

# Guía de Seguridad de las TIC

## CCN-STIC 803

### ENS. Valoración de los sistemas



Noviembre 2017

Edita:



© Centro Criptológico Nacional, 2017

NIPO: 785-17-078-3

Fecha de Edición: noviembre de 2017

José Antonio Mañas y AUDERTIS han colaborado en la revisión del presente documento y sus anexos

#### **LIMITACIÓN DE RESPONSABILIDAD**

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

#### **AVISO LEGAL**

Quedan rigurosamente prohibidas, sin la autorización escrita del Centro Criptológico Nacional, bajo las sanciones establecidas en las leyes, la reproducción parcial o total de este documento por cualquier medio o procedimiento, comprendidos la reprografía y el tratamiento informático, y la distribución de ejemplares del mismo mediante alquiler o préstamo públicos.

## PRÓLOGO

El uso masivo de las tecnologías de la información y la comunicación (TIC), en todos los ámbitos de la sociedad, ha creado un nuevo espacio, el ciberespacio, donde se producirán conflictos y agresiones, y donde existen ciberamenazas que atentarán contra la seguridad nacional, el estado de derecho, la prosperidad económica, el estado de bienestar y el normal funcionamiento de la sociedad y de las administraciones públicas.

La Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia (CNI), encomienda al Centro Nacional de Inteligencia el ejercicio de las funciones relativas a la seguridad de las tecnologías de la información en su artículo 4.e), y de protección de la información clasificada en su artículo 4.f), a la vez que confiere a su Secretario de Estado Director la responsabilidad de dirigir el Centro Criptológico Nacional (CCN) en su artículo 9.2.f).

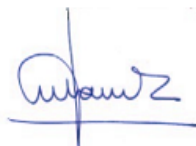
Partiendo del conocimiento y la experiencia del CNI sobre amenazas y vulnerabilidades en materia de riesgos emergentes, el Centro realiza, a través de su Centro Criptológico Nacional, regulado por el Real Decreto 421/2004, de 12 de marzo, diversas actividades directamente relacionadas con la seguridad de las TIC, orientadas a la formación de personal experto, a la aplicación de políticas y procedimientos de seguridad, y al empleo de tecnologías de seguridad adecuadas.

El Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica (ENS, en adelante), al que se refiere el apartado segundo del artículo 156 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, establece la política de seguridad en la utilización de medios electrónicos que permita una protección adecuada de la información.

Precisamente el Real Decreto 3/2010 de 8 de enero, modificado por el Real Decreto 951/2015, de 23 de octubre, fija los principios básicos y requisitos mínimos, así como las medidas de protección a implantar en los sistemas de la Administración, y promueve la elaboración y difusión de guías de seguridad de las tecnologías de la información y la comunicación (STIC) por parte de CCN para facilitar un mejor cumplimiento de dichos requisitos mínimos.

En definitiva, la serie de documentos CCN-STIC se elabora para dar cumplimiento a los cometidos del Centro Criptológico Nacional y a lo reflejado en el Esquema Nacional de Seguridad, conscientes de la importancia que tiene el establecimiento de un marco de referencia en esta materia que sirva de apoyo para que el personal de la Administración lleve a cabo su difícil, y en ocasiones, ingrata tarea de proporcionar seguridad a los sistemas de las TIC bajo su responsabilidad.

Noviembre de 2017



Félix Sanz Roldán

Secretario de Estado

Director del Centro Criptológico Nacional

## ÍNDICE

<b>1. INTRODUCCIÓN .....</b>	<b>1</b>
1.1. NECESIDAD DE VALORAR.....	2
1.2. PROCEDIMIENTO DE VALORACIÓN .....	2
1.3. NOTIFICACIONES Y PUBLICACIONES ELECTRÓNICAS.....	3
<b>2. CRITERIOS DE VALORACIÓN .....</b>	<b>4</b>
2.1. CRITERIOS COMUNES APLICABLES A TODAS LAS DIMENSIONES.....	4
2.2. CRITERIOS PARA TIPOS DE INFORMACIÓN CON DATOS DE CARÁCTER PERSONAL.....	7
2.3. CRITERIOS PARA LA DISPONIBILIDAD DE LOS SERVICIOS.....	12
2.3.1. PERIODOS CRÍTICOS.....	12
2.3.2. RTO (TIEMPO DE RECUPERACIÓN OBJETIVO) .....	12
2.4. CRITERIOS ESPECÍFICOS .....	13
2.5. CRITERIOS ESPECÍFICOS PARA OPERADORES CRÍTICOS DEL SECTOR PÚBLICO.....	13
<b>3. TIPOS DE INFORMACIÓN.....</b>	<b>14</b>
3.1. IDENTIFICACIÓN.....	14
3.2. VALORACIÓN.....	15
3.2.1. CONFIDENCIALIDAD.....	15
3.2.2. INTEGRIDAD .....	16
3.2.3. AUTENTICIDAD.....	16
3.2.4. TRAZABILIDAD.....	16
<b>4. SERVICIOS.....</b>	<b>17</b>
4.1. IDENTIFICACIÓN.....	17
4.2. VALORACIÓN.....	17
4.2.1. DISPONIBILIDAD.....	18
<b>5. DETERMINACIÓN DE LOS NIVELES Y CATEGORÍA DEL SISTEMA .....</b>	<b>19</b>
5.1. VALORACIÓN DE LAS DIMENSIONES DE LOS ACTIVOS ESENCIALES.....	19
5.2. DETERMINACIÓN DE SUBSISTEMAS .....	19
5.3. FORMULACIÓN DE LA CATEGORÍA DE UN SISTEMA.....	20
5.4. TERCERAS PARTES.....	21
5.5. DOCUMENTACIÓN .....	22
<b>6. ANEXO A. GLOSARIO DE TÉRMINOS .....</b>	<b>23</b>
<b>7. ANEXO B. ABREVIATURAS.....</b>	<b>26</b>
<b>8. ANEXO C. REFERENCIAS .....</b>	<b>27</b>



CCN-STIC-803



SIN CLASIFICAR

ENS Valoración de los sistemas

## 1. INTRODUCCIÓN

1. Esta guía establece unas pautas de carácter general que son aplicables a entidades de distinta naturaleza, dimensión y sensibilidad, sin entrar en casuísticas particulares. Se espera que cada organización las particularice para adaptarlas a su entorno singular.
2. El Esquema Nacional de Seguridad establece una serie de medidas de seguridad en su Anexo II que están condicionadas a la valoración del nivel de seguridad en cada dimensión, y a la categoría (artículo 43) del sistema de información de que se trate. A su vez, la categoría del sistema se calcula en función del nivel de seguridad más alto de las dimensiones valoradas.
3. El proceso de determinación de niveles y categorías se establece en el Anexo I, que aporta una serie de criterios generales para determinar si los requisitos de seguridad son de nivel ALTO, MEDIO o BAJO en cada una de las dimensiones de seguridad: confidencialidad [C], integridad [I], disponibilidad [D], autenticidad [A], y trazabilidad [T].
4. El Esquema Nacional de Seguridad establece tres categorías para los sistemas: BÁSICA, MEDIA y ALTA.
  - Un sistema de información será de categoría ALTA si alguna de sus dimensiones de seguridad alcanza el nivel ALTO.
  - Un sistema de información será de categoría MEDIA si alguna de sus dimensiones de seguridad alcanza el nivel MEDIO y ninguna alcanza un nivel superior.
  - Un sistema de información será de categoría BÁSICA si alguna de sus dimensiones de seguridad alcanza el nivel BAJO y ninguna alcanza un nivel superior.
5. La Agencia Española de Protección de Datos señala en su nota “El impacto del reglamento general de protección de datos sobre la actividad de las administraciones públicas” que “en el caso de las AAPP, la aplicación de las medidas de seguridad estará marcada por los criterios establecidos en el Esquema Nacional de Seguridad”.
6. Asimismo el 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 (en adelante, RGPD) obliga a que cuando se traten datos de carácter personal se realice un análisis de riesgos para los derechos y libertades de los ciudadanos y hace depender la aplicación de todas las medidas de cumplimiento que prevé (entre ellas las de seguridad) del nivel y tipo de riesgo que cada tratamiento implique para los derechos y libertades de los afectados.
7. Esta guía pretende definir los criterios para determinar el nivel de seguridad requerido en cada dimensión y ofrecer recomendaciones considerando también los marcos normativos mencionados, que podrán ser desarrollados

posteriormente en su propia legislación. Para ello se analizan los elementos esenciales, información y servicios, pivotando alrededor de ellos los criterios que el responsable de cada tipo de información y cada servicio podrá utilizar, teniendo en cuenta que la facultad para determinar la categoría del sistema corresponde al responsable del mismo.

### 1.1. NECESIDAD DE VALORAR

8. Con frecuencia, el valor del sistema en materia de seguridad se concentra en unos pocos activos que son la esencia y razón de ser del sistema, denominados activos esenciales, y en unas pocas dimensiones. Es conveniente centrarse en aquellos activos y en aquellas dimensiones en las que el impacto de un incidente sea mayor, obviando aquellas combinaciones en las que el impacto sea despreciable o irrelevante.
9. Conviene comenzar por los activos de tipo información, valorando en este orden: confidencialidad, integridad, autenticidad, trazabilidad y, si fuera relevante, disponibilidad. Es frecuente que la disponibilidad no sea un atributo relevante de la información y quede sin adscribir a ningún nivel.
10. Conviene seguir con los activos de tipo servicio, valorando para los mismos la disponibilidad. Los requisitos en materia de confidencialidad, integridad, autenticidad y trazabilidad suelen venir impuestos por los tipos de información que maneja el servicio, asumiendo los establecidos en el párrafo anterior.
11. Un sistema asumirá, para cada dimensión, el valor máximo considerado para la misma en los distintos tipos de información manejados y en los servicios prestados.
12. La categoría del sistema se determina considerando el valor máximo de todas sus dimensiones.

### 1.2. PROCEDIMIENTO DE VALORACIÓN

13. Si la entidad ha creado un Comité TIC<sup>1</sup> y un Comité STIC<sup>2</sup>, una de las funciones del Comité TIC puede ser la determinación de los tipos de información que se van a manejar y de los servicios que se van a prestar, priorizando los denominados activos esenciales que pueden tener una mayor criticidad. Definidos los tipos de información y de servicios, una tarea del Comité STIC puede ser el establecimiento de los niveles de seguridad recomendados en cada dimensión para cada uno de estos activos esenciales. Estas valoraciones deben ser aprobadas dentro del juego de normativa que rige las actuaciones de la entidad.
14. Los niveles así establecidos podrán ser posteriormente ajustados por los responsables correspondientes. Idealmente, todas las valoraciones vendrán establecidas por la normativa.

---

<sup>1</sup> Comité TIC: de Tecnologías de la Información y la Comunicación.

<sup>2</sup> Comité STIC: de Seguridad en las Tecnologías de Información y la Comunicación.

15. La responsabilidad de la valoración de la información y de los servicios es exclusivamente del responsable de la información y del servicio correspondiente, pero puede ser propuesta por el Responsable del Sistema, por el Responsable de la Seguridad o por el Comité STIC y aprobada posteriormente por el Responsable de la Información o del Servicio correspondiente si éste la considera adecuada.
16. Exceptuando aquellos puntos en los que exista un mandato legal o administrativo, la opinión del Responsable de la Seguridad y del Responsable del Sistema deben ser recabadas y consideradas en el proceso de valoración.
17. Cuando el sistema trate datos de carácter personal, esta guía incluye unos criterios para facilitar la determinación de los niveles mínimos de las dimensiones de seguridad a adoptar en función de los tipos de datos personales y las características de los tratamientos de los que sean objeto, si bien será la Agencia Española de Protección de Datos la que los establezca reglamentariamente.
18. Una vez determinadas las valoraciones de los diferentes tipos de información que se manejan y los diferentes servicios que se prestan, el Responsable de la Seguridad se encarga de aplicar el procedimiento descrito en el Anexo I del Real Decreto 3/2010 para, de acuerdo a los niveles máximos de cada dimensión de seguridad y por tanto de la categoría del sistema, determinar el conjunto mínimo de medidas de seguridad del Anexo II del Real Decreto 3/2010 que son de aplicación en el sistema considerando las condiciones indicadas en dicho anexo.
19. La determinación de la categoría de un sistema no implica que se altere, por este hecho, el nivel de las dimensiones de seguridad que no han influido en la determinación de la categoría del mismo. Sin embargo, cabe tener en cuenta que la asignación de una categoría al sistema puede requerir elevar el nivel de madurez de las medidas que resulten de aplicación.
20. Por último, se deberá enriquecer el conjunto de medidas con aquéllas que puedan derivarse del ordenamiento relativo a datos de carácter personal, infraestructuras críticas o cualquier otro que establezca requisitos sobre la seguridad de los sistemas.

### 1.3. NOTIFICACIONES Y PUBLICACIONES ELECTRÓNICAS

21. El Esquema Nacional de Seguridad establece en su artículo 32 relativo a “Requerimientos técnicos de notificaciones y publicaciones electrónicas” que:
  - *Las notificaciones y publicaciones electrónicas de resoluciones y actos administrativos se realizarán de forma que cumplan, de acuerdo con lo establecido en el presente real decreto, las siguientes exigencias técnicas:*
    - *Aseguren la autenticidad del organismo que lo publique.*
    - *Aseguren la integridad de la información publicada.*



- *Dejen constancia de la fecha y hora de la puesta a disposición del interesado de la resolución o acto objeto de publicación o notificación, así como del acceso a su contenido.*
  - *Aseguren la autenticidad del destinatario de la publicación o notificación.*
22. Un sistema que preste un servicio de notificación o publicación electrónica deberá en primer lugar disponer de la valoración en materia de seguridad de la información que notifica o publicita. Típicamente, la valoración de la información establece los niveles en materia de confidencialidad, integridad, autenticidad y trazabilidad.
  23. El servicio de notificación o publicación hace propias dichas valoraciones, y añade los requisitos de disponibilidad que determine el Responsable del Servicio.
  24. La categoría del sistema vendrá expresada en función del máximo de los niveles en cada dimensión de los tipos de información gestionados y los servicios prestados.

## 2. CRITERIOS DE VALORACIÓN

25. Habitualmente se procede a la valoración individualizada de los distintos tipos de información y servicios en el ámbito de aplicación, considerando las dimensiones relevantes para cada uno de ellos.
26. Sin embargo, la valoración individual de cada información manejada y cada servicio prestado puede no ser la forma más efectiva de trabajar y puede dar lugar a escenarios más heterogéneos de lo necesario, tanto dentro de una misma entidad, como en sistemas de intercambio de información o prestación de servicios. Por ello se recomienda en primer lugar proceder a la valoración de los activos esenciales que sin duda van a exigir las valoraciones más restrictivas en las dimensiones de seguridad y que determinarán con ello la categoría del sistema.
27. Esta guía incluye criterios que pueden resultar de aplicación a una o varias dimensiones, tanto de tipos de información como de servicios.
28. Cada criterio de valoración es codificado para facilitar su referencia cuando se justifiquen las decisiones de valoración.

### 2.1. CRITERIOS COMUNES APLICABLES A TODAS LAS DIMENSIONES

29. Se establecen criterios que son de aplicación a todas las dimensiones de seguridad (seleccionando un nivel BAJO, MEDIO o ALTO de acuerdo al ENS), tanto de tipos de información como de servicios, considerando las consecuencias de un impacto negativo sobre la seguridad de la información y de los servicios, atendiendo, conforme al artículo 43 del Real Decreto 3/2010, a su repercusión en la capacidad de la organización para el logro de sus objetivos,

la protección de sus activos, el cumplimiento de sus obligaciones de servicio, el respeto de la legalidad y los derechos de los ciudadanos<sup>3</sup>.

30. Los criterios de impacto considerados son los siguientes:

- Disposición legal: Existencia de una disposición legal o administrativa que condicione el nivel de la dimensión.
- Perjuicio directo: Existencia de un perjuicio directo para el ciudadano.
- Incumplimiento de una norma: Implica el incumplimiento de una norma (legal, regulatoria, contractual o interna).
- Pérdidas económicas: Implica pérdidas económicas para la entidad.
- Reputación: Implica daño reputacional para la entidad.
- Protestas: Previsión de que pueda desembocar en protestas.
- Delitos: Facilitaría la comisión de delitos o dificultaría su investigación.

---

<sup>3</sup> En las tablas siguientes la expresión "N/A" indica que la dimensión no está adscrita a ningún nivel.

**CRITERIOS COMUNES APLICABLES A TODAS LAS DIMENSIONES DE TIPOS DE INFORMACIÓN Y SERVICIOS**

		No Adscrito (N/A)	BAJO	MEDIO	ALTO
<b>Disposición legal o administrativa</b>		COM.DIS.N No existe ninguna disposición legal que condicione su nivel.	COM.DIS.B Por disposición legal o administrativa: ley, decreto, orden, reglamento...	COM.DIS.M Por disposición legal o administrativa: ley, decreto, orden, reglamento...	COM.DIS.A Por disposición legal o administrativa: ley, decreto, orden, reglamento...
<b>Perjuicio Directo al ciudadano</b>		COM.PER.N No supone ningún perjuicio directo al ciudadano	COM.PER.B Algún perjuicio al ciudadano	COM.PER.M Daño importante, aunque subsanable al ciudadano	COM.PER.A Grave daño, de difícil o imposible reparación al ciudadano
<b>Incumplimiento de una Norma</b>	<b>Legal</b>	COM.LEG.N No implica incumplimiento de una norma jurídica	COM.LEG.B Incumplimiento formal leve de una norma jurídica, de carácter subsanable	COM.LEG.M Incumplimiento material de una norma jurídica, o incumplimiento formal no subsanable	COM.LEG.A Incumplimiento grave de una norma jurídica
	<b>Regulatoria</b>	COM.REG.N No implica incumplimiento de normativa de un regulador	COM.REG.B Implica incumplimiento de normativa de un regulador	COM.REG.M Implica sanción significativa de un regulador	COM.REG.A Implica sanción grave de un regulador y/o pérdida de licencia de operar
	<b>Contractual</b>	COM.CON.N No implica incumplimiento de una obligación contractual	COM.CON.B Incumplimiento leve de una obligación contractual	COM.CON.M Incumplimiento material o formal de una obligación contractual	COM.CON.A Incumplimiento grave de una obligación contractual
	<b>Interna</b>	COM.INT.N No implica incumplimiento de normativa interna	COM.INT.B Incumplimiento leve de una norma interna	COM.INT.M Incumplimiento material o formal de una norma interna	COM.INT.A Incumplimiento grave de una norma interna

<b>CRITERIOS COMUNES APLICABLES A TODAS LAS DIMENSIONES DE TIPOS DE INFORMACIÓN Y SERVICIOS</b>				
	<b>No Adscrito (N/A)</b>	<b>BAJO</b>	<b>MEDIO</b>	<b>ALTO</b>
<b>Pérdidas económicas</b>	<b>COM.ECO.N</b> No implica pérdidas económicas	<b>COM.ECO.B</b> Pérdidas económicas apreciables (inferior a un 4% del presupuesto anual de la organización)	<b>COM.ECO.M</b> Pérdidas económicas importantes (igual o superior a un 4% e inferior a un 10% del presupuesto anual de la organización)	<b>COM.ECO.A</b> Pérdidas económicas o alteraciones financieras significativas (igual o superior a un 10% del presupuesto anual de la organización)
<b>Reputación</b>	<b>COM.REP.N</b> No implica daño reputacional	<b>COM.REP.B</b> Daño reputacional apreciable con los ciudadanos o con otras organizaciones	<b>COM.REP.M</b> Daño reputacional importante con los ciudadanos o con otras organizaciones	<b>COM.REP.A</b> Daño reputacional grave con los ciudadanos o con otras organizaciones
<b>Protestas</b>	<b>COM.PRO.N</b> No se prevé que pueda desembocar en protestas.	<b>COM.PRO.B</b> Múltiples protestas individuales.	<b>COM.PRO.M</b> Protestas públicas (alteración del orden público)	<b>COM.PRO.A</b> Protestas masivas (alteración seria del orden público)
<b>Delitos</b>	<b>COM.DEL.N</b> No facilitaría la comisión de delitos ni dificultaría su investigación.	<b>COM.DEL.B</b> Favorecería la comisión de delitos	<b>COM.DEL.M</b> Favorecería significativamente la comisión de delitos o dificultaría su investigación.	<b>COM.DEL.A</b> Incitaría a la comisión de delitos, constituiría en sí un delito, o dificultaría enormemente su investigación.

Tabla 1. Criterios comunes aplicables a todas las Dimensiones de Tipos de Información y Servicios

## 2.2. CRITERIOS PARA TIPOS DE INFORMACIÓN CON DATOS DE CARÁCTER PERSONAL

31. Cuando el sistema tenga por objeto el tratamiento de datos personales se tendrá en cuenta lo previsto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y su normativa de desarrollo.
32. A partir del 25 de mayo de 2018, cuando el sistema tenga por objeto el tratamiento de datos personales, se tendrá en cuenta el 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, así como la normativa nacional que en su momento complementa lo dispuesto en dicha norma europea y por el que se deroga la Directiva 95/46/CE.

33. De acuerdo con dicha regulación, el responsable del tratamiento debe adoptar políticas internas y aplicar medidas que cumplan en particular los principios de protección de datos desde el diseño y por defecto.
34. La Agencia Española de Protección de Datos señala en su nota “El impacto del reglamento general de protección de datos sobre la actividad de las administraciones públicas” lo siguiente:
  - La *“necesidad de hacer un análisis de riesgo para los derechos y libertades de los ciudadanos de todos los tratamientos de datos que se desarrollen. El RGPD hace depender la aplicación de todas las medidas de cumplimiento que prevé para responsables y encargados del nivel y tipo de riesgo que cada tratamiento implique para los derechos y libertades de los afectados. Por ello, todo tratamiento, tanto los ya existentes como los que se pretenda iniciar, deben ser objeto de un análisis de riesgos. Los responsables y los encargados del tratamiento deberán realizar un análisis de riesgo para los derechos y libertades de los ciudadanos”*.
  - *“La determinación de las medidas de cumplimiento (entre ellas las de seguridad) dependerán del nivel y tipo de riesgo que cada tratamiento implique para los derechos y libertades de los afectados”*.
  - *“En el caso de las AAPP, la aplicación de las medidas de seguridad estará marcada por los criterios establecidos en el Esquema Nacional de Seguridad”*.
35. Es función del Responsable de la Seguridad determinar el conjunto de medidas requerido, uniendo los que se requieren por una y otra norma, e imponiendo la exigencia superior.
36. Si bien será la Agencia Española de Protección de Datos la que establezca reglamentariamente los criterios a emplear, en este apartado se incluyen algunos a título orientativo para facilitar la labor de los Responsables de la Información y de los Servicios (o incluso del de la Seguridad si va a presentar una propuesta a los anteriores), de forma que permitan determinar la seguridad de los sistemas que intervienen en las actividades de tratamiento de datos de carácter personal, en función de dos criterios:
  - El tipo de datos personales incluidos en los tipos de información identificados.
  - Determinadas características de las operaciones de tratamiento, como son:
    - Cantidad considerable de datos personales.
    - Importante riesgo para los derechos y libertades de los interesados.
    - Evaluación sistemática y exhaustiva de aspectos personales.
    - Control de zonas de acceso público a gran escala.

37. Los niveles obtenidos aplicando estos criterios son orientativos. Deberá tenerse en cuenta el resultado del análisis de riesgos para los derechos y libertades de los afectados, pudiendo en todo caso adoptarse medidas de seguridad adicionales, así como complementarlas con otros controles de naturaleza jurídica relacionados con el cumplimiento normativo.
38. El nivel determinado por el criterio de la siguiente tabla será de aplicación a las cuatro dimensiones de seguridad relacionadas con el tipo de información (confidencialidad, integridad, autenticidad, trazabilidad).
39. Para su valoración se analizarán los tipos de información resultantes de la operación de tratamiento de la que se esté realizando la evaluación de impacto en la privacidad o el análisis de riesgo.

CRITERIOS PARA TIPOS DE INFORMACIÓN CON DATOS PERSONALES EN FUNCIÓN DEL TIPO		
BAJO	MEDIO	ALTO
<p><b>PRI.TIP.B</b></p> <p>Datos de carácter personal con carácter general.</p>	<p><b>PRI.TIP.M</b></p> <p>Incluye datos de carácter personal:</p> <ul style="list-style-type: none"> <li>a) Relativos a la comisión de infracciones administrativas.</li> <li>b) Aquellos cuyo funcionamiento se rija por el artículo 29 de L.O. 15/1999, de 13 de diciembre.</li> <li>c) Aquellos de los que sean responsables Administraciones tributarias y se relacionen con el ejercicio de sus potestades tributarias.</li> <li>d) Aquéllos de los que sean responsables las entidades financieras para finalidades relacionadas con la prestación de servicios financieros.</li> <li>e) Aquéllos de los que sean responsables las Entidades Gestoras y Servicios Comunes de la Seguridad Social y se relacionen con el ejercicio de sus competencias. De igual modo, aquellos de los que sean responsables las mutuas de accidentes de trabajo y enfermedades profesionales de la Seguridad Social.</li> <li>f) Aquéllos que contengan un conjunto de datos de carácter personal que ofrezcan una definición de las características o de la personalidad de los ciudadanos y que permitan evaluar determinados aspectos de la personalidad o del comportamiento de los mismos.</li> </ul> <p>Datos personales que, por su naturaleza, son particularmente sensibles en relación con los derechos y libertades fundamentales, incluidos:</p> <ul style="list-style-type: none"> <li>• Origen étnico o racial (RGPD, art. 9).</li> <li>• Opiniones políticas (RGPD, art. 9).</li> <li>• Convicciones religiosas o filosóficas (RGPD, art. 9).</li> <li>• Afiliación sindical (RGPD, art. 9).</li> <li>• Datos genéticos (RGPD, art. 9).</li> <li>• Datos biométricos dirigidos a identificar de manera unívoca a una persona física (RGPD, art. 9).</li> <li>• Datos relativos a salud (RGPD, art. 9).</li> <li>• Datos relativos a la vida sexual u orientaciones sexuales (RGPD, art. 9).</li> <li>• Condenas e infracciones penales (RGPD, art. 10).</li> </ul>	

Tabla 2. Criterios para Tipos de Información con Datos Personales en función del tipo.

CRITERIOS PARA TIPOS DE INFORMACIÓN CON DATOS PERSONALES EN FUNCIÓN DEL TRATAMIENTO				
	N/A	BAJO	MEDIO	ALTO
<b>Cantidad considerable de datos personales</b>			<b>PRI.CAN.M</b> Operaciones de tratamiento a gran escala que persiguen tratar una cantidad considerable de datos personales a nivel regional, nacional o supranacional y que podrían afectar a un gran número de interesados y entrañen probablemente un alto riesgo, por ejemplo, debido a su sensibilidad, cuando, en función del nivel de conocimientos técnicos alcanzado, se haya utilizado una nueva tecnología a gran escala (RGPD, 91)	
<b>Importante riesgo para los derechos y libertades de los interesados</b>			<b>PRI.DER.M</b> Operación de tratamiento que entraña un alto riesgo para los derechos y libertades de los interesados, en particular cuando esta operación hace más difícil para los interesados el ejercicio de sus derechos (RGPD, 91)	
<b>Evaluación sistemática y exhaustiva de aspectos personales</b>			<b>PRI.ASP.M</b> Operación de tratamiento para adoptar decisiones relativas a personas físicas concretas a raíz de una evaluación sistemática y exhaustiva de aspectos personales propios de personas físicas, basada en la elaboración de perfiles de dichos datos o a raíz del tratamiento de categorías especiales de datos personales, datos biométricos o datos sobre condenas e infracciones penales o medidas de seguridad conexas (RGPD, 91)	
<b>Control de zonas de acceso público a gran escala</b>			<b>PRI.ACC.M</b> Operaciones de control de zonas de acceso público a gran escala, en particular cuando se utilicen dispositivos optoelectrónicos (RGPD, 91)	

Tabla 3. Criterios para tipos de información con datos personales en función del tratamiento.



## 2.3. CRITERIOS PARA LA DISPONIBILIDAD DE LOS SERVICIOS

### 2.3.1. PERIODOS CRÍTICOS

40. Los requisitos de disponibilidad pueden variar a lo largo del tiempo. Determinados servicios pueden tener una frecuencia de utilización heterogénea en el tiempo.
41. Hay servicios que son críticos en ciertos días del mes o del año, mientras que el resto del tiempo es menos importante. Los responsables deben ajustar las medidas de seguridad a la criticidad en cada momento. Por ejemplo, pueden contratarse servicios alternativos durante los periodos críticos, o elevar el nivel de servicio (SLA<sup>4</sup>) del Acuerdo requerido a proveedores.
42. Los pasos a seguir son los siguientes:
  - El Responsable del Servicio determina los periodos en los que se aplica cada nivel de seguridad (periodos críticos).
  - El Responsable de la Seguridad ajustará la valoración del sistema y determinará las medidas necesarias en cada periodo crítico.
  - El Responsable de la Seguridad velará porque el sistema se ajuste como mínimo a las medidas determinadas en cada periodo crítico, sin perjuicio de que las medidas de seguridad se prolonguen más allá del periodo exigido por razones de conveniencia operativa o de optimización de recursos.

### 2.3.2. RTO (TIEMPO DE RECUPERACIÓN OBJETIVO)

43. Uno de los criterios que son útiles para determinar los requisitos de disponibilidad de un servicio es el establecimiento de un tiempo de recuperación objetivo o tiempo de interrupción de referencia, que a menudo se conoce como RTO, y mide el tiempo máximo que el servicio puede permanecer interrumpido.
44. Antes de que se alcance el tiempo máximo establecido por el RTO<sup>5</sup> la organización deberá haber alcanzado los niveles mínimos de servicio (MBCO<sup>6</sup>) que deberá haber sido establecido por el Responsable del Servicio.
45. La valoración de la disponibilidad mide las consecuencias en caso de que ese tiempo se supere; es decir, que se quede por debajo del nivel mínimo de servicio por un periodo superior al RTO establecido.

---

<sup>4</sup> Service Level Agreement (en español, ANS)

<sup>5</sup> Recovery Time Objective (en español, TRO).

<sup>6</sup> Nivel mínimo de los servicios y/o productos que es aceptable para la organización para conseguir sus objetivos durante una disrupción

46. Los requisitos de seguridad son sensibles al RTO, pues un RTO muy corto (minutos u horas) supone una gran presión sobre la organización para garantizar su cumplimiento, mientras que un RTO largo (días) deja cierto margen a la improvisación.
47. La siguiente tabla puede usarse como referencia.

RTO	< 4 horas	4 horas -1día	1día – 5días	> 5días
nivel	Alto	Medio	Bajo	No Adscrito

Tabla 4. Plazos para la determinación de la disponibilidad de los servicios

4h = 4 horas

1d = 1 día = 24 horas

5d = 5 días (1 semana laboral)

CRITERIOS PARA LA DISPONIBILIDAD DE SERVICIOS				
	No Adscrito (N/A)	BAJO	MEDIO	ALTO
<b>RTO – Tiempo Objetivo de Recuperación</b>	DIS.RTO.N La restauración de los niveles mínimos de servicio puede realizarse en un plazo superior a 5 días (RTO)	DIS.RTO.B La restauración de los niveles mínimos de servicio debe realizarse en un plazo máximo de 5 días (RTO)	DIS.RTO.M La restauración de los niveles mínimos de servicio debe realizarse en un plazo máximo de 1 día (RTO)	DIS.RTO.A La restauración de los niveles mínimos de servicio debe realizarse en un plazo máximo de 4 horas (RTO)

Tabla 5. Criterios de determinación de la disponibilidad de los servicios

## 2.4. CRITERIOS ESPECÍFICOS

48. Para facilitar la labor de los diferentes organismos en la valoración de sus sistemas cuando estos manejan el mismo o similar tipo de información y de servicios, el Centro Criptológico Nacional tiene prevista la elaboración de anexos específicos que ofrezcan propuestas de valoración de las dimensiones de seguridad de los diferentes tipos de información y servicios habituales en determinadas organizaciones, sectores, colectivos, etc.
49. Como anexos a esta guía está previsto la elaboración de criterios para Universidades, Entidades Locales y en el futuro completarse con los correspondientes a otros colectivos que se determinen.

## 2.5. CRITERIOS ESPECÍFICOS PARA OPERADORES CRÍTICOS DEL SECTOR PÚBLICO

50. Los tipos de información identificados pueden contener información sensible para la seguridad de los servicios esenciales para la sociedad prestados por los operadores críticos, incluyendo información relacionada con el Plan de

- Seguridad del Operador o con los Planes de Protección Específicos de las infraestructuras críticas.
51. Así mismo, los servicios identificados para los distintos sistemas pueden ser utilizados para la prestación de esos servicios esenciales para la sociedad.
  52. El sistema categorizado respecto al ENS puede por ello ser utilizado por una infraestructura crítica, contribuyendo de forma más o menos significativa a la prestación de un servicio esencial para la sociedad.
  53. La protección de infraestructuras críticas tiene su propia legislación (LPIC<sup>7</sup>). De acuerdo con dicha regulación, los operadores designados críticos deben nombrar un Responsable de Seguridad y Enlace, y por cada infraestructura designada como crítica, un Delegado de Seguridad.
  54. Cuando en una entidad son de aplicación ambas normativas (ENS, LPIC) se debe determinar el conjunto de medidas de seguridad aplicables, estando previsto el desarrollo de una guía CCN-STIC específica que lo contemple.
  55. Será la Secretaria de Estado de Seguridad a través del Centro Nacional de Protección de Infraestructuras Críticas (CNPIC) la que establezca reglamentariamente los criterios a emplear para la protección de los servicios esenciales de las infraestructuras designadas como críticas en los correspondientes planes estratégicos sectoriales.
  56. La aplicación de dichos criterios podrá exigir la revisión de las medidas de seguridad a aplicar o incluso la adopción de medidas adicionales que pueda requerir la legislación específica o que hayan sido acordadas en la Comisión Nacional para la Protección de las Infraestructuras Críticas. Entre otras medidas, podrá requerir la clasificación legal de la información, de acuerdo a la Ley de Secretos Oficiales<sup>8</sup> y por tanto la necesaria acreditación de los sistemas clasificados que la manejan.

### 3. TIPOS DE INFORMACIÓN

#### 3.1. IDENTIFICACIÓN

57. Aunque información es cualquier conjunto de datos que tienen significado, el Esquema Nacional de Seguridad se limita a valorar los servicios de aquellas entidades que estén sometidos a la Ley 39/2015, de 1 de octubre, Procedimiento Administrativo Común de las Administraciones Públicas y Ley 40/2015, de 1 de octubre, Régimen Jurídico del Sector Público. Consecuentemente, los tipos de información a valorar serán los utilizados por los servicios dentro del ámbito de aplicación. Por ejemplo, datos médicos, fiscales, administrativos, contrataciones, resoluciones, notificaciones, etc. En general, cabe esperar que estos tipos de información estén identificados en algún tipo de ordenamiento general o particular de la entidad, lo que les

---

<sup>7</sup> Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas

<sup>8</sup> Ley 9/1998, de 5 de abril, sobre secretos oficiales

- confiere entidad propia e implica unos deberes del sector público respecto del tratamiento de dicho tipo de información.
58. No se valorarán directamente datos auxiliares que no son objeto directo del proceso administrativo y sólo aparecen como instrumentales para la prestación de los servicios. Por ejemplo, servicios de directorio, claves de acceso, etc.
  59. Para cada tipo de información, se debe determinar:
    - Su nombre, que la identifica unívocamente.
    - Su responsable, que establece sus requisitos de seguridad.
    - Otras características que se consideren relevantes a efectos operacionales, de asociación de vulnerabilidades, de estimación de riesgos o de auditoría.
  60. La determinación de los tipos de información y la figura del responsable vendrán determinadas en la Política de Seguridad o, en su defecto, la Política de Seguridad establecerá el marco para su identificación y el procedimiento de designación de la persona responsable.

## 3.2. VALORACIÓN

61. La valoración de la información la determina el responsable de la misma teniendo en cuenta su naturaleza y la normativa que pudiera serle de aplicación. Esta valoración requiere un conocimiento legal de la materia de que se trate.
62. La información suele imponer requisitos relevantes en las dimensiones de **confidencialidad, integridad, autenticidad y trazabilidad**. No suele haber requisitos relevantes en la dimensión de **disponibilidad**, considerándose en los servicios que gestionan esa información.
63. Cuando una dimensión no condiciona las medidas de seguridad, en el apartado de valoración se indicará como **“NO ADSCRITA”** o **“N/A”**.
64. A continuación, se describen criterios para establecer un valor en cada dimensión. Estos criterios son de carácter general, sirviendo de guía, pudiendo la política de seguridad concretar casos particulares de la entidad y que el responsable de la información fundamente la adscripción que determine como apropiada.

### 3.2.1. CONFIDENCIALIDAD

65. Son de aplicación los Criterios Generales del apartado 2.1, considerando las consecuencias que tendría su **revelación a personas no autorizadas o que no necesitan conocer la información**.
66. Son de aplicación los Criterios para Datos de Carácter Personal, detallados en el apartado 2.2.

67. Serán de aplicación los Criterios específicos determinados para ámbitos concretos que pudieran publicarse como anexos de esta guía o por la política de seguridad de la organización, conforme al apartado 49.
68. No estará adscrita (N/A) la valoración a la dimensión:
  - cuando se trata de información de carácter público, accesible por cualquier persona.

### 3.2.2. INTEGRIDAD

69. Son de aplicación los Criterios Generales del apartado 2.1, considerando las consecuencias que tendría su **modificación por alguien que no está autorizado a modificar la información.**
70. Son de aplicación los Criterios para Datos de Carácter Personal, detallados en el apartado 2.
71. Serán de aplicación los Criterios específicos determinados para ámbitos concretos que pudieran publicarse como anexos de esta guía o por la política de seguridad de la organización, conforme al apartado 49.
72. No estará adscrita (N/A) la valoración a la dimensión:
  - cuando los errores en su contenido carecen de consecuencias.
  - cuando los errores en su contenido son fácil y rápidamente reparables.

### 3.2.3. AUTENTICIDAD

73. Son de aplicación los Criterios Generales del apartado 2.1, considerando las consecuencias que tendría **el hecho de que la información no fuera auténtica.**
74. Son de aplicación los Criterios para Datos de Carácter Personal, detallados en el apartado 2.
75. Serán de aplicación los Criterios específicos determinados para ámbitos concretos que pudieran publicarse como anexos de esta guía o por la política de seguridad de la organización, conforme al apartado 49.
76. No estará adscrita (N/A) la valoración a la dimensión:
  - cuando el origen es irrelevante o ampliamente conocido por otros medios.
  - cuando el destinatario es irrelevante, por ejemplo, por tratarse de información de difusión anónima.

### 3.2.4. TRAZABILIDAD

77. Son de aplicación los Criterios Generales del apartado 2.1, considerando las consecuencias que tendría el **no poder comprobar a posteriori quién ha accedido a, o modificado, una cierta información.**
78. Son de aplicación los Criterios para Datos de Carácter Personal, detallados en el apartado 2.2.

79. Serán de aplicación los criterios específicos determinados para ámbitos concretos que pudieran publicarse como anexos de esta guía o por la política de seguridad de la organización, conforme al apartado 49.
80. No estará adscrita (N/A) la valoración a la dimensión:
  - cuando no se pueden producir errores de importancia, o son fácilmente reparables por otros medios.
  - cuando no se pueden perpetrar delitos relevantes, o su investigación es fácilmente realizable por otros medios.

## 4. SERVICIOS

### 4.1. IDENTIFICACIÓN

81. A los efectos de esta guía, se entiende por servicio aquéllos prestados por los sistemas de información de la entidad que estén sometidos a la Ley 39/2015, de 1 de octubre, Procedimiento Administrativo Común de las Administraciones Públicas y Ley 40/2015, de 1 de octubre, Régimen Jurídico del Sector Público.
82. Algunos de estos servicios pueden estar identificados en algún tipo de ordenamiento general, mientras que otros serán particulares de la entidad. En cualquier caso, los servicios aquí contemplados tienen identidad propia con independencia de los medios que se empleen para su prestación, asumiendo la entidad que los presta unas obligaciones con respecto a los mismos.
83. No se valoran servicios internos o auxiliares tales como correo electrónico, ficheros en red, servicios de directorio, de impresión, de copias de respaldo, etc.
84. Para cada servicio se debe determinar:
  - Su nombre, que lo identifica unívocamente.
  - Su responsable, que establece sus requisitos de seguridad.
  - Otras características que se consideren relevantes a efectos operacionales, de asociación de vulnerabilidades, de estimación de riesgos o de auditoría.
85. La determinación de los servicios que se prestan y la figura del responsable vendrán determinadas en la Política de Seguridad o, en su defecto, la Política de Seguridad establecerá el marco para su identificación y el procedimiento de designación de la persona responsable.

### 4.2. VALORACIÓN

86. La valoración de un servicio la determina el responsable del mismo teniendo en cuenta la naturaleza del servicio y la normativa que pudiera serle de aplicación. Esta valoración requiere un conocimiento legal de la materia de que se trate.
87. Habitualmente los servicios establecen requisitos relevantes en términos de **disponibilidad**. También es habitual que los demás requisitos de seguridad sobre los servicios deriven de los de la información que se utiliza.

88. El nivel de seguridad requerido en el aspecto de disponibilidad se establecerá en función de las consecuencias que tendría el que una persona autorizada no pudiera usar el servicio cuando lo necesita.
89. Los requisitos de **confidencialidad, integridad, autenticidad y trazabilidad** sobre un servicio derivan de la información que maneja. Incidentes en la autenticación o autorización del servicio pueden implicar incidentes de confidencialidad de la información gestionada. En el caso de la integridad, incluye la posibilidad de que la información quede incompleta o inexacta porque el servicio no se complete adecuadamente. Un error en la autenticación puede derivar en información no auténtica o en la incorrecta trazabilidad de los cambios sobre la misma.
90. Cuando una dimensión no condiciona las medidas de seguridad, en el apartado de valoración se indicará como **“NO ADSCRITA”** o **“N/A”**.
91. A continuación, se describen criterios para establecer un valor en la dimensión relevante en un servicio, la disponibilidad. Estos criterios son de carácter general, sirviendo de guía, pudiendo la política de seguridad concretar casos particulares de la entidad, y que el responsable de la información fundamente la adscripción que determine como apropiada.

#### 4.2.1. DISPONIBILIDAD

92. Son de aplicación los Criterios Generales del apartado 2.1, considerando las consecuencias que tendría **que una persona o sistema interconectado autorizado no pudiera usar el servicio cuando lo necesita dentro del periodo de servicio establecido y anunciado por la organización.**
93. Son de aplicación los Criterios para Disponibilidad, detallados en el apartado 2.3.
94. Serán de aplicación los criterios específicos determinados para ámbitos concretos que pudieran publicarse como anexos de esta guía o por la política de seguridad de la organización, conforme al apartado 2.4.
95. No estará adscrita (N/A) la valoración a la dimensión cuando apenas tenga consecuencias adversas la restauración de los niveles mínimos de servicio en un plazo superior a 5 días (RTO).

## 5. DETERMINACIÓN DE LOS NIVELES Y CATEGORÍA DEL SISTEMA

### 5.1. VALORACIÓN DE LAS DIMENSIONES DE LOS ACTIVOS ESENCIALES

96. Por cada activo esencial, sea de tipo información o de tipo servicio, se solicita la valoración de su nivel (bajo, medio o alto) en cada dimensión de seguridad (ver Anexo I del ENS):

- Para Servicios: Disponibilidad (D).
- Para Tipos de Información: C (Confidencialidad), I (Integridad), A (Autenticidad) y T (Trazabilidad).

97. Cuando un sistema maneje diferentes tipos de información y preste diferentes servicios, el nivel del sistema en cada dimensión será el mayor de los establecidos para cada tipo de información y cada servicio.

Denominación del Activo esencial	tipo <sup>8</sup>	C <sup>9</sup>	I	D	A	T
Valor máximo del nivel registrado en las dimensiones de seguridad						

Figura 1. Categorización de un Sistema a partir de los Niveles en cada Dimensión de sus Activos Esenciales.

98. La categoría, en materia de seguridad, modula el equilibrio entre la importancia de la información que maneja, los servicios que presta y el esfuerzo de seguridad requerido, en función de los riesgos a los que está expuesto, bajo el criterio del principio de proporcionalidad.

99. Los niveles de seguridad determinados para la información se imputarán a todos los activos que manejen la información correspondiente. Los niveles de seguridad determinados para los servicios se imputarán a todos los activos que concurren para prestar el servicio correspondiente.

### 5.2. DETERMINACIÓN DE SUBSISTEMAS

100. Puede darse la circunstancia de que diferentes activos del mismo sistema estén sometidos a requisitos diferentes, en virtud de que atiendan a distintos tipos de información o servicios. Esto llevará a fragmentar un sistema de información en varios subsistemas o a asumir para todo el conjunto el máximo nivel al que están sometidos sus dimensiones de seguridad.

<sup>8</sup> Tipo: Información o Servicio.

<sup>9</sup> C (Confidencialidad), I (integridad), D (Disponibilidad), A (Autenticidad) y T (Trazabilidad). Por cada dimensión de seguridad se elegirá entre los niveles Bajo, Medio, Alto o N/A (No adscrito a ningún nivel).



101. Conviene que el conjunto de medidas de seguridad adoptadas sea lo más homogéneo posible, con el menor número de activos singulares a los que aplicar medidas diferentes. La principal razón para no tener un criterio homogéneo suele ser económica, cuando algunas medidas de protección son de elevado coste y hay que aplicarlas en el menor número de activos posible. Como ejemplos de medidas que conviene acotar podemos citar equipos de cifrado, equipamiento alternativo en caso de exigir alta disponibilidad, etc.
102. La categoría de cada subsistema se determina atendiendo a lo establecido en el Anexo I del RD 3/2010.
103. La aplicabilidad de las medidas descritas en el Anexo II del RD 3/2010 se determinará para cada subsistema.
104. Un sistema de información cumple con el RD 3/2010 cuando todos sus subsistemas cumplen, de acuerdo con los niveles de seguridad para cada dimensión y la categoría que corresponde en cada caso.
105. La categoría del sistema (básica, media o alta) se determinará a partir de las dimensiones conforme al apartado anterior, o bien, cuando se hayan definido subsistemas, a la mayor categoría de los subsistemas que lo integran en el caso de que se decida considerarlos en un único sistema.

Subsistemas	Categoría <sup>10</sup>
Subsistema 1 ...	
Subsistema 2 ...	
Valor máximo de la categoría de los subsistemas	

Figura 1. Categorización de un Sistema a partir de sus Subsistemas.

### 5.3. FORMULACIÓN DE LA CATEGORÍA DE UN SISTEMA

106. La forma de representar la categoría de un sistema será la siguiente, explicitando el nivel en cada dimensión para ayudar a determinar las medidas de seguridad exactas que han sido de aplicación:

CATEGORÍA (BÁSICA-MEDIA-ALTA): [C=(N/A-B-M-A), I= (N/A-B-M-A), D=(N/A-B-M-A), A=(N/A-B-M-A), T= (N/A-B-M-A)]

107. A continuación, se presentan las dimensiones de seguridad que se han asignado:

<sup>10</sup> Puede ser BÁSICA, MEDIA o ALTA.

Categoría que se ha asignado al/los sistema(s) de << Nombre de la entidad >> es:

**(Categoría): [ C(Nivel), I(Nivel), D(Nivel), A(Nivel), T(Nivel) ]**

Figura 2. Categorización de un Sistema junto a los Niveles en sus Dimensiones de Seguridad.

Ejemplos:

CATEGORÍA BÁSICA: [C(N/A), I(B), D(B), A(B), T(B)]

CATEGORÍA MEDIA: [C(N/A), I(B), D(B), A(M), T(B)]

CATEGORÍA ALTA: [C(M), I(B), D(A), A(M), T(B)]

#### 5.4. TERCERAS PARTES

108. Con carácter general, los requisitos de seguridad de otros sistemas que dependan de los servicios prestados por el sistema analizado, serán requisitos del sistema analizado.
109. Cuando un sistema utiliza sistemas de terceros para manejar información o para prestar servicios, la valoración propia (el nivel determinado para cada dimensión) de esos activos esenciales será impuesta como un mínimo aceptable al tercero que colabora. Esta valoración será formalmente comunicada al Responsable del Sistema y al Responsable de la Seguridad para que se ajuste al nivel en cada dimensión y, con ello, pueda determinarse el conjunto de medidas de seguridad mínimas exigibles o requeridas.
  - Los requisitos de este sistema se convierten en los requisitos de los sistemas utilizados.
110. Cuando un sistema maneja información de terceros o presta servicios a terceros, la valoración propia (el nivel en cada dimensión) de los tipos de información y los servicios será como mínimo la determinada por dicho tercero.
  - Los requisitos de otros sistemas que dependen de los servicios prestados por este sistema son requisitos de este sistema.
111. Cuando un sistema maneje datos de carácter personal cedidos por otros o ceda datos de carácter personal a otros, a las medidas de seguridad requeridas por el Esquema Nacional de Seguridad se añadirán las requeridas por la normativa de tratamiento de datos de carácter personal.
112. Cuando un sistema contribuya a la prestación de servicios esenciales de terceros o contenga información que pueda poner en riesgo la seguridad de esos servicios esenciales de terceros, deberá determinarse si a las medidas de seguridad requeridas por el Esquema Nacional de Seguridad deben añadirse medidas adicionales requeridas por las infraestructuras críticas.

## 5.5. DOCUMENTACIÓN

113. Es esencial que queden perfectamente documentadas todas las actividades relativas a la valoración de los sistemas:
- criterios seguidos y razonamientos aplicados, para lo que puede utilizarse la codificación de los criterios de valoración proporcionada en esta guía.
  - opiniones o consideraciones de terceros que se han considerado relevantes.
  - normas, leyes, reglamentos o prácticas sectoriales que sean de aplicación.
  - circunstancias particulares que puedan tener un impacto en la valoración, de forma permanente o coyuntural, incluyendo:
    - periodos críticos de prestación del servicio,
    - agregación de información o de servicios,
    - circunstancias especiales de prestación como situaciones de emergencia
    - revisiones por terceras partes, incluyendo auditoría.
114. Todas las decisiones deben estar debida y formalmente aprobadas y la documentación disponible a efectos de auditoría.
- El Responsable de cada Información aprueba la valoración de dicha información.
  - El Responsable de cada Servicio aprueba la valoración de dicho servicio.
  - El Responsable de la Seguridad determina y aprueba las medidas de seguridad que son de aplicación (**Declaración de Aplicabilidad**) en el sistema o en cada subsistema y las acciones organizativas y técnicas que se adoptan para sustanciar dichas medidas de seguridad.
  - Si se toman decisiones de suspensión parcial o total de un sistema, éstas vendrán aprobadas por el Responsable del Sistema y los responsables de los Servicios afectados por la suspensión.
  - Los Responsables de la Información y del Servicio deben aprobar asimismo el riesgo residual que conlleve la adopción de las medidas de seguridad correspondientes.
  - Por ultimo dichos sistemas serán objeto de una auditoría de acuerdo al Anexo III del ENS.

## 6. ANEXO A. GLOSARIO DE TÉRMINOS

### Apreciación del riesgo

Proceso global que comprende la identificación del riesgo, el análisis del riesgo y la evaluación del riesgo (Guía ISO 73:2009).

### Autenticidad

Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos. ENS.

### Comité STIC

Comisión que reúne a los responsables de seguridad TIC y toma decisiones de coordinación. Guía CCN-STIC 402.

### Confidencialidad

Propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados. ENS.

### Datos de carácter personal

Cualquier información concerniente a personas físicas identificadas o identificables. Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

Toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona. Reglamento (UE) 2016/679 (RGPD).

### Información

Caso concreto de un cierto tipo de información.

**Information.** An instance of an information type. FIPS 199.

### Integridad

Propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada. ENS.

### Política de seguridad

Conjunto de directrices plasmadas en documento escrito, que rigen la forma en que una organización gestiona y protege la información y los servicios que considera críticos. ENS.

### Responsable de la Información

Persona que tiene la potestad de establecer los requisitos de una información en materia de seguridad.

**Information Owner.** Official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal. CNSS Inst. 4009.

### Responsable de la Seguridad

Persona que tiene la potestad de determinar las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios.

The **Computer Security Program Manager** (and support staff) directs the organization's day-to-day management of its computer security program. This individual is also responsible for coordinating all security-related interactions among organizational elements involved in the computer security program as well as those external to the organization. NIST Special Publication 800-12.

**Information systems security manager (ISSM).** Individual responsible for a program, organization, system, or enclave's information assurance program. CNSS Inst. 4009.

### Responsable del Servicio

Persona que tiene la potestad de establecer los requisitos de un servicio en materia de seguridad.

### Responsable del Sistema

Persona que se encarga de la explotación del sistema de información.

**Information System Owner (or Program Manager).** Official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system. CNSS Inst. 4009, Adapted.

### Servicio

Función o prestación desempeñada por alguna entidad oficial destinada a cuidar intereses o satisfacer necesidades de los ciudadanos.

### Sistema de Información

Conjunto organizado de recursos para que la información se pueda recoger, almacenar, procesar o tratar, mantener, usar, compartir, distribuir, poner a disposición, presentar o transmitir. ENS.

**Information System.** A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. 44 U.S.C., Sec. 3502; OMB Circular A-130, Appendix III.

### Tipo de Información

Una categoría específica de información (por ejemplo, datos de carácter personal, médicos, financieros, investigaciones, contratos, información delicada, ...). Estos tipos los define una organización y, en algunos casos, vienen definidos por alguna normativa de carácter legal.

**Information type.** A specific category of information (e.g., privacy, medical, proprietary, financial, investigative, contractor sensitive, security management) defined by an organization or in some instances, by a specific law, Executive Order, directive, policy, or regulation. FIPS 199.

### **Trazabilidad**

Propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad. ENS.

## 7. ANEXO B. ABREVIATURAS

Siglas	Definición
<b>ANS</b>	Acuerdo de Nivel de Servicio (en inglés, SLA)
<b>ENS</b>	Esquema Nacional de Seguridad
<b>LOPD</b>	Ley 15/1999, de 13 de diciembre, de protección de datos de carácter personal.
<b>LPIC</b>	Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas.
<b>MAGERIT</b>	Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información
<b>MBCO</b>	Nivel mínimo de los servicios y/o productos que es aceptable para la organización para conseguir sus objetivos durante una interrupción.
<b>RGPD</b>	Reglamento (UE) 2016/679.
<b>RTO</b>	Recovery Time Objective (en español, TRO)
<b>SLA</b>	Service Level Agreement (en español, ANS)
<b>TRO</b>	Tiempo de recuperación objetivo (en inglés RTO)

## 8. ANEXO C. REFERENCIAS

- 2001/264/CE Decisión del Consejo de 19 de marzo de 2001 por la que se adoptan las normas de seguridad del Consejo.
- 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
- Ley 9/1998, de 5 de abril, sobre secretos oficiales
- Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal
- Real Decreto 3/2010 del 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica
- Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica
- Real Decreto 951/2015, de 23 de octubre, de modificación del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica
- Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el reglamento de protección de datos de carácter personal
- Real Decreto 421/2004, de 12 de marzo, por el que se regula el Centro Criptológico Nacional
- Instrucción técnica de seguridad de Conformidad con el Esquema Nacional de Seguridad por Resolución de 13 de octubre de 2016, del Secretario de Estado de Administraciones Públicas
- Instrucción Técnica de Seguridad de Informe del Estado de la Seguridad por Resolución de 7 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas
- Guía de seguridad de las TIC - (CCN-STIC-801)- Esquema Nacional de Seguridad: Roles y Funciones. Febrero 2011.
- Guía de seguridad de las TIC - (CCN-STIC-830) - Ámbito de aplicación del Esquema Nacional de Seguridad
- MAGERIT – versión 3. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Consejo Superior de Administración Electrónica, 2012.
- FIPS 199 Standards for Security Categorization of Federal Information and Information Systems. Feb. 2004.
- SP 800-60 Rev.1 Guide for Mapping Types of Information and Information Systems to Security Categories. Volume 1: Guide. Volume 2: Appendices. Aug 2008.