

b) Personas con conocimientos o experiencias relacionadas con las necesidades de información.

c) Contactos externos de potencial interés.

d) Organizaciones como centros públicos de investigación, universidades, centros tecnológicos, ingenierías o asesorías.

e) Fuentes documentales a las que tiene acceso la organización: en soporte físico (revistas, catálogos, etc.), en soporte electrónico (bases de datos, *big data*, etc.), recursos de información en Internet (portales temáticos, noticias, redes sociales, foros, chat/IRC, etc.) o en formato multimedia (audio, vídeo, imágenes).

f) Documentación técnica como reglamentaciones, especificaciones, propiedad industrial e intelectual o normas.

g) Congresos, seminarios, ferias o exposiciones.

h) Resultados de análisis existentes sobre las tendencias de futuro, como estudios de prospectiva externos, o ejercicios de previsión internos (elaboración de escenarios, modelos econométricos, hojas de ruta, etc., véase 7.8).

La identificación de las fuentes de información externas debe estar basada en criterios de calidad, pertinencia, objetividad y fiabilidad de las mismas, como por ejemplo su origen “oficial”, su frecuencia de actualización, la citación de autores, el grado de distribución por países de las publicaciones y de los autores de los artículos (en publicaciones científicas se puede utilizar el "factor de impacto" basado en el número de citaciones), etc.

8.4 Planificación de la realización de la vigilancia e inteligencia

Normalmente, la vigilancia e inteligencia tienen en cuenta dos enfoques de trabajo posibles y complementarios en muchas ocasiones:

a) la búsqueda e investigación de nuevas áreas desconocidas; y

b) el seguimiento sistemático de novedades en áreas que ya están previamente identificadas.

En función de las necesidades de información detectadas para nuevas áreas, las fuentes de información y medios de acceso a las mismas, se deben planificar y dimensionar los recursos y plazos según datos de la experiencia y de acciones previsibles.

Ya que la vigilancia e inteligencia 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.

8.5 Búsqueda y tratamiento de la información

8.5.1 Búsqueda

La búsqueda y selección de información se debe realizar estableciendo una estrategia y acciones de búsqueda en las fuentes seleccionadas.

Las estrategias de búsqueda utilizadas podrán ser muy útiles en las fases posteriores de tratamiento y puesta en valor. Por ello, puede ser conveniente incluir, especialmente en aquellos casos en los que intervengan expertos externos, la estrategia seguida en la búsqueda, como por ejemplo los descriptores, terminología, palabras clave, operadores utilizados, la segmentación geográfica o temporal utilizada, etc.

Tras la **recopilación** de datos, se debe discriminar y **validar** cuáles de ellos contribuyen a satisfacer los requisitos de información formulados, en términos de fiabilidad de las fuentes, validez, oportunidad, pertinencia, relevancia y utilidad.

8.5.2 Tratamiento

El tratamiento de la información varía sustancialmente en función de la calidad de las fuentes de información. Normalmente requiere una primera **preparación** de los datos, consistente en una limpieza y normalización de los mismos, como por ejemplo conversión de monedas, formato de fecha y hora, corrección de datos postales, clasificación de actividades económicas, etc.

Si se trata con un volumen reducido de datos o la información manejada es simple, el tratamiento puede ser manual. El resultado de este análisis manual puede plasmarse directamente en productos de la vigilancia e inteligencia de nivel de análisis bajo (véase 8.8).

Si el volumen es más elevado o la información más compleja, será necesario un tratamiento más avanzado. Una vez de realizada la preparación se procede al **tratamiento inicial** de la información (análisis exploratorio), normalmente diferenciado entre información estructurada (series de datos) y no estructurada (textos, imágenes, gráficos, etc.).

a) Tratamiento inicial de información estructurada: A partir de los datos obtenidos, se inicia el tratamiento con el objeto de descubrir posibles estructuras o correlaciones ocultas a simple vista, e identificar posibles rutas de análisis. En esta fase se suelen aplicar técnicas visuales de agrupación (*clustering*) y reducción de dimensionalidad, incluyendo por ejemplo:

   – distribución de variables,

   – diagramas de dispersión,

   – análisis de correlación,

   – análisis de probabilidad condicional,

   – análisis multivariante,

   – análisis geoposicional.

b) Tratamiento inicial de información no estructurada: El análisis de esta información puede basarse en técnicas tanto de análisis de imagen, como de NLP (procesamiento de lenguaje natural, siglas en inglés) que permitan extraer características de los contenidos para que puedan ser procesados posteriormente.

   – El tratamiento de los textos preprocesados puede incluir: detección de idioma, normalización de nombres y de textos procedentes de redes sociales, lematización, extracción y reconocimiento de entidades nombradas, extracción de términos multipalabra, extracción de palabras clave, etc.

   – Para el contenido gráfico, una vez aplicadas diversas técnicas de extracción de características y aplicando las técnicas analíticas pertinentes, se podrán identificar y reconocer caras, logotipos, eventos, objetos, imágenes semejantes, etc.

Posteriormente, con los resultados de estos análisis iniciales, se puede pasar a una fase de **análisis matemático o estadístico**, en el que la técnica a utilizar depende en gran medida del tipo de problema a resolver. Lo más habitual es encontrarse con problemas de clasificación o *clustering*, asociación, predicción y optimización. Cada uno de estos problemas cuenta con una variedad de técnicas para resolverlos, cuyo resultado depende de la naturaleza de los datos, su calidad y su cantidad. Las técnicas a aplicar incluyen, por ejemplo:

– inferencia estadística;

– modelos de regresión (incluyendo ANOVA o ANCOVA, análisis de residuos y variabilidad, suavizados de dispersión, etc.);

– *machine learning* (arboles de clasificación, clasificadores bayesianos, *random forest*, etc.);

Además del procesado mediante métodos establecidos o software específico, es importante el análisis humano que matice y valide la pertinencia de los resultados obtenidos.

La información en esta etapa puede ser directamente suficiente para la toma de algunos tipos de decisiones. En ese caso, se traduce en productos de la vigilancia e inteligencia de nivel de análisis medio (véase 8.8). En caso contrario, se debe poner en valor mediante un análisis más profundo.

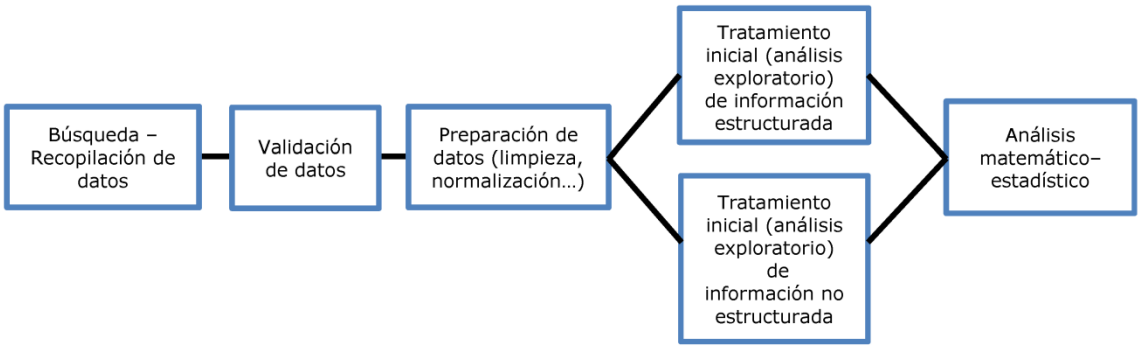

Figura 2 – Etapas habituales en la fase de búsqueda y tratamiento avanzado de la información

8.6 Puesta en valor de la información

En aquellos casos en los que el formato y contenidos de la información obtenida no satisfagan las necesidades planteadas y requieran una mayor profundidad de análisis, la información se debe poner en valor de cara a la toma de decisiones.

La puesta en valor es normalmente tarea de analistas expertos en política, economía, tecnología, etc., que posean tanto conocimientos técnicos como suficiente capacidad de análisis, imaginación y creatividad para relacionar la información con aspectos como identificación de oportunidades, reducción de riesgos, innovación, cooperación, adecuación a la estrategia de la organización, etc., véase el rol del analista en los apartados 5.3 y 7.2.

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.

– Representaciones gráficas, infografías, etc. que faciliten una comprensión rápida y sencilla (véase 7.9).

– Obtención del significado de los hechos analizados y de sus probables implicaciones y consecuencias para la organización.

– Recomendaciones de actuación, si bien es importante considerar que es el lector o consumidor el que acaba de dar valor al producto de vigilancia e inteligencia y es quien, en base a su conocimiento, instinto, experiencia, etc., decide las acciones a tomar (acciones derivadas, véase 8.9.2).

Este análisis profundo generará productos de vigilancia e inteligencia de nivel de análisis medio o alto (véase 8.8).

8.7 Distribución y almacenamiento

Los productos de la vigilancia e inteligencia (véase 8.8) se deben distribuir a las partes interesadas de la organización según sus necesidades.

La distribución y almacenamiento se debe apoyar en los circuitos de comunicación de la organización y puede ser completada con actuaciones de seguimiento y dinamización, con objeto de asegurarse que se da el tratamiento que la organización desea.

La información tratada debe almacenarse convenientemente según se haya definido para cada tipo de producto de vigilancia e inteligencia y ser recuperable y accesible para las posibles futuras actualizaciones que se requieran.

8.8 Productos de la vigilancia e inteligencia

Atendiendo a las particularidades de cada organización y a las necesidades de información identificadas, la organización debe determinar en qué soporte/formato se elabora y distribuye la información. Los diferentes soportes/formatos disponibles se pueden considerar como la cartera de productos de vigilancia e inteligencia que tenga la organización, como por ejemplo:

a) Productos que incluyen un nivel bajo de análisis: por ejemplo, listados de noticias validadas, etiquetadas, clasificadas o comentadas. Normalmente 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: por ejemplo informes, estados del arte o de la técnica, estudios bibliográficos, estudios de patentabilidad, etc.

c) Productos que incluyen un nivel profundo de análisis: por ejemplo, estudios exhaustivos, análisis de tendencias, etc.

Se debe definir y documentar, para cada tipo de producto de vigilancia e inteligencia, cómo se realiza:

– el control de las fuentes externas de información (véase 8.3);

– la búsqueda y el tratamiento de la información (véase 8.5);

– la puesta en valor de la información (véase 8.6);

– la distribución y almacenamiento de la información (véase 8.7).

8.9 Resultados de la vigilancia e inteligencia

8.9.1 Generalidades

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 es por lo general un intangible de difícil cuantificación inmediata que se puede clasificar según lo indicado a continuación.

8.9.2 Acciones derivadas de la vigilancia e inteligencia

Las acciones que se derivan de la vigilancia e inteligencia pueden estar condicionadas por factores exteriores al sistema que hacen que, en mayor o menor medida, queden fuera del sistema de gestión de vigilancia e inteligencia.

NOTA 1 Por ejemplo, el desarrollo de proyectos de I+D+i puede ser una acción derivada, pero ésta también depende del diseño del sistema de gestión de la I+D+i, de los recursos y prioridades establecidos por la Dirección, etc.

NOTA 2 En el caso de organizaciones proveedoras de servicios de vigilancia e inteligencia, las acciones derivadas de la vigilancia e inteligencia son completamente ajenas al sistema y a la organización.

Las acciones derivadas de la vigilancia e inteligencia pueden contener categorías como:

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.

8.9.3 Entornos de interés para la organización

Otro resultado de la vigilancia e inteligencia puede ser la identificación de “señales débiles” que pueden constituir oportunidades en nuevos entornos tecnológicos y/o mercados 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.

9 Evaluación del desempeño

9.1 Seguimiento, medición, análisis y evaluación

La organización debe determinar:

– a qué es necesario hacer seguimiento y qué es necesario medir;

– los métodos de seguimiento, medición, análisis y evaluación, según sea aplicable, para asegurar resultados válidos;

– cuándo se debe realizar el seguimiento y la medición;

– cuándo se deben analizar y evaluar los resultados del seguimiento y la medición.

La organización debe conservar la información documentada adecuada como evidencia de los resultados.

La organización debe evaluar el desempeño de la vigilancia e inteligencia y la eficacia del sistema de gestión de vigilancia e inteligencia.

9.2 Auditoría interna

9.2.1 La organización debe llevar a cabo auditorías internas a intervalos planificados, para proporcionar información acerca de si el sistema de gestión de vigilancia e inteligencia:

a) es conforme con:

   – los requisitos propios de la organización para su sistema de gestión de vigilancia e inteligencia,

   – los requisitos de esta norma;

b) se implementa y mantiene eficazmente.

9.2.2 La organización debe:

a) planificar, establecer, implementar y mantener uno o varios programas de auditoría que incluyan la frecuencia, los métodos, las responsabilidades, los requisitos de planificación, y la elaboración de informes, que deben tener en consideración la importancia de los procesos involucrados y los resultados de las auditorías previas;

b) definir los criterios de la auditoría y el alcance para cada auditoría;

c) seleccionar los auditores y llevar a cabo auditorías para asegurarse de la objetividad y la imparcialidad del proceso de auditoría;

d) asegurarse de que los resultados de las auditorías se informan a la dirección pertinente;

e) conservar información documentada como evidencia de la implementación del programa de auditoría y de los resultados de las auditorías.

9.3 Revisión por la dirección

La alta dirección debe revisar el sistema de gestión de vigilancia e inteligencia de la organización a intervalos planificados, para asegurarse de su idoneidad, adecuación y eficacia continuas.

La revisión por la dirección debe considerar:

a) el estado de las acciones de las revisiones por la dirección previas;

b) los cambios en las cuestiones externas e internas que sean pertinentes al sistema de gestión de vigilancia e inteligencia;

c) la información sobre el desempeño de la vigilancia e inteligencia, incluidas las tendencias relativas a:

   – no conformidades y acciones correctivas;

   – seguimiento y resultados de las mediciones;

   – resultados de la auditoría;

d) las oportunidades de mejora continua.

Las salidas de la revisión por la dirección deben incluir las decisiones relacionadas con las oportunidades de mejora continua y cualquier necesidad de cambio en el sistema de gestión de vigilancia e inteligencia.

La organización debe conservar información documentada como evidencia de los resultados de las revisiones por la dirección.

10 Mejora

10.1 No conformidades y acciones correctivas

Cuando ocurra una no conformidad, la organización debe:

a) reaccionar ante la no conformidad, y según sea aplicable

   – tomar acciones para controlarla y corregirla;

   – hacer frente a las consecuencias;

b) evaluar la necesidad de acciones para eliminar las causas de la no conformidad, con el fin de que no vuelva a ocurrir ni ocurra en otra parte, mediante:

   – revisando la no conformidad;

   – determinando las causas de la no conformidad;

   – determinando si existen no conformidades similares, o que potencialmente podrían ocurrir;

c) implementar cualquier acción necesaria;

d) revisar la eficacia de cualquier acción correctiva tomada;

e) si es necesario, hacer cambios al sistema de gestión de vigilancia e inteligencia.

Las acciones correctivas deben ser adecuadas a los efectos de las no conformidades encontradas.

La organización debe conservar información documentada, como evidencia de:

– la naturaleza de las no conformidades y cualquier acción tomada posteriormente;

– los resultados de cualquier acción correctiva.

10.2 Mejora continua

La organización debe mejorar continuamente la idoneidad, adecuación y eficacia del sistema de gestión de vigilancia e inteligencia.

11 Bibliografía

UNE 166002:2014, *Gestión de la I+D+i. Requisitos del sistema de gestión de la I+D+i.*

UNE 412001:2008 IN, *Guía práctica para la gestión del conocimiento.*

[1] Especificación abierta RedAlerta v1.0
http://es.slideshare.net/RedAlerta/especificacin-redalerta-v01-para-plataformas-de-inteligencia-en-red

Para información relacionada con el desarrollo de las normas contacte con:

Asociación Española de Normalización
Génova, 6
28004 MADRID-España
Tel.: 915 294 900
info@une.org
www.une.org

Para información relacionada con la venta y distribución de las normas contacte con:

AENOR INTERNACIONAL S.A.U.
Tel.: 914 326 000
normas@aenor.com
www.aenor.com

UNE NormalizaciónEspañola organismo de normalización español en: