IV. Normas internas para el tratamiento de la información privilegiada

3 de julio de 2016

Índice
/

Preámbulo

Estas *Normas internas para el tratamiento de la información privilegiada* (las "***Normas***") forman parte del Sistema de gobierno corporativo de IBERDROLA, S.A. (la "**Sociedad**") y se aprueban, a propuesta de la Unidad de Cumplimiento, por el Consejo de Administración de la Sociedad en desarrollo del *Reglamento interno de conducta en los Mercados de Valores* (el "***Reglamento interno de conducta***"), cuyo artículo 9.4.c) prevé que se deberán establecer medidas de seguridad para la custodia, archivo, acceso, reproducción y distribución de la Información Privilegiada, tal y como este término se define en dicho *Reglamento interno de conducta*.

Con este fin, estas *Normas* establecen las reglas para la gestión, control y transmisión, interna y externa, de la Información Privilegiada, cualquiera que sea su ubicación, formato, soporte o medio de transmisión, con el fin de tutelar los intereses de los accionistas e inversores y de prevenir y evitar cualquier situación de abuso.

TÍTULO PRELIMINAR

Artículo 1. Definiciones

Los términos que comiencen en mayúsculas utilizados en estas *Normas* y no definidos expresamente tendrán el significado que se les otorga en el *Reglamento interno de conducta*.

Por su parte, a los efectos de estas *Normas*, se entenderá por:

a) Director del Área: se refiere al director del Área responsable de la coordinación de los trabajos u operación a la que se refiera la Información Privilegiada y de la custodia de dicha información.
b) Guía: la *Guía de protección de información privilegiada y confidencial* elaborada por la Dirección de Finanzas y Recursos de la Sociedad, que resultará de aplicación supletoria en todo lo no previsto expresamente en estas *Normas*.
c) Iniciados: las personas definidas como tales en el *Reglamento interno de conducta*, incluyendo a estos efectos a los Receptores Externos.
d) Personas Autorizadas: se refiere, en el contexto de una determinada operación, proceso interno o actividad en la que se reciba, genere o acceda a Información Privilegiada, al conjunto de Personas Afectadas y/o Iniciados que estén autorizados a acceder a dicha información.
e) Receptores Externos: se refiere a aquellas personas que no sean empleados ni administradores de las sociedades integradas en el grupo cuya entidad dominante, en el sentido establecido por la ley, es la Sociedad (el "**Grupo**"), que necesiten conocer la Información Privilegiada para poder prestar sus servicios profesionales (por ejemplo, asesorar o analizar alguna operación) o realizar transacciones con el Grupo (por ejemplo, financiar alguna operación), las cuales no estarán obligadas al cumplimiento de estas *Normas* con excepción de lo dispuesto en su artículo 10.4.b).

Artículo 2. Objeto

El objeto de estas *Normas* es establecer las reglas y procedimientos de la Sociedad para el tratamiento interno de la Información Privilegiada y su transmisión a terceras personas ajenas al Grupo, con el fin de tutelar los intereses de los accionistas e inversores y de prevenir y evitar cualquier situación de abuso. Todo ello, sin perjuicio de lo dispuesto en la *Guía*, que resultará de aplicación supletoria en todo lo no previsto expresamente en estas *Normas*.

Artículo 3. Ámbito de aplicación

1. Estas *Normas* resultan de aplicación a todas las sociedades que integran el Grupo, incluyendo las sociedades participadas sobre las que tiene un control efectivo, dentro de los límites previstos en la normativa aplicable a las actividades reguladas desarrolladas por el Grupo en los distintos países en los que está presente.
2. Quedarán excluidas del ámbito de aplicación de estas *Normas* las sociedades del Grupo que sean cotizadas y dispongan de normas de gobierno corporativo similares a las de la Sociedad, así como sus sociedades dependientes.

Artículo 4. Difusión

Estas *Normas* se comunicarán y difundirán de conformidad con el plan diseñado al efecto por la Unidad entre las Personas Afectadas y los Iniciados, quienes tendrán la obligación de conocerlas y cumplirlas.

Artículo 5. Obligaciones de las Personas Afectadas y los Iniciados en relación con la Información Privilegiada

Las Personas Afectadas que dispongan de Información Privilegiada y, en todo caso, los Iniciados, estarán obligados a:

a) Salvaguardar la confidencialidad de la Información Privilegiada a la que tengan acceso, sin perjuicio de su deber de comunicación y colaboración con las autoridades judiciales y administrativas en los términos previstos en el RAM y demás legislación aplicable.
b) Adoptar las medidas adecuadas para evitar que la Información Privilegiada pueda ser objeto de utilización abusiva o desleal.
c) Comunicar a la Unidad de forma inmediata cualquier uso abusivo o desleal de Información Privilegiada del que tengan conocimiento.

Artículo 6. Interpretación

1. Estas *Normas* se interpretarán de conformidad con la normativa legal que resulte aplicable al Grupo y las disposiciones del Sistema de gobierno corporativo de la Sociedad y, en particular, con las contenidas en el *Reglamento interno de conducta*.
2. Corresponde a la Unidad resolver cualesquiera consultas o dudas que se originen en relación con el contenido, interpretación, aplicación o cumplimiento de estas *Normas*.

TÍTULO I. REGLAS Y PROCEDIMIENTOS PARA EL TRATAMIENTO Y TRANSMISIÓN, INTERNA Y EXTERNA, DE INFORMACIÓN PRIVILEGIADA

Artículo 7. Procedimiento para la determinación del carácter privilegiado de la información

Corresponde al Director del Área responsable de la coordinación de los trabajos u operación a que se refiera la información susceptible de ser calificada como Información Privilegiada determinar su carácter privilegiado. A estos efectos:

a) El Director del Área responsable de la coordinación de cualquier proceso interno que conlleve el acceso a información susceptible de ser considerada Información Privilegiada o de cualquier operación, financiera o jurídica, en fase de estudio o negociación, en la que se reciba o genere dicha información, deberá analizarla con el objeto de verificar si reúne las características para ser considerada Información Privilegiada, declarando, en su caso, su carácter privilegiado.

b) En el supuesto de que el Director del Área determine efectivamente que se trata de Información Privilegiada, el tratamiento y transmisión de la información deberán ajustarse a lo dispuesto en estas *Normas*. Asimismo, deberá informar a la mayor brevedad posible a la Unidad, a través de su director, de que existe un proceso interno o un proyecto en el que se va a recibir, generar o manejar Información Privilegiada y de que se han puesto en marcha las medidas oportunas para salvaguardar su confidencialidad.

c) En todo caso, el Director del Área podrá consultar a la Unidad en aquellos supuestos en que no pueda determinar claramente si se halla o no ante Información Privilegiada.

d) Sin perjuicio de lo anterior, la Unidad podrá solicitar en todo momento información adicional al Director del Área sobre un determinado proyecto, así como revocar, en su caso, la calificación otorgada por el Director del Área en el supuesto de que concluya que no se trata de Información Privilegiada, en cuyo caso deberá fundar debidamente su decisión y explicar por escrito al Director del Área los motivos de la discrepancia.

Artículo 8. Autorización de acceso

1. Corresponde al Director del Área autorizar o denegar el acceso a la Información Privilegiada, que solo se concederá a las personas cuyo acceso resulte imprescindible por motivo de su trabajo.
2. Con la periodicidad que determine la Unidad, se procederá a la revisión de las autorizaciones concedidas, a fin de garantizar que no existe, más allá de un plazo razonable (que deberá ser el mínimo posible), ninguna persona que, sin tener necesidad justificada de poseer autorización para acceder a Información Privilegiada, esté autorizada para ello.

Artículo 9. Registro de Iniciados

El Director del Área o la persona en quien este delegue deberá adoptar las medidas necesarias para que todas las personas que acceden a Información Privilegiada queden debidamente incorporadas a un Registro de Iniciados, conforme a lo dispuesto en el *Reglamento interno de conducta*.

Artículo 10. Gestión de documentos confidenciales

1. Denominación y nombre en clave: el Área responsable asignará un nombre en clave a cada operación en la que se reciba o genere Información Privilegiada. Dicho nombre se empleará en todas las comunicaciones relacionadas con la operación, de tal forma que no se pueda identificar a las partes involucradas ni sus características.
2. Marcado o etiquetado: los documentos confidenciales deberán etiquetarse con la leyenda "CONFIDENCIAL" en la portada y en cada una de las restantes páginas, incluyéndose su fecha de emisión.
3. Uso, control de acceso y almacenamiento
   a) Principio general

      El acceso a los documentos confidenciales, cualquiera que sea su formato, medio y ubicación de almacenamiento, deberá estar restringido a las Personas Autorizadas.

      Los administradores de sistemas, el personal técnico de sistemas y el personal de otros servicios auxiliares deberán tener restringida al máximo la posibilidad de acceso a equipos o ubicaciones en los que se almacene Información Privilegiada. En el caso de que el acceso por parte de alguna de las personas anteriores resulte imprescindible, el número de personas con acceso deberá ser el mínimo necesario, dicho acceso deberá registrarse y, en el caso del personal de un prestador de servicios externo al Grupo, el contrato de prestación de servicios deberá incluir cláusulas que garanticen la confidencialidad de la Información Privilegiada a la que, en su caso, se haya podido tener acceso durante la prestación del servicio.

   b) Documentación en formato electrónico

      Las Personas Autorizadas deberán usar sitios de la red interna de acceso restringido para el depósito temporal o permanente de documentos confidenciales, a los que únicamente dichas personas puedan acceder. En cuanto a los correos electrónicos que contengan Información Privilegiada o que incorporen anexos con Información Privilegiada, es recomendable eliminarlos de los buzones de correo y guardarlos en sitios de la red interna de acceso restringido. En ningún caso se emplearán lápices de memoria o memorias USB para almacenar o transmitir Información Privilegiada.

      Los documentos confidenciales en formato electrónico deberán estar cifrados. A este respecto, se puede considerar que un documento está cifrado si lo está el soporte o ubicación en que esté contenido.

      Asimismo, las Personas Autorizadas tendrán la máxima precaución para evitar que personas no autorizadas puedan ver los documentos confidenciales mientras estén trabajando con ellos en el ordenador. Los documentos confidenciales de-

berán imprimirse en impresoras locales o que requieran el uso de una contraseña, ubicadas en zonas de acceso limitado, y se deberán recoger inmediatamente después de su impresión. En el caso particular de que un equipo que contenga Información Privilegiada deba sufrir operaciones de reparación o mantenimiento y estas tengan lugar en el propio puesto de trabajo, el usuario del equipo deberá estar presente durante las mismas. Si las operaciones antes mencionadas requirieren el traslado del equipo, pero no afectaran a la unidad de memoria en la que estén alojados los datos, esta deberá ser desmontada y dejada en custodia del usuario, quien deberá guardarla bajo llave. Por el contrario, si las operaciones antes mencionadas requieren el traslado del equipo y requieren o pueden requerir intervención sobre la unidad de memoria en la que estén alojados los datos, el traslado del equipo deberá contar con la autorización expresa del Director del Área. Siempre que fuera posible, previamente al traslado, deberá eliminarse la Información Privilegiada contenida en la memoria del equipo (véase el apartado 5 siguiente).

c) Documentación en papel

Cuando una Persona Autorizada se ausente de su puesto de trabajo, deberá guardar de forma segura los documentos confidenciales.

Las Personas Autorizadas evitarán, en lo posible, depositar en mesas o salas de reuniones los documentos confidenciales, que deberán guardarse en lugares de acceso restringido (tales como despachos y archivos) y depositarse en archivadores (que, como regla general, deberán permanecer cerrados), cuyas llaves o combinaciones de acceso estarán exclusivamente al alcance de dichas personas. En el caso de que se detectara el riesgo de copias de llaves o códigos de acceso, deberá procederse a su sustitución o cambio.

d) Uso en viajes y lugares/transportes públicos

Cuando las Personas Autorizadas viajen con documentos confidenciales (tanto en soporte electrónico como en papel) tendrán la máxima precaución en lugares y transportes públicos (aeropuertos, aviones, trenes, taxis, etc.) para evitar el olvido, extravío o robo de los documentos confidenciales e impedir que personas no autorizadas puedan ver su contenido de forma accidental o intencionada.

En particular, las Personas Autorizadas deberán mantener los documentos confidenciales bajo su control en todo momento, evitando depositarlos en equipajes que vayan a facturarse, dejarlos en el interior de un vehículo (aunque este permanezca cerrado) o en una habitación de hotel al ausentarse de ella. Si fuera imprescindible dejar los documentos confidenciales en un hotel, se deberá hacer uso de la caja fuerte.

4. Copia, distribución y transmisión

a) Normas generales

Se prohíbe la realización de copias de documentos confidenciales, salvo que el Director del Área lo autorice, previa y expresamente, para la entrega de dichas copias a una Persona Autorizada. Los destinatarios de las copias deberán ser advertidos de la prohibición de realizar segundas copias. Únicamente las Personas Autorizadas podrán realizar copias de documentos confidenciales. Las copias de un documento confidencial estarán sujetas a los mismos requerimientos de protección y control que el original.

La distribución o transmisión, interna o externa, de Información Privilegiada se llevará a cabo previa autorización expresa del Director del Área.

En cuanto responsable de la custodia de la Información Privilegiada, el área encargada de la coordinación de los trabajos u operación a la que se refiera dicha información establecerá un mecanismo (manual o automatizado) para el control de la copia, distribución y transmisión de la Información Privilegiada que garantice su trazabilidad, es decir, que pueda ser identificado el documento confidencial del que proviene cada copia, quién ha sido el responsable de hacerla, qué copias se han hecho y quién es el responsable de cada una.

Asimismo, cuando resulte proporcionado y factible a criterio de la Unidad, se establecerán mecanismos que posibiliten la detección de filtraciones o envíos no autorizados de Información Privilegiada, los cuales estarán diseñados para facilitar una posterior auditoría de procedimientos que permita conocer el origen de tal filtración.

— Medidas específicas para documentación en formato electrónico

Las Personas Autorizadas emplearán canales seguros (correo cifrado, VPN, FTP seguro, etc.) para la distribución de documentos confidenciales en formato electrónico y, en particular, no se utilizarán con este fin sitios de la red interna que no sean de acceso restringido.

Para la distribución de soportes informáticos, serán de aplicación las medidas del punto siguiente y, además, se deberá cifrar su contenido.

— Medidas específicas para documentación en papel

Los documentos confidenciales en versión impresa deberán transmitirse en sobre cerrado a nombre de la Persona Autorizada destinataria y con una marca indicando la naturaleza de la información que contiene (por ejemplo, “INFORMACIÓN CONFIDENCIAL”). El sobre deberá ser de un solo uso y permitir revelar su apertura no autorizada. Adicionalmente, deberá enviarse un correo electrónico al receptor indicando que se le va a enviar información, sin indicar su naturaleza, y requerirse el envío de un correo electrónico de respuesta por parte del receptor cuando se haya producido la recepción efectiva. La recogida y entrega de los documentos confidenciales con Información Privilegiada deberá realizarse en mano, evitando depositarla en bandejas o en la mesa del destinatario sin estar este presente.

En los envíos al exterior, sea a otros edificios de la Sociedad o no, el transporte de los documentos confidenciales deberá realizarse por personal autorizado y con las suficientes medidas de seguridad para garantizar su transporte seguro. Si el envío es fuera de la Sociedad se deberá realizar a través de mensajero, con albarán de entrega. En cualquier caso, deberá existir un registro de entradas y salidas de este tipo de envíos.

Durante el proceso de entrega, los documentos confidenciales deberán almacenarse en lugares que cumplan las medidas de acceso y almacenamiento arriba especificadas. En caso de pérdida o robo, se deberá avisar inmediatamente al emisor.

Se deberá evitar el uso del fax como medio de transmisión de Información Privilegiada. En caso de ser imprescindible su uso, deberá avisarse al destinatario en el momento del envío para asegurarse de que recoge el documento en el mismo momento de su impresión en destino.

b) Previsiones adicionales para la transmisión de Información Privilegiada a terceros

Sin perjuicio de la aplicación de las reglas y procedimientos descritos en los apartados precedentes de estas *Normas*, la transmisión de Información Privilegiada a los Receptores Externos deberá restringirse a aquellos supuestos en los que, a juicio del Director del Área, resulte imprescindible, y se ajustará particularmente a lo dispuesto en este apartado:

— La Información Privilegiada se transmitirá a los Receptores Externos tan tarde como sea posible atendiendo a las características de la operación de que se trate.

— Con anterioridad a la transmisión de cualquier Información Privilegiada, los Receptores Externos deberán suscribir un compromiso de confidencialidad con la Sociedad, salvo cuando el Receptor Externo esté sometido a un régimen legal o contractual que recoja el deber de confidencialidad. En todo caso, los Receptores Externos serán informados y deberán manifestar, al menos, que conocen: (i) el carácter confidencial de la información transmitida, (ii) las obligaciones derivadas de la normativa aplicable a la Información Privilegiada y (iii) las consecuencias de la infracción de dicha normativa, así como que (iv) disponen de los medios necesarios para garantizar el carácter confidencial de la Información Privilegiada. Se les informará, asimismo, de su inclusión en el Registro de Iniciados.

Se exigirá, asimismo, la firma de dicho compromiso de confidencialidad a aquellos Receptores Externos con los que se contacte en una fase preliminar y a los que se presenten las líneas generales de una operación para solicitar ofertas de financiación o asesoramiento, aunque finalmente no participen en la misma.

— En el supuesto de que se transmita Información Privilegiada a uno o varios Receptores Externos integrados en una misma firma o entidad, el compromiso de confidencialidad previsto en el apartado anterior deberá suscribirse con la firma o entidad correspondiente, obligando por igual a todos los miembros de su organización que lleguen a tener conocimiento de la Información Privilegiada. En estos casos, no será necesaria la autorización previa y expresa del Director del Área para transmitir la Información Privilegiada internamente a los miembros de la organización que precisen conocerla.

Asimismo, en los supuestos previstos en el párrafo anterior, el tratamiento interno de la Información Privilegiada se someterá a las previsiones que a estos efectos tengan establecidas las organizaciones a las que pertenezcan los Receptores Externos.

— El contenido y las implicaciones del compromiso de confidencialidad deberán exponerse verbalmente de forma clara y precisa cuando se trate de Receptores Externos que puedan no estar familiarizados con el régimen legal aplicable.

— En todo caso, la transmisión de Información Privilegiada por un Receptor Externo requerirá la autorización previa por escrito del Director del Área y la firma por el segundo Receptor Externo de un compromiso de confidencialidad equivalente.

— La Unidad podrá condicionar la transmisión electrónica de Información Privilegiada a los Receptores Externos a la encriptación de los documentos confidenciales a través de cualquier procedimiento informático que restrinja el acceso a la Información Privilegiada a los Receptores Externos.

5. Eliminación: las Personas Autorizadas que hayan tenido acceso a Información Privilegiada deberán destruir cualquier soporte que contenga esta información en el momento en el que haya dejado de ser útil, salvo que exista algún requisito, legal o de negocio, que justifique su mantenimiento. En este sentido, se deberá tener en cuenta que no solo han de destruirse versiones definitivas de los documentos confidenciales, sino también todos los borradores, copias, extractos y demás documentos de trabajo que contengan Información Privilegiada.

Cuando resulte proporcionado y factible a criterio de la Unidad, los documentos confidenciales en formato electrónico deberán eliminarse utilizando una herramienta de borrado que garantice que la información eliminada es irrecuperable.

En el caso particular de que se retire o se dé de baja un ordenador del Grupo (que contenga o haya contenido Información Privilegiada) o se sustituya la memoria interna u otro dispositivo de almacenamiento de datos, este deberá destruirse de forma que no pueda recuperarse la información almacenada.

Por su parte, para la destrucción de documentos confidenciales en papel se emplearán los medios dispuestos por la Sociedad al efecto, consistentes en destructoras de papel (para cantidades pequeñas de documentación) y en un servicio centralizado de destrucción masiva de documentación (para grandes volúmenes).

La destrucción de los documentos confidenciales será ejecutada exclusivamente por las Personas Autorizadas; en particular, no se encomendará la destrucción de documentos confidenciales a personas que no estén autorizadas para acceder a ellos.

En el supuesto de que en el proceso de destrucción de la documentación participaran agentes externos a la Sociedad (por ejemplo, empresas especializadas en destrucción en el caso de destrucción de grandes volúmenes de documentación) en los contratos de prestación de servicios deberán incluirse cláusulas que garanticen la confidencialidad de la Información Privilegiada a la que hayan podido tener acceso dichos agentes externos durante el proceso de su destrucción. Asimismo, se requerirá la expedición de un certificado acreditativo de la destrucción de los documentos confidenciales por parte de los agentes externos.

Artículo 11. Protección de conversaciones

1. No se tratará de asuntos relacionados con Información Privilegiada en conversaciones con personas que no estén autorizadas a acceder a esa información o en entornos o condiciones en los que las conversaciones puedan ser escuchadas por personas no autorizadas.
2. Las conversaciones en las que se trate Información Privilegiada se llevarán a cabo en salas que garanticen el adecuado aislamiento acústico y visual. Dichas salas deberán cerrarse desde el interior para evitar irrupciones imprevistas de personas no autorizadas.
3. Se evitará en la medida de lo posible tratar Información Privilegiada mediante conversaciones telefónicas. Cualquier conversación telefónica en la que se trate Información Privilegiada se deberá llevar a cabo utilizando, en ambos extremos, teléfonos digitales o móviles. Debe tenerse en cuenta que los sistemas de mensajes de voz pueden ser objeto de intrusión. Por ello, habrá que tomar ciertas precauciones en su uso:
   a) Cambiar la clave de acceso por defecto al sistema de mensajes de voz.
   b) No dejar nunca mensajes de voz que contengan o traten sobre Información Privilegiada.
4. Para las videoconferencias o audioconferencias en las que se trate Información Privilegiada solo se deberán usar los medios proporcionados al efecto por la Sociedad. Asimismo, será de aplicación lo expuesto en el apartado 2 anterior.

TÍTULO II. PROTOCOLO DE ACTUACIÓN EN CASO DE FILTRACIÓN O USO ILÍCITO DE INFORMACIÓN PRIVILEGIADA

Artículo 12. Protocolo de actuación en caso de filtración o uso ilícito de Información Privilegiada

En el supuesto de que cualquier Persona Autorizada detecte una posible filtración o un uso ilícito de Información Privilegiada, se procederá conforme a lo dispuesto seguidamente:

a) El denunciante trasladará, lo antes posible, la filtración o uso ilícito de Información Privilegiada del que haya tenido conocimiento a la Unidad en la persona de su presidente o, en su defecto, del director o del secretario de la Unidad. A estos efectos, la Unidad establecerá canales seguros para la denuncia de las filtraciones o usos ilícitos de Información Privilegiada, procurándose la máxima protección respecto de la identidad del denunciante.
b) La Unidad analizará y verificará la veracidad de la información proporcionada por el denunciante, a cuyos efectos podrá solicitar a la Dirección de Finanzas y Recursos, así como a cualquier otra Dirección de la Sociedad, aquellos datos e informaciones adicionales que estime necesarios.
c) De comprobarse la veracidad de la denuncia, si la filtración o uso ilícito de la Información Privilegiada es atribuible a un miembro del Consejo de Administración de la Sociedad, la Unidad lo pondrá en conocimiento del secretario del Consejo de Administración, que adoptará las medidas correspondientes de acuerdo con lo dispuesto en las normas del Sistema de gobierno corporativo de la Sociedad y en la legislación aplicable.
d) En cambio, si la filtración o uso ilícito de la Información Privilegiada es atribuible a un empleado del Grupo, la Unidad lo pondrá en conocimiento de la Dirección de Finanzas y Recursos, que aplicará las medidas disciplinarias conforme al régimen de faltas y sanciones previsto en el Convenio Colectivo aplicable a la sociedad del Grupo a la que pertenezca dicho empleado o en la legislación laboral que resulte de aplicación, así como de la Dirección de los Servicios Jurídicos de la Corporación, que evaluará la procedencia de emprender, en su caso, las acciones legales que correspondan contra el empleado responsable de la filtración o uso ilícito de la Información Privilegiada, conforme a la legislación vigente en cada momento.
e) Finalmente, en el supuesto de que, verificada la veracidad de la denuncia, la filtración o uso ilícito de la Información Privilegiada sea atribuible a un Receptor Externo o a cualquier otra persona o entidad ajena al Grupo, la Unidad lo pondrá en conocimiento de la Dirección de los Servicios Jurídicos de la Corporación con el objeto de determinar la adopción de las medidas que se estimen convenientes respecto de la persona o entidad responsable de la filtración o uso ilícito de la Información Privilegiada.
f) Sin perjuicio de lo anterior, cuando una filtración o uso ilícito de Información Privilegiada trascienda al mercado, de manera que se generen noticias o rumores que versen sobre una Información Privilegiada que no haya sido previamente comunicada a la CNMV o se produzca una evolución anormal de los volúmenes contratados o de los precios negociados de los Valores Afectados, resultarán de aplicación, asimismo, las disposiciones contenidas en el *Protocolo de actuación para la gestión de noticias y rumores*.