Guía de Seguridad de las TIC
CCN-STIC 803

ENS. Valoración de los sistemas

Junio 2025

Edita:
centro criptológico nacional

Fecha de Edición: junio de 2025

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

ÍNDICE

1. INTRODUCCIÓN

1. Esta guía establece unas pautas de carácter general que son aplicables a los sistemas de información de aquellas entidades de naturaleza pública o privada, que se encuentren comprendidos en el alcance del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (en adelante, ENS). Se espera que cada entidad las particularice para adaptarlas a su entorno singular.

2. El ENS 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 de seguridad (artículo 40) del sistema de información de que se trate. A su vez, la categoría de seguridad 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], trazabilidad [T], autenticidad [A], y disponibilidad [D].

4. El ENS establece tres categorías de seguridad para los sistemas de información: BÁSICA, MEDIA y ALTA, según el ANEXO I apartado 4:

   > *"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. Esta guía, de acuerdo con el apartado 5.2 del ANEXO I del ENS, recoge los criterios generales para la categorización de los sistemas de información.

1.1. SERVICIOS E INFORMACIÓN

6. Con carácter general, los servicios prestados por las entidades del ámbito de aplicación del ENS pueden ser finalistas e instrumentales. Se considera que un servicio es finalista cuando forma parte de las competencias que tiene atribuidas legal o estatutariamente la entidad de que se trate, siendo los servicios instrumentales aquellos que sirven de apoyo a la ejecución de los anteriores pero que, en sentido estricto, no constituyen competencias legales de la entidad.

7. Tanto los servicios como la información deben identificarse en un inventario mediante:

   - Nombre, que los identifique unívocamente.

- Persona responsable (Responsable(s) de la Información y de los Servicios), que valora sus requisitos de seguridad.
- Otras características que se consideren relevantes a efectos operacionales, de asociación de vulnerabilidades, de estimación de riesgos o de auditoría.

8. La determinación de los servicios prestados y la información tratada, así como la figura de su Responsable o Responsables vendrán determinadas en la Política de Seguridad o, en su defecto, establecerá el marco para su identificación y el procedimiento de designación de la(s) persona(s) responsable(s).

1.2. NECESIDAD DE VALORAR

9. Para la categorización de la seguridad del sistema, en primer lugar, se debe partir de la identificación de los servicios prestados por la entidad y la información que se gestiona en cada uno de ellos. En esta valoración se podrá tener en cuenta la distinción de los servicios finalistas de aquellos otros denominados instrumentales que sirven de apoyo para poder prestar los finalistas. Habiendo identificado previamente los **servicios finalistas** prestados por la entidad, sujetos al cumplimiento del ENS, así como aquellos otros **instrumentales** y la información[1] que tratan dichos servicios, conviene comenzar la valoración por los activos de tipo **información**, en este orden: *confidencialidad, integridad, trazabilidad, autenticidad*

10. Conviene seguir con los **servicios**, valorando para los mismos la *disponibilidad*. Los requisitos en materia de confidencialidad, integridad, trazabilidad y autenticidad suelen venir impuestos por los tipos de información que maneja cada servicio.

11. Un sistema asumirá, para cada dimensión, el valor máximo considerado para la misma en los distintos tipos de información manejados por los servicios prestados.

12. La categoría de seguridad de sistema se determina considerando el valor máximo de todas sus dimensiones para todos los servicios prestados incluidos en el alcance del ENS.

1.3. PROCEDIMIENTO DE VALORACIÓN

13. El Responsable de la Información será el encargado de inventariar la información dentro del alcance del ENS y el Responsable del Servicio de inventariar los servicios de la entidad dentro de dicho alcance. Para ello podrán contar con la ayuda del Responsable del Sistema, el Responsable de la Seguridad, el Delegado de Protección de Datos y el resto de las áreas de la entidad que se considere conveniente consultar.

[1] Dentro de la información se tendrán en cuenta los datos personales tratados que estarán identificados en el Registro de Actividades del Tratamiento de la entidad ya que, en función de su tipología, pueden afectar a las dimensiones de seguridad del ENS.

14. Opcionalmente, en función de lo establecido en la Política de Seguridad, podrá ser el Comité de Seguridad de la Información, apoyado por el resto de los órganos o departamentos de la entidad, el encargado de realizar el inventario de servicios e información.

15. Este inventario de servicios e información deberá quedar documentando e indicará también la definición de cada activo y el responsable directo de cada uno de ellos. La responsabilidad de la valoración de la información y de los servicios es exclusivamente del responsable de la información y del servicio, respectivamente, aunque puede ser propuesta por el Responsable del Sistema, por el Responsable de la Seguridad y aprobada posteriormente por el Responsable de la Información o del Servicio correspondiente, si éste la considera adecuada. Se deberá conservar el registro de las valoraciones realizadas. Naturalmente, la aprobación final de las valoraciones deberá realizarse en el seno del Comité de Seguridad de la Información, si existe.

16. La opinión del Responsable de la Seguridad y del Responsable del Sistema deben ser recabadas y consideradas en el proceso de valoración.

17. 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 encargará de aplicar el procedimiento descrito en el Anexo I del ENS, de acuerdo con los niveles máximos de cada dimensión de seguridad, obteniendo la categoría de seguridad del sistema.

18. La determinación de la categoría de seguridad 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, hay que 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.

2. CRITERIOS DE VALORACIÓN

19. Habitualmente, se procede a la valoración individualizada de los distintos tipos de información y servicios, dentro del ámbito de aplicación considerado, teniendo en cuenta las dimensiones relevantes para cada uno de ellos.

20. Se recomienda proceder, en primer lugar, a la valoración de los servicios finalistas, puesto que son los que van a exigir las valoraciones más restrictivas en las dimensiones de seguridad y que determinarán con ello la categoría del sistema.

21. Esta guía incluye criterios que pueden resultar de aplicación a una o varias dimensiones, ya se trate de información como de servicios.

22. 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

23. En los párrafos siguientes 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 40 del ENS , a su repercusión en la capacidad de la organización para el logro de sus objetivos, la protección de sus activos y garantizar el cumplimiento del ordenamiento jurídico.

    Así, se valorará el impacto sobre:

    - La capacidad de la organización para el logro de sus objetivos.
    - Sobre sus activos.
    - El cumplimiento de la normativa que le sea de aplicación, incluyendo el perjuicio sobre los derechos y libertades de las personas.

CRITERIOS COMUNES APLICABLES A TODAS LAS DIMENSIONES DE TIPOS DE INFORMACIÓN Y SERVICIOS				
	No aplicable (N/A)	**BAJO**	**MEDIO**	**ALTO**
		Perjuicio limitado	**Perjuicio grave**	**Perjuicio muy grave**
Capacidad de la entidad para lograr sus objetivos	No existe un impedimento.	Existe algún inconveniente leve para alcanzarlo, pero que es subsanable a corto plazo.	Existe una pérdida de la capacidad que es subsanable a medio plazo.	Existe una pérdida de la capacidad no subsanable a medio plazo.
Activos entidades	No existe perjuicio.	Existe un perjuicio leve y subsanable.	Existe un daño importante, aunque subsanable.	Existe un daño grave de difícil o imposible reparación
Cumplimiento de normativa	No implica un incumplimiento.	Incumplimiento leve de una regulación, de carácter subsanable.	Incumplimiento material de una regulación, no subsanable.	Incumplimiento formal y material de una regulación, no subsanable.

Tabla 1. Ejemplos de criterios comunes aplicables a todas las dimensiones de Tipos de Información y Servicios

2.2. CRITERIOS PARA LA VALORACIÓN DE LA DISPONIBILIDAD DE LOS SERVICIOS

2.2.1. PERIODOS CRÍTICOS

24. Determinados servicios pueden tener una frecuencia de utilización heterogénea, por lo que los requisitos de disponibilidad pueden variar a lo largo del tiempo.

25. Hay servicios que son críticos solamente ciertos días del mes o del año. 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[2]) requerido a proveedores.

26. Un proceso razonable que seguir sería el siguiente:

    - El Responsable del Servicio determina los periodos en los que se aplica cada nivel de seguridad con especial consideración a los periodos críticos.
    - El Responsable de la Seguridad ajustará la valoración de seguridad del sistema y determinará las medidas necesarias en cada uno de los periodos considerados.
    - El Responsable de la Seguridad velará por que la seguridad del sistema en cada periodo se garantice con las medidas de seguridad adecuadas.

2.2.2. RTO (TIEMPO DE RECUPERACIÓN OBJETIVO)

27. Uno de los criterios 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**, que señala el tiempo máximo que el servicio puede permanecer interrumpido.

28. Antes de que se alcance el tiempo máximo establecido por el RTO[3] la organización deberá haber alcanzado el nivel mínimo de servicio (MBCO[4]) que deberá haber sido establecido por el Responsable del Servicio.

29. 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.

30. Los requisitos de seguridad son sensibles al RTO. 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 de maniobra.

31. La siguiente tabla puede usarse como referencia.

IMPACTO	BAJO	MEDIO	ALTO
RTO (Tiempo de Recuperación del Servicio)	1 día < RTO < 5 días	4 horas < RTO < 1 día	< 4 horas

Tabla 2. Ejemplos de plazos para la determinación de la disponibilidad de los servicios.

3. VALORACIÓN DE LOS SERVICIOS E INFORMACIÓN

32. La información suele imponer requisitos relevantes en las dimensiones de **confidencialidad**, **integridad**, **trazabilidad** y **autenticidad**, mientras que los servicios establen requisitos relevantes en términos de **disponibilidad,** estableciéndose en

[2] Service Level Agreement (en español, ANS)
[3] Recovery Time Objective (en español, TRO).
[4] Nivel mínimo de los servicios y/o productos que es aceptable para la organización para conseguir sus objetivos durante una disrupción

función de las consecuencias que tendría la imposibilidad de acceder al servicio por persona o entidad autorizada cuando se le necesita.

33. Los requisitos de **confidencialidad**, **integridad**, **trazabilidad** y **autenticidad** 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.

34. A continuación, se describen algunos ejemplos de criterios para establecer un valor en cada dimensión. Estos criterios son de carácter general y orientativo, pudiendo la política de seguridad concretar casos particulares de la entidad y que el responsable de la información y/o del servicio fundamente la adscripción que determine como apropiada.

3.1. CONFIDENCIALIDAD

35. Son de aplicación los Criterios Generales del apartado 2.1, considerando las consecuencias que tendría su **revelación a personas no autorizadas**.

3.2. INTEGRIDAD

36. Son de aplicación los Criterios Generales del apartado 2.1, considerando las consecuencias que tendría su **modificación por alguien no autorizado a modificar la información.**

3.3. TRAZABILIDAD

37. 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**.

3.4. AUTENTICIDAD

38. Son de aplicación los Criterios Generales del apartado 2.1, considerando las consecuencias que tendría **el hecho de que la información no fuera auténtica**.

3.5. DISPONIBILIDAD

39. Son de aplicación los Criterios Generales del apartado 2.2, considerando las consecuencias que tendría que una persona o sistema interconectado autorizado **no pudiera usar el servicio** cuando lo necesita dentro del periodo de prestación de servicio establecido y anunciado por la organización.

3.6. VALORACIÓN DE LOS DATOS PERSONALES

40. Para el tratamiento de datos personales será de aplicación lo dispuesto en 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 (RGPD), además de lo preceptuado en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de datos y garantía de los derechos digitales (LOPDGDD) y, especialmente, lo dispuesto en su Disposición Adicional primera: medidas de seguridad en el ámbito del sector público, que prescribe:

> *"Disposición adicional primera. Medidas de seguridad en el ámbito del sector público.*
>
> *1. El Esquema Nacional de Seguridad incluirá las medidas que deban implantarse en caso de tratamiento de datos personales para evitar su pérdida, alteración o acceso no autorizado, adaptando los criterios de determinación del riesgo en el tratamiento de los datos a lo establecido en el artículo 32 del Reglamento (UE) 2016/679.*
>
> *2. Los responsables enumerados en el artículo 77.1 de esta ley orgánica deberán aplicar a los tratamientos de datos personales las medidas de seguridad que correspondan de las previstas en el Esquema Nacional de Seguridad, así como impulsar un grado de implementación de medidas equivalentes en las empresas o fundaciones vinculadas a los mismos sujetas al Derecho privado.*
>
> *En los casos en los que un tercero preste un servicio en régimen de concesión, encomienda de gestión o contrato, las medidas de seguridad se corresponderán con las de la Administración pública de origen y se ajustarán al Esquema Nacional de Seguridad."*

41. 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:

> *"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".

42. El artículo 2 del ENS además señala que:

"Cuando un sistema de información trate datos personales le será de aplicación lo dispuesto en 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 (Reglamento General de Protección de Datos) y en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, o, en su caso, la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales, el resto de normativa de aplicación, así como los criterios que se establezcan por la Agencia Española de Protección de Datos o en su ámbito competencial, por las autoridades autonómicas de protección de datos, sin perjuicio de los requisitos establecidos en el presente real decreto.

En estos supuestos, el responsable o el encargado del tratamiento, asesorado por el delegado de protección de datos, realizarán un análisis de riesgos conforme al artículo 24 del Reglamento General de Protección de Datos y, en los supuestos de su artículo 35, una evaluación de impacto en la protección de datos.

En todo caso, prevalecerán las medidas a implantar como consecuencia del análisis de riesgos y, en su caso, de la evaluación de impacto a los que se refiere el apartado anterior, en caso de resultar agravadas respecto de las previstas en el presente real decreto".

43. Por lo tanto, la valoración de los datos personales deberá atender al análisis de riesgos y/o evaluaciones de impacto en protección de datos que se realizan sobre los tratamientos identificados en el registro de actividades del tratamiento de la entidad.

3.7. CRITERIOS ESPECÍFICOS PERFILES CUMPLIMIENTO ESPECÍFICO

44. Para facilitar la valoración de diferentes tipos de organismos, tales como las Entidades Locales, las Universidades, servicios de salud, organismos pagadores, etc. el Centro Criptológico Nacional ha elaborado Perfiles de Cumplimiento Específicos, según lo recogido en el artículo 30 del ENS.

45. Concretamente, en los Anexos de las Guías de los Perfiles presentan la valoración de las dimensiones de seguridad de catálogos de activos (información y servicios), teniendo en cuenta las características propias de la entidad o el sector concreto.

3.8. CRITERIOS ESPECÍFICOS PARA OPERADORES CRÍTICOS DEL SECTOR PÚBLICO

46. Los tipos de información identificados pueden contener información sensible para la seguridad de servicios prestados por operadores críticos, incluyendo información relacionada con el Plan de Seguridad del Operador o con los Planes de Protección Específicos de las infraestructuras críticas.

47. Análogamente, los servicios identificados para los distintos sistemas pueden ser utilizados para la prestación de dichos servicios esenciales.

48. El sistema categorizado respecto al ENS podría ser utilizado por una infraestructura crítica, contribuyendo a la garantía de seguridad de la prestación de un servicio esencial para la sociedad.

49. 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 con la Ley de Secretos Oficiales[5] y por tanto la necesaria acreditación de los sistemas clasificados que la manejan.

4. DETERMINACIÓN DE LOS NIVELES Y CATEGORÍA DEL SISTEMA

4.1. VALORACIÓN DE LAS DIMENSIONES DE LOS ACTIVOS ESENCIALES

50. 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), T (Trazabilidad) y A (Autenticidad).

51. 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.

[5] Ley 9/1968, de 5 de abril, sobre secretos oficiales.

Denominación del activo esencial	tipo[6]	C[7]	I	T	A	D
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.

52. 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.

53. 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 concurran para prestar el servicio correspondiente.

4.2. DETERMINACIÓN DE SUBSISTEMAS

54. 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.

55. 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.

56. La categoría de cada subsistema se determina atendiendo a lo establecido en el Anexo I del ENS.

57. La aplicabilidad de las medidas descritas en el Anexo II del ENS se determinará para cada subsistema.

[6] Tipo: Información o Servicio.
[7] C (Confidencialidad), I (integridad), T (Trazabilidad), A (Autenticidad) y D (Disponibilidad). Por cada dimensión de seguridad se elegirá entre los niveles Bajo, Medio, Alto o N/A (No adscrito a ningún nivel).

58. Un sistema de información cumple con el ENS cuando todos sus subsistemas cumplen, de acuerdo con los niveles de seguridad para cada dimensión y la categoría que corresponde en cada caso.

59. 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
Subsistema 1 …	
Subsistema 2 …	
Valor máximo de la categoría de los subsistemas	

Figura 2. Categorización de un Sistema a partir de sus Subsistemas.

4.3. FORMULACIÓN DE LA CATEGORÍA DE UN SISTEMA

60. 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)]

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

Categoría que se ha asignado al/los sistemas(s) de << Nombre de la entidad>> es:
(Categoría): [C(Nivel), I(Nivel), T(Nivel), A(Nivel), D(Nivel)]

Figura 3. Categorización de un Sistema junto a los Niveles en sus Dimensiones de Seguridad.

Ejemplos:

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

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

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

4.4. SISTEMAS DE INFORMACIÓN DE TERCEROS

62. Cuando un sistema utiliza otros de terceros para gestionar información o para prestar servicios, la valoración propia (el nivel determinado para cada dimensión) de esos

activos esenciales podrá exigirse como un mínimo aceptable al tercero, debiendo el sistema del tercero ajustarse al nivel en cada dimensión.

63. Con carácter general, la categorización del sistema de información será extensible a los sistemas de terceros que se utilicen en la prestación de los servicios o gestión de la información, por lo que se exigirá a los sistemas de terceros la conformidad del ENS en la categoría correspondiente, bien mediante certificación en MEDIA o ALTA o declaración responsable en BÁSICA o bien que las medidas de seguridad del sistema sean acordes con la categoría. Esta exigencia es independiente de la forma por la que se adquieren los sistemas de terceros (compra, cesión…).

64. Para las entidades incluidas en el artículo 77.1 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de derechos digitales (en adelante, LOPDGDD), cuando se traten datos personales por un tercero (encargado del tratamiento), el sistema de información, de acuerdo con la Disposición Adicional Primera de la LOPDGDD, deberá contar con las medidas del ANEXO II adecuadas a la valoración realizada y al análisis de riesgos, sin perjuicio de otras medidas derivadas del cumplimiento de la normativa de protección de datos.

65. 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 o por otra normativa sectorial específica.

4.5. DOCUMENTACIÓN

66. 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.
    - leyes, reglamentos, normas 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.

67. Todas las decisiones deben estar debida y formalmente aprobadas, así como 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.
- 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 último, dichos sistemas serán objeto de una auditoría de conformidad con lo dispuesto en el art. 31 y Anexo III del ENS.

5. ANEXO A. ABREVIATURAS

Siglas	Definición
ANS	Acuerdo de Nivel de Servicio (en inglés, SLA)
ENS	Esquema Nacional de Seguridad
LOPDGDD	Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales
LPIC	Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas.
MAGERIT	Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información
MBCO	Nivel mínimo de los servicios y/o productos que es aceptable para la organización para conseguir sus objetivos durante una disrupción.
RGPD	Reglamento (UE) 2016/679.
RTO	Recovery Time Objective (en español, TRO)
SLA	Service Level Agreement (en español, ANS)
TRO	Tiempo de recuperación objetivo (en inglés RTO)