Subdirección General de Coordinación Normativa
Refª: L/4/2022-Z
ILA

Remitido a esta unidad administrativa el **Anteproyecto de Ley por el que se crea la Agencia de Ciberseguridad de la Comunidad de Madrid",** se comunica lo siguiente:

En relación con el contenido del **borrador del anteproyecto**:

En la Exposición de Motivos, concretamente en el último párrafo de la primera página, se señala que la Agencia de Ciberseguridad que se pretende crear estará sometida al derecho privado. Sin embargo, en el artículo 1.3 también indica que estará sujeta al derecho administrativo en el ejercicio de aquellas potestades administrativas que tenga atribuida. Se propone que este aspecto también se recoja al presentar el régimen jurídico de la Agencia en la Exposición de Motivos.

Asimismo en el artículo 10, relativo a la financiación, se señalan las subvenciones como recursos de la Agencia tanto en el apartado a) como en el apartado d), por lo que parecería conveniente que se recogieran únicamente en uno de los dos apartados.

Finalmente, se recomienda adaptar el texto del borrador a las Directrices de técnica normativa, establecidas mediante Acuerdo del Consejo de Ministros, de 22 de julio de 2005, en cuanto a los títulos de los artículos y la subdivisión y consiguiente numeración de los artículos 4, 5, 6, 7, 8, 10 y 13; asimismo señalar que el artículo 5 carece de apartado 1.

En relación con el contenido de la **Memoria de Análisis de Impacto Normativo**:

En primer lugar, no parece ser el último borrador elaborado o estar actualizado. El anteproyecto de ley que se acompaña no coincide en ciertos aspectos con lo recogido en la MAIN, como es el caso de la disposición adicional única que aparece en la página 10 de la MAIN pero no en el anteproyecto (Si bien tampoco se recoge en la página 8 de la MAIN cuando hace referencia a la estructura de la norma). Algo similar ocurre en relación con el artículo 3.2.d) al que se hace referencia en la página 10 de la MAIN, que no parece corresponderse con lo recogido en este artículo en el anteproyecto.

En la ficha de resumen ejecutivo, en el apartado de impacto económico y presupuestario se estima un gasto, el primer año, de 1.200.000€. Sin embargo, en el apartado 6.3 de la MAIN, en la tabla que desglosa el presupuesto estimado para el primer año de funcionamiento, se recoge un gasto total estimado de 1.515.225€.

Por su parte, la **Dirección General de Sistemas de Información y Equipamientos Sanitarios del Servicio Madrileño de Salud**, ha realizado las siguientes observaciones:

"*El desarrollo de la sociedad de la información requiere de un marco de confianza en los ciudadanos en la relación (con las Administraciones) a través de medios electrónicos*, se señala en el párrafo primero de la Exposición de Motivos. Continúa consagrando el *derecho de los ciudadanos a comunicarse con ellas a través de medios electrónicos*, lo que comporta para esas Administraciones la obligación de *crear las condiciones necesarias para optimizar el correcto funcionamiento de las infraestructuras esenciales en su relación con los ciudadanos.*

Continúa la misma Exposición de Motivos señalando que varios *retos y amenazas afectan al desarrollo de la sociedad de la información y ponen en peligro su seguridad La interrelación y dependencia de las infraestructuras y los servicios de comunicaciones hacen que su protección ante ciberamenazas se haya convertido en un pilar básico.*

En el Programa Marco Europa Digital 21-27, la Unión Europea establece que la ciberseguridad debe ser un pilar fundamental en el desarrollo de políticas públicas.

Estando absolutamente de acuerdo con las anteriores manifestaciones, parece correcta la conclusión de dotar a la Comunidad de Madrid de un organismo que actúe como catalizador de una cultura de ciberseguridad que genere un clima de confianza y seguridad que contribuya al desarrollo de la economía y la sociedad digital. Con la creación de esta Agencia de Ciberseguridad, se dota a esta Administración de un ente encargado de ayudar y cooperar en el cumplimiento del Esquema Nacional de Seguridad.

Desde hace tiempo supone una actuación absolutamente prioritaria para el Servicio Madrileño de Salud (SERMAS), todo aquello que tenga que ver con la ciberseguridad de todos sus sistemas en el ámbito sanitario. No solo referido a los pacientes, o en general a los ciudadanos en sus relaciones con esa administración sanitaria en lo referente a sus temas de salud, sino también a los profesionales sanitarios que son los responsables directos de los problemas de salud de esos ciudadanos, y de todos los datos que sus actuaciones producen y que están relaciones con las prestaciones sanitarias. Así mismo están dentro de esas actuaciones prioritarias en materia de ciberseguridad, buscar la adecuada coordinación y sinergias tanto con la Agencia para la Transformación Digital de la Comunidad de Madrid, como los órganos correspondientes de la Administración Central, como son el Centro Criptológico Nacional (CCN) y el Centro Nacional de Inteligencia (CNI).

Todo ello ha llevado a que dentro del SERMAS se haya desarrollado una importante y sólida estructura en todo aquello que son competencias de la Dirección General de Sistemas de Información y Equipamientos Sanitarios (DGSIES) que no sólo afecta a los Servicios Centrales del SERMAS, sino a todos y cada uno de los centros sanitarios e instituciones que dependen del mismo. No sólo desde el aspecto técnico y de estructuras, sino con un personal altamente cualificado en materia de protección de datos y de ciberseguridad.

Al respecto, advertir que el Servicio Madrileño de Salud (SERMAS), provee de asistencia sanitaria a los más de 6,6 millones de ciudadanos de la Comunidad de Madrid, se monitorizan más de 150.000 activos de información, dispone de más de 1.200 sistemas de información

sanitarios que engloban más de 430 centros de atención primaria, 35 hospitales y más de 80.000 puestos de trabajo.

No es casual la existencia de un CISO en la Consejería de Sanidad, adscrito a la DGSIES, o que el Delegado de Protección de Datos en esta Consejería esté sustituido por un Comité Delegado de Protección de Datos, también adscrito a la misma Dirección General.

Lo anterior tiene reflejo en la Ley 12/2001, de 21 de diciembre, de Ordenación Sanitaria de la Comunidad de Madrid, que recoge entre las competencias de la Consejería de Sanidad, la siguiente: " *(…) k) La definición y gestión del sistema de información y análisis de los factores que, por repercutir sobre la salud, puedan requerir acciones de la Autoridad Sanitaria".*

En este sentido, dentro de la referida Ley se señala que **la Consejería de Sanidad de la Comunidad de Madrid ejerce la función de Autoridad Sanitaria**. Para la garantía de los derechos de los ciudadanos y del interés público, corresponde a la Consejería de Sanidad las siguientes funciones como Autoridad Sanitaria:

a) El desarrollo de la función de aseguramiento a través de las Agencias Sanitarias.

b) La normativa en materia de organización del Sistema Sanitario, salud pública y de ordenación farmacéutica.

c) La ejecución de la legislación de productos farmacéuticos y sanitarios.

d) La autorización de apertura, modificación y cierre de centros, establecimientos y servicios sanitarios.

e) La definición de los estándares y mecanismos de acreditación para los centros, establecimientos y servicios sanitarios.

f) La realización de la evaluación e inspección sanitaria.

g) La coordinación de las relaciones administrativas e institucionales.

h) La creación, acreditación y supervisión de los Comités de Ética.

i) La promoción de la investigación, la formación y los estudios sanitarios.

De otra parte, a través del DECRETO 2/2022, de 26 de enero, por el que se establece la estructura directiva del Servicio Madrileño de Salud, se otorga a la *Dirección General de Sistemas de Información y Equipamiento Sanitario*, entre otras, las siguientes competencias:

"*a) La planificación, diseño, implantación y mantenimiento de los sistemas y tecnologías de la información para la organización y funcionamiento del Servicio Madrileño de Salud, de acuerdo con las necesidades explicitadas por las unidades directivas.*

b) La implantación de las aplicaciones informáticas y la garantía de su integración y homogeneidad en el ámbito sanitario.

(…)d) ***La autorización, diseño y posterior dirección y supervisión de cualquier iniciativa o proyecto en el ámbito del Servicio Madrileño de Salud que implique el uso o desarrollo***

de aplicaciones o elementos informáticos, independientemente de su alcance, tecnología o aplicación sobre la actividad asistencial.

f) El establecimiento de medidas de seguridad en el Servicio Madrileño de Salud, de acuerdo con la normativa vigente de las actividades de tratamiento que contengan datos de carácter personal, y la realización de auditorías en el ámbito de la protección de datos de carácter personal.

g) El establecimiento de mecanismos para garantizar el acceso y la autentificación de los usuarios a los sistemas de información en el Servicio Madrileño de Salud.

h) El establecimiento y promoción de estándares mínimos y comunes, y de la lógica de interconexión, que deberán seguir todas las entidades del Servicio Madrileño de Salud en el diseño y desarrollo de los sistemas de información de soporte, y garantizar su cumplimiento.

(…) j) La implantación, de acuerdo con las necesidades detectadas por la dirección del Servicio Madrileño de Salud, de nuevas Tecnologías de la Información y la Comunicación (TIC) y de tramitación electrónica en el Servicio Madrileño de Salud, que estén en relación con los ciudadanos, los profesionales y la atención sanitaria.

k) La participación en el desarrollo de los modelos organizativos y de procesos que integren los sistemas, las tecnologías de la información y la comunicación, que se hayan planificado desde la dirección del Servicio Madrileño de Salud.

(…) m) ***Garantizar la coordinación dentro de la estrategia de transformación digital del proyecto GENESIS, así como de los aspectos de seguridad y estandarización de tecnologías*** *que permitan la integración con los sistemas SERMAS. (…)".*

Teniendo en cuenta el contenido del "Artículo 3. Objeto y competencias." Del Anteproyecto de Ley por la que se crea la Agencia de Ciberseguridad de la Comunidad de Madrid, que en su apartado 1, señala "…*como objetivo dirigir y coordinar la ciberseguridad en la Administración de la Comunidad de Madrid y …*", se concluye fácilmente que su objetivo es dirigir y coordinar, y no sólo en el ámbito de la Administración sino en todos los ámbitos de la Comunidad de Madrid, como señala, tanto por su materia como por su extensión.

En el mismo artículo 3.2 ,se señala otro objetivo …*definir y velar por la ejecución de las políticas públicas en materia de ciberseguridad…"* con diversos apartados como casos particulares de ese objetivo.

En relación con estos objetivos, al hablar de ciberseguridad en el ámbito sanitario hay que tener en cuenta algunas cuestiones que obligan a considerarlo de una forma específica, no pudiendo ser incluido con carácter general en la Administración general o institucional. Así pues, debe tenerse en consideración que en el SERMAS se utilizan una gran de cantidad de dispositivos MIoT/OT (dispositivos médicos conectados en línea) que, dado el riesgo que pueden conllevar este tipo de aparatos, implican que sea necesario que se realicen tareas específicas de monitorización, detección y alertas ante eventos de seguridad que se generen.

Para lograr este objetivo la Oficina de Seguridad de Sistemas de Información de la DGSIES **está inscrito como instrumento que permite la prevención, detección, respuesta a amenazas y riesgos de seguridad como CERT Sectorial**, así como la coordinación e implantación de políticas y medidas de seguridad de la organización, y que, a su vez, presta

servicios tanto reactivos, como preventivos (monitorización, formación, concienciación, alertas), con el objeto de impulsar y dar soporte a la implantación de las medidas de seguridad en sus distintos centros.

El propio Centro Criptológico Nacional (CCN) en el recientemente publicado documento sobre el desarrollo de la red nacional de SOC recomienda que se utilicen servicios sectoriales para aquellos servicios esenciales como los del ámbito de salud, distribución alimentaria, aguas, etc.; dado que son propicios a ser objetivos de ciberataques.

Por lo anterior, **se propone que en el artículo 3.2 e) sobre Objetivo y competencias, se incluyan dentro de la colaboración que se prevé con otras entidades, expresamente a estos CERT/CSIRT sectoriales** y la necesaria participación y colaboración con los mismos. Para ello proponemos que quede redactado de la siguiente manera:

"*e) Constituir y gestionar el CSIRT (Equipo de Respuesta a Incidentes de Ciberseguridad) de referencia de la Comunidad de Madrid, ejerciendo las funciones de alerta temprana y de ayuda en la respuesta ante amenazas, vulnerabilidades, ataques e incidentes de seguridad, en colaboración con el resto de* ***CSIRT/CERT sectoriales de la Comunidad de Madrid****, nacionales e internacionales".*

Con carácter general, en cuanto a las competencias que este artículo 3.2 señala para la Agencia de Ciberseguridad, se produce una situación similar a la que se contempla en el caso de la Agencia para la Transformación Digital de la Comunidad de Madrid, que viene regulada en el artículo 10 de la Ley 7/2005, de 23 de diciembre, de Medidas Fiscales y Administrativas. Esta Ley lo resuelve con una Disposición Adicional que excluye del ámbito de competencias de la Agencia para la Transformación Digital todo lo específicamente relacionado con el ámbito sanitario, y lo hace de forma expresa: "*Las funciones de la Agencia de … de la Comunidad de Madrid no se extienden a las competencias sobre los sistemas de informática médica, gestión sanitaria y a aquellas relativas a las relaciones del sistema sanitario con los ciudadanos, profesionales sanitarios, oficinas de farmacia, sanidad privada y cualesquiera otras personas físicas o jurídicas distintas de la Administración de la Comunidad de Madrid, sus organismos autónomos, entidades de derecho público y demás entes públicos."*

Se propone una solución similar para el Anteproyecto de Ley por el que se crea la Agencia de Ciberseguridad de la Comunidad de Madrid, donde se debería añadir una Disposición Adicional que declarase que no se extienden al ámbito sanitario determinadas competencias de las incluidas en el artículo 3 del Anteproyecto.

Se propone que sea a través de una Disposición Adicional, ya que de acuerdo con las Directrices de técnica normativa (39) las disposiciones adicionales deberán regular:

a) Los regímenes jurídicos especiales que no puedan situarse en el articulado.

El régimen jurídico especial implica la creación de normas reguladoras de situaciones jurídicas diferentes de las previstas en la parte dispositiva de la norma. Estos regímenes deben determinar de forma clara y precisa el ámbito de aplicación, y su regulación debe ser suficientemente completa para que puedan ser aplicados inmediatamente.

b) Las excepciones, dispensas y reservas a la aplicación de la norma o de alguno de sus preceptos, cuando no sea posible o adecuado regular estos aspectos en el articulado.

Se propone la inclusión en el Anteproyecto de Ley, de una Disposición Adicional con el siguiente texto:

"Las funciones relacionadas en el artículo 3.2 no se extenderán a las competencias específicas de la Consejería de Sanidad de la Comunidad de Madrid en cuanto a los sistemas de información que puedan tener efectos en la salud de los pacientes y en la actuación de los profesionales sanitarios"."

Madrid a fecha de firma
EL SECRETARIO GENERAL TÉCNICO

SECRETARÍA GENERAL TÉCNICA
CONSEJERÍA DE ADMINISTRACIÓN LOCAL Y DIGITALIZACIÓN