ISSN 1977-0685

Diario Oficial de la Unión Europea

L 301

Edición en lengua española

Legislación

54° año

18 de noviembre de 2011

Sumario

(continúa al dorso)

Precio: 3 EUR

([1]) Texto pertinente a efectos del EEE

ES

Los actos cuyos títulos van impresos en caracteres finos son actos de gestión corriente, adoptados en el marco de la política agraria, y que tienen generalmente un período de validez limitado.

Los actos cuyos títulos van impresos en caracteres gruesos y precedidos de un asterisco son todos los demás actos.

I

(Actos legislativos)

DIRECTIVAS

DIRECTIVA 2011/87/UE DEL PARLAMENTO EUROPEO Y DEL CONSEJO

de 16 de noviembre de 2011

por la que se modifica la Directiva 2000/25/CE en lo que respecta a la aplicación de fases de emisiones a los tractores de vía estrecha

(Texto pertinente a efectos del EEE)

EL PARLAMENTO EUROPEO Y EL CONSEJO DE LA UNIÓN EUROPEA,

Visto el Tratado de Funcionamiento de la Unión Europea y, en particular, su artículo 114,

Vista la propuesta de la Comisión Europea,

Previa transmisión del proyecto de acto legislativo a los Parlamentos nacionales,

Visto el dictamen del Comité Económico y Social Europeo [1],

Actuando de conformidad con el procedimiento legislativo ordinario [2],

Considerando lo siguiente:

(1) La Directiva 2000/25/CE del Parlamento Europeo y del Consejo, de 22 de mayo de 2000, relativa a las medidas que deben adoptarse contra las emisiones de gases contaminantes y de partículas contaminantes procedentes de motores destinados a propulsar tractores agrícolas o forestales [3], regula las emisiones de escape de los motores instalados en los tractores agrícolas y forestales con miras a reforzar la protección de la salud humana y del medio ambiente. La Directiva 2000/25/CE estableció que los límites de emisiones aplicables en 2010 a la homologación de la mayoría de los motores de encendido por compresión, denominados «límites de la fase III A» debían sustituirse por los de la fase III B, más estrictos, que entraban en vigor progresivamente a partir del 1 de enero de 2011 para la homologación, y a partir del 1 de enero de 2010 para la puesta en el mercado de dichos motores. La fase IV, que prevé valores límite más estrictos que la fase III B, entrará en vigor progresivamente a partir del 1 de enero de 2013 para la homologación de dichos motores y a partir del 1 de enero de 2014 para la puesta en el mercado.

(2) El artículo 2, letra b), de la Directiva 2004/26/CE del Parlamento Europeo y del Consejo, de 21 de abril de 2004, por la que se modifica la Directiva 97/68/CE relativa a la aproximación de las legislaciones de los Estados miembros sobre medidas contra la emisión de gases y partículas contaminantes procedentes de los motores de combustión interna que se instalen en las máquinas móviles no de carretera [4], dispone que la Comisión debe evaluar la tecnología disponible, incluida la relación costes-beneficios, con el fin de confirmar los valores límite de las fases III B y IV y valorar la necesidad de disposiciones de flexibilidad adicionales, excepciones o retrasos de las fechas de introducción para determinados tipos de equipos o motores, tomando en consideración los motores instalados en máquinas móviles no de carretera utilizadas en aplicaciones estacionales. Además, el artículo 4, apartado 8, de la Directiva 2000/25/CE establece una cláusula de revisión para tener en cuenta las especificidades de los tractores de las categorías T2, T4.1 y C2.

(3) La Directiva 97/68/CE del Parlamento Europeo y del Consejo [5] ha sido objeto de varios estudios técnicos. Como resultado de dichos estudios técnicos efectuados en 2007, 2009 y 2010, confirmados por la evaluación de impacto realizada por la Comisión, se ha determinado que para los tractores de las categorías T2, T4.1 y C2 no es técnicamente viable cumplir los requisitos de las fases III B y IV en las fechas previstas en dicha Directiva.

(4) Por lo tanto, para que la legislación de la Unión no prescriba requisitos técnicos que aún no pueden ser cumplidos y evitar una situación en que los tractores de las categorías T2, T4.1 y C2 dejen de poder ser homologados y puestos en el mercado o puestos en circulación, es necesario establecer un período transitorio de tres años durante el cual los tractores clasificados en las categorías T2, T4.1 y C2 puedan seguir siendo homologados y puestos en el mercado o puestos en circulación.

(5) La Comisión debe informar anualmente al Parlamento Europeo y al Consejo acerca de los progresos en el desarrollo de soluciones técnicas para la tecnología que respete los límites de la fase IV.

[1] DO C 132 de 3.5.2011, p. 53.
[2] Posición del Parlamento Europeo de 25 de octubre de2011 (no publicada aún en el Diario Oficial) y Decisión del Consejo de 8 de noviembre de 2011.
[3] DO L 173 de 12.7.2000, p. 1.
[4] DO L 146 de 30.4.2004, p. 1.
[5] DO L 59 de 27.2.1998, p. 1.

(6) Procede, por tanto, modificar la Directiva 2000/25/CE en consecuencia.

HAN ADOPTADO LA PRESENTE DIRECTIVA:

Artículo 1

Modificaciones de la Directiva 2000/25/CE

En el artículo 4 de la Directiva 2000/25/CE, se añade el apartado siguiente:

«9. No obstante lo dispuesto para los tractores de las categorías T2, T4.1 y C2 definidos en el anexo II, capítulo A, punto A.1, segundo guion; en el anexo II, capítulo B, apéndice 1, parte I, punto 1.1, y en el anexo II, capítulo A, punto A. 2 del anexo II de la Directiva 2003/37/CE, respectivamente, y equipados con motores de las categorías L a R, las fechas establecidas en el apartado 2, letras d) y e), y en el apartado 3 se aplazarán tres años. Hasta tales fechas, seguirán aplicándose los requisitos establecidos en la presente Directiva para la fase III A.».

Artículo 2

Disponibilidad de tecnología compatible

La Comisión deberá, antes del 31 de diciembre de 2014, considerar la tecnología disponible que pueda satisfacer los requisitos de la fase IV y sea compatible con las necesidades de las categorías T2, T4.1 y C2 y, en su caso, presentar propuestas al Parlamento Europeo y al Consejo.

Artículo 3

Transposición

1. Los Estados miembros adoptarán y publicarán, a más tardar el 9 de diciembre de 2012, las disposiciones legales, reglamentarias y administrativas necesarias para dar cumplimiento a lo dispuesto en la presente Directiva. Comunicarán inmediatamente a la Comisión el texto de dichas disposiciones.

Cuando los Estados miembros adopten dichas disposiciones, estas incluirán una referencia a la presente Directiva o irán acompañadas de dicha referencia en su publicación oficial. Los Estados miembros establecerán las modalidades de la mencionada referencia.

2. Los Estados miembros comunicarán inmediatamente a la Comisión el texto de las principales disposiciones de Derecho interno que adopten en el ámbito regulado por la presente Directiva.

Artículo 4

Entrada en vigor

La presente Directiva entrará en vigor a los veinte días de su publicación en el *Diario Oficial de la Unión Europea*.

Artículo 5

Destinatarios

Los destinatarios de la presente Directiva serán los Estados miembros.

Hecho en Estrasburgo, el 16 de noviembre de 2011.

Por el Parlamento Europeo	*Por el Consejo*
El Presidente	*El Presidente*
J. BUZEK	W. SZCZUKA

II

(Actos no legislativos)

REGLAMENTOS

REGLAMENTO DE EJECUCIÓN (UE) Nº 1179/2011 DE LA COMISIÓN

de 17 de noviembre de 2011

por el que se establecen especificaciones técnicas para sistemas de recogida a través de páginas web, de conformidad con el Reglamento (UE) nº 211/2011 del Parlamento Europeo y del Consejo sobre la iniciativa ciudadana

LA COMISIÓN EUROPEA,

Visto el Tratado de Funcionamiento de la Unión Europea,

Visto el Reglamento (UE) nº 211/2011, del Parlamento Europeo y del Consejo, de 16 de febrero de 2011, sobre la iniciativa ciudadana [1], y, en particular, su artículo 6, apartado 5,

Previa consulta al Supervisor Europeo de Protección de Datos,

Considerando lo siguiente:

(1) El Reglamento (UE) nº 211/2011 establece que, cuando las declaraciones de apoyo se recojan a través de páginas web, el sistema utilizado a ese fin debe cumplir determinados requisitos técnicos y de seguridad y debe estar acreditado por la autoridad competente del Estado miembro correspondiente.

(2) Un sistema de recogida a través de páginas web en el sentido de lo dispuesto en el Reglamento (UE) nº 211/2011 es un sistema de información compuesto por programas y equipos informáticos, un entorno de alojamiento, unos métodos profesionales y un personal que lleve a cabo la recogida de declaraciones de apoyo.

(3) El Reglamento (UE) nº 211/2011 establece los requisitos que deben cumplir los sistemas de recogida a través de páginas web para estar acreditados y dispone que la Comisión debe adoptar especificaciones técnicas para la aplicación de esos requisitos.

(4) El Proyecto de seguridad de aplicaciones web abiertas (OWASP) — «Top 10 2010» presenta una panorámica de los riesgos de seguridad más críticos de las aplicaciones web, así como herramientas para hacer frente a estos riesgos; por consiguiente, las especificaciones técnicas se basan en las conclusiones de este proyecto.

(5) La aplicación de las especificaciones técnicas por parte de los organizadores debe garantizar la acreditación de los sistemas de recogida a través de páginas web por las autoridades de los Estados miembros y contribuir a garantizar la aplicación de las medidas técnicas y organizativas adecuadas necesarias para dar cumplimiento a las obligaciones impuestas por la Directiva 95/46/CE del Parlamento Europeo y del Consejo [2] relativas a la seguridad de las actividades de tratamiento, tanto en el momento del diseño del sistema de tratamiento como en el momento del tratamiento propiamente dicho, con el fin de mantener la seguridad y, con ello, evitar cualquier tratamiento irregular y proteger los datos personales contra la destrucción, accidental o ilícita, la pérdida accidental, la alteración o la difusión o acceso no autorizados sin autorización.

(6) El proceso de acreditación debería facilitarse mediante el uso por parte de los organizadores de los programas informáticos proporcionados por la Comisión de conformidad con el artículo 6, apartado 2, del Reglamento (UE) nº 211/2011.

(7) Cuando los organizadores de iniciativas ciudadanas recojan declaraciones de apoyo a través de páginas web deben, como responsables del tratamiento de datos, aplicar las especificaciones técnicas establecidas en el presente Reglamento con el fin de garantizar la protección de los datos personales procesados. Cuando el tratamiento sea efectuado por personal especializado, los organizadores deben velar por que actúe siguiendo únicamente las instrucciones de los organizadores y aplique las especificaciones técnicas establecidas en el presente Reglamento.

(8) El presente Reglamento respeta los derechos fundamentales y observa los principios consagrados en la Carta de los Derechos Fundamentales de la Unión Europea, en particular su artículo 8, que establece que toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan.

(9) Las medidas previstas en el presente Reglamento se ajustan al dictamen del Comité contemplado en el artículo 20 de Reglamento (UE) nº 211/2011.

[1] DO L 65 de 11.3.2011, p. 1.

[2] DO L 281 de 23.11.1995, p. 31.

HA ADOPTADO EL PRESENTE REGLAMENTO:

Artículo 1

Las especificaciones técnicas a que se refiere el artículo 6, apartado 5, del Reglamento (UE) nº 211/2011 se recogen en el anexo.

Artículo 2

El presente Reglamento entrará en vigor el vigésimo día siguiente al de su publicación en el *Diario Oficial de la Unión Europea*.

El presente Reglamento será obligatorio en todos sus elementos y directamente aplicable en todos los Estados miembros.

Hecho en Bruselas, el 17 de noviembre de 2011.

Por la Comisión
El Presidente
José Manuel BARROSO

ANEXO

1. ESPECIFICACIONES TÉCNICAS DE APLICACIÓN DEL ARTÍCULO 6, APARTADO 4, LETRA a), DEL REGLAMENTO (UE) Nº 211/2011

Con objeto de evitar la presentación automatizada de una declaración de apoyo utilizando el sistema, el firmante debe pasar por un proceso adecuado de verificación, en consonancia con la práctica actual previa a la presentación de una declaración de apoyo. Un posible proceso de verificación es el uso de un *captcha* seguro.

2. ESPECIFICACIONES TÉCNICAS DE APLICACIÓN DEL ARTÍCULO 6, APARTADO 4, LETRA b), DEL REGLAMENTO (UE) Nº 211/2011

Normas de aseguramiento de la información

2.1. Los organizadores deben facilitar documentación que indique que cumplen los requisitos de la norma ISO/IEC 27001, aunque no la hayan adoptado. A tal efecto, deben haber:

a) llevado a cabo una evaluación completa del riesgo que identifique el alcance del sistema, destaque el impacto operativo en caso de que se quebrante el aseguramiento de la información, enumere las amenazas y vulnerabilidades del sistema de información, presente un documento de análisis de riesgo que también indique las contramedidas para evitar estas amenazas y las soluciones que se tomarán si se produce una amenaza y, por último, contenga una lista de mejoras por orden de prioridad;

b) diseñado y aplicado medidas para el tratamiento de riesgos con respecto a la protección de los datos personales y a la protección de la vida privada y familiar y las medidas que se tomarán si se produce un riesgo;

c) identificado por escrito los riesgos residuales;

d) previsto los medios organizativos para mantenerse informados sobre las nuevas amenazas y las mejoras de seguridad.

2.2. Los organizadores deben elegir controles de seguridad basados en el análisis de riesgos mencionado en el punto 2.1, letra a), de entre las siguientes normas:

1) ISO/IEC 27002, o

2) las normas de buenas prácticas (SoGP) del Foro de Seguridad de la Información

para abordar los siguientes aspectos:

a) evaluaciones del riesgo (se recomienda la norma ISO/IEC 27005 u otra metodología apropiada y específica de evaluación del riesgo);

b) seguridad física y del entorno;

c) seguridad de los recursos humanos;

d) gestión de las comunicaciones y operaciones;

e) medidas estándar de control de acceso, además de las previstas en el presente Reglamento de Ejecución;

f) adquisición, desarrollo y mantenimiento de sistemas de información;

g) gestión de incidentes de la seguridad de la información;

h) medidas para remediar y mitigar los quebrantamientos de los sistemas de información que den lugar a la destrucción, accidental o ilícita, la pérdida accidental, la alteración o la difusión o acceso sin autorización de los datos personales procesados;

i) cumplimiento;

j) seguridad de la red informática (se recomiendan las normas ISO/IEC 27033 o SoGP).

La aplicación de estas normas puede limitarse a las partes de la organización que intervienen en el sistema de recogida a través de páginas web. Por ejemplo, la seguridad de los recursos humanos puede limitarse a las personas que tengan acceso físico o por conexión en red al sistema de recogida a través de páginas web, y la seguridad física y del entorno puede limitarse al edificio o edificios que alojen el sistema.

Requisitos funcionales

2.3. El sistema de recogida a través de páginas web debe consistir en una aplicación basada en la web y creada para recoger declaraciones de apoyo a una iniciativa ciudadana.

2.4. Si la administración del sistema exige diferentes funciones, los distintos niveles de control de acceso se deben establecer según el principio del privilegio mínimo.

2.5. Los elementos accesibles al público deben estar claramente separados de los destinados a efectos administrativos. Ningún control de acceso impedirá leer la información disponible en la zona pública del sistema, incluida la información sobre la iniciativa y el formulario electrónico de declaración de apoyo. Solo debe ser posible firmar en apoyo de una iniciativa a través de esta zona pública.

2.6. El sistema debe detectar e impedir la presentación de declaraciones de apoyo por duplicado.

Seguridad al nivel de la aplicación

2.7. El sistema debe estar protegido de forma adecuada contra las vulnerabilidades y programas maliciosos conocidos. A tal fin debe cumplir, entre otros, los siguientes requisitos:

2.7.1. El sistema debe proteger contra fallos de inyección como las consultas SQL (Lenguaje de Consulta Estructurado), LDAP (Protocolo Ligero de Acceso a Directorios), XML Path Language (Xpath), y comandos del sistema operativo (SO) o argumentos de programa. Para ello, se requiere, como mínimo, que:

a) se validen todas las entradas de los usuarios;

b) la validación se realice al menos por la lógica del lado del servidor;

c) todo uso de intérpretes distinga claramente entre los datos no confiables y el comando o consulta. Para las llamadas SQL esto significa utilizar variables ligadas en todas las sentencias preparadas y procesos almacenados, evitando las consultas dinámicas.

2.7.2. El sistema debe proteger contra los ataques XSS (*Cross-Site Scripting*). Para ello, es necesario, como mínimo, que:

a) se compruebe la seguridad de todas las entradas de los usuarios reenviadas al navegador (mediante validación de las entradas);

b) se utilice una secuencia de escape adecuada para todas las entradas de los usuarios antes de incluirlas en la página de resultados;

c) la correcta codificación de las entradas garantice que estas se procesan siempre como texto en el navegador. No se utilizará ningún contenido activo.

2.7.3. El sistema debe tener una sólida gestión de autenticación y de sesión, lo cual exige al menos que:

a) las credenciales siempre se protejan mediante *hashing* o encriptado al almacenarse. El riesgo de que alguien se autentique utilizando técnicas de *pass-the-hash* estará atenuado;

b) las credenciales no se puedan adivinar o sobreescribir debido a la fragilidad de las funciones de gestión de cuentas [por ejemplo, creación de cuentas, cambio de contraseñas, recuperación de contraseñas, identificadores de sesión (ID) débiles];

c) los ID y los datos de sesión no aparezcan en el localizador uniforme de recursos (URL);

d) los ID de sesión no sean vulnerables a ataques de fijación de sesiones;

e) los ID de sesión expiren, lo que garantiza la desconexión de los usuarios;

f) una vez iniciada la sesión, los ID de sesión no se roten;

g) las contraseñas, los ID de sesión y otras credenciales solo se envíen mediante *Transport Layer Security* (TLS);

h) la vertiente administrativa del sistema esté protegida. Si está protegida mediante autenticación basada en un factor único, la contraseña se compondrá de un mínimo de 10 caracteres que incluirán al menos una letra, una cifra y un carácter especial. Alternativamente se puede utilizar una autenticación basada en dos factores. Cuando solo se utilice una autenticación basada en un factor único, debe incluir un mecanismo de verificación en dos fases para acceder a la vertiente administrativa del sistema a través de Internet, mediante el cual al factor único se añadirá otro medio de autenticación, como una frase de contraseña o un código de un solo uso enviados por SMS o una secuencia de respuesta aleatoria encriptada asimétricamente que se deba desencriptar utilizando la clave privada de los organizadores o administradores, desconocida por el sistema.

2.7.4. El sistema no debe tener referencias directas inseguras a objetos. Para ello, es necesario, como mínimo, que:

a) para las referencias directas a recursos restringidos, la aplicación verifique que el usuario está autorizado a acceder al recurso exacto solicitado;

b) si la referencia es indirecta, el enlace a la referencia directa se limite a los valores autorizados para el usuario actual.

2.7.5. El sistema debe proteger contra falsificaciones de petición en sitios cruzados (CSFR).

2.7.6. Debe existir una configuración de seguridad adecuada, lo que exige, como mínimo, que:

a) todos los componentes de los programas informáticos estén actualizados, incluidos el SO, el servidor de la web/aplicación, el sistema de gestión de bases de datos (DBMS), las aplicaciones y todas las bibliotecas de códigos;

b) los servicios innecesarios del SO y del servidor de la web/aplicación estén desactivados o se hayan suprimido o desinstalado;

c) las contraseñas por defecto de las cuentas se hayan cambiado o estén desactivadas;

d) la gestión de errores esté configurada para impedir la filtración de trazas de la pila y otros mensajes de error que faciliten demasiada información;

e) los parámetros de seguridad de los marcos de desarrollo y de las bibliotecas estén configurados conforme a las mejores prácticas, tales como las directrices OWASP.

2.7.7. El sistema debe prever el encriptado de datos de la siguiente manera:

a) los datos personales en formato electrónico están codificados cuando se almacenan o presentan a las autoridades competentes de los Estados miembros de conformidad con el artículo 8, apartado 1, del Reglamento (UE) nº 211/2011, y se gestionan las claves y se hace una copia de seguridad por separado;

b) se usan algoritmos estándar sólidos y claves sólidas en línea de conformidad con las normas internacionales. Existe una gestión de claves;

c) las contraseñas se almacenan en forma de *hash* con un algoritmo estándar robusto y con una «sal» adecuada

d) todas las claves y las contraseñas están protegidas contra los accesos no autorizados.

2.7.8. El sistema debe restringir el acceso a URL basándose en los niveles de acceso y permisos de los usuarios. Para ello, se requiere, como mínimo, que:

a) si se utilizan mecanismos externos de seguridad para establecer controles de autenticación y autorización de acceso a las páginas, deben estar correctamente configurados para cada página;

b) si se utiliza una protección a nivel del código, esta debe existir para cada página solicitada.

2.7.9. El sistema debe utilizar una protección suficiente de la capa de transporte (TLS). Con este fin, deben existir todas las medidas siguientes o al menos unas medidas de seguridad equivalente:

a) el sistema exige la versión más reciente del Protocolo Seguro de Transferencia de Hipertexto (HTTPS) para acceder a cualquier recurso sensible utilizando certificados válidos, no expirados, no revocados y que correspondan a todos los dominios utilizados por el sitio;

b) el sistema atribuye el marcador «seguro» a todas las *cookies* sensibles;

c) el servidor configura el proveedor de TLS para que acepte únicamente algoritmos de encriptado en consonancia con las mejores prácticas. Se informa a los usuarios de que deben activar en su navegador la opción de aceptar TLS.

2.7.10. El sistema protege contra las redirecciones y los reenvíos no validados.

Seguridad de la base de datos e integridad de los datos

2.8. Cuando los sistemas de recogida a través de páginas web utilizados para diferentes iniciativas ciudadanas compartan recursos del equipo informático y del sistema operativo, no deben compartir ningún dato, incluidas las credenciales de acceso/encriptado. Además, esto se debe reflejar en la evaluación de riesgos y en las contramedidas aplicadas.

2.9. El riesgo de que alguien se autentique en la base de datos utilizando técnicas de *pass-the-hash* debe estar atenuado.

2.10. Solo el administrador/organizador de la base de datos debe poder acceder a los datos facilitados por los firmantes.

2.11. Las credenciales administrativas, los datos personales recogidos de los firmantes y sus copias de seguridad están protegidos mediante algoritmos de encriptado sólidos, en consonancia con el punto 2.7.7, letra b). No obstante, el Estado miembro en el que se vaya a contabilizar la declaración de apoyo, la fecha de presentación de la declaración de apoyo y la lengua en la que el firmante ha rellenado el formulario de declaración de apoyo podrán almacenarse en el sistema sin encriptar.

2.12. Los firmantes solo deben tener acceso a los datos presentados durante la sesión en que cumplimentan el formulario de declaración de apoyo. Una vez enviado el formulario de declaración de apoyo, dicha sesión se cierra y ya no se puede acceder a la información presentada.

2.13. Los datos personales de los firmantes, incluidas las copias de seguridad, solo deben estar disponibles en el sistema en formato encriptado. A efectos de la consulta de datos o de su certificación por las autoridades nacionales de acuerdo con el artículo 8 del Reglamento (CE) nº 211/2011, los organizadores podrán exportar los datos encriptados de conformidad con el punto 2.7.7, letra a).

2.14. La persistencia de los datos introducidos en el formulario de declaración de apoyo debe ser atómica. Es decir, una vez que el usuario ha introducido todos los detalles exigidos en el formulario de declaración de apoyo y validado su decisión de apoyar la iniciativa, el sistema o bien asignará con éxito todos los datos del formulario a la base de datos o bien, en caso de error, falla y no guarda ningún dato. El sistema debe informar al usuario del éxito o fallo de su solicitud.

2.15. El sistema de gestión de la base de datos (DBMS) utilizado se debe actualizar y parchear continuamente para proteger contra los programas maliciosos más recientes.

2.16. Todos los registros de actividad del sistema deben estar instalados. El sistema se debe asegurar de que los registros de auditoría que registran las excepciones y otros hechos pertinentes para la seguridad enumerados a continuación se puedan presentar y conservar hasta que los datos se destruyan de conformidad con el artículo 12, apartados 3 y 5, del Reglamento (UE) nº 211/2011. Los registros deben estar adecuadamente protegidos, por ejemplo, almacenándose en medios encriptados. Los organizadores/administradores deben comprobar periódicamente los registros para controlar las actividades sospechosas. Los registros deben contener al menos:

a) las fechas y horas de conexión y desconexión de los organizadores/administradores;

b) las copias de seguridad realizadas;

c) todas las modificaciones y actualizaciones de la base de datos por parte del administrador.

Seguridad de infraestructuras-localización física, infraestructura de red y entorno del servidor

2.17. *Seguridad física*

Cualquiera que sea el tipo de alojamiento utilizado, la máquina que aloje la aplicación debe estar adecuadamente protegida y ofrecer:

a) control de acceso a la zona de alojamiento y registro de auditoría;

b) protección física de las copias de seguridad de los datos frente a robos o pérdidas accidentales;

c) un armario de seguridad en el que está instalado el servidor que aloja la aplicación.

2.18. *Seguridad de la red*

2.18.1. El sistema debe estar alojado en un servidor conectado a Internet instalado en una zona desmilitarizada (ZDM) y protegido por un cortafuegos.

2.18.2. Cuando las actualizaciones y parches pertinentes del cortafuegos se hagan públicos, estas actualizaciones o parches se deben instalar de forma expeditiva.

2.18.3. Las normas de los cortafuegos deben inspeccionar todo el tráfico entrante y saliente al servidor (dirigido al sistema de recogida a través de una página web) y aquel debe quedar registrado. Las normas de los cortafuegos deben impedir todo el tráfico que no sea necesario para la utilización y administración seguras del sistema.

2.18.4. El sistema de recogida a través de páginas web debe estar alojado en un segmento de la red de producción adecuadamente protegido y que esté separado de los segmentos utilizados para alojar sistemas que no son de producción, tales como entornos de desarrollo o de prueba.

2.18.5. Deben existir medidas de seguridad de la red de área local (LAN) tales como:

a) lista de acceso a la capa 2 (L2)/seguridad de los conmutadores de puertos;

b) los puertos de conmutación no utilizados están desactivados;

c) la ZDM está en una red virtual de área local/LAN (VLAN) específica;

d) en puertos innecesarios no está activado el *trunking* (enlace troncal) de la L2.

2.19. *Seguridad del SO y del servidor web y de aplicaciones*

2.19.1. Debe existir una configuración de seguridad adecuada que incluya los elementos que figuran en el punto 2.7.6.

2.19.2. Las aplicaciones deben funcionar con el menor conjunto de privilegios necesario.

2.19.3. El acceso del administrador a la interfaz de gestión del sistema de recogida a través de páginas web debe tener un tiempo breve de desconexión de sesión (máximo de 15 minutos).

2.19.4. Cuando se hagan públicos las actualizaciones y parches pertinentes del SO, del sistema en tiempo de ejecución de la aplicación, de las aplicaciones ejecutadas en los servidores o de los programas contra códigos maliciosos, estas actualizaciones o parches se deben instalar de forma expeditiva.

2.19.5. Se debe atenuar el riesgo de que alguien se autentique en el sistema utilizando técnicas de *pass-the-hash*.

2.20. *Seguridad de los clientes del organizador*

En aras de la seguridad de extremo a extremo, los organizadores deben tomar las medidas necesarias para garantizar la seguridad del dispositivo o aplicación cliente que utilicen para gestionar y acceder al sistema de recogida a través de páginas web, tales como:

2.20.1. Los usuarios deben realizar las tareas que no sean de mantenimiento (tales como ofimática) con el menor conjunto de privilegios necesarios para funcionar.

2.20.2. Cuando se hagan públicos las actualizaciones y parches pertinentes del SO, de cualquiera de las aplicaciones instaladas o de los programas contra códigos maliciosos, estas actualizaciones o parches se deben instalar de forma expeditiva.

3. ESPECIFICACIONES TÉCNICAS DE APLICACIÓN DEL ARTÍCULO 6, APARTADO 4, LETRA c), DEL REGLAMENTO (UE) Nº 211/2011

3.1. El sistema debe prever la posibilidad de generar para cada Estado miembro un informe con una relación de que enumere la iniciativa y los datos personales de los firmantes sujetos a verificación por la autoridad competente de dicho Estado miembro.

3.2. Debe ser posible exportar declaraciones de apoyo de firmantes en el formato del anexo III del Reglamento nº 211/2011. El sistema podrá además prever la posibilidad de exportar las declaraciones de apoyo en un formato interoperable tal como el lenguaje extensible de marcado (XML).

3.3. Las declaraciones de apoyo exportadas se deben marcar con la etiqueta de *distribución limitada* al Estado miembro de que se trate y se deben etiquetar como *datos personales*.

3.4. La transmisión electrónica de datos exportados a los Estados miembros debe estar protegida contra las intrusiones mediante encriptado de extremo a extremo.

REGLAMENTO DE EJECUCIÓN (UE) Nº 1180/2011 DE LA COMISIÓN

de 17 de noviembre de 2011

por el que se establecen valores de importación a tanto alzado para la determinación del precio de entrada de determinadas frutas y hortalizas

LA COMISIÓN EUROPEA,

Visto el Tratado de Funcionamiento de la Unión Europea,

Visto el Reglamento (CE) nº 1234/2007 del Consejo, de 22 de octubre de 2007, por el que se crea una organización común de mercados agrícolas y se establecen disposiciones específicas para determinados productos agrícolas (Reglamento único para las OCM) ([1]),

Visto el Reglamento de Ejecución (UE) nº 543/2011 de la Comisión, de 7 de junio de 2011, por el que se establecen disposiciones de aplicación del Reglamento (CE) nº 1234/2007 del Consejo en los sectores de las frutas y hortalizas y de las frutas y hortalizas transformadas ([2]), y, en particular, su artículo 136, apartado 1,

Considerando lo siguiente:

El Reglamento de Ejecución (UE) nº 543/2011 establece, en aplicación de los resultados de las negociaciones comerciales multilaterales de la Ronda Uruguay, los criterios para que la Comisión fije los valores de importación a tanto alzado de terceros países correspondientes a los productos y períodos que figuran en el anexo XVI, parte A, de dicho Reglamento.

HA ADOPTADO EL PRESENTE REGLAMENTO:

Artículo 1

En el anexo del presente Reglamento quedan fijados los valores de importación a tanto alzado a que se refiere el artículo 136 del Reglamento de Ejecución (UE) nº 543/2011.

Artículo 2

El presente Reglamento entrará en vigor el 18 de noviembre de 2011.

El presente Reglamento será obligatorio en todos sus elementos y directamente aplicable en cada Estado miembro.

Hecho en Bruselas, el 17 de noviembre de 2011.

Por la Comisión,
en nombre del Presidente
José Manuel SILVA RODRÍGUEZ
Director General de Agricultura y Desarrollo Rural

([1]) DO L 299 de 16.11.2007, p. 1.
([2]) DO L 157 de 15.6.2011, p. 1.

ANEXO

Valores de importación a tanto alzado para la determinación del precio de entrada de determinadas frutas y hortalizas

(EUR/100 kg)

Código NC	Código país tercero [1]	Valor global de importación
0702 00 00	AL	62,0
	AR	40,4
	MA	48,6
	MK	64,0
	TR	89,6
	ZZ	60,9
0707 00 05	AL	73,2
	EG	161,4
	TR	110,1
	ZZ	114,9
0709 90 70	MA	61,4
	TR	131,5
	ZZ	96,5
0805 20 10	MA	94,7
	ZA	65,5
	ZZ	80,1
0805 20 30, 0805 20 50, 0805 20 70, 0805 20 90	HR	82,7
	IL	73,3
	MA	79,7
	TR	81,7
	UY	42,7
	ZA	62,9
	ZZ	70,5
0805 50 10	TR	58,5
	ZA	43,5
	ZZ	51,0
0806 10 10	BR	226,9
	CL	70,8
	LB	291,7
	PE	200,1
	TR	144,9
	US	300,4
	ZA	82,6
	ZZ	188,2
0808 10 80	CA	86,1
	CL	90,0
	NZ	120,0
	TR	95,1
	US	124,3
	ZA	108,8
	ZZ	104,1
0808 20 50	CL	73,3
	CN	77,1
	TR	85,0
	ZA	73,2
	ZZ	77,2

[1] Nomenclatura de países fijada por el Reglamento (CE) nº 1833/2006 de la Comisión (DO L 354 de 14.12.2006, p. 19). El código «ZZ» significa «otros orígenes».

REGLAMENTO DE EJECUCIÓN (UE) Nº 1181/2011 DE LA COMISIÓN

de 17 de noviembre de 2011

sobre la expedición de certificados de importación para las solicitudes presentadas durante los primeros 7 días de noviembre de 2011 en virtud del contingente arancelario de carne de vacuno de calidad superior gestionado por el Reglamento (CE) nº 620/2009

LA COMISIÓN EUROPEA,

Visto el Tratado de Funcionamiento de la Unión Europea,

Visto el Reglamento (CE) nº 1234/2007 del Consejo, de 22 de octubre de 2007, por el que se crea una organización común de mercados agrícolas y se establecen disposiciones específicas para determinados productos agrícolas (Reglamento único para las OCM) ([1]),

Visto el Reglamento (CE) nº 1301/2006 de la Comisión, de 31 de agosto de 2006, por el que se establecen normas comunes de gestión de los contingentes arancelarios de importación de productos agrícolas sujetos a un sistema de certificados de importación ([2]), y, en particular, su artículo 7, apartado 2,

Considerando lo siguiente:

(1) El Reglamento (CE) nº 620/2009 de la Comisión, de 13 de julio de 2009, sobre la gestión de un contingente arancelario de importación de carne de vacuno de calidad superior ([3]) establece normas detalladas para la presentación y expedición de certificados de importación.

(2) El artículo 7, apartado 2, del Reglamento (CE) nº 1301/2006 dispone que cuando las cantidades a que se refieran las solicitudes de certificado excedan de las cantidades disponibles para el período del contingente arancelario en cuestión, deben fijarse coeficientes de asignación para las cantidades a que se refiera cada solicitud. Las solicitudes de certificados de importación presentadas en virtud del artículo 3 del Reglamento (CE) nº 620/2009 entre el 1 y el 7 de noviembre de 2011 exceden de las cantidades disponibles. Por lo tanto, deben determinarse la cantidad de licencias que puede expedirse y el coeficiente de asignación.

HA ADOPTADO EL PRESENTE REGLAMENTO:

Artículo 1

Se aplicará un coeficiente de asignación del 0,414127 % a las solicitudes de certificados de importación del contingente con el número de orden 09.4449 presentadas entre el 1 y el 7 de noviembre de 2011 de conformidad con el artículo 3 del Reglamento (CE) nº 620/2009.

Artículo 2

El presente Reglamento entrará en vigor el día siguiente al de su publicación en el *Diario Oficial de la Unión Europea*.

El presente Reglamento será obligatorio en todos sus elementos y directamente aplicable en cada Estado miembro.

Hecho en Bruselas, el 17 de noviembre de 2011.

Por la Comisión,
en nombre del Presidente
José Manuel SILVA RODRÍGUEZ
Director General de Agricultura y Desarrollo Rural

([1]) DO L 299 de 16.11.2007, p. 1.
([2]) DO L 238 de 1.9.2006, p. 13.
([3]) DO L 182 de 15.7.2009, p. 25.

REGLAMENTO DE EJECUCIÓN (UE) Nº 1182/2011 DE LA COMISIÓN

de 17 de noviembre de 2011

por el que se fijan los precios representativos en los sectores de la carne de aves de corral, los huevos y la ovoalbúmina, y por el que se modifica el Reglamento (CE) nº 1484/95

LA COMISIÓN EUROPEA,

Visto el Tratado de Funcionamiento de la Unión Europea,

Visto el Reglamento (CE) nº 1234/2007 del Consejo, de 22 de octubre de 2007, por el que se crea una organización común de mercados agrícolas y se establecen disposiciones específicas para determinados productos agrícolas (Reglamento único para las OCM) [1], y, en particular, su artículo 143,

Visto el Reglamento (CE) nº 614/2009 del Consejo, de 7 de julio de 2009, relativo al régimen de intercambios para la ovoalbúmina y la lactoalbúmina [2], y, en particular, su artículo 3, apartado 4,

Considerando lo siguiente:

(1) El Reglamento (CE) nº 1484/95 de la Comisión [3] estableció las disposiciones de aplicación del régimen de aplicación de derechos adicionales de importación y fijó los precios representativos en los sectores de la carne de aves de corral, los huevos y la ovoalbúmina.

(2) Según se desprende del control periódico de los datos en que se basa el establecimiento de los precios representativos de los productos de los sectores de la carne de aves de corral, los huevos y la ovoalbúmina, es preciso modificar los precios representativos de importación de determinados productos, teniendo en cuenta las variaciones de precios según su origen. Es necesario, por consiguiente, publicar los precios representativos.

(3) Teniendo en cuenta la situación del mercado, es preciso aplicar esta modificación a la mayor brevedad posible.

(4) Las medidas previstas en el presente Reglamento se ajustan al dictamen del Comité de gestión de la organización común de mercados agrícolas.

HA ADOPTADO EL PRESENTE REGLAMENTO:

Artículo 1

El anexo I del Reglamento (CE) nº 1484/95 se sustituye por el anexo del presente Reglamento.

Artículo 2

El presente Reglamento entrará en vigor el día de su publicación en el *Diario Oficial de la Unión Europea*.

El presente Reglamento será obligatorio en todos sus elementos y directamente aplicable en cada Estado miembro.

Hecho en Bruselas, el 17 de noviembre de 2011.

Por la Comisión,
en nombre del Presidente
José Manuel SILVA RODRÍGUEZ
Director General de Agricultura y Desarrollo Rural

---

[1] DO L 299 de 16.11.2007, p. 1.
[2] DO L 181 de 14.7.2009, p. 8.
[3] DO L 145 de 29.6.1995, p. 47.

ANEXO

del Reglamento de la Comisión, de 17 de noviembre de 2011, por el que se fijan los precios representativos en los sectores de la carne de aves de corral, los huevos y la ovoalbúmina, y por el que se modifica el Reglamento (CE) nº 1484/95

«*ANEXO I*

Código NC	Designación de la mercancía	Precio representativo (EUR/100 kg)	Garantía contemplada en el artículo 3, apartado 3 (EUR/100 kg)	Origen [1]
0207 12 10	Gallos o gallinas desplumados, eviscerados, sin la cabeza ni las patas y sin el cuello, el corazón, el hígado ni la molleja, llamados "pollos 70 %"	128,7	0	BR
		128,8	0	AR
0207 12 90	Gallos o gallinas desplumados, eviscerados, sin la cabeza ni las patas y sin el cuello, el corazón, el hígado ni la molleja, llamados "pollos 65 %"	138,3	0	BR
		141,1	0	AR
0207 14 10	Trozos deshuesados de gallo o gallina, congelados	224,7	23	BR
		266,1	10	AR
		341,6	0	CL
0207 14 60	Muslos y contramuslos de gallo o de gallina, y sus trozos, congelados	249,8	0	BR
0207 27 10	Trozos deshuesados de pavo, congelados	372,8	0	BR
		413,1	0	CL
0408 11 80	Yemas de huevo	303,9	2	AR
0408 91 80	Huevos sin cáscara secos	314,9	0	AR
1602 32 11	Preparaciones de gallo o gallina, sin cocer	283,4	1	BR
		356,5	0	CL
3502 11 90	Ovoalbúmina seca	483,9	0	AR

[1] Nomenclatura de países establecida por el Reglamento (CE) nº 1833/2006 de la Comisión (DO L 354 de 14.12.2006, p. 19). El código "ZZ" representa "otros orígenes".»

Precio de suscripción 2011 (sin IVA, gastos de envío ordinario incluidos)

Diario Oficial de la UE, series L + C, solo edición impresa	22 lenguas oficiales de la UE	1 100 EUR al año
Diario Oficial de la UE, series L + C, edición impresa + DVD anual	22 lenguas oficiales de la UE	1 200 EUR al año
Diario Oficial de la UE, serie L, solo edición impresa	22 lenguas oficiales de la UE	770 EUR al año
Diario Oficial de la UE, series L + C, DVD mensual (acumulativo)	22 lenguas oficiales de la UE	400 EUR al año
Suplemento del Diario Oficial (serie S: Anuncios de contratos públicos), DVD semanal	Plurilingüe: 23 lenguas oficiales de la UE	300 EUR al año
Diario Oficial de la UE, serie C: Oposiciones	Lengua(s) en función de la oposición	50 EUR al año

La suscripción al *Diario Oficial de la Unión Europea*, que se publica en las lenguas oficiales de la Unión Europea, está disponible en 22 versiones lingüísticas. Incluye las series L (Legislación) y C (Comunicaciones e informaciones).

Cada versión lingüística es objeto de una suscripción aparte.

Con arreglo al Reglamento (CE) nº 920/2005 del Consejo, publicado en el Diario Oficial L 156 de 18 de junio de 2005, que establece que las instituciones de la Unión Europea no estarán temporalmente vinculadas por la obligación de redactar todos los actos en irlandés y de publicarlos en esta lengua, los Diarios Oficiales publicados en lengua irlandesa se comercializan aparte.

La suscripción al Suplemento del Diario Oficial (serie S: Anuncios de contratos públicos) reagrupa las 23 versiones lingüísticas oficiales en un solo DVD plurilingüe.

Previa petición, las personas suscritas al *Diario Oficial de la Unión Europea* podrán recibir los anexos del Diario Oficial. La publicación de estos anexos se comunica mediante una «Nota al lector» insertada en el *Diario Oficial de la Unión Europea*.

Venta y suscripciones

Las suscripciones a diversas publicaciones periódicas de pago, como la suscripción al *Diario Oficial de la Unión Europea*, están disponibles en nuestra red de distribuidores comerciales, cuya relación figura en la dirección siguiente de Internet:

http://publications.europa.eu/others/agents/index_es.htm

EUR-Lex (http://eur-lex.europa.eu) ofrece acceso directo y gratuito a la legislación de la Unión Europea. Desde este sitio puede consultarse el *Diario Oficial de la Unión Europea,* así como los Tratados, la legislación, la jurisprudencia y la legislación en preparación.

Para más información acerca de la Unión Europea, consulte: http://europa.eu

Oficina de Publicaciones de la Unión Europea
2985 Luxemburgo
LUXEMBURGO

ES