GUÍA DE SEGURIDAD
(CCN-STIC-803)

ESQUEMA NACIONAL DE SEGURIDAD
VALORACIÓN DE LOS SISTEMAS

ENERO 2011

Edita:

NIPO: 075-11-053-3

Tirada: 1000 ejemplares
Fecha de Edición: enero de 2011
Informática de la Comunidad de Madrid (ICM) ha participado en la redacción de documento.

PRÓLOGO

El uso masivo de las tecnologías de la información y las telecomunicaciones (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, 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 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.

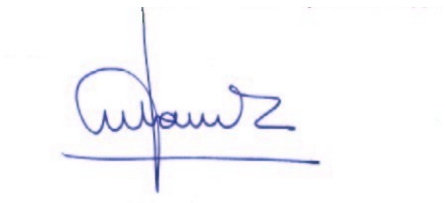
Una de las funciones más destacables del Centro Criptológico Nacional es la de elaborar y difundir normas, instrucciones, guías y recomendaciones para garantizar la seguridad de los sistemas de las tecnologías de la información y las comunicaciones de la Administración, materializada en la existencia de la serie de documentos CCN-STIC.

Disponer de un marco de referencia que establezca las condiciones necesarias de confianza en el uso de los medios electrónicos es, además, uno de los principios que establece la ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos, en su artículo 42.2 sobre el Esquema Nacional de Seguridad (ENS).

Precisamente el Real Decreto 3/2010 de 8 de Enero de desarrollo del Esquema Nacional de Seguridad 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 las comunicaciones 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.

Enero de 2011



Félix Sanz Roldán
Secretario de Estado
Director 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 (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 en cada dimensión.
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: disponibilidad [D], autenticidad [A], integridad [I], confidencialidad [C] y trazabilidad [T].
4. El Esquema Nacional de Seguridad establece tres categorías: 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. En esta guía se busca ampliar los criterios para determinar el nivel de seguridad requerido en cada dimensión. Para ello se analizan los elementos esenciales: información y servicios, pivotando alrededor de ellos los criterios que el responsable de cada información y cada servicio podrá utilizar.

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, 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.
7. 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.
8. Conviene seguir con los activos de tipo servicio, valorando en este orden: disponibilidad, autenticidad y trazabilidad. Los requisitos en materia de confidencialidad e integridad suelen venir impuestos por la información que maneja el servicio, heredándose los establecidos en el párrafo anterior.
9. El sistema queda valorado por los valores máximos de la información que maneja y los servicios que presta.

1.2. PROTOCOLO

10. Si el organismo ha creado un Comité TIC[1] y un Comité STIC[2], una de las funciones del comité TIC puede ser la determinación de los tipos de información que se van a manejar y una clasificación de los servicios que se van a prestar. Definidos los tipos de información y de servicios, una tarea del Comité STIC puede ser el establecimiento de los niveles de seguridad recomendados para cada uno de los tipos de información y servicios. Estas definiciones deben ser aprobadas dentro del juego de normativa que rige las actuaciones del organismo.
11. Los niveles así establecidos podrán ser posteriormente ajustados por los responsables correspondientes. Idealmente, todas las valoraciones vendrán establecidas por la normativa.
12. La responsabilidad de la valoración de la información y de los servicios es exclusivamente del responsable correspondiente. La valoración puede ser propuesta por el Responsable del Sistema o por el Responsable de Seguridad y aprobada por el responsable de la información o del servicio correspondiente si éste la considera adecuada.
13. Exceptuando aquellos puntos en los que exista un mandato legal o administrativo, la opinión del Responsable de Seguridad y del Responsable del Sistema deben ser recabadas y consideradas en el proceso de valoración.
14. Cuando el sistema trate datos de carácter personal, deberá establecerse el nivel de medidas de seguridad necesarias según se indica en la normativa correspondiente.
15. Una vez determinadas las valoraciones de las diferentes informaciones 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 para
    a. determinar la valoración del sistema en cada dimensión
    b. determinar la categoría del sistema
    c. determinar el conjunto mínimo de medidas de seguridad del Anexo II que son de aplicación en el sistema aplicando las condiciones indicadas en dicho anexo
16. Por último, se deberá enriquecer el conjunto de medidas con aquellas que derivan del ordenamiento relativo a datos de carácter personal.

2. INFORMACIÓN

2.1. IDENTIFICACIÓN

17. Aunque información es cualquier conjunto de datos que tienen significado, el Esquema Nacional de Seguridad se limita a valorar aquellos tipos de información que son relevantes para el proceso administrativo y pueden ser tratados en algún servicio afecto a la ley 11/2007 de acceso electrónico de los ciudadanos a los servicios públicos. 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 del organismo, lo que les confiere entidad propia e implica unos deberes de la administración respecto del tratamiento de dicho tipo de información.

[1] Comité TIC: de Tecnologías de la Información y Comunicaciones.
[2] Comité STIC: de Seguridad en las Tecnologías de Información y Comunicaciones.

18. 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.

19. Para cada elemento 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

20. La determinación de los elementos 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. La Política de Seguridad identificará igualmente el procedimiento de designación de la persona responsable.

2.2. VALORACIÓN

21. La valoración de la información la determina el responsable de la misma teniendo en cuenta la naturaleza de la información y la normativa que pudiera serle de aplicación. Esta valoración requiere un conocimiento legal de la materia de que se trate.

22. La información suele imponer requisitos relevantes en las dimensiones de confidencialidad, integridad, autenticidad y trazabilidad. No suelen haber requisitos relevantes en la dimensión de disponibilidad.

23. El nivel de seguridad requerido en el aspecto de **confidencialidad** se establecerá en función de las consecuencias que tendría su revelación a personas no autorizadas o que no necesitan conocer la información.

24. El nivel de seguridad requerido en el aspecto de **integridad** se establecerá en función de las consecuencias que tendría su modificación por alguien que no está autorizado a modificar la información.

25. El nivel de seguridad requerido en el aspecto de **autenticidad** se establecerá en función de las consecuencias que tendría el hecho de que la información no fuera auténtica.

26. El nivel de seguridad requerido en el aspecto de **trazabilidad** se establecerá en función de las consecuencias que tendría el no poder rastrear a posteriori quién ha accedido a o modificado una cierta información.

27. 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 acceder a la información cuando la necesita.

28. Cuando un aspecto no requiere medidas de seguridad, en el apartado de valoración se indicará **SIN VALORAR**.

29. A continuación se describen criterios para establecer un valor en cada dimensión. Estos criterios son de carácter general, sirviendo de mera guía para que la política de seguridad concrete casos particulares del organismo, y que el responsable de la información fundamente la adscripción que determine como apropiada.

2.2.1. CRITERIOS GENERALES PARA VALORAR LA CONFIDENCIALIDAD NECESARIA

30. [C=A] Nivel ALTO
    - porque la información debe conocerla un número muy reducido de personas
    - por disposición legal o administrativa: ley, decreto, orden, reglamento, …
    - porque su revelación causaría un grave daño, de difícil o imposible reparación
    - porque su revelación supondría el incumplimiento grave de una norma
    - porque su revelación causaría pérdidas económicas elevadas o alteraciones financieras significativas
    - porque su revelación causaría un daño reputacional grave con los ciudadanos o con otras organizaciones
    - porque su revelación podría desembocar en protestas masivas (alteración seria del orden público)

31. [C=M] Nivel MEDIO
    - porque la información deben conocerla sólo quienes lo necesiten para su trabajo, con autorización explícita
    - por disposición legal o administrativa: ley, decreto, orden, reglamento, …
    - porque su revelación causaría un daño importante aunque subsanable
    - porque su revelación supondría el incumplimiento material o formal de una norma
    - porque su revelación causaría pérdidas económicas importantes
    - porque su revelación causaría un daño reputacional importante con los ciudadanos o con otras organizaciones
    - porque su revelación podría desembocar en protestas públicas (alteración del orden público)

32. [C=B] Nivel BAJO
    - porque la información no deben conocerla personas ajenas a la organización
    - por disposición legal o administrativa: ley, decreto, orden, reglamento, …
    - porque su revelación causaría algún perjuicio
    - porque su revelación supondría el incumplimiento leve de una norma
    - porque su revelación supondría pérdidas económicas apreciables
    - porque su revelación causaría un daño reputacional apreciable con los ciudadanos o con otras organizaciones
    - porque su revelación podría desembocar en múltiples protestas individuales

33. Sin valorar
    - información de carácter público, accesible por cualquier persona

2.2.2. CRITERIOS GENERALES PARA VALORAR LA INTEGRIDAD NECESARIA

34. [I=A] Nivel ALTO

- por disposición legal o administrativa: ley, decreto, orden, reglamento, …
- porque su manipulación o modificación no autorizada causaría un grave daño, de difícil o imposible reparación
- porque su manipulación o alteración no autorizada causaría pérdidas económicas elevadas o alteraciones financieras significativas
- porque su manipulación o alteración no autorizada causaría un daño reputacional grave con los ciudadanos o con otras organizaciones
- porque su manipulación o alteración no autorizada podría desembocar en protestas masivas (alteración seria del orden público)

35. [I=M] Nivel MEDIO

- por disposición legal o administrativa: ley, decreto, orden, reglamento, …
- porque su manipulación o modificación no autorizada causaría un daño importante aunque subsanable
- porque su manipulación o modificación no autorizada supondría el incumplimiento material o formal de una norma
- porque su manipulación o modificación no autorizada causaría pérdidas económicas importantes
- porque su manipulación o modificación no autorizada causaría un daño reputacional importante con los ciudadanos o con otras organizaciones
- porque su manipulación o modificación no autorizada podría desembocar en protestas públicas (alteración del orden público)

36. [I=B] Nivel BAJO

- por disposición legal o administrativa: ley, decreto, orden, reglamento, …
- porque su manipulación o modificación no autorizada causaría algún perjuicio
- porque su manipulación o modificación no autorizada supondría el incumplimiento leve de una norma
- porque su manipulación o modificación no autorizada supondría pérdidas económicas apreciables
- porque su manipulación o modificación no autorizada causaría un daño reputacional apreciable con los ciudadanos o con otras organizaciones
- porque su manipulación o modificación no autorizada podría desembocar en múltiples protestas individuales

37. Sin valorar

- cuando los errores en su contenido carecen de consecuencias o son fácil y rápidamente reparables

2.2.3. CRITERIOS GENERALES PARA VALORAR LA AUTENTICIDAD NECESARIA

38. [A=A] Nivel ALTO

- por disposición legal o administrativa: ley, decreto, orden, reglamento, …
- porque la falsedad en su origen o en su destinatario causaría un grave daño, de difícil o imposible reparación
- porque la falsedad en su origen o en su destinatario causaría pérdidas económicas elevadas o alteraciones financieras significativas
- porque la falsedad en su origen o en su destinatario causaría un daño reputacional grave con los ciudadanos o con otras organizaciones
- porque la falsedad en su origen o en su destinatario podría desembocar en protestas masivas (alteración seria del orden público)

39. [A=M] Nivel MEDIO

- por disposición legal o administrativa: ley, decreto, orden, reglamento, …
- porque la falsedad en su origen o en su destinatario causaría un daño importante aunque subsanable
- porque la falsedad en su origen o en su destinatario causaría pérdidas económicas importantes
- porque la falsedad en su origen o en su destinatario causaría un daño reputacional importante con los ciudadanos o con otras organizaciones
- porque la falsedad en su origen o en su destinatario podría desembocar en protestas públicas (alteración del orden público)

40. [A=B] Nivel BAJO

- por disposición legal o administrativa: ley, decreto, orden, reglamento, …
- porque la falsedad en su origen o en su destinatario causaría algún perjuicio
- porque la falsedad en su origen o en su destinatario causaría pérdidas económicas apreciables
- porque la falsedad en su origen o en su destinatario causaría un daño reputacional apreciable con los ciudadanos o con otras organizaciones
- porque la falsedad en su origen o en su destinatario podría desembocar en múltiples protestas individuales

41. Sin valorar

- 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

2.2.4. CRITERIOS GENERALES PARA VALORAR LA TRAZABILIDAD NECESARIA

42. [T=A] Nivel ALTO
    - por disposición legal o administrativa: ley, decreto, orden, reglamento, …
    - porque la incapacidad para rastrear un acceso a la información impediría o dificultaría notablemente la capacidad de subsanar un error grave
    - porque la incapacidad para rastrear un acceso a la información dificultaría notablemente la capacidad para perseguir delitos
    - porque la incapacidad para rastrear un acceso a la información facilitaría enormemente la comisión de delitos graves

43. [T=M] Nivel MEDIO
    - por disposición legal o administrativa: ley, decreto, orden, reglamento, …
    - porque la incapacidad para rastrear un acceso a la información impediría o dificultaría notablemente la capacidad de subsanar un error importante
    - porque la incapacidad para rastrear un acceso a la información dificultaría notablemente la capacidad para perseguir delitos
    - porque la incapacidad para rastrear un acceso a la información facilitaría la comisión de delitos

44. [T=B] Nivel BAJO
    - por disposición legal o administrativa: ley, decreto, orden, reglamento, …
    - porque la incapacidad para rastrear un acceso a la información dificultaría la capacidad de subsanar errores
    - porque la incapacidad para rastrear un acceso a la información dificultaría la capacidad para perseguir delitos

45. Sin valorar
    - cuando no se pueden producir errores de importancia, o son fácilmente reparables por otros medios
    - cuando no se pueden perpetrar delitos relevante, o su investigación es fácilmente realizable por otros medios

2.2.5. CRITERIOS GENERALES PARA VALORAR LA DISPONIBILIDAD NECESARIA

46. Los requisitos de disponibilidad de la información derivan de su uso o necesidad de ser utilizada.

47. Si su uso es a través de servicios contemplados en el sistema de información, basta valorar dichos servicios e imputar[3] los mismos valores a la información necesaria. Véase cómo se valoran los requisitos de disponibilidad de los servicios, más adelante.

[3] La imputación se realizará usando los conceptos de “dependencias entre activos” de Magerit.

48. Si la información se emplea para otros menesteres, puede ser necesario explicitar los requisitos de estas actividades adicionales como se explica a continuación bajo el nombre genérico de *servicios*, sean o no telemáticos.

49. Uno de los criterios que son útiles para determinar los requisitos de disponibilidad de un *servicio* es el establecimiento de un tiempo de interrupción de referencia, que a menudo se conoce como RTO4, y mide el tiempo máximo que el *servicio* puede permanecer interrumpido. La valoración de la disponibilidad mide las consecuencias en caso de que ese tiempo se supere; es decir, que quedemos fuera de *servicio* por un periodo superior al RTO establecido[5].

50. 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 margen a la improvisación.

51. La siguiente tabla puede usarse como referencia.

RTO	< 4h	4h – 1d	1d – 5d	> 5d
nivel	alto	medio	bajo	sin valorar

4h = 4 horas

1d = 1 día = 24 horas

5d = 5 días (1 semana)

52. Los requisitos de disponibilidad pueden variar. Hay *servicios* que son críticos en ciertos días del mes o del año, mientras que el resto del tiempo es menos importante. Los responsables del sistema deben ajustar las medidas de seguridad a la criticidad en cada momento.

53. [D=A] Nivel ALTO

- por disposición legal o administrativa: ley, decreto, orden, reglamento, …
- porque la indisponibilidad de la información causaría un grave daño, de difícil o imposible reparación
- porque la indisponibilidad de la información supondría el incumplimiento grave de una norma
- porque la indisponibilidad de la información causaría un daño reputacional grave con los ciudadanos o con otras organizaciones
- porque la indisponibilidad de la información podría desembocar en protestas masivas (alteración seria del orden público)
- cuando el RTO es inferior a 4 horas

54. [D=M] Nivel MEDIO

- por disposición legal o administrativa: ley, decreto, orden, reglamento, …

[4] Recovery Time Objective. Tiempo de Recuperación del Servicio (TRS).
[5] En esta guía sólo se cubre el aspecto de valoración y las referencias a los tiempos de recuperación son aproximaciones groseras. En el desarrollo de las medidas de seguridad, el Anexo II puede requerir la elaboración de un Análisis de Impacto. Para realizar este análisis habrá que determinar los tiempos de recuperación con mayor precisión y asegurar los medios que los garanticen.

- porque la indisponibilidad de la información causaría un daño importante aunque subsanable
- porque la indisponibilidad de la información supondría el incumplimiento material o formal de una norma
- porque la indisponibilidad de la información causaría un daño reputacional importante con los ciudadanos o con otras organizaciones
- porque la indisponibilidad de la información podría desembocar en protestas públicas (alteración del orden público)
- cuando el RTO se sitúa entre 4 y 24 horas (un día)

55. [D=B] Nivel BAJO
    - por disposición legal o administrativa: ley, decreto, orden, reglamento, …
    - porque la indisponibilidad de la información causaría algún perjuicio
    - porque la indisponibilidad de la información supondría el incumplimiento leve de una norma
    - porque la indisponibilidad de la información causaría un daño reputacional apreciable con los ciudadanos o con otras organizaciones
    - porque la indisponibilidad de la información podría desembocar en múltiples protestas individuales
    - cuando el RTO se sitúa entre 1 y 5 días (una semana)

56. Sin valorar
    - cuando la información es prescindible por tiempo indefinido
    - cuando el RTO es superior a 5 días laborables (una semana)

3. SERVICIOS

3.1. IDENTIFICACIÓN

57. Se entiende por servicio cada actividad llevada a cabo por la Administración o, bajo un cierto control y regulación de esta, por una organización, especializada o no, y destinada a satisfacer necesidades de la colectividad.
58. El Esquema Nacional de Seguridad se limita a valorar aquellos servicios que son relevantes para el proceso administrativo, estando sometidos a la ley 11/2007 de acceso electrónico de los ciudadanos a los servicios públicos. Algunos de estos servicios pueden estar identificados en algún tipo de ordenamiento general, mientras que otros serán particulares del organismo. En cualquier caso, los servicios aquí contemplados tienen identidad propia con independencia de los medios que se empleen para su prestación, asumiendo el organismo que los presta unas obligaciones con respecto a los mismos.
59. No se valoran servicios internos o auxiliares tales como correo electrónico, ficheros en red, servicios de directorio, de impresión, de copias de respaldo, etc.

60. 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
61. 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. La Política de Seguridad identificará igualmente el procedimiento de designación de la persona responsable.

3.2. VALORACIÓN

62. 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.
63. 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 maneja.
64. 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 al servicio cuando lo necesita.
65. El nivel de seguridad requerido en el aspecto de confidencialidad se establecerá en función de las consecuencias que tendría su revelación a alguien que no necesita conocer la información.
66. El nivel de seguridad requerido en el aspecto de autenticidad se establecerá en función de las consecuencias que tendría el hecho de que el servicio fuera usado por personas indebidamente autenticadas; o sea, por personas que no son quienes se cree que son
67. El nivel de seguridad requerido en el aspecto de trazabilidad se establecerá en función de las consecuencias que tendría el no poder rastrear a posteriori quién ha accedido al servicio.
68. Cuando un aspecto no requiere medidas de seguridad, en el apartado de valoración se indicará SIN VALORAR
69. A continuación se describen criterios para establecer un valor en cada dimensión.

3.2.1. CRITERIOS GENERALES PARA VALORAR LA DISPONIBILIDAD NECESARIA

70. Uno de los criterios que son útiles para determinar los requisitos de disponibilidad de un servicio es el establecimiento de un tiempo de interrupción de referencia, que a menudo se conoce como RTO[6], y mide el tiempo máximo que el servicio puede permanecer interrumpido. La valoración de la disponibilidad mide las consecuencias en caso de que ese tiempo se supere; es decir, que quedemos fuera de servicio por un periodo superior al RTO establecido.

[6] Recovery Time Objective. Tiempo de Recuperación del Servicio (TRS).

71. 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.

72. La siguiente tabla puede usarse como referencia.

RTO	< 4h	4h – 1d	1d – 5d	> 5d
nivel	alto	medio	bajo	sin valorar

4h = 4 horas

1d = 1 día = 24 horas

5d = 5 días (1 semana)

73. Los requisitos de disponibilidad pueden variar a lo largo del tiempo. 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 (SLA7) requerido a proveedores. Los pasos a seguir son los siguientes:

- El Responsable del Servicio marca los periodos en los que se aplica cada nivel de seguridad.
- El Responsable de Seguridad ajustará la valoración del sistema y determinará las medidas necesarias en cada periodo.
- El Responsable de Seguridad velará porque el sistema se ajuste como mínimo a las medidas determinadas en cada periodo, 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.

74. [D=A] Nivel ALTO

- por disposición legal o administrativa: ley, decreto, orden, reglamento, …
- porque la detención del servicio causaría un grave daño, de difícil o imposible reparación
- porque la detención del servicio supondría el incumplimiento grave de una norma
- porque la detención del servicio causaría un daño reputacional grave con los ciudadanos o con otras organizaciones
- porque la detención del servicio podría desembocar en protestas masivas (alteración seria del orden público)
- cuando el RTO es inferior a 4 horas

75. [D=M] Nivel MEDIO

- por disposición legal o administrativa: ley, decreto, orden, reglamento, …
- porque la detención del servicio causaría un daño importante aunque subsanable

[7] Service Level Agreement. Acuerdo de Nivel de Servicio (ANS).

- porque la detención del servicio supondría el incumplimiento material o formal de una norma
- porque la detención del servicio causaría un daño reputacional importante con los ciudadanos o con otras organizaciones
- porque la detención del servicio podría desembocar en protestas públicas (alteración del orden público)
- cuando el RTO se sitúa entre 4 y 24 horas (un día)

76. [D=B] Nivel BAJO
    - por disposición legal o administrativa: ley, decreto, orden, reglamento, …
    - porque la detención del servicio causaría algún perjuicio
    - porque la detención del servicio supondría el incumplimiento leve de una norma
    - porque la detención del servicio causaría un daño reputacional apreciable con los ciudadanos o con otras organizaciones
    - porque la detención del servicio podría desembocar en múltiples protestas individuales
    - cuando el RTO se sitúa entre 1 y 5 días (una semana)

77. Sin valorar
    - cuando el servicio es prescindible por tiempo indefinido
    - cuando el RTO es superior a 5 días laborables (una semana)

3.2.2. CRITERIOS GENERALES PARA VALORAR LA AUTENTICIDAD NECESARIA

78. [A=A] Nivel ALTO
    - por disposición legal o administrativa: ley, decreto, orden, reglamento, …
    - porque la falsedad en su origen o en su destinatario causaría un grave daño, de difícil o imposible reparación
    - porque la falsedad en su origen o en su destinatario causaría pérdidas económicas elevadas o alteraciones financieras significativas
    - porque la falsedad en su origen o en su destinatario causaría un daño reputacional grave con los ciudadanos o con otras organizaciones
    - porque la falsedad en su origen o en su destinatario podría desembocar en protestas masivas (alteración seria del orden público)

79. [A=M] Nivel MEDIO
    - por disposición legal o administrativa: ley, decreto, orden, reglamento, …
    - porque la falsedad en su origen o en su destinatario causaría un daño importante aunque subsanable
    - porque la falsedad en su origen o en su destinatario causaría pérdidas económicas importantes

- porque la falsedad en su origen o en su destinatario causaría un daño reputacional importante con los ciudadanos o con otras organizaciones
- porque la falsedad en su origen o en su destinatario podría desembocar en protestas públicas (alteración del orden público)

80. [A=B] Nivel BAJO
    - por disposición legal o administrativa: ley, decreto, orden, reglamento, …
    - porque la falsedad en su origen o en su destinatario causaría algún perjuicio
    - porque la falsedad en su origen o en su destinatario causaría pérdidas económicas apreciables
    - porque la falsedad en su origen o en su destinatario causaría un daño reputacional apreciable con los ciudadanos o con otras organizaciones
    - porque la falsedad en su origen o en su destinatario podría desembocar en múltiples protestas individuales

81. Sin valorar
    - 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

3.2.3. CRITERIOS GENERALES PARA VALORAR LA TRAZABILIDAD NECESARIA

82. [T=A] Nivel ALTO
    - por disposición legal o administrativa: ley, decreto, orden, reglamento, …
    - porque la incapacidad para rastrear un acceso al servicio impediría o dificultaría notablemente la capacidad de subsanar un error grave
    - porque la incapacidad para rastrear un acceso al servicio dificultaría notablemente la capacidad para perseguir delitos
    - porque la incapacidad para rastrear un acceso al servicio facilitaría enormemente la comisión de delitos graves

83. [T=M] Nivel MEDIO
    - por disposición legal o administrativa: ley, decreto, orden, reglamento, …
    - porque la incapacidad para rastrear un acceso al servicio impediría o dificultaría notablemente la capacidad de subsanar un error importante
    - porque la incapacidad para rastrear un acceso al servicio dificultaría notablemente la capacidad para perseguir delitos
    - porque la incapacidad para rastrear un acceso al servicio facilitaría la comisión de delitos

84. [T=B] Nivel BAJO
    - por disposición legal o administrativa: ley, decreto, orden, reglamento, …

- porque la incapacidad para rastrear un acceso al servicio dificultaría la capacidad de subsanar errores
- porque la incapacidad para rastrear un acceso al servicio dificultaría la capacidad para perseguir delitos

85. Sin valorar
    - 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. CRITERIOS GENERALES PARA VALORAR LA CONFIDENCIALIDAD NECESARIA

86. Los requisitos de confidencialidad sobre un servicio derivan de la información que maneja.
87. [C=A] Nivel ALTO
    - porque la información que se maneja deben conocerla un número muy reducido de personas
    - por disposición legal o administrativa: ley, decreto, orden, reglamento, …
    - porque la revelación de la información que se maneja de causaría un grave daño, de difícil o imposible reparación
    - porque la revelación de la información que se maneja supondría el incumplimiento grave de una norma
    - porque la revelación de la información que se maneja causaría pérdidas económicas elevadas o alteraciones financieras significativas
    - porque la revelación de la información que se maneja causaría un daño reputacional grave con los ciudadanos o con otras organizaciones
    - porque la revelación de la información que se maneja podría desembocar en protestas masivas (alteración seria del orden público)

88. [C=M] Nivel MEDIO
    - porque la información que se maneja deben conocerla sólo quienes lo necesiten para su trabajo, con autorización explícita
    - por disposición legal o administrativa: ley, decreto, orden, reglamento, …
    - porque la revelación de la información que se maneja causaría un daño importante aunque subsanable
    - porque la revelación de la información que se maneja supondría el incumplimiento material o formal de una norma
    - porque la revelación de la información que se maneja causaría pérdidas económicas importantes
    - porque la revelación de la información que se maneja causaría un daño reputacional importante con los ciudadanos o con otras organizaciones

- porque la revelación de la información que se maneja podría desembocar en protestas públicas (alteración del orden público)

89. [C=B] Nivel BAJO
    - porque la información que se maneja no deben conocerla personas ajenas a la organización
    - por disposición legal o administrativa: ley, decreto, orden, reglamento, …
    - porque la revelación de la información que se maneja causaría algún perjuicio
    - porque la revelación de la información que se maneja supondría el incumplimiento leve de una norma
    - porque la revelación de la información que se maneja supondría pérdidas económicas apreciables
    - porque la revelación de la información que se maneja causaría un daño reputacional apreciable con los ciudadanos o con otras organizaciones
    - porque la revelación de la información que se maneja podría desembocar en múltiples protestas individuales

90. Sin valorar
    - la información que se maneja es de carácter público, accesible por cualquier persona

3.2.5. CRITERIOS GENERALES PARA VALORAR LA INTEGRIDAD NECESARIA

91. Los requisitos de integridad sobre un servicio derivan de la información que maneja. Esto incluye la posibilidad de que la información quede en un estado impropio porque el servicio no se complete adecuadamente.
92. [I=A] Nivel ALTO
    - por disposición legal o administrativa: ley, decreto, orden, reglamento, …
    - porque la manipulación o modificación no autorizada de la información que maneja causaría un grave daño, de difícil o imposible reparación
    - porque su manipulación o alteración no autorizada causaría pérdidas económicas elevadas o alteraciones financieras significativas
    - porque su manipulación o alteración no autorizada causaría un daño reputacional grave con los ciudadanos o con otras organizaciones
    - porque su manipulación o alteración no autorizada podría desembocar en protestas masivas (alteración seria del orden público)

93. [I=M] Nivel MEDIO
    - por disposición legal o administrativa: ley, decreto, orden, reglamento, …
    - porque la manipulación o modificación no autorizada de la información que maneja causaría un daño importante aunque subsanable

- porque su manipulación o modificación no autorizada supondría el incumplimiento material o formal de una norma
- porque su manipulación o modificación no autorizada causaría pérdidas económicas importantes
- porque su manipulación o modificación no autorizada causaría un daño reputacional importante con los ciudadanos o con otras organizaciones
- porque su manipulación o modificación no autorizada podría desembocar en protestas públicas (alteración del orden público)

94. [I=B] Nivel BAJO
    - por disposición legal o administrativa: ley, decreto, orden, reglamento, …
    - porque la manipulación o modificación no autorizada de la información que maneja causaría algún perjuicio
    - porque la falsedad en su origen o en su destinatario causaría un daño reputacional apreciable con los ciudadanos o con otras organizaciones
    - porque la falsedad en su origen o en su destinatario podría desembocar en múltiples protestas individuales

95. Sin valorar
    - cuando los errores en la información que se maneja carecen de consecuencias o son fácil y rápidamente reparables

4. DETERMINACIÓN DE LOS NIVELES Y CATEGORÍA DEL SISTEMA

96. Los niveles de seguridad determinados para la información se imputaran[8] a todos los activos que manejen la información correspondiente. Los niveles de seguridad determinados para los servicios se imputaran a todos los activos que concurran para prestar el servicio correspondiente. Puede darse la circunstancia de que diferentes activos del mismo sistema estén sometidos a requisitos diferentes, en virtud de que atiendan a distintas informaciones o servicios. Esto llevará a fragmentar un sistema de información en varios subsistemas.

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

98. La aplicabilidad de las medidas descritas en el Anexo II se determinará para cada sub-sistema.

99. Un sistema de información cumple con el RD 3/2010 cuando todos sus subsistemas cumplen, de acuerdo a los niveles de seguridad y la categoría que corresponde en cada caso.

100. Conviene reducir el número de subsistemas al mínimo imprescindible, haciendo el sistema lo más homogéneo posible. 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 los menos sitios posibles. Como ejemplos de medidas que conviene acotar podemos citar sistemas hardware de cifrado, equipamiento alternativo de alta disponibilidad, etc.

[8] La imputación se realizará usando los conceptos de “dependencias entre activos” de Magerit

4.1. TERCERAS PARTES

101. Cuando un sistema maneja información de terceros o presta servicios a terceros, la valoración de la información y los servicios será la determinada por dicho tercero. Esta valoración será formalmente comunicada al Responsable del Sistema y al Responsable de Seguridad para que se ajuste la categoría y el conjunto de medidas de seguridad requeridas.

    - Los requisitos de otros sistemas que dependen servicios prestados por este sistema, son requisitos de este sistema.

102. Cuando un sistema utiliza sistemas de tercero para manejar información o para prestar servicios, la valoración propia será impuesta al tercero que colabora.

    - Los requisitos de este sistema se convierten en los requisitos de los sistemas utilizados.

103. 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.

5. DOCUMENTACIÓN

104. Es esencial que queden perfectamente documentadas todas las actividades relativas a la valoración de los sistemas:

    - criterios seguidos y razonamientos aplicados
    - 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 recomendaciones de auditoría

105. 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 las medidas de seguridad que son de aplicación (Declaración de Aplicabilidad) y las medidas técnicas que se toman para sustanciar dichas medidas de seguridad.
    - El Responsable de Seguridad aprueba las medidas de seguridad que son de aplicación (Declaración de Aplicabilidad) y las medidas técnicas que se toman para sustanciar dichas medidas de seguridad.
    - Si se toman decisiones de suspensión parcial o total de un sistema, estás vendrán aprobadas por el Responsable del Sistema y los responsables de los servicios afectados por la suspensión.

6. CRITERIOS ESPECÍFICOS

106. 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 los necesarios, dentro de un organismo o en sistemas de intercambio de información o prestación de servicios entre organismos.

107. Dentro de un organismo, lo idóneo es identificar los tipos de información que se manejan. Puede utilizarse la guía SP 800-60, a título ilustrativo, aunque carece de carácter normativo en nuestro ámbito.

108. Idealmente esta identificación de tipos de información puede ser compartida y esperamos que futuras versiones de esta guía puedan incorporar tipos identificados que sean de aplicación en diferentes organismos.

109. Igualmente sería conveniente identificar tipos de servicios prestados bajo la ley 11/1997.

110. Identificados los tipos de información y los tipos de servicio, el comité STIC de cada organismo puede establecer una propuesta de niveles de valoración en cada dimensión. Puede utilizarse la guía SP 800-60, volumen 2, a título ilustrativo, respetando siempre la decisión que adopte el alto cargo que ostente la responsabilidad sobre la información y el servicio en cada caso.

111. Idealmente estas valoraciones de referencia pueden ser compartidas y esperamos que futuras versiones de esta guía puedan incorporar tablas que sean de aplicación en diferentes organismos.

6.1.1. NOTIFICACIONES Y PUBLICACIONES ELECTRÓNICAS

112. El Esquema Nacional de Seguridad establece en su artículo 32 relativo a "Requerimientos técnicos de notificaciones y publicaciones electrónicas" que:

    1. 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:

        a) Aseguren la autenticidad del organismo que lo publique.
        b) Aseguren la integridad de la información publicada.
        c) 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.
        d) Aseguren la autenticidad del destinatario de la publicación o notificación.

113. 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. La valoración de dicha información es entrada para los cálculos del Anexo I. Típicamente, la valoración de la información establece los niveles en materia de confidencialidad, integridad, autenticidad y trazabilidad.

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

6.1.2. DATOS DE CARÁCTER PERSONAL

115. Los datos de carácter personal tienen su propia legislación:

- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (B.O.E. Nº 298, de 14 de diciembre de 1999)
- Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal

116. De acuerdo dicha regulación, los datos de carácter personal requieren una serie de medidas de seguridad de un cierto nivel determinado por su naturaleza y la finalidad con la que se manejan.

117. Muchas medidas de seguridad vienen requeridas tanto por el Esquema Nacional de Seguridad como por el Reglamento de Protección de Datos de Carácter Personal, por lo que su implantación puede ser unificada, sin perjuicio de que en los procesos de auditoría se verifique su idoneidad para proteger tanto los datos de carácter personal como los servicios prestados a los ciudadanos.

118. Es función del responsable de seguridad determinar el conjunto de medidas requerido, uniendo los que se requieren por una y otra norma, e imponiendo la exigencia superior.

119. La existencia de datos de carácter personal requiere la realización de un documento de seguridad y la designación de una serie de responsables. Parece natural que estos requisitos se contemplen en la Política de Seguridad requerida por el Esquema Nacional de Seguridad.

ANEXO A. GLOSARIO DE TÉRMINOS Y ABREVIATURAS

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.

Disponibilidad

Propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren. ENS.

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

El responsable de seguridad determinará 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.

ABREVIATURAS

ANS	Acuerdo de Nivel de Servicio (en inglés, SLA)
ENS	Esquema Nacional de Seguridad
Magerit	Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información
RTO	Recovery Time Objective (en español, TRS)
SLA	Service Level Agreement (en español, ANS)
TRS	Tiempo de Recuperación del Sistema (en inglés, RTO)

REFERENCIAS

2001/264/CE

Decisión del Consejo de 19 de marzo de 2001 por la que se adoptan las normas de seguridad del Consejo.

CCN-STIC-402

Organización y Gestión para la Seguridad de los Sistemas TIC. Diciembre 2006.

CCN-STIC-801

Esquema Nacional de Seguridad: Roles y Funciones. Diciembre 2010.

FIPS 199

Standards for Security Categorization of Federal Information and Information Systems. Feb. 2004.

Ley 15/1999

Protección de datos de carácter personal. Diciembre 1999.

Magerit

Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Versión 2. Junio 2006.

RD 1720/2007

Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal. BOE de 19 de enero de 2008.

RD 3/2010

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. BOE de 29 de enero de 2010.

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.