centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 891

Anexo III. Categoría del Sistema determinada por la Postura de Seguridad
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
SUBSECRETARÍA 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
2024.02.08 12:32:57 +01'00'

Pº de la Castellana 109, 28046 Madrid

Fecha de Edición: febrero de 2024

ÍNDICE

1. OBJETO

El presente informe se elabora para documentar la categorización del sistema que se Certifica de Conformidad con el Esquema Nacional de Seguridad, en base al Perfil de Cumplimiento Específico de Salud (PCE-SALUD).

Su objetivo es que pase a formar parte del conjunto documental del sistema de información que soporta los servicios orientados a la prestación sanitaria a pacientes.

2. ALCANCE DEL SISTEMA

Para determinar el alcance de los sistemas a certificar es necesario partir de un catálogo identificando los activos esenciales, es decir, los servicios prestados a los pacientes y la información que estos servicios tratan.

Se recomienda, en la medida de lo posible, englobar los activos esenciales en el menor número de sistemas posibles. En este sentido, se ha considerado que existe un único sistema, entendido éste en sentido amplio como el conjunto de personas y tecnología que soporta dichos activos esenciales y que se protegerá con la implantación de las medidas de seguridad descritas el Perfil de Cumplimiento Específico para Salud (PCE-SALUD).

Se define la cartera común de servicios del Sistema Nacional de Salud en el artículo 8 de la Ley 16/2003, de 28 de mayo, de cohesión y calidad del Sistema Nacional de Salud, como el "*conjunto de técnicas, tecnologías o procedimientos, entendiendo por tales cada uno de los métodos, actividades y recursos basados en el conocimiento y experimentación científica, mediante los que se hacen efectivas las prestaciones sanitarias*".

Se ha elaborado un catálogo de servicios estándar, de acuerdo con la cartera común de servicios mínimos. Se ha dividido entre servicios de Atención Primaria, servicios de Atención Especializada y servicios de soporte.

2.1 Servicios de Atención Primaria

Respecto a la Atención Primaria, identificamos:

SERVICIOS IDENTIFICADOS	DESCRIPCIÓN DE LOS SERVICIOS	DIVISIONES
Servicios de Atención Primaria	La atención primaria es el nivel básico e inicial de atención, que garantiza la globalidad y continuidad de la atención a lo largo de toda la vida del paciente, actuando como gestor y coordinador de casos y regulador de flujos. Comprenderá actividades de promoción de la salud, educación sanitaria, prevención de la enfermedad, asistencia sanitaria, mantenimiento y recuperación de la salud, así como la rehabilitación física y el trabajo social".	Medicina general y pediatría
		Gestión de información administrativa y clínica de los procesos asistenciales de los pacientes
		Unidades de apoyo
		Electromedicina
		Acciones de promoción de la salud
		Enfermería

SERVICIOS IDENTIFICADOS	DESCRIPCIÓN DE LOS SERVICIOS	DIVISIONES
		Transporte urgente
		Trabajo social

2.2 Servicios de Atención Especializada

Asimismo, respecto a la Atención Especializada, identificamos:

SERVICIOS IDENTIFICADOS	DESCRIPCIÓN DE LOS SERVICIOS	DIVISIONES
Servicios de Atención Especializada	La atención especializada comprende las actividades asistenciales, diagnósticas, terapéuticas y de rehabilitación y cuidados, así como aquellas de promoción de la salud, educación sanitaria y prevención de la enfermedad, cuya naturaleza aconseja que se realicen en este nivel. La atención especializada garantizará la continuidad de la atención integral al paciente, una vez superadas las posibilidades de la atención primaria y hasta que aquél pueda reintegrarse en dicho nivel.	Gestión de información administrativa y clínica de los procesos asistenciales de los pacientes
		Consultas externas
		Consultas Externas
		Atención paliativa a enfermos terminales
		Rehabilitaciones pacientes
		Especialidades: cardiología, oncología, neurología, traumatología, ginecología, alergología, oftalmología, mental.
		Área Quirúrgica
		Cirugía general y especializada (quirófanos)
		Área de diagnóstico y apoyo clínico
		Análisis Clínicos
		Anatomía Patológica
		Microbiología
		Protección radiológica
		Diagnóstico por imagen
		Hospital de Día
		Hospital a Domicilio
		Hospitalización
		Trabajo social
		Transporte urgente

2.3 Servicios de soporte

Se han excluido la mayoría de servicios de soporte a los anteriores, tales como:

- **Servicios administrativos** relativos a la gestión administrativa de los procesos asistenciales a pacientes y de la tarjeta sanitaria. Archivo documental (referido a documentación administrativa). Gestión contable, presupuestaria, tesorería y de las compras y aprovisionamientos propias de los servicios antes citados.

- **Gestión de personal** relativos a la gestión del personal 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** relativos a la gestión de quejas y sugerencias, así como reclamaciones relacionadas con el ámbito asistencial**.**
- **Servicios de Tecnologías de la Información y Comunicaciones** relacionados con los Sistemas de gestión de la información que dan soporte a los servicios asistenciales.

Aparte de dichas exclusiones, sí que se consideran los siguientes servicios de soporte:

SERVICIOS IDENTIFICADOS	DESCRIPCIÓN DE LOS SERVICIOS	DIVISIONES
Servicios de soporte	Aquellos servicios de soporte directamente relacionados con la prestación sanitaria a los pacientes.	Historia Clínica. Gestión del archivo documental conteniendo datos de patologías de los pacientes, sus tratamientos, etc.
		Gestión de las peticiones de los pacientes, citaciones, etc.

2.4 Información requerida por los servicios

Se considera asimismo la información requerida para poder realizar la prestación sanitaria a los pacientes, siendo la más relevante la Historia Clínica y la información relacionada con peticiones y citaciones de pacientes.

En este sentido, el art. 14.2 de la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica, señala: "*Cada centro archivará las historias clínicas de sus pacientes, cualquiera que sea el soporte papel, audiovisual, informático o de otro tipo en el que consten, de manera que queden garantizadas su seguridad, su correcta conservación y la recuperación de la información*".

3. VALORACIÓN DE ACTIVOS ESENCIALES: SERVICIOS E INFORMACIÓN

El *Responsable del Servicio y Responsable de la Información* contando con la opinión del *Responsable de Seguridad* y del *Responsable del Sistema,* suscribe la valoración de los Servicios y de la Información teniendo en cuenta la naturaleza de cada uno y la normativa que pudiera ser de aplicación, adoptando una **'Postura de Seguridad' basada en el Perfil de Cumplimiento Específico para Salud (PCE-SALUD).**

La precitada postura de seguridad adoptada deberá ser revisada con el transcurso del tiempo en función de la mejora continua de la seguridad alcanzada por el sistema de información que soporta los servicios y la información tratada por éstos.

4. CATEGORÍA DEL SISTEMA

Se determina la categoría del sistema, partiendo de la Postura de Seguridad resultante de la Declaración de Aplicabilidad que incorpora el PCE-SALUD, obtenida en base a las medidas determinadas para mitigar los riesgos generales identificados en relación a los activos esenciales incluidos en el alcance.

Eso no es obstáculo para que cada organización, en base al Análisis de Riesgos particular que realice, determine salvaguardas adicionales a las determinadas para este PCE-SALUD. Para mayor abundamiento, no debe olvidarse 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.

De las **54** medidas adoptadas, **43** corresponden a categoría MEDIA o son comunes a MEDIA y BÁSICA (equiparando categoría y nivel a efectos de simplificación), lo que representa la mayoría y 11 a categoría BÁSICA (o nivel Bajo en alguna dimensión).

Como conclusión, la categoría del sistema resultante, en base a la Postura de Seguridad conforme la Declaración de Aplicabilidad correspondiente al PCE-SALUD es la siguiente:

SERVICIOS ESENCIALES		VALORACIÓN / CATEGORIZACIÓN					
SERVICIOS	INFORMACION	C	I	D	A	T	CATEGORÍA
En el alcance	En el alcance	M	M	M	M	M	MEDIA

ESTABECIMIENTO DE LA POSTURA DE SEGURIDAD PARA SERVICIOS E INFORMACIÓN	CATEGORÍA DEL SISTEMA EN BASE AL PCE-RES
Firmado:	Firmado:
Responsable del Servicio y Responsable de la Información	*Responsable de Seguridad*

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