SESIÓN PLENARIA ORDINARIA

11.- Pregunta N.º 409, relativa a número de ciberincidentes producidos durante 2020 en los sistemas informáticos de la Consejería de Sanidad y del Servicio Cántabro de Salud, presentada por D. César Pascual Fernández, del Grupo Parlamentario Popular. [10L/5100-0409]

12.- Pregunta N.º 410, relativa a número de ciberincidentes producidos durante 2020 en los sistemas informáticos de la Consejería de Sanidad y del Servicio Cántabro de Salud debidos a agentes externos y número de los debidos a agentes internos, presentada por D. César Pascual Fernández, del Grupo Parlamentario Popular. [10L/5100-0410]

13.- Pregunta N.º 411, relativa a ciberincidentes producidos durante 2020 en los sistemas informáticos de la Consejería de Sanidad y del Servicio Cántabro de Salud según el nivel porcentual de peligrosidad, presentada por D. César Pascual Fernández, del Grupo Parlamentario Popular. [10L/5100-0411]

14.- Pregunta N.º 412, relativa a tipología de los ciberincidentes producidos durante 2020 en los sistemas informáticos de la Consejería de Sanidad y del Servicio Cántabro de Salud, presentada por D. César Pascual Fernández, del Grupo Parlamentario Popular. [10L/5100-0412]

15.- Pregunta N.º 413, relativa a valoración ante el despliegue de entornos tecnológicos de teletrabajo para salvaguardar la continuidad de actividades sanitarias, presentada por D. César Pascual Fernández, del Grupo Parlamentario Popular. [10L/5100-0413]

EL SR. PRESIDENTE (Gómez Gómez J.): Y como ya está entre nosotros, el consejero de Sanidad, recuperamos los puntos 11 a 15.

Secretaria primera.

LA SRA. OBREGÓN ABASCAL: ¿Las vuelvo a leer?

EL SR. PRESIDENTE (Gómez Gómez J.): Sí, vuélvalas a leer.

LA SRA. OBREGÓN ABASCAL: Pregunta número 409 relativa al número de ciberincidentes producidos durante 2020, en los sistemas informáticos de la Consejería de Sanidad y del Servicio Cántabro de Salud.

Pregunta número 410, relativa al número de ciberincidentes producidos durante 2020, debidos a agentes externos y número de los debidos a agentes internos.

Pregunta número 411, relativa a ciberincidentes producidos durante 2020, en los sistemas informáticos, según el nivel porcentual de peligrosidad.

Pregunta número 412, relativo a tipología de los ciberincidentes.

Y pregunta número 413, relativa a valoración ante el despliegue de entornos tecnológicos de teletrabajo, para salvaguardar la continuidad de actividades sanitarias, presentadas por D. César Pascual Fernández, del Grupo Parlamentario Popular.

EL SR. PRESIDENTE (Gómez Gómez J.): Formula las preguntas, el Sr. Pascual, del Grupo Popular.

EL SR. PASCUAL FERNÁNDEZ: Gracias, señor presidente, señorías. Señor consejero, buenas tardes.

Vamos a ver si conseguimos tener un debate sereno, sin gritos y entendiéndonos. Llevamos un día un poco complicado en el pleno.

España sufre diariamente ciberataques de peligrosidad crítica muy alta contra el sector público y contra las empresas estratégicas. Lo hemos estado viendo cómo en los últimos meses ha habido ataques masivos a ministerios y la situación que ha tenido el Servicio de Empleo Público Estatal que estaba bloqueado durante largo tiempo, por virus ransomware.

También es verdad que ha habido muchos ataques dañinos a organizaciones sanitarias, que son ejemplos claros de ciberespionaje. Por no decir algún dato, en el año pasado Francia tuvo un ataque cibernético a la semana; más de 20 hospitales sufrieron ciberataques severos y se vieron absolutamente bloqueados; Reino Unido, en Bélgica se ha, en un

hospital desgraciadamente, se ha contabilizado una muerte directamente involucrada por un ataque cibernético. Y en nuestro país los datos de, ha habido hasta 50.000 ataques, de los cuales 375 tuvieron éxito. Bien.

El caso más importante conocidos el hospital de Torrejón, el año pasado, que afectó a la disponibilidad de todos sus sistemas informáticos, un ataque que bloqueó todo el acceso a las historias clínicas y que un mes después todavía seguían padeciendo las consecuencias de aquello.

Otro tipo de empresas, como la propia EMA, Agencia Europea del Medicamento o Moderna, también tuvo un ataque brutal, Fresenius que es el dueño de Quirón Salud también se ha visto durante este año en mayo justamente bloqueado con un ataque.

Es cierto también que las medidas de confinamiento adoptadas por la COVID han propiciado el teletrabajo en todos, todos los sectores, también en sanidad, para salvaguardar la continuidad de los servicios sanitarios, pero esto lleva sus riesgos y situaciones de brechas de seguridad posibles que se hayan producido. Y este aumento de conexiones en la nube y tener las conexiones al alcance de cualquiera, pues propicia estas situaciones en que es previsible que los ataques y vulnerabilidades relacionados con redes domésticas puedan llegar a las redes sanitarias.

Y, por tanto, esta es la pregunta iba dirigida a las preguntas todas en este sentido, qué medidas se salvaguarda la ciberseguridad de los sistemas de nuestra Administración sanitaria y de los centros del Servicio Cántabro de Salud sin que por supuesto, esta pregunta suponga entrar en detalles que requieran la necesaria confidencialidad, por supuesto, pero sí nos gustaría tener información al respecto.

Muchas gracias.

EL SR. PRESIDENTE (Gómez Gómez J.): Gracias, Sr. Pascual.

Responde por parte del Gobierno el consejero de Sanidad, Sr. Rodríguez.

EL SR. CONSEJERO (Rodríguez Gómez): Gracias presidente, buenas tardes señorías.

En primer lugar, quiero pedir disculpas por el retraso, que ha sido totalmente ajeno a mi voluntad y que agradecer que se haya alterado el orden de las preguntas.

En respuesta a las preguntas concretas que nos plantea el Grupo Popular, decirle que los ciberincidentes recibidos por la consejería, por el Servicio Cántabro de Salud durante el año 2020 han sido 7, todos ellos detectados por el servicio de informática del Hospital Universitario Marqués de Valdecilla, todos ellos de baja intensidad y de origen variado, habiendo tanto agentes internos en algún caso había implicado algún equipo nuestro como agentes externos, porque evidentemente los agentes externos que se conectan a la wifi pues también pueden ser objeto de ciberincidentes como son visitantes o con proveedores; pero todos ellos, de estos 7 ninguno, tenía una clara intención dañina sino que han saltado como ciberincidentes pero, como le digo, sigue intención dañina.

La tipología de las amenazas también ha sido variada, pero su impacto, como le digo, leve, y básicamente se han tratado de vulnerabilidades y algún equipo nuestro o la detección de un código de un código malicioso, es decir, la presencia de algún virus.

Sobre la pregunta 413, sobre el despliego de entornos informáticos para poder desplegar el teletrabajo, informarle de que ya existía un procedimiento de conexión con VPN, con cifrado de la conexión para teletrabajo siguiendo las medidas de seguridad y las recomendaciones habituales. Y lo que hemos hecho es extender el servicio a más profesionales de la habitual entregándoles por lo general un equipo portátil corporativo del propio Servicio Cántabro de Salud, como, por ejemplo, han estado los radiólogos del Hospital Marqués de Valdecilla, que incluso han tenido una estación completa de trabajo en su domicilio. Una estación de radiología implica dos monitores de un tamaño especial, etcétera, etcétera.

Siempre hemos tenido presente que la ciberseguridad es un elemento muy a tener en cuenta nuestros planes de transformación digital del sistema sanitario público de Cantabria, y, por ello, hemos tomado medidas adicionales que sirvan para garantizarla y proteger nuestro trabajo. Por una parte, estamos en permanente contacto permanente, contacto con el Centro Criptológico Nacional, dependiente del CNI, hemos estado y estamos trabajando en la concienciación del personal al Servicio Cántabro de Salud, que es un elemento fundamental porque muchos de los ciberincidentes tienen relación con pinchar, con clicar en enlaces de correo externos.

Además, hemos estado, hemos establecido formación básica en ciberseguridad para los profesionales mediante cursos realizados a través de la plataforma SOFOS. También hemos procedido a reforzar el cortafuegos, el Firewall de los hospitales de Sierrallana y de Laredo y actualmente nos encontramos trabajando en dos cuestiones: por una parte, en los pliegos de un nuevo contrato de comunicaciones, reforzando el apartado de la seguridad, y también en los pliegos de la

nueva Oficina de Seguridad del Servicio Cántabro de Salud para disponer de personal específicamente dedicado a estas funciones.

EL SR. PRESIDENTE (Gómez Gómez J.): Gracias señor consejero.

Sr. Pascual.

EL SR. PASCUAL FERNÁNDEZ: Muchas gracias, señor consejero, por la información.

Lo cierto es que efectivamente, independientemente de las medidas de precaución que se hayan podido poner en marcha por parte de los sistemas de informática y los encargados de seguridad informática del Gobierno, tanto el Centro Criptográfico Nacional, que usted ha mencionado dependiente del CNI y la propia Interpol, han emitido comunicados alertando del riesgo grave que nos situamos en este final de pandemia, y de ahí también el origen de las preguntas.

Pero también quería hilarlo porque el Gobierno de Cantabria tiene una iniciativa para avanzar a nivel nacional en ciberseguridad, aunque directamente implicada no es una iniciativa sanitaria, pero supongo yo que participar en la red de excelencia Nacional de Investigación en Ciberseguridad por el Gobierno de Cantabria, pues también pueda tener alguna aportación de valor, que era también una de las respuestas que esperaba que usted me informara acerca de si la Consejería de Sanidad también va a poder intervenir o va a participar de alguna manera en este, en este proyecto tan interesante, pero sí que poder dar.

Lo cierto es que a raíz de lo que publican las distintas comunidades autónomas una cuestión que usted ha mencionado que espero que se solucione, siga siendo segura, como es la aportación de equipos a los profesionales que hacen teletrabajo, porque es la causa que más comunidades autónomas o sistemas de salud notifican como causa de los ciberataques, la brecha de seguridad que se hace con VPN y con los profesionales. Por tanto, si van a seguir por esta línea, a seguir entregando teletrabajo, equipos y desarrollando mecanismos de ciberseguridad.

El último incidente conocido, por lo menos en hospitales españoles, que ha sido el Hospital Quirón Salud, ha provocado una, fue muy corto afortunadamente solo duró 6 horas, pero hubo una crisis gravísima porque bloqueó todos los sistemas, incluso los de UCI y ese quería también preguntarle acerca de los posibles planes de contingencia que al respecto podía tener la Consejería de Sanidad.

Nada más, muchas gracias.

EL SR. PRESIDENTE (Gómez Gómez J.): Muchas gracias Sr. Pascual.

Señor consejero.

EL SR. CONSEJERO (Rodríguez Gómez): Bueno, pues lógicamente la Consejería de Sanidad es un departamento del Gobierno de Cantabria y por lo tanto participará en todos los proyectos que desde el Gobierno de Cantabria se hagan en materia de ciberseguridad.

En el caso concreto del Servicio Cántabro de Salud, como ya he comentado, que es un organismo autónomo estamos trabajando en el nuevo contrato de comunicaciones, reforzando, como le decía, el apartado de la seguridad, y estamos creando, estamos con la redacción de los pliegos para una nueva oficina de ciberseguridad específica de todo lo que es el Servicio Cántabro de Salud, que es el mayor poseedor de datos sanitarios. La Consejería de Sanidad tiene muy poca concentración de datos de las personas, el que los tiene es el Servicio Cántabro de Salud, y, evidentemente, tendremos una oficina de ciberseguridad en el ámbito del Servicio Cántabro de Salud específica, con personal específico dedicado a esas funciones.

Y no sé qué otra pregunta, me han hecho, ¿UCI? Ah, no, los planes de contingencia. Yo creo que si quieren en concreto ya la información de los planes de contingencia lo tendríamos que hacer explícitamente en otra pregunta yo no tengo ningún inconveniente en explicarle tanto aquí como en Comisión los planes de contingencia tienen el ámbito de la seguridad.

EL SR. PRESIDENTE (Gómez Gómez J.): Gracias, señor consejero.