NORMA DE GESTIÓN DE SUMINISTRADORES

MUFACE

Documentación: MUFACE -Seguridad

Oficina de Seguridad de la Información

Referencia: Seguridad de la Información

Versión del documento 1.0

INDICE

Cuadro Resumen del Documento

Tipo de Documento	Norma sobre responsabilidad de la información y criterios para su calificación
Autor	Oficina de Seguridad de la Información MUFACE
Fecha de elaboración	03/10/2025
Revisado por	Leonardo González García
Aprobado por	Silvia Lacleta (Responsable de Seguridad)

Control de Cambios

Versión	Fecha	Descripción de la modificación
1.0	03/10/2025	Versión inicial

1 Introducción

El Real Decreto 311/2022, de 3 de mayo, que regula el Esquema Nacional de Seguridad (ENS) en el ámbito de aplicación al sector público, según el artículo 2 de la Ley 40/2015 del 1 de octubre, y según el artículo 156.2, establece los principios básicos y requisitos mínimos requeridos para proteger la información. Las Administraciones Públicas deberán aplicarlo para asegurar el acceso, integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad y conservación de los datos, informaciones y servicios utilizados en medios electrónicos que gestionen en el ejercicio de sus competencias.

El objeto de este documento es identificar las directrices a seguir tanto en la adquisición de productos como en la contratación de servicios externos por parte de MUFACE de manera que quede garantizada la seguridad en todo el proceso.

2 Ámbito de aplicación

Esta norma aplica a todos los usuarios (tanto internos como externos) con responsabilidad en la gestión de la adquisición de productos en MUFACE, así como, a aquellos con responsabilidad en la contratación de servicios externos. De igual manera, involucra a aquellos responsables de la realización del seguimiento del cumplimiento de los requisitos establecidos, como por ejemplo el cumplimiento del Acuerdo de Nivel de
Servicio (SLA) si fuera diferente a los anteriores.

En ambos casos, el ámbito de aplicación estricto se refiere a aquellos productos y servicios relacionados con el ejercicio de derechos, con el cumplimiento de deberes por medios electrónicos o con el acceso por medios electrónicos de los ciudadanos a la información, los servicios y al procedimiento administrativo, de acuerdo con lo previsto en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas y con lo establecido por el ENS.

No obstante, lo establecido en el presente documento podrá ser, asimismo, de aplicación a todos aquellos sistemas o servicios que no queden contenidos en el ámbito de aplicación del ENS, si así se determinara por los responsables competentes.

3 Contexto

Este documento forma parte del cuerpo normativo de la Política de Seguridad de la Información (PSI) de MUFACE, desarrollado para garantizar la seguridad de la información en la misma.

El *Responsable de Seguridad* correspondiente aprobará los procedimientos específicos que sean necesarios para el desarrollo de esta norma.

4 Vigencia

El presente documento producirá efectos desde la fecha de aprobación, indicada en la segunda página del mismo, y hasta que sea reemplazado por una nueva versión.

Las versiones anteriores que hayan podido distribuirse constituyen borradores o versiones obsoletas, por lo que su vigencia queda anulada por la última versión de este documento. En cualquier caso, toda la información referente a versiones, modificaciones, etc., aparece descrita en la ficha de versiones al inicio del documento.

5 Adquisición de nuevos componentes

Se llevará a cabo la planificación de la adquisición de nuevos componentes del sistema según el procedimiento correspondiente, de manera que se considere todo aquello que deba serle demandado al proveedor.

Se tendrán en cuenta para ello los requisitos de seguridad necesarios teniendo en cuenta los análisis de riesgos efectuados. Tendrán mayor importancia cuanto más alta sea la categoría del sistema. De igual manera, se considerarán los requisitos requeridos para su compatibilidad tecnológica con la arquitectura de seguridad.

Dicha planificación recogerá asimismo las actividades de evaluación o aceptación que permitan garantizar que se cumplen los requisitos especificados, entre las que se incluirán, entre otros temas, comprobaciones relacionadas con el cumplimiento de la calidad mínima esperada, con la integridad de los embalajes y de los propios

componentes, con la documentación de seguridad aportada o con el dimensionamiento requerido.

Por otra parte, según el artículo 18 del ENS, en la adquisición de productos de seguridad de las tecnologías de la información y comunicaciones que vayan a ser utilizados por las Administraciones públicas se utilizarán, de forma proporcionada a la categoría del sistema y el nivel de seguridad determinados, aquellos que tengan certificada la funcionalidad de seguridad relacionada con el objeto de su adquisición. Según indica la medida op.pl.5 Se utilizará el Catálogo de Productos y Servicios de Seguridad de las Tecnologías de la Información y Comunicación (CPSTIC) del CCN, para seleccionar los productos o servicios suministrados por un tercero que formen parte de la arquitectura de seguridad del sistema y aquellos que se referencien expresamente en las medidas de este real decreto. En caso de que no existan productos o servicios en el CPSTIC que implementen las funcionalidades requeridas, se utilizarán productos certificados de acuerdo con lo descrito en el artículo 19 ENS.

Se establecerá un acuerdo de nivel de servicio (SLA) a cumplir por el proveedor, que garantice la reparación o el reemplazo de los componentes defectuosos o que sufran una avería en el plazo máximo de tiempo fijado, que se estimará en función de la criticidad del componente. Incluirá las consecuencias derivadas de su incumplimiento.

Se procurará incluir en la contratación la formación que pueda ser necesaria para la instalación y manejo seguro del componente.

Una vez recibido e instalado el nuevo componente, se actualizará la documentación de seguridad y los procedimientos operativos de los sistemas en los que se integre.

Se deberá exigir el borrado seguro de la información o ficheros de configuración que contengan los equipos o componentes cuando lleguen al final de su vida útil de manera previa a su reutilización o desafectación.

6 Contratación de servicios externos

Según indica la medida op.ext.1, de forma previa al establecimiento de una relación con terceros, se establecerán las características del servicio a prestar, lo que debe entenderse

como «servicio mínimo admisible», las responsabilidades de las partes y las consecuencias en caso de incumplimiento.

El Pliego de Prescripciones Técnicas deberá recoger la especificación de requisitos funcionales, incluyendo la calidad mínima esperada y los entregables de documentación a aportar por el proveedor. Asimismo, contendrá los requisitos de seguridad, que habrán sido obtenidos a partir del análisis de riesgos.

Tendrá en cuenta además las posibles especificidades ocasionadas por, entre otros aspectos, el lugar de ejecución del servicio, la propiedad de la infraestructura o sistemas TIC utilizados en el marco del contrato o la necesidad de disponer de accesos privilegiados.

Se deberán recoger en los pliegos de contratación al menos unas cláusulas en las que figure el contenido mínimo y esencial que se indica a continuación, según los modelos recogidos en el Anexo II o similares, en orden a garantizar el cumplimiento de las medidas de seguridad:

- Confidencialidad (por ejemplo, suscribiendo el correspondiente Acuerdo de Confidencialidad con Terceros)
- Propiedad intelectual.
- Responsabilidad de las partes.
- Resolución anticipada de contrato.
- Privacidad y protección de datos (contrato del art. 28 RGPD).
- Ley aplicable y jurisdicción.
- Auditabilidad.
- Medidas de seguridad a aplicar en el marco del contrato.
- Acuerdo de nivel de servicio (SLA).
    1. Mecanismos de medición del cumplimiento del SLA.
    2. Consecuencias por incumplimiento de SLA.
- j) Deberes y Obligaciones del personal externo.

En el caso de contratación de servicios prestados en modalidad de servicios en nube (“cloud computing”), se tomará como referencia las recomendaciones de la guía CCNSTIC 823, así como, el contenido del op.nub.1 del ENS.

Se exigirá al proveedor respetar el deber de secreto, según el modelo recogido en el Anexo II de este documento o similar, en especial en contratos de prestación de servicios en los que se maneje información calificada en niveles medio o alto según la dimensión de confidencialidad del ENS

Se informará a la empresa adjudicataria de los riesgos laborales, medidas preventivas y medidas de emergencia relativos a la actividad que deberán llevar a cabo en las instalaciones de MUFACE y las personas designadas por la misma para el cumplimiento del contrato, en el caso de que así sea. Se solicitará a la empresa confirmación del conocimiento de esta información por parte de las citadas personas. Se seguirá para ello el procedimiento correspondiente.

Se realizará un seguimiento de la ejecución del servicio y se atenderá en especial a los aspectos de seguridad que se deben cumplir por parte de los proveedores del mismo y del personal contratado para ello y que se regulan en la Norma de deberes y obligaciones del personal y empresas externas.

7 Responsabilidades

El contenido de esta norma es de obligado conocimiento y cumplimiento por parte de las personas con responsabilidad en la gestión de la seguridad en MUFACE, así como, por aquellos con responsabilidad en la adquisición de componentes y servicios y en el seguimiento del cumplimiento de los requisitos especificados, pudiéndose derivar de su incumplimiento la pertinente responsabilidad en el ámbito disciplinario, si a ello hubiera lugar en aplicación de las disposiciones reguladoras del estatuto jurídico del usuario.

Las responsabilidades asociadas a cada componente de la estructura organizativa para la gestión de la seguridad en MUFACE es la definida en la Norma de Organización de Seguridad y Responsabilidades.

La detección de actuaciones irregulares, ilícitas o ilegales podrá acarrear la iniciación de las medidas disciplinarias oportunas y, en su caso, de las acciones legales correspondientes.

8 Revisión de la norma

La presente norma y cualquier modificación a la misma, entrará en vigor en el momento en que sea aprobada por el *Comité de Seguridad de la Información* de MUFACE, lo que se notificará oportunamente mediante su publicación en la Intranet MUFACE.

Las modificaciones totales o parciales de la presente normativa, así como la referencia de los documentos o versiones que sustituyen a este documento serán registradas mediante control de cambios y versión del documento.

9 Anexo I: Modelo de cláusula administrativa particular sobre certificación de sistemas o componentes

31. «Cláusula administrativa particular.– En cumplimiento con lo dispuesto en el artículo 19 del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, el licitador incluirá referencia precisa, documentada y acreditativa de que los productos de seguridad, equipos, sistemas, aplicaciones o sus componentes, cumplen con lo indicado en la medida op.pl.5 sobre componentes certificados, recogida en el Anexo II del citado Real Decreto 311/2022.

Cuando estos sean empleados para el tratamiento de datos de carácter personal, el licitador incluirá, también, lo establecido en la Disposición adicional única del Real Decreto 1720/2007, de 21 de diciembre.»

10 Anexo II: Cláusulas sobre confidencialidad, propiedad intelectual, auditabilidad y protección de datos

10.1 Modelo de acuerdo de confidencialidad

Podrá utilizarse como referencia lo indicado en la guía CCN-STIC-821: Esquema Nacional de Seguridad. Normas de seguridad, en su apéndice VI: Acuerdo de confidencialidad para terceros.

10.2 Propiedad Intelectual

En línea con lo expresado en el artículo 308.3 del Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, y en aras de garantizar la dimensión de seguridad de disponibilidad, se define la siguiente cláusula respecto a la Propiedad Intelectual.

El adjudicatario acepta expresamente que los derechos de propiedad sobre los soportes materiales a los que se incorporen los trabajos realizados en cumplimiento de las obligaciones derivadas del contrato objeto de este expediente corresponden a la administración contratante. Por lo tanto, queda expresamente prohibida la utilización, reproducción o difusión, fuera del objeto contractual del presente contrato, por cualquier persona física o jurídica, de todo o parte tanto de los productos y documentación entregada por la administración para el cumplimiento de las obligaciones derivadas del presente contrato, así como de los productos generados por el proyecto, bien sean entregables o productos intermedios de trabajo. Para ello se requiere el consentimiento escrito de MUFACE a través del responsable correspondiente o persona que quede oficialmente identificada a tal fin.

MUFACE podrá reproducir, publicar y divulgar, total o parcialmente, todos los productos y entregables elaborados durante la ejecución del presente contrato sin que pueda oponerse a ello el/los adjudicatario/s y/o autor/es de los trabajos.

Específicamente, todos los derechos de explotación y titularidad de las aplicaciones informáticas y programas de ordenador desarrollados al amparo del contrato resultante de la adjudicación del presente concurso, incluyendo su código fuente, corresponden únicamente a la organización contratante.

10.3 Deber de secreto

El contratista, en tanto en cuanto acceda a información calificada según la dimensión de confidencialidad establecida en el ENS o datos de carácter personal contenidos en cualquier soporte que los haga susceptibles de tratamiento de los que sea responsable MUFACE o intervenga en cualquier fase de su tratamiento, es decir, en su recogida, grabación, conservación, elaboración, modificación, bloqueo, cancelación y cesiones a terceros, se obliga al secreto profesional respecto de los mismos, comprometiéndose a no divulgarlos, publicarlos, revelarlos ni de otra forma, directa o indirecta, ponerlos a disposición de terceros, ni total ni parcialmente, y a cumplir esta obligación incluso con sus propios familiares y otros miembros de la Dirección que no estén autorizados a acceder a dichos datos, cualquiera que sea el soporte en el que se encuentre la información. La obligación del deber de secreto subsistirá aun después de finalizar sus relaciones con MUFACE, por lo que el usuario garantiza que, una vez terminada la relación, guardará el mismo secreto profesional respecto de dichos datos a los que haya tenido acceso durante el desempeño de sus funciones.

Si la empresa adjudicataria aporta equipos informáticos, una vez finalizadas las tareas el adjudicatario, previamente a retirar los equipos informáticos, deberá borrar toda la información utilizada o que se derive de la ejecución del contrato, mediante el procedimiento técnico adecuado. La destrucción de la documentación de apoyo, si no se considerará indispensable, se efectuará mediante máquina destructora de papel o cualquier otro medio que garantice la ilegibilidad, efectuándose esta operación en el lugar donde se realicen los trabajos. Esto mismo será aplicable a cualquier otro soporte de información.

10.4 Ley Orgánica de Protección de Datos

MUFACE y el contratista, como encargado del tratamiento, tal y como se define en el apartado 8) del artículo 4 del RGPD tendrán el deber de firmar el correspondiente contrato

de encargo del tratamiento que recogerá todas las especificaciones establecidas en el art. 28 del RGPD, que establece, como contenido mínimo el siguiente:

- El objeto.
- La duración.
- La naturaleza.
- La finalidad del tratamiento.
- El tipo de datos personales.
- Categorías de interesados.
- Las obligaciones y derechos del responsable.

Estipulándose, en concreto que el encargado:

a) tratará los datos personales únicamente siguiendo instrucciones documentadas del responsable, inclusive con respecto a las transferencias de datos personales a un tercer país o una organización internacional, salvo que esté obligado a ello en virtud del Derecho de la Unión o de los Estados miembros que se aplique al encargado; en tal caso, el encargado informará al responsable de esa exigencia legal previa al tratamiento, salvo que tal Derecho lo prohíba por razones importantes de interés público;

b) garantizará que las personas autorizadas para tratar datos personales se hayan comprometido a respetar la confidencialidad o estén sujetas a una obligación de confidencialidad de naturaleza estatutaria;

c) tomará todas las medidas necesarias de conformidad con el artículo 32;

d) respetará las condiciones indicadas en los apartados 2 y 4 para recurrir a otro encargado del tratamiento;

e) asistirá al responsable, teniendo cuenta la naturaleza del tratamiento, a través de medidas técnicas y organizativas apropiadas, siempre que sea posible, para que este pueda cumplir con su obligación de responder a las solicitudes que tengan por objeto el ejercicio de los derechos de los interesados establecidos en el capítulo III;

f) ayudará al responsable a garantizar el cumplimiento de las obligaciones establecidas en los artículos 32 a 36, teniendo en cuenta la naturaleza del tratamiento y la información a disposición del encargado;

g) a elección del responsable, suprimirá o devolverá todos los datos personales una vez finalice la prestación de los servicios de tratamiento, y suprimirá las copias

existentes a menos que se requiera la conservación de los datos personales en virtud del Derecho de la Unión o de los Estados miembros;

h) pondrá a disposición del responsable toda la información necesaria para demostrar el cumplimiento de las obligaciones establecidas en el presente artículo, así como para permitir y contribuir a la realización de auditorías, incluidas inspecciones, por parte del responsable o de otro auditor autorizado por dicho responsable.

En relación con lo dispuesto en la letra h) del párrafo primero, el encargado informará inmediatamente al responsable si, en su opinión, una instrucción infringe el presente Reglamento u otras disposiciones en materia de protección de datos de la Unión o de los Estados miembros.

10.5 Auditabilidad

MUFACE se reserva el derecho de verificar, mediante auditorías, el cumplimiento de toda medida de seguridad indicada en los documentos asociados al contrato. Esto incluye la posibilidad de realización de revisiones o auditorías del código fuente o de la documentación en el caso de servicios de desarrollo de software.

Asimismo, se reserva el derecho de realizar un seguimiento de los servicios contratados mediante las correspondientes auditorías, con objeto de verificar el cumplimiento de los acuerdos firmados.

10.6 Deberes y Obligaciones de los Empleados

El adjudicatario queda obligado a comunicar y hacer cumplir a sus empleados los deberes y obligaciones establecidas en los apartados anteriores y las derivadas del cumplimiento de la Norma de Deberes y Obligaciones del Personal y Empresas Externas, así como cualquier otra necesaria para el cumplimiento de los Acuerdos de Nivel de Servicio o de cualquier otro documento contractual o regulatorio.

11 Anexo III: Productos a certificar

Para los sistemas de categoría alta, según medida op.pl.5, se valorará preferentemente que sus funcionalidades de seguridad estén certificadas. Además, en el Anexo II del ENS,

se establece, por cada una de las medidas de seguridad, basadas en componentes, cuando es obligatorio o preferente que los productos estén certificados, tal y como se muestra a continuación:

Tipo de Producto	Nivel del Requisito de Certificación	Medida Anexo II ENS	Categoría desde la que aplica
Mecanismos de autenticación	Preferentemente certificado	op.acc.5 op.pl.5	ALTO
Protección de las claves criptográficas	Obligatoriamente certificado (aplica desde nivel medio	op.exp.11 op.pl.5	MEDIA
Protección de la confidencialidad en las comunicaciones	Preferentemente certificado	mp.com.2 op.pl.5	ALTO
Protección de la autenticidad y de la integridad en las comunicaciones	Preferentemente certificado	mp.com.3 op.pl.5	ALTO
Criptografía de la información en soportes	Preferentemente certificado	mp.si.2 op.pl.5	ALTO
Productos de borrado y destrucción de soportes	Preferentemente certificado (aplica desde nivel medio)	mp.si.5 op.pl.5	MEDIA
Productos de firma electrónica	Preferentemente certificado	mp.info.4 op.pl.5	ALTO
Sellado de tiempo	Obligatoriamente certificado	mp.info.5 op.pl.5	ALTO

12 Anexo IV: Referencias

Se deberán tomar en consideración los siguientes textos y normativas:

- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- PSI Política de Seguridad de la Información de MUFACE.
- Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público.
- Centro Criptológico Nacional. Guía de Seguridad CCN-STIC-205: Actividades de seguridad en el ciclo de vida de los sistemas TIC.
- Centro Criptológico Nacional. Guía de Seguridad CCN-STIC-404: Control de soportes informáticos.
- Centro Criptológico Nacional. Guía de Seguridad CCN-STIC-800: Esquema Nacional de Seguridad - Glosario de Términos y Abreviaturas.
- Centro Criptológico Nacional. Guía de Seguridad CCN-STIC-804: Esquema Nacional de Seguridad. Guía de implantación.
- Centro Criptológico Nacional. Guía de Seguridad CCN-STIC-808: Verificación del Cumplimiento de las Medidas en el ENS.
- Centro Criptológico Nacional. Guía de Seguridad CCN-STIC-813: Componentes certificados en el ENS.
- Centro Criptológico Nacional. Guía de Seguridad CCN-STIC-819: Esquema Nacional de Seguridad. Contratación en el ENS.
- Centro Criptológico Nacional. Guía de Seguridad CCN-STIC-821: Esquema Nacional de Seguridad. Normas de seguridad.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).
- Magerit versión 3.0: Metodología de Análisis de Gestión de Riesgos de los Sistemas de información.

Las directrices estipuladas en esta norma se fundamentan en los requisitos establecidos en el ENS que se mencionan a continuación[1].

12.1 Artículo 19 del ENS: Adquisición de productos de seguridad.

Adquisición de productos de seguridad y contratación de servicios de seguridad.

1. En la adquisición de productos de seguridad o contratación de servicios de seguridad de las tecnologías de la información y la comunicación que vayan a ser empleados en los sistemas de información del ámbito de aplicación de este real decreto, se utilizarán, de forma proporcionada a la categoría del sistema y el nivel de seguridad determinados, aquellos que tengan certificada la funcionalidad de seguridad relacionada con el objeto de su adquisición.

2. El Organismo de Certificación del Esquema Nacional de Evaluación y Certificación de Seguridad de las Tecnologías de la Información del Centro Criptológico Nacional (en adelante, CCN), constituido al amparo de lo dispuesto en el artículo 2.2.c) del Real Decreto 421/2004, de 12 de marzo, por el que se regula el Centro Criptológico Nacional, teniendo en cuenta los criterios y metodologías de evaluación nacionales e internacionales reconocidas por este organismo y en función del uso previsto del producto o servicio concreto dentro de sus competencias, determinará los siguientes aspectos:

- Los requisitos funcionales de seguridad y de aseguramiento de la certificación.
- Otras certificaciones de seguridad adicionales que se requieran normativamente.
- Excepcionalmente, el criterio a seguir en los casos en que no existan productos o servicios certificados.

3. Para la contratación de servicios de seguridad se estará a lo señalado en los apartados anteriores y a lo dispuesto en el artículo 16 ENS.

12.2 Medida op.pl.3

Se establecerá un proceso formal para planificar la adquisición de nuevos componentes del sistema, proceso que:

- Atenderá a las conclusiones del análisis de riesgos ([op.pl.1]).

[1] Se trata de una extracción de aspectos o medidas específicos del ENS (Real Decreto 311/2022) en relación con lo tratado en esta norma, con el fin de que el presente documento sea auto contenido y de más fácil lectura.

- Será acorde a la arquitectura de seguridad escogida ([op.pl.2]).
- Contemplará las necesidades técnicas, de formación y de financiación, de forma conjunta.

12.3 Medida op.pl.4

Con carácter previo a la puesta en explotación, se realizará un estudio que cubrirá los siguientes aspectos:

- Necesidades de procesamiento.
- Necesidades de almacenamiento de información: durante su procesamiento y durante el periodo que deba retenerse.
- Necesidades de comunicación.
- Necesidades de personal: cantidad y cualificación profesional.
- Necesidades de instalaciones y medios auxiliares.

Refuerzo R1 –Mejora continua de la gestión de la capacidad.

- Se realizará una previsión de la capacidad y se mantendrá actualizada durante todo el ciclo de vida del sistema.
- Se emplearán herramientas y recursos para la monitorización de la capacidad.

12.4 Medida op.pl.5

Se utilizará el Catálogo de Productos y Servicios de Seguridad de las Tecnologías de la Información y Comunicación (CPSTIC) del CCN, para seleccionar los productos o servicios suministrados por un tercero que formen parte de la arquitectura de seguridad del sistema y aquellos que se referencien expresamente en las medidas de este real decreto.

En caso de que no existan productos o servicios en el CPSTIC que implementen las funcionalidades requeridas, se utilizarán productos certificados de acuerdo a lo descrito en el artículo 19.

Una Instrucción Técnica de Seguridad detallará los criterios relativos a la adquisición de productos de seguridad.

- Si el sistema suministra un servicio de seguridad a un tercero bajo el alcance del ENS, el producto o productos que en los que se sustente dicho servicio debe superar un proceso de cualificación y ser incluido en el CPSTIC, o aportar una

certificación que cumpla con los requisitos funcionales de seguridad y de aseguramiento de acuerdo a lo establecido en el artículo 19.

Refuerzo R1-Protección de emisiones electromagnéticas.

- La información deberá ser protegida frente a las amenazas TEMPEST de acuerdo con la normativa en vigor.

12.5 Medida op.ext.1

Con anterioridad a la efectiva utilización de los recursos externos se establecerá contractualmente un Acuerdo de Nivel de Servicio, que incluirá las características del servicio prestado, lo que debe entenderse como «servicio mínimo admisible», así como, la responsabilidad del prestador y las consecuencias de eventuales incumplimientos.