centro criptológico nacional

Perfil de Cumplimiento Especifico
CCN-STIC 891

Perfil de Cumplimiento Especifico para Salud
Prestación sanitaria a pacientes
(Atención Primaria y Atención Especializada)

Febrero 2024

MINISTERIO DE DEFENSA

Catálogo de Publicaciones de la Administración General del Estado
https://cpage.mpr.gob.es

Edita:

MINISTERIO DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

CCN centro criptológico nacional

CENTRO CRIPTOLOGICO NACIONAL
cn=CENTRO CRIPTOLOGICO NACIONAL, 2.5.4.97=VATES-S2800155J, ou=CENTRO CRIPTOLOGICO NACIONAL, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2024.03.01 11:12:03 +01'00'

Pº de la Castellana 109, 28046 Madrid

NIPO: 083-24-093-4

Fecha de Edición: febrero de 2024

ÍNDICE

1. INTRODUCCIÓN

En virtud del principio de proporcionalidad y para facilitar la conformidad con el Esquema Nacional de Seguridad (ENS) a determinadas entidades o sectores de actividad concretos, se podrán implementar perfiles de cumplimiento específicos que comprenderán aquel conjunto de medidas de seguridad que, trayendo causa del preceptivo análisis de riesgos, resulten de aplicación para una concreta categoría de seguridad.

Un perfil de cumplimiento específico es un conjunto de medidas de seguridad, comprendidas o no en el Real Decreto 311/2022, de 3 de mayo, que, como consecuencia del preceptivo análisis de riesgos, resulten de aplicación a una entidad o sector de actividad concreta y para una determinada categoría de seguridad.

Las Guías CCN-STIC, del Centro Criptológico Nacional, podrán establecer perfiles de cumplimiento específicos para entidades o sectores concretos, que incluirán la relación de requisitos, medidas y refuerzos que en cada caso resulten aplicables, o los criterios para su determinación.

El Centro Criptológico Nacional, en el ejercicio de sus competencias, validará y publicará los correspondientes perfiles de cumplimiento específicos que se definan, como se dispone en el artículo 30.3 del ENS, permitiendo a aquellas entidades comprendidas en su ámbito de aplicación alcanzar una mejor y más eficiente adaptación al ENS, racionalizando los recursos requeridos sin menoscabo de la protección perseguida y exigible, todo ello de acuerdo con las instrucciones técnicas de seguridad y guías de seguridad aprobadas conforme a lo previsto en la disposición adicional segunda.

Las auditorías se realizarán en función de la categoría del sistema y, en su caso, del perfil de cumplimiento específico que corresponda, según lo dispuesto en el Anexo I y Anexo III del Real Decreto 311/2022, de 3 de mayo, y de conformidad con lo regulado en la Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los Sistemas de la Información.

A tal fin, tras realizar un análisis de riesgos contemplando las vulnerabilidades y amenazas generalizadas a las que hacen frente todas las entidades, públicas o privadas, orientadas a la **prestación sanitaria a pacientes en lo relativo a la ejecución de los servicios de Atención Primaria y Atención Especializada**, con el objetivo de garantizar la máxima seguridad de los sistemas de información necesarios para la prestación de dichos servicios, se da cumplimiento al mandato impuesto al CCN validando el siguiente **Perfil de Cumplimiento Especifico para garantizar un nivel mínimo de seguridad a las organizaciones en su ámbito de aplicación**.

2. SOBRE LA APLICABILIDAD DEL ENS

2.1 Ámbito de aplicación del ENS

El Real Decreto 311/2022, de 3 de mayo, por el que se regula el ENS, es una norma jurídica de obligado cumplimiento, según su art. 2, para los sistemas de información de, entre otros:

- Todo el sector público español, según lo determina el art. 2 de la Ley 40/2015.
- Las entidades del sector privado, cuando, en virtud de una relación contractual, convenio o encomienda de gestión, presten servicios o provean soluciones a las entidades del sector público para el ejercicio por éstas de sus competencias y potestades administrativas.

En el alcance de este Perfil de Cumplimiento Específico para Salud (PCE-SALUD), se pueden considerar como entidades del sector privado, las entidades **colaboradoras en virtud de los conciertos celebrados al amparo de la legislación específica** que corresponda a las diferentes administraciones públicas competentes, dedicadas a la prestación de servicios sanitarios con medios ajenos a las referidas administraciones, según se determina en la disposición adicional tercera de la Ley 16/2003, de 28 de mayo, de cohesión y calidad del Sistema Nacional de Salud.

2.2 Determinación del alcance

El alcance del PCE-SALUD comprende la prestación sanitaria a pacientes en lo relativo a la ejecución de los servicios de Atención Primaria y Atención Especializada.

No obstante, hay una serie de **servicios que quedan excluidos**, como son aquellos considerados de soporte a los servicios finalistas dirigidos a pacientes, como son:

- **Servicios administrativos** relativos a la gestión administrativa de los procesos asistenciales a pacientes y de la tarjeta sanitaria. Archivo documental (excluyendo datos de las patologías de los pacientes y sus tratamientos, que sí que quedan incluidos). Gestión contable, presupuestaria, tesorería y de las compras y aprovisionamientos propias de los servicios finalistas prestados a los pacientes.
- **Gestión de personal** abarcando desde los procesos de selección, hasta el pago de nóminas y control de la relación laboral, estatutaria o funcionarial con los empleados de los servicios asistenciales y, en su caso de soporte.
- **Servicios de Atención e Información al paciente**, como son las sugerencias, quejas y reclamaciones relacionadas con el ámbito asistencial. Sí que quedan incluidos la gestión de las peticiones de clientes y las citaciones.
- **Servicios de Tecnologías de la Información y Comunicaciones** relacionados con los Sistemas de gestión de la información que dan soporte a los servicios asistenciales.

2.3 Organismos de certificación del ENS

Las Certificaciones de Conformidad con el ENS, incluidas las que se rijan por este PCE-SALUD, las pueden otorgar los siguientes organismos de certificación que se basarán internamente entre otras, en la norma ISO/IEC 17065:2012:

- Una Entidad de Certificación (EC) acreditada por la Entidad Nacional de Acreditación (ENAC).
- Un Órgano de Auditoría Técnica (OAT) del Sector Público, reconocido por el Centro Criptológico Nacional (CCN), en su ámbito de competencias.
- En determinados casos específicos, directamente el CCN.

3. DECLARACIÓN DE APLICABILIDAD

3.1 Consideraciones previas

Como es sabido, la declaración de aplicabilidad comprende el conjunto de medidas de seguridad que son de aplicación para el cumplimiento del ENS en un sistema concreto. Tal conjunto de medidas dependerá de la categoría del sistema y de los niveles asociados a las dimensiones de seguridad.

En el Anexo II del RD 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, se tiene en cuenta para cada medida de seguridad, no únicamente la aplicabilidad de requisitos base, sino la de posibles refuerzos obligatorios.

Se ha determinado así, para aquellas organizaciones en el ámbito de la prestación de asistencia sanitaria en relación a la Atención Primaria y la Atención Especializada, las medidas que son de aplicación, y, en caso de aplicar, la exigencia de los diferentes requisitos base y de los posibles refuerzos obligatorios, mediante una tabla modulada mediante los comentarios del apartado 4 de este mismo documento.

Debe tenerse en cuenta que existen diferentes tipos de organizaciones en el ámbito de este PCE-SALUD. En consecuencia, podría ser que alguna de esas organizaciones, en base a sus especificidades (al riesgo), se viera obligada a ajustar su Declaración de Aplicabilidad a requisitos más exigentes del ENS que los determinados en este Perfil de Cumplimiento Específico. Esta circunstancia podría llegar a ser debida, por ejemplo, a que la entidad trate categorías especiales de datos sensibles de salud (art. 9 RGPD), siendo importante recordar en ese caso que, conforme establece el artículo 3 del RD 311/2022, se tendrán asimismo en cuenta las posibles salvaguardas resultantes del análisis de riesgos de protección de datos (art. 24 RGPD) y de la EIPD (en los supuestos de aplicación art. 35 RGPD).

No debemos olvidar que esta Guía refleja un perfil de cumplimiento específico para los sistemas de información involucrados en el sector salud, que contempla exclusivamente ciertos REQUISITOS ESENCIALES o MÍNIMOS de seguridad, siendo lo deseable que las organizaciones que decidan adoptarlo asuman el compromiso de elevar las medidas de seguridad por encima del nivel Medio, especialmente en aquellas

situaciones en las que un compromiso con la confidencialidad y la integridad se correspondan con los resultados del preceptivo análisis de riesgos.

En la tabla de criterios de aplicación se reproduce literalmente la exigencia de requisitos base y refuerzos obligatorios del Anexo II del ENS para cada una de las categorías del sistema, adicionando a la derecha la columna 'Aplicación' con los requisitos específicos para este perfil, junto a una columna 'Ref' con la referencia al detalle de aplicación para aquellas medidas con exigencias distintas a las determinadas por la categoría del ENS que se considera.

3.2 Detalle de la Declaración de Aplicabilidad

Dimensiones						
Afectadas	**CAT B**	**CAT M**	**CAT A**			
				Medida	**Aplicación[1]**	**Ref.**
Categoría	aplica	aplica	aplica	org.1	TODAS	
Categoría	aplica	aplica	aplica	org.2	TODAS	
Categoría	aplica	aplica	aplica	org.3	TODAS	
Categoría	aplica	aplica	aplica	org.4	TODAS	
Categoría	aplica	+ R1	+ R2	op.pl.1	MEDIA *	**4.1**
Categoría	aplica	+ R1	+ R1 + R2 + R3	op.pl.2	MEDIA *	**4.2**
Categoría	aplica	aplica	aplica	op.pl.3	TODAS	
D	aplica	+ R1	+ R1	op.pl.4	N/A	
Categoría	n.a.	aplica	aplica	op.pl.5	MEDIA *	**4.3**
T A	aplica	+ R1	+ R1	op.acc.1	Medio	
C I T A	aplica	aplica	+ R1	op.acc.2	Medio	
C I T A	n.a.	aplica	+ R1	op.acc.3	N/A	
C I T A	aplica	aplica	aplica	op.acc.4	TODOS	
C I T A	+ [R1 o R2 o R3 o R4]	+ [R2 o R3 o R4] + R5	+ [R2 o R3 o R4] + R5	op.acc.5	Bajo *	**4.4**
C I T A	+ [R1 o R2 o R3 o R4] + R8 + R9	+ [R1 o R2 o R3 o R4] + R5 + R8 + R9	+ [R1 o R2 o R3 o R4] + R5 + R6 + R7 + R8 + R9	op.acc.6	Medio	
Categoría	aplica	aplica	aplica	op.exp.1	TODAS	
Categoría	aplica	aplica	aplica	op.exp.2	TODAS	
Categoría	aplica	+ R1	+ R1 + R2 + R3	op.exp.3	MEDIA	
Categoría	aplica	+ R1	+ R1 + R2	op.exp.4	MEDIA	
Categoría	n.a.	aplica	+ R1	op.exp.5	N/A	
Categoría	aplica	+ R1 + R2	+ R1 + R2 + R3 + R4	op.exp.6	MEDIA	
Categoría	aplica	+ R1 + R2	+ R1 + R2 + R3	op.exp.7	MEDIA	
T	aplica	+ R1 + R2 + R3 + R4	+ R1 + R2 + R3 + R4 + R5	op.exp.8	Bajo	
Categoría	aplica	aplica	aplica	op.exp.9	BÁSICA *	**4.5**
Categoría	aplica	+ R1	+ R1	op.exp.10	MEDIA	
Categoría	n.a.	aplica	aplica	op.ext.1	N/A	
Categoría	n.a.	aplica	aplica	op.ext.2	N/A	
Categoría	n.a.	n.a.	aplica	op.ext.3	N/A	

[1] En la columna "Aplicación", se reflejará la categoría (BÁSICA, MEDIA, ALTA) que corresponda en caso de que en esa medida se vean afectadas las cinco (5) dimensiones de seguridad (Confidencialidad- C, Integridad-I, Autenticidad-A, Trazabilidad-T, Disponibilidad-D); si afecta a cualquier categoría del sistema se reflejará 'TODAS'. En caso, de que no se vean afectadas las cinco (5) dimensiones, se reflejará el nivel a aplicar (Bajo, Medio, Alto).

Dimensiones						
Afectadas	CAT B	CAT M	CAT A	Medida	Aplicación[1]	Ref.
Categoría	n.a.	aplica	+ R1	op.ext.4	N/A	
Categoría	aplica	+ R1	+ R1 + R2	op.nub.1	MEDIA	
D	n.a.	aplica	aplica	op.cont.1	MEDIO	
D	n.a.	n.a.	aplica	op.cont.2	MEDIO *	**4.6**
D	n.a.	n.a.	aplica	op.cont.3	N/A	
D	n.a.	n.a.	aplica	op.cont.4	N/A	
Categoría	aplica	+ R1	+ R1 + R2	op.mon.1	BÁSICA	
Categoría	aplica	+ R1 + R2	+ R1 + R2	op.mon.2	BÁSICA	
Categoría	aplica	+ R1 + R2	+ R1 + R2 + R3 + R4 + R5 +R6	op.mon.3	MEDIA *	**4.7**
Categoría	aplica	aplica	aplica	mp.if.1	N/A	
Categoría	aplica	aplica	aplica	mp.if.2	N/A	
Categoría	aplica	aplica	aplica	mp.if.3	N/A	
D	aplica	+ R1	+ R1	mp.if.4	MEDIO	
D	aplica	aplica	aplica	mp.if.5	BÁSICO	
D	n.a.	aplica	aplica	mp.if.6	MEDIO	
Categoría	aplica	aplica	aplica	mp.if.7	N/A	
Categoría	n.a.	aplica	aplica	mp.per.1	N/A	
Categoría	aplica	+ R1	+ R1	mp.per.2	BÁSICA	
Categoría	aplica	aplica	aplica	mp.per.3	BÁSICA	
Categoría	aplica	aplica	aplica	mp.per.4	BÁSICA	
Categoría	aplica	+ R1	+ R1	mp.eq.1	BÁSICA	
A	n.a.	aplica	+ R1	mp.eq.2	MEDIO *	**4.8**
Categoría	aplica	aplica	+ R1 + R2	mp.eq.3	BÁSICA	
C	aplica	+ R1	+ R1	mp.eq.4	BAJO *	**4.9**
Categoría	aplica	aplica	aplica	mp.com.1	TODAS	
C	aplica	+ R1	+ R1 + R2 + R3	mp.com.2	MEDIO	
I A	aplica	+ R1 + R2	+ R1 + R2 + R3 + R4	mp.com.3	BAJO	
Categoría	n.a.	+ [R1 o R2 o R3]	+ [R2 o R3] + R4	mp.com.4	N/A	
C	n.a.	aplica	aplica	mp.si.1	N/A	
C I	n.a.	aplica	+ R1 + R2	mp.si.2	N/A	
Categoría	aplica	aplica	aplica	mp.si.3	TODAS	
Categoría	aplica	aplica	aplica	mp.si.4	TODAS	
C	aplica	+ R1	+ R1	mp.si.5	BAJO	
Categoría	n.a.	+ R1 + R2 + R3 + R4	+ R1 + R2 + R3 + R4	mp.sw.1	MEDIA	
Categoría	aplica	+ R1	+ R1	mp.sw.2	BÁSICA	
Categoría	aplica	aplica	aplica	mp.info.1	TODAS	
C	n.a.	aplica	aplica	mp.info.2	N/A	
I A	aplica	+ R1 + R2 + R3	+ R1 + R2 + R3 + R4	mp.info.3	BAJO	
T	n.a.	n.a.	aplica	mp.info.4	N/A	
C	aplica	aplica	aplica	mp.info.5	BAJO	
D	aplica	+ R1	+ R1 + R2	mp.info.6	MEDIO *	**4.10**
Categoría	aplica	aplica	aplica	mp.s.1	BÁSICA	
Categoría	+ [R1 o R2]	+ [R1 o R2]	+ R2 + R3	mp.s.2	BÁSICA	
Categoría	aplica	aplica	+ R1	mp.s.3	MEDIA	
D	n.a.	aplica	+ R1	mp.s.4	MEDIA *	**4.11**

Detalles del criterio específico de aplicación de la medida en el apartado 4 de este documento.

Se considera que la medida, salvo excepciones, no será de aplicación al PCE-SALUD.

3.3 Medidas que son de aplicación

Aplican al presente PCE-SALUD **54 de las 73 medidas de seguridad** definidas en el Anexo II del RD 311/2022.

Veintitrés (23) de dichas medidas de seguridad se adoptan de las requeridas para sistemas de categoría MEDIA, otras diecinueve (19) para sistemas de categoría BÁSICA y (12) comunes a todas las categorías.

También existen consideraciones para once (11) medidas, las cuales se han marcado con referencias de color azul al apartado 4 de este PCE-SALUD.

Se muestran a continuación aquellas diecinueve (19) medidas que no aplican de base en el PCE-SALUD, aunque podrían incorporarse para mitigar aquellos riesgos evaluados como inaceptables, por una organización específica, tras realizar el correspondiente análisis de riesgos:

Marco operacional:

[op.pl.4] Dimensionamiento / Gestión de la capacidad.

[op.acc.3] Segregación de funciones y tareas.

[op.exp.5] Gestión de cabios.

[op.ext.1] Contratación y acuerdos de nivel de servicio.

[op.ext.2] Gestión diaria.

[op.ext.3] Protección de la cadena de suministro.

[op.ext.4] Interconexión de sistemas.

[op.cont.3] Pruebas periódicas.

[op.cont.4] Medios alternativos.

Medidas de Protección:

[mp.if.1] Áreas separadas y con control de acceso.

[mp.if.2] Identificación de las personas.

[mp.if.3] Acondicionamiento de los locales.

[mp.if.7] Registro de entrada y salida de equipamiento.

[mp.per.1] Caracterización del puesto de trabajo.

[mp.com.4] Separación de flujos de información en la red.

[mp.si.1] Marcado de soportes.

[mp.si.2] Criptografía.

[mp.info.2] Calificación de la información.

[mp.info.4] Sellos de tiempo.

4. CRITERIOS DE APLICACIÓN DE MEDIDAS

4.1 [op.pl.1] Análisis de Riesgos

Con independencia del Análisis de Riesgos (AA.RR.) general que se ha realizado para poder elaborar este PCE-SALUD, cada entidad en el ámbito del mismo que lo adopte deberá realizar, al menos con periodicidad anual o siempre que se modifique de forma relevante el sistema de información que soporta los servicios en el alcance, una nueva iteración del AA.RR. orientado a la propia organización.

Para elaborar el AA.RR. podrá emplearse la herramienta o los recursos que se estimen oportunos, mientras sigan una clara metodología. Ésta considerará los activos más valiosos del sistema y un catálogo de amenazas que puedan llegar a materializarse para cada tipología de activo.

4.2 [op.pl.2] Arquitectura de seguridad

Se construirá un sistema de gestión de la seguridad, basado en la mejora continua, que se aplicará sobre el sistema de información que soporte los servicios en el alcance.

Se controlará la documentación del sistema (políticas, normas internas, procedimientos, actas, etc.), se planificarán las revisiones de la PSI, del AA.RR. y del BIA, se coordinarán las auditorías internas, así como las de certificación, entre otras actuaciones necesarias no solo para mantener la seguridad del sistema con el transcurrir del tiempo, sino para su mejora continua.

4.3 [op.pl.5] Componentes certificados

Se considera relevante exigir la certificación de los componentes a los proveedores.

Su aplicación a los equipos médicos probablemente requerirá de medidas compensatorias (basadas en disponer de otro tipo de certificación/estándar de seguridad, acreditación de producto reconocida en el sector, etc.), por lo que podría plantearse para esa tipología de equipos como una mejora a la licitación.

4.4 [op.acc.5] Mecanismo de autenticación (usuarios externos)

Para el acceso a servicios de historia clínica y relacionados, serán de aplicación los refuerzos [R2 o R3 o R4].

Para otros servicios como son la petición de cita, o similares, el acceso se podrá realizar mediante el Código de Identificación Personal (CIP) de la tarjeta sanitaria complementado, por ejemplo, con la fecha de nacimiento del paciente.

4.5 [op.exp.9] Registro de la gestión de incidentes

Esta medida se orientará especialmente al aprendizaje de los incidentes registrados para, partiendo de ellos, obtener conclusiones que permitan mejorar la seguridad del sistema, evitando así que vuelvan a repetirse los mismos incidentes, o se produzcan otros nuevos relacionados con la misma causa.

4.6 [op.cont.2] Plan de Continuidad

La elaboración de un Plan de Continuidad no es una medida que aplique a este PCE-SALUD ya que es un requisito únicamente para sistemas de información cuya dimensión de Disponibilidad 'D' tenga el valor ALTO.

No obstante, cada organización que se acoja al PCE-SALUD, en función de un Análisis de Riesgos (AA.RR.) específico que realice, podrá decidir elaborarlo, o no.

Caso de decidí realizarlo, recordar que no es necesario recoger en él a todos los servicios en el alcance. Por ejemplo, una organización podría elaborar el Plan de Continuidad circunscrito a urgencias médicas y hospitalarias.

4.7 [op.mon.3] Vigilancia

Como norma general, este servicio será proporcionado externamente por un tercero, como puede ser un CERT de referencia o la Red Nacional de SOC.

4.8 [mp.eq.2] Bloqueo del puesto de trabajo

Como norma general se bloquearán los puestos de trabajo al cabo de un tiempo prudencial, que se estimará en función del tipo de equipamiento y su entorno operativo.

Se prestará especial atención a los puestos de trabajo móviles que estén ubicados en zonas públicas al alcance de pacientes, visitas, etc.

Esta medida no será de aplicación a 'equipos médicos' empleados en los servicios de urgencias, en los que el tiempo necesario para desbloqueo puede poner en riesgo la vida de los pacientes. En esas circunstancias se procurará tenerlos vigilados en la medida de lo posible.

4.9 [mp.eq.4] Otros dispositivos conectados a la red

Esta medida focalizará especialmente a los dispositivos médicos conectados a la red interna y especialmente a aquellos que se conocen en inglés como *Internet of Medical Things* (IoMT).

Debe asimismo considerarse el futuro desarrollo normativo en base al Real Decreto-ley 7/2022, de 29 de marzo, sobre requisitos para garantizar la seguridad de las redes y servicios de comunicaciones electrónicas de quinta generación (5G), respecto a suministradores relacionados con las redes y servicios de comunicaciones electrónicas

5G, con especial atención a aquellos considerados “de alto riesgo” por la precitada normativa.

4.10 [mp.info.6] Copias de seguridad

Esta medida se cetra en realizar copias de seguridad efectivas y documentadas en base a elaborar procedimientos adecuados que indiquen la frecuencia de las copias, los requisitos de almacenamiento en el lugar donde se realizan y en otras ubicaciones externas (ya sean propias o contratadas como servicio de custodia de copias), así como las medidas de seguridad respecto a las mismas.

No obstante, se considera una buena práctica incluir en los procedimientos la verificación y prueba de restauración regular de las copias que se realicen.

4.11 [mp.s.4] Protección frente a Denegación de Servicio

Se dimensionarán los componentes del sistema, especialmente los accesibles a través de Internet, con capacidad suficiente para atender con holgura la carga prevista.

Asimismo, se desplegarán tecnologías para prevenir los ataques de denegación de servicio conocidos, ya sean propias o contratadas a la operadora de servicios de telecomunicaciones e internet (TSP).

No obstante, se recomienda adicionalmente establecer sistemas de detección y tratamiento de esta tipología de ataques.

PUBLICACIONES DE DEFENSA

GOBIERNO DE ESPAÑA
MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA
SUBDIRECCIÓN GENERAL DE PUBLICACIONES Y PATRIMONIO CULTURAL