III. OTRAS DISPOSICIONES

MINISTERIO DE POLÍTICA TERRITORIAL Y ADMINISTRACIÓN PÚBLICA

18187 *Orden TAP/3148/2011, de 7 de octubre, por la que se aprueba la política de seguridad de la información en el ámbito de la administración electrónica del Ministerio de Política Territorial y Administración Pública.*

La Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, señala entre sus fines el crear las condiciones de confianza en el uso de los medios electrónicos, estableciendo las medidas necesarias para la preservación de la integridad de los derechos fundamentales, y en especial los relacionados con la intimidad y la protección de datos de carácter personal. Para ello indica que es preciso garantizar la seguridad de los sistemas de información y comunicaciones, y de los datos y servicios por ellos manejados. Dichos sistemas de información son hoy en día cada vez más críticos y están sometidos a diferentes tipos de amenazas y vulnerabilidades.

En la Administración Electrónica se entiende por seguridad la capacidad de las redes o de los sistemas de información para resistir, con un determinado nivel de confianza, los accidentes y acciones ilícitas o malintencionadas que comprometan la disponibilidad, autenticidad, integridad, confidencialidad y trazabilidad de los datos almacenados o transmitidos y de los servicios que dichas redes o sistemas ofrecen, o a través de los cuales se realiza el acceso.

El Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad (ENS) en el ámbito de la Administración Electrónica, persigue fundamentar la confianza en que los sistemas de información prestarán sus servicios y custodiarán la información de acuerdo con sus especificaciones funcionales, sin interrupciones o modificaciones fuera de control, y sin que la información pueda llegar a conocimiento de personas no autorizadas.

El ENS establece el marco regulatorio de la Política de Seguridad de la Información (PSI), que se plasma en un documento, accesible y comprensible para todos los miembros, que define lo que significa seguridad de la información en una organización determinada y que rige la forma en que una organización gestiona y protege la información y los servicios que considera críticos, disponiendo que:

1. Todos los órganos superiores, esto es, Ministerios y Secretarías de Estado en la Administración General del Estado (AGE), deberán disponer formalmente de su PSI, que será aprobada por el titular del órgano superior correspondiente (artículo 11).
2. La PSI debe comprometer a todos los miembros de la organización, por los que debe ser conocida, e identificar unos claros responsables de velar por su cumplimiento (artículo 13).
3. El contenido mínimo de la PSI debe precisar de forma clara los objetivos o misión de la organización, el marco legal y regulatorio en que desarrolla sus actividades, los roles o funciones de seguridad, definiendo para cada uno sus deberes y responsabilidades, así como el procedimiento para su designación y renovación, la estructura del comité para la gestión y coordinación de la seguridad, detallando su ámbito de responsabilidad, sus miembros y su relación con otros elementos de la organización, y las directrices para la estructuración de la documentación de seguridad del sistema, su gestión y acceso [anexo II.3 Política de Seguridad (org 1)].
4. Además, la PSI debe ser coherente con lo establecido en el Documento de Seguridad que exige el artículo 88 del Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, aprobado por

cve: BOE-A-2011-18187

Real Decreto 1720/2007, de 21 de diciembre, en lo que corresponda, prevaleciendo lo relativo a la protección de datos de carácter personal en caso de discrepancias.

5. Para la elaboración de la PSI son una referencia las guías CCN-STIC 001, 201, 402, 801 y 805 elaboradas por el Centro Criptológico Nacional (CCN) del Centro Nacional de Inteligencia (CNI), que establecen las pautas de carácter general relativas a la organización de seguridad y sus responsables, así como sobre la estructura y contenido mínimo de la PSI.

El proyecto de orden ministerial ha sido informado por la Comisión Ministerial de Administración Electrónica y por el Consejo Superior de Administración Electrónica.

En su virtud, dispongo:

Artículo 1. *Objeto y ámbito de aplicación.*

1. Constituye el objeto de la presente orden la aprobación de la Política de Seguridad de la Información (en adelante, PSI) en el ámbito de la Administración Electrónica del Ministerio de Política Territorial y Administración Pública, así como el establecimiento del marco organizativo y tecnológico de la misma.

2. La PSI que se aprueba por esta orden se aplicará con carácter imperativo por todos los órganos y unidades centrales y territoriales del Ministerio de Política Territorial y Administración Pública, así como por los organismos públicos adscritos al mismo (Instituto Nacional de Administración Pública, Mutualidad General de Funcionarios Civiles del Estado y Agencia Estatal de Evaluación de las Políticas Públicas y la Calidad de los Servicios), siendo de aplicación a todos sus sistemas de información y debiendo ser observada por todo el personal destinado en dichos órganos, unidades y organismos, así como por aquellas personas que, aunque no estén destinadas en los mismos, tengan acceso a sus sistemas de información o a la información gestionada por ellos.

Artículo 2. *Misión del Departamento.*

Corresponde al Ministerio de Política Territorial y Administración Pública lo previsto en el Real Decreto 393/2011, de 18 de marzo, de desarrollo de la estructura orgánica básica del Ministerio de Política Territorial y Administración Pública.

Artículo 3. *Marco normativo.*

1. El marco normativo en que se desarrollan las actividades del Ministerio de Política Territorial y Administración Pública comprende la legislación sectorial reguladora de la actuación de los órganos superiores y directivos del Ministerio y de los organismos públicos adscritos, así como la normativa en vigor correspondiente a la administración electrónica.

2. También forman parte del marco normativo las restantes normas aplicables a la administración electrónica del Departamento derivadas de las anteriores y publicadas en las sedes electrónicas comprendidas dentro del ámbito de aplicación de la PSI.

Artículo 4. *Estructura organizativa de la PSI.*

La estructura organizativa de la gestión de la seguridad de la información en el ámbito de la Administración Electrónica del Ministerio de Política Territorial y Administración Pública está compuesta por los siguientes agentes:

a) El Comité para la Gestión y Coordinación de la Seguridad de la Información.
b) Los Responsables de Seguridad.
c) Los Responsables de la Información.
d) Los Responsables del Servicio.
e) Los Responsables del Sistema.

cve: BOE-A-2011-18187

Artículo 5. *El Comité para la Gestión y Coordinación de la Seguridad de la Información.*

1. Se crea el Comité para la Gestión y Coordinación de la Seguridad de la Información (en adelante, el Comité). El Comité se configura como un grupo de trabajo en el seno de la Comisión Ministerial de Administración Electrónica del Departamento. El Comité estará compuesto por los siguientes miembros:

a) Presidencia: El titular de la Dirección General de Relaciones Institucionales y Organización.
b) Vicepresidencia: El titular de la Dirección General de Impulso para la Administración Electrónica.
c) Vocalías: Con categoría mínima de Subdirector General o asimilado, pudiendo delegar en un suplente, por cada uno de los siguientes órganos u organismos del Departamento:

i. Gabinete del Vicepresidente de Política Territorial y Ministro de Política Territorial y Administración Pública.
ii. Secretaría de Estado para la Función Pública.
iii. Secretaría de Estado de Cooperación Territorial.
iv. Subsecretaría de Política Territorial y Administración Pública.
v. Instituto Nacional de Administración Pública (INAP).
vi. Mutualidad General de Funcionarios Civiles del Estado (MUFACE)
vii. Agencia Estatal de Evaluación de las Políticas Públicas y la Calidad de los Servicios (AEVAL).

d) Secretaría: con voz y voto, el Director de la División de Sistemas de Información y Comunicaciones, que ejecutará las decisiones del Comité, convocará sus reuniones y preparará los temas a tratar. En caso de ausencia, vacante o enfermedad, ejercerá sus funciones el vocal que designe el Comité.

2. El Comité coordinará todas las actividades relacionadas con la seguridad de los sistemas de información y ejercerá las siguientes funciones:

a) Elaborar las propuestas de modificación y actualización de la PSI.
b) Velar por el cumplimiento y difusión de la PSI, promoviendo las actividades de concienciación y formación en materia de seguridad para el personal del Departamento.
c) Elaborar y aprobar unas directrices y normas de seguridad generales para todo el Ministerio que deberá cumplir todo el desarrollo normativo indicado en el artículo 13.
d) Aprobar la normativa de seguridad de segundo nivel, que según el artículo 13 se corresponde con las políticas específicas de seguridad y con las normas STIC, de obligado cumplimiento.
e) Coordinación, supervisión y seguimiento de las decisiones y actuaciones de los diferentes Responsables de Seguridad, resolviendo los posibles conflictos entre los mismos bajo el criterio de garantizar la seguridad de las infraestructuras tecnológicas compartidas.
f) Impulsar los proyectos para la adecuación al cumplimiento del Esquema Nacional de Seguridad.
g) Coordinar la comunicación con el Centro Criptológico Nacional en la utilización de servicios de respuesta a incidentes de seguridad de especial gravedad.
h) Informar sobre el estado de las principales variables de seguridad en los sistemas de información al Comité de Seguridad de la Información de las Administraciones Públicas para la elaboración de un perfil general del estado de seguridad de las mismas.
i) Compartir experiencias de éxito en materia de seguridad entre sus miembros para velar por el cumplimiento de la PSI y su normativa de desarrollo.
j) Tomar todas aquellas decisiones que garanticen, en última instancia, la seguridad de la información y servicios del Ministerio.

cve: BOE-A-2011-18187

3. El Comité ajustará su funcionamiento a las previsiones contenidas en el capítulo II de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, relativo a los órganos colegiados.

4. El Comité se reunirá con carácter ordinario al menos una vez al año, y con carácter extraordinario cuando lo decida su Presidente.

5. Los vocales indicados en el artículo 5.1.c serán designados por el Presidente del Comité, a propuesta de los titulares de los correspondientes órganos y organismos.

6. El Comité podrá recabar de personal técnico, propio o externo, la información pertinente para la toma de sus decisiones. En caso necesario este personal podrá ser convocado por el Comité para su asistencia a las reuniones, en calidad de asesores, con voz pero sin voto.

Artículo 6. *Los Responsables de Seguridad.*

1. Conforme al artículo 10 del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica (ENS), el Responsable de Seguridad es la persona que determina las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios.

2. Se designarán los siguientes Responsables de Seguridad, según su ámbito de responsabilidad:

a. Responsable de Seguridad cuyo ámbito de responsabilidad comprende la información y servicios afectados por los sistemas de información gestionados por la Subsecretaría de Política Territorial y Administración Pública. Será un funcionario perteneciente a la Subsecretaría de Política Territorial y Administración Pública.

b. Responsable de Seguridad cuyo ámbito de responsabilidad comprende la información y servicios afectados por aquellos sistemas de información gestionados por la Dirección General para el Impulso de la Administración Electrónica que de manera general se ofrecen a las Administraciones Públicas. Será un funcionario perteneciente a la Dirección General para el Impulso de la Administración Electrónica.

c. Responsables de Seguridad de cada uno de los organismos públicos adscritos al Departamento (INAP, MUFACE Y AEVAL), cuyo ámbito de responsabilidad comprende la información y servicios afectados por los sistemas de información gestionados por el organismo. Para cada organismo en cuestión será un funcionario perteneciente al mismo.

3. Los Responsables de Seguridad serán nombrados y cesados por el Comité.

4. Serán funciones de cada Responsable de Seguridad, dentro de su ámbito de actuación, las siguientes:

a) Promover la seguridad de la información manejada y de los servicios electrónicos prestados por los sistemas de información.

b) Proponer al Comité de Seguridad la normativa de seguridad de segundo nivel, que según el artículo 13 se corresponde con las políticas específicas de seguridad y con las normas STIC, de obligado cumplimiento.

c) Aprobar la normativa de seguridad de tercer nivel, que según el artículo 13 se corresponde a los procesos, procedimientos STIC e instrucciones técnicas STIC, de obligado cumplimiento.

d) Encargarse de que la documentación de seguridad se mantenga organizada y actualizada, y de gestionar los mecanismos de acceso a la misma.

e) Promover las actividades de concienciación y formación en materia de seguridad en su ámbito de responsabilidad, siguiendo las directrices marcadas por el Comité.

f) Realizar la coordinación y seguimiento de la implantación de los proyectos de adecuación al Esquema Nacional de Seguridad.

g) Asesorar, en colaboración con el Responsable del Sistema, a los Responsables de la Información y a los Responsables del Servicio en la realización de los preceptivos análisis de riesgos, y revisar el proceso de gestión del riesgo, elevando un informe anual al Comité.

cve: BOE-A-2011-18187

h) Promover auditorías periódicas para verificar el cumplimiento de las obligaciones en materia de seguridad de la información, y analizar los informes de auditoría, elaborando las conclusiones a presentar a los Responsable del Servicio y los Responsables de la Información para que adopten las medidas correctoras adecuadas.

i) Coordinar el proceso de Gestión de la Seguridad.

j) Firmar la Declaración de Aplicabilidad, que comprende la relación de medidas de seguridad seleccionadas para un sistema (art. 27 y anexo II.2 del ENS).

k) Elaborar informes periódicos de seguridad para el Comité que incluyan los incidentes más relevantes de cada período, así como cualquier otra documentación de apoyo que el Comité necesite recabar dentro del ámbito de actuación del Responsable de Seguridad.

5. Cuando la complejidad, distribución, separación física de sus elementos o número de usuarios de los sistemas de información lo justifiquen, cada Responsable de Seguridad podrá designar los responsables de seguridad delegados que considere necesarios, que tendrán dependencia funcional directa de aquél y serán responsables en su ámbito de todas aquellas acciones que les delegue el mismo.

Artículo 7. *Los Responsables de la Información.*

1. Conforme a los artículos 10 y 44 del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica (ENS), el Responsable de la Información es la persona que establece las necesidades de seguridad de la información que se maneja y efectúa las valoraciones del impacto que tendría un incidente que afectara a su seguridad. Tiene además, en exclusiva, la potestad de modificar el nivel de seguridad requerido para la misma (anexo II.5.7.2 del ENS).

2. Esta responsabilidad recaerá en el titular del órgano o unidad administrativa que gestione el procedimiento o trámite.

3. Son funciones de cada Responsable de Información, dentro de su ámbito de actuación, las siguientes:

a. Determinar los niveles de seguridad de la información tratada, valorando los impactos de los incidentes que afecten a la seguridad de la información (artículo 44 del ENS).

b. Son los encargados, junto a los Responsables del Servicio y contando con la participación y asesoramiento del Responsable de Seguridad y del Responsable del Sistema, de realizar los preceptivos análisis de riesgos, y de seleccionar las salvaguardas a implantar.

c. Son los responsables, junto a los Responsables del Servicio, de aceptar los riesgos residuales calculados en el análisis de riesgos, y de realizar su seguimiento y control, sin perjuicio de la posibilidad de delegar esta tarea.

Artículo 8. *Los Responsables del Servicio.*

1. Conforme al artículo 10 del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica (ENS) el Responsable del Servicio es la persona que determina los requisitos de seguridad de los servicios prestados.

2. Esta responsabilidad recaerá en el titular del órgano o unidad administrativa que gestione cada servicio.

3. Respecto al proceso de gestión del riesgo, los Responsables del Servicio:

a. Son los encargados, junto a los Responsables de la Información y contando con la participación y asesoramiento del Responsable de Seguridad y del Responsable del Sistema, de realizar los preceptivos análisis de riesgos, y de seleccionar las salvaguardas a implantar.

cve: BOE-A-2011-18187

b. Son los responsables, junto a los Responsables de la Información, de aceptar los riesgos residuales calculados en el análisis, y de realizar su seguimiento y control, sin perjuicio de la posibilidad de delegar esta tarea.

Artículo 9. *Los Responsables del Sistema.*

1. Esta responsabilidad recaerá en los titulares de los órganos responsables del desarrollo, mantenimiento y explotación del sistema de información que soporte los servicios correspondientes.
2. Las funciones de los Responsables del Sistema serán las siguientes:

a) Implantar las medidas necesarias para garantizar la seguridad del servicio durante todo su ciclo de vida, siguiendo las indicaciones del Responsable de Seguridad del ámbito de competencia correspondiente.
b) Aprobar toda modificación sustancial de la configuración de cualquier elemento del sistema.
c) Asesorar en colaboración con el Responsable de Seguridad, a los Responsables de la Información y a los Responsables del Servicio en la realización de los preceptivos análisis de riesgos.
d) Determinar la categoría del sistema según el procedimiento descrito en el anexo I del Real Decreto 3/2010, de 8 de enero y las medidas de seguridad que deben aplicarse de acuerdo con lo previsto en el anexo II del mismo real decreto.
e) Suspender el manejo de una determinada información o la prestación de un servicio electrónico si es informado de deficiencias graves de seguridad, previo acuerdo con el Responsable de dicha información o servicio, y con el Responsable de Seguridad.

3. Las funciones citadas en el punto anterior podrán recaer en diferentes personas, en el caso de que las competencias sobre los diferentes activos que componen el sistema (aplicaciones, redes, etc.) o las diferentes fases del ciclo de vida del sistema recaigan sobre unidades distintas.

Artículo 10. *Resolución de conflictos.*

1. En caso de conflicto entre los diferentes responsables que componen la estructura organizativa de la PSI, éste será resuelto por el superior jerárquico de los mismos. En defecto de lo anterior, prevalecerá la decisión del Comité para la Gestión y Coordinación de la Seguridad de la Información.
2. En caso de conflictos entre los responsables que componen la estructura organizativa de la PSI y los definidos en seguimiento de la normativa de protección de datos de carácter personal, prevalecerá la decisión que presente un mayor nivel de exigencia respecto a la protección de los datos de carácter personal.

Artículo 11. *Obligaciones del personal.*

1. Todo el personal que presta servicios en el Departamento y sus organismos públicos adscritos, tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y la normativa de seguridad derivada, siendo responsabilidad del Comité disponer los medios necesarios para que la información llegue a los afectados.
2. Todo el personal que se incorpore al Ministerio de Política Territorial y Administración Pública o vaya a tener acceso a alguno de sus sistemas de información o la información gestionada por ellos deberá ser informado de la PSI.
3. El incumplimiento manifiesto de la Política de Seguridad de la Información o la normativa de seguridad derivada podrá acarrear el inicio de las medidas disciplinarias oportunas y, en su caso, las responsabilidades legales correspondientes.

cve: BOE-A-2011-18187

Artículo 12. *Gestión de riesgos.*

1. La gestión de riesgos debe realizarse de manera continua sobre el sistema de información, conforme a los principios de gestión de la seguridad basada en los riesgos (artículo 6 del Real Decreto 3/2010, de 8 de enero) y reevaluación periódica (artículo 9 del Real Decreto 3/2010, de 8 de enero).

2. Los Responsables de la Información y del Servicio son los encargados, contando en el proceso con la participación y asesoramiento del Responsable de Seguridad y del Responsable del Sistema, de realizar los preceptivos análisis de riesgos, y de seleccionar las salvaguardas a implantar.

3. Los Responsables de la Información y del Servicio son los responsables de los riesgos sobre la información y sobre los servicios, respectivamente, y por tanto de aceptar los riesgos residuales calculados en el análisis, y de realizar su seguimiento y control, sin perjuicio de la posibilidad de delegar esta tarea.

4. El proceso de gestión de riesgos, que comprende las fases de categorización de los sistemas, análisis de riesgos y selección de medidas de seguridad a aplicar, que deberán ser proporcionales a los riesgos y estar justificadas, deberá revisarse cada año por parte del Responsable de Seguridad, que elevará un informe al Comité de Seguridad.

Artículo 13. *Desarrollo normativo de la PSI. Documentación de seguridad.*

1. El cuerpo normativo sobre seguridad de la información es de obligado cumplimiento y se desarrollará en tres niveles, según el ámbito de aplicación y nivel de detalle técnico, de manera que cada norma de un determinado nivel de desarrollo se fundamente en las normas de nivel superior. Dichos niveles de desarrollo normativo son los siguientes:

a) Primer nivel normativo*:* Política de Seguridad de la Información (PSI, constituida por la presente orden), y directrices y normas de seguridad generales para todo el Ministerio que deberá cumplir el resto del desarrollo normativo.

b) Segundo nivel normativo: Políticas Específicas de Seguridad de la Información y Normas de Seguridad TIC (Normas STIC). Las Políticas Específicas desarrollan con un mayor grado de detalle la PSI dentro de un ámbito determinado. Las Normas dan respuesta, sin entrar en detalles de implementación ni tecnológicos, a qué se puede hacer y qué no en relación a un cierto tema desde el punto de vista de la seguridad: qué se considera un uso apropiado o inapropiado, las consecuencias derivadas del incumplimiento, etc.

Los documentos relativos a este segundo nivel normativo los propone cada Responsable de Seguridad, dentro de su ámbito de competencia, y los aprueba el Comité para la Gestión y Coordinación de la Seguridad de la Información.

c) Tercer nivel normativo: Procesos y Procedimientos STIC e Instrucciones Técnicas STIC. Son documentos que dan respuesta, incluyendo detalles de implementación y tecnológicos, a cómo se puede realizar una determinada tarea respetando los principios de seguridad de la organización, y los procesos internos en ella establecidos.

Los Procesos, Procedimientos STIC e Instrucciones Técnicas STIC de un determinado ámbito de actuación los aprueba el correspondiente Responsable de Seguridad.

2. Aparte de los documentos citados en el apartado 1, la documentación de seguridad del sistema podrá contar, bajo criterio del Responsable de Seguridad correspondiente, con otros documentos de carácter no vinculante: recomendaciones, buenas prácticas, informes, registros, evidencias electrónicas, etc.

3. Cada Responsable de Seguridad será responsable dentro de su ámbito de actuación de mantener la documentación de seguridad actualizada y organizada, y de gestionar los mecanismos de acceso a la misma.

4. El Comité establecerá los mecanismos necesarios para compartir la documentación derivada del desarrollo normativo con el propósito de normalizarlo, en la medida de lo posible, en todo el ámbito de aplicación de la PSI.

cve: BOE-A-2011-18187

Artículo 14. *Protección de datos de carácter personal.*

1. En lo que se refiere a los ficheros con datos de carácter personal, estarán referenciados en el correspondiente Documento de Seguridad donde se hará constar tanto los ficheros afectados como los responsables correspondientes.
2. Todos los sistemas de información del Ministerio de la Política Territorial y Administración Pública se ajustarán a los niveles de seguridad requeridos por la normativa de protección de datos de carácter personal. En caso de conflicto con la normativa de seguridad indicada en el artículo 13, prevalecerá la norma que presente un mayor nivel de exigencia respecto a la protección de los datos de carácter personal.

Artículo 15. *Formación y concienciación.*

1. Se desarrollarán actividades formativas específicas orientadas a la concienciación y formación de los empleados públicos del Departamento, así como a la difusión entre los mismos de la PSI y de su desarrollo normativo.
2. A estos efectos, deberán incluirse actividades formativas en esta materia dentro de los Planes de Formación del Ministerio de Política Territorial y Administración Pública.
3. El Comité y los Responsables de Seguridad se encargarán de promover las actividades de formación y concienciación en materia de seguridad, según lo indicado en el artículo 5, apartado 2, letra b y en el artículo 6, apartado 4, letra e de esta Política.

Artículo 16. *Actualización de la PSI.*

Las propuestas de las revisiones de la PSI las elaborará el Comité y serán aprobadas por el titular del Departamento ministerial.

Disposición final primera. *Deber de colaboración de órganos y unidades del Departamento.*

Todos los órganos y unidades del Departamento ministerial y de sus organismos públicos adscritos prestarán su colaboración en las actuaciones de implementación de la PSI aprobada por esta orden.

Disposición final segunda. *Publicidad de la PSI.*

La presente orden se publicará, además de en el «Boletín Oficial del Estado», en la sede electrónica del Ministerio de Política Territorial y Administración Pública.

Disposición final tercera. *Entrada en vigor.*

La presente Orden entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado»

Madrid, 7 de octubre de 2011.–El Vicepresidente del Gobierno de Política Territorial y Ministro de Política Territorial y Administración Pública, Manuel Chaves González.

cve: BOE-A-2011-18187