GOBIERNO DE ESPAÑA
MINISTERIO DE DEFENSA

CCN
centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 824

INFORME NACIONAL DEL ESTADO DE SEGURIDAD DE LOS SISTEMAS TIC

Octubre 2018

Edita:

GOBIERNO DE ESPAÑA MINISTERIO DE DEFENSA

CCN centro criptológico nacional

CENTRO CRIPTOLOGICO NACIONAL
2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, cn=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2019.01.02 09:06:45 +01'00'

NIPO: 083-19-021-2

Fecha de Edición: octubre de 2018
J.A. Mañas ha participado en el desarrollo del presente documento, que ha sido financiado por el Ministerio de Hacienda y Función Pública.

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

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

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

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

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

Octubre de 2018

Félix Sanz Roldán
Secretario de Estado
Director del Centro Criptológico Nacional

ÍNDICE

1. INTRODUCCIÓN

1. El Informe Nacional del Estado de la Seguridad (INES) de los sistemas de las tecnologías de la información y la comunicación responde a lo previsto en el artículo 35 del Real Decreto 3/2010, de 8 de enero, modificado por el RD 951/2015, de 23 de octubre, por el que se regula el Esquema Nacional de Seguridad (ENS), al que se refiere el apartado segundo del artículo 156 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público:

   Artículo 35. Informe del estado de la seguridad.

   El Comité Sectorial de Administración Electrónica recogerá la información relacionada con el estado de las principales variables de la seguridad en los sistemas de información a los que se refiere el presente Real Decreto, de forma que permita elaborar un perfil general del estado de la seguridad en las Administraciones públicas.

   El Centro Criptológico Nacional articulará los procedimientos necesarios para la recogida y consolidación de la información, así como los aspectos metodológicos para su tratamiento y explotación, a través de los correspondientes grupos de trabajo que se constituyan al efecto en el Comité Sectorial de Administración Electrónica y en la Comisión de Estrategia TIC para la Administración General del Estado.

2. Los organismos a los que se aplica el ENS de acuerdo con el artículo 2 de la citada Ley 40/2015, están obligados a cumplimentar dicho informe, en los términos que refleja la Resolución de 7 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de Informe del Estado de la Seguridad.

   Artículo 2. Ámbito Subjetivo.

   1. La presente Ley se aplica al sector público que comprende:

   a) La Administración General del Estado.
   b) Las Administraciones de las Comunidades Autónomas.
   c) Las Entidades que integran la Administración Local.
   d) El sector público institucional.

   2. El sector público institucional se integra por:

   a) Cualesquiera organismos públicos y entidades de derecho público vinculados o dependientes de las Administraciones Públicas.
   b) Las entidades de derecho privado vinculadas o dependientes de las Administraciones Públicas que quedarán sujetas a lo dispuesto en las normas de esta Ley que específicamente se refieran a las mismas, en particular a los principios previstos en el artículo 3, y en todo caso, cuando ejerzan potestades administrativas.
   c) Las Universidades públicas que se regirán por su normativa específica y supletoriamente por las previsiones de la presente Ley.

   3. Tienen la consideración de Administraciones Públicas la Administración General del Estado, las Administraciones de las Comunidades Autónomas, las Entidades que integran la Administración Local, así como los organismos públicos y entidades de derecho público previstos en la letra a) del apartado 2.

3. El anexo II del ENS exige establecer un sistema de medición de la seguridad del sistema, en función de la categoría que ha sido asignada al sistema (consultar CCN-STIC-803 '*Valoración de Sistemas*').

Categoría del sistema	*BÁSICA*	*MEDIA*	*ALTA*
Sistema de métricas op.mon.2	*aplica*	*+*	*++*

Figura 1.- Sistema de métricas

Categoría Básica
Se recopilarán los datos necesarios atendiendo a la categoría del sistema para conocer el grado de implantación de las medidas de seguridad que apliquen de las detalladas en el Anexo II y, en su caso, para proveer el informe anual requerido por el artículo 35.

Categoría Media
Además, se recopilarán datos para valorar el sistema de gestión de incidentes, permitiendo conocer:
- *Número de incidentes de seguridad tratados.*
- *Tiempo empleado para cerrar el 50% de los incidentes.*
- *Tiempo empleado para cerrar el 90% de los incidentes.*

Categoría Alta
Se recopilarán datos para conocer la eficiencia del sistema de seguridad TIC, en términos de recursos consumidos: horas y presupuesto.

4. Este documento describe una serie de medidas e indicadores con 2 destinatarios:
   - el propio organismo propietario del sistema de información.
   - el informe anual del estado de seguridad del sector público español.
5. En ambos casos se busca:
   - una estimación preventiva de la seguridad, vía análisis del cumplimiento de determinados aspectos que se han estimado críticos para cualquier organismo.
   - una estimación de la eficacia y eficiencia de las actividades llevadas a cabo en materia de seguridad.
   - una estimación del esfuerzo humano y económico dedicado a seguridad TIC.
6. Para algunos indicadores se marcan:
   - líneas amarillas que detectan una deficiencia leve, un problema potencial que debe estudiarse antes de que sea grave.
   - líneas rojas que detectan una deficiencia grave que debe corregirse a la mayor brevedad posible.
7. Se prevé recopilar esta información anualmente sobre un amplio espectro del sector público español y no solo de las Administraciones públicas como hasta ahora, de forma que podamos al cabo de unos años ver la evolución del país, y que cada organismo pueda

cotejar su posición particular respecto de la media nacional y la media del su propio ámbito (Administración General del Estado, Comunidades Autónomas, Entidades Locales y Universidades).

8. A tal fin, las herramientas PILAR (de análisis y gestión de riesgos), LUCÍA (de gestión de ciberincidentes) y otras, incorporarán mecanismos para recopilar y exportar los indicadores que les competan, facilitando la recopilación de datos solicitados en INES.
9. Las métricas e indicadores presentados en esta guía derivan del marco descrito en la guía CCN-STIC-815 *'ENS - Métricas e Indicadores'*.

2. MÉTRICAS BÁSICAS

10. Esta sección describe algunas métricas que se van a usar en diferentes indicadores.

2.1 NIVELES DE MADUREZ

11. Es habitual el empleo de niveles de madurez para caracterizar la implementación de un proceso. El modelo de madurez (CMM)[1] permite describir las características que hacen un proceso efectivo, midiendo el grado o nivel de profesionalización de la actividad.
12. En varios indicadores de la herramienta INES se utilizan los niveles de madurez para evaluarlos y en varias fórmulas que agregan datos para derivar indicadores se traduce dicho nivel de madurez por un porcentaje.
13. Los niveles identificados son los siguientes:

Nivel de Madurez de la medida de seguridad		Breve descripción del Nivel
Nivel	%	
L0	0	***Inexistente***. Esta medida no existe o no se está siendo aplicada en este momento.
L1	10	***Inicial/ad hoc***. En el nivel L1 de madurez, el proceso existe, pero no se gestiona. Cuando la organización no proporciona un entorno estable. El éxito o fracaso del proceso depende de la competencia y buena voluntad de las personas y es difícil prever la reacción ante una situación de emergencia. En este caso, las organizaciones exceden con frecuencia presupuestos y tiempos de respuesta. El éxito del nivel L1 depende de tener personal de alta calidad.

[1] CMM - *Capability Maturity Model*, Carnegie Mellon University, CMU. Modelo de madurez de capacidad o proceso

Nivel de Madurez de la medida de seguridad		Breve descripción del Nivel
Nivel	%	
L2	50	***Reproducible, pero intuitivo***. En el nivel L2 de madurez, la eficacia del proceso depende de la buena suerte y de la buena voluntad de las personas. Existe un mínimo de planificación que proporciona una pauta a seguir cuando se repiten las mismas circunstancias. Es impredecible el resultado si se dan circunstancias nuevas. Todavía hay un riesgo significativo de exceder las estimaciones de coste y riesgo.
L3	80	***Proceso definido***. Se dispone un catálogo de procesos que se mantiene actualizado. Estos procesos garantizan la consistencia de las actuaciones entre las diferentes partes de la organización, que adaptan sus procesos particulares al proceso general. Hay normativa establecida y procedimientos para garantizar la reacción profesional ante los incidentes. Se ejerce un mantenimiento regular. Las oportunidades de sobrevivir son altas, aunque siempre queda el factor de lo desconocido (o no planificado). El éxito es algo más que buena suerte: se merece. Una diferencia importante entre el nivel 2 y el nivel 3 es la coordinación entre departamentos y proyectos, coordinación que no existe en el nivel 2, y que se gestiona en el nivel 3.
L4	90	***Gestionado y medible.*** Cuando se dispone de un sistema de medidas y métricas para conocer el desempeño (eficacia y eficiencia) de los procesos. La Dirección es capaz de establecer objetivos cualitativos a alcanzar y dispone de medios para valorar si se han alcanzado los objetivos y en qué medida. En el nivel L4 de madurez, el funcionamiento de los procesos está bajo control con técnicas estadísticas y cuantitativas. La confianza es cuantitativa, mientras que en el nivel L3, la confianza era solamente cualitativa.
L5	100	***Optimizado***. El nivel L5 de madurez se centra en la mejora continua de los procesos con mejoras tecnológicas incrementales e innovadoras. Se establecen objetivos cuantitativos de mejora. Y se revisan continuamente para reflejar los cambios en los objetivos de negocio, utilizándose como indicadores en la gestión de la mejora de los procesos. En este nivel la organización es capaz de mejorar el desempeño de los sistemas a base de una mejora continua de los procesos basada en los resultados de las medidas e indicadores.

Figura 2.- Niveles de madurez y equivalencia en %

14. A continuación, se recoge un ejemplo de determinación de niveles de madurez. El ejemplo está basando en la gestión de un cortafuegos implantado en el sistema como salvaguarda:

- No aplica nivel: No hay interconexión y, por tanto, el cortafuegos no es necesario.
- L0 (0%): El sistema está interconectado pero el cortafuegos requerido no ha sido implantado en la interconexión.
- L1 (10%): El cortafuegos está implantado en la interconexión con los valores por defecto y sin realizar ningún mantenimiento sobre el mismo.
- L2 (50%): El cortafuegos es revisado temporalmente sin tener un procedimiento establecido para ello.
- L3 (80%): El cortafuegos es revisado de la forma y con la periodicidad establecida en el procedimiento documentado.
- L4 (90%): El procedimiento de gestión del cortafuegos es analizado temporalmente para determinar su eficacia y eficiencia.
- L5 (100%): El procedimiento de gestión del cortafuegos es mejorado periódicamente en función de los análisis de eficacia y eficiencia.

15. Los niveles mínimos de madurez requeridos por el Esquema Nacional de Seguridad en función de la categoría del sistema son:

Categoría del sistema	Nivel mínimo de madurez requerido
BÁSICA	L2 – Reproducible, pero intuitivo (50%)
MEDIA	L3 – Proceso definido (80%)
ALTA	L4 – Gestionado y medible (90%)

Figura 3.- Niveles mínimos de madurez del sistema requeridos en el Esquema Nacional de Seguridad

16. Umbrales de madurez de la categoría de un sistema.

Categoría del Sistema	Rojo	Amarillo	Nivel Adecuado
BÁSICA	< 40%	< 50%	≥50% (L2 o superior)
MEDIA	< 70%	< 80%	≥80% (L3 o superior)
ALTA	< 80%	< 90	≥90% (L4 o superior)

Figura 4.- Umbrales de madurez del sistema

2.2 NIVEL DE IMPACTO DE UN INCIDENTE

17. Un incidente de seguridad tiene un cierto impacto sobre el sistema de información.
18. Los niveles de impacto de un incidente de acuerdo a los criterios de determinación de la guía CCN-STIC 817 *'Gestión de Ciberincidentes'* son los descritos a continuación:

Nivel de impacto de un incidente	Descripción
I0 – IRRELEVANTE	No hay impacto apreciable sobre el sistema. No hay daños reputacionales apreciables.
I1 – BAJO	La categoría más alta de los sistemas de información afectados es BÁSICA. El ciberincidente precisa para resolverse menos de 1 JP[2]. Daños reputacionales puntuales, sin eco mediático.
I2 – MEDIO	La categoría más alta de los sistemas de información afectados es MEDIA. Afecta a más de 10 equipos con información cuya máxima categoría es BÁSICA. El ciberincidente precisa para resolverse entre 1 y 10 JP. Daños reputacionales apreciables, con eco mediático (amplia cobertura en los medios de comunicación).
I3 – ALTO	La categoría más alta de los sistemas de información afectados es ALTA. Afecta a más de 50 equipos con información cuya máxima categoría es BÁSICA. Afecta a más de 10 equipos con información cuya máxima categoría es MEDIA. El ciberincidente precisa para resolverse entre 10 y 20 JP. Daños reputacionales de difícil reparación, con eco mediático (amplia cobertura en los medios de comunicación) y afectando a la reputación de terceros.
I4 – MUY ALTO	Afecta a sistemas clasificados RESERVADO. Afecta a más de 100 equipos con información cuya máxima categoría es BÁSICA. Afecta a más de 50 equipos con información cuya máxima categoría es MEDIA. Afecta a más de 10 equipos con información cuya máxima categoría es ALTA. El ciberincidente precisa para resolverse entre 20 y 50 JP. Daños reputacionales a la imagen del país (marca España). Afecta apreciablemente a actividades oficiales o misiones en el extranjero. Afecta apreciablemente a una infraestructura crítica.
I5 - CRÍTICO	Afecta a sistemas clasificados SECRETO. Afecta a más de 100 equipos con información cuya máxima categoría es MEDIA. Afecta a más de 50 equipos con información cuya máxima categoría es ALTA. Afecta a más de 10 equipos con información clasificada RESERVADO. El ciberincidente precisa para resolverse más de 50 JP. Afecta apreciablemente a la seguridad nacional. Afecta gravemente a una infraestructura crítica.

Figura 5.- Nivel de impacto de un incidente

[2] JP – Jornada-persona; estimación del esfuerzo necesario para realizar una tarea cuya unidad equivale a una jornada de trabajo ininterrumpido de un trabajador medio.

3. CARACTERIZACIÓN DEL SISTEMA DE INFORMACIÓN

19. En esta sección se trata de caracterizar el sistema de información evaluado. Tiene interés a efectos estadísticos, aunque también proporciona una foto de alto nivel de lo que maneja el organismo.

3.1 IDENTIFICACIÓN

20. Datos generales:
    - Nombre del organismo completo incluyendo el nivel más alto orgánico del que depende.
    - Número de identificación fiscal (NIF/CIF).
    - Directorio Común de Unidades Orgánicas y Oficinas (DIR3).
    - Tipo de organismo (el que más se ajuste):
        - Organismo estatal independiente
        - Administración General del Estado (AGE), organismo dependiente de la AGE.
        - Administración General del Estado (AGE), Confederación Hidrográfica.
        - Administración General del Estado (AGE), Autoridad Portuaria.
        - Comunidades y ciudades autonómicas (CC.AA.), entidades locales u organismo dependiente de CC.AA.
        - Entidades locales (EE.LL.): Diputaciones provinciales y cabildos, ayuntamientos (desglosados por número de habitantes: x <20.000, 20.000> x< 75.000, x>75.000) y organismos dependientes de EE.LL.
        - Universidades y organismos dependientes de Universidades.
        - Confederación Hidrográfica (AGE-CH)
        - Autoridad Portuaria (AGE-AP)
    - Responsable de la seguridad:
        - nombre y apellidos.
        - correo electrónico.
        - teléfonos de contacto.
    - Número de sistemas de cada categoría (BÁSICA, MEDIA y ALTA) cuyos datos agrupados se incluyen dentro de una misma ficha.
    - Número total de usuarios con acceso al sistema de información: Es el número de usuarios con acceso al sistema de información se puede medir por el número de cuentas en el sistema, asumiendo que el número de cuentas por persona es prácticamente uno, aunque los administradores de seguridad además dispongan de otras cuentas de servicio.

Identificación	Datos

Identificación	Datos
Nombre del organismo completo incluyendo el nivel más alto orgánico del que depende.	
Número de identificación fiscal (**NIF/CIF**).	
Directorio Común de Unidades Orgánicas y Oficinas (DIR3)	
Tipo de organismo: – Organismo estatal independiente – Administración General del Estado (AGE), organismo dependiente de la AGE. – Comunidades y ciudades autonómicas (CC.AA.), entidades locales u organismo dependiente de CC.AA. – Entidades locales (EE.LL.): Diputaciones provinciales y cabildos, ayuntamientos (desglosados por número de habitantes: <20.000, 20.000> x< 75.000, >75.000), organismos dependientes de EE.LL. – Universidades, organismos dependientes de Universidades. – Confederación Hidrográfica (AGE-CH) – Autoridad Portuaria (AGE-AP)	
Responsable de la seguridad: – nombre y apellidos. – correo electrónico. – teléfonos de contacto.	
Número total de sistemas de cada categoría (BÁSICA, MEDIA y ALTA) cuyos datos agregados se incluyen dentro de una misma ficha INES.	
Número total de usuarios con acceso al conjunto de los sistemas de información incluidos en una misma ficha INES.	

Figura 6.- Identificación

3.2 CATEGORÍA DEL SISTEMA BASADA EN LA VALORACIÓN DE ACTIVOS ESENCIALES

21. A los sistemas de las tecnologías de la información y la comunicación de los organismos del sector público, obligados al cumplimiento del ENS, se les asigna una categoría en función de la valoración del impacto que tendría un incidente que afectara a la seguridad de la información o de los servicios con perjuicio para la confidencialidad, integridad, trazabilidad, autenticidad o disponibilidad, como dimensiones de seguridad, siguiendo el procedimiento establecido en el Anexo I del ENS.

22. Por cada activo esencial, sea de tipo información o de tipo servicio, se solicita la valoración de su nivel (bajo, medio o alto) o no adscrito a ningún nivel en cada dimensión de seguridad (D (Disponibilidad), A (Autenticidad), I (Integridad), C (Confidencialidad), y T (Trazabilidad). Ver Anexo I del ENS y guía CCN-STIC 803. Valoración de los sistemas. Por ejemplo, un activo tipo información no estará adscrito a ningún nivel en la dimensión de seguridad Confidencialidad si la información de la que se trate es de carácter público, accesible por cualquier persona.

23. Los niveles de seguridad asociados a las dimensiones se asignarán de forma individual para cada una de las categorías de las cuales el organismo ha declarado tener algún sistema.

24. Cuando un sistema maneje diferentes informaciones y preste diferentes servicios, el nivel del sistema en cada dimensión será el mayor de los establecidos para cada información y cada servicio.
25. 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.
26. La categoría del sistema (BÁSICA, MEDIA o ALTA) se corresponde con el mayor nivel de cualquiera de las dimensiones de seguridad valoradas en cada activo esencial.
27. La determinación de la categoría de un sistema no implica que se altere el nivel de las dimensiones de seguridad que no han influido en la determinación de dicha categoría, aunque si se verán afectadas por una mayor exigencia en el nivel de madurez que deben alcanzar.
28. A continuación, se presenta la nomenclatura utilizada para indicar los niveles de seguridad asociados a las dimensiones de seguridad, junto con la categoría resultante:

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

Figura 7.- Categoría del sistema junto a los niveles de sus dimensiones de seguridad

4. ANÁLISIS Y GESTIÓN DE RIESGOS

29. Se debe informar de si se ha realizado un análisis de riesgos proporcional a la categoría del sistema (bastará un análisis informal para categoría Básica, semi-formal para categoría Media o formal para categoría Alta) en el que se identifique, como mínimo lo siguiente:
    - Los activos más valiosos del sistema.
    - Las amenazas más probables.
    - Las salvaguardas que protegen dichas amenazas.
    - La valoración del riesgo residual
30. Se solicita información para conocer si el análisis de riesgos está actualizado al último año.

Análisis y gestión de riesgos	Datos
El análisis de riesgos del sistema esta actualizado al último año	Si/No
Número de activos totales en el análisis de riesgos	Número
Número de activos esenciales identificados	Número
Porcentaje de activos esenciales incluidos en un análisis de riesgos actualizado en el último año	%

Figura 8.- Análisis y gestión de riesgos

5. ACTIVIDADES ORGANIZATIVAS

31. Se analizan varias actividades organizativas, estableciéndose una escala cualitativa de valoración en 6 niveles.

32. Para valorar las actividades organizativas se utiliza la escala en tanto por ciento (%).

Porcentaje de avance %	Descripción del nivel
0	*No se ha iniciado la actividad.*
10	*La actividad está solamente iniciada*.
50	*La actividad está a medias*.
80	*La actividad está muy avanzada.*
90	*La actividad está prácticamente acabada.*
100	*La actividad está completa.*

Figura 9.- Escala de valoración de las actividades organizativas

33. Actividades organizativas a considerar:

- Roles y Responsabilidades: El responsable de la seguridad es independiente del responsable del sistema. Verificar si están designados formalmente / informalmente estas figuras según el ENS y que existe independencia entre ellas. Esta designación es de carácter obligatorio dentro del Esquema.
- Política de Seguridad: Se dispone de una política de seguridad aprobada. Se debe aportar esta política y se verifica si está aprobada por la autoridad correspondiente.
- Declaración de Aplicabilidad: Se dispone de una declaración de aplicabilidad actualizada que contiene el inventario de medidas del Anexo II que aplican al Sistema en función de su categoría firmado por el responsable de la seguridad del sistema.
- Plan de Adecuación: Se mantiene actualizado el plan de adecuación. Se debe aportar este plan de adecuación aprobado por la dirección. Se ha verificado si cumple con CCN-STIC 806.
- Normas de seguridad implantadas. Se debe aportar el (%) de las normas de seguridad implantadas. Consultar guía CCN-STIC 821.
- Procedimientos de seguridad implantados. Se debe aportar el (%) de los procedimientos de seguridad implantados. Consultar guía CCN-STIC 822.

Actividades organizativas	Datos
Roles y responsabilidades: El responsable de la seguridad es independiente del responsable del sistema	SI/NO

Política de Seguridad: Se dispone de una política de seguridad aprobada	L0...L5
Porcentaje de normas de seguridad implantadas	%
Porcentaje de procedimientos de seguridad implantados	%
Declaración de aplicabilidad: Se dispone de una declaración de aplicabilidad en actualizada	L0...L5
Plan de adecuación: Se mantiene actualizado el plan de adecuación	L0...L5

Figura 10.- Actividades organizativas

34. Es muy difícil establece porcentajes de implantación por lo que el responsable de la seguridad realizará una estimación aproximada.

6. RECURSOS

6.1 EQUIPO DE SEGURIDAD

35. Se solicita información sobre el número de administradores de seguridad y el número de personas con responsabilidad en la seguridad TIC.
36. El número de administradores de seguridad TIC son el número de personas con permisos de administrador sobre la seguridad del sistema o de algún componente del sistema (se incluyen tanto servidores como equipos de usuario final y los que administran productos de seguridad).
37. El número de personas con responsabilidad en la seguridad TIC incluye el número de administradores de seguridad, y personas con otras actividades de seguridad TIC, como responsables, directivos, sin ser administradores de seguridad propiamente dicho.
38. No se consideran administradores de seguridad y por tanto se excluyen aquellas personas que dentro de una aplicación específica su rol es el de administrador de dicha aplicación (por ejemplo, controlando los cambios de claves de las cuentas de usuarios de su departamento).
39. No se hará distinciones en función de la categoría de la persona. Suma lo mismo personal fijo o temporal, propio, desplazado o subcontratado. Cuando se subcontraten servicios de seguridad, se imputarán también los recursos humanos indicados en el contrato de prestación de servicios.

Equipo de seguridad TIC	
Número de administradores de seguridad	
Número de personas con responsabilidad en la STIC	

Figura 11. Equipo de seguridad

6.2 RECURSOS DEDICADOS A SEGURIDAD TIC SOBRE TOTAL DE TIC

40. Se solicita la declaración de la siguiente información:

- Estimación de la fracción en horas dedicadas a Seguridad de las Tecnologías de la Información y la Comunicación, en el último periodo anual, sobre el total de horas dedicadas a las Tecnologías de la Comunicación y la Información.
- Estimación del presupuesto global TIC dedicado a Seguridad de las TIC.

Recursos dedicados a Seguridad TIC sobre el total de recursos dedicados a TIC	
Fracción de horas (en el último periodo anual)	%
Fracción del presupuesto (en el último periodo anual)	%

Figura 12.- Recursos dedicados a Seguridad TIC (%)

41. Umbrales: Cada organismo puede comprobar su ubicación en la siguiente escala de rangos, donde se indican los umbrales verde, amarillo y rojo, inferior y superior, para cada categoría de sistema.

Categoría	< 1%	1% - 2%	2% - 4%	4% - 8%	8% - 16%	> 16%
BÁSICA						
MEDIA						
ALTA						

Figura 13.- Umbrales del porcentaje de recursos dedicados a la STIC respecto a los dedicados a las TIC

42. Son datos anuales, bien porque son estables a lo largo del año, bien sumando los datos de cada periodo. No cabe esperar una precisión superior al ±10%.
43. Dedicación TIC incluye todas las tareas relacionadas con Tecnologías de la Información y Comunicaciones:
    - tareas técnicas
    - tareas administrativas, incluyendo contratación de personas, bienes y servicios.
    - tareas docentes (formación)
44. Dedicación STIC incluye todas las tareas relacionadas con la Seguridad de las TIC. Pueden usarse las tareas a las que hace mención el ENS como inventario:
    - tareas técnicas: preventivas y de resolución de incidentes.
    - tareas administrativas, incluyendo contratación de personas, bienes y servicios.
    - tareas de concienciación y formación.
    - tareas de comunicación con las autoridades.
45. No se hará distinciones en función de la categoría de la persona. Suma lo mismo personal fijo o temporal, propio, desplazado o subcontratado. Cuando se subcontraten servicios, se imputará la carga de trabajo indicada en el contrato de prestación de servicios.
46. Este indicador es predictivo. Una deficiencia de recursos es una invitación a tener problemas y dificultades para solucionar los incidentes. No obstante, no se dispone de suficiente información de dónde deben estar las líneas amarillas y rojas. Probablemente los umbrales haya que revisarlos tras analizar los resultados obtenidos en las sucesivas campañas.

47. En todo caso deben usarse para que los organismos busquen recursos o reubiquen los recursos disponibles, en caso de debilidad.

6.3 DESGLOSE DEL PRESUPUESTO STIC

48. Se solicita información sobre el desglose del presupuesto de seguridad TIC dedicado a:

    - Concienciación y formación.
    - Subcontratación de personal externo.
    - Contratación de servicios de seguridad.
    - Adquisición y mantenimiento de productos de STIC.

49. Son datos anuales, bien porque son estables a lo largo del año, bien promediando los datos de cada periodo. No cabe esperar una precisión superior al ±10%. El desglose del presupuesto en STIC debe sumar 100%.

50. La contratación de servicios de seguridad abarca:

    - Servicios de asesoría, consultoría o auditoría (incluyendo *hacking* ético, test de penetración (*pen-testing* o *penetration testing*), peritaje, etc.) sobre aspectos específicos de seguridad.
    - Servicios de externalización de procesos de seguridad (Centro de Operaciones de Seguridad (*Security Operations Center SOC*), Equipo de respuesta rápida ante incidentes informáticos (*Computer Emergency Response Team CERT*, etc.).

51. La adquisición y mantenimiento de productos de seguridad incluye todos los productos tecnológicos cuya finalidad principal es la seguridad:

    - Gestores de identidades y accesos, gestores de contraseñas, herramientas contra código dañino y correo basura, cifrado, firma electrónica, sellado de tiempo, cortafuegos (*firewall*), Sistemas de detección de intrusiones (*Intrusion Deteccion Systems IDS*), Sistemas de prevención de intrusiones (*Intrusion Prevention Systems IPS*), Sistemas de Información de Seguridad y Administración de eventos (*Security Information and Event Management SIEM*), filtros de contenidos, equipos y sistemas trampa (*Honeypot*), limpieza de metadatos, herramientas de auditoría, etc.

Fracción del presupuesto STIC dedicado a:	
Concienciación y formación	%
Subcontratación de personal externo	%
Servicios externos de seguridad	%
Adquisición y mantenimiento de productos STIC	%
Total	100%

Figura 14.- Distribución de recursos dedicados a Seguridad TIC (%)

7. CUMPLIMIENTO DE LAS MEDIDAS DEL ANEXO II DEL ENS

52. Para cada medida aplicada, se debe indicar su nivel de madurez de acuerdo a lo establecido en la sección 2.1. El conjunto de estos valores individuales de valoración de cada medida de seguridad es utilizado posteriormente para calcular el Índice de Madurez del sistema, verdadera medida de seguridad.

53. En algunas medidas, de forma excepcional, se puede seleccionar "No aplica". Esta opción está disponible en todas las medidas y debe marcarse cuando, por las características del sistema, la implantación de una medida carecería de sentido. Un ejemplo sería la implantación de la medida *[mp.com.1] Perímetro Seguro* para sistemas aislados sin conexión con el exterior.

54. Para aquellos casos en los que, por los niveles y categoría asignados al sistema, haya algunas medidas que no le sean de aplicación para cumplir con el ENS, los valores deben ser rellenados ya que serán contabilizados para el cálculo de su Indicador de Madurez (IM), aunque no para el Indicador de Cumplimiento (IC). Para más información, se puede consultar el apartado 14 de este documento y el Anexo B en el que se incluyen ejemplos del cálculo de los citados indicadores.

55. El nivel de madurez de las medidas de seguridad se solicitará de forma independiente para cada uno de las categorías para las cuales el organismo ha declarado tener algún sistema. De esta forma, si un organismo, por ejemplo, cuenta con sistemas de categoría MEDIA y ALTA, obtendrá dos (2) IM y dos (2) IC. Es decir, por cada categoría habrá un IM y un IC.

7.1 MEDIDAS DEL MARCO ORGANIZATIVO:

Medidas Anexo II - Marco Organizativo		Nivel de madurez
Medidas marco organizativo	org	Valor medio org
Política de Seguridad	org.1	
Normativa de Seguridad	org.2	
Procedimientos de Seguridad	org.3	
Proceso de Autorización	org.4	

Figura 15.- Medidas Anexo II - Marco Organizativo

56. Respecto a los procesos de autorización se recuerda que se refiere a que se disponga de un proceso formal de autorizaciones que cubra todos los elementos del sistema de información, como son: utilización de instalaciones, medios de comunicación habituales y alternativos, entrada de equipos o aplicaciones en producción, establecimiento de enlaces con otros sistemas, utilización de soportes, medios etc. Ver Anexo II del ENS medida [org.4].

7.2 MEDIDAS DEL MARCO OPERACIONAL:

Medidas Anexo II - Marco Operacional	Nivel de madurez

Medidas Anexo II - Marco Operacional		Nivel de madurez
Planificación	**op.pl**	**Valor medio p.pl**
Análisis de Riesgos	op.pl.1	
Arquitectura de Seguridad	op.pl.2	
Adquisición de nuevos componentes	op.pl.3	
Dimensionamiento - Gestión de capacidades	op.pl.4	
Componentes certificados	op.pl.5	
Control de acceso	**op.acc**	**Valor medio op.acc**
Identificación	op.acc.1	
Requisitos de acceso	op.acc.2	
Segregación de funciones y tareas	op.acc.3	
Proceso de gestión de derechos de acceso	op.acc.4	
Mecanismo de autenticación	op.acc.5	
Acceso local	op.acc.6	
Acceso remoto	op.acc.7	
Explotación	**op.exp**	**Valor medio op.exp**
Inventario de activos	op.exp.1	
Configuración de seguridad.	op.exp.2	
Gestión de la configuración	op.exp.3	
Mantenimiento	op.exp.4	
Gestión de cambios	op.exp.5	
Protección frente a código dañino	op.exp.6	
Gestión de incidentes	op.exp.7	
Registro de la actividad de los usuarios	op.exp.8	
Registro de la gestión de incidentes	op.exp.9	
Protección de los registros de actividad	op.exp.10	
Protección de claves criptográficas	op.exp.11	
Servicios externos	**op.ext**	**Valor medio op.ext**
Contratación y acuerdos de nivel de servicio	op.ext.1	
Gestión diaria	op.ext.2	
Medios alternativos	op.ext.9	
Continuidad del servicio	**op.cont**	**Valor medio op.cont**

Medidas Anexo II - Marco Operacional		Nivel de madurez
Análisis de Impacto	op.cont.1	
Plan de Continuidad	op.cont.2	
Pruebas periódicas	op.cont.3	
Monitorización del sistema	**op.mon**	**Valor medio op.mon**
Detección de intrusión	op.mon.1	
Sistema de métricas	op.mon.2	

Figura 16- Medidas Anexo II - Marco Operacional

7.3 MEDIDAS DE PROTECCIÓN:

Medidas Anexo II - Medidas de Protección		Nivel de madurez
Protección de las instalaciones e infraestructuras	**mp.if**	**Valor medio mp.if**
Áreas separadas y con control de acceso	mp.if.1	
Identificación de las personas	mp.if.2	
Acondicionamiento de los locales	mp.if.3	
Energía eléctrica	mp.if.4	
Protección frente a incendios	mp.if.5	
Protección frente a inundaciones	mp.if.6	
Registro de entrada y salida de equipamiento	mp.if.7	
Instalaciones alternativas	mp.if.9	
Gestión del personal	**mp.per**	**Valor medio mp.per**
Caracterización del puesto de trabajo	mp.per.1	
Deberes y obligaciones	mp.per.2	
Concienciación	mp.per.3	
Formación	mp.per.4	
Personal alternativo	mp.per.9	
Protección de los equipos	**mp.eq**	**Valor medio mp.eq**
Puesto de trabajo despejado	mp.eq.1	
Bloqueo del puesto de trabajo	mp.eq.2	
Protección de equipos portátiles	mp.eq.3	
Medios alternativos	mp.eq.9	
Protección de las comunicaciones	**mp.com**	**Valor medio mp.com**

Medidas Anexo II - Medidas de Protección		Nivel de madurez
Perímetro seguro	mp.com.1	
Protección de la confidencialidad	mp.com.2	
Protección de la autenticidad y de la integridad	mp.com.3	
Segregación de redes	mp.com.4	
Medios alternativos	mp.com.9	
Protección de los soportes de información	**mp.si**	**Valor medio mp.si**
Etiquetado	mp.si.1	
Criptografía	mp.si.2	
Custodia	mp.si.3	
Transporte	mp.si.4	
Borrado y destrucción	mp.si.5	
Protección de aplicaciones informáticas	**mp.sw**	**Valor medio mp.sw**
Desarrollo de aplicaciones	mp.sw.1	
Aceptación y puesta en servicio	mp.sw.2	
Protección de la información	**mp.info**	**Valor medio mp.info**
Datos de carácter personal	mp.info.1	
Calificación de la información	mp.info.2	
Cifrado de la información	mp.info.3	
Firma electrónica	mp.info.4	
Sellos de tiempo	mp.info.5	
Limpieza de documentos	mp.info.6	
Copias de seguridad (backup)	mp.info.9	
Protección de los servicios	**mp.s**	**Valor medio mp.s**
Protección del correo electrónico (e-mail)	mp.s.1	
Protección de servicios y aplicaciones web	mp.s.2	
Protección frente a la denegación de servicio	mp.s.8	
Medios alternativos	mp.s.9	

Figura 17.- Medidas Anexo II - Medidas de protección

8. INTERCONEXIÓN CON OTROS SISTEMAS

57. Se usará como referencia la guía CCN-STIC 811 *'Interconexión en el ENS'*, que es de aplicación a aquellos sistemas de información que se conectan a otros para intercambiar

datos y servicios. Para el informe INES nos centraremos en la interconexión de nuestra red con Internet.

58. La primera pregunta determina si está sección es aplicable o no:

Descripción	Selección
Indique de qué forma se conecta su organismo a Internet, en su caso.	☐ No se tiene conexión a Internet ☐ Si, conexión directa a Internet (sin mediación de otro organismo o ente) ☐ Si, conexión indirecta, a través de otro organismo o ente. Si es a través de otro organismo o ente, indique cuál : (CIF / nombre)

Figura 18.- Conexión a Internet

59. Si la respuesta a esta primera pregunta es distinta de SÍ, las secciones 8.1 y 8.2 no aplican (n.a.).

8.1 ARQUITECTURA DE PROTECCIÓN PERIMETRAL

60. Si tiene conexión directa a Internet, indique cómo. Se marca la arquitectura de la frontera que corresponda.

Tipo	Arquitectura de protección perímetro	Seleccionar
APP-1	Un (1) cortafuego (*firewall)*	☐
APP-2	Un (1) intermediario (*proxy*)	☐
APP-3	Un (1) cortafuego (*firewall*), un (1) intermediario (*proxy*)	☐
APP-4	Zona desmilitarizada (*DMZ*) con un (1) cortafuego (*firewall*), un (1) intermediario (*proxy*)	☐
APP-5	Zona desmilitarizada (DMZ) con dos (2) cortafuegos de diferente fabricante(*firewall*), un (1) intermediario (*proxy*)	☐
OTRA	Otra arquitectura: indique tipo	texto

Figura 19.- Arquitectura de protección de perímetro

61. Para la arquitectura que se haya seleccionado, indique la madurez de los procesos de implantación y operación asociados a la misma.

Descripción	Nivel de madurez
Indique nivel de madurez de la arquitectura de protección de perímetro	

Figura 20.- Nivel de madurez de la arquitectura de protección de perímetro

8.2 HERRAMIENTAS DE SEGURIDAD

62. Se debe indicar las herramientas de seguridad implantadas en el Sistema. Se solicita valorar la madurez del despliegue de herramientas de seguridad en los servicios de protección de perímetro o frontera: L0…L5. En caso de que alguna de las herramientas no esté implantada, se debe indicar (L0).

63. Si la herramienta es obligatoria por categoría del sistema, pero no está desplegada, la madurez es también L0, tanto si no se ha desplegado por falta de recursos, como si no se ha desplegado porque parece desproporcionada. Ver guía CCN-STIC 811 '*Interconexión en el ENS*'.

Herramientas de seguridad	Nivel de madurez
Herramienta anti código dañino	
Análisis de vulnerabilidades	
Análisis de los registros de actividad (*logs*)	
IDS[3] / IPS[4] – Detección y prevención de intrusión	
Monitorización de tráfico	
Verificación de la configuración de seguridad	
DLP – Prevención de fuga de datos	

Figura 21.- Herramientas de seguridad y nivel de madurez

8.3 ACCESO REMOTO DE EQUIPOS

64. Si se permite el acceso de equipos exteriores a través de Internet, responda a las siguientes preguntas. Si no se permite, indique no aplica (n.a.).

65. Si se permite el acceso en claro de equipos exteriores a través de Internet, seleccione L0. Seleccione el nivel de madurez de acuerdo a la sección 2.1 si el acceso se realiza utilizando Redes privadas virtuales (VPN[5]) para valorar los mecanismos y los procesos que soportan dicho tipo de acceso remoto.

Acceso remoto al Organismo	Seleccionar
No hay accesos remotos al Sistema	No aplicable (n.a.)
Se accede en claro (no se usan Redes privadas virtuales)	L0

[3] *IDS – Intrusion Detection System* – Sistema de detección de intrusión.
[4] *IPS – Intrusion Prevention System* – Sistema de prevención de intrusión.
[5] *VPN- Virtual Private Network*. Redes privadas virtuales. Cuando se establecen canales seguros de comunicación a través de la red externa.

Se accede a través de Redes Privadas Virtuales (VPN)	L1…L5

Figura 22.- Acceso remoto de equipos y nivel de madurez

9. APLICACIÓN DE LA SEGURIDAD

9.1 IDENTIFICACIÓN Y AUTENTICACIÓN

66. Con la solicitud de datos de este apartado, se intenta conocer el uso de los diferentes mecanismos de autenticación disponibles en los sistemas. Se contabiliza el tanto por ciento de los tipos de acceso que requiere el usuario para la identificación para utilizar el sistema.

67. Se hace la distinción entre usuarios internos (trabajadores del organismo, propios o subcontratados) y usuarios externos.

9.1.1 USUARIOS INTERNOS

68. Mecanismo de autenticación para usuarios internos (trabajadores del organismo, propios o subcontratados).

69. Para la identificación de los usuarios internos de los sistemas, se recogen los porcentajes (%) de los usuarios que emplean mecanismos de usuario-contraseña (*user*/*password*), tarjetas o dispositivos electrónicos (*tokens*[6]) o biometría. Es decir, sistemas que emplean:

    - Usuario / Contraseñas (*user*/*password*).
    - Tarjetas o dispositivos electrónicos (*tokens*).
    - Biometría.

Organismo	*Usuario / Contraseña*	*Tarjetas o Dispositivos*	Biometría
Usuarios internos	%	%	%

Figura 23.-Identificación personal interno

9.1.2 USUARIOS EXTERNOS

70. Mecanismo de autenticación para usuarios externos: usuarios que no son personal del organismo (trabajadores propios o subcontratados).

71. Para la identificación de usuarios externos, se recogen los porcentajes (%) de los usuarios que emplean usuario-contraseña (*user* /*password*), claves concertadas, tarjetas o dispositivos electrónicos (*tokens*), o doble canal[7]. Es decir, sistemas que emplean:

    - Usuario / Contraseñas (*user*/*password*).
    - Tarjetas o dispositivos electrónicos (*tokens*).

[6] Tarjeta o dispositivo electrónico que utiliza un usuario autorizado para acceder a un sistema informático.

[7] Como por ejemplo contraseñas de un solo uso que se reciben por mensaje corto SMS y que completan la identificación de usuario-contraseña inicial que tienen implantado alunas instituciones.

- Claves concertadas.
- Doble canal.

72. El sistema de claves concertadas permite a los ciudadanos identificarse para realizar trámites administrativos sin necesidad de disponer de certificado electrónico. Para utilizar el sistema de claves concertadas, en primer lugar, deberá realizar la solicitud de clave siguiendo las instrucciones que en cada caso apliquen para la correcta identificación del usuario. Una vez obtenida ésta se podrá utilizar para identificarse como usuario externo (usuario-clave concertada) para los trámites que se establezcan. Ej.: El sistema Cl@ve de la Administración para acceder electrónico a los distintos servicios públicos.

Organismo	*Usuario / Contraseña*	*Tarjetas o Dispositivos*	Claves concertadas	Doble canal
Usuarios externos	%	%	%	%

Figura 24.- Identificación de usuarios externos

9.2 SERVICIOS EXTERNALIZADOS O SUBCONTRATADOS

73. Se solicita información sobre algunos servicios específicos que los organismos puedan tener externalizados, con el fin de determinar el grado de dependencias externas existentes y los tipos de riesgos a los que se puedan enfrentar por dicha circunstancia. Esta información viene recogida en una serie de indicadores.

74. En los servicios externalizados o proporcionados por terceros, no se distingue si lo es por medio de contrato o de convenio.

75. Solo se incluirán los que estén en producción, sin que consten los que estén en pruebas o experimentación.

76. Se marcarán los que apliquen de los siguientes:

- Servicios de comunicaciones
- Servicios de acceso a Internet (*ISP*[8])
- Servicios de alojamiento de servidor web (Sede electrónica)
- Servicios de correo electrónico
- Servicios de copias de seguridad
- Servicios de equipamiento hardware de respaldo
- Servicios de instalaciones de respaldo (centro alternativo)
- Servicios en la nube (*cloud*[9])
- Servicios de identificación y autenticación
- Servicios de firma electrónica
- Servicios de sello de tiempo
- Servicios de seguridad gestionada (monitorización, gestión de registros (logs)….)

[8] *Internet Service Provider* – Proveedor de acceso a Internet.
[9] *Cloud*. Servicios en la nube.

77. También se solicitan las direcciones IP fijas del organismo en su caso, de forma que se pueda determinar ante un incidente de ciberseguridad, si la IP afectada corresponde a un organismo determinado, perteneciente a la comunidad de referencia del Equipo de respuesta del Centro Criptológico Nacional (CCN-CERT).

Servicios externalizados:		Si /No
Comunicaciones		
Acceso a Internet ISP		
Alojamiento del servidor web (Sede electrónica / portal institucional)	*Hosting*[10]	
	Housing[11]	
Correo electrónico		
Copias de seguridad		
Equipamiento de respaldo		
Instalación de respaldo centro alternativo		
Servicios en la nube (cloud)	*SaaS*[12]	
	IaaS[13]	
	PaaS[14]	
Identificación y autenticación		
Firma electrónica		
Sello de tiempo		
Seguridad gestionada		
Indique las direcciones IP fijas de su organismo		

Figura 25- Servicios externalizados

9.3 GESTIÓN DE CAMBIOS

78. Se solicita información sobre el número de veces en el año que se han producido actualizaciones en los distintos servidores, dispositivos de red y equipos de trabajo.

[10] *Hosting* – Hospedaje donde el proveedor proporciona la infraestructura física y lógico.

[11] *Housing* -Hospedaje donde los equipos son del cliente y el proveedor simplemente los acoge en sus instalaciones.

[12] *Software as a Service* – El proveedor proporciona la aplicación software.
[13] *Infrastructure as a Service* – El proveedor proporciona el equipo y el cliente instala desde el sistema operativo en adelante.
[14] *Platform as a Service* – El proveedor proporciona la plataforma y el cliente instala sus aplicaciones

Destacando el tiempo que se tarda en aplicar el 50% y el 90% de las actualizaciones y los casos en que estas llevan más de 30 días sin aplicarse al sistema.

79. Se considera igualmente relevante el porcentaje de equipos y dispositivos de red que tiene sistemas operativos fuera de soporte y que, por tanto, no se realiza mantenimiento de seguridad por parte del fabricante.

Instalación de actualizaciones (parches) de seguridad en el último año	Número[15]	T(50)[16]	T(90)[17]	Sup[18]
Sede electrónica / Portal institucional y servidores Web expuestos a Internet				
En servidores (Web no expuestos a Internet, SQL[19], Controladores de Dominio, etc…)				
En equipos de trabajo				
En los dispositivos de electrónica de red (enrutadores, conmutadores, *firewalls*, etc…)				
Equipos con sistemas operativos fuera de soporte	**Porcentaje**			
Porcentaje de equipos (servidores y estaciones de trabajo) con sistemas operativos fuera de soporte				
Porcentaje de dispositivos de electrónica de red (enrutadores, conmutadores, *firewalls*, etc…) cuyo *firmware* está fuera de soporte.				

Figura 26.- Gestión de cambios

80. Umbrales: Días que se tarda en aplicar las diferentes actualizaciones teniendo en cuenta que aquellas consideradas críticas se aplicarán tan pronto como sea posible.

[15] Número de actualizaciones de cada tipo en el último año. Es decir, suma del número de actualización al año x cada tipo de producto afectado. Se entiende que instalada en la totalidad de los servidores/ equipos de la organización.
[16] T (50): tiempo que se tarda en aplicar el 50% de las actualizaciones
[17] T (90): tiempo que se tarda en aplicar el 90% de las actualizaciones
[18] Sup.: Número de actualizaciones que llevan más de 30 días sin aplicarse al sistema
[19] *Structured Query Language*; en español lenguaje de consulta estructurada

Actualizaciones en	T(50)			T(90)		
	verde	amarillo	rojo	verde	amarillo	rojo
Sede Electrónica	< 5 d	≥ 5 d	≥ 14 d	< 7 d	≥ 7 d	≥ 21 d
Resto servidores	< 15 d	≥ 15 d	≥ 30 d	< 20 d	≥ 20 d	≥ 40 d
Equipos de trabajo	< 10 d	≥ 10 d	≥ 21 d	< 12 d	≥ 12 d	≥ 25 d
Electrónica de red	< 15 d	≥ 15 d	≥ 30 d	< 20 d	≥ 20 d	≥ 40 d

Figura 27.- Gestión de actualizaciones (parches) de seguridad. Umbrales de aplicación en días

9.4 CONTINUIDAD DE OPERACIONES

81. Se solicita información del porcentaje de activos esenciales[20] de nivel Alto incluidos dentro de un análisis de impacto[21] actualizado en el último año, el de los incluidos en el plan de continuidad e información asociada al plan de pruebas asociado al plan de continuidad, que verifique el correcto funcionamiento del plan de continuidad. También se pregunta por el número de horas sin servicio de los activos esenciales de nivel Alto en dicho periodo anual.

82. El número de horas sin servicio de los servicios esenciales de nivel Alto (indisponibilidad) se debe interpretar considerando el tiempo en horas que todos los sistemas de información han estado simultáneamente sin servicio en los últimos 12 meses (cortes de servicio globales). Si no se ha producido ningún corte global, este dato se debe definir como el mínimo de los tiempos que cada uno de los sistemas de información ha estado sin servicio.

Indicadores asociados a la continuidad de operaciones de los activos esenciales de nivel Alto	%/Horas
Porcentaje de activos esenciales de nivel Alto con un análisis de impacto actualizado al último año	%
Porcentaje de activos esenciales de nivel Alto con un plan de continuidad actualizado al último año	%
Porcentaje de activos esenciales de nivel Alto cuyo plan de continuidad ha sido verificado en el último año	%
Número de horas sin servicio (indisponibilidad) en el año de los activos esenciales de nivel Alto	Horas

Figura 28.- Continuidad de operaciones

[20] Ver Guía CCN-STIC 470 I2 PILAR Continuidad. Manual de usuario
[21] Impacto: Consecuencia que sobre un activo tiene la materialización de una amenaza Ver medida op.com continuidad del servicio

9.5 FORMACIÓN Y CONCIENCIACIÓN

83. Se pregunta por el esfuerzo realizado tanto en cursos de formación STIC al equipo de seguridad TIC, como a los cursos de formación y sesiones de concienciación STIC dirigidos a toda la organización, incluida la formación a distancia y los cursos *online* en ambos casos. Ver apartado 6.1 Equipo de seguridad

84. Respecto a las personas pertenecientes al equipo de seguridad (STIC) no se hará distinciones en función de la categoría. Suma lo mismo personal fijo o temporal, propio, desplazado o subcontratado. Cuando se subcontraten servicios de seguridad, se imputará también los recursos humanos indicados en el contrato de prestación de servicios.

85. El resultado de los cálculos para cursos de formación al equipo de seguridad (STIC) se expresa en horas/persona, es decir, por cada curso de formación se calcula el número de horas de formación (incluidos los realizados *online*) multiplicado por número de asistentes. Se suman los totales obtenidos de todos los cursos y el resultado se divide por el número total de personas del equipo de seguridad, obteniendo un factor de horas/persona. Un valor de referencia orientativo para esta formación podría ser 20 horas al año para el equipo de seguridad.

86. El resultado de los cálculos para los cursos de formación o concienciación a todo el personal (incluyendo el personal del equipo STIC) también se expresará en horas/persona. Es decir, por cada curso o sesión de concienciación se calcula el número de horas dedicadas (incluidas los realizados *online*) multiplicado por número de asistentes o destinatarios del curso o sesión. Se suman los totales obtenidos de todos los cursos o sesiones y el resultado se divide por número de personas (ver apartado 9.1.1). Un valor de referencia orientativo para esta formación o concienciación podría ser 3 horas al año para todo el personal.

Formación y Concienciación	Horas
Equipo de seguridad (STIC): Número de horas por persona dedicadas a cursos de **formación** (incluidos los cursos *online*).	
Usuarios internos: Número de horas por persona empleadas en cursos de formación o sesiones de **concienciación** (incluida la realizada *online*).	

Figura 29.- Formación y concienciación

87. Tasas bajas de formación y concienciación pueden exigir un esfuerzo especial en la materia y la utilización de recursos centrales para su desarrollo e implantación.

10. GESTIÓN DE INCIDENTES

88. La Instrucción Técnica de Seguridad de Notificación de incidentes de seguridad[22] determina los criterios de notificación de incidentes de impacto significativo al CCN.

89. Se dice que un incidente tiene impacto significativo cuando, por su magnitud o características, impide el tratamiento de la información o los servicios prestados. A estos efectos, se considerará que tienen un impacto significativo los niveles alto, muy alto y crítico recogidos en la tabla Criterios de Determinación del Nivel de Impacto de la Guía CCN-STIC 817 *'ENS. Gestión de Ciberincidentes'*. (ver sección 2.2)

90. Interesa en este apartado conocer los incidentes considerados de impacto significativo (alto/muy alto/crítico) que afecten por un lado a la disponibilidad y por otro al resto de clases de ciberincidentes (código dañino, obtención de información, intrusiones, compromiso de la información (que incluye confidencialidad o integridad), fraude, contenido abusivo, política de seguridad u otros, según CCN-STIC 817).

Nivel de impacto del incidente: Alto, Muy Alto o Crítico	Número[23]	T(50)[24]	T(90)[25]	Sup[26]
Interrupción del servicio (disponibilidad): horas				
Resto de clases de ciberincidentes: días				

Figura 30.- Gestión de incidentes de impacto significativo - Tiempo de respuesta

91. Umbrales de interrupción del servicio (disponibilidad): horas que se tarda en cubrir el porcentaje de incidentes significativos (alto/ muy alto / crítico) cerrados, relativos a interrupción del servicio (disponibilidad).

T(50)			T(90)		
verde	amarillo	rojo	verde	amarillo	rojo
< 24h	≥ 24h	≥48h	< 36h	≥ 36h	≥48h

Figura 31.- Gestión de incidentes. Umbrales de interrupción del servicio en horas

92. Umbrales del resto de clases de incidentes: días que se tarda en cubrir el porcentaje de incidentes significativos (alto/ muy alto / crítico) cerrados, relativos al resto de clases de incidentes distintos a los de interrupción del servicio (disponibilidad).

[22] De inminente publicación por el Secretaria de Estado de Función Pública.
[23] Es el número de incidentes clasificados como alto/muy alto o critico en el último año.
[24] T (50): Tiempo que se tarda en resolver el 50% de los incidentes.
[25] T (90): Tiempo que se tarda en resolver el 90% de los incidentes.
[26] Sup: Número de incidentes de disponibilidad que llevan más de 36 horas abiertos o más de 21 días abiertos en el resto de los casos.

T(50)			T(90)		
Verde	Amarillo	Rojo	Verde	Amarillo	Rojo
< 4d	≥ 4d	≥ 14d	< 5d	≥ 5d	≥ 18d

Figura 32.- Gestión de incidentes. Umbrales del resto de clases de incidentes en días

93. Los niveles de madurez nos indican la calidad de las actividades desarrolladas para gestionar la seguridad, son indicadores predictivos, pues una baja madurez de los mismos denota una debilidad de cara a enfrentarnos a incidentes.

94. En cambio, los incidentes nos muestran la eficacia conseguida. El número de incidentes es un poco relativo, pues no depende tanto del organismo atacado como de la parte atacante y, además puede haber diferentes criterios para clasificar un incidente de forma individualizada o fragmentada en componentes. En cambio, los tiempos de respuesta son indicativos de la ventana de oportunidad que le cedemos al atacante.

95. Lo idóneo es cerrar todos los incidentes con presteza, aunque se mide el T (90) para descartar incidentes insidiosos aislados.

96. Si T (90) es alto, es indicación clara de que hay que mejorar el proceso de gestión de incidentes, quizás se necesiten más medios.

97. Si T (50) es claramente inferior a T (90) puede que se disponga de un sistema de resolución de incidentes profesionalizado pues si el sistema de gestión está bien dotado y se dispone de buenos procedimientos de seguridad, T (50) debe ser cercano a T (90). En estos casos se debe poner énfasis en elaborar procedimientos que hagan el proceso sistemático.

11. AUDITORÍAS

98. Una auditoría del Esquema Nacional de Seguridad debe cubrir tanto aspectos de gobierno de la seguridad como aspectos de implantación de las medidas de seguridad de acuerdo con la Instrucción Técnica de Seguridad (ITS) de Auditoría de la Seguridad de los sistemas de información[27].

99. Para obtener la Certificación de Conformidad con el ENS, los sistemas de información de categorías MEDIA o ALTA precisarán superar una Auditoría de Seguridad, al menos cada dos (2) años. Los sistemas de información de categoría Básica solo requerirán de una autoevaluación que, de ser favorable, permitirá la exhibición de la Declaración de Conformidad. Nada impide que un sistema de categoría BÁSICA se someta asimismo a un proceso de Auditoría de Seguridad para la Certificación de la Conformidad, siendo siempre esta posibilidad la deseable.

100. El desarrollo de la Auditoría de la Seguridad se realizará con sujeción a dicha ITS de Auditoría y complementariamente, cuando corresponda, atendiendo a las normas nacionales e internacionales sobre auditoría de sistemas de información, entre ellas las

[27] Inminente publicación por la Secretaría de Estado de la Función Pública.

guías CCN-STIC 802 *'Guía de auditoría'*, CCN-STIC 804 *'Guía de Implantación'* y CCN-STIC 808 *'Verificación del cumplimiento de las medidas en el ENS'*.

101. Como resultado de la auditoría se pueden identificar una serie de hallazgos de no conformidades. Estos se clasificarán de acuerdo a los siguientes grados:
    - "No Conformidad Menor": Se documentará una "No Conformidad Menor" ante la ausencia o el fallo en la implantación o mantenimiento de uno o más de los requisitos del ENS, incluyendo cualquier situación que pudiese, en base a una evidencia objetiva, sustentar una duda significativa sobre la conformidad del sistema de información con uno o más de tales requisitos.
    - "No Conformidad Mayor": Se documentará una "No Conformidad Mayor" cuando se detecten "No Conformidades Menores" en relación con cualquiera de los preceptos contenidos en el RD 3/2010, de 8 de enero del ENS.

102. El dictamen final de la Auditoría de la Seguridad será uno de los tres siguientes:
    - "FAVORABLE": Cuando no se evidencie ninguna "No Conformidad Mayor" o "No Conformidad Menor".
    - "FAVORABLE CON NO CONFORMIDADES": Cuando se evidencie cualquier no conformidad, mayor o menor. En este caso, la entidad titular responsable del sistema de información auditado deberá presentar, en el plazo máximo de un mes, un Plan de Acciones Correctivas sobre tales hallazgos de no conformidad a la entidad certificadora para su evaluación.
    - "DESFAVORABLE": Cuando, por el número o la transcendencia de las no conformidades detectadas, no sea posible decidir sobre su resolución a través de un Plan de Acciones Correctivas. En este caso se requerirá la realización de una auditoría extraordinaria que verifique la adopción de las medidas correctoras adecuadas.

103. Se documentará una "Observación" cuando se encuentren evidencias de una debilidad, una vulnerabilidad o una situación que, sin comprometer cualquier área del sistema de gestión definida en el ENS o por la organización, pueda, en la actualidad o en el futuro, derivar en un problema.

104. La Certificación de Conformidad con el ENS únicamente podrá expedirse si el dictamen fuera "FAVORABLE" o, si habiendo sido "FAVORABLE CON NO CONFORMIDADES", el Plan de Acciones Correctivas presentado por la entidad titular del sistema de información, trata y resuelve los hallazgos de no conformidad evidenciados, a criterio de la entidad certificadora.

105. Una auditoría puede terminar en una declaración o certificación de conformidad con el ENS de acuerdo a lo se establece en la Instrucción Técnica de Seguridad de Conformidad con el Esquema Nacional de Seguridad, regulada por Resolución de 13 de octubre de 2016, del Secretario de Estado de Administraciones Públicas.

106. Los sistemas también pueden someterse a otro tipo de auditorías distintas de las del ENS, como las de cumplimiento de tratamiento de datos, ISO 27001 o exclusivamente auditorías técnicas como pueden ser las correspondientes a un test de penetración[28].

107. La información asociada al número de auditorías realizadas de conformidad con el ENS y de obtención de la declaración o certificación de conformidad se solicita a nivel de categoría de sistema.

Auditorías del ENS realizadas, en función de la categoría	
Se dispone de una auditoría en vigor del ENS (últimos dos años)	Si/No
Número de no conformidades MAYORES	Número
Número de no conformidades MENORES	Número
Certificaciones o Declaración de conformidad con el ENS, en función de la categoría	
El sistema disfruta de una certificación o declaración de conformidad en vigor con el ENS	Si/No
Fecha de concesión de la certificación o declaración de conformidad con el ENS	Fecha
Otras auditorías	
Se dispone de una auditoría técnica u otro tipo de auditorías, distinta del ENS en vigor. Indicar cual/ es:	Texto
Número de no conformidades MAYORES	Número
Número de no conformidades MENORES	Número
Otras certificaciones de seguridad actualizadas:	
El sistema disfruta de una certificación en vigor de cualquier otro tipo, distinto del ENS. Indicar cual/es y la fecha de concesión de la certificación.	Texto

Figura 33.- Información solicitada en relación a auditorías de seguridad

[28] *Pentesting*/*Hacking* ético.

12. INDICADORES CLAVE DE RIESGO (KRI – KEY RISK INDICATORS)

108. Se han considerado tres (3) indicadores clave de riesgo: indicador de derechos de usuarios, indicador de dispositivos propios de usuarios y el indicador de rotación de personal.

109. El indicador de derechos de los usuarios hace referencia al porcentaje de los equipos cliente empleados por el personal interno en los que la configuración y su gestión están bajo control exclusivo de los administradores de seguridad del organismo.

110. El indicador de dispositivos propios de usuario se refiere al porcentaje de equipos del personal interno que emplean dispositivos propios para acceder a los sistemas. Por ejemplo, portátiles, tabletas, teléfonos inteligentes, etc.

111. El indicador de rotación de personal es el número de personas dedicado a la seguridad TIC que ha causado baja en el último año, aunque se hay podido cubrir su vacante.

Indicadores Clave de riesgo KRI	
Derechos de los usuarios	
Porcentaje de los equipos cliente empleados por el personal en los que la configuración y su gestión están bajo control exclusivo de los administradores de seguridad del organismo.	%
Dispositivos propiedad del usuario (BYOD)	
Porcentaje de equipos que son propiedad del personal (es decir, no de la organización) sobre el total de equipos del sistema, empleados para acceder a los sistemas	%
Porcentaje de los equipos que son propiedad del personal sobre el total de equipos del sistema, en los que la configuración y su gestión están bajo control exclusivo de los administradores de seguridad del organismo	%
Rotación de personal de Seguridad TIC	**Número**
Número de personas dedicadas a la seguridad TIC que ha causado baja en el último año, aunque se haya podido cubrir la vacante	

Figura 34.- Indicadores clave de riesgo

13. PROCESOS CRÍTICOS

112. Se definen una serie de procesos críticos, entendidos como medidas independientes o agrupaciones de medidas por tipología.

113. Este apartado no aparece en la ficha de INES ya que su contenido será completado automáticamente a partir de los datos introducidos por el usuario en el apartado 7 “Medidas del Anexo II del ENS”. Se incluye este apartado a nivel informativo ya que estos indicadores aparecerán en el informe del organismo. Ver apartado 16.

114. Los valores asociados a dichos procesos toman como resultado un valor entre 0 y 100, que se presenta como un entero entre 0 y 100 o como un porcentaje entre 0% y 100%.

115. En la siguiente tabla se recogen las medidas (o agrupaciones de medidas) que constituyen los procesos críticos.

Procesos Críticos	Nivel de Madurez
Proceso de autorización [org.4]	
Análisis de riesgos [op.pl.1]	
Gestión de derechos de acceso [op.acc.4]	
Gestión de incidentes [op.exp.7]	
Concienciación y formación [mp.per.3 + mp.per.4]	
Configuración de seguridad [op.exp.2] + Gestión de la configuración [op.exp.3]	
Mantenimiento [op.exp.4] + Gestión de cambios [op.exp.5]	
Continuidad de operaciones [op.cont.1, op.cont.2, op.cont.3, mp.if.9, mp.per.9, mp.eq.9, mp.com.9, mp.info.9, mp.s.9, op.ext.9]	

Figura 35.- Procesos críticos

116. Para aquellos procesos constituidos por más de una medida, el valor asociado a dicho proceso se calcula como la media de las medidas que los constituyen.

14. INDICADORES AGREGADOS

117. Se presentan una serie de indicadores que agregan varios de los indicadores detallados definidos en la sección anterior. El objetivo es un cuadro de mando con unos pocos indicadores que sinteticen el estado de seguridad del sistema de información.

118. Obviamente, cuando un indicador es bajo, hay que recurrir a su desglose para entender el motivo.

14.1 ORGANIZACIÓN DE LA SEGURIDAD

119. En la siguiente tabla se recogen los indicadores que se van a considerar para el cálculo del indicador agregado de Organización de Seguridad. Se usará la media de los mismos:

Descripción	Fórmula

Política de seguridad aprobada	0% → 0 puntos 10% → 10 puntos 50% → 50 puntos 80% → 80 puntos 90% → 90 puntos 100%→ 100 puntos
Responsables independientes	
Análisis de riesgos actualizados	
Declaración de aplicabilidad actualizada	
Plan de adecuación al ENS actualizado	
Declaración o certificación de conformidad actualizada	
Normas de seguridad implantadas	porcentaje → puntos ej. 75% → 75 puntos
Procedimientos de seguridad implantados	
Indicador agregado de Organización de seguridad	**suma(puntos) / 8**

Figura 36.- Detalle indicador agregado de Organización de la seguridad

120. El objetivo es que el indicador sea lo más alto posible, siendo el valor final a alcanzar 100 puntos.

121. Si se dispone de una declaración o certificación de conformidad con el ENS en vigor el indicador será 100.

14.2 ENS – ANEXO II del RD 3/2010

122. Se definen dos (2) indicadores para calibrar los niveles de adecuación de un sistema de información sujeto al Esquema Nacional de Seguridad: Indicador de Madurez (IM) e Indicador de Cumplimiento (IC).

123. Ambos indicadores toman como resultado un valor entre 0 y 100, que se presenta como un entero entre 0 y 100 o como un porcentaje entre 0% y 100%.

124. El Índice de Madurez se calcula a partir de las medidas del Anexo II que se aplican, independientemente de la categoría del sistema. Véase apartado 14.2.1.

125. El Índice de Cumplimiento se calcula a partir de las medidas del Anexo II que son de aplicación y además las correspondientes según los niveles (Bajo, Medio, Alto) asignados a cada una de las dimensiones de seguridad. Véase apartado 14.2.2.

14.2.1 ÍNDICE DE MADUREZ (IM)

126. Se toman en consideración las medidas de seguridad que el responsable de la seguridad marca como aplicables en su sistema. Solamente se consideran las medidas detalladas, sin tener en cuenta los agrupamientos; es decir, las siguientes:

- *org.**
- *op.pl.*, op.acc.*, op.exp.*, op.ext.*, op.cont.*, op.mon.**
- *mp.if.*, mp.per.*, mp.eq.*, mp.com.*, mp.si.*, mp.sw.*, mp.info.*, mp.s.**

127. Si una medida es aplicable, tendrá una valoración de madurez (M) dentro de la tabla estándar de niveles: L0, L1, L2, L3, L4 y L5.

128. Si la medida está valorada en un rango, como puede ser L2-L3, se usa el valor medio de los puntos de cada nivel; por ejemplo

puntos(L2-L3) = (puntos(L2) + puntos(L3)) / 2 = (50 + 80) / 2 = 65

129. Por último, para todas las medidas que son aplicables se calcula el valor medio de los puntos asignados. Ver Anexo B Ejemplos de cálculo de Índice de Madurez y de Cumplimiento.

130. Se definen los siguientes umbrales y colores:

Categoría del Sistema	Rojo	Amarillo	Nivel Adecuado
BÁSICA	< 40%	< 50%	≥50% (L2 o superior)
MEDIA	< 70%	< 80%	≥80% (L3 o superior)
ALTA	< 80%	< 90	≥90% (L4 o superior)

Figura 37.- Umbrales y colores asociados al Índice de Madurez

131. En la inspección del sistema de información, se puede llegar a una estimación más elaborada del nivel numérico de puntos, siempre dentro de los rangos arriba indicados. Se admite el uso de esta estimación en lugar de la propuesta en los párrafos anteriores. En el informe de inspección se documentará por qué se ha llegado a esta estimación.

14.2.2 ÍNDICE DE CUMPLIMIENTO (IC)

132. Se tienen en cuenta las medidas de seguridad del Anexo II que cumplen las siguientes condiciones:

- Se cumplen los requisitos de obligatoriedad descritos en el Anexo II para esa medida.
- El responsable de la seguridad marca la medida como aplicable en su sistema.

133. Cada medida tendrá una valoración de madurez (M) dentro de la tabla estándar de valores: L0, L1, L2, L3, L4, L5 y el sistema tiene una categoría Básica, Media o Alta siguiendo los criterios de valoración del Anexo I del ENS.

134. La determinación de la categoría de un sistema no implica que se altere el nivel de las dimensiones de seguridad que no han influido en dicha determinación, aunque si se verán afectadas por la mayor exigencia en el nivel de madurez que ahora vendrá marcada por dicha categoría.

135. A cada medida de seguridad se la asigna una puntuación (valor ajustado) que depende de la categoría del sistema:

136. Si la medida está valorada en un rango, como puede ser L2-L3, se calcula primero el valor medio de los puntos de cada nivel y posteriormente se ajusta teniendo en cuenta la categoría del sistema. Ejemplo:

puntos(L2-L3) = (puntos(L2) + puntos(L3)) / 2 = (50 + 80) / 2 = 65

137. El cálculo de los indicadores de cumplimiento individuales puede realizarse a través del siguiente algoritmo:

```
double cumplimiento(int cat, int pm) {
if (cat == ALTA) {
      double r = pm * 100.0 / 90;
      if (r > 100)
            r= 100;
      return r;
}
if (cat == MEDIA) {
      double r = pm * 100.0 / 80;
      if (r > 100)
            r= 100;
      return r;
}
if (cat == BASICA) {
      double r = pm * 100.0 / 50;
      if (r > 100)
            r= 100;
      return r;
}
return 0;
}
```

138. Las fórmulas a aplicar para obtener el valor ajustado son las siguientes:

- Categoría Básica: V*alor ajustado = (Valor de la madurez x 100) / 50*
- Categoría Media: V*alor ajustado = (Valor de la madurez x 100) / 80*
- Categoría Alta: *Valor ajustado = (Valor de la madurez x 100) / 90*

139. En todos los casos si el valor ajustado después de aplicar estas fórmulas es mayor de 100 se selecciona 100, que es el valor máximo.

140. Si aplicamos el algoritmo propuesto en el apartado 122 a los niveles de madurez se obtiene la siguiente tabla:

Categoría	Básica L2 (50%)	Media L3 (80%)	Alta L4 (90%)
Madurez	**Puntos**		
L0 (0%)	0	0	0
L1 (10%)	20	12	11
L2 (50%)	100	62	56

L3 (80%)	100	100	89
L4 (90%)	100	100	100
L5 (100%)	100	100	100

Figura 38.- Tabla aclaratoria de ajuste de valores del Índice de Cumplimiento

141. Por último, el Índice de cumplimiento se calcula como el valor medio de los valores ajustados de todas las medidas que son obligatorias y aplicables. Ver Anexo B Ejemplos de cálculo de Índice de Madurez y de Cumplimiento.

142. Se definen los siguientes umbrales y colores correspondientes al Índice de cumplimiento (valores ajustados). Esta tabla se aplicará a todos los sistemas independientemente de su categoría. El objetivo es obtener 100% o 100 puntos.

Categorías	Rojo	Amarillo	Adecuado
Todas las categorías de sistema	< 87	< 97	≥ 97

Figura 39.- Umbrales y colores asociados al Índice de Cumplimiento

15. TRANSFERENCIA DE DATOS EN XML[29]

143. Se pueden completar algunos de los valores solicitados en la herramienta INES a través de la transferencia de dichos datos (en formato XML) desde otras herramientas del Centro Criptológico Nacional.

144. Las herramientas PILAR (de análisis y gestión de riesgos), LUCÍA (de gestión de ciberincidentes) y otras, incorporarán mecanismos para recopilar y exportar los indicadores que les competan, facilitando la recopilación de datos solicitados en INES.

145. Los valores asociados a la gestión de incidentes (véase apartado 10) podrán ser calculados en la herramienta INES a partir de un fichero XML extraído de la herramienta LUCIA (Gestión de ciberincidentes).

146. Los niveles de madurez de las medidas de seguridad del Anexo II del Esquema Nacional de Seguridad (véase apartado 7) y otros datos podrán ser cargados en la herramienta INES a partir de un fichero XML extraído de la herramienta PILAR (Análisis y gestión de riesgos).

16. INFORMES GENERADOS CON INES

147. Una vez completados por parte del organismo los datos solicitados por la herramienta INES y una vez finalizada la correspondiente campaña de recogida de datos se preparan diferentes informes:

[29] XML – eXtensible Markup Language

- El informe anual del estado de seguridad del sector público español e informes anuales por ámbitos (Administración General del Estado, Comunidades Autónomas, Entidades Locales y Universidades) que se confeccionarán por el Centro Criptológico Nacional.
- El informe ejecutivo individual del propio organismo propietario del sistema de información, que se genera por la propia herramienta INES, una vez finalizado el proceso y a solicitud del responsable de la seguridad. En este informe se incluyen, además de los datos propios del organismo, valores generales (medianas) de todas las fichas registradas en la campaña, además de las correspondientes por ámbitos (Administración General del Estado, Comunidades Autónomas, Entidades Locales y Universidades), con carácter comparativo. Los valores generales no serán definitivos hasta que la campaña se haya cerrado. Por tanto, se recomienda generar o actualizar dicho informe tras el fin del periodo de carga de datos, estando previsto que el CCN emita un comunicado indicando que se ha completado el proceso anual.

ANEXO A. BIBLIOGRAFÍA DE REFERENCIA

En la realización de esta auditoría se utilizarán, además de los mínimos requisitos de esta guía, los criterios, métodos de trabajo y de conducta generalmente reconocidos, así como la normalización nacional e internacional aplicables a las auditorías.

A continuación, se incluyen referencias bibliográficas que pueden ayudar a los auditores en el desarrollo de su trabajo:

- Real Decreto 3/2010 del 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
- Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.
- Real Decreto 951/2015, de 23 de octubre, de modificación del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
- Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.
- 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
- Instrucción técnica de seguridad de las TIC - Inspección STIC - Centro Criptológico Nacional - CCN-STIC-303.
- Guía de seguridad de las TIC - (CCN-STIC-411) - Modelo de plan de verificación STIC - (ST&E PLAN) - CCN-STIC-411.
- Guía de seguridad de las TIC - (CCN-STIC-808) - Verificación del cumplimiento de las medidas en el ENS.
- Guía de seguridad de las TIC - (CCN-STIC-811) Interconexión en el ENS.
- Guía de seguridad de las TIC - (CCN-STIC-815) - ENS Métricas e Indicadores.
- Guía de seguridad de las TIC – (CCN-STIC-818) – Herramientas de seguridad en el ENS.
- Guía de seguridad de las TIC - (CCN-STIC-824) – Esquema Nacional De Seguridad. Informe del Estado de Seguridad.
- 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-844) – Esquema Nacional De Seguridad. Informe del Estado de Seguridad. Manual de usuario
-

- Esquema de evaluación y certificación de la seguridad de las tecnologías de información - Auditorías internas – PO-001.
- ISO/IEC 27001[30] - Information technology -- Security techniques -- Information security management systems – Requirements.
- UNE-ISO/IEC 27001 – Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información (SGSI).
- ISO/IEC 27005 - Information technology -- Security techniques -- Information security risk management.
- ISO/IEC 27006 - Information technology -- Security techniques -- Requirements for bodies providing audit and certification of information security management systems.
- UNE 71504 – Metodología de análisis y gestión de riesgos para los sistemas de información.
- UNE-EN ISO/IEC 17065:2012 - Evaluación de la conformidad. Requisitos para organismos que certifican productos, procesos y servicios.
- MAGERIT – versión 3. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Consejo Superior de Administración Electrónica, 2012.
- *Information Systems Audit and Control Association* - www.isaca.org: en esta entidad se pone a disposición de los auditores de sistemas de información, distintos estándares, directrices y procedimientos de auditoría que pueden ser de utilidad para los auditores, ya que la mayoría de ellos tienen en cuenta los aspectos de seguridad, incluyendo algunos específicos sobre seguridad.
    - Las normas son de obligado cumplimiento para los auditores de sistemas tales como Independencia, Ética profesional, Planificación, aplicación de análisis de riesgos en la planificación, utilización del trabajo de expertos, emisión de informes, y similares.
    - Las directrices son una ampliación de los estándares, para facilitar la aplicación de estos últimos: requisitos de las evidencias de auditoría, utilización de herramientas de software de auditoría, externalización de servicios, documentación y registros de la auditoría, análisis forense, privacidad, revisión de la seguridad, y otras más, en algunos casos relacionadas con sistemas de información específicos.
    - Los procedimientos de auditoría proporcionan ejemplos concretos o modelos de programas y pruebas de auditoría: evaluación de sistemas de cifrado, de cortafuegos, firmas electrónicas, y similares.
- El *Institute of Internal Auditors* – ww.theiia.org también tiene disponibles guías de auditoría para diversos sistemas, y de controles para sistemas de información.

[30] Tanto los estándares ISO como UNE se entenderán referidos a su última versión vigente.

ANEXO B. EJEMPLOS DE CÁLCULO DEL ÍNDICE DE MADUREZ Y DE CUMPLIMIENTO

Ejemplo 1:

Sea un sistema de información con los siguientes niveles en cada dimensión de seguridad:

Sistema 1		
NIVELES DE LAS DIMENSIONES DE SEGURIDAD	CONFIDENCIALIDAD (C)	A
	INTEGRIDAD (I)	A
	DISPONIBILDAD (D)	A
	AUTENTICIDAD (A)	A
	TRAZABILIDAD (T)	B

Su categoría corresponde con el nivel más elevado asociado a alguna de las dimensiones. Por tanto, la **categoría de este sistema es Alta: [C(A), I(A), D(A), A(A), T(B)]**.

En la siguiente tabla se recogen los valores registrados por el organismo para cada una de las medidas de seguridad aplicadas al sistema:

Dimensiones afectadas	Básica	Media	Alta	Medida de seguridad	Valor registrado por el organismo
categoría	aplica	=	=	[org.1]	**80**
categoría	aplica	=	=	[org.2]	**50**
categoría	aplica	=	=	[org.3]	**39**
categoría	aplica	=	=	[org.4]	**50**
categoría	aplica	+	++	[op.pl.1]	**70**
categoría	aplica	+	++	[op.pl.2]	**61**
categoría	aplica	=	=	[op.pl.3]	**60**
D	n.a.	aplica	=	[op.pl.4]	**59**
categoría	n.a.	n.a.	aplica	[op.pl.5]	**57**
A T	aplica	=	=	[op.acc.1]	**77**
I C A T	aplica	=	=	[op.acc.2]	**80**
I C A T	n.a.	aplica	=	[op.acc.3]	**67**
I C A T	aplica	=	=	[op.acc.4]	**73**
I C A T	aplica	+	++	[op.acc.5]	**77**
I C A T	aplica	+	++	[op.acc.6]	**71**
I C A T	aplica	+	=	[op.acc.7]	**75**
categoría	aplica	=	=	[op.exp.1]	**74**
categoría	aplica	=	=	[op.exp.2]	**71**
categoría	n.a.	aplica	=	[op.exp.3]	**68**
categoría	aplica	=	=	[op.exp.4]	**71**
categoría	n.a.	aplica	=	[op.exp.5]	**64**

Dimensiones afectadas	Básica	Media	Alta	Medida de seguridad	Valor registrado por el organismo
categoría	aplica	=	=	[op.exp.6]	**75**
categoría	n.a.	aplica	=	[op.exp.7]	**66**
T	aplica	+	++	[op.exp.8]	**60**
categoría	n.a.	aplica	=	[op.exp.9]	**62**
T	n.a.	n.a.	aplica	[op.exp.10]	**60**
categoría	aplica	+	=	[op.exp.11]	**62**
categoría	n.a.	aplica	=	[op.ext.1]	**73**
categoría	n.a.	aplica	=	[op.ext.2]	**69**
D	n.a.	n.a.	aplica	[op.ext.9]	**56**
D	n.a.	aplica	=	[op.cont.1]	**52**
D	n.a.	n.a.	aplica	[op.cont.2]	**51**
D	n.a.	n.a.	aplica	[op.cont.3]	**48**
categoría	n.a.	aplica	=	[op.mon.1]	**63**
categoría	aplica	+	++	[op.mon.2]	**49**
categoría	aplica	=	=	[mp.if.1]	**77**
categoría	aplica	=	=	[mp.if.2]	**72**
categoría	aplica	=	=	[mp.if.3]	**76**
D	aplica	+	=	[mp.if.4]	**80**
D	aplica	=	=	[mp.if.5]	**80**
D	n.a.	aplica	=	[mp.if.6]	**70**
categoría	aplica	=	=	[mp.if.7]	**67**
D	n.a.	n.a.	aplica	[mp.if.9]	**50**
categoría	n.a.	aplica	=	[mp.per.1]	**64**
categoría	aplica	=	=	[mp.per.2]	**69**
categoría	aplica	=	=	[mp.per.3]	**60**
categoría	aplica	=	=	[mp.per.4]	**54**
D	n.a.	n.a.	aplica	[mp.per.9]	**50**
categoría	aplica	+	=	[mp.eq.1]	**67**
A	n.a.	aplica	+	[mp.eq.2]	**76**
categoría	aplica	=	+	[mp.eq.3]	**66**
D	n.a.	aplica	=	[mp.eq.9]	**70**
categoría	aplica	=	+	[mp.com.1]	**80**
C	n.a.	aplica	+	[mp.com.2]	**77**
I A	aplica	+	++	[mp.com.3]	**74**
categoría	n.a.	n.a.	aplica	[mp.com.4]	**75**
D	n.a.	n.a.	aplica	[mp.com.9]	**75**
C	aplica	=	=	[mp.si.1]	**71**
I C	n.a.	aplica	+	[mp.si.2]	**51**
categoría	aplica	=	=	[mp.si.3]	**71**
categoría	aplica	=	=	[mp.si.4]	**65**

Dimensiones afectadas	Básica	Media	Alta	Medida de seguridad	Valor registrado por el organismo
C	aplica	+	=	[mp.si.5]	**71**
categoría	n.a.	aplica	=	[mp.sw.1]	**72**
categoría	aplica	+	++	[mp.sw.2]	**65**
categoría	aplica	=	=	[mp.info.1]	**78**
C	aplica	+	=	[mp.info.2]	**67**
C	n.a.	n.a.	aplica	[mp.info.3]	**54**
I A	aplica	+	++	[mp.info.4]	**73**
T	n.a.	n.a.	aplica	[mp.info.5]	**61**
C	aplica	=	=	[mp.info.6]	**53**
D	aplica	=	=	[mp.info.9]	**86**
categoría	aplica	=	=	[mp.s.1]	**77**
categoría	aplica	=	+	[mp.s.2]	**71**
D	n.a.	aplica	+	[mp.s.8]	**63**
D	n.a.	n.a.	aplica	[mp.s.9]	**55**
Índice de Madurez					**66,3**

El **Índice de Madurez (IM)** de este sistema es básicamente la media de los 75 valores registrados. Si hay alguna medida de seguridad que no aplica por las características del sistema, por ejemplo, medidas de interconexión para un sistema aislado (mp.com.1 perímetro seguro), no se tendrá en cuenta para este cálculo. La exclusión de medidas en el cálculo del IM debe estar claramente justificada. Por tanto, el IM del ejemplo sería 66,3%.

Para el **cálculo del Índice de Cumplimiento (IC)** se parte igualmente del nivel establecido a cada dimensión de seguridad y se debe determinar si una medida de seguridad del anexo II del ENS en concreto aplica o no (en función del valor de los niveles de las dimensiones de seguridad) y si aplica, se determina por el organismo el nivel de madurez asociado a la misma.

En este ejemplo, recordemos que el sistema es de categoría Alta y que todas las dimensiones de seguridad tienen un nivel Alto, excepto la Trazabilidad que lo tiene Bajo:

Categoría del Sistema Alta: [C(A), I(A), D(A), A(A), T(B)].

Por tanto, aplicarían todas las medidas de seguridad exigidas para nivel alto exceptuando aquellas que sólo apliquen a trazabilidad (nivel Medio o Alto). Es decir, no se tendrán en cuenta para el cálculo del Índice de cumplimiento las medidas, [op.exp.10: Protección de los registros de actividad] y [mp.info.5: Sellos de tiempo], pero si se tendrá en cuenta la medida [op.exp.8: Registro de la actividad de los usuarios] correspondiente a un nivel de Trazabilidad Bajo, pero **solo la parte de la medida exigible a dicho nivel Bajo**: Se registrarán las actividades que se indican de los usuarios del sistema, pero **solo se activarán los registros en los servidores.**

En concreto, según el apartado 4.3.8 Registro de la actividad de los usuarios [op.exp.8] del ENS:

Dimensiones	Trazabilidad		
Nivel	Bajo	Medio	Alto
op.exp.8	aplica	+	++

Se registrarán las actividades de los usuarios en el sistema, de forma que:

a) El registro indicará quién realiza la actividad, cuándo la realiza y sobre qué información.
b) Se incluirá la actividad de los usuarios y, especialmente, la de los operadores y administradores en cuanto puedan acceder a la configuración y actuar en el mantenimiento del sistema.
c) Deberán registrarse las actividades realizadas con éxito y los intentos fracasados.
d) La determinación de qué actividades deben registrarse y con qué niveles de detalle se adoptará a la vista del análisis de riesgos realizado sobre el sistema ([op.pl.1]).

- Nivel BAJO: Se activarán los registros de actividad en los servidores.
- Nivel MEDIO: Se revisarán informalmente los registros de actividad buscando patrones anormales.
- Nivel ALTO: Se dispondrá de un sistema automático de recolección de registros y correlación de eventos; es decir, una consola de seguridad centralizada.

A continuación, se muestra una tabla con los niveles asociados a cada una de las medidas. En este ejemplo, todas las medidas tendrán asignadas un nivel alto exceptuando tres (3):

- [op.exp.8: Registro de la actividad de los usuarios]: Aplica nivel Bajo ya que es el nivel que se ha asignado a la dimensión de trazabilidad como se ha indicado y además el valor ajustado lo será respecto a la exigencia de la categoría del sistema es decir Alta (L4= 90%).
- [op.exp.10 Protección de los registros de actividad] y [mp.info.5 Sellos de tiempo]: A estas medidas no se asigna un nivel ya que no aplican para el cálculo del IC. Sólo son exigidas en sistemas con nivel alto en la dimensión de trazabilidad y en el ejemplo se ha asignado un nivel bajo.

Dimensiones afectadas	Básica	Media	Alta	Medida de seguridad	Selección de la medida por nivel asociado	Valor registrado	Valor ajustado[31]
categoría	aplica	=	=	[org.1]	Alto	80	**88,9**
categoría	aplica	=	=	[org.2]	Alto	50	**55,6**
categoría	aplica	=	=	[org.3]	Alto	39	**43,3**
categoría	aplica	=	=	[org.4]	Alto	50	**55,6**

[31] Al ser sistema de categoría Alta para calcular el valor ajustado de las medidas se aplica la fórmula (ver 14.1.3) valor ajustado = (valor de la madurez de la medida de seguridad * 100)/90

Dimensiones afectadas	Básica	Media	Alta	Medida de seguridad	Selección de la medida por nivel asociado	Valor registrado	Valor ajustado[31]
categoría	aplica	+	++	[op.pl.1]	Alto	70	**77,8**
categoría	aplica	+	++	[op.pl.2]	Alto	61	**67,8**
categoría	aplica	=	=	[op.pl.3]	Alto	60	**66,7**
D	n.a.	aplica	=	[op.pl.4]	Alto	59	**65,6**
categoría	n.a.	n.a.	aplica	[op.pl.5]	Alto	57	**63,3**
A T	aplica	=	=	[op.acc.1]	Alto	77	**85,6**
I C A T	aplica	=	=	[op.acc.2]	Alto	80	**88,9**
I C A T	n.a.	aplica	=	[op.acc.3]	Alto	67	**74,4**
I C A T	aplica	=	=	[op.acc.4]	Alto	73	**81,1**
I C A T	aplica	+	++	[op.acc.5]	Alto	77	**85,6**
I C A T	aplica	+	++	[op.acc.6]	Alto	71	**78,9**
I C A T	aplica	+	=	[op.acc.7]	Alto	75	**83,3**
categoría	aplica	=	=	[op.exp.1]	Alto	74	**82,2**
categoría	aplica	=	=	[op.exp.2]	Alto	71	**78,9**
categoría	n.a.	aplica	=	[op.exp.3]	Alto	68	**75,6**
categoría	aplica	=	=	[op.exp.4]	Alto	71	**78,9**
categoría	n.a.	aplica	=	[op.exp.5]	Alto	64	**71,1**
categoría	aplica	=	=	[op.exp.6]	Alto	75	**83,3**
categoría	n.a.	aplica	=	[op.exp.7]	Alto	66	**73,3**
T	aplica	+	++	[op.exp.8]	Bajo	60	**66,7**
categoría	n.a.	aplica	=	[op.exp.9]	Alto	62	**68,9**
T	n.a.	n.a.	aplica	[op.exp.10]	No aplica	60	-
categoría	aplica	+	=	[op.exp.11]	Alto	62	**68,9**
categoría	n.a.	aplica	=	[op.ext.1]	Alto	73	**81,1**
categoría	n.a.	aplica	=	[op.ext.2]	Alto	69	**76,7**
D	n.a.	n.a.	aplica	[op.ext.9]	Alto	56	**62,2**
D	n.a.	aplica	=	[op.cont.1]	Alto	52	**57,8**
D	n.a.	n.a.	aplica	[op.cont.2]	Alto	51	**56,7**
D	n.a.	n.a.	aplica	[op.cont.3]	Alto	48	**53,3**
categoría	n.a.	aplica	=	[op.mon.1]	Alto	63	**70,0**
categoría	aplica	+	++	[op.mon.2]	Alto	49	**54,4**
categoría	aplica	=	=	[mp.if.1]	Alto	77	**85,6**
categoría	aplica	=	=	[mp.if.2]	Alto	72	**80,0**
categoría	aplica	=	=	[mp.if.3]	Alto	76	**84,4**
D	aplica	+	=	[mp.if.4]	Alto	80	**88,9**
D	aplica	=	=	[mp.if.5]	Alto	80	**88,9**
D	n.a.	aplica	=	[mp.if.6]	Alto	70	**77,8**
categoría	aplica	=	=	[mp.if.7]	Alto	67	**74,4**
D	n.a.	n.a.	aplica	[mp.if.9]	Alto	50	**55,6**
categoría	n.a.	aplica	=	[mp.per.1]	Alto	64	**71,1**

Dimensiones afectadas	Básica	Media	Alta	Medida de seguridad	Selección de la medida por nivel asociado	Valor registrado	Valor ajustado[31]
categoría	aplica	=	=	[mp.per.2]	Alto	69	**76,7**
categoría	aplica	=	=	[mp.per.3]	Alto	60	**66,7**
categoría	aplica	=	=	[mp.per.4]	Alto	54	**60,0**
D	n.a.	n.a.	aplica	[mp.per.9]	Alto	50	**55,6**
categoría	aplica	+	=	[mp.eq.1]	Alto	67	**74,4**
A	n.a.	aplica	+	[mp.eq.2]	Alto	76	**84,4**
categoría	aplica	=	+	[mp.eq.3]	Alto	66	**73,3**
D	n.a.	aplica	=	[mp.eq.9]	Alto	70	**77,8**
categoría	aplica	=	+	[mp.com.1]	Alto	80	**88,9**
C	n.a.	aplica	+	[mp.com.2]	Alto	77	**85,6**
I A	aplica	+	++	[mp.com.3]	Alto	74	**82,2**
categoría	n.a.	n.a.	aplica	[mp.com.4]	Alto	75	**83,3**
D	n.a.	n.a.	aplica	[mp.com.9]	Alto	75	**83,3**
C	aplica	=	=	[mp.si.1]	Alto	71	**78,9**
I C	n.a.	aplica	+	[mp.si.2]	Alto	51	**56,7**
categoría	aplica	=	=	[mp.si.3]	Alto	71	**78,9**
categoría	aplica	=	=	[mp.si.4]	Alto	65	**72,2**
C	aplica	+	=	[mp.si.5]	Alto	71	**78,9**
categoría	n.a.	aplica	=	[mp.sw.1]	Alto	72	**80,0**
categoría	aplica	+	++	[mp.sw.2]	Alto	65	**72,2**
categoría	aplica	=	=	[mp.info.1]	Alto	78	**86,7**
C	aplica	+	=	[mp.info.2]	Alto	67	**74,4**
C	n.a.	n.a.	aplica	[mp.info.3]	Alto	54	**60,0**
I A	aplica	+	++	[mp.info.4]	Alto	73	**81,1**
T	n.a.	n.a.	aplica	[mp.info.5]	No aplica	61	-
C	aplica	=	=	[mp.info.6]	Alto	53	**58,9**
D	aplica	=	=	[mp.info.9]	Alto	86	**95,6**
categoría	aplica	=	=	[mp.s.1]	Alto	77	**85,6**
categoría	aplica	=	+	[mp.s.2]	Alto	71	**78,9**
D	n.a.	aplica	+	[mp.s.8]	Alto	63	**70,0**
D	n.a.	n.a.	aplica	[mp.s.9]	Alto	55	**61,1**
Índice de cumplimiento							**73,85**

La última columna representa los valores ajustados en función del nivel asignado. Por ejemplo:

- [mp.if.6]: Aplica nivel Alto ya que es el nivel que se ha asignado a la dimensión de disponibilidad. En este caso el valor indicado es de 70% y dado que el nivel mínimo exigido para Alto es 90%, se considera que, si el IM fuera 90% o superior, su IC será 100%. El cálculo sería el siguiente:

Valor Ajustado mp.if.6 = (70 x 100) / 90= 77,78% aprox. 78%

- [op.exp.8]: A esta medida se le ha asignado un nivel bajo correspondiente a trazabilidad sin embargo, al ser la categoría del sistema alta, el nivel mínimo exigido para alta es 90% y por tanto se precisa ajustar como en el caso anterior. El cálculo sería el siguiente:

Valor Ajustado op.exp.8 = (60 x 100) / 90= 66,66 % aprox. 67%

El Índice de cumplimiento se calculará como la media de los valores ajustados de las medidas que aplican teniendo en cuenta la categoría del sistema. El valor obtenido en este ejemplo es: 73,85%.

Ejemplo 2:

Sea un sistema de información con los siguientes niveles en cada dimensión de seguridad:

Sistema 2		
NIVELES DE LAS DIMENSIONES DE SEGURIDAD	CONFIDENCIALIDAD (C)	M
	INTEGRIDAD (I)	A
	DISPONIBILDAD (D)	A
	AUTENTICIDAD (A)	M
	TRAZABILIDAD (T)	B

Su categoría corresponde con el nivel más elevado asociado a alguna de las dimensiones. Por tanto, su **categoría es ALTA: [C(M), I(A), D(A), A(M), T(B)]**.

En la siguiente tabla se recogen los valores registrados para cada una de las medidas:

Dimensiones Afectadas	BÁSICA	MEDIA	ALTA	Medida de seguridad	Valor registrado por el organismo
categoría	aplica	=	=	[org.1]	**80**
categoría	aplica	=	=	[org.2]	**50**
categoría	aplica	=	=	[org.3]	**50**
categoría	aplica	=	=	[org.4]	**50**
categoría	aplica	+	++	[op.pl.1]	**10**
categoría	aplica	+	++	[op.pl.2]	**50**
categoría	aplica	=	=	[op.pl.3]	**50**
D	n.a.	aplica	=	[op.pl.4]	**50**
categoría	n.a.	n.a.	aplica	[op.pl.5]	**50**
A T	aplica	=	=	[op.acc.1]	**80**
I C A T	aplica	=	=	[op.acc.2]	**80**
I C A T	n.a.	aplica	=	[op.acc.3]	**50**
I C A T	aplica	=	=	[op.acc.4]	**80**
I C A T	aplica	+	++	[op.acc.5]	**80**
I C A T	aplica	+	++	[op.acc.6]	**80**

Dimensiones Afectadas	BÁSICA	MEDIA	ALTA	Medida de seguridad	Valor registrado por el organismo
I C A T	aplica	+	=	[op.acc.7]	**80**
categoría	aplica	=	=	[op.exp.1]	**80**
categoría	aplica	=	=	[op.exp.2]	**50**
categoría	n.a.	aplica	=	[op.exp.3]	**50**
categoría	aplica	=	=	[op.exp.4]	**50**
categoría	n.a.	aplica	=	[op.exp.5]	**50**
categoría	aplica	=	=	[op.exp.6]	**80**
categoría	n.a.	aplica	=	[op.exp.7]	**80**
T	aplica	+	++	[op.exp.8]	**10**
categoría	n.a.	aplica	=	[op.exp.9]	**10**
T	n.a.	n.a.	aplica	[op.exp.10]	**50**
categoría	aplica	+	=	[op.exp.11]	**80**
categoría	n.a.	aplica	=	[op.ext.1]	**80**
categoría	n.a.	aplica	=	[op.ext.2]	**50**
D	n.a.	n.a.	aplica	[op.ext.9]	**50**
D	n.a.	aplica	=	[op.cont.1]	**10**
D	n.a.	n.a.	aplica	[op.cont.2]	**10**
D	n.a.	n.a.	aplica	[op.cont.3]	**0**
categoría	n.a.	aplica	=	[op.mon.1]	**10**
categoría	aplica	+	++	[op.mon.2]	**50**
categoría	aplica	=	=	[mp.if.1]	**90**
categoría	aplica	=	=	[mp.if.2]	**80**
categoría	aplica	=	=	[mp.if.3]	**90**
D	aplica	+	=	[mp.if.4]	**90**
D	aplica	=	=	[mp.if.5]	**90**
D	n.a.	aplica	=	[mp.if.6]	**90**
categoría	aplica	=	=	[mp.if.7]	**50**
D	n.a.	n.a.	aplica	[mp.if.9]	**90**
categoría	n.a.	aplica	=	[mp.per.1]	**80**
categoría	aplica	=	=	[mp.per.2]	**60**
categoría	aplica	=	=	[mp.per.3]	**10**
categoría	aplica	=	=	[mp.per.4]	**10**
D	n.a.	n.a.	aplica	[mp.per.9]	**50**
categoría	aplica	+	=	[mp.eq.1]	**10**
A	n.a.	aplica	+	[mp.eq.2]	**10**
categoría	aplica	=	+	[mp.eq.3]	**50**
D	n.a.	aplica	=	[mp.eq.9]	**50**
categoría	aplica	=	+	[mp.com.1]	**80**
C	n.a.	aplica	+	[mp.com.2]	**50**
I A	aplica	+	++	[mp.com.3]	**50**
categoría	n.a.	n.a.	aplica	[mp.com.4]	**80**

Dimensiones Afectadas	BÁSICA	MEDIA	ALTA	Medida de seguridad	Valor registrado por el organismo
D	n.a.	n.a.	aplica	[mp.com.9]	**80**
C	aplica	=	=	[mp.si.1]	**50**
I C	n.a.	aplica	+	[mp.si.2]	**50**
categoría	aplica	=	=	[mp.si.3]	**50**
categoría	aplica	=	=	[mp.si.4]	**50**
C	aplica	+	=	[mp.si.5]	**50**
categoría	n.a.	aplica	=	[mp.sw.1]	**50**
categoría	aplica	+	++	[mp.sw.2]	**80**
categoría	aplica	=	=	[mp.info.1]	**80**
C	aplica	+	=	[mp.info.2]	**80**
C	n.a.	n.a.	aplica	[mp.info.3]	**50**
I A	aplica	+	++	[mp.info.4]	**50**
T	n.a.	n.a.	aplica	[mp.info.5]	**50**
C	aplica	=	=	[mp.info.6]	**50**
D	aplica	=	=	[mp.info.9]	**80**
categoría	aplica	=	=	[mp.s.1]	**50**
categoría	aplica	=	+	[mp.s.2]	**50**
D	n.a.	aplica	+	[mp.s.8]	**80**
D	n.a.	n.a.	aplica	[mp.s.9]	**80**
Índice de Madurez					**56,5**

El **Índice de Madurez (IM)** es básicamente la media de los 75 valores registrados. Si hay alguna que no aplica por las características del sistema, por ejemplo, medidas de interconexión para un sistema aislado, no se tendrá en cuenta para este cálculo. La exclusión de medidas en el cálculo del IM debe estar claramente justificada. Por tanto, el IM del ejemplo sería 56,53%.

Para el cálculo del **Índice de Cumplimiento (IC)** es necesario establecer el nivel con el que afecta cada una de las medidas de seguridad. Se debe determinar si una medida aplica o no (en función de dichos niveles) y si aplica, se determina el nivel asociado a la misma. En concreto, para este ejemplo:

Categoría del sistema 2 es ALTA: [C(M), I(A), D(A), A(M), T(B)].

- Se han seleccionado todas las medidas que afectan a las dimensiones de Integridad y Disponibilidad de nivel Alto.
- Se han seleccionado todas las medidas que afectan a las dimensiones de Confidencialidad y Autenticidad de nivel Medio (sin afectar a las dimensiones de Integridad y Disponibilidad).
- Se han seleccionado aquellas medidas que sólo afecta a la dimensión de Trazabilidad de nivel Bajo. Es decir, no aplican las medidas [op.exp.10 Protección de los registros de actividad], la medida [mp.info.5 Sellos de tiempo] ni la medida [mp.info.3 Cifrado de la Información].

A continuación, se muestra una tabla con dichos niveles:

Dimensiones Afectadas	B	M	A	Medida	Selección de la medida por nivel asociado	Valor registrado	Valor ajustado[32]
categoría	aplica	=	=	[org.1]	Alto	80	**88,9**
categoría	aplica	=	=	[org.2]	Alto	50	**55,6**
categoría	aplica	=	=	[org.3]	Alto	50	**55,6**
categoría	aplica	=	=	[org.4]	Alto	50	**55,6**
categoría	aplica	+	++	[op.pl.1]	Alto	10	**11,1**
categoría	aplica	+	++	[op.pl.2]	Alto	50	**55,6**
categoría	aplica	=	=	[op.pl.3]	Alto	50	**55,6**
D	n.a.	aplica	=	[op.pl.4]	Alto	50	**55,6**
categoría	n.a.	n.a.	aplica	[op.pl.5]	Alto	50	**55,6**
A T	aplica	=	=	[op.acc.1]	Medio	80	**88,9**
I C A T	aplica	=	=	[op.acc.2]	Alto	80	**88,9**
I C A T	n.a.	aplica	=	[op.acc.3]	Alto	50	**55,6**
I C A T	aplica	=	=	[op.acc.4]	Alto	80	**88,9**
I C A T	aplica	+	++	[op.acc.5]	Alto	80	**88,9**
I C A T	aplica	+	++	[op.acc.6]	Alto	80	**88,9**
I C A T	aplica	+	=	[op.acc.7]	Alto	80	**88,9**
categoría	aplica	=	=	[op.exp.1]	Alto	80	**88,9**
categoría	aplica	=	=	[op.exp.2]	Alto	50	**55,6**
categoría	n.a.	aplica	=	[op.exp.3]	Alto	50	**55,6**
categoría	aplica	=	=	[op.exp.4]	Alto	50	**55,6**
categoría	n.a.	aplica	=	[op.exp.5]	Alto	50	**55,6**
categoría	aplica	=	=	[op.exp.6]	Alto	80	**88,9**
categoría	n.a.	aplica	=	[op.exp.7]	Alto	80	**88,9**
T	aplica	+	++	[op.exp.8]	Bajo	10	**11,1**
categoría	n.a.	aplica	=	[op.exp.9]	Alto	10	**11,1**
T	n.a.	n.a.	aplica	[op.exp.10]	No Aplica	50	**-**
categoría	aplica	+	=	[op.exp.11]	Alto	80	**88,9**
categoría	n.a.	aplica	=	[op.ext.1]	Alto	80	**88,9**
categoría	n.a.	aplica	=	[op.ext.2]	Alto	50	**55,6**
D	n.a.	n.a.	aplica	[op.ext.9]	Alto	50	**55,6**
D	n.a.	aplica	=	[op.cont.1]	Alto	10	**11,1**
D	n.a.	n.a.	aplica	[op.cont.2]	Alto	10	**11,1**
D	n.a.	n.a.	aplica	[op.cont.3]	Alto	0	**0,0**
categoría	n.a.	aplica	=	[op.mon.1]	Alto	10	**11,1**
categoría	aplica	+	++	[op.mon.2]	Alto	50	**55,6**
categoría	aplica	=	=	[mp.if.1]	Alto	90	**100,0**
categoría	aplica	=	=	[mp.if.2]	Alto	80	**88,9**

[32] Al ser sistema de categoría Alta para calcular el valor ajustado de las medidas se aplica la fórmula (ver 14.1.3) valor ajustado = (valor de la madurez de la medida de seguridad * 100)/90

categoría	aplica	=	=	[mp.if.3]	Alto	90	**100,0**
D	aplica	+	=	[mp.if.4]	Alto	90	**100,0**
D	aplica	=	=	[mp.if.5]	Alto	90	**100,0**
D	n.a.	aplica	=	[mp.if.6]	Alto	90	**100,0**
categoría	aplica	=	=	[mp.if.7]	Alto	50	**55,6**
D	n.a.	n.a.	aplica	[mp.if.9]	Alto	90	**100,0**
categoría	n.a.	aplica	=	[mp.per.1]	Alto	80	**88,9**
categoría	aplica	=	=	[mp.per.2]	Alto	60	**66,7**
categoría	aplica	=	=	[mp.per.3]	Alto	10	**11,1**
categoría	aplica	=	=	[mp.per.4]	Alto	10	**11,1**
D	n.a.	n.a.	aplica	[mp.per.9]	Alto	50	**55,6**
categoría	aplica	+	=	[mp.eq.1]	Alto	10	**11,1**
A	n.a.	aplica	+	[mp.eq.2]	Medio	10	**11,1**
categoría	aplica	=	+	[mp.eq.3]	Alto	50	**55,6**
D	n.a.	aplica	=	[mp.eq.9]	Alto	50	**55,6**
categoría	aplica	=	+	[mp.com.1]	Alto	80	**88,9**
C	n.a.	aplica	+	[mp.com.2]	Medio	50	**55,6**
I A	aplica	+	++	[mp.com.3]	Alto	50	**55,6**
categoría	n.a.	n.a.	aplica	[mp.com.4]	Alto	80	**88,9**
D	n.a.	n.a.	aplica	[mp.com.9]	Alto	80	**88,9**
C	aplica	=	=	[mp.si.1]	Medio	50	**55,6**
I C	n.a.	aplica	+	[mp.si.2]	Alto	50	**55,6**
categoría	aplica	=	=	[mp.si.3]	Alto	50	**55,6**
categoría	aplica	=	=	[mp.si.4]	Alto	50	**55,6**
C	aplica	+	=	[mp.si.5]	Medio	50	**55,6**
categoría	n.a.	aplica	=	[mp.sw.1]	Alto	50	**55,6**
categoría	aplica	+	++	[mp.sw.2]	Alto	80	**88,9**
categoría	aplica	=	=	[mp.info.1]	Alto	80	**88,9**
C	aplica	+	=	[mp.info.2]	Medio	80	**88,9**
C	n.a.	n.a.	aplica	[mp.info.3]	No Aplica	50	**-**
I A	aplica	+	++	[mp.info.4]	Alto	50	**55,6**
T	n.a.	n.a.	aplica	[mp.info.5]	No Aplica	50	**-**
C	aplica	=	=	[mp.info.6]	Medio	50	**55,6**
D	aplica	=	=	[mp.info.9]	Alto	80	**88,9**
categoría	aplica	=	=	[mp.s.1]	Alto	50	**55,6**
categoría	aplica	=	+	[mp.s.2]	Alto	50	**55,6**
D	n.a.	aplica	+	[mp.s.8]	Alto	80	**88,9**
D	n.a.	n.a.	aplica	[mp.s.9]	Alto	80	**88,9**
Índice de cumplimiento							**63,12**

La última columna representa los valores ajustados en función de la categoría del sistema. Al ser sistema de categoría Alta para calcular el valor ajustado de las medidas se aplica la fórmula (ver 14.1.3):

*Valor ajustado = (valor de la madurez de la medida de seguridad * 100) /90*

Por ejemplo:

- [mp.info.6 Limpieza de documentos]: Aplica desde nivel bajo a la dimensión de confidencialidad. El cálculo sería el siguiente:

  Valor Ajustado mp.info.6 = (50 x 100) / 90= 55,6%

- [mp.info.2 Calificación de la información]: A esta medida se le ha asignado un valor de 80 que ajustado sería el siguiente:

  Valor Ajustado mp.info.2 = (80 x 100) / 90= 88,9%

- [op.exp.8: Registro de la actividad de los usuarios]: A esta medida se le ha asignado un nivel bajo correspondiente a Trazabilidad sin embargo al ser la categoría del sistema alta, el nivel mínimo exigido para alta es 90% y por tanto se precisa ajustar como en el caso anterior. El cálculo sería el siguiente:

  Valor Ajustado op.exp.8 = (10 x 100) / 90= 11,1 %

El IC se calculará como la media de los valores ajustados (los de las medidas que aplican dados los niveles de sistema). El valor obtenido en este ejemplo es: 63,12%.

ANEXO C. CALCULO AUTOMÁTICO DEL ÍNDICE DE MADUREZ Y DE CUMPLIMIENTO (ARCHIVO EXCEL)

El anexo C está constituido por un documento Excel. Dicho documento permite, introduciendo los valores asociados a las 75 medidas y los niveles asociados a las dimensiones de seguridad, obtener de forma automática los valores asociados al Índice de Madurez y el Índice de Cumplimiento.

En primer lugar, se deben indicar los niveles asociados a las dimensiones de seguridad en la tabla que se encuentra en la parte superior derecha (de la celda H5 a la celda L5). Los valores que se pueden registrar son los siguientes:

- **A:** Nivel Alto
- **M:** Nivel Medio
- **B:** Nivel Bajo
- **N/A:** Dadas las características del sistema, se determina que no está adscrito ningún nivel a la dimensión concreta. Esta selección debe estar pertinentemente justificada.

La categoría del Sistema se autocompletará con el nivel más alto asociado a algunas de las dimensiones.

Los valores asociados a las 75 medidas deben ser registrados en la columna I (en concreto, desde la celda [I11] a la [I85]).

En caso de que haya medidas que no deban ser tenidas en cuenta al considerar que alguna dimensión de seguridad no está adscrita a ningún nivel, el valor correspondiente a dicha medida (columna I) debería de registrarse como **un guión** (-).

A continuación, se muestra un ejemplo. Para el sistema en cuestión, se ha considerado que la dimensión de disponibilidad no tiene adscrito ningún nivel. Por tanto, las medidas que sólo estén asociadas a la disponibilidad no se tendrán en cuenta ni para el cálculo del Índice de Madurez ni para el del Índice de Cumplimiento.

ORDEN	MEDIDAS	DIMENSIONES	B	M	A	VAL.	VALORES AJUSTADOS
6	[op.pl.2]	CAT	aplica	aplica	aplica	50	55,6
7	[op.pl.3]	CAT	aplica	aplica	aplica	50	55,6
8	[op.pl.4]	D	n.a.	aplica	aplica	-	
9	[op.pl.5]	CAT	n.a.	n.a.	aplica	50	55,6
10	[op.acc.1]	AT	aplica	aplica	aplica	80	88,9
11	[op.acc.2]	ICAT	aplica	aplica	aplica	80	88,9