centro criptológico nacional

# Guía de Seguridad de las TIC
# CCN-STIC 803

## ENS. Valoración de los sistemas


Mayo 2020

MINISTERIO DE DEFENSA

Edita:



2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2020.11.17 09:54:50 +01'00'



NIPO: 785-17-078-3

Fecha de Edición: mayo de 2020

**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**

# PRÓLOGO

En un mundo cada vez más complejo y globalizado, en el que las tecnologías de la información y la comunicación (TIC) desempeñan un papel de suma importancia, hemos de ser conscientes de que la gestión adecuada de la ciberseguridad constituye un reto colectivo al que necesariamente hemos de enfrentar. Resulta necesario garantizar la protección de la capacidad económica, tecnológica y política de nuestro país, máxime cuando la proliferación de ataques dirigidos y el robo de información sensible representan una realidad incontestable.

Por ello, resulta imprescindible estar al día de las amenazas y vulnerabilidades asociadas al uso de las nuevas tecnologías. El conocimiento de los riesgos que se ciernen sobre el ciberespacio ha de servir para implementar con garantías las medidas, tanto procedimentales como técnicas y organizativas, que permitan un entorno seguro y confiable.

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 y de protección de la información clasificada, a la vez que confiere a su Secretario de Estado Director la responsabilidad de dirigir el Centro Criptológico Nacional (CCN).

Partiendo del conocimiento y la experiencia del CNI sobre amenazas y vulnerabilidades en materia de riesgos emergentes, el Centro realiza, a través del 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, al empleo de tecnologías de seguridad adecuadas y a la aplicación de políticas y procedimientos de seguridad.

Precisamente, esta serie de documentos CCN-STIC es un claro reflejo de la labor que este organismo lleva a cabo en materia de implementación de seguridad, permitiendo la aplicación de políticas y procedimientos, pues las guías han sido elaboradas con un claro objetivo: mejorar el grado de ciberseguridad de las organizaciones, 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 la difícil tarea de proporcionar seguridad a los sistemas de las TIC bajo su responsabilidad.

Con esta serie de documentos, el Centro Criptológico Nacional, en cumplimiento de sus cometidos y de lo reflejado en el Real Decreto 3/2010 por el que se regula el Esquema Nacional en el ámbito de la Administración electrónica, contribuye a mejorar la ciberseguridad española y mantener las infraestructuras y los sistemas de información de todas las administraciones públicas con unos niveles óptimos de seguridad. Todo ello, con el fin de generar confianza y garantías en el uso de estas tecnologías, protegiendo la confidencialidad de los datos y garantizando su autenticidad, integridad y disponibilidad.

Mayo de 2020

Paz Esteban López
Secretaria de Estado
Directora del Centro Criptológico Nacional

# ÍNDICE

## 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 de seguridad (artículo 43) 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 Esquema Nacional de Seguridad establece tres categorías de seguridad para los sistemas de información: 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. Esta guía pretende definir los criterios para determinar el nivel de seguridad requerido en cada dimensión y ofrecer recomendaciones considerando también otros marcos normativos (tales como los derivados de la protección de datos o la seguridad de los operadores críticos, por ejemplo), 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

6. 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 pueda ser mayor, obviando aquellas combinaciones en las que el impacto sea despreciable o irrelevante.

7. Habiendo identificado previamente los servicios prestados por la entidad, sujetos al cumplimiento del ENS, conviene comenzar la valoración por los activos de tipo **información** utilizados por tales servicios, valorando, en este orden: *confidencialidad, integridad, trazabilidad, autenticidad* 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.

8. Conviene seguir con los activos de tipo **servicio**, 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, asumiendo los establecidos en el párrafo anterior.

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

10. La categoría del sistema se determina considerando el valor máximo de todas sus dimensiones, para todos los servicios prestados por el sistema.

## 1.2. PROCEDIMIENTO DE VALORACIÓN

11. Si la entidad ha creado un Comité TIC[1] y un Comité STIC[2], una de las funciones del Comité TIC puede ser la identificación de los tipos de información que se van a manejar y los servicios que se van a prestar, priorizando la consideración de los denominados activos esenciales que pueden tener una mayor criticidad. Definidos los tipos de información y de servicios, una tarea del Comité STIC podrá 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 marco normativo que rija las actuaciones de la entidad en materia de seguridad de la información.

12. Los niveles así establecidos podrán ser posteriormente ajustados por los responsables correspondientes (Responsable(s) de la Información y de los Servicios). Idealmente, todas las valoraciones vendrán establecidas por la normativa.

13. 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 o por el Comité STIC y aprobada posteriormente por el Responsable de la Información o del Servicio correspondiente, si éste la considera adecuada.

[1] Comité TIC: de Tecnologías de la Información y la Comunicación.

[2] Comité STIC: de Seguridad en las Tecnologías de Información y la Comunicación.

14. Exceptuando en aquellas cuestiones 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.

15. 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.

16. 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.

17. 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

18. 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.*

19. 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, trazabilidad y autenticidad.

20. El servicio de notificación o publicación hace propias dichas valoraciones, y añade los requisitos de disponibilidad que determine el Responsable del Servicio.

21. 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

22. 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.

23. 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.

24. Esta guía incluye criterios que pueden resultar de aplicación a una o varias dimensiones, tanto de tipos de información como de servicios.

25. 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

26. 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[3].

27. Los criterios de impacto considerados son los siguientes:

- Disposición legal: Existencia de una disposición legal o administrativa que condicione el nivel de la dimensión.

[3] En las tablas siguientes la expresión “N/A” indica que la dimensión no está adscrita a ningún nivel.

- Perjuicio directo: Existencia de un perjuicio directo para el ciudadano, entendido como persona física, jurídica o profesional, y de cualquier índole.
- Incumplimiento de una norma: Implica el incumplimiento de una norma (legal o administrativa, 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.

| CRITERIOS COMUNES APLICABLES A TODAS LAS DIMENSIONES DE TIPOS DE INFORMACIÓN Y SERVICIOS | | | | | |
|---|---|---|---|---|---|
| | | **No Aplicable (N/A)** | **BAJO** | **MEDIO** | **ALTO** |
| **Disposición legal o administrativa** | | COM.DIS.N<br>No existe ninguna disposición legal o administrativa que condicione su nivel. | COM.DIS.B<br>Por disposición legal o administrativa: ley, decreto, orden, resolución… | COM.DIS.M<br>Por disposición legal o administrativa: ley, decreto, orden, resolución… | COM.DIS.A<br>Por disposición legal o administrativa: ley, decreto, orden, resolución… |
| **Perjuicio Directo al ciudadano (de cualquier índole)** | | COM.PER.N<br>No supone ningún perjuicio directo al ciudadano. | COM.PER.B<br>Algún perjuicio. | COM.PER.M<br>Daño importante, aunque subsanable. | COM.PER.A<br>Grave daño, de difícil o imposible reparación. |
| **Incumplimiento de una Norma** | **Legal o administrativa** | COM.LEG.N<br>No implica incumplimiento de una norma jurídica. | COM.LEG.B<br>Incumplimiento formal leve de una norma jurídica, de carácter subsanable. | COM.LEG.M<br>Incumplimiento material de una norma jurídica, o incumplimiento formal no subsanable. | COM.LEG.A<br>Incumplimiento formal y material grave de una norma jurídica. |
| | **Regulatoria** | COM.REG.N<br>No implica incumplimiento de normativa de un regulador. | COM.REG.B<br>Implica incumplimiento de normativa de un regulador. | COM.REG.M<br>Implica sanción significativa de un regulador. | COM.REG.A<br>Implica sanción grave de un regulador y/o pérdida de licencia de operar. |
| | **Contractual** | COM.CON.N<br>No implica incumplimiento de una obligación contractual. | COM.CON.B<br>Incumplimiento formal leve de una obligación contractual. | COM.CON.M<br>Incumplimiento material o formal de una obligación contractual. | COM.CON.A<br>Incumplimiento formal o material grave de una obligación contractual. |
| | **Interna** | COM.INT.N<br>No implica incumplimiento de normativa interna. | COM.INT.B<br>Incumplimiento formal leve de una norma interna. | COM.INT.M<br>Incumplimiento material o formal de una norma interna. | COM.INT.A<br>Incumplimiento formal o material grave de una norma interna. |

| CRITERIOS COMUNES APLICABLES A TODAS LAS DIMENSIONES DE TIPOS DE INFORMACIÓN Y SERVICIOS | | | | |
|---|---|---|---|---|
| | **No Adscrito (N/A)** | **BAJO** | **MEDIO** | **ALTO** |
| **Pérdidas económicas** | COM.ECO.N<br>No implica pérdidas económicas. | COM.ECO.B<br>Pérdidas económicas apreciables (no superiores al 4% del presupuesto anual de la organización). | COM.ECO.M<br>Pérdidas económicas importantes (superiores al 4% e inferiores al 10% del presupuesto anual de la organización). | COM.ECO.A<br>Pérdidas económicas o alteraciones financieras significativas (superiores al 10% del presupuesto anual de la organización). |
| **Reputación** | COM.REP.N<br>No implica daño reputacional. | COM.REP.B<br>Daño reputacional moderado con los ciudadanos o con otras organizaciones. | COM.REP.M<br>Daño reputacional significativo con los ciudadanos o con otras organizaciones. | COM.REP.A<br>Daño reputacional grave con los ciudadanos o con otras organizaciones. |
| **Protestas** | COM.PRO.N<br>No se prevé que pueda desembocar en protestas. | COM.PRO.B<br>Múltiples protestas individuales. | COM.PRO.M<br>Protestas públicas (alteración del orden público). | COM.PRO.A<br>Protestas masivas (alteración seria del orden público). |
| **Delitos** | COM.DEL.N<br>No facilitaría la comisión de delitos ni dificultaría su investigación. | COM.DEL.B<br>Favorecería la comisión de delitos. | COM.DEL.M<br>Favorecería significativamente la comisión de delitos o dificultaría su investigación. | COM.DEL.A<br>Podría incitar 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

28. 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."*

29. 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".*

30. Por todo ello, el conjunto de medidas que finalmente hayan de aplicarse, además de contemplar los principios de protección de datos desde el diseño y por defecto y el resto de los preceptos legales de aplicación, habrán de dirigirse a la protección de los derechos fundamentales de los titulares de los datos personales.

31. Finalmente, recordar que, en tanto no sea transpuesta a nuestro ordenamiento jurídico la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, siguen vigentes, exclusivamente para el tratamiento de este tipo de datos, la Ley Orgánica 15/1999 y el Real Decreto 1720/2007 que la desarrolla, tal y como señala la Disposición transitoria cuarta de la LOPDGDD.

## 2.3. CRITERIOS PARA LA DISPONIBILIDAD DE LOS SERVICIOS

### 2.3.1. PERIODOS CRÍTICOS

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

33. 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[4]) requerido a proveedores.

34. 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)

35. 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.

[4] Service Level Agreement (en español, ANS)

36. Antes de que se alcance el tiempo máximo establecido por el RTO[5] la organización deberá haber alcanzado el nivel mínimo de servicio (MBCO[6]) que deberá haber sido establecido por el Responsable del Servicio.

37. 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.

38. 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.

39. Las siguientes tablas pueden usarse como referencia.

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

Tabla 2. 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 Aplicable (N/A)** | **BAJO** | **MEDIO** | **ALTO** |
| **RTO – Tiempo Objetivo de Recuperación** | DIS.RTO.N<br>La restauración de los niveles mínimos de servicio puede realizarse en un plazo superior a 5 días (RTO) | DIS.RTO.B<br>La restauración de los niveles mínimos de servicio debe realizarse en un plazo máximo de 5 días (RTO) | DIS.RTO.M<br>La restauración de los niveles mínimos de servicio debe realizarse en un plazo máximo de 1 día (RTO) | DIS.RTO.A<br>La restauración de los niveles mínimos de servicio debe realizarse en un plazo máximo de 4 horas (RTO) |

Tabla 3. Criterios de determinación de la disponibilidad de los servicios

## 2.4. CRITERIOS ESPECÍFICOS

Para facilitar la valoración de diferentes tipos de organismos, tales como las Entidades Locales o las Universidades, el Centro Criptológico Nacional ha elaborado la Guía CCN-STIC-883 Implantación del ENS en las EELL.

[5] Recovery Time Objective (en español, TRO).

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

Concretamente, los Anexos I, II y III de dicha Guía presentan la valoración de las dimensiones de seguridad de catálogos de activos (información y servicios), teniendo en cuenta los rangos de población y el papel esencial de las Diputaciones, Cabildos insulares u otros organismos competencialmente encargados de la seguridad de la información y la implantación de la Administración Electrónica. Las referencias a la normativa aplicable están recogidas en el epígrafe 8 del presente documento.

40. Por otro lado, se ha incluido, como Anexo I de la presente Guía, unos criterios específicos para Universidades.

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

41. Los tipos de información identificados pueden contener información sensible para la seguridad de servicios esenciales para la sociedad 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.

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

43. 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.

44. La protección de infraestructuras críticas tiene su propia legislación (LPIC[7]). 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.

45. 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.

46. 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.

47. 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

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

medidas, podrá requerir la clasificación legal de la información, de acuerdo a la Ley de Secretos Oficiales[8] y por tanto la necesaria acreditación de los sistemas clasificados que la manejan.

# 3. TIPOS DE INFORMACIÓN

## 3.1. IDENTIFICACIÓN

48. Aunque *información* es cualquier conjunto de datos que tiene significado, el Esquema Nacional de Seguridad se concentra en valorar los servicios de aquellas entidades que, directa o indirectamente, estén sometidos a la Ley 39/2015, de 1 de octubre, Procedimiento Administrativo Común de las Administraciones Públicas y a la 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 de dicho ámbito de aplicación[9]. 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 confiere entidad propia e implica unos deberes del sector público respecto del tratamiento de dicho tipo de información.

49. No se valorarán directamente datos auxiliares que no son objeto directo del proceso administrativo o no estén comprendidos en las competencias de la entidad de que se trate, y sólo aparezcan como instrumentales para la prestación de los servicios. Por ejemplo, servicios de directorio, claves de acceso, etc.

50. 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.

51. La determinación de los tipos de información y la figura de su Responsable o Responsables 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(s) persona(s) responsable(s).

[8] Ley 9/1998, de 5 de abril, sobre secretos oficiales.

[9] Para mayor detalle, véase Guía CCN-STIC 830 Ámbito de aplicación del ENS.

## 3.2. VALORACIÓN

52. 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.

53. La información suele imponer requisitos relevantes en las dimensiones de **confidencialidad**, **integridad**, **trazabilidad** y **autenticidad**. No suele haber requisitos relevantes en la dimensión de **disponibilidad**, que se considera en los servicios que gestionan esa información.

54. Cuando una dimensión no condiciona las medidas de seguridad, en el apartado de valoración se indicará como "**No Aplicable**" o "**N/A**".

55. A continuación, se describen 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 fundamente la adscripción que determine como apropiada.

### 3.2.1. CONFIDENCIALIDAD

56. 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**.

57. Son de aplicación los Criterios para Datos de Carácter Personal, detallados en el apartado 2.2.

58. 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 2.5.

- No será aplicable (N/A) la valoración a la dimensión cuando se trata de información de carácter público, accesible por cualquier persona.

### 3.2.2. INTEGRIDAD

59. 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.**

60. Son de aplicación los Criterios para Datos de Carácter Personal, detallados en el apartado 2.

61. 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 2.5.

62. No será aplicable (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. TRAZABILIDAD

63. 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**.
64. Son de aplicación los Criterios para Datos de Carácter Personal, detallados en el apartado 2.2.
65. 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 2.5.
66. No será aplicable (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.

### 3.2.4. AUTENTICIDAD

67. Son de aplicación los Criterios Generales del apartado 2.1, considerando las consecuencias que tendría **el hecho de que la información no fuera auténtica**.
68. Son de aplicación los Criterios para Datos de Carácter Personal, detallados en el apartado 2.
69. 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 2.5.
70. No será aplicable (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.

## 4. SERVICIOS

## 4.1. IDENTIFICACIÓN

71. A los efectos de esta guía, se entiende por *servicio* aquel prestado por los sistemas de información de la entidad que esté sometidos, directa o indirectamente, 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.

72. 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.

73. No se valoran servicios internos, auxiliares o instrumentales tales como correo electrónico, ficheros en red, servicios de directorio, de impresión, de copias de respaldo, etc., salvo que constituyen elementos esenciales para la prestación de los servicios al ciudadano.

74. 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.

75. 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

76. 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.

77. 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.

78. 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.

79. 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.

80. Cuando una dimensión no condiciona las medidas de seguridad, en el apartado de valoración se indicará como **“No Aplicable**” o **“N/A”.**

81. A continuación, se describen criterios para establecer un valor en la dimensión relevante en un servicio: la disponibilidad. 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 fundamente la adscripción que determine como apropiada.

### 4.2.1. DISPONIBILIDAD

82. 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.**

83. Son de aplicación los Criterios para Disponibilidad, detallados en el apartado 2.3.

84. 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.

85. No será aplicable (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

86. 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).

87. 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[10] | C[11] | 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.

88. 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.

89. 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.

[10] Tipo: Información o Servicio.

[11] 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).

## 5.2. DETERMINACIÓN DE SUBSISTEMAS

90. 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.

91. 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.

92. La categoría de cada subsistema se determina atendiendo a lo establecido en el Anexo I del RD 3/2010.

93. La aplicabilidad de las medidas descritas en el Anexo II del RD 3/2010 se determinará para cada subsistema.

94. 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.

95. 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[12] |
|---|---|
| Subsistema 1 … | |
| Subsistema 2 … | |
| Valor máximo de la categoría de los subsistemas | |

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

## 5.3. FORMULACIÓN DE LA CATEGORÍA DE UN SISTEMA

96. 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:

[12] Puede ser BÁSICA, MEDIA o ALTA.

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)]

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

| Categoría que se ha asignado al/los sistema(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)]

## 5.4. TERCERAS PARTES

98. 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.

99. 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.

100. 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.

101. 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.

102. 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

103. 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.

104. 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.
- 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 último, dichos sistemas serán objeto de una auditoría de conformidad con lo dispuesto en el art. 34 y 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**

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-today 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 |
|---|---|
| **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) |

## 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 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales
- 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 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
- Guía de seguridad de las TIC – (CCN-STIC-883) - Implantación del ENS para EELL

Los Anexos de la Guía 883 presentan los Perfiles de Cumplimiento Específicos y ejemplos de Planes de adecuación para EELL en función de rangos de población.

- Ayuntamientos pequeños y con limitados recursos, de menos de 5.000 habitantes:
    - Anexo I. Plan de Adecuación Ayuntamientos de menos de 20.000 habitantes.
    - CCN-STIC 883A - Perfil de Cumplimiento Específico Ayuntamientos pequeños y con limitados recursos (<5.000 habitantes).

- Ayuntamientos entre 5.000 y 20.000 habitantes:
  - Anexo I. Plan de Adecuación Ayuntamientos de menos de 20.000 habitantes.
  - CCN-STIC 883B - Perfil de Cumplimiento Específico Ayuntamientos de menos de 20.000 habitantes.
- Ayuntamientos entre 20.000 y 75.000 habitantes:
  - Anexo II. Plan de Adecuación Ayuntamientos entre 20.000 y 75.000 habitantes.
  - CCN-STIC 883C - Perfil de Cumplimiento Específico Ayuntamientos entre 20.000 y 75.000 habitantes.
- Diputaciones, Cabildos, Consejos Insulares u Órgano Competente Equivalente:
  - Anexo III. Plan de Adecuación Diputaciones, Cabildos, Consejos insulares u órgano competente equivalente.
  - CCN-STIC 883D - Perfil de Cumplimiento Específico Diputaciones.

• 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.