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.