

				Introduzca aquí la denominación de la entidad jurídica registrada							
Número de documento: PII06				Título del documento: <b>Política de gestión de derechos del interesado</b>							
Versión: 1.0		Fecha de entrada en vigor: 01.01.2025		Propietario del documento:							
X	Política		Norma		Procedimiento		Formulario		Registro		Otro

Historial de revisiones				
Número de revisión	Fecha de revisión	Cambios	Revisado por	Propietario del proceso

Aprobaciones			
Nombre	Cargo	Fecha	Firma

**Aviso legal (derechos de autor y restricciones de uso)**  
(C) 2025 Clarysec LLC. All rights reserved.

Este documento es propiedad intelectual de Clarysec LLC. Ninguna parte de este documento podrá copiarse, reutilizarse, distribuirse ni modificarse con fines comerciales o de implantación sin autorización previa y expresa por escrito.

El uso no autorizado está estrictamente prohibido y puede dar lugar a acciones legales.

Para cuestiones de licenciamiento, contacte con: [info@clarysec.com](mailto:info@clarysec.com)

## Alineación con normas y regulaciones

Standard / Regulation	Clause / Control / Article	Applicability	Coverage Type	Comment
ISO/IEC 27701:2025	Clause 7.5; Clause 8.1	Both	Primary	Evidencias de solicitudes de derechos y control operacional
ISO/IEC 27701:2025	Clause 9.1; Clause 10.2	Both	Supporting	Seguimiento, no conformidad y acción correctiva
ISO/IEC 27701:2025	Annex A.1.3.2	Controller	Primary	Obligaciones frente a los interesados
ISO/IEC 27701:2025	Annex A.1.3.6; Annex A.1.3.7	Controller	Primary	Oposición, acceso, rectificación y supresión
ISO/IEC 27701:2025	Annex A.1.3.8; Annex A.1.3.9	Controller	Primary	Notificación a terceros y copia de la PII tratada
ISO/IEC 27701:2025	Annex A.1.3.10; Annex A.1.3.11	Controller	Primary	Gestión de solicitudes y obligaciones sobre decisiones automatizadas
ISO/IEC 27701:2025	Annex A.1.2.9	Controller	Supporting	Registros de tratamiento del responsable del tratamiento
ISO/IEC 27701:2025	Annex A.2.2.2; Annex A.2.2.6; Annex A.2.2.7	Processor	Supporting	Acuerdo con el cliente, apoyo a obligaciones y registros del encargado del tratamiento
ISO/IEC 27701:2025	Annex A.2.3.2	Processor	Primary	Apoyo del encargado del tratamiento a las obligaciones frente al interesado
ISO/IEC 27701:2025	Annex A.3.14	Both	Supporting	Protección de registros de solicitudes de derechos
GDPR	Article 5(1)(a); Article 5(2)	Controller	Supporting	Transparencia y responsabilidad proactiva

GDPR	Article 11; Article 12	Controller	Primary	Identificación, modalidades de solicitud, plazos y gobierno de la respuesta
GDPR	Article 15; Article 16; Article 17	Controller	Primary	Acceso, rectificación y supresión
GDPR	Article 18; Article 19; Article 20	Controller	Primary	Limitación, notificación y portabilidad
GDPR	Article 21; Article 22	Controller	Primary	Oposición y decisiones automatizadas
GDPR	Article 24	Controller	Supporting	Responsabilidad y medidas del responsable del tratamiento
GDPR	Article 26	Joint Controller	Supporting	Asignación de derechos entre corresponsables del tratamiento
GDPR	Article 28	Both	Primary	Asistencia del encargado del tratamiento para solicitudes de derechos
GDPR	Article 30	Both	Supporting	Vinculación con registros de tratamiento
GDPR	Article 32	Both	Supporting	Gestión segura de evidencias de derechos y comunicaciones de PII
GDPR	Article 39	Conditional	Supporting	Asesoramiento y seguimiento del DPO cuando sea aplicable
ISO/IEC 29100:2020	Clause 5.8; Clause 5.9; Clause 5.10; Clause 5.12	Both	Supporting	Transparencia, participación individual, responsabilidad proactiva y cumplimiento

ISO/IEC 29151:2022	Annex A.10	Controller	Supporting	Participación y acceso del interesado
-----------------------	------------	------------	------------	---

## **1. Alcance**

- 1.1 Esta política define los requisitos obligatorios para recibir, validar, evaluar, atender, denegar, prorrogar, cerrar, hacer seguimiento y evidenciar las solicitudes de derechos de los interesados.
- 1.2 Esta política se aplica a las solicitudes presentadas por interesados o representantes autorizados relativas al acceso, rectificación, supresión, limitación, portabilidad, oposición, decisiones automatizadas, enrutamiento de la retirada del consentimiento, reclamaciones y consultas relacionadas.
- 1.3 Esta política se aplica a contextos de responsable del tratamiento, corresponsable del tratamiento, encargado del tratamiento y subencargado. Las obligaciones del encargado del tratamiento y del subencargado solo se aplican cuando la organización presta apoyo a un responsable del tratamiento, cliente o encargado del tratamiento anterior conforme a instrucciones documentadas.

### **1.4 Esta política no sustituye a:**

- 1.4.1 PII03 para el inventario de tratamientos y los registros de base jurídica;
- 1.4.2 PII04 para el contenido y la publicación del aviso de privacidad;
- 1.4.3 PII05 para la ejecución del consentimiento y las preferencias;
- 1.4.4 PII10 para la ejecución de la conservación, la eliminación y la disposición;
- 1.4.5 PII11 para el gobierno de la exactitud y la calidad;
- 1.4.6 PII12 para el gobierno del ciclo de vida de encargados del tratamiento y subencargados;
- 1.4.7 PII15 para la gestión de incidentes y brechas de seguridad.

## **2. Finalidad**

- 2.1 La finalidad de esta política es asegurar que las solicitudes de derechos de los interesados se gestionen de forma coherente, lícita y segura, dentro de plazos definidos y con evidencias preparadas para auditoría.
- 2.2 Esta política asegura que la organización pueda demostrar responsabilidad proactiva respecto de la recepción de solicitudes, verificación de identidad, evaluación, atención, denegación, prórroga, cooperación del encargado del tratamiento, cierre y mejora continua.

## **3. Objetivos**

### **3.1 Los objetivos de esta política son:**

- 3.1.1 Proporcionar una recepción y un seguimiento coherentes para todas las solicitudes de derechos de los interesados.
- 3.1.2 Verificar la identidad o la autoridad del solicitante antes de la divulgación, rectificación, supresión, limitación o portabilidad.
- 3.1.3 Evaluar las solicitudes frente a los registros de tratamiento, la clasificación del rol, las obligaciones legales, las obligaciones contractuales y la viabilidad técnica.
- 3.1.4 Atender las solicitudes válidas dentro de los plazos documentados.
- 3.1.5 Registrar evidencias de denegación, atención parcial, prórroga y cierre.
- 3.1.6 Apoyar las obligaciones del responsable del tratamiento cuando la organización actúe como encargado del tratamiento o subencargado.
- 3.1.7 Proteger los registros de solicitudes de derechos y los paquetes de respuesta frente a la divulgación o alteración no autorizadas.
- 3.1.8 Hacer seguimiento del desempeño de las solicitudes de derechos e impulsar acciones correctivas cuando sea necesario.

## **4. Declaraciones de la política**

### **4.1 Recepción, registro y clasificación**

- 4.1.1 [All] Privacy Lead / PIMS Manager DEBE registrar cada solicitud de derechos del interesado en REG06 dentro de los dos días hábiles siguientes a su recepción.
- 4.1.2 [All] Privacy Lead / PIMS Manager DEBE clasificar cada tipo de solicitud, canal de solicitud, fecha de solicitud, referencia de identidad del solicitante, propietario asignado, fecha límite interna, fecha límite legal o contractual y estado actual en REG06 antes de que comience la evaluación.
- 4.1.3 [Controller] Privacy Lead / PIMS Manager DEBE acusar recibo o proporcionar la siguiente comunicación requerida al solicitante dentro de los cinco días hábiles siguientes a la recepción y registrar la comunicación en REG06.
- 4.1.4 [Controller] Process Owner / Business Owner DEBE vincular cada solicitud con la actividad de tratamiento pertinente de REG02 antes de asignar acciones de atención.
- 4.1.5 [Joint Controller] Privacy Lead / PIMS Manager DEBE identificar a la parte corresponsable del tratamiento responsable de gestionar la solicitud en REG02, REG06 o REG08 antes de que comience la evaluación sustantiva.
- 4.1.6 [Processor] Privacy Lead / PIMS Manager DEBE registrar cada instrucción del cliente relativa a una solicitud de derechos del interesado en REG06 y REG08 antes de que comience la actividad de apoyo.
- 4.1.7 [Subprocessor] Vendor / Procurement Owner DEBE registrar cada instrucción del eslabón anterior relativa a una solicitud de derechos del interesado en REG06 o REG08 antes de que comience la actividad de apoyo del subencargado.
- 4.1.8 [All] Incident Response Coordinator DEBE registrar un escalado en REG10 dentro de un día hábil cuando una solicitud de derechos indique un posible incidente de PII o brecha de seguridad de PII.

#### **4.2 Verificación de identidad, alcance y evaluación**

- 4.2.1 [Controller] Privacy Lead / PIMS Manager DEBE verificar la identidad del solicitante o la autoridad del representante en REG06 antes de divulgar PII o efectuar un cambio solicitado.
- 4.2.2 [Controller] Privacy Lead / PIMS Manager DEBE solicitar únicamente la información adicional mínima necesaria para la verificación y registrar la solicitud en REG06 cuando la identidad o la autoridad sea insuficiente.
- 4.2.3 [Controller] Process Owner / Business Owner DEBE identificar los sistemas, registros, finalidades, categorías de PII, destinatarios y restricciones de conservación pertinentes a partir de REG02 antes de evaluar la atención.
- 4.2.4 [Controller] Data Protection Officer / Privacy Advisor DEBE revisar las solicitudes de alto riesgo, disputadas, poco claras, excesivas, repetidas, denegadas o atendidas parcialmente en REG06 antes de comunicar la decisión.
- 4.2.5 [Controller] System Owner / Application Owner DEBE verificar que los extractos de respuesta propuestos excluyan PII no relacionada y datos de terceros no autorizados antes de liberar el paquete de respuesta.
- 4.2.6 [Controller] Information Security Lead DEBE revisar el método de entrega de la respuesta en REG06 o REG12 antes de divulgar PII de gran volumen, sensible, de categorías especiales o de alto riesgo.
- 4.2.7 [Controller] Data Protection Officer / Privacy Advisor DEBE revisar las solicitudes relacionadas con decisiones automatizadas o elaboración de perfiles en REG06 y REG04 antes de la atención, denegación o escalado.

- 4.2.8 [Both] Privacy Lead / PIMS Manager DEBE registrar el resultado de la evaluación, el tipo de solicitud aplicable, la decisión, la justificación y la siguiente acción en REG06 antes de la atención o denegación.

[ ... Las secciones 4.3–8 no están incluidas en esta vista previa. Adquiera el documento completo para acceder al contenido íntegro. ... ]

## 9. Excepciones

- 9.1.1 [All] Process Owner / Business Owner DEBE solicitar una excepción en REG12 antes de desviarse de los requisitos aprobados de recepción, verificación, atención, respuesta o cierre de derechos.
- 9.1.2 [All] Privacy Lead / PIMS Manager DEBE aprobar o rechazar cada excepción de gestión de derechos en REG12 antes de su implementación.
- 9.1.3 [Controller] Data Protection Officer / Privacy Advisor DEBE revisar cualquier excepción que implique denegación, atención parcial, incertidumbre de identidad, PII sensible, decisiones automatizadas, solicitudes relacionadas con menores o tratamiento de alto riesgo antes de su aprobación.
- 9.1.4 [Both] System Owner / Application Owner DEBE bloquear la actividad de divulgación, rectificación, eliminación, limitación o exportación cuando una excepción requerida no haya sido aprobada en REG12 antes de la acción.
- 9.1.5 [All] Privacy Lead / PIMS Manager DEBE asignar una fecha de caducidad, propietario y control compensatorio para cada excepción aprobada de gestión de derechos en REG12 antes de que la excepción pase a estar activa.

## 10. Aplicación

- 10.1.1 [All] Privacy Lead / PIMS Manager DEBE registrar una no conformidad en REG12 dentro de los cinco días hábiles siguientes a la identificación de un registro de solicitud de derechos vencido, ausente, incompleto, no verificado o no respaldado.
- 10.1.2 [Controller] System Owner / Application Owner DEBE suspender la divulgación de la respuesta hasta que las comprobaciones de identidad, autoridad y paquete de respuesta estén registradas en REG06.
- 10.1.3 [Both] Vendor / Procurement Owner DEBE escalar la falta de cooperación de encargados del tratamiento, subencargados o terceros en REG08 y REG12 dentro de los cinco días hábiles siguientes a su identificación.
- 10.1.4 [All] Top Management DEBE asignar la propiedad de acciones correctivas en REG12 cuando los fallos de solicitudes de derechos sean sistémicos, repetidos o pertinentes para la certificación.
- 10.1.5 [All] Internal Audit / Compliance Reviewer DEBE verificar las evidencias de cierre de acciones correctivas relacionadas con derechos en REG12 antes de la fecha límite asignada.
- 10.1.6 [All] Incident Response Coordinator DEBE iniciar una revisión en REG10 dentro de un día hábil cuando una no conformidad de solicitud de derechos indique divulgación no autorizada, pérdida, alteración, indisponibilidad u otro incidente de PII sospechado.

## 11. Revisión y mantenimiento

- 11.1.1 [All] Privacy Lead / PIMS Manager DEBE revisar esta política anualmente y registrar el resultado de la revisión en REG12.
- 11.1.2 [All] Privacy Lead / PIMS Manager DEBE revisar esta política dentro de los 30 días siguientes a un cambio material en la normativa sobre solicitudes de derechos, el alcance de la actividad de tratamiento, las herramientas de derechos, el método de verificación de

identidad, el modelo de servicio de encargados del tratamiento o los requisitos de certificación PIMS.

11.1.3 [All] Data Protection Officer / Privacy Advisor DEBE revisar los cambios significativos para la privacidad de esta política en REG12 antes de su aprobación.

11.1.4 [All] Top Management DEBE aprobar los cambios materiales en esta política en REG12 antes de la publicación.

11.1.5 [All] Privacy Lead / PIMS Manager DEBE registrar la comunicación de los cambios aprobados de la política en REG11 dentro de los 30 días siguientes a la publicación.

## 12. Políticas relacionadas

- 12.1 Esta política está respaldada por las siguientes políticas relacionadas:
- 12.2 PII01 - Política del Sistema de Gestión de la Privacidad de la Información
- 12.3 PII02 - Política de roles, responsabilidades y responsabilidad proactiva de privacidad
- 12.4 PII03 - Política de inventario de tratamientos de PII y base jurídica
- 12.5 PII04 - Política de aviso de privacidad y transparencia
- 12.6 PII05 - Política de gestión del consentimiento y preferencias
- 12.7 PII07 - Política de evaluación de riesgos de privacidad y DPIA
- 12.8 PII08 - Política de privacidad desde el diseño y por defecto
- 12.9 PII09 - Política de recogida, uso, divulgación e intercambio de PII
- 12.10 PII10 - Política de conservación, eliminación y disposición de PII
- 12.11 PII11 - Política de exactitud y calidad de PII
- 12.12 PII12 - Política de gestión de privacidad de encargados del tratamiento, subencargados y terceros
- 12.13 PII13 - Política de transferencias internacionales de PII
- 12.14 PII14 - Política de seguridad de PII y control de acceso
- 12.15 PII15 - Política de gestión de incidentes y brechas de seguridad de PII
- 12.16 PII16 - Política de formación, concienciación y competencia en privacidad
- 12.17 PII17 - Política de información documentada y gestión de evidencias del PIMS
- 12.18 PII18 - Política de seguimiento, auditoría y mejora del PIMS

## 13. Normas y marcos de referencia

13.1 Esta política está mapeada con las siguientes normas y regulaciones. El mapeo explica cómo la política apoya los requisitos citados e identifica las cláusulas internas que los implementan o respaldan.

### 13.2 ISO/IEC 27701:2025

13.2.1 **Clause 7.5; Clause 8.1** - Mapeado con registros documentados de solicitudes de derechos, flujo de trabajo operativo de solicitudes, verificación de identidad, atención, respuesta, cierre y evidencias de apoyo del encargado del tratamiento. Addressed by clauses [4.1.1; 4.1.2; 4.1.4; 4.1.6; 4.2.1; 4.2.2; 4.2.3; 4.2.8; 4.3.10; 4.4.5; 7.1.1; 7.1.2; 7.1.3].

13.2.2 **Clause 9.1; Clause 10.2** - Mapeado con métricas de solicitudes de derechos, seguimiento de solicitudes vencidas, muestreo de auditoría, registro de no conformidades, acción correctiva y verificación de eficacia. Addressed by clauses [4.5.6; 8.1.1; 8.1.2; 8.1.3; 8.1.4; 8.1.5; 8.1.6; 10.1.1; 10.1.3; 10.1.4; 10.1.5].

13.2.3 **Annex A.1.3.2** - Mapeado con la determinación y atención de obligaciones frente a los interesados mediante categorías de derechos documentadas, canales de recepción, criterios

- de verificación, evaluación, respuesta y cierre. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.2.1; 4.2.8; 4.4.1; 4.4.4; 6.1.1; 7.1.1].
- 13.2.4 **Annex A.1.3.6; Annex A.1.3.7** - Mapeado con la gestión de oposición, acceso, rectificación, supresión y limitación, verificación, atención y gestión de disputas sobre exactitud. Addressed by clauses [4.2.1; 4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.3.6; 4.4.6].
- 13.2.5 **Annex A.1.3.8; Annex A.1.3.9** - Mapeado con la notificación a terceros tras resultados de derechos y la provisión de copias o paquetes de respuesta portables. Addressed by clauses [4.3.5; 4.3.8; 4.5.5].
- 13.2.6 **Annex A.1.3.10; Annex A.1.3.11** - Mapeado con la gestión documentada de solicitudes legítimas, plazos, prórrogas, denegación, cierre y revisión de solicitudes sobre decisiones automatizadas. Addressed by clauses [4.1.2; 4.2.4; 4.2.7; 4.4.1; 4.4.2; 4.4.3; 4.4.4; 4.4.5].
- 13.2.7 **Annex A.1.2.9** - Mapeado con la vinculación de solicitudes de derechos a registros de tratamiento, finalidades de tratamiento, sistemas, categorías, destinatarios y restricciones de conservación. Addressed by clauses [4.1.4; 4.2.3; 4.3.8; 7.1.3].
- 13.2.8 **Annex A.2.2.2; Annex A.2.2.6; Annex A.2.2.7** - Mapeado con instrucciones de acuerdos con clientes, apoyo del encargado del tratamiento a las obligaciones del cliente y registros del encargado del tratamiento para actividades de apoyo a derechos. Addressed by clauses [4.1.6; 4.1.7; 4.5.1; 4.5.2; 4.5.3; 4.5.4; 7.1.7].
- 13.2.9 **Annex A.2.3.2** - Mapeado con medios del encargado del tratamiento para apoyar las obligaciones del responsable del tratamiento frente a los interesados, incluido el apoyo a recuperación, rectificación, limitación, eliminación y exportación conforme a instrucciones documentadas. Addressed by clauses [4.5.1; 4.5.2; 4.5.3; 7.1.7].
- 13.2.10 **Annex A.3.14** - Mapeado con la protección de registros de solicitudes de derechos, la gestión segura de paquetes de respuesta, las comprobaciones de entrega de respuestas y la protección de evidencias de cierre. Addressed by clauses [4.2.5; 4.2.6; 4.4.5; 4.4.7; 7.1.4; 7.1.5; 10.1.2].

### 13.3 **GDPR**

- 13.3.1 **Article 5(1)(a); Article 5(2)** - Mapeado con la gestión transparente de derechos, evidencias de responsabilidad proactiva, registros de solicitudes, registros de respuesta, muestreo de auditoría y acción correctiva. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.4.4; 4.4.5; 8.1.5; 10.1.1].
- 13.3.2 **Article 11; Article 12** - Mapeado con identificación, información adicional cuando sea necesaria, plazos de respuesta, comunicaciones, prórroga, denegación y cierre de solicitudes. Addressed by clauses [4.2.1; 4.2.2; 4.4.1; 4.4.2; 4.4.3; 4.4.4; 4.4.5].
- 13.3.3 **Article 15; Article 16; Article 17** - Mapeado con resultados de búsqueda de acceso, rectificación, supresión, verificación, evidencias de atención y entrega del paquete de respuesta. Addressed by clauses [4.2.1; 4.3.1; 4.3.2; 4.3.3; 4.3.5; 4.3.10].
- 13.3.4 **Article 18; Article 19; Article 20** - Mapeado con limitación, notificación de resultados de derechos a las partes pertinentes y portabilidad o entrega de copias. Addressed by clauses [4.3.4; 4.3.5; 4.3.8; 4.5.5].
- 13.3.5 **Article 21; Article 22** - Mapeado con evaluación de oposición y revisión de solicitudes sobre decisiones automatizadas o elaboración de perfiles. Addressed by clauses [4.2.7; 4.3.6; 4.3.7].
- 13.3.6 **Article 24** - Mapeado con medidas de gobierno del responsable del tratamiento, roles, propiedad del flujo de trabajo, revisión, excepciones, acción correctiva y supervisión por la dirección para la gestión de derechos. Addressed by clauses [5.1.1; 5.1.2; 6.1.1; 6.1.3; 6.1.4; 9.1.1; 9.1.2; 10.1.4; 11.1.1].

13.3.7 **Article 26** - Mapeado con la identificación de la responsabilidad del corresponsable del tratamiento para gestionar solicitudes antes de que comience la evaluación sustantiva. Addressed by clauses [4.1.5; 6.1.5].

13.3.8 **Article 28** - Mapeado con asistencia del encargado del tratamiento y subencargado, instrucciones documentadas del cliente, plazos de apoyo, ausencia de respuesta directa sin autorización y escalado de la falta de cooperación. Addressed by clauses [4.1.6; 4.1.7; 4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.5.6; 6.1.6].

13.3.9 **Article 30** - Mapeado con la vinculación de solicitudes de derechos a registros de tratamiento, actividades de tratamiento, sistemas, categorías de PII, destinatarios y registros del encargado del tratamiento. Addressed by clauses [4.1.4; 4.2.3; 4.3.8; 4.5.1; 7.1.3].

13.3.10 **Article 32** - Mapeado con gestión segura de solicitudes de derechos, protección de la entrega de respuestas, prevención de divulgación no autorizada y protección de evidencias de derechos. Addressed by clauses [4.2.5; 4.2.6; 7.1.4; 7.1.5; 10.1.2; 10.1.6].

13.3.11 **Article 39** - Mapeado con el asesoramiento y el seguimiento de Data Protection Officer / Privacy Advisor para solicitudes de derechos de alto riesgo, disputadas, denegadas, prorrogadas y relacionadas con decisiones automatizadas. Addressed by clauses [4.2.4; 4.2.7; 4.3.7; 4.4.3; 6.1.3; 9.1.3; 11.1.3].

#### **13.4 ISO/IEC 29100:2020**

13.4.1 **Clause 5.8; Clause 5.9; Clause 5.10; Clause 5.12** - Mapeado con transparencia de los canales de derechos, participación individual y acceso, responsabilidad proactiva, procedimientos de reclamación/recurso, seguimiento del cumplimiento de privacidad y evidencias de auditoría. Addressed by clauses [4.1.3; 4.2.1; 4.3.1; 4.3.2; 4.3.3; 4.3.8; 4.4.6; 7.1.1; 8.1.5; 10.1.1].

#### **13.5 ISO/IEC 29151:2022**

13.5.1 **Annex A.10** - Mapeado con participación y acceso del interesado, verificación de identidad, acceso, rectificación, eliminación, actualizaciones de estado, apoyo del encargado del tratamiento y mecanismos de reclamación/recurso. Addressed by clauses [4.1.1; 4.2.1; 4.3.1; 4.3.2; 4.3.3; 4.4.4; 4.5.1; 4.5.4; 8.1.6].

#### **13.6 Requisitos internos**

13.6.1 **Internal requirement** - Las cláusulas que definen REG06 como el objeto de evidencia principal de derechos, la formación, la aprobación de flujos de trabajo no estándar, la caducidad de excepciones, la revisión de la política y la comunicación de cambios de la política apoyan la coherencia de la implementación, pero no están mapeadas directamente con una única cláusula externa. Addressed by clauses [5.1.2; 6.1.7; 7.1.6; 9.1.4; 9.1.5; 11.1.2; 11.1.4; 11.1.5].