# I. DISPOSICIONES GENERALES

## MINISTERIO DE INDUSTRIA, TURISMO Y COMERCIO

**1771** *Orden ITC/110/2009, de 28 de enero, por la que se determinan los requisitos y las especificaciones técnicas que resultan necesarios para el desarrollo del capítulo II del título V del reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios, aprobado por Real Decreto 424/2005, de 15 de abril.*

La presente orden tiene por objeto desarrollar algunos aspectos generales del capítulo II del título V del Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios, aprobado por Real Decreto 424/2005, de 15 de abril.

Lo dispuesto en esta orden se entiende sin perjuicio de las órdenes ministeriales relativas a las obligaciones específicas derivadas de la aplicación de una concreta tecnología de telecomunicaciones que se aprueben previo informe de la comisión interministerial creada por Orden PRE/1575/2006, de 19 de mayo, para la elaboración del informe previo a la aprobación de las órdenes ministeriales que se dicten de conformidad con lo establecido en la disposición transitoria sexta del Reglamento sobre condiciones para la prestación de servicios de comunicaciones electrónicas, servicio universal y la protección de los usuarios, aprobado por Real Decreto 424/2005, de 15 de abril.

Los artículos 95 y 98 de este Reglamento facultan al Ministerio de Industria, Turismo y Comercio para establecer reglamentariamente determinadas especificaciones técnicas. Asimismo, la disposición final quinta del Real Decreto 424/2005, de 15 de abril, autoriza al Ministro de Industria, Turismo y Comercio a dictar las disposiciones necesarias para el desarrollo y aplicación de este real decreto.

De conformidad con lo establecido en la disposición adicional quinta de la Ley 32/2003, de 3 noviembre, General de Telecomunicaciones, esta orden ha sido conocida e informada por el Consejo Asesor de las Telecomunicaciones y de la Sociedad de la Información, lo que equivale a la realización del trámite de audiencia regulado por el artículo 24.1.c) de la Ley 50/1997, de 27 de noviembre, del Gobierno.

Por otra parte, la orden que se aprueba ha sido objeto del informe preceptivo de la Comisión del Mercado de las Telecomunicaciones previsto en el artículo 48.3.h) de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones.

En su virtud, con la aprobación previa de la Ministra de Administraciones Públicas, dispongo:

Artículo 1. *Objeto.*

1. Constituye el objeto de esta orden la determinación de los requisitos y de las especificaciones técnicas para la ejecución de lo previsto en el capítulo II del título V del Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios, aprobado por Real Decreto 424/2005, de 15 de abril.

2. Lo dispuesto en esta orden se entiende sin perjuicio de las órdenes ministeriales, relativas a las obligaciones específicas derivadas de la aplicación de una concreta tecnología de telecomunicaciones, que se aprueben previo informe de la comisión interministerial creada por Orden PRE/1575/2006, de 19 de mayo, para la elaboración del informe previo a la aprobación de las órdenes ministeriales que se dicten de conformidad con lo establecido en la disposición transitoria sexta del Reglamento sobre condiciones para la prestación de servicios de comunicaciones electrónicas, servicio universal y la protección de los usuarios, aprobado por Real Decreto 424/2005, de 15 de abril, en materia de interceptación legal de comunicaciones electrónicas.

cve: BOE-A-2009-1771

Artículo 2. *Cumplimiento de las obligaciones de proveer la interceptación legal de las comunicaciones y de colaboración con los sujetos obligados.*

1. En desarrollo del artículo 85 del Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios, se establecen las siguientes reglas:

a) Cuando el sujeto obligado ofrezca servicios de comunicaciones electrónicas a través de redes de comunicaciones de las que no sea titular o a través de otros proveedores de servicios y sea necesaria la colaboración de éstos para satisfacer sus obligaciones relativas a la interceptación legal de las comunicaciones de sus abonados y usuarios, deberá llegar a un acuerdo con los mismos para el cumplimiento de estas obligaciones.

b) Un sujeto obligado podrá llegar a un acuerdo con otro operador para la realización de las interceptaciones legales de las comunicaciones de sus abonados y usuarios aún cuando no sea necesaria su colaboración, siempre y cuando sea técnicamente posible y se satisfagan los requisitos establecidos en la legislación sobre la interceptación legal de comunicaciones.

c) Sin perjuicio de lo establecido en la disposición transitoria segunda de esta orden, cuando el sujeto obligado tenga la condición de operador pequeño, de conformidad con la definición establecida en el apartado dd) del apéndice, y no se acoja a la posibilidad enunciada en el párrafo anterior, en lugar de usar una infraestructura permanente para realizar la interceptación legal, podrá optar por utilizar sistemas no permanentes propios o compartidos con otros operadores que tengan la misma condición, según el estado de la tecnología en cada momento. Para ello las características técnicas y el procedimiento de interceptación a seguir deberán haber sido aprobados por los agentes facultados.

Para el cálculo de la capacidad que debe tener este sistema no permanente se emplearán las fórmulas establecidas en el artículo 15, considerando el factor «x» igual a la suma de los abonados y usuarios de los operadores pequeños que compartan los medios técnicos que formen el sistema no permanente antes citado. Esta opción no exime del cumplimiento del resto de las disposiciones establecidas en esta orden, ni de la adopción de las medidas necesarias para garantizar la seguridad de la interceptación legal de las comunicaciones.

d) Los acuerdos a los que hacen referencia las reglas a) y b) de este artículo deberán ser notificados a los agentes facultados en un plazo máximo de 15 días desde su adopción. Estos acuerdos deberán celebrarse en condiciones transparentes, objetivas y no discriminatorias.

e) Cuando un sujeto obligado tenga previsto dejar de hacer uso de alguna de las facultades previstas en las reglas b) y c) de este artículo, deberá notificarlo previamente, con al menos 15 días de antelación, a los agentes facultados.

f) Los sujetos obligados y sus colaboradores adoptarán las medidas necesarias para que, en ningún caso, la colaboración entre operadores para la provisión de la interceptación legal de comunicaciones suponga menoscabo alguno de la seguridad de las mismas.

2. A los efectos de este artículo no tendrán la condición de sujetos obligados los operadores habilitados para prestar servicios de información telefónica cuando se limiten a la prestación del servicio de consulta sobre números de abonado.

Artículo 3. *Comunicación de información relacionada con la interceptación legal entre sujetos obligados.*

1. La información relacionada con el mandamiento de la interceptación legal de comunicaciones que se intercambie entre sujetos obligados, se limitará a la estrictamente necesaria para satisfacer las necesidades derivadas de la obligación de colaborar entre operadores para la realización de la interceptación legal de comunicaciones. Los sujetos obligados garantizarán en todo momento la confidencialidad de la información transmitida o almacenada, no pudiendo ser utilizada para ningún otro fin.

cve: BOE-A-2009-1771

2. Las órdenes de interceptación y cualquier otra información importante para la seguridad del sistema de interceptación, debe transmitirse mediante un canal seguro, según se define en el apéndice de esta orden.

Artículo 4. *Especificaciones técnicas.*

1. La realización técnica de los sistemas de interceptación legal de los sujetos obligados se ajustará a lo que establezcan las especificaciones técnicas sobre interceptación legal elaboradas por el Instituto Europeo de Normalización de Telecomunicaciones (ETSI) y el Proyecto de Asociación de Tercera Generación (3GPP).

2. La referencia a las especificaciones técnicas que serán de aplicación para cada tecnología concreta, junto con la determinación de los correspondientes parámetros optativos nacionales, las observaciones pertinentes para facilitar su cumplimiento y el plazo máximo para su implantación se publicará mediante órdenes del Ministerio de Industria, Turismo y Comercio, previo informe de la comisión interministerial creada por la Orden PRE/1575/2006, de 19 de mayo.

3. Sin perjuicio de lo dispuesto en los apartados anteriores de este artículo, en el diseño y en la realización del sistema de interceptación se procurará el empleo de estándares abiertos, a fin de garantizar la interoperabilidad entre equipos de diferentes suministradores, y el empleo de sistemas operativos y software de código abierto en el sistema de interceptación.

Artículo 5. *Bloques funcionales e interfaces del sistema de interceptación legal.*

1. Conforme a las especificaciones del ETSI y del 3GPP sobre interceptación legal de las comunicaciones, los bloques funcionales y las interfaces del sistema de interceptación legal que ha de tener el sujeto obligado se muestran en la figura del anexo I de esta orden.

2. La definición de cada bloque funcional y cada interfaz se encuentra en el apéndice de esta orden.

3. Los sujetos obligados deberán garantizar la disponibilidad, instalación y mantenimiento, en el ámbito de la presente orden, de los elementos del sistema de interceptación legal correspondientes a su infraestructura (IIF), la función de mediación (MF) y la función de administración (ADMF).

4. Los sujetos obligados deberán permitir a los agentes facultados la instalación y mantenimiento de los elementos de seguridad que los agentes facultados consideren oportunos para la protección de todas y cada una de las interfaces de comunicación (HI), siempre y cuando se garantice por parte de éstos la total inocuidad de estos equipos en la prestación del servicio por parte de los sujetos obligados. La instalación y mantenimiento de dichos equipos correrá a costa de los agentes facultados.

Artículo 6. *Canales para la interfaz HI1.*

1. La interfaz de administración HI1 es una interfaz bidireccional entre el agente facultado y el sujeto obligado para el intercambio de información de administración. Se utiliza para intercambiar información, diversa y poco normalizada, que incluye desde las órdenes de interceptación hasta la resolución de incidencias técnicas.

2. El sujeto obligado tendrá disponibles los siguientes canales para la interfaz HI1:

a) Canales no seguros: No se podrán utilizar nunca para transmitir datos personales, contenidos de comunicaciones, ni cualquier otro dato que pueda comprometer la seguridad de las interceptaciones legales de comunicaciones, en cuyo caso es obligatorio el uso de un canal seguro. Cuando sea necesario referirse a una orden de interceptación legal concreta, a través de un canal no seguro, se utilizará el identificador de interceptación legal (LIID) o algún otro procedimiento que permita hacer referencia a la orden sin desvelar su contenido.

b) Un canal seguro electrónico: Éste será único para cada agente facultado, sin perjuicio de la redundancia que pueda exigir el requisito de disponibilidad. El canal seguro

cve: BOE-A-2009-1771

electrónico para la interfaz HI1 se ajustará a las especificaciones establecidas en el artículo 7.

c) Un canal seguro no electrónico: el sujeto obligado dispondrá de un canal seguro no electrónico. Los extremos de este canal seguro serán los coordinadores de los centros de recepción de los agentes facultados y los interlocutores únicos por parte de los sujetos obligados en las acepciones definidas en el apéndice de esta orden. El interlocutor de la parte del sujeto obligado debe encontrarse en territorio español. Se devolverá un acuse de recibo con la consignación de la fecha y hora de la recepción de los mensajes remitidos por este canal desde cualquiera de sus extremos.

3. El intercambio de información de administración entre los sujetos obligados y los agentes facultados que requiera el uso de un canal seguro, se realizará preferentemente mediante el canal seguro electrónico.

4. Las informaciones de administración se podrán enviar al agente facultado por los canales físicos que corresponden a la interfaz HI2, siempre que se satisfagan los requisitos establecidos, para la interfaz HI1, en esta orden ministerial.

Artículo 7. *Canal seguro electrónico para la interfaz HI1.*

1. El canal seguro electrónico, para la interfaz HI1, se realizará mediante una red privada virtual IPSec (VPN IPSec), configurada para garantizar los requisitos de un canal seguro, tal como está definido en el apéndice. Esta VPN IPSec empleará el servicio ESP (Encapsulating Security Payload) con el algoritmo de cifrado AES (Advanced Encryption Standard).

2. La información de administración se enviará mediante mensajes de correo electrónico cifrados y firmados mediante firma electrónica reconocida.

3. Serán notificadas al remitente, mediante mensajes diferenciados tanto la recepción como la apertura del mensaje enviado desde cualquiera de los extremos de la interfaz, consignándose la fecha y hora de la recepción o la apertura. El canal podrá configurarse para que estos mensajes se envíen de forma automática.

4. El canal seguro electrónico para la interfaz HI1 se podrá realizar mediante soluciones tecnológicas alternativas a ésta, siempre que logren un nivel de seguridad igual o superior y se acuerde con los agentes facultados.

La interfaz HI1 podrá compartir canal físico con la interfaz HI2, siempre y cuando este canal satisfaga los requisitos establecidos para la interfaz HI1 en el apartado 1 de este artículo.

Artículo 8. *Gestión de una orden de interceptación legal.*

1. El agente facultado remitirá la orden de interceptación legal, a través de un canal seguro, al sujeto obligado que preste uno o varios servicios objetivo, de acuerdo con la definición incluida en el apartado gg) del apéndice de esta orden.

Sin perjuicio de esta obligación, una vez que la autoridad judicial haya autorizado la orden de interceptación, el agente facultado podrá enviar, por adelantado, una copia de la orden de interceptación a través de un canal seguro. En este caso, el agente facultado deberá remitir la orden de interceptación legal original en un plazo máximo de 15 días, desde que tenga lugar el envío de este adelanto, si bien las partes (agente facultado y sujeto obligado) podrán acordar expresamente otro plazo.

En el caso de emplearse un canal seguro electrónico para enviar la orden de interceptación legal o copia de la misma, la función de administración (ADMF) del sujeto obligado, para evitar errores y retrasos de trascripción, podrá cargar automáticamente, desde la orden de interceptación, los datos necesarios para activar la interceptación. Pero en ningún caso podrá activarse la interceptación de forma automática por el sistema, sin la autorización del sujeto obligado.

2. El sujeto obligado acusará recibo de la recepción, a través de un canal seguro, en cuanto ésta ocurra, tanto de la orden de interceptación como, en su caso, del adelanto de

cve: BOE-A-2009-1771

la misma, consignando la fecha y hora de la recepción en la forma especificada en los artículos 6.2.c) ó 7.3, dependiendo del tipo de canal seguro utilizado.

Los plazos establecidos en el artículo 99 del Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios, contarán a partir de la fecha y hora consignada en el acuse de recibo de la recepción de la orden de interceptación o, en su caso, del envío por adelantado de la misma.

Para garantizar el cumplimiento del plazo de ejecución de las órdenes de interceptación fuera del horario laboral, el sujeto obligado dispondrá de un punto de contacto permanente que será comunicado a los coordinadores de los centros de recepción de los agentes facultados.

3. Cuando la orden de interceptación haya sido activada técnicamente por el sujeto obligado en su sistema de interceptación, se notificará, a través de un canal seguro, al agente facultado que la orden de interceptación se encuentra activa, consignándose la fecha y hora a la cuál se ha activado la interceptación. Esta notificación se podrá realizar a través de la interfaz HI2.

Se entiende que una orden de interceptación está activa a partir del momento en que el sistema de interceptación legal puede extraer la información relativa a la interceptación (IRI) y el contenido de la comunicación (CC) de las comunicaciones determinadas por la orden de interceptación legal y puede enviarse al centro de recepción de las interceptaciones del agente facultado.

4. El agente facultado remitirá, a través de un canal seguro, cualquier resolución de la autoridad judicial que ordene la prórroga, modificación o cese de la citada orden de interceptación legal. El sujeto obligado notificará el cumplimiento de esta resolución, consignando la fecha y hora a partir de la cual se ha modificado su sistema de interceptación legal, para satisfacer lo solicitado por la autoridad judicial.

5. Cuando expire el plazo autorizado para realizar la interceptación o cuando lo solicite la autoridad judicial, el sujeto obligado desactivará los mecanismos de interceptación y notificará, a través de un canal seguro, al agente facultado que la orden de interceptación ha sido desactivada, consignándose la fecha y hora a partir de la cuál se desactivó la interceptación. Esta notificación se podrá realizar a través de la interfaz HI2.

Artículo 9. *Incidencias técnicas, notificación de modificaciones y realización de pruebas.*

1. En caso de que exista algún periodo durante el cual no sea posible remitir al agente facultado los resultados de una interceptación activa, el sujeto obligado deberá notificarlo, siempre que sea posible, a través de un canal seguro, al agente facultado consignando el periodo durante el cual esto no fue posible.

Si la interrupción es prolongada, el sujeto obligado deberá notificar, a través de un canal seguro, en mensajes separados, el comienzo y el final de la interrupción, consignado la fecha y hora de cada suceso.

Si el período de interrupción es previsible, ya sea por tareas de mantenimiento programadas o por cualquier otra circunstancia, el sujeto obligado deberá notificarlo con al menos 10 días de antelación al agente facultado a través de un canal seguro.

2. Para la resolución de incidencias técnicas y la realización de pruebas, se podrá emplear canales HI1 no seguros, siempre que se cumplan los requisitos para ello establecidos en el artículo 6.

En determinados casos, tratándose de incidencias relacionadas con un sujeto objeto de la medida de la interceptación o una identidad, entendida ésta en los términos del artículo 84 del Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios, dichas incidencias se podrán notificar por los canales físicos que corresponden a la interfaz HI2.

3. Las modificaciones del sistema de interceptación legal o de cualquier otro elemento del sujeto obligado, incluyendo la provisión de nuevos servicios, que pueda afectar a la interceptación legal, se notificarán a los agentes facultados con una antelación de tres meses.

cve: BOE-A-2009-1771

4. Para la realización de pruebas de los sistemas de interceptación legal, el sujeto obligado permitirá, a cada agente facultado, contratar al menos dos identidades, de acuerdo con la definición prevista en el artículo 84 del citado Reglamento aprobado por el Real Decreto 424/2005, de 15 de abril, de cada servicio de comunicaciones electrónicas que preste. Estas identidades no corresponderán a ninguna persona física, sólo se emplearán para la realización de pruebas y podrán ser interceptadas sin necesidad de orden de interceptación.

5. La disponibilidad del sistema de interceptación legal del sujeto obligado, no será inferior al del servicio de comunicaciones electrónicas prestado por el sujeto obligado a sus abonados y usuarios, ni el plazo para resolver fallos del mismo será superior al establecido por el sujeto obligado en la prestación, a sus abonados y usuarios, del servicio de comunicaciones electrónicas.

6. Para asuntos muy urgentes, fuera del horario laboral, relacionados con la interceptación legal, los sujetos obligados dispondrán de un punto de contacto permanente a disposición de los coordinadores de los centros de recepción de los agentes facultados.

Artículo 10. *Formato del identificador de interceptación legal (LIID).*

1. El formato del LIID es una cadena de 1 a 25 caracteres ASCII, pertenecientes al subconjunto constituido por los caracteres «a» a «z», «A» a «Z», «-», «_», «.» y «0» a «9».

2. El valor del LIID se acuerda entre el sujeto obligado y el agente facultado, satisfaciendo las siguientes condiciones:

a) Si varios agentes facultados solicitan la interceptación del mismo sujeto objeto de la medida de la interceptación, el LIID será diferente para cada agente facultado.

b) El LIID permitirá identificar al sujeto obligado y al agente facultado.

c) El LIID no contendrá ninguna información que permita identificar al sujeto interceptado, incluida la identidad, de acuerdo con la definición prevista en el artículo 84 del Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios.

Artículo 11. *Medidas de seguridad.*

En el anexo II de esta orden, se establecen las medidas técnicas y organizativas que los sujetos obligados deben implementar para garantizar la autenticidad, confidencialidad, integridad y no repudio de los datos relacionados con la interceptación legal de las comunicaciones y la disponibilidad de la interceptación, así como prevenir su uso ilegal. Dichas medidas se articulan en ocho apartados:

1. Documento de seguridad y gestión de incidencias.
2. Personal relacionado con la interceptación legal de las comunicaciones.
3. Recinto para el sistema de interceptación.
4. Seguridad de los documentos.
5. Seguridad del sistema de interceptación.
6. Seguridad de las funciones de interceptación internas (IIF).
7. Registros de auditoría.
8. Medidas de seguridad adicionales.

Artículo 12. *Reloj del sistema de interceptación.*

1. Los relojes de los elementos del sistema de interceptación legal tendrán un error máximo inferior al medio segundo. Estos relojes serán la fuente de tiempo para la consignación de fecha y hora de todos los eventos relacionados con los mecanismos de interceptación legal.

2. Se tomará como referencia el patrón nacional de tiempo proporcionado por el Centro Nacional de Metrología.

cve: BOE-A-2009-1771

Artículo 13. *Cohabitación con el sistema de conservación de datos.*

El sistema de interceptación podrá compartir recursos con el sistema de conservación de datos previsto por la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones y, en su caso, sus normas de desarrollo reglamentario, siempre que esto no perjudique sus funciones ni la seguridad del sistema de interceptación legal.

Artículo 14. *Información complementaria a la interceptación.*

1. Los sujetos obligados conforme al artículo 85 del Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios, aprobado por el Real Decreto 424/2005, de 15 de abril, pondrán a disposición del agente facultado que lleve a cabo la interceptación legal, los datos a que hacen referencia los artículos 88.2, 88.3 y 89.2 del citado Reglamento mediante el procedimiento que se describe en el apartado siguiente.

2. La petición será concreta y en ningún caso se podrán ejercitar solicitudes masivas de datos. En la misma se identificará al agente facultado que esté llevando a cabo la interceptación legal y que realiza la solicitud, cuyo coordinador del centro de recepción de las interceptaciones asumirá la responsabilidad de la solicitud de datos, y la referencia del identificador o identificadores de interceptación legal (LIID) que corresponden a la interceptación legal en cuyo marco se realiza dicha solicitud.

3. La solicitud de esta información y su respuesta se realizarán a través de un canal HI1 seguro. El agente facultado acusará recibo, a través de este canal, de la recepción de la respuesta consignándose la fecha y hora de la misma.

La información solicitada se remitirá antes de las 12:00 horas del día hábil siguiente al que el sujeto obligado reciba la solicitud. Cuando la solicitud sea urgente, los sujetos obligados deberán ejecutarla con la mayor brevedad que les sea posible, para lo cual el sujeto obligado dispondrá de un punto de contacto permanente que estará a disposición de los coordinadores de los centros de recepción de los agentes facultados.

Artículo 15. *Número máximo de interceptaciones simultáneas.*

1. El sujeto obligado dispondrá su sistema de interceptación legal de modo que sea capaz de mantener activas, simultáneamente, el siguiente número de interceptaciones:

$$\text{Si } x \leq 60\text{: } MI = x$$

$$\text{Si } x > 60\text{: } MI = 60 + a\left(\sqrt{(x-60)}\right)$$

Donde:

MI = Número máximo de interceptaciones activas simultáneamente.

x = Número de abonados o usuarios (entendidos como el número de identidades, de acuerdo con la definición dada por el artículo 84 del Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios, aprobado por Real Decreto 424/2005, de 15 de abril, proporcionadas por el sujeto obligado a sus abonados o usuarios).

a = Coeficiente que depende de la tecnología de telecomunicaciones concreta y que se especificará en las órdenes ministeriales correspondientes. Su valor está acotado al rango [0,25 - 1].

Nota: Las cantidades con decimales de «MI» se redondearán al número entero inmediatamente inferior.

2. El número máximo de interceptaciones activas simultáneamente se calcula para cada servicio de comunicaciones electrónicas ofrecido por el sujeto obligado. En la fórmula anterior, por tanto, el valor x es el número total de identidades, de acuerdo con la definición prevista en el artículo 84 del citado Reglamento sobre las condiciones para la prestación

cve: BOE-A-2009-1771

de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios, proporcionadas por el sujeto obligado a los abonados o usuarios de cada servicio de telecomunicaciones.

3. El número de interceptaciones que el sujeto obligado deberá ser capaz de transmitir simultáneamente a los agentes facultados se especificará en las órdenes ministeriales concretas correspondientes a cada tecnología de telecomunicaciones.

Artículo 16. *Acceso al registro de los números transferidos entre operadores.*

1. Los coordinadores de los centros de recepción de los agentes facultados podrán acceder al registro actualizado de los números transferidos entre operadores como consecuencia del ejercicio del derecho a la conservación de números, al que hace referencia el artículo 44.5 del Reglamento sobre mercados de comunicaciones electrónicas, acceso a las redes y numeración, aprobado por el Real Decreto 2296/2004, de 10 de diciembre, con el fin de recabar los datos a que hacen referencia los artículos 88.2, 88.3, 89.1,y 89.2 del Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios, aprobado por Real Decreto 424/2005, de 15 de abril.

2. Los coordinadores de los centros de recepción de los agentes facultados se podrán dirigir, con el fin de obtener información para identificar al operador a cargo de un número telefónico portado así como de posibles procedimientos de portabilidad en curso, al gestor encargado de la operación de la entidad de referencia o base de datos que pueda proporcionar la información requerida de acuerdo a las especificaciones vigentes y aprobadas por la Comisión del Mercado de las Telecomunicaciones.

3. Los datos obtenidos serán utilizados exclusivamente para los fines previstos, siendo responsabilidad del agente facultado el adecuado uso de los mismos que, en todo caso, estará sometido a la legislación vigente sobre protección de datos de carácter personal.

Artículo 17. *Estadísticas.*

1. Los sujetos obligados elaborarán estadísticas, sobre las medidas de interceptación, con periodicidad anual. El período contabilizado será desde las 00:00 horas (incluidas) del día 1 de enero hasta las 24:00 horas (excluidas) del día 31 de diciembre del año correspondiente. Se contabilizarán las órdenes de interceptación y las modificaciones y prórrogas de las mismas activadas durante ese periodo, así como las identidades (de acuerdo con la definición prevista en el artículo 84 del Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios) interceptadas con motivo de las mismas. Si una misma identidad técnica es interceptada con motivo de diferentes órdenes de interceptación, se contabilizará cada vez por separado.

2. Las estadísticas se elaborarán conforme al formulario previsto en el anexo III de esta orden y se remitirán a la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información antes del 15 de febrero del año siguiente.

Disposición transitoria primera. *Plazo para el cumplimiento.*

1. Los sujetos obligados deberán cumplir las obligaciones establecidas en los apartados 5 y 7 del anexo II de esta orden en el plazo de dieciocho meses desde su entrada en vigor.

2. Las demás obligaciones establecidas en esta orden deberán cumplirse en el plazo de nueve meses desde su entrada en vigor.

3. Si durante el plazo del apartado anterior se diera la circunstancia de que un sujeto obligado tuviera que materializar una orden de interceptación legal y no estuviera todavía en condiciones de llevarla a efecto con sus propios medios, el sujeto obligado deberá facilitar el acceso de los agentes facultados a sus instalaciones para realizar la interceptación con los medios proporcionados por éstos, en caso de que dispongan de ellos.

cve: BOE-A-2009-1771

4. Aquellos sujetos obligados que inicien su actividad, transcurridos estos plazos, deberán cumplir las obligaciones establecidas en esta orden desde el inicio de su actividad.

Disposición transitoria segunda. *Régimen transitorio especial para sujetos obligados que cumplan determinadas condiciones.*

1. Los sujetos obligados que no tengan la condición de operadores pequeños –de acuerdo con la definición establecida en el apartado dd) del apéndice de esta orden– y dispongan de red de comunicaciones electrónica propia, a través de la cual se encaminen las comunicaciones de sus abonados, podrán acogerse al procedimiento descrito en el artículo 2.1.c) de esta orden si el número total de órdenes de interceptación recibidas durante el año anterior ha sido inferior o igual a cinco.

2. Los sujetos obligados, a que se refiere el apartado anterior, dispondrán de un plazo de seis meses desde el momento en que en un año se superen las cinco interceptaciones, para implantar su propio sistema de interceptación, que satisfaga todos los requisitos establecidos en la legislación vigente sobre interceptación legal de las comunicaciones.

Disposición transitoria tercera. *Servicios y tecnologías no contemplados en órdenes ministeriales específicas.*

Los sujetos obligados que exploten redes o presten servicios de comunicaciones electrónicas, cuya tecnología no haya sido incluida en las órdenes ministeriales relativas a las obligaciones específicas derivadas de la aplicación de una concreta tecnología de telecomunicaciones, deberán acordar con los agentes facultados la forma de cumplir las obligaciones del capítulo II, del título V del citado Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios, relativo a la interceptación legal de las comunicaciones, así como lo dispuesto en esta orden, hasta que se aprueben las correspondientes órdenes ministeriales específicas.

Disposición final primera. *Título competencial.*

Esta orden se dicta al amparo de lo dispuesto en el artículo 149.1.21.ª de la Constitución, que atribuye al Estado la competencia exclusiva en materia de telecomunicaciones.

Disposición final segunda. *Modificación de la Orden CTE/711/2002, de 26 de marzo, por la que se establecen las condiciones de prestación del servicio de consulta telefónica sobre números de abonado.*

La Orden CTE/711/2002, de 26 de marzo, por la que se establecen las condiciones de prestación del servicio de consulta telefónica sobre números de abonado, se modifica en los siguientes términos:

Uno. En el apartado primero. 3 se añaden un párrafo d) y otro e), con la siguiente redacción:

«d) estén autorizados para solicitar información previa a la interceptación en virtud del artículo 89.1 del Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios, aprobado por Real Decreto 424/2005, de 15 de abril.

e) estén autorizados para solicitar información complementaria a la interceptación en virtud de los artículos 88.2, 88.3 y 89.2 del Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios, aprobado por Real Decreto 424/2005, de 15 de abril.»

Dos. Los apartados decimoquinto.3 y 4 se renumeran como 4 y 5, respectivamente.

Tres. Se añade un nuevo apartado decimoquinto.3, con la siguiente redacción:

cve: BOE-A-2009-1771

«3. La Comisión del Mercado de las Telecomunicaciones, previa petición, facilitará a los agentes facultados, la información actualizada a la que se refiere el apartado decimocuarto, con el formato establecido por la Comisión del Mercado de las Telecomunicaciones.

Los datos obtenidos serán utilizados exclusivamente para los fines previstos en los artículos 88.2, 88.3, 89.1 y 89.2 del Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios, aprobado por Real Decreto 424/2005, de 15 de abril, siendo responsabilidad del agente facultado el adecuado uso de los mismos, que, en todo caso, estará sometido a la legislación vigente sobre protección de datos de carácter personal.»

Disposición final tercera. *Convenio de asistencia judicial en materia penal entre los Estados de la Unión Europea.*

Las medidas establecidas en esta orden son, asimismo, de aplicación para el cumplimiento de las obligaciones derivadas del Convenio de asistencia judicial en materia penal entre los Estados de la Unión Europea, de 29 de mayo de 2000, en lo relativo a la interceptación legal de comunicaciones.

Disposición final cuarta. *Entrada en vigor.*

Esta orden entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado».

Madrid, 28 de enero de 2009.–El Ministro de Industria, Turismo y Comercio, Miguel Sebastián Gascón.

## ANEXO I

### Bloques funcionales e interfaces

1. Los bloques funcionales del sistema de interceptación legal son los siguientes:

a) Función de administración (ADMF).
b) Función de mediación (MF) para la Información correlativa a la interceptación (IRI).
c) Función de mediación (MF) para el Contenido de la comunicación (CC).
d) Función de interceptación interna (IIF).

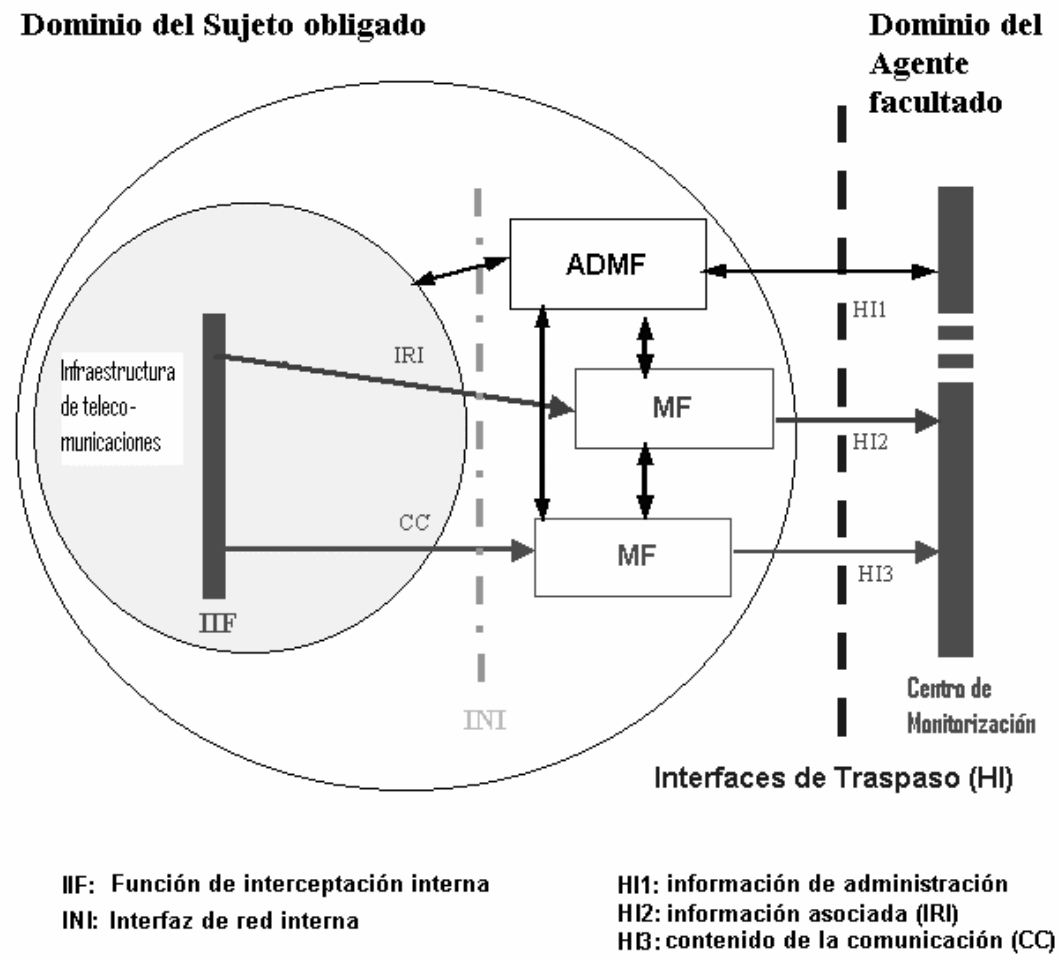
2. Las interfaces del sistema de interceptación legal son las siguientes:

1. Interfaces internas.
2. Interfaces de Traspaso (HI), que se componen de tres interfaces:

2.1. Interfaz de traspaso 1 (HI1).
2.2. Interfaz de traspaso 2 (HI2).
2.3. Interfaz de traspaso 3 (HI3).

3. La siguiente figura representa el diagrama de bloques funcionales e interfaces del sistema de interceptación legal del sujeto obligado (fuente: ETSI ES 201 671 V3.1.1 (2006-10)):

cve: BOE-A-2009-1771




Notas:

Esta figura muestra una configuración de referencia, con una representación lógica de las entidades involucradas en la interceptación legal que no determina entidades físicas separadas.

La función de mediación puede ser transparente, si no es preciso realizar ninguna de sus funciones.

## ANEXO II

### Medidas de seguridad

1. *Documento de seguridad y gestión de incidencias*

1. El sujeto obligado deberá realizar el análisis y gestión de riesgos de sus mecanismos de interceptación legal y elaborar y mantener actualizado un documento de seguridad relativo a la interceptación legal de las comunicaciones en el que se recojan los siguientes aspectos:

a) La relación del personal con acceso a los mecanismos de interceptación.
b) Las funciones, obligaciones, y perfiles de acceso del personal autorizado.
c) La identificación del responsable de seguridad.
d) Las medidas, normas, procedimientos de actuación, reglas y estándares aplicados que garanticen el cumplimiento de las medidas de seguridad establecidas en esta orden y las derivadas de los requisitos establecidos en el Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la

cve: BOE-A-2009-1771

protección de los usuarios, aprobado por Real Decreto 424/2005, de 15 de abril, en las órdenes ministeriales relativas a las obligaciones específicas derivadas de la aplicación de una concreta tecnología de telecomunicaciones o en otras normas de rango legal o reglamentario que sean de aplicación.

e) La configuración del sistema operativo y la relación de aplicaciones que sea necesario instalar en el sistema de interceptación.

f) Las medidas que resulten necesarias para proteger el sistema de interceptación frente a programas maliciosos, intrusiones, accesos no autorizados y otras amenazas; y evitar la instalación de dispositivos y aplicaciones maliciosas en el sistema de interceptación.

g) Las medidas que resulten necesarias para que el acceso remoto al sistema de interceptación no comprometa la seguridad del sistema ni la confidencialidad de los datos, así como una relación actualizada de las personas autorizadas para acceder remotamente al sistema.

h) Los procedimientos de instalación, configuración, mantenimiento y reparación del sistema de interceptación detallando las medidas que resulten necesarias para que estos procesos no pongan en peligro la seguridad del sistema de interceptación ni la confidencialidad de los datos relacionados con la interceptación.

i) Los controles periódicos que se deban realizar para verificar el cumplimiento de lo dispuesto en el propio documento.

j) Los procedimientos de notificación, gestión y respuesta ante las incidencias.

2. Se tenderá a aplicar en la medida de lo posible el código de buenas prácticas de gestión de la seguridad de la información de la norma UNE-ISO/IEC 17799.

3. El documento de seguridad deberá mantenerse en todo momento actualizado y será revisado siempre que se realice una actualización o cambio del sistema.

4. Deberá existir un procedimiento de notificación y gestión de las incidencias relacionadas con los mecanismos de interceptación y establecer un registro en el que se haga constar el tipo de incidencia, la fecha y hora en que se ha producido o detectado, los efectos que se hubieran derivado de la misma y las medidas correctoras aplicadas.

### 2. *Personal relacionado con la interceptación legal de comunicaciones*

1. Las personas que puedan acceder a los mecanismos de interceptación así como a cualquier información relacionada con la interceptación legal de comunicaciones será el mínimo necesario para garantizar la ejecución de las órdenes de interceptación en las condiciones establecidas.

2. Su acceso a la información y demás recursos relacionados con la interceptación estará basado en los principios de necesidad de conocer, menor privilegio, separación de tareas y autorización, entendidos éstos en sus acepciones definidas en el apéndice de esta orden.

3. La relación de personas con acceso al sistema de interceptación así como sus funciones y obligaciones en relación con la interceptación legal de las comunicaciones, que deberán estar claramente definidas, se recogerán en el documento de seguridad a que hace referencia el apartado 1 de este anexo.

4. Las personas con acceso al sistema de interceptación deberán firmar una declaración de seguridad, en el formato que acuerden el sujeto obligado y los agentes facultados, por la que se declare haber recibido la formación adecuada para el desempeño de sus funciones y sobre los procedimientos operativos de seguridad, se comprometa a guardar estricta confidencialidad sobre toda la información relacionada con la interceptación legal de comunicaciones, y declare su conocimiento de las consecuencias del uso indebido de los mecanismos de interceptación.

### 3. *Recinto para el sistema de interceptación*

1. Todo el sistema de interceptación, con excepción de funciones de interceptación internas (IIF) que se hallen distribuidas en la infraestructura de telecomunicaciones del

cve: BOE-A-2009-1771

sujeto obligado, se situará en recintos que han de satisfacer los siguientes requisitos de seguridad:

a) Deberán estar protegidos mediante mecanismos de control de acceso de forma que los accesos no autorizados o los intentos de acceso no autorizados sean detectados y se puedan tomar acciones inmediatas.

b) Se adoptarán las medidas necesarias para que la presencia de personal exterior al equipo de interceptación, que se limitará al mínimo estrictamente necesario, no comprometa la seguridad. Su presencia deberá quedar adecuadamente registrada de acuerdo con el procedimiento establecido al efecto en el documento de seguridad.

4. *Seguridad de los documentos*

1. Se establecerán por parte de cada sujeto obligado unos criterios claros de clasificación de la información electrónica y en papel según las medidas de seguridad a aplicar, que se recogerán en el documento de seguridad.

2. Las órdenes de interceptación, los registros de auditoría, las copias de seguridad, la documentación del sistema de interceptación y cualesquiera otros documentos en papel o electrónicos importantes para la seguridad del sistema de interceptación deberán guardarse en cajas fuertes, armarios o archivadores dotados de sistema de apertura mediante llave u otro dispositivo equivalente.

3. Los documentos citados en el apartado anterior no deben salir del mencionado almacén salvo que sea estrictamente necesario, en cuyo caso se adoptarán las medidas necesarias para garantizar su confidencialidad, integridad y disponibilidad, y serán transportados por el personal expresamente autorizado para ello.

4. Deberá establecerse por cada sujeto obligado un sistema de registro de entrada y salida de documentos en papel y electrónicos, en el que deberá constar la fecha y hora, además, la identidad de la persona que los saque o introduzca.

Cuando expire el período de conservación de estos documentos, el responsable de seguridad los destruirá de forma segura mediante la adopción de medidas dirigidas a evitar el acceso o recuperación posterior de la información eliminada. Se guardará registro de la destrucción de los documentos.

5. *Seguridad del sistema de interceptación*

1. El sistema de interceptación comprende todos los bloques e interfaces citados en el artículo 6, así como cualesquiera otros componentes necesarios para proveer la interceptación legal, incluidos los necesarios para garantizar la seguridad del sistema, como el sistema de registros de auditoría establecido en el apartado 7 de este anexo. Las medidas del presente apartado atañen a todos componentes del sistema de interceptación excepto las funciones de interceptación internas (IIF), cuyas medidas de seguridad se establecen en el apartado 6 de este anexo.

2. Sólo se podrá acceder al sistema de interceptación mediante usuarios definidos en el mismo que serán exclusivos para cada persona. El documento de seguridad al que hace referencia el apartado 1 de este anexo deberá incluir una relación actualizada e histórica de usuarios y perfiles de usuarios y los accesos autorizados a cada uno de ellos. Los permisos de acceso a la información y a otros recursos del sistema de interceptación deberán corresponderse estrictamente con el cometido de la persona a quien corresponde el usuario. El acceso tanto de personas como de procesos a la información y otros recursos del sistema de interceptación estará basado en los principios de necesidad de conocer, menor privilegio, separación de tareas y autorización, entendidos éstos en sus acepciones definidas en el apéndice de esta orden.

3. El acceso al sistema sólo será posible tras comprobar la identidad y la autorización de todo aquel que intente acceder, tras superar previamente con éxito los procesos de identificación, autenticación y autorización. Esta comprobación se hará preferiblemente mediante un dispositivo de autenticación fuerte conforme a la definición recogida en el apartado k) del apéndice.

cve: BOE-A-2009-1771

Se deberá establecer un mecanismo para limitar la posibilidad de intentar reiteradamente el acceso no autorizado del sistema, provocando el bloqueo del mismo.

Se establecerán mecanismos de bloqueo del sistema ante eventos que puedan considerarse potencialmente peligrosos tales como la extracción del dispositivo seguro de autenticación del dispositivo lector y/o tiempos de inactividad del sistema excesivamente largos.

El documento de seguridad al que hace referencia el apartado 1 de este anexo incluirá una descripción de estos mecanismos de bloqueo y los correspondientes procesos de reactivación del sistema.

4. El sistema operativo estará actualizado y estarán instaladas las aplicaciones necesarias para la detección y protección frente a programas maliciosos, intrusiones y otras amenazas. Se recomienda el empleo de sistemas operativos y, en general, software de código abierto en el sistema de interceptación.

5. La información en los discos duros estará cifrada.

6. El sistema garantizará que el borrado de información se realice de forma segura evitando así el acceso a la información o su recuperación posterior, sin perjuicio de la actividad de auditoría descrita en el apartado 7 de este anexo.

7. Se adoptarán las medidas necesarias para impedir la comunicación del sistema con cualquier dirección que no sea estrictamente necesaria para la interceptación legal de comunicaciones. Las comunicaciones a través de Internet sólo serán posibles con las direcciones pertinentes de los centros de recepción de las interceptaciones de los agentes facultados.

8. Se adoptarán las medidas necesarias para que el acceso remoto al sistema de interceptación, que sólo será posible cuando sea estrictamente necesario y por las personas debidamente autorizadas por el responsable de seguridad, no comprometa la seguridad del sistema ni la confidencialidad de los datos relacionados con la interceptación de las comunicaciones.

El conjunto de medidas y la relación de personas autorizadas a que hace referencia el párrafo anterior deberán estar especificadas en el documento de seguridad.

9. Se adoptarán las medidas necesarias para garantizar que las interfaces de traspaso y las interfaces internas del sistema de interceptación no puedan comprometer la seguridad.

La instalación, configuración, mantenimiento y reparación del sistema se realizarán, en la medida de lo posible, en los recintos para el sistema de interceptación y aplicando el procedimiento y las medidas de seguridad previstas en el documento de seguridad. Se adoptarán las medidas necesarias para garantizar que los fabricantes, integradores e instaladores del sistema de interceptación no puedan comprometer la seguridad del sistema ni accedan a informaciones confidenciales en relación con la interceptación legal.

### 6. *Seguridad de las funciones de interceptación internas (IIF)*

1. El acceso físico a las funciones de interceptación internas (IIF) estará protegido con las medidas de seguridad propias de la infraestructura de telecomunicaciones del sujeto obligado según el estado del arte.

2. La ubicación de las funciones de interceptación internas será discreta y cualquier información sobre ellas será secreta.

3. Cualquier actuación sobre las mismas (instalación o resolución de averías) se realizará con discreción por personal expresamente autorizado. Se mantendrá una relación actualizada e histórica del personal autorizado para realizar estos cometidos.

4. El acceso lógico y control de las funciones de interceptación internas sólo será posible desde la función de administración (ADMF) del sistema de interceptación legal.

### 7. *Registros de auditoría*

1. Los sujetos obligados dispondrán de un sistema centralizado para la gestión de los registros de auditoría de los diferentes componentes del sistema de interceptación. Dicho

cve: BOE-A-2009-1771

sistema dará soporte a la generación, transmisión, almacenamiento, firma electrónica, verificación y análisis de los mismos, y garantizará su autenticidad, confidencialidad, integridad y disponibilidad durante todo su ciclo de vida.

2. El formato de los registros de auditoría, los sucesos sobre los que se deberán generar registros de auditoría, los procedimientos para la verificación de su autenticidad e integridad y los procedimientos de inspección y de custodia se desarrollará, en su caso, mediante orden ministerial.

8. *Medidas de seguridad adicionales*

1. Las medidas de seguridad establecidas en esta orden se aplicarán sin perjuicio de cualesquiera otras medidas de seguridad adicionales necesarias que se establezcan para satisfacer los requisitos establecidos en el Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios, aprobado por Real Decreto 424/2005, de 15 de abril, en las órdenes ministeriales relativas a las obligaciones específicas derivadas de la aplicación de una concreta tecnología de telecomunicaciones o en otras normas de rango legal o reglamentario.

2. Las medidas de seguridad se actualizarán por parte de los sujetos obligados según la evolución de la tecnología.

cve: BOE-A-2009-1771

**ANEXO III**

**Formulario para las estadísticas anuales sobre medidas de interceptación legal de comunicaciones**

( Empresa )

Estadística anual correspondiente al año: _____

sobre las medidas de interceptación legal de las comunicaciones

1. Número órdenes de interceptación iniciadas: _____

1.1. Número modificaciones y prórrogas de órdenes de interceptación iniciadas:_____

2. Número de identidades interceptadas:_____

3. Contabilidad desagregada por servicios:

| | Servicio de comunicaciones electrónicas | Órdenes iniciadas | Modificaciones / Prórrogas de órdenes | Identidades interceptadas |
|---|---|---|---|---|
| 1 | Líneas analógicas | | | |
| 2 | RDSI – acceso básico | | | |
| 3 | RDSI – acceso primario | | | |
| 4 | Telefonía móvil | | | |
| 5 | Correo electrónico | | | |
| 6 | Acceso a Internet (v.gr. xDSL, CATV) | | | |
| 7 | | | | |

4. Número de órdenes de interceptación fuera del horario laboral en relación con el número total de órdenes de interceptación.

_____ _____

(Lugar, Fecha) (Representante legal de la Empresa)

Normas para realizar esta estadística:

1. En el epígrafe 1, contabilízense las órdenes de interceptación *activadas* desde las 00:00 horas (incluidas) del día 1 de enero hasta las 24:00 horas (excluidas) del día 31 de diciembre del año correspondiente.
2. En el epígrafe 2, el término identidad, de conformidad con el artículo 84 del Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios, aprobado por el Real Decreto 424/2005, de 15 de abril, se define como "etiqueta técnica que puede representar el origen o el destino de cualquier tráfico de comunicaciones electrónicas, en general identificada mediante un número de identidad de comunicaciones electrónicas físico (tal como un número de teléfono) o un código de identidad de comunicaciones electrónicas lógico o virtual (tal como un número personal) que el abonado puede asignar a un acceso físico caso a caso".
3. En el epígrafe 2, contabilízense identidades cuya interceptación se *activó* desde las 00:00 horas (incluidas) del día 1 de enero hasta las 24:00 horas (excluidas) del día 31 de diciembre del año correspondiente.
4. En el epígrafe 2, si una misma identidad es interceptada con motivo de diferentes órdenes de interceptación, contabilízese cada vez por separado.
5. Bajo el epígrafe 3, táchense los servicios de telecomunicaciones que no sean prestados por el sujeto obligado.
6. Bajo el epígrafe 3, añádanse los servicios de telecomunicaciones que sean prestados por el sujeto obligado y no figuren en la tabla.
7. Todos las campos numéricos han de ser cumplimentados. Si no hubo ningún caso, indíquese con el número "0".

cve: BOE-A-2009-1771

APÉNDICE

**Definiciones**

A los efectos de lo dispuesto en esta orden, se entiende por:

a) Autenticación: Verificación de la identidad declarada.

b) Autorización: Acción de facultar para acceder con determinadas capacidades a determinados recursos con arreglo a lo que corresponda a la identidad del que solicita el acceso.

c) Canal: Medio de comunicación empleado para el intercambio de información entre el sujeto obligado y el agente facultado. Por analogía, se denominarán canal HI1, canal HI2 y canal HI3 los canales correspondientes a las interfaces HI1, HI2 y HI3 respectivamente.

d) Canal electrónico: Canal que hace uso de redes de comunicaciones electrónicas, entendidas éstas en la acepción que figura en el anexo II (Definiciones) de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones.

e) Canal no seguro: Canal que no requiere cumplir los requisitos establecidos en la definición de canal seguro.

f) Canal seguro: Un canal se define como seguro, a los efectos de esta orden, si garantiza, según el estado de la tecnología en cada momento, la confidencialidad, la integridad, la disponibilidad y el no repudio de la información por él transmitida, así como la autenticación inequívoca de las partes implicadas en la comunicación, proporcionando la máxima garantía jurídica de acuerdo con la legislación vigente. (Un canal seguro no es necesariamente electrónico).

g) Confidencialidad: La propiedad de que la información no se haga disponible ni se revele a personas, entidades o procesos no autorizados.

h) Contenido de la comunicación (CC, «Content of communication»): Información intercambiada entre dos o más usuarios de un servicio de comunicaciones electrónicas, excluyendo la información relativa a la interceptación (IRI). Incluye la información que puede, como parte de algún servicio de comunicaciones electrónicas, ser almacenada por un usuario para su posterior recuperación por otro.

i) Coordinador de los centros de recepción de los agentes facultados: persona o grupo de personas perteneciente a cada uno de los agentes facultados que será el único enlace válido para los sujetos obligados a los efectos de tratar asuntos relacionados con la interceptación legal de las comunicaciones.

j) Disponibilidad: La propiedad de ser accesible y utilizable a petición por una entidad autorizada y según las especificaciones de calidad de funcionamiento.

k) Dispositivo de autenticación fuerte: Un dispositivo de autenticación basado en al menos dos factores de identificación de entre los tres siguientes: de conocimiento (v.gr., una palabra de paso), de posesión (v.gr., una tarjeta criptográfica) y de características personales (v.gr., reconocimiento biométrico).

l) Firma electrónica: Conforme a la Ley 59/2003, de 19 de diciembre, de firma electrónica, es el conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante.

m) Firma electrónica avanzada: Conforme a la Ley 59/2003, de 19 de diciembre, de firma electrónica, es la firma electrónica que permite identificar al firmante y detectar cualquier cambio ulterior de los datos firmados, que está vinculada al firmante de manera única y a los datos a que se refiere y que ha sido creada por medios que el firmante puede mantener bajo su exclusivo control.

n) Firma electrónica reconocida: Conforme a la Ley 59/2003, de 19 de diciembre, de firma electrónica, es la firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma. Nótese que, aunque puedan emplear la misma tecnología, los actos de cifrar y de firmar electrónicamente son distintos. Nótese asimismo que la firma electrónica reconocida sirve también para garantizar la integridad de los datos firmados.

o) Función de administración (ADMF, «Administration Function»): Función que controla el sistema de interceptación legal del sujeto obligado. Entre otras tareas, recibe

cve: BOE-A-2009-1771

las órdenes de interceptación legal y genera las instrucciones para que el sistema ejecute una interceptación legal. Esta función impide el control del sistema de interceptación legal del sujeto obligado por los agentes facultados.

p) Función de entrega (DF, «Delivery Function»): En sentido amplio, término que equivale a la función de mediación. En sentido estricto, parte de la pasarela MF/DF responsable del envío del contenido de la comunicación (CC) y la información correlativa a la interceptación (IRI) al centro de recepción de las interceptaciones. Por defecto se entenderá en sentido amplio.

q) Función de interceptación interna (IIF, «Internal Interception Function»): Punto de la red o de un elemento de red donde se obtienen el contenido de la comunicación (CC) y/o la información relativa a la interceptación (IRI).

r) Función de mediación (MF, «Mediation Function»): En sentido amplio, el mecanismo que transforma la información obtenida en la función de interceptación interna (IIF) y la transfiere hasta la interfaz de traspaso (HI). También recibe el nombre de pasarela MF/DF (MF/DF Gateway). En sentido estricto, la función que transforma los formatos de la información relativa a la interceptación (IRI) y del contenido de la comunicación (CC) de su formato en la interfaz de red interna (INI) al formato normalizado de la interfaz de traspaso (HI). En algunos casos esta transformación puede no ser necesaria. Por defecto se entenderá en sentido amplio.

s) Identificador de interceptación legal (LIID, «Lawful Interception IDentifier»): Es un código que sirve para correlacionar las distintas informaciones que, transmitidas a través de las interfaces HI, corresponden a un mismo sujeto a la interceptación o a una misma identidad, entendida ésta en los términos del artículo 84 del Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios, aprobado por el Real Decreto 424/2005, de 15 de abril.

t) Información complementaria a la interceptación: Es la información definida en los apartados 88.2, 88.3, y 89.2 del Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios, aprobado por Real Decreto 424/2005, de 15 de abril.

u) Información relativa a la interceptación (IRI, «Intercept Related Information»): Es la información definida en el artículo 88.1 del Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios, aprobado por Real Decreto 424/2005, de 15 de abril.

v) Integridad: La propiedad de que la información no sea modificada o destruida sin autorización.

w) Interfaz de red interna (INI, «Internal Network Interface»): En sentido estricto, interfaz entre la función de interceptación interna y la función de mediación. En sentido amplio, sinónimo de interfaz interna. Por defecto se entenderá en sentido estricto.

x) Interfaz de traspaso (HI, «Handover Interface)»: Interfaz física y lógica entre el dominio del sujeto obligado y el dominio del agente facultado. A través de la HI el agente facultado solicita al sujeto obligado la ejecución de medidas de interceptación legal y éste entrega los resultados de la interceptación al centro de recepción de las interceptaciones. Esta interfaz se compone, a su vez, de tres interfaces distintas:

Interfaz de traspaso 1 (HI1): Interfaz para el intercambio de información de administración entre el centro de recepción de las interceptaciones del agente facultado y la Función de administración (ADMF) del sujeto obligado. Se utiliza para intercambiar información diversa y poco normalizada que incluye desde las órdenes de interceptación hasta la resolución de incidencias técnicas.

Interfaz de traspaso 2 (HI2): Interfaz para la entrega de la información asociada con la interceptación (IRI) al centro de recepción de las interceptaciones.

Interfaz de traspaso 3 (HI3): Interfaz para la entrega del contenido de la comunicación (CC) al centro de recepción de las interceptaciones.

cve: BOE-A-2009-1771

Esta es una distinción lógica. En su realización, en ocasiones pueden compartir la interfaz física.

y) Interfaz interna (X): Cualquier interfaz del sistema de interceptación legal del sujeto obligado excepto la interfaz de traspaso. Incluye las interfaces entre los elementos del sistema de interceptación.

z) Interlocutor único: Persona o grupo de personas perteneciente a cada uno de los sujetos obligados que será el único enlace válido para los agentes facultados a los efectos de tratar asuntos relacionados con la interceptación legal de las comunicaciones.

aa) Menor privilegio: Principio de seguridad que exige que se otorgue el menor número de facultades para el acceso y el uso de recursos e información que permita desempeñar aquellos cometidos para los que se esté expresamente autorizado.

bb) Necesidad de conocer: Principio de seguridad que exige que sólo se conozca, se tenga acceso o se posea aquella información o recursos que sean estrictamente necesarios para el desempeño de aquellos cometidos para los que se esté expresamente autorizado.

cc) No repudio: La propiedad de poder probar que una acción o evento ha tenido lugar, de modo que tal acción o evento no pueda ser negado posteriormente.

dd) Operador pequeño: Aquel sujeto obligado, según lo establecido en el artículo 85 del Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios, aprobado por el Real Decreto 424/2005, de 15 de abril, que además cumple todos y cada uno de los siguientes requisitos, sin perjuicio de otros requisitos adicionales que se puedan establecer en las órdenes ministeriales relativas a las obligaciones específicas derivadas de la aplicación de una concreta tecnología de telecomunicaciones:

Tener red de comunicaciones electrónicas propia a través de la cual se encaminen las comunicaciones de sus abonados.

Cumplir todos los requisitos para tener la clasificación de microempresa de acuerdo con lo dispuesto en el título I del anexo de la Recomendación n.º 2003/361/CE de la Comisión de 6 de mayo de 2003, sobre la definición de microempresas, pequeñas y medianas empresas (DOUE L 124, de 20 de mayo de 2003); o su eventual revisión conforme a lo dispuesto en el artículo 9 del anexo de la propia Recomendación.

ee) Resultado de la interceptación (result of interception): Información relativa a un servicio objetivo, incluyendo el contenido de la comunicación (CC) y/o la información relativa a la interceptación (IRI), que el sujeto obligado entrega al centro de recepción de las interceptaciones.

ff) Separación de tareas: Principio de seguridad que exige que los procesos se dividan en etapas asignadas a distintas personas de modo que no sea posible que una sola persona pueda subvertir el proceso.

gg) Servicio objetivo: Servicio de comunicaciones electrónicas que puede ser utilizado por un sujeto a la interceptación. Puede haber más de un servicio objetivo relacionado con el mismo sujeto a la interceptación.

cve: BOE-A-2009-1771