



**COMISIÓN EUROPEA**

DG Mercado Interior y Servicios

Servicios

**Cooperación administrativa y redes entre Estados miembros**

**COOPERACIÓN ADMINISTRATIVA CON ARREGLO A LA DIRECTIVA DE SERVICIOS**

**MECANISMO DE ALERTA EN EL  
SISTEMA DE INFORMACIÓN DEL MERCADO INTERIOR (IMI)**

**Orientaciones y manual para el usuario**

## INTRODUCCIÓN

En virtud de los artículos 29.3 y 32.1 de la Directiva de servicios, los Estados miembros están obligados a informar a otros Estados miembros y a la Comisión sobre las actividades de servicios que puedan causar un perjuicio grave para la salud o la seguridad de las personas o del medio ambiente (“**mecanismo de alerta**”). Esta información ayuda a los Estados miembros a prevenir riesgos y proteger a los destinatarios de los servicios.

El intercambio rápido y seguro de información que requiere el mecanismo de alerta queda garantizado mediante una aplicación específica del Sistema de Información del Mercado interior (IMI).

Esta **guía práctica** está dirigida a las autoridades de los Estados miembros que participan en la gestión de las alertas. Consta de dos partes:

### **Parte 1: Orientaciones sobre el uso del mecanismo de alerta**

Las orientaciones tienen por objeto favorecer una interpretación homogénea de los **criterios y condiciones para el envío de las alertas**, con el fin de limitarlo a los casos en que sea estrictamente necesario y se cumplan los criterios establecidos en la Directiva de servicios. En las orientaciones también se explica cómo utilizar otras funciones del sistema IMI relacionadas con el cierre, retirada y rectificación de las alertas. Varios ejemplos ilustran el funcionamiento práctico de dichas funciones.

### **Parte 2: Manual para el usuario del mecanismo de alerta**

El manual para el usuario se ocupa de los **aspectos técnicos** de la gestión de alertas en el sistema IMI. Detalla las distintas funciones que pueden desempeñar las autoridades y los usuarios y describe el uso de todas las herramientas disponibles para cada fase del procedimiento. Además, explica cómo configurar el sistema para lograr un tratamiento eficaz de las alertas.

Más información sobre la Directiva de servicios:

[http://ec.europa.eu/internal\\_market/services/services-dir/index\\_en.htm](http://ec.europa.eu/internal_market/services/services-dir/index_en.htm)

Más información sobre el sistema IMI: [http://ec.europa.eu/internal\\_market/imi-net](http://ec.europa.eu/internal_market/imi-net)

Si tiene algún problema técnico relacionado con el mecanismo de alerta, diríjase al coordinador que haya efectuado su registro en el sistema. Para las situaciones que no puedan resolverse a ese nivel, la Comisión ha creado un servicio de ayuda cuya dirección de contacto es: [ec-imi-alerts@ec.europa.eu](mailto:ec-imi-alerts@ec.europa.eu).

## ÍNDICE

PARTE 1: ORIENTACIONES SOBRE EL USO DEL MECANISMO DE ALERTA.....	5
1. INTRODUCCIÓN: ¿PARA QUÉ SIRVEN ESTAS ORIENTACIONES?.....	6
TABLA 1: LISTA DE CONTROL: EVALUAR LA POSIBILIDAD DE ENVIAR UNA ALERTA.....	7
TABLA 2: RELACIÓN ENTRE LA GRAVEDAD DEL PERJUICIO Y LA PROBABILIDAD DE QUE SE PRODUZCA.....	8
TABLA 3: VALORACIÓN PASO A PASO DE CUÁNDO ENVIAR UNA ALERTA ...	9
2. RESUMEN DE LOS CRITERIOS PARA EL ENVÍO DE UNA ALERTA.....	12
3. LOS CRITERIOS EN DETALLE.....	12
3.1. Conducta, actos o circunstancias específicos relativos a una actividad de servicios .....	12
3.2. Perjuicio grave para la salud o la seguridad de las personas o del medio ambiente.....	14
3.3. Relación causal entre la situación relacionada con los servicios y el potencial perjuicio grave .....	15
3.4. Riesgo real/concreto .....	15
3.5. El riesgo deberá tener un efecto transfronterizo.....	17
4. ¿QUIÉN ENVÍA UNA ALERTA? .....	17
4.1. Alertas enviadas por el Estado miembro de establecimiento .....	17
4.2. Alertas enviadas por Estados miembros diferentes del Estado de establecimiento .....	19
4.3. Alertas enviadas por el Estado miembro de establecimiento relacionadas con una alerta previa enviada por otro Estado miembro .....	19
5. ¿QUIÉN DEBERÍA RECIBIR UNA ALERTA?.....	19
6. CIERRE DE LAS ALERTAS .....	20
6.1. ¿Cuándo debería cerrarse una alerta? .....	20
6.2. Objeciones al cierre de la alerta.....	20
7. RETIRADA/CANCELACIÓN DE LAS ALERTAS .....	20
8. RECTIFICACIÓN DE LA INFORMACIÓN .....	21
9. ENVÍO DE INFORMACIÓN ADICIONAL .....	21
PARTE 2: MANUAL PARA EL USUARIO DEL MECANISMO DE ALERTA .....	23

10. INTRODUCCIÓN.....	24
11. PROCEDIMIENTO DE ALERTA EN EL SISTEMA IMI.....	24
11.1. Estructura modular del sistema.....	24
11.2. Ciclo de vida de las alertas .....	24
12. AGENTES QUE INTERVIENEN Y FUNCIONES RESPECTIVAS.....	25
12.1. Funciones de las autoridades .....	25
12.2. Funciones de los usuarios .....	27
13. TRATAMIENTO DE LAS ALERTAS EN EL IMI .....	29
13.1. Envío de las alertas .....	29
13.2. Modificación y rectificación de las alertas.....	30
13.3. Retirada de las alertas .....	31
13.4. Gestión de destinatarios.....	31
13.5. Envío y solicitud de información adicional.....	32
13.6. Cierre de las alertas.....	32
14. SEGUIMIENTO DE LAS ALERTAS .....	34
14.1. Notificaciones por correo electrónico.....	34
14.2. Lista de alertas .....	35
14.3. Impresión de las alertas .....	35
15. ALERTAS Y PROTECCIÓN DE DATOS.....	35
16. INFORMACIÓN ADICIONAL PARA LOS COORDINADORES – CÓMO ESTABLECER LA ESTRUCTURA QUE REQUIERE EL MECANISMO DE ALERTA EN CADA PAÍS .....	36
16.1. Registro inicial por la Comisión.....	36
16.2. Registro de autoridades y acceso al procedimiento de alerta.....	37
16.3. Autoridades y coordinadores vinculados.....	38

## **PARTE 1: ORIENTACIONES SOBRE EL USO DEL MECANISMO DE ALERTA**

## **1. INTRODUCCIÓN: ¿PARA QUÉ SIRVEN ESTAS ORIENTACIONES?**

La Directiva de servicios, en su artículo 29, apartado 3, y artículo 32, apartado 1, establece la obligación de los Estados miembros de informar a otros Estados miembros y a la Comisión sobre las actividades de servicios que puedan causar un perjuicio grave para la salud o la seguridad de las personas o del medio ambiente («mecanismo de alerta»). Esta información ayudará a los Estados miembros a prevenir riesgos y a proteger a los destinatarios de los servicios.

El intercambio rápido y seguro de información a través del «mecanismo de alerta» estará garantizado gracias al uso de una aplicación específica del sistema de información del mercado interior (en lo sucesivo denominado IMI).

También es importante que todas las partes interpreten de igual modo los criterios y las condiciones de las alertas, para reducir el riesgo de enviar alertas innecesarias o infundadas. Además, es necesario llegar a un consenso sobre el uso de las otras funciones adicionales del sistema IMI, como el cierre, la retirada/cancelación y la rectificación de alertas y el envío de información adicional.

Estas orientaciones están basadas en los conceptos recogidos en la Directiva de servicios y no limitan ni aumentan en ningún caso las obligaciones de los Estados miembros. Están concebidas para ayudar a los Estados miembros a orientar a las autoridades nacionales en la utilización del mecanismo de alerta.

Estas orientaciones no son exhaustivas y no pretenden dar cuenta de todas las situaciones y circunstancias posibles. Las autoridades nacionales deberán juzgar cada caso individualmente, teniendo en cuenta los criterios fijados en la Directiva de servicios, su propia experiencia y práctica y cualquier otra consideración y método que resulten procedentes.

Es importante tener en cuenta que las orientaciones se entienden sin perjuicio de las normas nacionales sobre quién es la autoridad responsable de enviar una alerta o de adoptar las medidas pertinentes.

Habida cuenta de las repercusiones que una alerta puede tener para el prestador de servicios, los Estados miembros tendrán que garantizar que el sujeto objeto de la alerta esté adecuadamente protegido en todo momento (antes, durante y después del envío de las alertas). Resulta especialmente importante garantizar que sólo se envíen alertas realmente justificadas. Estas orientaciones se limitan a ofrecer criterios de fondo para enviar, cerrar, retirar y rectificar una alerta, y para enviar información adicional. No abordan la aplicación de la legislación nacional o comunitaria en materia de derechos de defensa.

TABLA 1: LISTA DE CONTROL: EVALUAR LA POSIBILIDAD DE ENVIAR UNA ALERTA

<b>Paso 1</b>	<u>¿El perjuicio grave potencial está relacionado con una actividad de servicios/con la conducta de un prestador de servicios?</u>	→ No × → No envíe alerta					
<b>Paso 2</b>	↓ Sí √→	<u>¿La actividad de servicios está cubierta por la Directiva de servicios?</u>	→ No × → No envíe alerta				
<b>Paso 3</b>	↓ Sí √→	↓ Sí √→	<u>¿Existe riesgo de provocar perjuicios graves a la salud o la seguridad de las personas o el medio ambiente?</u>	→ No × → N envíe alerta			
<b>Paso 4</b>	Sí √	Sí √	↓ Sí √→	<u>¿Existe una relación causal entre la prestación del servicio y el potencial perjuicio grave?</u>	→ No × → No envíe alerta		
<b>Paso 5</b>	Sí √	Sí √	↓ Sí √→	<u>¿Existe un riesgo real/concreto de que se produzca un perjuicio grave?</u>	→ No × → No envíe alerta		
<b>Paso 6</b>	Sí √	Sí √	Sí √	Sí √	↓ Sí √→	<u>¿Existe el riesgo de que el perjuicio se produzca en otros Estados miembros?</u>	→ No × → No envíe alerta
¿Se ha respondido positivamente en <b>todos</b> los pasos? Sí √→		ENVIAR ALERTA					

TABLA 2: RELACIÓN ENTRE LA GRAVEDAD DEL PERJUICIO Y LA PROBABILIDAD DE QUE SE PRODUZCA

	(Probabilidad menor←) Probabilidad (→ Probabilidad mayor)	
(Perjuicio potencial más grave)←Perjuicio potencial grave →(Perjuicio potencial menos grave)	<p><u>Caso 4</u>: perjuicio potencial menos grave y probabilidad de que ocurra relativamente baja</p> <p><b>En general, no envíe una alerta</b></p>	<p><u>Caso 3</u>: perjuicio potencial menos grave y probabilidad de que ocurra relativamente alta/muy alta</p> <p><b>Envíe una alerta en algunos casos</b></p>
	<p><u>Caso 2</u>: perjuicio potencial (muy) grave y probabilidad de que ocurra relativamente baja</p> <p><b>En general, envíe una alerta</b></p>	<p><u>Caso 1</u>: perjuicio potencial (muy) grave y probabilidad de que ocurra relativamente alta/muy alta</p> <p><b>Envíe una alerta</b></p>

Nota: el objetivo de esta tabla es ilustrar la búsqueda de un posible equilibrio entre la gravedad del daño potencial y la posibilidad de que suceda. Esta tabla no tiene en consideración los demás criterios para enviar alertas descritos en estas orientaciones, que también se tienen que cumplir antes de poder enviar una alerta.

TABLA 3: VALORACIÓN PASO A PASO DE CUÁNDO ENVIAR UNA ALERTA

**Paso 1:** [¿El perjuicio grave potencial está relacionado con una actividad de servicios o con la conducta de un prestador de servicios?](#)

Sí, el potencial perjuicio grave está relacionado con una actividad de servicios o con la conducta de un prestador de servicios.

→ **Continúe con el paso dos**

No

→ **No envíe la alerta**

**Paso 2:** [¿La actividad de servicios está cubierta por la Directiva de servicios?](#)

*Si tiene dudas acerca del ámbito de aplicación de la Directiva de Servicios, haga clic aquí para obtener más información:*

[http://ec.europa.eu/internal\\_market/services/docs/services-dir/guides/handbook\\_es.pdf](http://ec.europa.eu/internal_market/services/docs/services-dir/guides/handbook_es.pdf)

Sí

→ **Continúe con el paso tres**

No

→ **No envíe la alerta**

**Paso 3:** [¿Existe riesgo de perjuicio grave para la salud o la seguridad de las personas o del medio ambiente?](#)

Para responder, tenga en cuenta la gravedad y el alcance del perjuicio potencial. Si el perjuicio potencial es especialmente grave o su alcance muy grande, puede ser necesario enviar una alerta incluso si la probabilidad de que se produzca un perjuicio es baja.

Sí: la conducta, ciertos actos o circunstancias específicos pueden ocasionar un perjuicio grave a la salud o la seguridad de las personas o del medio ambiente.

→ **Continúe con el paso cuatro**

No, el riesgo de que se produzca un perjuicio grave no es suficiente

→ **No envíe la alerta**

**Paso 4:** [¿Existe una relación causal entre la situación relacionada con los servicios y el potencial perjuicio grave?](#)

Sí, existe una relación causal. El potencial perjuicio estaría ocasionado esencialmente por la conducta, actos o circunstancias específicos.

→ **Continúe con el paso cinco**

No: no se ha podido detectar una relación causal entre la conducta, actos o circunstancias específicos y el potencial perjuicio grave

→ **No envíe la alerta**

**Paso 5:** [¿Existe un riesgo real/concreto de perjuicio grave? Antes de ofrecer una respuesta, tenga en cuenta los siguientes elementos en particular:](#)

- ¿Todavía existe el riesgo de un perjuicio grave o es probable que dicho riesgo exista en el futuro próximo? *(si la respuesta es no, no envíe la alerta)*
- ¿Se ha hecho algo para eliminar o reducir el riesgo? *(si esta acción ha eliminado el riesgo/si el riesgo residual es insignificante, no envíe ninguna alerta)*
- ¿Quién es el destinatario medio del servicio? *(si el destinatario es el tipo de persona a quien le resulta difícil detectar los riesgos o tomar precauciones, el riesgo de perjuicio suele ser mayor)*

Sí: existe un riesgo real de perjuicio grave.

→ **Continúe con el paso seis**

No, el riesgo no persiste/no es probable que vuelva a producirse en un futuro próximo.

→ **No envíe la alerta**

**Paso 6: ¿Existe riesgo de que se produzca algún perjuicio en otros Estados miembros?**

Antes de ofrecer una respuesta, tenga en cuenta los siguientes elementos:

- ¿El prestador ofrece servicios en otros Estados miembros?
- ¿El prestador tiene su sede en una región fronteriza?
- ¿El tipo de servicio en cuestión tiene probabilidades de ser prestado transfronterizamente?

Sí, hay un efecto transfronterizo.

→ **Envíe la alerta**

No, no hay ningún efecto transfronterizo.

→ **No envíe la alerta**

## 2. RESUMEN DE LOS CRITERIOS PARA EL ENVÍO DE UNA ALERTA

Los requisitos para enviar una alerta y los pertinentes criterios se establecen en el artículo 29, apartado 3, y en el artículo 32, apartado 1, de la Directiva de servicios. El artículo 29, apartado 3, se refiere a los casos en los que el Estado miembro de establecimiento tiene conocimiento de conductas o actos que podrían ocasionar un perjuicio grave, mientras que el artículo 32, apartado 1, recoge una obligación de información similar para los Estados miembros diferentes del Estado de establecimiento. A pesar de que ambos artículos abordan situaciones diferentes, tienen el mismo objetivo y están basados en criterios y principios esencialmente similares. Así pues, los criterios para enviar alertas son los siguientes:

- a) conducta, actos o circunstancias específicos relativos a una actividad de servicios;
- b) existencia de un riesgo de perjuicio grave para la salud o la seguridad de las personas o del medio ambiente;
- c) existencia de una relación causal entre la situación relacionada con los servicios y el potencial perjuicio grave;
- d) existencia de un riesgo real;
- e) efecto transfronterizo del riesgo.

Para enviar una alerta, **todos** estos criterios tienen que cumplirse en la situación específica.

## 3. LOS CRITERIOS EN DETALLE

### 3.1. Conducta, actos o circunstancias específicos relativos a una actividad de servicios

#### 3.1.1. Situaciones posibles

Sólo deberá enviarse una alerta si se detecta que una actividad de servicios **que entra dentro del ámbito de la Directiva de servicios**<sup>1</sup> puede causar un perjuicio grave. Por ejemplo, el «mecanismo de alerta» no se aplica en situaciones en las que los servicios de transporte, los servicios sanitarios o los servicios de seguridad privada puedan ocasionar un perjuicio, ya que estos servicios no entran en el ámbito de aplicación de la Directiva.

El hecho de que un servicio se esté ofreciendo de forma legal en un Estado miembro no significa que el Estado miembro no pueda enviar una alerta por razón de una conducta o de actos específicos que, en el contexto de la prestación de ese servicio, generan un riesgo de perjuicio grave para la salud o la seguridad de las personas o del medio ambiente.

El riesgo de un perjuicio grave deberá derivarse de la **conducta** del prestador del servicio o de cualquier **otra circunstancia** relativa a la actividad de servicio. De este modo, no deberá enviarse

---

<sup>1</sup> Artículo 2 de la Directiva de servicios. Si desea una explicación más detallada sobre el ámbito de aplicación de la Directiva de servicios, consulte la sección 2.1 del Manual sobre la transposición de la Directiva de servicios en [http://ec.europa.eu/internal\\_market/services/docs/services-dir/guides/handbook\\_es.pdf](http://ec.europa.eu/internal_market/services/docs/services-dir/guides/handbook_es.pdf).

ninguna alerta por conductas o acciones que pudiesen suponer un peligro, pero que **no estén relacionadas con la prestación de servicios**.

*Ejemplo*

*Si un prestador de servicios que ofrece cursos de idiomas es arrestado por conducir de forma temeraria, no habrá ningún motivo para enviar una alerta a otros Estados miembros. La conducta que ha generado el peligro no tiene relación alguna con la prestación del servicio.*

Entre los ejemplos de conductas que pueden generar riesgos, destacamos<sup>2</sup>:

- **Acción positiva** del prestador del servicio, como presentar una conducta peligrosa o facilitar información falsa (por ejemplo, tratar los residuos de forma irresponsable, lo cual podría dañar el medio ambiente, u ofrecer asesoramiento nutricional incorrecto, lo que podría dañar la salud de las personas).
- **Omisión o falta de supervisión** por parte del prestador del servicio, como no adoptar las medidas preventivas necesarias o no ofrecer las instrucciones básicas a los destinatarios del servicio (por ejemplo, sobre la duración máxima de una sesión de solarium).
- La **utilización inapropiada de un equipo seguro o la utilización de un equipo peligroso** para la prestación del servicio (por ejemplo, la utilización en interiores de un equipo de sonido diseñado sólo para exteriores o el uso de atracciones no seguras en ferias de atracciones itinerantes).

*3.1.2. Situaciones en las que el mecanismo de alerta no se puede utilizar: relación entre el mecanismo de alerta de la Directiva de servicios y los mecanismos de alerta ya existentes para productos*

Para este mecanismo de alerta, **el riesgo deberá estar relacionado con la conducta, actos o circunstancias específicos dentro del contexto de una actividad de servicios**.

**El mecanismo de alerta no deberá utilizarse en los casos en los que el riesgo se origina en productos de consumo**. En esos casos, deberán utilizarse los sistemas de alerta rápida para productos<sup>3</sup>. Esto permitirá a los Estados miembros conocer los detalles del riesgo del producto a fin de que puedan tomar medidas para retirarlo del mercado.

Sin embargo, en ciertos casos, **la conducta del prestador de servicios puede estar relacionada con el uso de productos como parte de una prestación de servicios** y, en el caso de un riesgo grave, deberá emplearse el mecanismo de alerta. Este sería el caso, por ejemplo, si un prestador de servicios hiciese un **uso inadecuado de productos seguros** a la hora de ofrecer un servicio, generando un riesgo para la salud o la seguridad de las personas o del medio ambiente.

*Ejemplo*

*En determinados tratamientos de belleza, el prestador de servicios X utiliza cremas anestésicas en una dosis superior a la indicada. El uso inadecuado de estas cremas supone un riesgo para la salud de las personas. Dado que el mal uso de una anestesia (y no la*

---

<sup>2</sup> Para tomar la decisión de enviar una alerta, no es necesario determinar error o negligencia en relación con la conducta en cuestión.

<sup>3</sup> Es decir, sistemas de alerta rápida para la seguridad de productos de consumo no alimentarios (RAPEX), alimentos y pienso (RASFF) o productos médicos, sistema de «vigilancia» para dispositivos médicos.

*anestesia en sí) provoca la prestación de un servicio no seguro, deberá utilizarse el mecanismo de alerta de la Directiva de servicios.*

Otro ejemplo es la utilización de un producto peligroso en la prestación de un servicio. En este caso, puede ser necesario enviar una alerta complementaria a través del mecanismo de alerta de la Directiva de servicios incluso aunque ya se haya enviado una alerta a través del mecanismo de alerta para productos. Este sería el caso, por ejemplo, de un prestador de servicios que siguiese utilizando productos peligrosos para el consumidor en la prestación de una actividad de servicios a pesar de que esos productos ya hubiesen sido retirados del mercado o recogidos por productores o distribuidores.

#### Ejemplo

*Una alerta RAPEX informa de un juguete peligroso que, por lo tanto, se retira del mercado en todos los Estados miembros. El Estado miembro A sabe que la empresa de espectáculos infantiles X sigue utilizando ese juguete peligroso en sus actuaciones en varios Estados miembros. Esta conducta podría poner en grave peligro la salud de los niños. El Estado miembro A debería enviar una alerta a través del mecanismo de alerta de la Directiva de servicios advirtiendo del peligro del servicio recreativo prestado por X.*

### **3.2. Perjuicio grave para la salud o la seguridad de las personas o del medio ambiente**

Para enviar una alerta, el posible perjuicio para la salud o la seguridad de las personas o del medio ambiente ha de ser **grave**. En este sentido, distinguimos dos factores de especial importancia: a) la potencial gravedad del perjuicio y b) el potencial alcance del perjuicio.

#### *3.2.1. Gravedad del perjuicio*

Para valorar la potencial gravedad del perjuicio será necesario tener en cuenta las posibles consecuencias de la conducta del prestador de servicios o de las circunstancias.

- **Un perjuicio grave para la salud o la seguridad de las personas** incluiría daños a su integridad física o mental, como lesiones graves (por ejemplo, fracturas, daños a órganos internos, daños a la vista o al oído, cortes o quemaduras de piel severos, etc.), enfermedades crónicas u otro tipo de enfermedades graves, trastornos mentales, etc.
- **Un perjuicio grave para el medio ambiente** (natural y urbano) incluiría contaminación grave en sus diferentes formas (contaminación del agua y del aire, contaminación del suelo por herbicidas, pesticidas o metales pesados, contaminación acústica y lumínica), incendios y destrucción de los ecosistemas y de la biodiversidad.

#### *3.2.2. Alcance del perjuicio*

Deberá tenerse en cuenta el número de personas o la extensión de la zona que podría resultar afectada a la hora de calcular la gravedad del daño potencial. Si el alcance es especialmente grande, obviamente la gravedad del perjuicio será mayor.

#### Ejemplo

*Un prestador de servicios establecido en el Estado miembro A no cumple las normas higiénicas y su prestación del servicio de catering ha provocado una intoxicación alimentaria leve a un elevado número de personas en el Estado miembro B. A pesar de que, en principio, podría considerarse que*

*el perjuicio ocasionado por una intoxicación alimentaria leve no es grave para la salud de las personas, habida cuenta del gran número de personas afectadas, el perjuicio puede considerarse grave.*

### **3.3. Relación causal entre la situación relacionada con los servicios y el potencial perjuicio grave**

Debe existir una **relación causal directa** entre la conducta o las circunstancias y el potencial perjuicio grave. No se tendrá en cuenta tal relación en el caso de que el riesgo que genera la alerta haya sido provocado o causado en un importante grado por motivos de fuerza mayor o por un tercero (incluido el destinatario del servicio).

#### Ejemplo

*El destinatario X de un servicio sufre un perjuicio grave debido a que no cumplió las instrucciones que claramente se le indicó que debía seguir al utilizar el equipo de buceo. En este caso, el daño no se origina en la conducta del prestador del servicio, sino en la conducta del destinatario del servicio.*

### **3.4. Riesgo real/concreto**

Es importante tener en cuenta que el conocimiento de actos específicos o conductas peligrosas por parte de un prestador de servicios en un Estado miembro no debería resultar automáticamente en el envío de una alerta por parte de dicho Estado miembro. Lo importante es determinar la **existencia real de un riesgo**. Existirá un riesgo real si una situación peligrosa relativa a una actividad de servicios:

- **todavía existe** en el momento en que se envía la alerta o
- es (suficientemente) **probable que se produzca** en un futuro (próximo).

Para llegar a la conclusión de que es **suficientemente probable** que se produzca una situación peligrosa en el futuro deberán tenerse en consideración todos **los hechos/las circunstancias**, y muy especialmente, si estas situaciones peligrosas o posibles daños ya han tenido lugar en el pasado y si hay indicios de que puedan producirse cambios en la conducta del prestador o en sus circunstancias.

Los accidentes totalmente fortuitos no se pueden predecir ni prevenir. Si nada indica que un accidente que haya sucedido durante el transcurso de la prestación de un servicio pueda volver a ocurrir, no será necesario enviar una alerta aunque el daño ocasionado haya sido muy grave.

#### Ejemplo

*El prestador de servicios X ofrece un tratamiento innovador para la piel que supone un perjuicio claro para la salud de las personas. Hay razones para creer que no se van a producir cambios en la conducta del prestador de servicios X a no ser que se vea obligado. El riesgo de daño seguirá existiendo en tanto el prestador de servicios X continúe ofreciendo sus servicios. Cualquier Estado miembro que conozca el perjuicio deberá alertar al Estado miembro de establecimiento y a cualquier Estado miembro en el que se considere que X pueda ofrecer sus servicios.*

Algunos servicios conllevan un **grado de riesgo inherente**, como ciertos deportes de «alto riesgo» (por ejemplo, parapente, paracaídas, puentismo, etc.) o ciertos eventos, como las carreras de coches urbanas.

Cuando un servicio intrínsecamente peligroso se realiza de forma legal en un Estado miembro determinado, está claro que no debería enviarse ninguna alerta a ningún otro Estado miembro. Sin embargo, si una conducta o los actos específicos de un determinado prestador de servicios aumentasen considerablemente el riesgo inherente a dicho servicio, debería enviarse una alerta para informar a otros Estados miembros del perjuicio que podría representar la conducta o los actos específicos del prestador de servicios en cuestión (siempre y cuando se cumplan todos los criterios necesarios para enviar una alerta).

#### Ejemplo

*Si el Estado miembro A permite que se ofrezcan servicios de puentismo, no podrá enviar una alerta porque el prestador de servicios X esté ofreciendo tales servicios de forma legal en su territorio. No obstante, si hay pruebas de que el prestador de servicios X está aumentando el riesgo inherente al puentismo al ofrecer servicios que no cumplen las normas de seguridad, el Estado miembro A deberá enviar una alerta al Estado miembro de establecimiento de X.*

Obviamente, si el potencial perjuicio es especialmente grave, aun cuando la probabilidad de que suceda en el futuro sea baja, el envío de la alerta estaría justificado.

Hay dos factores que parecen tener especial importancia: a) el efecto de las posibles medidas adoptadas por el prestador de servicios o por los Estados miembros a fin de eliminar o de reducir el riesgo, y b) el destinatario medio del servicio y su capacidad para detectar y evitar el riesgo.

#### *3.4.1. Efecto de las posibles medidas adoptadas por el prestador de servicios o por un Estado miembro a fin de eliminar o reducir el riesgo*

En determinadas situaciones, medidas adoptadas voluntariamente por el prestador de servicios podrían eliminar el riesgo. De igual modo, medidas adoptadas por el Estado miembro de establecimiento o por otros Estados miembros de conformidad con la legislación comunitaria y, en especial, con la Directiva de servicios, pueden reducir considerablemente el riesgo o eliminarlo en su totalidad. Si no hay riesgo, no deberá enviarse ninguna alerta.

En general, el Estado miembro de establecimiento podrá tomar medidas para eliminar el riesgo, por lo que en principio habrá más alertas enviadas por los Estados miembros distintos del país de establecimiento.

#### *3.4.2. Tipo de destinatario y su capacidad para detectar y evitar el riesgo*

A la hora de evaluar la probabilidad de un perjuicio, también es importante tener en cuenta el **conocimiento del riesgo por el destinatario medio del servicio y la posibilidad de tomar precauciones** a fin de poder clasificar el riesgo.

El conocimiento del riesgo puede depender del **tipo de usuario del servicio**. Cuando es una empresa la que ofrece un servicio a otra empresa, el destinatario puede tener más conocimientos y ser más capaz de tomar precauciones que cuando la empresa ofrece el servicio a un consumidor individual. De igual modo, cuando un servicio está destinado a personas mayores, niños o personas con discapacidad física o psíquica, el riesgo de daño derivado de una conducta o acto específico puede ser mayor.

#### Ejemplo

*Un Estado miembro tiene conocimiento de una actividad de servicios destinada a niños que podría causar graves perjuicios a su seguridad. Dado que los niños, por regla general, son menos*

*conscientes de los riesgos y, por lo tanto, incapaces de tomar precauciones para evitarlo, la probabilidad del daño parece ser más elevada que si las actividades de riesgo están dirigidas a personas adultas.*

Para otros grupos de personas, la probabilidad del perjuicio puede ser más elevada si el prestador del servicio no ofrece instrucciones, advertencias o garantías adecuadas y el riesgo no es obvio.

#### Ejemplo

*El prestador de servicios A ofrece orientaciones en materia de nutrición que pueden causar un daño considerable a las personas que sufren desequilibrios nutricionales específicos. Los destinatarios parecen no ser conscientes de este perjuicio. Habida cuenta de la novedad que supone este tipo de información, la sociedad en general dispone de muy poca información sobre los riesgos. A la hora de valorar si es probable que se produzca un perjuicio en el futuro, los Estados miembros tienen que tener en cuenta que los adultos no podrán tomar suficientes medidas de precaución para evitarlo.*

### **3.5. El riesgo deberá tener un efecto transfronterizo**

Antes de que un Estado miembro envíe una alerta, debería asegurarse de que la probabilidad de que se produzca un perjuicio **en otros Estados miembros** es suficiente, lo que significa que ha de tener en cuenta otros factores que podrían indicar que el prestador del servicio probablemente también esté presente en otros Estados miembros.

Obviamente, es más fácil presumir que exista riesgo de perjuicio en otro Estado miembro si el prestador del servicio está establecido en otro Estado miembro diferente del Estado donde aparece el riesgo. El tipo de servicio que presta o el lugar de establecimiento del prestador del servicio pueden ofrecer también ciertos indicios; si dicho lugar está geográficamente cerca de otro Estado miembro cabría suponer que tuviese actividad en otros Estados miembros. En el caso de los servicios en línea es más fácil suponer que tienen un efecto transfronterizo.

Cuando el perjuicio viene dado por el uso de equipos defectuosos que pueden utilizarse en otros Estados miembros, será más fácil determinar el efecto transfronterizo del riesgo.

## **4. ¿QUIÉN ENVÍA UNA ALERTA?**

La Directiva de servicios distingue entre alertas enviadas por el Estado miembro de establecimiento (artículo 29, apartado 3) y otros (artículo 32, apartado 1). Ambas situaciones se examinan por separado a continuación.

### **4.1. Alertas enviadas por el Estado miembro de establecimiento**

En muchos casos, no será necesario que el Estado miembro de establecimiento envíe una alerta porque, en cuanto tenga conocimiento de un perjuicio grave para la salud o la seguridad de las personas o del medio ambiente, por lo general, tomará de inmediato medidas para evitar cualquier riesgo. Estas medidas, en general, deberán garantizar que el riesgo deja de existir (por ejemplo, retirar la autorización a un prestador de servicios para evitar que pueda seguir realizando sus actividades, reparar el equipo defectuoso, etc.). Si no hay ningún riesgo (persistente) de perjuicio grave para la salud o la seguridad de las personas o del medio ambiente en otros Estados miembros, no deberá enviarse ninguna alerta.

Sin embargo, en determinados casos, el Estado miembro de establecimiento puede tener que enviar una alerta pese a haber tomado las medidas pertinentes, por ejemplo:

- Cuando el Estado miembro de establecimiento no tiene la certeza de que las medidas tomadas contra el prestador del servicio puedan aplicarse de forma eficaz o de que son suficientes para evitar que aparezca el riesgo.

Ejemplo

*El Estado miembro A recibe quejas sobre un prestador de servicios que está creando un riesgo muy grave para la salud de los destinatarios del servicio. No se pueden adoptar medidas efectivas e inmediatas para eliminar o evitar el riesgo en el lugar de establecimiento porque el prestador del servicio está actualmente fuera de su territorio ofreciendo sus servicios en otros Estados miembros.*

- Cuando el Estado miembro de establecimiento tiene conocimiento de que el prestador de servicios está utilizando el mismo equipo para ofrecer servicios en otros Estados miembros.

Ejemplo

*El Estado miembro A tiene conocimiento de que el prestador de servicios X organiza excursiones en bicicleta en A y en el Estado miembro B. En el Estado miembro A, X está utilizando bicicletas cuyo mantenimiento no es correcto, por lo que están creando un riesgo para la seguridad de las personas. El Estado miembro A tiene motivos fundados para creer que se están utilizando las mismas bicicletas en el Estado miembro B.*

- En algunas ocasiones, el perjuicio grave infligido a la salud y la seguridad de las personas no se deriva de forma inmediata de la conducta o de los actos específicos que lo causan, sino que tarda tiempo en aparecer. Si la conducta o los actos específicos que crean el riesgo ya se han producido en otros Estados miembros, ya no será posible que el Estado miembro de establecimiento haga nada para eliminar el riesgo. En tales casos, deberá enviarse una alerta para que los demás Estados miembros puedan tomar las medidas oportunas.

Ejemplo

*El prestador de servicios X, establecido en el Estado miembro A, trabaja en el sector de instalación de techos. Algunos de sus techos se han hundido y han originado un grave riesgo de daño a las personas que viven en los apartamentos. Las inspecciones han concluido que el hundimiento ha sido debido a una negligencia. El Estado miembro A tiene conocimiento de que el prestador X ha trabajado en otros Estados miembros y, por lo tanto, envía una alerta a todos los Estados miembros para ayudarles a evitar más daños.*

El hecho de que el Estado miembro de establecimiento no haya adoptado ninguna medida no impide que envíe una alerta. Sin embargo, si no se adoptan medidas por carecer de pruebas en relación con la existencia de un riesgo o con la gravedad del potencial perjuicio, dicho Estado miembro no deberá enviar una alerta a los demás.

Ejemplo

*El Estado miembro A recibe varias quejas contra el prestador de servicios X en las que se acusa a X de ocasionar un riesgo grave para la salud de las personas. Las quejas son claramente infundadas. Como resultado, no se adopta ninguna medida contra X. En tal caso, el Estado miembro A no deberá enviar ninguna alerta a ningún otro Estado miembro.*

## **4.2. Alertas enviadas por Estados miembros diferentes del Estado de establecimiento**

Cuando un Estado miembro diferente del país de establecimiento tiene conocimiento de circunstancias o actos específicos graves que podrían ocasionar un daño grave a la salud o a la seguridad de las personas o del medio ambiente en su territorio o en otros Estados miembros, dicho Estado deberá informar al Estado de establecimiento, a los demás Estados miembros afectados y a la Comisión a la mayor brevedad posible.

En la mayoría de los casos, será el Estado miembro donde se presta el servicio el que envíe este tipo de alerta

A diferencia de las medidas tomadas por el Estado miembro de establecimiento, las medidas tomadas por el país en el que se presta el servicio suelen evitar riesgos sólo en su propio territorio. Como consecuencia, persisten los riesgos para los demás Estados miembros. En tales casos, debería enviarse una alerta al Estado miembro de establecimiento, otro u otros Estados miembros afectados y la Comisión.

### Ejemplo

*El prestador de servicios X, establecido en el Estado miembro A, está prestando servicios de limpieza industrial en el Estado miembro B. Después de las quejas recibidas, el Estado miembro B realiza una inspección y descubre que X ha eliminado los residuos generados durante su trabajo en un modo en el que expone al medio ambiente a un elevado riesgo de daño. Las autoridades del Estado miembro B reciben información de que X sigue realizando tal práctica. X está ofreciendo también sus servicios en los Estados miembros C y D. Como medida de precaución, envían una alerta al Estado miembro de establecimiento A, al Estado miembro C y al Estado miembro D.*

Al recibir la alerta, el Estado miembro de establecimiento deberá examinar el caso y tomar medidas para prevenir el riesgo en general.

## **4.3. Alertas enviadas por el Estado miembro de establecimiento relacionadas con una alerta previa enviada por otro Estado miembro**

En el caso de que persista el riesgo, a pesar de que el Estado miembro de establecimiento haya tomado medidas, éste deberá, en virtud del artículo 29, apartado 3, de la Directiva de servicios, informar a todos los demás Estados miembros correspondientes, es decir, se enviará una alerta a aquellos Estados miembros que todavía no hayan recibido la alerta, y se transmitirá la información actualizada a los demás Estados miembros<sup>4</sup>.

## **5. ¿QUIÉN DEBERÍA RECIBIR UNA ALERTA?**

La Directiva de servicios distingue entre alertas enviadas por el Estado miembro de establecimiento (artículo 29, apartado 3) y otros (artículo 32, apartado 1). En el caso de que los Estados miembros tengan que decidir a qué Estados miembros afecta una alerta, las autoridades competentes podrán tener en cuenta los siguientes factores:

---

<sup>4</sup> Para evitar confusiones y garantizar la coherencia, esta nueva información se relacionará claramente con la alerta que ya esté presente en el sistema.

- constancia documental de la prestación de servicios en otros Estados miembros en el pasado. Este factor será incluso más relevante si la persona que está prestando el servicio en otro Estado miembro es la misma cuya conducta está provocando el daño o si se está utilizando el mismo equipo que el que está causando el riesgo.
- el tipo de servicio.
- el lugar de establecimiento del prestador del servicio.

## **6. CIERRE DE LAS ALERTAS**

### **6.1. ¿Cuándo debería cerrarse una alerta?**

A fin de garantizar la protección de los prestadores de servicios objeto de una alerta, éstas deberán enviarse sólo si están justificadas, es decir, si cumplen todos los criterios descritos en la sección III de estas orientaciones. Resulta igualmente importante garantizar el cierre de las alertas tan pronto como la causa subyacente deje de existir.

Normalmente, el cierre de la alerta viene dado por la desaparición del riesgo de perjuicio grave para la salud o la seguridad de las personas o del medio ambiente. Por ejemplo, el prestador de servicios puede haber tomado medidas voluntarias para eliminar el riesgo (por ejemplo, puede haber sustituido el equipo defectuoso o haber facilitado instrucciones adecuadas a los destinatarios, eliminando así el riesgo que haya dado lugar a la alerta). También puede ser que el riesgo haya desaparecido gracias a las medidas tomadas por los Estados miembros, medidas que deberán ser siempre compatibles con el derecho comunitario (por ejemplo, el Estado miembro de establecimiento puede haber suspendido temporalmente la autorización del prestador para ejercer sus actividades).

La información de que el riesgo ha dejado de existir puede haber sido obtenida por el propio Estado miembro de establecimiento y/o puede haber sido facilitada por otros Estados miembros mediante el mecanismo de alerta (véase la sección IX más abajo). Una vez que se sabe que el riesgo ha desaparecido, el Estado miembro que haya enviado la alerta deberá enviar de inmediato una propuesta para cerrarla.

### **6.2. Objeciones al cierre de la alerta**

Para evitar una mala utilización de la función de cierre de la alerta y prevenir situaciones en las que se dé por finalizada una alerta a pesar de que uno o más Estados miembros tienen conocimiento de que el riesgo persiste, la propuesta de cierre deberá estar debidamente motivada y los demás Estados miembros implicados deberán poder presentar sus objeciones si tienen constancia de que el riesgo persiste. Los Estados miembros que se ven afectados por una alerta deberán poder oponerse a su fin sólo si tienen información específica de que el riesgo todavía persiste. Los Estados miembros deberán, por lo tanto, ofrecer razones y motivar sus posibles objeciones.

## **7. RETIRADA/CANCELACIÓN DE LAS ALERTAS**

Los criterios para el envío de alertas descritos en estas orientaciones están ideados para evitar el envío de alertas injustificadas o infundadas. A pesar de todas estas garantías, un Estado miembro puede enviar una alerta sobre la base de información o indicios incorrectos o imprecisos, y el error puede tardar tiempo en descubrirse.

### Ejemplo

*Las autoridades competentes del Estado miembro A han recibido información de que el prestador de servicios X, que está establecido en el Estado miembro B y presta servicios de construcción en el Estado miembro A, ha vertido los residuos en este territorio de forma ilegal, por lo que ha causado un daño al medio ambiente. El Estado miembro A envía una alerta al Estado miembro B para evitar futuros daños. En comprobaciones realizadas por el Estado miembro A se ha detectado que los residuos no han sido vertidos por el prestador de servicios X, sino por el prestador de servicios Y, que ha estado trabajando en el mismo lugar que el prestador X. El prestador de servicios Y está establecido en el Estado miembro A y no presta servicios transfronterizos. Por lo tanto, el Estado miembro A retira la alerta.*

Una vez que se conoce el error, el Estado miembro que ha enviado la alerta deberá enviar de inmediato una solicitud para retirarla o cancelarla, que se comunicará de forma automática a todos los destinatarios de la alerta original. Deberá explicarse por qué la alerta era infundada (y, por lo tanto, debe retirarse).

Es importante observar que una alerta sólo podrá retirarse si el Estado miembro que la haya iniciado se da cuenta de que los criterios de su envío no eran válidos desde el primer momento. Si cuando se envió la alerta, el riesgo existía, pero posteriormente desaparece, deberá procederse al cierre de la alerta (no a su retirada), tal y como se describe más arriba.

## **8. RECTIFICACIÓN DE LA INFORMACIÓN**

Por más atención y cuidado que se ponga en la comprobación y motivación de las alertas antes de su envío, puede ser necesario rectificarlas más adelante. Esto puede suceder, por ejemplo, si la información inicial contenida en la alerta resulta ser parcialmente incorrecta. Por ejemplo, en el momento del envío de la alerta, el Estado miembro que la inicia puede haber introducido un nombre o dirección incorrectos del prestador del servicio (o puede no haber facilitado esta información por carecer de ella). En tales casos, es importante rectificar la alerta inicial tan pronto como la información incorrecta salga a la luz.

## **9. ENVÍO DE INFORMACIÓN ADICIONAL**

Con vistas a minimizar el riesgo y garantizar una buena cooperación entre los Estados miembros, es importante que la información contenida en una alerta sea lo más completa posible y que los Estados miembros afectados dispongan de toda la información pertinente. Será especialmente importante ofrecer información adicional si puede ayudar a acelerar el cierre de la alerta o a hacer que los Estados miembros sean más conscientes de la existencia de un riesgo grave. De esta forma, el Estado miembro que envió la alerta y todos los demás Estados miembros implicados tendrán la posibilidad de ofrecer a los demás Estados miembros información de retorno o información adicional sobre las alertas, que estarán claramente relacionadas con el mensaje original de alerta. A continuación se recogen ejemplos al respecto:

- Los Estados miembros que han recibido la alerta quieren confirmar que el servicio en cuestión está siendo prestado efectivamente en su territorio, y que confirman o desmienten la información contenida en la alerta inicial sobre la base de sus observaciones/indicaciones.
- Los Estados miembros que han enviado o recibido la alerta quieren ofrecer información sobre las medidas que han tomado contra el prestador del servicio, de conformidad con el derecho comunitario, para reducir o eliminar el riesgo.

- Los Estados miembros que han recibido la alerta quieren solicitar información adicional del Estado miembro que envió la alerta, por ejemplo, si consideran que la información contenida en la alerta es poco clara o incompleta.
- Los Estados miembros que han recibido la alerta quieren decirles a los demás Estados miembros que, desde su punto de vista, podría cerrarse tal alerta porque creen que el riesgo no persiste ya (en su territorio).

Es importante evitar el envío de información repetitiva o irrelevante/poco importante sobre las alertas.

## **PARTE 2: MANUAL PARA EL USUARIO DEL MECANISMO DE ALERTA**

## 10. INTRODUCCIÓN

Este manual se ocupa de los **aspectos técnicos** del tratamiento de las alertas en el Sistema de Información del Mercado Interior (IMI). Detalla las distintas funciones que pueden desempeñar las autoridades y los usuarios y describe el uso de todas las herramientas que ofrece el sistema para cada fase del procedimiento. Además, explica cómo configurar el sistema para lograr un tratamiento eficaz de las alertas en cada Estado.

El manual se ciñe a los elementos del sistema **directamente relacionados con las alertas**. Para información de carácter general (registro en el IMI y acceso al mismo, intercambios de información a través del sistema, etc.), consulte los materiales disponibles en la web IMI. Recomendamos en particular:

- el **Manual del usuario** y
- los **módulos de formación interactivos** (en Adobe Captivate).

Los criterios y condiciones para el envío de las alertas se detallan en la primera parte del presente documento (“Orientaciones sobre el uso del mecanismo de alerta”).

## 11. PROCEDIMIENTO DE ALERTA EN EL SISTEMA IMI

### 11.1. Estructura modular del sistema

IMI es un sistema único de información constituido por **módulos** independientes para cada ámbito legislativo. Un módulo puede albergar uno o varios **procedimientos** (workflows). El módulo de la Directiva de servicios tiene dos procedimientos distintos, uno para el intercambio de información y otro para el mecanismo de alerta. El acceso a cada procedimiento está restringido a las autoridades específicamente registradas. Por consiguiente, las autoridades que gestionan las alertas deben tener acceso al sistema IMI, al módulo de servicios y al procedimiento de alerta.

### 11.2. Ciclo de vida de las alertas

El ciclo de vida básico de las alertas presenta cinco fases, determinadas por los agentes que intervienen.

- (1) Cualquier autoridad de un Estado miembro del Espacio Económico Europeo (EEE) que esté registrada en este procedimiento y tenga conocimiento de una actividad de servicios peligrosa en su ámbito de competencia está habilitada para **iniciar** una alerta y **presentarla** ante un coordinador de su propio país. El coordinador **verifica** la alerta y la **difunde** a otros Estados miembros.
- (2) En cada Estado miembro destinatario, un coordinador designado como “buzón de entrada de alertas” **acusa recibo** de la alerta en cuestión y la **emite** a los coordinadores y las autoridades de su propio país que estime oportuno. Los coordinadores pueden **añadir otros destinatarios**.

En el mecanismo de alerta del sistema IMI, las expresiones “*presentar*” y “*emitir*” siempre se refieren a actuaciones limitadas al ámbito de un único Estado miembro. A su vez, la “*difusión*” de las alertas alude al envío de información a otros Estados miembros.

- (3) El Estado miembro de establecimiento del prestador de servicios es el responsable de **gestionar el cierre** de la alerta una vez que el riesgo ha sido eliminado. Si se desconoce la identidad de dicho Estado, debe hacerse cargo del cierre el Estado miembro que inició la alerta.

Cualquier autoridad que haya recibido una alerta en el Estado miembro de establecimiento puede **iniciar una propuesta de cierre** y las demás autoridades de ese Estado que participen en la alerta pueden hacer **observaciones** sobre la propuesta. Tras llegar a un acuerdo, el coordinador designado como “**coordinador del cierre**” se ocupa de **difundir la propuesta de cierre** a los demás Estados miembros implicados en la alerta.

- (4) A continuación, los demás Estados miembros implicados pueden formular **objeciones al cierre** si tienen constancia de que el riesgo persiste. Se procede de la siguiente manera: las autoridades **presentan** sus objeciones ante un coordinador y este las **difunde** a los demás Estados miembros implicados.

Las autoridades del Estado miembro que propone el cierre de una alerta pueden hacer “*observaciones*” antes de que se difunda la propuesta. Después de la difusión de la propuesta, las autoridades de los demás Estados miembros pueden formular sus “*objeciones*” a la misma.

- (5) Cuando queda establecida la eliminación del riesgo, el coordinador designado en el Estado miembro de establecimiento puede **cerrar** la alerta.

Hasta el cierre de la alerta, todos los Estados miembros implicados tienen la posibilidad de añadir información adicional en cualquier fase del procedimiento.

## 12. AGENTES QUE INTERVIENEN Y FUNCIONES RESPECTIVAS

### 12.1. Funciones de las autoridades

Cuando las autoridades obtienen acceso al procedimiento de alerta, se les asigna la función de **autoridad** o de **coordinador**. Uno de los coordinadores queda designado como responsable del **buzón de entrada de alertas** de su Estado Miembro<sup>5</sup>. Estas funciones son independientes de las que puedan desempeñarse en otros ámbitos del sistema IMI. Así, por ejemplo, un coordinador nacional (NIMIC) puede intervenir como autoridad en el procedimiento de alerta y una autoridad que esté bajo la supervisión de un coordinador en el procedimiento de intercambio de información puede ser coordinador en el procedimiento de alerta.

---

<sup>5</sup> Para facilitar la coordinación y por motivos de protección de datos, la Comisión recomienda que cada Estado miembro cuente con un único buzón de entrada de alertas. No obstante, existe la posibilidad de designar varios buzones (por ejemplo, en un Estado de estructura federal).

### *12.1.1. Autoridades*

Las autoridades que intervienen en el procedimiento de alerta suelen ser competentes en campos como el medio ambiente o la salud y la seguridad de las personas. Están facultadas para **iniciar** alertas y **presentarlas** ante un coordinador con el que estén vinculadas. También pueden **recibir** las alertas emitidas por el “buzón de entrada” o por un coordinador y **reaccionar** ante ellas. Tienen capacidad para **presentar propuestas de cierre** y **hacer observaciones** sobre las propuestas de cierre procedentes de otras autoridades de su propio país. Si otro Estado miembro propone el cierre de una alerta, pueden **presentar objeciones** ante su coordinador.

### *12.1.2. Coordinadores*

La función de los coordinadores es garantizar que solo se difundan alertas cuando sea estrictamente necesario y que estas reciban un tratamiento adecuado. Los coordinadores suelen ser competentes en campos como el medio ambiente o la salud y la seguridad de las personas. Además, deben poseer una buena visión de conjunto de las estructuras administrativas pertinentes para el procedimiento de alerta en su propio Estado miembro. Los coordinadores están facultados para **difundir** alertas a otros Estados miembros y **añadir otros coordinadores y autoridades como destinatarios** de las alertas recibidas. Asimismo, pueden **difundir información adicional, propuestas de cierre** de las alertas y **objeciones al cierre** de una alerta propuesto por otro Estado miembro. Asimismo, los coordinadores pueden ejercer todas las funciones propias de una autoridad. Por ejemplo, pueden iniciar sus propias alertas y después difundirlas.

### *12.1.3. Coordinadores designados como “buzón de entrada de alertas”*

Los coordinadores designados como “buzón de entrada” centralizan la recepción de las alertas en su propio Estado miembro. Su función es **acusar recibo** de toda alerta de la que sean destinatarios y proceder a su **emisión inicial** a otros coordinadores y autoridades de su Estado miembro participantes en el procedimiento. La intervención del “buzón de entrada” garantiza que cada alerta se remita exclusivamente a los agentes capacitados para ocuparse de ella. Ello exige un buen conocimiento de las estructuras administrativas del propio país.

El “buzón de entrada” también **recibe automáticamente todas las alertas difundidas** desde su propio Estado miembro. Gracias a ello puede tener un panorama de conjunto del tráfico de alertas en ambos sentidos.

Además, el “buzón de entrada” tiene las mismas posibilidades de actuación que los coordinadores y las autoridades. Por ejemplo, puede iniciar sus propias alertas y después difundirlas.

### *12.1.4. Aprobación definitiva de las alertas*

El sistema IMI permite a los Estados miembros cierto grado de flexibilidad a la hora de definir la relación entre coordinadores y autoridades. Los coordinadores (incluidos aquellos que actúan como “buzón de entrada”) pueden quedar habilitados para **modificar o eliminar el contenido** de las alertas que se les presentan y de cualquier otra información relacionada con las mismas. Para ello, en los **parámetros del procedimiento de alerta** debe marcarse la casilla que indica que el coordinador se reserva la **“autorización definitiva”** de las alertas que difunde en nombre de su Estado miembro.

En caso contrario, la autoridad que inició la alerta retiene esa capacidad.

## 12.2. Funciones de los usuarios

Cuando una autoridad obtiene acceso al procedimiento de alerta del módulo de servicios del sistema, su **administrador local de datos** (responsable del registro de otros usuarios y de la gestión de los datos relativos a su propia autoridad) recibe automáticamente todos los derechos de usuario<sup>6</sup>. Ello le permite asignar a sus compañeros los derechos de usuario oportunos en función del tamaño de la autoridad y de las responsabilidades de estos dentro del procedimiento.

### 12.2.1. Visualizador

El “visualizador” puede **ver el contenido completo de todas las alertas** a las que tiene acceso su autoridad (esto incluye los datos personales que figuran en las mismas). Aunque se le permite guardar o imprimir dicho contenido, **no está autorizado para intervenir en el procedimiento**. Es decir, no puede iniciar o actualizar alertas, ni proponer su cierre.

### 12.2.2. Gestor

El “gestor” se ocupa de las alertas en nombre de su autoridad. Entre sus cometidos están los siguientes: **iniciar** alertas y **presentarlas** ante un coordinador para que sean difundidas; **recibir** alertas y **reaccionar** ante ellas; **presentar y solicitar información adicional** sobre las alertas; presentar propuestas de cierre, hacer observaciones sobre las propuestas de cierre presentadas por otras autoridades de su propio Estado miembro y formular objeciones a las propuestas de cierre procedentes de otro Estado miembro. Conviene aclarar que los gestores de una autoridad que actúe como coordinador **no pueden difundir ni emitir** alertas.

### 12.2.3. Emisor

La función de “emisor” está reservada a los usuarios de los coordinadores. Su cometido es la **emisión** de alertas dentro de su propio Estado miembro y la **difusión** de alertas e información conexa a otros Estados miembros. En los coordinadores que actúan como “buzón de entrada”, el emisor es el encargado de **acusar recibo** de las alertas y proceder a su emisión inicial a los coordinadores y autoridades del propio país. En los demás coordinadores, el emisor decide si hay **otras autoridades** de su ámbito territorial o competencial que deben recibir la alerta.

Los emisores de todos los coordinadores están habilitados para **difundir** nuevas alertas a otros Estados miembros, presentar y difundir información adicional sobre las alertas en curso y difundir la retirada de las alertas, las propuestas de cierre y las objeciones a dichas propuestas.

En los coordinadores con capacidad de **autorización definitiva**, los emisores pueden **modificar o eliminar las alertas** y cualquier información conexa antes de su difusión.

### 12.2.4. Usuario básico

Todos los usuarios de una autoridad activa en el procedimiento de alerta que no sean administradores locales de datos, ni desempeñen las funciones específicas descritas más arriba, reciben automáticamente un acceso básico a las alertas. Esto les permite obtener un **resumen general** de todas las alertas recibidas o cursadas por la autoridad a la que pertenecen, pero no les

---

<sup>6</sup> Si hay varios administradores locales de datos en una misma autoridad, todos ellos reciben la totalidad de los derechos de usuario para el procedimiento de alerta.

autoriza a visualizar su contenido completo. Dichos usuarios **no pueden** iniciar nuevas alertas ni **intervenir** en las que ya están en curso.

Este es también el acceso por defecto asignado a todos los usuarios que ya participan en el procedimiento de intercambio de información del módulo de servicios. Así, por ejemplo, un usuario “gestor” en dicho procedimiento recibe automáticamente los derechos de usuario básico en el procedimiento de alerta. Si es necesario, este usuario puede asumir otra función más activa en relación con las alertas y combinarla con la de gestor en el intercambio de información.

#### 12.2.5. Funciones combinadas

El sistema IMI permite asignar más de una función a un mismo usuario. Así, por ejemplo, un “emisor” dentro de un coordinador también puede desempeñar las funciones propias del “gestor”, lo que le habilita para **iniciar, presentar y difundir alertas**.

Ahora bien, debe tenerse en cuenta que la presentación y la difusión de alertas son **fases independientes** que deben realizarse por separado, aunque sea la misma persona quien las lleve a cabo.

#### Diferencias entre “gestor” y “emisor” de alertas – ¿Quién puede hacer qué?

		<b>Gestor</b> <i>(en autoridades y coordinadores)</i>	<b>Emisor</b> <i>(solo en coordinadores)</i>
<b>Iniciar una alerta</b>	Presentar	√	
	Difundir		√
<b>Enviar y solicitar información adicional</b>	Presentar	√	√
	Difundir		√
<b>Retirar una alerta</b> <i>(autoridad y coordinador iniciadores exclusivamente)</i>	Presentar	√	
	Difundir		√

		<b>Gestor</b> <i>(en autoridades y coordinadores)</i>	<b>Emisor</b> <i>(solo en coordinadores)</i>
<b>Proponer el cierre de una alerta</b> <i>(EM de establecimiento exclusivamente)</i>	Presentar	√	
	Hacer observaciones	√	√
	Difundir		√
<b>Formular objeciones a una propuesta de cierre</b>	Presentar	√	√
	Difundir		√
<b>Cerrar una alerta</b> <i>(coordinador difusor de la propuesta de cierre exclusivamente)</i>			√

### 13. TRATAMIENTO DE LAS ALERTAS EN EL IMI

Las alertas tienen un **ciclo de vida** bien definido, consistente en una serie de etapas básicas (véase el apartado 2.2) a las que pueden añadirse otras opcionales en determinados casos. Cuando la alerta pasa de una etapa a otra, su **estado** queda automáticamente actualizado y se muestra en pantalla.

#### 13.1. Envío de las alertas

##### 13.1.1. Inicio y presentación

Todo “gestor” de una autoridad o coordinador puede iniciar alertas. Para hacerlo, primero debe comprobar si se cumplen las condiciones recogidas en una **lista de criterios** (para saber más sobre dichos criterios, véase la Parte 1 del presente documento). El sistema guía paso a paso al usuario para completar este proceso. Si se cumplen todos los criterios, el “gestor” puede introducir los **datos del prestador de servicios** causante del riesgo potencial, junto con la **descripción del caso**. Además, puede adjuntar la documentación oportuna. A continuación, en la lista de coordinadores vinculados a su autoridad **selecciona el coordinador responsable** de la difusión de la alerta y después indica los **Estados miembros destinatarios** de la misma. En caso necesario, también puede especificar en un campo de texto libre todas aquellas autoridades de los Estados miembros destinatarios que, a su juicio, deban ser alertadas.

En cualquier momento de la introducción de datos se puede guardar un borrador. Al hacerlo, el sistema asigna un **número** a la alerta, cuyo estado en esta fase es:

#### “Borrador de alerta”

Tras completar todos los pasos, el “gestor” **presenta** la alerta ante el coordinador seleccionado. La alerta pasa al estado:

### “Alerta presentada para difusión”

#### *13.1.2. Difusión*

El sistema envía una notificación automática a todos los “emisores” del coordinador seleccionado para informarles de que han recibido una alerta para difusión.

Si consideran que su autoridad no es competente para pronunciarse al respecto, pueden **remitir** la alerta a otro coordinador.

En el momento en que un “emisor” acepta la alerta, esta pasa al estado:

### “Alerta pendiente de difusión”

El “emisor” debe **verificar** que realmente se cumplan todos los criterios y la información proporcionada sea correcta y completa.

En los coordinadores con capacidad de “**autorización definitiva**”, el “emisor” puede **modificar el contenido** de la alerta e incluso **eliminarla** si decide no proceder a su envío.

Si el coordinador carece de dicha capacidad y el “emisor” detecta que falta información importante en la alerta, puede ponerse en contacto por un canal exterior al sistema con la autoridad que la inició y pedirle que la modifique. Si el “emisor” llega a la conclusión de que no procede el envío de la alerta, puede pedir a la autoridad que la elimine.

Con independencia de la “autorización definitiva”, cualquier “emisor” puede **añadir más Estados miembros a la lista de destinatarios de la alerta** si considera posible que el riesgo también se extienda a ellos.

Cuando el “emisor” tiene la certeza de que la alerta está lista, la **difunde** a los Estados miembros seleccionados. Por defecto, toda alerta se envía asimismo a la Comisión, en cumplimiento de lo establecido en la Directiva de servicios.

Llegado este punto, el procedimiento entra en la fase de “**Alerta difundida**”.

## **13.2. Modificación y rectificación de las alertas**

La modificación o rectificación del contenido de una alerta ya difundida es potestad exclusiva del Estado miembro que la inició. En función de los datos que vaya recibiendo sobre el objeto de la alerta, dicho Estado puede:

- incorporar nuevos **Estados miembros destinatarios**
- cambiar el **Estado miembro de establecimiento** del prestador de servicios<sup>7</sup>
- actualizar los **datos del prestador de servicios** y

---

<sup>7</sup> A condición de que no haya una propuesta de cierre pendiente.

- modificar la **descripción del caso**.

El coordinador que difundió la alerta es el único habilitado para incorporar nuevos Estados miembros destinatarios y modificar el Estado miembro de establecimiento. Si dicho coordinador tiene capacidad de “autorización definitiva”, también puede modificar los datos del prestador de servicios y la descripción del caso. De lo contrario, solo puede hacerlo la autoridad iniciadora de la alerta.

Los cambios **se aplican automáticamente** a la alerta y son **inmediatamente visibles** para todos los destinatarios, sin que sea precisa una nueva difusión.

La modificación del Estado miembro de establecimiento se notifica automáticamente por correo electrónico a todos los destinatarios de la alerta.

### 13.3. Retirada de las alertas

A pesar de los mecanismos de control con que cuenta el sistema, un Estado miembro puede enviar una alerta sobre la base de información o indicios incorrectos o imprecisos y descubrir el error pasado un tiempo. En tales casos, debe proceder a la **retirada** de la alerta. La alerta puede retirarse en cualquier fase de su ciclo de vida mediante un procedimiento que, como el de envío, consta de dos etapas. En primer lugar, la autoridad iniciadora **presenta una propuesta de retirada** y el estado de la alerta pasa a “**Retirada remitida para difusión**”.

A continuación el coordinador **difunde la retirada** (pulsando el botón que se encuentra en la pestaña “**Gestión de la retirada**”). A partir de ese momento, la alerta deja de estar activa y ya no es posible incorporar nueva información. En este estado de “**Alerta retirada**” los destinatarios todavía pueden visualizar un extracto de su contenido.

### 13.4. Gestión de destinatarios

#### 13.4.1. Acuse de recibo

Las alertas difundidas se transmiten a los “buzones de entrada” de los Estados miembros destinatarios y a la Comisión Europea<sup>8</sup>.

En cada “buzón de entrada” el **acuse de recibo** de las alertas es competencia de los “emisores”, quienes reciben una notificación automática por correo electrónico a cada llegada de una nueva “**Alerta pendiente de acuse de recibo**”.

#### 13.4.2. Emisión de las alertas

La **emisión inicial** de las alertas recibidas compete asimismo a los “emisores” del “buzón de entrada”. Estos seleccionan los coordinadores y autoridades para quienes la alerta es pertinente y se la hacen llegar. Existe la posibilidad de que el Estado miembro iniciador **haya sugerido autoridades** destinatarias. En tal caso, los “emisores” pueden incluirlas en la lista correspondiente si son de la misma opinión.

---

<sup>8</sup> Por motivos de protección de datos, la Comisión no puede visualizar la información personal que contienen las alertas.

Los “emisores” de los coordinadores que reciben la alerta pueden **añadir más destinatarios**.

Una vez emitida la alerta, los “emisores” de los “buzones de entrada” son los únicos autorizados para **suprimir destinatarios**, a condición de que estos no hayan realizado ninguna actuación en relación con la alerta. Esta situación puede producirse cuando un destinatario determine que la alerta recibida no es pertinente para su autoridad y lo ponga en conocimiento del “buzón de entrada”. Al ser retirada de la lista de destinatarios, la autoridad deja de recibir información relacionada con las etapas posteriores del ciclo de vida de la alerta.

La **emisión** de la alerta también se lleva a cabo **en el Estado miembro que la inició**. El “buzón de entrada” del Estado iniciador recibe automáticamente todas las alertas cursadas. Tras la difusión de la alerta, el “buzón de entrada” del Estado iniciador puede seleccionar **destinatarios adicionales** dentro de su propio país y hacerles llegar la alerta.

### 13.5. Envío y solicitud de información adicional

En todo momento del ciclo de vida de una alerta, cualquier Estado miembro implicado puede **añadir información** a la misma, por ejemplo para informar a los demás Estados miembros destinatarios de las medidas que haya adoptado contra el prestador de servicios de que se trate (más ejemplos en la Parte 1 del presente documento). Esta función también puede utilizarse para sugerir el cierre de la alerta al Estado miembro responsable. Asimismo, los Estados miembros destinatarios pueden **solicitar información adicional** al Estado miembro iniciador de la alerta o a cualquier otro Estado miembro que ya haya aportado alguna información.

El envío y solicitud de información adicional se lleva a cabo **en dos etapas**. En primer lugar, un “gestor” o “emisor” envía la información a un coordinador, quien la comprueba y difunde (dentro del coordinador, esta tarea compete a un usuario con perfil de “emisor”).

A continuación, el sistema notifica automáticamente por correo electrónico la incorporación de información adicional a todos los “gestores” y “emisores” de las autoridades implicadas en la alerta.

### 13.6. Cierre de las alertas

Como se explica en las orientaciones del mecanismo de alerta, la puesta en marcha del proceso de cierre compete al **Estado miembro en el que esté establecido el prestador de servicios** y debe producirse inmediatamente después de la eliminación del riesgo.

Si el Estado miembro de establecimiento es **desconocido**, el cierre de la alerta pasa a ser responsabilidad del Estado miembro que la inició.

El cierre de las alertas se lleva a cabo en dos fases:

- En la primera fase, todas las autoridades del Estado miembro de establecimiento pueden pronunciarse sobre la conveniencia de proponer el cierre a los demás Estados miembros (= **periodo de formulación de observaciones**).
- En la segunda fase, posterior a la difusión de la propuesta de cierre, todos los demás Estados miembros implicados tienen la posibilidad de oponerse al cierre si consideran que la alerta debe permanecer activa (= **periodo de presentación de objeciones**).

### 13.6.1. Propuesta de cierre

Los “gestores” de las autoridades destinatarias del Estado miembro de establecimiento pueden **proponer el cierre de una alerta** si tienen constancia de que el riesgo ha dejado de existir. La propuesta puede presentarse ante cualquier coordinador vinculado con la autoridad, que se convierte de este modo en “**coordinador del cierre**”.

Cuando se **presenta una propuesta de cierre**, el sistema notifica por correo electrónico a las demás autoridades receptoras de la alerta en el Estado miembro de establecimiento que pueden incorporar sus observaciones a la misma. Esto sucede de forma automática y sin intervención alguna por parte del “coordinador del cierre”. Ahora bien, si el coordinador tiene capacidad de “autorización definitiva”, ello le habilita para modificar o eliminar la propuesta de cierre en todo momento.

La fase de formulación de observaciones se circunscribe a un único Estado miembro, motivo por el cual no se realiza una segunda etapa que exija la intervención de un coordinador.

En esta fase, la alerta pasa al estado “**Propuesta de cierre abierta a observaciones**”.

### 13.6.2. Observaciones sobre la propuesta de cierre

La propuesta de cierre debe permanecer **abierta a observaciones** procedentes del Estado miembro de establecimiento durante un periodo de tiempo fijado de común acuerdo por todos los Estados miembros. Durante ese periodo, la propuesta todavía puede ser **modificada o anulada** por la autoridad que la presentó (o bien por el “coordinador del cierre”, si tiene capacidad de “autorización definitiva”).

El sistema notifica por correo electrónico a los “emisores” del “coordinador del cierre” la expiración del plazo para formular observaciones. A partir de ese momento, no pueden incorporarse comentarios adicionales. Sin embargo, la **propuesta de cierre todavía puede ser modificada o anulada**. En esta fase, la alerta pasa al estado “**Propuesta de cierre pendiente de difusión**”.

### 13.6.3. Difusión de la propuesta de cierre

Llegado este punto, un “emisor” del “coordinador del cierre” **evalúa todas las observaciones** recibidas y determina si procede difundir la propuesta de cierre a los demás Estados miembros.

Si el “emisor” llega a la conclusión de que la alerta debe permanecer activa, puede **anular la propuesta de cierre** siempre y cuando el coordinador al que pertenece tenga capacidad de “autorización definitiva”. De lo contrario, debe pedir la anulación a la autoridad que planteó la propuesta de cierre.

Si el “emisor” decide que la alerta debe cerrarse, **difunde la propuesta** (pulsando el botón que se encuentra en la pestaña “Gestión del cierre”). Además, puede optar por **incluir en la propuesta todas o algunas de las observaciones** recibidas en su Estado miembro. La difusión genera una notificación automática por correo electrónico en la que se anuncia la propuesta de cierre a todos los “gestores” y “emisores” que hayan recibido la alerta en los Estados miembros implicados. En esta fase, la alerta pasa al estado “**Propuesta de cierre abierta a objeciones**”.

#### *13.6.4. Objeciones a la propuesta de cierre*

Los Estados miembros implicados que tengan constancia de que el riesgo persiste pueden oponer **objeciones** al cierre de la alerta.

El plazo para la presentación de objeciones también se fija de común acuerdo con todos los Estados miembros. Durante ese periodo los “gestores” y “emisores” de las autoridades y los coordinadores participantes pueden **presentar objeciones** ante un coordinador, utilizando para ello la **función de información adicional** denominada “Objeción a una propuesta de cierre”.

Al igual que ocurre con cualquier otro tipo de información adicional, la presentación y difusión de las objeciones **se lleva a cabo en dos etapas**. Un “emisor” del coordinador ante el que se presenta la objeción decide si procede su **difusión** a otros Estados miembros. Al efectuarse la difusión, el sistema notifica la objeción por correo electrónico a todos los destinatarios de la alerta en los demás Estados miembros.

El sistema notifica por correo electrónico a los “emisores” del “coordinador del cierre” en el Estado miembro de establecimiento la expiración del plazo para formular objeciones.

#### *13.6.5. Cierre de la alerta*

El “coordinador del cierre” en el Estado miembro de establecimiento decide si procede cerrar la alerta, teniendo en consideración las posibles objeciones recibidas de otros Estados miembros. Los “emisores” del “coordinador del cierre” son los únicos usuarios habilitados para **cerrar una alerta**.

En esta fase, la alerta pasa al estado “**Alerta cerrada**”.

Tras el cierre de una alerta, los usuarios del sistema pueden seguir visualizando una cantidad limitada de datos, que incluyen:

- un extracto de la alerta sin datos personales
- la lista de destinatarios
- el historial de las actuaciones.

A los seis meses del cierre, todos los datos personales se suprimen automáticamente del sistema.

Cualquier Estado miembro que tenga la convicción de que el riesgo no se ha eliminado, a pesar del cierre de la alerta por el Estado miembro de establecimiento, puede **iniciar otra una nueva alerta**.

## **14. SEGUIMIENTO DE LAS ALERTAS**

### **14.1. Notificaciones por correo electrónico**

El sistema envía notificaciones automáticas a todas las partes implicadas cada vez que se puede **intervenir** en relación con una alerta o se recibe **nueva información**. Los mensajes se envían exclusivamente a las direcciones de los usuarios con el perfil adecuado en el procedimiento de alerta. Por lo tanto, es fundamental la consulta frecuente de las direcciones electrónicas registradas en el sistema.

Las notificaciones, que se ajustan a un modelo estándar, no contienen información sobre el contenido de la alerta, ni los datos personales del prestador de servicios en cuestión.

## 14.2. Lista de alertas

Todo usuario con acceso al procedimiento de alerta puede consultar la lista de las alertas en las que participa su autoridad, en la que figura la siguiente información:

- número de alerta
- actividad afectada
- Estado miembro de establecimiento del prestador de servicios
- autoridad iniciadora de la alerta
- estado actual de la alerta
- fecha de difusión.

El sistema permite realizar **búsquedas** sobre el contenido de la lista, aplicando diversos criterios. Además, el acceso a la lista puede efectuarse a través de la opción “Buscar alertas”.

Los usuarios habilitados para hacerlo pueden abrir las alertas desde esta lista y realizar las actuaciones oportunas.

## 14.3. Impresión de las alertas

Es probable que las autoridades y los coordinadores participantes en el procedimiento quieran **llevar un registro** de las alertas enviadas y recibidas a través del sistema. Para ello, pueden generar e imprimir informes en cualquier fase del ciclo de vida de la alerta, a partir del momento en que se crea un borrador.

Todo usuario puede imprimir informes con el nivel de detalle que está autorizado a visualizar en pantalla. Por lo tanto, los usuarios básicos solo pueden imprimir un resumen general de las alertas (que contiene la lista de destinatarios y el historial), mientras que los “visualizadores” y los “gestores” tienen la posibilidad de imprimir su contenido completo.

Tras la retirada o el cierre de una alerta, solo puede imprimirse el extracto de la misma que permanece visible en pantalla.

Cualquier tratamiento posterior de los documentos impresos debe hacerse con arreglo a las normativas nacionales y europea en materia de protección de datos.

## 15. ALERTAS Y PROTECCIÓN DE DATOS

El intercambio de información en el marco del procedimiento de alerta del IMI resulta **necesario para cumplir una obligación legal** y, por lo tanto, es plenamente lícito desde el punto de vista de la protección de datos. Sin embargo, la Comisión es consciente de sus consecuencias y ha hecho todo lo posible para concebir un procedimiento que facilite la protección de datos. Además, insta a los Estados miembros —responsables de aplicar la legislación sobre protección de datos al enviar o

recibir las alertas— a que **permanezcan vigilantes** en cuanto a la correcta utilización de la normativa en la materia.

El mecanismo de alerta está dotado de una serie de **garantías de protección de datos**:

- El **acceso** a los datos está **reservado** a las autoridades específicamente facultadas.
- La lista de comprobación para crear un borrador de alerta y el procedimiento de envío en dos etapas con intervención de un coordinador **impiden que se produzcan alertas innecesarias**.
- El Estado que inicia la alerta selecciona los Estados miembros destinatarios. Esta circunstancia, unida al hecho de que el “buzón de entrada” determine qué autoridades deben recibir la alerta en su propio Estado miembro, garantiza que el intercambio **se limite a lo necesario** para cumplir los requisitos de información.
- Tal y como prevé la Directiva de servicios, la **Comisión** recibe todas las alertas cursadas. Sin embargo, solo puede visualizar un extracto de su contenido y **carece de acceso a los datos personales**.
- El mecanismo prevé la rápida **retirada** de las alertas infundadas que pudieran enviarse a pesar de todas estas precauciones. Además, permite **rectificar o suprimir** los datos incorrectos.
- Las alertas **se cierran en el momento en que el riesgo deja de existir**. Al cerrarse la alerta, se interrumpe inmediatamente el acceso de los usuarios a los datos. A los seis meses del cierre, los datos personales se suprimen del sistema.

Encontrará más información sobre la protección de datos en el contexto del mecanismo de alerta y del IMI en general en el informe de la Comisión sobre la situación de la protección de datos en el Sistema de Información del Mercado Interior y la Recomendación de la Comisión sobre directrices para la protección de datos en dicho sistema<sup>9</sup>.

## **16. INFORMACIÓN ADICIONAL PARA LOS COORDINADORES – CÓMO ESTABLECER LA ESTRUCTURA QUE REQUIERE EL MECANISMO DE ALERTA EN CADA PAÍS**

### **16.1. Registro inicial por la Comisión**

El único requisito del sistema para que los Estados miembros hagan uso del mecanismo es la existencia de una autoridad registrada que actúe como “**buzón de entrada de alertas**”. Cuando el mecanismo entró en funcionamiento, la Comisión registró en el sistema los “**buzones de entrada de alertas**” de todos los Estados miembros (en los casos en los que se trataba de autoridades ya registradas, les otorgó esa función tras habilitar su acceso a las alertas).

El posterior registro de coordinadores y autoridades adicionales en el procedimiento de alerta compete a los Estados miembros.

Por definición, dentro del IMI los coordinadores nacionales (NIMIC) y los supercoordinadores delegados (SDIMIC) son **plenamente responsables** en su espacio geográfico de todos los ámbitos legislativos y los procedimientos asociados. Por consiguiente, la Comisión les ha brindado acceso al

---

<sup>9</sup> C(2009) 2041final. DO L 100 de 18.4.2009, p. 12.

procedimiento de alerta para que puedan **ampliar dicho acceso a las autoridades de sus respectivos países**.

Sin embargo, esta **función administrativa** de los NIMIC y SDIMIC no determina su actuación en cuanto al **contenido de las alertas**. De hecho, pueden desempeñar cualquiera de las funciones descritas en el apartado 3.1, dependiendo de sus competencias y de la estructura administrativa del propio país.

## 16.2. Registro de autoridades y acceso al procedimiento de alerta

El registro y acceso de los **coordinadores** es competencia de los:

- NIMIC
- SDIMIC
- LIMIC (coordinadores de ámbito legislativo en el marco de la Directiva de servicios)<sup>10</sup>.

El registro y acceso de las **autoridades** es competencia de los:

- NIMIC
- SDIMIC
- LIMIC
- DIMIC (coordinadores delegados).

En otras palabras, los DIMIC no están capacitados para registrar coordinadores.

Al registrar un coordinador en el sistema es importante establecer si tendrá capacidad de **“autorización definitiva”** en el procedimiento de alerta (es decir, si podrá modificar o eliminar el contenido de la información que le presente una autoridad).

Los **accesos al procedimiento de alerta y al ámbito legislativo** de los servicios se otorgan **por separado**. Por consiguiente, para intervenir en las alertas toda nueva autoridad debe:

1. estar registrada en el sistema
2. tener acceso al ámbito legislativo de los servicios
3. tener acceso al procedimiento de alerta.

---

<sup>10</sup> El LIMIC es un coordinador con competencia global sobre un ámbito legislativo. En cada Estado miembro solo puede haber un LIMIC por ámbito legislativo.

### **16.3. Autoridades y coordinadores vinculados**

Cuando una **autoridad** obtiene acceso al procedimiento de alerta, debe quedar **vinculada**, como mínimo, a un **coordinador** de su propio país. Con posterioridad, pueden añadirse otros coordinadores vinculados o poner fin a dicha relación.

Es fundamental que la selección de coordinadores vinculados sea la correcta, ya que las autoridades **solo pueden presentar información relativa a las alertas ante dichos coordinadores.**

Por su parte, los coordinadores pueden **emitir alertas a cualquier autoridad o coordinador** de su propio país, con independencia de que estén vinculados o no.