DIARIO DE SESIONES

DEL

PARLAMENTO DE NAVARRA

IX Legislatura | Pamplona, 30 de mayo de 2018 | NÚM. 40

TRANSCRIPCIÓN LITERAL

COMISIÓN DE PRESIDENCIA, FUNCIÓN PÚBLICA, INTERIOR Y JUSTICIA

PRESIDENCIA DE LA ILMA. SRA. D.ª ISABEL ARANBURU BERGUA

SESIÓN CELEBRADA EL DÍA 30 DE MAYO DE 2018

ORDEN DEL DÍA

— Comparecencia, a instancia de la Junta de Portavoces, del Consejero de Hacienda y Política Financiera y de la Consejera de Presidencia, Función Pública, Interior y Justicia para informar sobre las causas, consecuencias y responsabilidades de la brecha de seguridad denunciada por un ciudadano según la cual, el Gobierno ha tenido al descubierto los datos fiscales de los contribuyentes navarros.

(Comienza la sesión a las 15 horas y 21 minutos).

Comparecencia, a instancia de la Junta de Portavoces, del Consejero de Hacienda y Política Financiera y de la Consejera de Presidencia, Función Pública, Interior y Justicia para informar sobre las causas, consecuencias y responsabilidades de la brecha de seguridad denunciada por un ciudadano según la cual, el Gobierno ha tenido al descubierto los datos fiscales de los contribuyentes navarros.

SRA. PRESIDENTA (Sra. Aranburu Bergua): Arratsalde on guztioi. Damos comienzo a una nueva sesión de la Comisión de Hacienda y Política Financiera, aunque en este caso es una Comisión Especial porque va a ir ligada a la Comisión también de Presidencia, Función Pública, Interior y Justicia. Tenemos un único punto en el orden del día que viene enunciado como la comparecencia del Consejero de Hacienda y Política Financiera y de la Consejera de Presidencia, Función Pública, Interior y Justicia para informar sobre las causas, consecuencias y responsabilidades de la brecha de seguridad denunciada por un ciudadano según la cual el Gobierno ha tenido al descubierto los datos fiscales de los contribuyentes navarros. Damos, para esta comparecencia, la bienvenida a la señora Consejera de Presidencia, Función Pública, Interior y Justicia, al señor Consejero de Hacienda y Política Financiera y puesto que las dos comparecencias han sido pedidas por tres grupos, tienen primero la palabra para hacer su presentación. Corresponde el primer turno de palabra al señor Sánchez de Muniáin.

SR. SÁNCHEZ DE MUNIÁIN LACASIA: Buenas tardes, muchas gracias y bienvenidos a los Consejeros, responsables y a todos los que estamos aquí. Esto fue como consecuencia de que, por medio de los medios de comunicación, en concreto por el *Diario de Navarra*, tuvimos conocimiento de que se había producido lo que, a nuestro juicio, es la brecha de seguridad más grave e importante que conocemos. Yo he repasado y no he conocido otra, porque en plena campaña de la Renta, afectaba a los datos fiscales de todos los contribuyentes navarros. Posteriormente, conocimos que además afectaba también a otros datos confidenciales de ciudadanos navarros que los prestaban a la Administración para diversos trámites y, obviamente, no para que fueran accesibles por toda la ciudadanía. Ante la gravedad de estos hechos y con el fin de desentrañar qué es lo que había ocurrido, solicitamos, entre otras, las comparecencias del Consejero de Hacienda y Política Financiera como máximo responsable de la custodia de los datos fiscales, y también de la Consejera de Presidencia, Función Pública, Interior y Justicia como responsable de la seguridad informática.

Posteriormente, como ya se ha sabido, se nos solicitó la posibilidad de celebrar una comparecencia conjunta, a lo cual no nos opusimos, y, por lo tanto, en la manera en que ustedes tengan previsto escucharemos las explicaciones sobre este grave fallo de seguridad y cómo se ha abordado desde el Gobierno de Navarra.

SRA. PRESIDENTA (Sra. Aranburu Bergua): Gracias, señor Sánchez de Muniáin. Tiene, a continuación, la palabra el señor García del Partido Popular.

SR. GARCÍA JIMÉNEZ: Muchísimas gracias, Presidenta. Cómo no, agradezco la presencia tanto de la Consejera de Presidencia, Función Pública, Interior y Justicia como del Consejero de Hacienda y Política Financiera, que es a quien nosotros solicitamos en su día la comparecencia, para que explique, efectivamente, de lo que nos enteramos todos el pasado 21 de abril, en el cual se da a conocer que los datos fiscales de los contribuyentes navarros habían estado

expuestos a la luz pública, durante aproximadamente cinco horas, debido a un fallo informático de Hacienda. Lo cierto es que todos son errores y son fallos en este Gobierno. Poco asumir responsabilidades o ninguna, quizás, y todo son errores de terceros. Nunca son errores, en este caso, del propio Gobierno.

Según el Gobierno, como digo, fue un error informático y fue un informático quien, a título personal, denunció los hechos ante la policía y también ante la propia Hacienda. Por lo tanto, queremos saber, independientemente de las explicaciones que se han dado en la respuesta a algunas de las preguntas, qué es lo que realmente sucedió y tenemos una serie de preguntas que queremos conocer, si hay algún dato que se ha podido filtrar de alguno de los contribuyentes de nuestra Comunidad y, en concreto, qué medidas se van a tomar de cara a evitar cualquier tipo de problema similar a este. Muchas gracias.

SRA. PRESIDENTA (Sra. Aranburu Bergua): Gracias, señor García. A continuación, el Partido Socialista entiendo que no quiere hacer presentación. En ese caso, tiene la palabra cualquiera de los dos, Consejero o Consejera, como estimen más conveniente, por un tiempo máximo de 30 minutos cada uno, aunque espero, realmente, que no lo agoten.

SRA. CONSEJERA DE PRESIDENCIA, FUNCIÓN PÚBLICA, INTERIOR Y JUSTICIA (Sra. Beaumont Aristu): Arratsalde on denori. Yo me voy a limitar a presentar al equipo que nos acompaña. Él es ya conocido, supongo que, para todos ustedes, don Mikel Sagüés García, Director General de Informática, Telecomunicaciones e Innovación Pública. Y también están presentes don Roumen Boyanov, que es Jefe de la Sección de Seguridad y Gestión del Rendimiento de la propia Dirección General, así como don Luis Arlegui, que es Jefe de la Sección de Proyectos de Sistemas de Información en las áreas de Hacienda y Política Financiera, adscrito también a la propia Dirección General de Informática, Telecomunicaciones e Innovación Pública. Y va a ser el Consejero de Hacienda, don Mikel Aranburu, el que hará el planteamiento de la comparecencia y, a continuación, las explicaciones más completas y técnicas con la base de la documentación que se les ha entregado y que la tienen delante, las dará don Mikel Sagüés, Director General de Informática. Eskerrik asko.

SR. CONSEJERO DE HACIENDA Y POLÍTICA FINANCIERA (Sr. Aranburu Urtasun): Eskerrik asko. Arratsalde on guztioi. Dado que se trata de la Comisión de Hacienda, me corresponde hacer esta presentación, pero, realmente, va a ser el Director General de Informática quien va a dar las explicaciones oportunas. Nosotros comparecemos hoy, tanto la Consejera Beaumont como yo, para informar sobre las acciones que se tomaron por el Gobierno de Navarra en relación con este caso de vulnerabilidad informática en la credencial DNI+PIN detectada por un ciudadano el pasado 19 de abril.

Con independencia de que a lo largo de esta comparecencia se entre en el detalle de cada uno de los aspectos –que luego resumiré a continuación–, considero importante describir, aunque sea someramente, lo que consideramos que han sido las claves en relación con la actuación del Gobierno de Navarra en este tema. En primer lugar, es importante, porque no se están manejando los conceptos correctamente, entender de qué estamos hablando cuando nos referimos a una vulnerabilidad informática y más en concreto a las características que tiene la vulnerabilidad de la credencial DNI+PIN, detectada por el ciudadano, una credencial operativa en Hacienda desde 2005.

A continuación, nos gustaría resaltar la celeridad con que se actuó una vez conocida dicha vulnerabilidad, corrigiéndola en un tiempo récord, únicamente en seis horas desde que se tuvo conocimiento de la misma.

Una vez corregida la vulnerabilidad, se procedió, lógicamente, a realizar un análisis, una auditoría, un análisis forense diríamos, que permitiera cuantificar el alcance de la misma, es decir, saber qué efectos había podido tener, haciendo especial hincapié en la posible exposición de datos personales a que esta dio lugar, no solo en este momento, sino también en el pasado. Eso es un trabajo de auditoría complejo, que llevó un tiempo.

La conclusión de dicho análisis forense, y que algunos de ustedes ya conocen tras las peticiones de información parlamentaria a las que se ha dado respuesta en semanas anteriores, es que la vulnerabilidad no había sido explotada con anterioridad, por lo que la exposición de datos se circunscribe únicamente a la actividad del ciudadano que la encontró y comunicó su existencia al Gobierno de Navarra.

Una vez constatada dicha exposición de datos, se notificó a los afectados por vía telefónica y por correo postal, procediendo también a renovar sus credenciales, evitando de este modo una posible exposición de datos.

Además, tal y como dicta el Esquema Nacional de Seguridad, se notificó el incidente al Centro Criptológico Nacional, cumpliendo de este modo con las obligaciones marcadas por la ley en materia de seguridad de la información.

Por otro lado, aprovechando la comparecencia, nos gustaría aprovechar para comentar algunas de las acciones más relevantes que se han llevado a cabo a lo largo de la presente legislatura en materia de protección de datos y de seguridad de la información con el objetivo de hacer patente la clarísima implicación de este Gobierno en relación con esta materia. Besterik gabe, Mikel Sagüés jaunari emango diot hitza.

SR. DIRECTOR GENERAL DE INFORMÁTICA, TELECOMUNICACIONES E INNOVACIÓN PÚBLICA (Sr. Sagüés García): Mila Esker, Aranburu jauna. Arratsalde on. Buenas tardes a todos. Plazer bat da, beti bezala, hemen egotea azalpenak emateko. Un placer, digo, estar aquí para dar todas las explicaciones que consideren necesarias. El Consejero Aranburu ha hecho una descripción de cuáles son las claves. Yo voy a entrar en lo mismo, entrando un poquito más en detalle para intentar explicarlas mejor. Voy a intentar ser relativamente breve y luego en las preguntas y respuestas entramos en todo el detalle que necesiten.

Probablemente, lo primero que tengamos que aclarar es qué es una vulnerabilidad informática, a qué nos estamos refiriendo cuando hablamos de vulnerabilidad informática. Una vulnerabilidad es un error, un fallo, una debilidad que tiene un programa informático, un sistema de información, una aplicación informática. Esa debilidad permite que un atacante, explotando dicha vulnerabilidad, sea capaz de comprometer el servicio. Ese servicio se puede comprometer porque hace que los datos que eran accesibles para los usuarios no sean accesibles, digamos que los bloquea. Este es el caso más famoso, el famoso WannaCry del año pasado que atacó a muchísimas administraciones y empresas. Es un ataque que bloquea los datos. No permite que accedas y después te pide una contraprestación económica para desbloquear ese bloqueo. Pero también tenemos un posible ataque que vulnere la confidencialidad de los datos, es decir, que permite que alguien que no debería tener permiso

para acceder a unos datos, acceda a ellos, o podemos tener una vulnerabilidad que ataque la integridad de los datos, es decir, que modifique algún dato, que haga que un dato desaparezca, que un dato cambie su valor. Esto son tipos de actuaciones, todas, motivadas por una vulnerabilidad que no es otra cosa más que un error en un programa informático.

Aquí es importante destacar y, sinceramente, no lo hacemos con idea de descargarnos de culpa. Evidentemente, si hay una vulnerabilidad en un sistema de información de Gobierno de Navarra, la responsabilidad es, en concreto, de la Dirección General de Informática y Telecomunicaciones y eso es impepinable. Esto es así. Pero es cierto también que vulnerabilidades informáticas existen en todos los sistemas de información, en todas las empresas y en todas las Administraciones Públicas.

Sin ir más lejos, y por poner un ejemplo conocido, Microsoft cada dos meses, creo que es el primer martes cada dos meses, publica decenas o cientos de vulnerabilidades de sus sistemas de información: en su paquete de Office, en su sistema operativo, en sus bases de datos. Cada dos meses, centenares o decenas. Y lo mismo pasa para IBM, Intel o cualquiera de las grandes corporaciones informáticas que podamos conocer. Entonces, es importante asumir que las vulnerabilidades existen y que las tenemos todos.

Cuando Microsoft, por seguir con ese ejemplo, publica una vulnerabilidad, lo que hace es darla a conocer para que cualquiera sea consciente de que esa vulnerabilidad existe, de tal forma que los usuarios corrijan esa vulnerabilidad en su casa. Pero, al hacerla pública, también lo que hace es que los atacantes sean conscientes de que hay una posibilidad de atacar esa vulnerabilidad en el modo que he descrito anteriormente. Entonces, en ese punto, estamos hablando de una vulnerabilidad conocida, es una vulnerabilidad pública, y, por lo tanto, atacable.

La inmensa mayoría de los ataques que sufrimos –y en Gobierno de Navarra son cientos de miles al año– son ataques contra vulnerabilidades conocidas. Y ahí sí que es responsabilidad de los gestores de la infraestructura, es decir, de la Dirección General de Informática y Telecomunicaciones en este caso, estar protegidos frente a esos ataques. Son conocidos y, por lo tanto, es nuestra responsabilidad haber corregido lo que es público. Cuando digo que es nuestra responsabilidad, ahí también tengo que insistir en que no es fácil estar al día. El esfuerzo que implica estar al día en este tema es muy grande y, de hecho, tampoco hay nadie que esté absolutamente libre. En el minuto uno se publican, en el minuto dos es imposible que lo tengas corregido. Pero es algo público y, por lo tanto, si existe un problema de este tipo, la responsabilidad sí que es muy clara en decir que no se estaban gestionando bien esas infraestructuras.

Ese es el caso, por ejemplo, del WannaCry que he mencionado antes. Explotaba una vulnerabilidad conocida y muchísimas administraciones no tenían esa vulnerabilidad corregida y, por lo tanto, fueron atacadas con este virus. Pero hay muchísimos más, insisto, cientos de miles de ataques al año.

Y luego, hay otro tipo de vulnerabilidades que son las que no son conocidas. Aquí estamos hablando de que alguien, un experto informático o una empresa con malas intenciones, un gobierno que, no sé, está buscando vulnerabilidades específicamente en sistemas de información concretos de una administración o de una empresa, con idea de romper su seguridad. Y lo que ocurre es que es posible que las encuentre y que las explote. En ese caso,

la vulnerabilidad no era conocida para esa empresa o para esa administración. Es conocida, únicamente, para esa empresa o esa persona que la descubre y en ese momento puede explotarla. Es este segundo el caso del que estamos hablando en la credencial DNI+PIN. Es una vulnerabilidad no conocida que una persona, un experto informático, detecta en el sistema de información.

Una vez descrito qué es una vulnerabilidad y los tipos que hay, es importante hablar de las consecuencias a partir de una vulnerabilidad. Una vulnerabilidad se ha podido utilizar y, por lo tanto, ha podido ser explotada para obtener información, para bloquear información, etcétera, o ha podido ser simplemente detectada y comunicada. El caso de Microsoft que comentaba antes.

Nosotros estamos en el segundo caso. Estamos en el caso de que una persona detecta una vulnerabilidad y se pone en contacto con Gobierno de Navarra para decirnos: «Oye, fijaros que de esta forma se puede birlar la seguridad en Gobierno de Navarra y se podría acceder a datos de los contribuyentes de Hacienda». Nos avisa a Gobierno de Navarra.

No sé si con esto queda claro el concepto de vulnerabilidad, los tipos y, sobre todo, ante qué nos enfrentamos en relación con la exposición de datos.

Voy a intentar explicar muy brevemente en qué consistía en concreto la vulnerabilidad en la credencial DNI+PIN. Voy a intentar hacerlo sin emplear palabras muy técnicas, pero para que se comprenda someramente.

El camino habitual por el cual se accede, un usuario accede, un contribuyente accede a los sistemas de información de Gobierno de Navarra es el que está dibujado en la parte de arriba de la presentación. El usuario, a través de su navegador web –el Explorer, el Firefox, el Chrome, el que sea–, accede a una página web de Gobierno de Navarra, se identifica en esa página web de Gobierno de Navarra y esa página web de Gobierno de Navarra le da acceso a la infraestructura interna de Gobierno de Navarra, de tal forma que puede acceder a sus datos, modificarlos, hacer su declaración de la renta o lo que sea. En este caso, lo que hacía o lo que detectó este experto informático, es que, en lugar de utilizar un navegador web convencional, en lugar de utilizar el camino convencional para el cual está diseñada la aplicación, lo que hace es utilizar una herramienta de hacking, una herramienta informática de hackeo, y se salta ese navegador. Al saltarse el navegador, lo que consigue es saltarse una primera comprobación de seguridad que se hace –o que se hacía, porque la vulnerabilidad ya está corregida– en el navegador, que es la comprobación de que el número del DNI o del NIF se corresponde con la letra. Entonces, al saltar el navegador, es capaz de atacar a los servidores de Gobierno de Navarra o acceder a esos servidores con un número NIF correcto, pero una letra incorrecta. Cuando en esos servidores una persona introduce cinco veces de manera incorrecta el PIN, el servidor bloquea el acceso a ese NIF, de tal forma que evita que se sigan probando combinaciones hasta obtener el PIN de la persona a la que se quiere acceder. Sin embargo, si el usuario lo hace en la forma que he descrito anteriormente, como el NIF no existe, porque la letra no tiene una correspondencia con el número, como no existe, no hay nada que bloquear, el sistema no bloqueaba el acceso y, por lo tanto, permitía que el usuario hiciera tantos intentos como quisiera con tantas combinaciones del PIN como quisiera hasta encontrar una combinación correcta. Esa es la vulnerabilidad.

Una vez descubierta y una vez descrita es algo muy sencillo y efectivamente es «cómo es posible que esto estuviera así». Pero la realidad es que quince años lleva así y ninguno de los informáticos de la Dirección General ni externo se había dado cuenta de que esto podía hacerse. Es muy imaginativo y la realidad es que tenemos o teníamos un problema y la realidad es que es un problema que tengo que asumir como responsabilidad mía.

Una vez que el ciudadano detecta esta vulnerabilidad, lo que hace es comunicarla a Gobierno de Navarra. Llama al 112. El 112 transfiere a la Unidad de Delitos Informáticos de la Policía Foral. La Policía Foral pasa la llamada a la Dirección General de Informática que, a su vez, se pone en contacto con Hacienda Tributaria de Navarra y nos ponemos manos a la obra a corregir este problema. Seis horas después de la llamada del contribuyente, el problema estaba corregido. Seis horas después. Con esto quiero decir que la actuación reactiva de Gobierno de Navarra a la hora de corregir esta vulnerabilidad solo puede clasificarse como de muy buena. Es un tiempo muy rápido para corregir esa vulnerabilidad. En este punto, un poco... Bueno, no sigo, porque no me escucha.

Una vez que se corrige la vulnerabilidad, el siguiente paso es analizar si, efectivamente, ha habido o no una exposición de datos explotando esa vulnerabilidad. Este es el análisis forense que comentaba el Consejero Aranburu. Este análisis forense lleva varios días, de hecho, lleva varias semanas llevarlo a cabo y una vez concluido la conclusión es que, efectivamente, esta vulnerabilidad no había sido explotada antes. Nadie se había dado cuenta de esto o nadie se había dado cuenta y lo había explotado. Por lo tanto, antes de que el ciudadano que detecta esta vulnerabilidad nos lo comunique, nunca había habido una exposición de datos de contribuyentes de Hacienda. Y la exposición de datos que sí ha habido se circunscribe únicamente a la actividad del ciudadano. Esto es lógico porque alguien no puede detectar que algo falla si no prueba que efectivamente falla. Entonces esta persona probó, hizo varias pruebas de varias formas diferentes además y consiguió romper el sistema y, por lo tanto, consiguió romper varias credenciales de contribuyentes de Hacienda o de ciudadanos de Navarra, lo cual es grave, pero insisto, está circunscrito o está limitado a la actividad de esta persona que detecta esa vulnerabilidad.

A partir de conocer y corregir la vulnerabilidad y ver cuál ha sido su alcance, el siguiente paso es notificarlo. Hay que hacer una notificación a los ciudadanos afectados. Se les revocan las credenciales, se les da unas nuevas, se les informa de lo que ha pasado por teléfono y por escrito. Digamos que se informa a los afectados de que ha ocurrido esto en Gobierno de Navarra. Y, por otra parte, se notifica también este incidente de seguridad al Centro Criptológico Nacional. El Centro Criptológico Nacional es la autoridad a nivel estatal a la cual, por normativa, digamos, por ley, hay que comunicar los incidentes de seguridad. Entonces, en ese sentido, entendemos que Gobierno de Navarra también actuó de manera correcta comunicándolo inmediatamente al Centro Criptológico Nacional y comunicándolo inmediatamente a los afectados.

Y, por último, también en alguna noticia o en alguna intervención parlamentaria se ha comentado que habría que haberlo puesto en conocimiento de la ciudadanía. La realidad es que, en ningún caso, podemos poner en conocimiento de la ciudadanía algo sin primero corregirlo. No podemos decir «aquí hay un problema» y el que quiera que lo intente explotar. Lo primero era corregirlo en esas seis horas y lo segundo era detectar o determinar cuál había sido el acceso, si efectivamente había habido, o no, una explotación de esos datos.

Y es cierto que antes de que podamos casi comenzar, porque es al día siguiente, con este análisis forense, la noticia salta a prensa y, por lo tanto, es público, pero lo lógico es determinar su alcance y después comunicarlo a la población, en su caso.

Y creo que esto es básicamente lo que hay que explicar con relación a esta vulnerabilidad o a este fallo en el sistema de información de Gobierno de Navarra.

Aprovecho un minuto, tampoco quiero tomarme demasiado tiempo en eso, para decir que creo, sinceramente, que Gobierno de Navarra, históricamente, es una Administración que se ha preocupado mucho por la seguridad de la información. Creo que eso es justo reconocerlo. Y creo que es justo reconocer también que este Gobierno en particular hereda esa determinación y no solo la hereda, sino que la estamos potenciando muchísimo en esta legislatura.

Entonces, les voy a dar una serie de ejemplos de cosas que se han hecho en esta legislatura para que quede claro que esto no son palabras, sino que efectivamente hay una realidad detrás de lo que estoy diciendo.

En primer lugar, lo que es el presupuesto, el esfuerzo presupuestario que se está haciendo en la asistencia técnica de seguridad en Gobierno de Navarra se ha incrementado en un 60 por ciento desde 2015. Un esfuerzo presupuestario muy fuerte. Y, además, es todo el esfuerzo presupuestario que podemos hacer y controlar al mismo tiempo lo que estamos haciendo. No es sencillo incorporar recursos en este tipo de actuaciones y estamos haciendo todo lo que podemos, realmente, a nivel práctico y a nivel presupuestario.

Por otra parte, también se ha renovado el antivirus. Teníamos un antivirus muy bueno. Ahora tenemos un antivirus mucho mejor. Un antivirus de última generación sobre el cual, además, la propia Dirección General, en el Servicio de Infraestructuras, ha desarrollado una capa adicional que permite analizar los datos cruzándolos de varias bases de datos, sistemas de información en Gobierno de Navarra, de tal forma que desde que hemos hecho esta actuación, no tenemos ni una sola infección por virus informático en Gobierno de Navarra. Esto no lo quiero decir muy alto tampoco, aunque lo estoy diciendo en público, porque soy consciente de que algún día la tendremos, por lo que decía antes: nadie está seguro al cien por cien de problemas informáticos. Pero creo que el salto que se ha dado es muy significativo y, de hecho, esta actuación ha sido premiada con el premio ASLAN en las Administraciones Públicas en seguridad de la información este año, con lo cual, es un reconocimiento a nivel estatal del trabajo que se ha hecho.

También se ha renovado el cortafuegos –no me extiendo mucho en eso– y también se está actuando con más intensidad de la que se hacía antes en lo que son auditorías de las aplicaciones. Se están auditando de manera automática más aplicaciones y con una herramienta más avanzada de la que se tenía, y también se ha iniciado un nuevo camino, un camino que hasta ahora no existía en Gobierno de Navarra, de auditoría de código de las aplicaciones. Desde... no sé si fue finales de 2015 o primeros de 2016, iniciamos este proyecto. Es un proyecto muy complejo y que requiere de mucha comunicación dentro de la Dirección General pero que ya está en marcha, ya se han hecho los primeros pilotos, este año se va a auditar una aplicación para cada uno de los departamentos de Gobierno de Navarra. Un camino, digamos, en la mejora de la seguridad de las aplicaciones informáticas en Gobierno de Navarra.

Y, por último, en cumplimiento normativo, no solo en el cumplimento técnico, también hemos avanzado mucho. Hemos hecho auditorías en departamentos donde nunca se había hecho ninguna auditoría y, sobre todo, se ha hecho el esfuerzo de identificar y nombrar responsables de seguridad en cada una de las Direcciones Generales de Gobierno de Navarra. Este perfil es el interlocutor de la Dirección General de Informática con el resto de Direcciones Generales, es el responsable de que las aplicaciones de esas Direcciones Generales cumplan con los criterios de seguridad. Y no solamente se han identificado, sino que se está en un proceso de incluir, en el decreto de estructura, estas funciones para cada una de estas Direcciones Generales. Es un proceso que ya se ha completado en Presidencia, en Hacienda, en Desarrollo Rural y Medio Ambiente y ahora se está trabajando en ello en el resto de departamentos.

Con esto, lo que se consigue –estoy aprovechando un poco para contarles, pero bueno– es que la función no dependa de la persona. Cuando esa persona se jubila, se va, le nombran jefe en otro sitio, normalmente lo que ocurría es que desaparecía la función y otra vez a arrancar desde cero. Incluyéndolo en la estructura, lo que garantizamos es que quien venga a ocupar ese puesto asume, directamente, esas responsabilidades.

Se ha creado el Comité de Seguridad del Gobierno de Navarra. Esto era un déficit, digamos, o un debe desde 2010 porque está marcado en el Esquema Nacional de Seguridad y se ha creado en esta legislatura. Ese comité es donde se juntan todos estos responsables de seguridad, toman las decisiones pertinentes que les afectan a todos y, sobre todo, comparten información entre ellos y se apoyan entre ellos para mejorar en su trabajo.

Y, por último, ligado un poco al Reglamento General de Protección de Datos que entraba en vigor el viernes pasado, precisamente, se ha creado una estructura dependiente de la Dirección General de Presidencia en el Departamento de Presidencia para albergar la función del Delegado de Protección de Datos en Navarra.

Esto lo digo, un poco, sin ánimo ni de echar para atrás, ni de echar para adelante, insisto en que Gobierno de Navarra es un referente a nivel estatal, lo era y ahora sigue siéndolo, y el esfuerzo que se está haciendo por parte de la Dirección General –he intentado describirlo en estos cinco puntos– creo que queda patente.

Y vuelvo a insistir en que la responsabilidad de que exista la falla de seguridad que existía en el DNI+PIN es mía, es de la Dirección General de Informática, Telecomunicaciones e Innovación Pública, y no voy a mirar que lleva otros doce años en el mismo punto, es mía y tengo que asumirla en ese sentido.

Y esto es un poco lo que les quería contar en primera ronda. Mila esker.

SRA. PRESIDENTA (Sra. Aranburu Bergua): Gracias a usted, señor Sagüés. Gracias también al señor Consejero y a la señora Consejera por sus intervenciones. Ahora es el turno de los y las portavoces de los diferentes grupos. En principio tiene la palabra el señor Sánchez de Muniáin por un tiempo, diremos, también, de entre diez y veinte minutos, con la idea de que tampoco lo agoten, a ser posible.

SR. SÁNCHEZ DE MUNIÁIN LACASIA: Muchas gracias, Presidenta. Y muchas gracias por las explicaciones técnicas, sobre todo, porque además han sido unas explicaciones comprensibles, lo cual, ya de por sí, es un... Comprensibles en cuanto a su lenguaje, luego ya las dudas que

tengamos ya las vamos a manifestar, pero sí que es un acierto el que se haga comprensible algo tan árido como es la terminología informática.

El contexto de esta situación, como hemos comentado antes, tiene lugar el 21 de abril. El 21 de abril, repetimos, en plena campaña de declaración de IRPF, conocimos que se había producido un fallo de seguridad que yo creo que no tiene precedentes, por lo menos, hasta donde nosotros podemos averiguar. Y ese fallo de seguridad había provocado que, de alguna forma, todos los datos de los contribuyentes navarros estaban, cuando menos, accesibles para cualquier persona con ciertos conocimientos informáticos, lo cual es grave. Y conocimos que el Gobierno no comunicó este grave suceso a la ciudadanía ni en el momento en que se produjo, ni una vez solucionado tampoco lo comunicó, ni días después tampoco lo comunicó.

Sin embargo, por parte del Gobierno, y creo que fue por parte de responsables de Hacienda, sí se confirmó tal fallo y el consiguiente riesgo, pero eso sí, cuando un medio de comunicación, en concreto, el *Diario de Navarra*, destapó la información o se interesó por los hechos. No a iniciativa del Gobierno, sino a iniciativa, en este caso, del *Diario de Navarra*.

Además, conocimos que no solo habían quedado accesibles los datos de Hacienda, sino también datos confidenciales relativos, por ejemplo, a trámites de ciudadanos, tales como las cédulas de habitabilidad, las ayudas a las empresas a la internacionalización o la tramitación de subvenciones, que también se acceden mediante este sistema del DNI+PIN. Todos estos datos, además de los relativos a la fiscalidad de todos los ciudadanos, han estado expuestos entre el 11 de abril y el 19 de abril –según figura en el informe que se nos ha remitido– y han sido conocidos cuando este ciudadano los ha comunicado.

El 23 de abril, creo que fue el 23 de abril, este grupo solicitó la siguiente información: uno, copia de la denuncia registrada o tramitada ante Policía Foral. La respuesta es que tal información no se nos suministra, alegando, para ello, un escrito del Jefe de Policía Foral en el que se afirma sobre el respecto que no consta ninguna información en los ficheros –es este documento– y que no se tiene constancia de que se haya registrado denuncia formal por la cuestión planteada. Sin embargo, en la misma respuesta parlamentaria, en el informe remitido por el Director General de Informática y Telecomunicaciones, se desmiente a nuestro juicio y se contradice esta información, puesto que se afirma textualmente que «el hecho denunciado se comunicó a través de una llamada al 112 y se derivó a la Policia Foral», tal y como se explica en el informe adjunto.

Por lo tanto, las primeras preguntas van dirigidas a la Consejera responsable, la Consejera Beaumont, en este sentido. ¿Quién dice la verdad?, ¿se ha extraviado una denuncia correspondiente a ese hecho de una posible fuga de datos –un hecho grave, como se ha puesto de manifiesto aquí–?, ¿quién es el responsable de esta denuncia o comunicación extraviada o que no consta en los ficheros de Policía Foral?, o ¿cuál es la causa porque se incurra en esta aparente contradicción?

Después, pedimos copia de los informes o escritos relacionados con esta cuestión y, efectivamente, se nos remite adjunto un informe detallado del Director General de Informática que comentaremos a continuación y que coincide básicamente con las explicaciones alegadas aquí, en esta comparecencia.

Tercero, pedimos un registro de todas las modificaciones, reprogramaciones, actualizaciones... El término yo no sé si es exacto, pero me refiero a todos los cambios y modificaciones que se han debido hacer en este sistema DNI+PIN durante su periodo de vigencia, lo cual tampoco se nos adjunta porque se nos indica que en todos estos años no se ha practicado ni una sola reprogramación del sistema DNI+PIN, lo cual nos sorprende.

Cuarto, pedimos una acreditación para transmitir la debida tranquilidad a los ciudadanos, una acreditación escrita acerca de la imposibilidad de que ninguna persona haya aprovechado este fallo de seguridad para hacerse, por ejemplo, con datos fiscales o esa otra información confidencial de contribuyentes o ciudadanos. Tampoco se nos adjunta esta acreditación y esto no cabe más que una explicación, en principio, que es porque es imposible acreditar negativamente que se haya podido producir ese robo de datos o usurpación de datos. Si es así, también se contradice con lo afirmado por el Consejero de Hacienda, cuando él mismo expresó que era imposible que se hubiese producido ese robo de datos y lo dijo, por lo que se ve, sin que ningún informe técnico acreditase tal afirmación de forma escrita, y creemos que no se lo acreditó, sencillamente, porque esa afirmación esgrimida por el Consejero es imposible, porque una vez detectado un fallo de seguridad de esta envergadura, creemos, salvo que se nos argumente otra cosa, que nadie con solvencia técnica puede acreditar que es imposible que se hayan sustraído datos de los contribuyentes. Por lo tanto, también le preguntamos al Consejero de Hacienda en qué se basó o por qué afirmó que nadie había retenido o robado información, sin disponer de la acreditación técnica que avalase tal afirmación tan rotunda. O a lo mejor se dispone de cualquier otra acreditación que no conocemos en este momento.

Y ya, con relación al informe que se nos remitió, se señala que, efectivamente, el fallo de seguridad es conocido por la denuncia de un ciudadano realizada el 19 de abril, comunicada ante Policía Foral, aunque, insisto, el jefe de este cuerpo policial afirma que no hay constancia. Es decir, que se produce, a nuestro juicio, el más grave fallo de seguridad conocido, que ha podido poner al descubierto los datos fiscales de todos los navarros, y el Gobierno, en principio, ha sido incapaz de detectarlo por sí mismo. El fallo y el ataque de fuerza bruta –en los términos que denomina en el informe y que son términos técnicos, no creo que sean como lo entendemos coloquialmente– se produce días atrás, se produce entre el 11 y el 19 de abril. Ocho días durante los cuales alguien está entrando continuamente y accediendo a los datos informáticos. Y el Gobierno no lo detecta. Es este ciudadano el que lo comunica.

Por cierto, entiendo que cuando se dice que son con herramientas hacker, porque lo he visto en algún sitio, herramientas de hackeo, no es este ciudadano, desde luego, ningún hacker. Al contrario, este ciudadano es un héroe al que ya le tendría que estar el Gobierno otorgándole algún reconocimiento. Los hackers entran, roban datos e incluso los venden, los comercializan o chantajean con los mismos. Con lo cual, si es así, no creo que este ciudadano sea tildado de hacker. Pero bueno, en cualquier caso, si hay otra explicación u otra información que no conocemos, estamos dispuestos a considerarlo.

Con lo cual, al fallo de seguridad en los datos de Hacienda, posible, y ahí sí que compartimos parte de las explicaciones expresadas, hay que añadir un fallo importante en la vigilancia y la detección de ese fallo. No lo descubre el Gobierno; lo descubre un ciudadano.

¿Qué preguntas se nos abren aquí? ¿Qué hubiera pasado si el ciudadano fuera realmente un hacker en toda la extensión del término y en lugar de poner en conocimiento esa

vulnerabilidad, se dedica a acceder continuamente al sistema? ¿Hasta cuándo y con qué consecuencias podrían seguir expuestos y accesibles los datos confidenciales de los ciudadanos sin que los máximos responsables de Hacienda o de Presidencia se enterasen?

En el informe, se nos aporta –claro, esto no se va a ver– una gráfica correspondiente a esos días donde se detalla el ataque o la incursión en los ficheros. Es una gráfica muy parecida a las escalas –desde un punto de vista profano– de la medición de los sismógrafos, de los terremotos, o de los electrocardiogramas, si se quiere personalizar. ¿Y qué vemos en esta gráfica? En esta gráfica vemos que, efectivamente, la escala es muy intensa, muy concentrada y muy llamativa, según se muestra. Y, sin embargo, a pesar de esa intensidad y de lo llamativa que es esa escala, no han saltado las alarmas, no se ha podido detectar.

Otro aspecto que nos ha llamado la atención es la ausencia de reprogramaciones, actualizaciones, reseteo, como se quiera entender. Esto nos sorprende, puesto que se nos comunica, como hemos comentado, que no se ha producido ninguna actualización, ninguna modificación, algo que parece que todos los sistemas lo hacen constantemente y, además, se ha comentado aquí referido a alguna compañía que lo hace de manera constante. Se nos hacía algo difícil de creer, efectivamente, a la vista de todos esos cambios que se abordan en cualquier sistema informático de datos. Y más con las constantes modificaciones normativas que, entre la que destaca es el conocidísimo ya por todos, ese reglamento que entró en vigor hace unos días, el 25 de mayo, pero que ya se conocía desde hace casi dos años, desde abril del 2016. Entonces, claro, sin embargo, pese a que no se producen reprogramaciones y que se ve cómo el sistema, entiendo yo, se va quedando algo obsoleto y, lo que es más grave, cuantos menos cambios se introducen, cuantas menos mejoras, más vulnerable, en el año 2017, ese sistema que no se había actualizado, que no se había reprogramado, la Consejera de Presidencia dicta una orden foral en la que extiende el sistema DNI+PIN. Ese sistema que no se había reprogramado, se extiende a más trámites y cada vez acoge más datos de los ciudadanos, que es cuando se extiende a los datos de las cédulas de habitabilidad, a los datos de las empresas que piden ayudas para la internacionalización... Es decir, un sistema que no se reprograma se extiende a permitir gestionar accesos a datos sobre más solicitudes ciudadanas.

Otro aspecto que también queremos poner de manifiesto es el que tiene que ver con la aprobación y entrada en vigor del nuevo reglamento europeo. Decía que entró en vigor hace unos días, el 25 de mayo, pero se conoce y, de hecho, se aplica y se adapta a todo el mundo a partir de abril del 2016. Por lo que, por nuestras informaciones, sabemos, y si no también se nos puede matizar, que ese sistema, el del DNI+PIN, no cumple íntegramente todos los requisitos de este reglamento y que, a pesar de que no lo cumple, a día de hoy, que nosotros sepamos, no está actualizado ni reprogramado. Por eso pregunto a la Consejera Beaumont: ¿cómo es posible que en 2017 se dicte esa orden foral permitiendo el acceso a más datos ciudadanos sin antes observar todas esas, aparentemente, prudentes medidas de seguridad? Un sistema que ya parece vulnerable y que no cumple la normativa, ¿se expone a más datos, sin antes reprogramarlo, sin antes adaptarlo a la nueva legislación, a la nueva normativa?

Y ya, entramos en las medidas adoptadas. Relata el informe una serie de medidas y protocolos realizados tras la comunicación y reparación del fallo, que entiendo yo que son los protocolos previstos y que se van verificando, como se ha comentado aquí, en el informe. Sin embargo, aunque no esté previsto en esos protocolos, no vemos que siquiera por elemental razón de prudencia, dado que el error afectó a datos fiscales de la totalidad de los contribuyentes, no se

hace lo que, a nuestro juicio, parece que es lo principal, que es lo primero que hacen todas las empresas para blindar y transmitir seguridad. Blindar, primero, asegurar, pero luego también transmitir seguridad a la población. La forma habitual de proceder, entendemos es, si el Gobierno quiere transmitir seguridad, lo que hacen todas estas empresas, que es, primero, por el tiempo necesario, bloquea el acceso al sistema. Segundo, notifica a todos los usuarios una vez solucionado el problema, a todos los usuarios. Tercero, se pide a los ciudadanos que cambien la contraseña o se les renueva la contraseña, si no pueden hacerlo por sus propios medios. Y, en cuarto lugar, se restablece el servicio.

Esto vemos, simplemente, con entrar en internet, «Twitter pide a usuarios cambiar de contraseña por fallo de seguridad» –hemos visto otros ejemplos–, «Yahoo pide a los usuarios que cambien sus contraseñas». La tecnología asegura que no se han comprometido datos bancarios, ni tarjetas de crédito, pero había habido un fallo de seguridad. Sin embargo, aquí, no se hace nada de eso.

Y lo último y más grave, creemos –y esto no es cuestión del Director de Telecomunicaciones– que se hace lo peor que se puede hacer, que es intentar ocultar el problema, porque ni Hacienda ni el propio Gobierno, a través de la Dirección de Comunicación, informan de este grave problema y su solución a los ciudadanos. Y digo, no lo informan ni cuando se produce, ni cuando se conoce, ni cuando se repara, ni pasados unos días, con lo cual, si no informan, ni antes ni después de resuelto, ni hasta que llega el momento en que un medio de comunicación se interesa, es que no informan porque no querían informar. Y no querer informar es tanto como querer ocultar. Y solo se conoce cuando lo publica *Diario de Navarra*. Y esa es la realidad. Y la prueba de esto es, por un lado, la contestación que dio el Consejero en el Parlamento en una respuesta que, cierto es, no iba dirigida a él, iba dirigida a la Responsable de Comunicación, presente en el Pleno, que no quiso responder, o lo que señala el propio informe.

El informe, en su último párrafo, dice: «Hubiese sido una temeridad informar a la ciudadanía antes de tener resuelto el problema». De acuerdo, vamos a aceptarlo. Pero claro, es que el informe, y aquí, y además se dice y se presume y me parece muy bien, se dice que «el problema se resolvió a las 17:21 horas del 19 de abril», a las seis horas de conocerse, ya estaba resuelto el problema. Y, a partir de esa hora, nadie informó. Y al día siguiente, nadie informó. Y al siguiente, nadie informó, hasta que *Diario de Navarra*, al descubrir el pastel, informó. Y el Gobierno, a través de Hacienda –creo–, hubo de confirmar los datos. Por tanto, la pregunta sigue pendiente. ¿Por qué no se informó a la ciudadanía del grave fallo inmediatamente después de resolver el problema? ¿Por qué no se informó a través del Servicio de Prensa, como se hizo en similares casos, aunque de menor envergadura? Por ejemplo, el 4 de septiembre de 2014: «Un fallo informático ha afectado esta mañana durante cerca de tres horas a los servicios del Gobierno de Navarra. La avería ha estado localizada y se ha solucionado y tal». O en el 2013, también hemos encontrado: «Un fallo informático causa interrupciones en la red de Salud, Hacienda y Desarrollo Rural. Técnicos del Gobierno de Navarra trabajan en restablecer el sistema y normalizar el acceso a las historias clínicas». Es decir, hay antecedentes en posibles fallos de seguridad, quizá no de esta envergadura, no lo sé, pero la información es inmediata. Se espera a la resolución del problema. Desde luego, y palabras textuales del informe, «sería una temeridad hasta no tener resuelto». Y en ese informe no se habla de hasta no tener validadas las consecuencias y así alargamos dos días en un informe forense... No, no, no. Hasta no tener resuelto, y en ese mismo informe se dice que

el problema estaba resuelto el 19 de abril a las cinco y media de la tarde. Y no se enteran los ciudadanos hasta que un medio de comunicación lo descubre dos días y medio después.

Y mientras se informaba eso, he visto las notas de prensa de esos días, y desde luego no las voy a volver a comentar, pero el Gobierno estaba informando de cosas que le interesaban más al Gobierno que a los ciudadanos. Y no voy a comparar, tampoco, la incidencia de unas y otras, pero ahí están. Por lo tanto, insistimos, se ha producido el más grave fallo de seguridad informática que afecta a los datos de los contribuyentes, se ha producido en plena campaña de la Renta, el Gobierno no se ha enterado hasta que un ciudadano lo ha comunicado, se ha extraviado o se ha perdido constancia de la denuncia en Policía Foral, no se ha reprogramado el sistema para cumplir la nueva normativa de seguridad y tampoco se ha recomendado a los usuarios cambiar la contraseña o el PIN y, además, insisto, se ha hecho lo peor que debe hacerse, que es no informar adecuadamente a la población de estos fallos que afectan a seguridad.

Ahí están estas preguntas para, según cómo se respondan, podremos despejar las dudas y algunas afirmaciones o conclusiones que hemos esgrimido. Muchas gracias.

SRA. PRESIDENTA (Sra. Aranburu Bergua): Gracias a usted, señor Sánchez de Muniáin. Turno de palabra ahora para el señor García.

SR. GARCÍA JIMÉNEZ: Muchísimas gracias, Presidenta. Agradezco, cómo no, las explicaciones dadas y las aclaraciones técnicas que se han dado en esta comparecencia. Sí que hemos visto, quizá, una falta de asunción de responsabilidades por parte tanto del señor Aranburu como de la Consejera de Presidencia, Función Pública, Interior y Justicia.

Yo tengo dos preguntas que no quedan, que es evidente que falta una respuesta. La primera es qué hubiera pasado si esta persona no se hubiera dado cuenta y no hubiese dado la voz de alerta, ¿nos hubiésemos enterado? Esa es una duda que existe.

Y una segunda, el por qué no se informa a la ciudadanía una vez, en este caso, solucionada la alerta y el problema, porque, efectivamente, tal y como ha recordado el portavoz de UPN, el mismo 19 a la tarde ya está resuelta y no se informó de esta cuestión o no tuvo transcendencia pública en este caso.

Aceptamos el mero hecho de que una vez no se ha puesto solución al problema, no se informe, claro está, yo creo que es compartido por todos. Evitar un sistema que está vulnerado, evitar la intromisión de cualquier hacker o lo que pueda suceder. Pero insisto, una vez solucionado el problema, no entendemos por qué no se informa, como ya se ha hecho en otras ocasiones. Es típico, entiendo, del Gobierno de la transparencia. Pues esto es ejemplo de transparencia para este Gobierno.

Y luego es especialmente grave el problema ocurrido, porque efectivamente ocurre o se produce en medio de la campaña de la declaración de la renta, un momento en el cual hay un mayor flujo de utilización y de datos.

Por lo tanto, creemos conveniente asumir responsabilidades por parte de uno de los dos Consejeros, porque insisto, aquí pocas explicaciones más allá de la presentación y el dejar los aspectos técnicos o al propio Director dar una explicación y dar la cara. Por lo tanto, yo creo

que quien debe dar la cara o debería haber dado la cara, insisto, son los propios Consejeros, más allá de las cuatro valoraciones que se han hecho por parte de ambos Consejeros.

Y claro, es una alerta que yo creo que no hace falta, y no es conveniente generar ningún tipo de alarma y creo que puede ser compartido por todos, pero sí que los ciudadanos deben de tener la certeza de que sus datos fiscales, evidentemente, están bien protegidos. Y para eso, efectivamente, hace falta invertir, más allá de la propia inversión que hace el Gobierno, en evitar que los datos sean vulnerados y, sobre todo, no vulnerar un derecho de confidencialidad de los contribuyentes y asegurar que, efectivamente, ninguna de las personas contribuyentes de nuestra Comunidad han sido afectadas, cosa que tampoco se sabe con certeza, como digo, si así ha ocurrido.

Creemos que son unos sucesos, desde nuestro punto de vista, de extrema gravedad, como también entendemos que es de extrema gravedad, insisto, esa falta de asunción de responsabilidades.

Lo decía antes en mi primera intervención, que este Gobierno, que nosotros creemos que no lo hace todo de manera correcta y adecuada, en vez de asumir cierta responsabilidad, siempre son errores puntuales o errores, insisto, de terceros.

Me gustaría poner algún ejemplo para que vean que no son palabras huecas ni vacías. Yo creo que son hechos fehacientes y reales que, por desgracia, estamos sufriendo todos los navarros. Y, efectivamente, también era un error reciente que el Departamento de Educación, con la suspensión de la OPE de maestros, se escudaron en la falta de respuesta de un recurso, por un error, en este caso, de la oficina de Correos. También era un error la doble convocatoria de los Inspectores de Educación. En este caso, un error del Servicio de Recursos Humanos. Nunca es responsabilidad política. También era lo que vimos ayer, la comparecencia del señor Laparra también era un error. Visto lo visto y vistas las explicaciones del señor Laparra, el hecho de que apareciese un nombre de una empresa privada en el pliego de condiciones de la adjudicación de un contrato público. Insisto en que también eso era un error. Tantos y tantos errores creo que debe de conllevar la asunción de algún tipo de responsabilidades.

Y volviendo a lo que hoy nos explican, entendemos que creemos que esto pone, en cierta medida, en tela de juicio no solo la seguridad de los datos fiscales de la ciudadanía, de los ciudadanos navarros, sino todos aquellos datos a los cuales tiene acceso, en este caso, la Administración.

Efectivamente, las aclaraciones técnicas y las dudas, se ha dado respuesta, pero quedan dudas de si esto, independientemente, se puede detectar que pueda volver a suceder, de cara al futuro. No hay garantías cien por cien y creo que así fue también respuesta, en este caso, del Consejero, con base en una pregunta. No hay fiabilidad cien por cien del sistema en este caso, por lo tanto, puede ser vulnerable de cara a otros posibles daños que, efectivamente, afecten también a los datos de todos los contribuyentes.

Poco más que añadir. El hecho de que creemos que se debe de invertir mucho más en garantizar la seguridad de la información relativa a todos los ciudadanos de nuestra Comunidad y lo cierto es que, tras un hecho grave que nosotros consideramos de extrema gravedad, insisto, es momento de que los Consejeros, el Consejero, la Consejera, asuman la responsabilidades que les corresponden como tal, porque todos, en su conjunto, el Gobierno

en su conjunto y, en particular ustedes como responsables, son los encargados de velar por la seguridad de los datos fiscales y los datos, en general, y la información, en general, de todos los navarros y navarras. Por lo tanto, queda aún necesaria, quizás, esa asunción de responsabilidades y, como digo, dos preguntas claras que creo que deben dar también respuesta y no solo al Partido Popular, sino a la ciudadanía en general. El hecho de qué hubiese ocurrido en caso de si esta persona no hubiera dado la voz de alerta, porque entendemos que, si no, no se hubiese detectado y qué se va a hacer, en este caso, para detectar la posibilidad de que vuelva a ocurrir esta vulnerabilidad del sistema. Muchas gracias.

SRA. PRESIDENTA (Sra. Aranburu Bergua): Gracias a usted, señor García. Tiene la palabra ahora el señor Garmendia.

SR. GARMENDIA PÉREZ: Muchas gracias, señora Presidenta, y muchas gracias a los Consejeros que hoy nos acompañan, junto con don Mikel Sagüés, el Director General, y el equipo que le acompaña. Nosotros, en esta comparecencia, la cuestión ha empezado muy clara con lo que ha dicho el señor Aranburu. El señor Aranburu ha dicho que nos van a presentar las acciones que se han tomado tras. Así ha empezado a hablar. Las acciones que se han tomado. Nosotros, lo que echamos de menos es que estas acciones no se hubiesen tomado antes. Eso es lo que a nosotros nos hubiese gustado. Y también agradecemos al señor Sagüés que sea tan claro y asuma sus responsabilidades. Desde luego, es loable y nosotros, desde luego, le felicitamos por ello. Y también habla y claramente dice que «una vulnerabilidad es un fallo». Efectivamente, es un fallo, y es que el Gobierno de Navarra ha cometido un fallo. Las cosas hay que reconocerlas y así están.

Nosotros, tras conocer este fallo, esta vulnerabilidad, hicimos una petición de información en la que tratamos de pedir explicaciones sobre lo que había pasado y lo recibimos aquí. El informe técnico de vulnerabilidad que nos pasaron en tiempo y forma y que es un poco la versión ampliada de lo que hoy se ha presentado. Tras leerlo, lo vamos a comentar un poco, porque es curioso que la primera página, en las primeras líneas, diga: «El Gobierno de Navarra se encuentra con todo esto». Claro, es que un Gobierno, cuando llega nuevo, se encuentra con cosas y, en principio, tendría que detectarlas y cambiarlas, que lleva tres años. Pero empezar un informe diciendo que todo esto se lo encuentra el Gobierno de Navarra es una obviedad tan grande... Se lo encuentra, pues claro que se lo encuentra. Es que es así. Gobierno de Navarra se ha encontrado en este caso con la vulnerabilidad que nos ocupa. Es que sería... Si ustedes venían para cambiar, pues claro, esto se lo encuentran. No van a seguir... ¿O es así con todo? ¿O no van a cambiar nada?

Y a partir de ahí, nos empieza a hablar del control de accesos y representación, lo que se llama CAR, y habla de claves o certificados. Mire, nosotros empezamos por ahí. En nuestra opinión, el error y el tema de la vulnerabilidad. Nosotros creemos que los sistemas informáticos navarros siguen siendo muy vulnerables, porque piden, exactamente, claves o certificados. Y es que tiene que ser claves y certificados. Yo creo que esa es una buena opción que ustedes tendrían que hacer y tomar nota. Claves o certificados, no. Claves y certificados. Eso es necesario, porque eso sí que, desde luego, no solo nos da seguridad de que los datos no van a ser asaltados, sino que vamos a tener trazabilidad de quién está accediendo a los datos, que me parece importantísimo. Por lo tanto, con claves no sabemos la trazabilidad.

Les voy a contar una anécdota que nos está pasando y que nosotros estamos comprobando. Mire, cualquiera que pida a través de un DNI hace bloquear el PIN de un DNI. Yo puedo hacer

bloquear el PIN de cualquiera de ustedes, lo puedo hacer bloquear. Lo bloqueo. No funciona. Y, a partir de ahí, meto, otra vez su DNI y pido que me llegue por correo ordinario el PIN. Estoy atento a su buzón, cojo la carta y ya tengo su PIN y su DNI. Eso pasa. Y eso no pasaría si hubiese PIN y certificado digital. Por lo tanto, háganlo. Es que lo tienen ustedes que hacer, porque esto...

Le tengo que decir que un ataque múltiple –como ustedes dicen aquí y detallan– de diez mil ataques, un ataque múltiple de una combinación DNI+PIN y que les entre en el sistema, perdone que le diga, pero es un error de principiante. Es una vulneración de chupete. Eso lo sabe cualquiera. Y entonces, ustedes llevan tres años, ya se lo que ustedes me van a decir, pero ustedes llevan tres años en el Gobierno y un señor o señora, porque todavía no sabemos lo que es, denuncia, por lo visto, llama por teléfono. Que no tenemos tampoco la traza de esa llamada y estaría bien lo que ha dicho el portavoz de UPN, saber la traza de esa persona, quién es y por qué, porque, a lo mejor, es que puede ser un héroe, es que habría que efectivamente compensarle, ¿o es un villano y antes de informarles se ha llevado datos? Es que no lo sabemos. Porque por lo visto la Policía Foral tampoco tiene constancia de la denuncia. Hombre, constancia de algo ya tendrá la Policía Foral, por lo menos de la llamada al 112. Algo habrá. Por lo tanto, nosotros, desde luego, creemos que aquí hay un error grave y, además, muy pueril.

Mire, usted dice que ha hecho un análisis forense desde 2007 a día de hoy y dice que no hubo ataques hasta entonces. Mire, eso no lo pueden saber. No sé cómo ustedes, con tanta alegría, dicen que han hecho un informe forense desde 2007 a nuestros días y no ha habido ningún ataque. Ustedes no pueden saber eso. Y si ustedes pueden saber con certeza que desde 2007 hasta hoy no ha habido ningún ataque, dígalo aquí. Dígalo aquí, señor Director General. No ha habido ningún ataque desde 2007 a nuestros días. Ningún ataque ni por mínimo que fuera. Es que no se puede saber. Se puede saber que no ha habido un ataque masivo, pero que ha habido gente que ha entrado con la vulneración del DNI+PIN, hombre, que si puede haber habido... Usted no puede negarlo. Puede haberlo habido, desde luego.

Pero nosotros pediremos ese informe forense. Vamos a hacer una petición de información y vamos a pedir ese informe forense porque no tenemos ningún porcentaje de certeza de que eso es así.

Quisiéramos saber qué tiene que decir de todo esto la empresa que le lleva la seguridad, porque nosotros podemos pedir compensaciones, porque la empresa de seguridad ustedes han dicho que –en la página 5, me refiero, del informe que ustedes me pasaron– en 2007 hubo un nuevo contrato de ciberseguridad, mucho más amplio, en el que invirtieron mucho más. Entonces, ¿no hicieron un primer análisis?, ¿no hicieron todas las pruebas necesarias para saber cuáles eran los puntos vulnerables? Porque es que ustedes dicen, también, en la página 4, que ustedes han detectado 308.819 ataques o intentos de explotación o vulnerabilidades. 308.000 ataques. Pero que ninguno ha sido para Hacienda. Es que no nos lo creemos. Ustedes dicen: «No ha habido ningún ataque a la aplicación de Hacienda DNI+PIN», y luego, a continuación, nos dice que ha habido 308.000 ataques o intentos de explotación de vulnerabilidad. No entienden ustedes que nosotros no nos creemos, por lo menos, la parte primera. ¿No lo entiende? ¿Es que no hubo ninguno a Hacienda? Pues no lo podemos saber, porque luego, en el punto 2 de la página 6, ponen, y en negrita, dice: «Nosotros estamos poniendo el foco y el esfuerzo de la actualidad en la auditoría de seguridad de las

aplicaciones». Pues vaya... Si ustedes han puesto el foco ahí, donde no hayan puesto el foco, mal andamos. Porque claro, si ustedes han puesto el foco donde se ha detectado una vulnerabilidad importante, grave y que, en nuestra opinión, no está corregida –no está corregida por el propio ámbito vulnerable de la aplicación de Hacienda–. Que insisto, yo les he dicho cómo sacar el PIN de cualquiera de ustedes. Así que yo, desde luego, tendría mucho cuidado. Porque ustedes siguen hablando, y en este informe lo único que hablan y lo único que dicen es, de la cantidad de cosas que están haciendo, que ya se hacían, porque aquí algunos ya sabíamos que esto se hacía. Luego, en la página 7, hablan de cortafuegos. Y de lo que ustedes están invirtiendo en cortafuegos. Otra. Si ustedes invierten en cortafuegos y no les corta ni esto...

Pues mire, yo le voy a decir cuál es la realidad de lo que está pasando en el Gobierno de Navarra y lo que está pasando en la informática del Gobierno de Navarra, aparte de que los señores Consejeros echen balones fuera y no asuman ninguna responsabilidad. Yo creo que es una pena que en Navarra y ahora mismo, en su parte tecnológica, haya tanto conocimiento teórico, porque hay mucho conocimiento teórico, pero no hay conocimiento práctico. No hay expresión de lo práctico en la parte tecnológica. Nosotros echamos de menos practicidad. Menos teoría y más practicidad. Y nosotros seguimos pensando que hay ahora mismo un riesgo para Navarra y más aún cuando ha entrado, efectivamente, la GDPR y nosotros no estamos preparados, porque, efectivamente, DNI+PIN no cumple GDPR. No cumple las mínimas exigencias de la normativa europea. Pero nosotros seguimos ahí y estoy seguro de que sus compañeros –no le estoy diciendo a usted, señor Director General–, los compañeros de los Consejeros ahora dirán que todo va bien y todo perfecto. Pero es que no. Podemos ser políticos y ponernos a un lado de la política o a un lado de la tecnología. Y la tecnología es verdad que no es inocente y muchas veces tiene cosas tecnológicas, pero, en este caso, ustedes le darán la razón y le dirán que está haciéndolo muy bien. Y están actuando en contra de los sistemas de seguridad navarros, que ustedes saben que no están cumpliendo con la normativa mínima de GDPR que Bruselas nos exige desde el 25 de mayo. Ustedes lo saben, pero bueno. Allá ustedes, porque, al final, son ustedes los responsables.

Ustedes y el Gobierno de Navarra no creen en la inteligencia artificial, no creen en la digitalización, no creen en la modernización, no creen en las nuevas tecnologías, porque, lo siento, señor Sagüés, y a usted no le incumbe, porque usted está puesto allí, es un cargo del Gobierno, efectivamente, pero entiendo que usted tiene que luchar mucho contra este Gobierno, porque es un gobierno viejuno, es un gobierno del pasado y que no tiene sensibilidad tecnológica. Con lo cual, desde aquí, a usted, señor Sagüés, todo mi aprecio y reconocimiento, porque luchar contra esto es muy complicado.

Pero en su informe, al final, ahora nos viene con que ustedes van a formalizar, ahora, de repente, con la figura del Responsable de Seguridad en cada departamento. Tres años después. La figura del Responsable de Seguridad, tres años después, y que van a constituir el Comité de Seguridad. Tres años después. Tarde y solo son promesas. Porque fíjese si solo son promesas que estamos esperando todavía el nombre de la persona responsable de la protección de datos, porque hasta ahora lo único que tenemos es un decreto de la posición. Y la normativa europea, a partir del 25 de mayo, era obligatorio, porque esta normativa es de abril de 2016 y ya pedía esta persona, que en Navarra no la tenemos. Tenemos el decreto, pero no tenemos la persona. Y entonces, ustedes no están cumpliendo y nos creemos que ahora porque hayan pasado estas cosas, como van a poner a otras personas con otros cargos y

otros títulos, van a meter más teoría, pero van a seguir sin cumplir con la práctica. Por lo tanto, nosotros, entendemos que no están apostando por la tecnología, que nos están pasando por encima otras Comunidades en tecnología y que eso, desde luego, redunda en la imagen y en el funcionamiento de esta Comunidad y afecta a los ciudadanos. Y vaya que si afecta. Porque usted sabe que el Gobierno ha sido denunciado por la Agencia Española de Protección de Datos, ¿verdad? Yo creo que los señores Consejeros también lo saben. Ha sido denunciado por la mala utilización de una herramienta tecnológica como es el WhatsApp.

Ustedes saben que el Consejo General del Poder Judicial está estudiando el acceso a nuestras herramientas judiciales, ¿verdad? Esa es la situación de la seguridad de los datos de Navarra. Nosotros insistimos, creemos que aquí hay, siendo el caso grave, sin llegar al extremo, creo que falta, desde luego, que se asuman responsabilidades, falta, desde luego, sensibilidad tecnológica y nosotros lo que queremos es que se adapte a los tiempos tecnológicos de mayo de 2018, como exige la Unión Europea, que Navarra se adapte a ese marco y nos dejemos de teorizar y pasemos a la práctica. Mojémonos. Pasemos a la acción. Muchas gracias.

SRA. PRESIDENTA (Sra. Aranburu Bergua): Gracias, señor Garmendia. Tiene la palabra ahora, por Geroa Bai, el señor Castiella.

SR. CASTIELLA IMAZ: Eskerrik asko, mahaiburu anderea. Arratsalde on, kontseilari jaun-andereok baita Sagüés jaunari. Eskerrik asko emandako azalpenengatik. Quiero dar la bienvenida también a los acompañantes, señor Etxeberri, señor Boyanov y señor Arlegui, creo recordar, a esta comparecencia. A mí, francamente, me gustaría saber tanto como el señor Garmendia sobre cuestiones de informática, pero, sintiéndolo mucho, soy un pequeño ignorante en estos temas. Ahora bien, me preocupa y mucho, además, que usted sea capaz de con mi DNI sacarme el PIN y hacer no sé qué perrerías que ha dicho usted que sería capaz de hacer como, por lo visto, lo ha podido ser una persona, según informaciones periodísticas, un joven hacker. Yo no sé si era señor, señora... bueno, informaciones periodísticas, señor Garmendia, más allá de ser un joven hacker, que no es lo mismo que un joven cracker, señor Sánchez de Muniáin, que es aquel que lo usa para objetivos ilícitos. El hacker es un aficionado a la informática, el cracker es aquel que lo usa para fines ilícitos.

En cualquiera de los casos, ya nos ha situado en un contexto más amplio de cuál era el objeto de la solicitud de comparecencia que cursaba Unión del Pueblo Navarro, tanto a la Consejera de Presidencia, Función Pública, Interior y Justicia como al Consejero de Hacienda y Política Financiera. Son ambas solicitudes en el mismo sentido y era en los términos de conocer dónde se había sustanciado esa brecha de seguridad y, sobre todo, subsanar responsabilidades. Ahí es donde centraba la solicitud de comparecencia el señor Sánchez de Muniáin, diciendo, además, que la brecha o la vulnerabilidad en el DNI+PIN se extendía a muchos más ámbitos que el de los datos tributarios. Pues evidentemente que se extiende a más ámbitos, a todos aquellos donde se usa el DNI+PIN. Evidentemente. A todos aquellos, incluso los que ejercían, los sistemas que se pusieron en marcha en gobiernos anteriores con DNI+PIN. Yo, desde luego, no quiero ser frívolo y decir que aquí no ha pasado nada, no quiero traslucir que a mí no me preocupa que ha habido aquí un problema que ha podido ser grave. Yo no lo niego. En cualquiera de los casos, creo que se ha solucionado con la suficiente solvencia y que el señor Sagüés, además, ha dado las explicaciones pertinentes que había que dar.

El señor Sánchez de Muniáin traía dos comparecencias por repetido, una para el Consejero de Hacienda y Política Financiera y otra para la Consejera de Presidencia, Función Pública, Interior

y Justicia. Ahora bien, si le preocupaba tanto haberla pedido también en la de Sanidad, donde también se emplea el mismo sistema, o en la de Desarrollo Económico, donde también se emplea el mismo sistema para según qué tipo de registros. En el Servicio de Energía y Minas, en cualquiera de ellos. Pregúntele al señor Zarraluqui y sabrá a lo que me refiero. Podría haber usted pedido a todos y cada uno de los Consejeros, porque el objetivo estaba claro, yo creo que era hacer una situación de alarma y, tal y como hizo usted en el Pleno del pasado 3 de mayo, generar una situación en la que quisiera cargar todas las culpas de todo ello al Consejero de turno, lo que me parece, entre comillas, bien, porque creo que también el Gobierno debe dar sus explicaciones. Yo lo que no sé es hasta qué punto por la publicación de una información periodística, esa información se ha podido precipitar o no. Como comprenderá, si la alarma de mi casa se estropea, yo no voy a anunciar, señor Sánchez de Muniáin, que la alarma de mi casa se ha estropeado. No voy a abrir esa puerta y a usted se lo explicó el señor Consejero, evidentemente –no me haga así–.

Desde luego, lo que no voy a tolerar son sus falsos dilemas y sus apelaciones a lo bien que lo hacía su Gobierno en legislaturas pasadas, porque ha mencionado usted una nota de prensa del año 2013 en la que decía «fíjese, nosotros, la misma mañana informamos de que había habido un fallo de seguridad». No, perdone. Usted se refería a una nota de prensa del año 2013 en el que decía que «la avería detectada a las 9 de la mañana ha dificultado el acceso a las historias clínicas informatizadas de Atención Primaria y Especializada», no se habían dejado a la luz pública ningún tipo de datos. Evidentemente que la gente se había dado cuenta de que había un fallo en la seguridad, porque no podía acceder a sus datos.

Pero no es, para nada, el mismo sistema y, por tanto, el procedimiento, el protocolo ante una brecha de seguridad, señor Sánchez de Muniáin, no es el mismo y no debe ser el mismo y usted lo que no puede es aplicar aquí un falso dilema, acusando al Gobierno de no sé qué ocultaciones, no sé qué tapar datos, con un interés completamente oportunista. Evidentemente, y si no lo ha leído y me hace el gesto así, craso error, señor Sánchez de Muniáin, porque, efectivamente, aquí también hay una responsabilidad y yo entiendo el interés que pueda usted tener en hacer un ataque político oportunista de machaque, porque es lo que les toca, evidentemente, ya lo sabemos. Han pasado tres años y ya nos hemos dado cuenta. Pero, desde luego, hágalo con un poco de seguridad y, sobre todo, aferrándose a unos datos comparables y aferrándose a unos datos que puedan ser seguros.

El exdirector general del ramo también nos mencionó una serie de responsabilidades. Yo no sé si estamos detectando hoy un fallo de seguridad que deriva desde la implantación de un sistema que usted, por lo visto, sabe hackear desde el año 2003. Francamente, me preocupa que un exresponsable del ramo me diga que es capaz de hackear eso y que no haya hecho nada, cuando haya tenido hace bien poco responsabilidades en ese ámbito. Me preocupa, y crease usted que mucho, cuando se habla de la falta de asunción de responsabilidades. Creo que se debería hacer con mucha mayor responsabilidad. Aquí se ha intentado una y otra vez traslucir y dejar encima de la mesa el mensaje de que se han sacado a la exposición pública, a la luz pública, una serie de datos. Yo, francamente, no sé si es tan fácil como lo dice el señor Sánchez de Muniáin, desde luego, supongo que yo no sería capaz de hacerlo.

En cualquier caso, tal y como decía, la solicitud de comparecencia del Partido Popular, para que explique la exposición pública de datos fiscales. Hombre, aquí yo creo que exposición pública en los términos en los que se entiende una exposición pública como lo es un proyecto

de Gobierno de Navarra en el portal de Gobierno abierto, pues no ha sido una exposición pública. Exposición pública, por ejemplo, puede ser lo que ayer mismo hacía el Departamento de Hacienda con la lista de deudores de Hacienda; el señor García, del Partido Popular. Eso sí que podemos considerar que es una exposición pública.

Aquí podemos considerar que ha habido un fallo, sí. Y, desde luego, mi grupo considera que ha habido un fallo. ¿Podemos considerar que haya un incumplimiento efectivo de la Ley Orgánica de Protección de Datos, de aplicación, hace cinco días? Pues no lo sé, porque estamos hablando de hace algo más. Ahora bien, lo que sí sabemos es que ese Reglamento General de Protección de Datos que viene de 2016, como bien nos lo recordaba el señor Garmendia, establece también una serie de protocolos, una serie de modos de proceder a la hora que se detectan, que se producen estas brechas de seguridad, estos fallos en la seguridad, y nos dice claramente lo que hay que hacer. Y lo tengo aquí. Y es que primero habla de registrar la incidencia. Después, averiguar si supone un riesgo para los afectados. El siguiente paso es notificar a la autoridad de control, cuestión que nos han informado que se ha hecho, e informar a las personas afectadas, cuestión que también se nos ha dicho que se ha hecho. Esto lo dice un manual de uso de la Ley Orgánica de Protección de Datos y el Reglamento General de Protección de Datos, que he conseguido en internet fácilmente y, a tenor de lo que nos ha contado el señor Sagüés, parece –ya le digo, no soy ningún experto en estas áreas, señor Garmendia– que se ha cumplido. Se podría hacer mejor, probablemente, se podrá hacer mejor absolutamente todo lo que se hace en esta vida.

Yo creo que este celo en que se aplique de la mejor manera posible todos los sistemas de seguridad de protección de datos debería ser reclamo de todos los grupos de esta Cámara. Desde luego no voy a ser yo el que diga que no se ha hecho. Ahora, lo que no voy a tolerar es que se intente hacer de esto ataque, que se haga derribo, que se haga acoso, ante unos hechos en los que entiendo que la responsabilidad, no voy a decir ni siquiera compartida, pero sí derivada, y además derivada de unos momentos en los que estamos acostumbrados como de cierto a cierto tiempo; también asistimos a los ataques de hackers rusos. Exactamente el mismo día en el que se dio a conocer esta noticia, en mi teléfono –que aquí lo tengo– me venía una actualización y era, concretamente, de seguridad por una serie de bugs que eran un fallo de seguridad de los datos protegidos del teléfono de la marca Apple. Decía el señor Sagüés de Microsoft, de IBM, de cualquiera de ellos.

A este señor, señora, o señorita, o señorito que ha detectado este fallo de seguridad, yo no sé si habría que proponerle la Medalla de Oro de Navarra, señor Sánchez de Muniáin, o si, por lo menos, habría que hacerle algún reconocimiento por haber llegado a este tipo de conclusiones en cuanto a la seguridad de los sistemas informáticos de Gobierno de Navarra, o si, por el contrario, lo que se debe hacer es, efectivamente, una revisión en profundidad, una auditoría –como ya nos están diciendo–. Desde luego tendremos mucho interés en comprobar también ese informe forense –si soy capaz de entenderlo– que hay solicitado y que nos adelantaba el señor Garmendia.

Yo creo que con lo que hemos oído aquí, en vez de dar un voto de confianza o, por lo menos, de profesionalidad, y no me estoy refiriendo a un voto de confianza política a los gestores, lo que estamos es dando legitimidad a esos ataques, a esas utilizaciones de fuerza bruta que nos comentaba el señor Sagüés, y que dejamos a los pies de los caballos a los técnicos propios del

departamento y de quienes se encargan de verdad en los diferentes departamentos del Gobierno de Navarra a gestionar esa seguridad.

Ya les digo, frente a cualquier tipo de mensaje que se quiera lanzar aquí sobre ocultación de información. Decía el señor Sánchez de Muniáin, concretamente, no querer informar es tanto como querer ocultar. Informar mal, señor Sánchez de Muniáin, alegar a esas notas de prensa que no tienen nada que ver con el caso que nos concierne, es tanto como engañar. Eskerrik asko.

SRA. PRESIDENTA (Sra. Aranburu Bergua): Gracias, señor Castiella. Tiene la palabra ahora, por EH Bildu, el señor Araiz.

SR. ARAIZ FLAMARIQUE: Eskerrik asko, lehendakari anderea. Ongietorria ematen diet Presidentzia eta Ogasuneko kontseilariei eta haiek datozen lankideei ere bai. La verdad, yo creo que hay que partir, por lo menos desde nuestro grupo parlamentario, de un desconocimiento importante en cuanto a algunas de las cuestiones que se plantean. Por lo tanto, creo que es interesante agradecer la información y, sobre todo, agradecer la posible respuesta a las preguntas que vayamos a formular en el sentido que se planteen desde esa ignorancia.

Creemos que el señor Sánchez de Muniáin y el señor Garmendia han venido a la comparecencia con la creencia de que tienen un hueso y que no hay que soltar este hueso bajo ninguna de las... Aquí han pillado hueso y hay que agarrarlo hasta que se acabe el hueso. En ese sentido, algunas de las preguntas que se han formulado, yo creo que son, digamos, que se las hace cualquiera esas preguntas, tampoco es que hayan descubierto el Mediterráneo y, a través de los informes que han solicitado al departamento o de la exposición que se haya hecho hoy aquí, se pretenda decir «bueno, ya le hemos pegado al Gobierno». Yo creo que hay que partir de una situación –y ese elemento, que ya se ha dicho, pero por parte del Director General, señor Sagüés–, de que fue un fallo, evidentemente, y un fallo, al haber una vulnerabilidad, hay un error y, además, se le ha calificado de grave. Es decir, no estamos ante cualquier situación, no estamos ante cualquier fallo en el sistema informático que permite internamente o no permite internamente a los usuarios, al funcionariado, al personal de las Administraciones Públicas acceder al servidor para, no sé, para acceder a no sé qué dato, a no sé qué informe en un momento determinado, es una cuestión interna. No. En este caso, puede tener repercusiones externas y desde ese punto de vista entiendo que esa gravedad ya la reconoce el propio Gobierno.

Por lo tanto, dicho esto, yo creo que hay que partir de aquí. Y en ese desconocimiento que decía, no entiendo muy bien cuando se plantea y cuando se nos dice que se ha detectado la vulnerabilidad, se ha detectado el acceso porque esta persona lo pone en conocimiento de Gobierno de Navarra, pero que no había sido explotado con anterioridad. Me gustaría que se nos explicara qué significa que no se ha explotado con anterioridad. Es decir, si se tiene la certeza, o la seguridad, o el conocimiento de que no había habido intrusiones anteriores parecidas a esta o que, teniendo esa certeza, incluso pudiendo haber detectado algún tipo de incursión, no se ha accedido directamente a los datos, que yo creo que es la preocupación que nos está embargando aquí. Es decir, si alguien sin conocimiento del Gobierno de Navarra y sin conocimiento del titular de esos datos, por supuesto, datos que son confidenciales y no estamos solo hablando de datos que tenga el Gobierno de Navarra en relación con, como se ha dicho, datos fiscales, sino a otra serie de datos, si se nos puede, en el lenguaje más simple

posible, explicarnos esto de «no explotado con anterioridad» y que solo fue por este ciudadano, ¿qué quiere decir? ¿Que este ciudadano fue el único que entró y aprovechó esa vulnerabilidad? –por lo menos, que se tiene constancia–. No sabemos si obtuvo datos, no sabemos si se lo dijo al Gobierno de Navarra o le dijo «ojo, que tenemos aquí una puerta, que tienen una puerta y que, si he entrado yo, cualquiera puede entrar».

Supongo que eso es lo que se planteó por este ciudadano o ciudadana que, desde luego, nosotros no lo calificamos ni de Robin Hood ni de villano, no sabemos exactamente lo que pudo ser. Probablemente hay que partir de que utilizó un acceso ilegal, un acceso ilícito, es decir, nadie de los que estamos aquí, supongo, que entramos... No sé si el señor Garmendia lo ha intentado alguna vez y ha bloqueado, conoce mi DNI y puede acceder a mi DNI del Parlamento, en cinco viajes pone un PIN erróneo y se va a mi buzón. No sé si se ha ido a mi buzón y no sé si... A mí no me ha llegado ninguna notificación de Hacienda diciendo que ha habido alguien y que me cambian el PIN. No sé si el señor Garmendia, en esa maldad que nos ha transmitido aquí, lo ha hecho con alguna otra persona, pero, desde luego, creemos que no es el común de los mortales quien hace este tipo de actuaciones, no sé si son hackers o son crackers, no distingo exactamente la maldad o no de ese tipo de personas, pero, en este caso, creo que lo importante es aclarar eso, es decir, que «la vulnerabilidad no ha sido explotada con anterioridad», ¿qué significa? Si se nos garantiza, como se nos ha dicho... Porque claro, supongo que no se podrá garantizar este no acceso si se desconocía la vulnerabilidad, que es lo que se ha dicho también.

Es decir, no estábamos ante una vulnerabilidad conocida, sino ante una vulnerabilidad desconocida por el propio sistema. No sé si el proveedor –desconozco también quien es el proveedor de este sistema de seguridad– en su momento le ha hecho al Gobierno de Navarra algún tipo de verificación del sistema, lo que se ha planteado aquí, no se han hecho reprogramaciones, no se han hecho... –¿cuál era el término?– En este sistema de credenciales hay ausencia de reprogramaciones. Pues supongo que, si hay ausencia de reprogramaciones desde el 2005, diez años serán imputables a los gobiernos de UPN y tres imputables a este gobierno, incluso con el añadido que se ha manifestado desde el año 2016, hay una nueva normativa, no sé tampoco, desconozco esta normativa y, por tanto, me siento incapaz de contradecir lo que dice el señor Sánchez de Muniáin, entendiendo que se ha puesto en cuestión el sistema de DNI+PIN, no lo sé. Si eso es así, habría que plantearse, si eso es así, lo primero, pregunto, si eso es así... Si este sistema ha quedado ya invalidado o no. Yo creo que este sistema no ha quedado invalidado porque los bancos, por ejemplo, yo el banco con el que trabajo habitualmente lo utiliza. Y supongo que los bancos también serán tan vulnerables o más como una Administración Pública y serán también tan celosos como debería ser una Administración Pública para ello. Por lo tanto, a mí me gustaría conocer hasta qué punto esas afirmaciones son ciertas. Han dicho aquí afirmaciones categóricas diciendo «el Gobierno de Navarra incumple y el sistema que tienen de acceso y acreditación vía DNI+PIN está ya superado por razones de seguridad». Pues que se nos diga a ver si es eso así.

Y luego, también se ha preguntado por Unión del Pueblo Navarro si los datos han estado expuestos desde el 11 de abril, no sé, nos habla de la gráfica y del sismógrafo y del momento en que se produce ese ataque masivo por parte de este ciudadano o ciudadana, supongo que sería, pero, con anterioridad, ¿ha habido o no ha habido vulnerabilidad? Esa es la pregunta. Es decir, ¿la puerta estaba abierta desde el día que le venden el sistema al Gobierno de Navarra en el año 2005 que se implanta? ¿Sí o no? Porque claro, eso es importante saberlo. Es decir, si

esa puerta estaba abierta y lo desconocían y lo han desconocido sistemáticamente todas las Direcciones Generales de Telecomunicaciones –no sé si la que dirigía el señor Garmendia también en esas nuevas tecnologías, en lo que tanto hizo, no se preocupó de esta puerta, al parecer–. No sé. Entonces, quiero decir que si esa puerta existía que se nos diga también desde cuándo y si era posible detectarla, o si había que poner medios, si había algún tipo de medios, o si las vulnerabilidades se producen una vez que el sistema detecta por terceros, porque le han robado los datos, porque se los han bloqueado, o cuáles son los medios normales de conocimiento de las vulnerabilidades de los titulares de estas aplicaciones.

Y luego, hay una pregunta, efectivamente, que yo creo que también nos la hemos hecho todos y todas al leer la información, cuando conocimos esta información, cuando conocimos las peticiones de información o, en su caso, la respuesta que dio el Consejero, esa de qué hubiera pasado si... Pues probablemente si no nos enteramos, si la vulnerabilidad era tan vulnerable, por repetirlo, ¿había en esa aplicación en el sistema había algún sistema de alarma? Valga la pregunta. Es decir, ¿era posible detectar...? Porque si esta persona no hubiera sido este Robin Hood y hubiera entrado y hubiera robado los datos, ¿nos hubiéramos enterado? ¿O nos hubiéramos enterado solo si esta persona trata, en su caso, de chantajear al titular de esos datos o trata de chantajear al Gobierno de Navarra o trata...? Eso es importante saberlo, porque los sistemas de seguridad que pueda tener el Gobierno de Navarra, desde luego, yo creo, que deben de dar respuesta a esta pregunta. Supongo que habrá esos elementos y, en todo caso, se ha preguntado por qué no han saltado las alarmas. La pregunta es: ¿había alarmas? ¿Esta aplicación tenía alarmas? Y lo digo desde el más absoluto desconocimiento tecnológico, como suele decir el señor Garmendia, de quienes somos, en cierta medida, analfabetos tecnológicos en esta materia, desde luego.

Voy a terminar. Yo creo que el señor Garmendia suele utilizar ciertos términos... Que este Gobierno no cree en la digitalización, no cree en todo... Vamos, tenemos un Gobierno ateo en materia de tecnología, no sé si en otras cuestiones también, pero, desde luego, da la impresión de que en materia de tecnología este es un Gobierno ateo y el señor Garmendia es un deísta absoluto porque cree en todo, en Dios todopoderoso, en la tecnología diosa todopoderosa, etcétera.

Entonces, desde luego, creemos que, efectivamente, coincido en eso con el señor Garmendia, pasemos a la acción, intentemos resolver estos problemas. Creemos que si el problema está resuelto hay que felicitarse y hay que intentar que, si no hay ese cien por cien de protección, nos pongamos al máximo de protección, porque evidentemente, la protección de los datos personales es un derecho ya también fundamental y no están solo en juego los datos económicos, hay otra serie de datos. Tenemos datos en el Departamento de Salud que creo que son tan importantes o más y que deben de garantizarse en la privacidad de las personas y que cualquier mínimo temor a que el sistema de seguridad... En este caso, conocemos ataques masivos a entidades tan importantes como la CIA, como el Pentágono, como las tecnológicas que nos han..., que supongo que tendrán muchos más poderes que el Gobierno de Navarra, y aun así, existe esa situación de ataques masivos de control de la información y, en todo caso, agradezco nuevamente la información y agradezco la posible respuesta que se nos dé, porque creo que es importante aclarar algunos de los conceptos que aquí se han dejado en el aire como si este Gobierno fuera un incapaz en materia tecnológica.

SRA. PRESIDENTA (Sra. Aranburu Bergua): Gracias, señor Araiz. Tiene ahora la palabra el señor Velasco.

SR. VELASCO FRAILE: Gracias, Presidenta. Buenas tardes. Bienvenida a la Consejera Beaumont, al señor Mikel Sagüés y al señor Aranburu y al equipo que le acompaña. Trataremos de no ser repetitivos. Consideramos que, efectivamente, sí que induce a reflexión todo lo que tiene que ver con el análisis forense, pero me imagino que existen unas huellas digitales de todo lo que hacemos, unos accesos, y que algo de eso quedará y se podrá tirar del hilo para saber exactamente qué es lo que ha pasado.

Sí que somos conscientes de que las vulnerabilidades existen, muchas, constantemente y no es difícil encontrar noticias en el periódico. Por ejemplo, esta: «Desactivada la firma digital de los DNI electrónicos por un fallo de seguridad». Esta se refería a los expedientes de DNI expedidos después de 2015 y era un fallo del chip, del fabricante. Estas cosas sabemos que pasan. Quisiéramos preguntarle si cuando informan de todo este suceso al Centro Criptológico Nacional y les cuentan los problemas de vulnerabilidad que han tenido con el DNI y el PIN, ellos les refieren si en determinadas comunidades autónomas también han tenido problemas parecidos o no.

También entendemos que, independientemente del hueco, de la vulnerabilidad, existe un elemento importante aquí, que es lo que se refiere a la herramienta de hacking, es decir, aquí no es que estuviesen expuestos los datos, sino que esta persona, este experto, a través de una herramienta, que no sé si años anteriores existía o estaba desarrollada y permitía acceder o no, imagino que esto irá evolucionando, ha conseguido franquear esto. Y la pregunta que nos hacemos es qué hacía ahí ese señor o señora, por qué estaba haciendo eso. Creo que es una pregunta bastante...

Y luego, todo lo que tiene que ver con la vulnerabilidad nos remite a dos palabras. Una es exposición, otra puede ser riesgo, y otra puede ser daños, posibles daños. Y claro, ahí, efectivamente, habría que ver un poco las denuncias que hubiese en Policía por cuestiones de chantajes de temas digitales, todo lo que tiene que ver con los datos.

Nosotros creemos que, efectivamente, también esto se trata de un tema en el que hay que hacer un esfuerzo presupuestario, ya veo que se ha hecho. No sabemos si, a partir de ahora, van a ser objeto de ataques cuando dicen que ahora han actualizado absolutamente todos los cortafuegos, antivirus, auditorías de seguridad y tal, y haya personas que quieran intentar a ver cómo de seguro es aquello.

Lo importante es que no se vuelva a repetir. Eso no se puede garantizar, porque efectivamente cien por cien de seguridad no hay. No sabemos si aquí la oposición ha querido dar más importancia al fallo de seguridad, que entendemos que ha sido puntual, si quiere dar más importancia a eso, al posible fallo, o al hecho de no informar o a las dos cosas. No sabemos exactamente, pero sí que es verdad que lo quiere magnificar, aunque cierto es que estamos hablando de datos bastante sensibles y sí que es verdad que todo lo que sea por garantizar la seguridad estará bien. Nada más.

SRA. PRESIDENTA (Sra. Aranburu Bergua): Gracias, señor Velasco. Y finalizando el turno de portavoces, tiene la palabra la señora De Simón.

SRA. DE SIMÓN CABALLERO: Muchas gracias, señora Presidenta. Muy buenas tardes, señor Consejero, señora Consejera y todas las personas de sus equipos que les acompañan. Yo quiero comenzar felicitando al departamento, a la Dirección de Informática, Telecomunicaciones e Innovación Pública por el trabajo que han realizado, por lo rápido que han actuado y porque existía una vulnerabilidad, entiendo –no sé si lo he entendido bien–, en el sistema desde hace doce o quince años y se ha descubierto ahora. El que se ha descubierto ahora quiere decir que nadie había podido ver o superar esa vulnerabilidad para acceder a los datos. Creo que lo he entendido bien... En todo caso, felicitarles y felicitar también al ciudadano o a la ciudadana que detectó esta vulnerabilidad.

Y desde luego claro que nos parece un fallo grave del sistema informático. Nos parece grave. Ya está, se ha detectado y a mí me parece que esto no va más allá. Y voy a decir por qué no va más allá. Porque mire, a mí me ha parecido –y lo voy a decir– un poco frívola la actitud del señor Sánchez de Muniáin y la actitud del portavoz del Partido Popular, el señor García. Me ha parecido frívola y un tanto alarmista. ¿Qué hubiese pasado si...? ¿Y si resulta que...? ¿Y si el señor este, el ciudadano, es un tal? A mí, francamente, de verdad, como estamos en la semana esta de la novela o del libro, no sé qué semana es, me estaba pareciendo el guion de una novela negra. Y a mí me parece una frivolidad, porque el tema es serio.

En mi opinión, se ha actuado correctamente. Ya lo comentaba. O sea, en poco más de seis, siete horas ya estaba solucionado ese error que había en el sistema y entiendo que solo ha accedido un ciudadano. Este. Eso es lo que he entendido de su exposición. Si no, me corrige, porque, la verdad, yo tengo que reconocer, y es así, que no soy una persona tampoco experta en estas cuestiones, pero yo lo he entendido así. Solo ha accedido un ciudadano o ciudadana, esa persona que ha hecho la denuncia. Luego nadie más lo ha hecho nunca más antes. Porque si no, evidentemente, se hubiese detectado la vulnerabilidad hace, por ejemplo, se me ocurre, ocho años, por ejemplo, podría haber sido, ¿verdad? Que el ciudadano este hubiese probado hace ocho años. Sí, ¿no?

Por lo tanto, yo no le veo tanta gravedad a lo que ha sucedido después. No a lo de antes, porque, evidentemente, insisto, que haya un fallo que permita acceder a datos personales teniendo en cuenta que cada vez hay más registros informáticos, más datos que se pueden acceder vía telemática, desde luego es un problema.

Me ha asustado mucho el señor Garmendia. Porque si es verdad lo que ha dicho, yo me imagino a un hacker, a una hacker que está escuchando hoy esta Comisión ya dale que te pego a ver cómo entra a los datos de no sé quién, conociendo su carnet de identidad y no sé cuál. Yo, supongo que se habrá expresado mal, porque a mí me ha dejado temblando, no por mí, en particular, que, en fin, mucho que ocultar parece que no hay, porque... Por cierto, yo no sé, ya hago una pregunta, no sé si en esta base de datos, ¿se accede solamente a los datos fiscales, o sea, a la declaración de la renta de uno o de una, o a más datos? Porque si fuera así, a mí, casi ni me parece tan grave, porque yo propondría que se hicieran públicos los de toda la ciudadanía. Quiero decir, si se accede a otro tipo de datos o solo son los fiscales. Esa pregunta ya, por favor, me la responde. Pero decía, que sí que me ha dejado preocupada el señor Garmendia en ese sentido, porque si realmente es tan fácil, pues, en fin, yo desearía que... Él no, ya se lo preguntaré después, porque no es el que comparece.

Y tengo dos preguntas más. Una es cómo llega esta información a los medios de comunicación, si ustedes están investigando si la información ha salido del propio servicio, de departamentos

del Gobierno de Navarra. Claro que ha podido ser de la Policía o ha podido ser del propio señor. Y cómo se ha producido el hallazgo. Ya sé que esto es puro morbo y pura curiosidad. O sea, cómo esta persona lo ha hecho, porque ha podido ser un hallazgo fortuito o quizás realmente estaba probando a ver si pillaba algo.

Pues nada más. Me voy a permitir una especie de expresión vulgar, pero yo creo que «donde no hay mata, no hay patata» y yo creo que esto ya está resuelto. Gracias.

SRA. PRESIDENTA (Sra. Aranburu Bergua): Gracias, señora De Simón. Antes de proceder al turno de réplica para responder a todas las preguntas que se han planteado, vamos a hacer un receso de diez minutos.

(Se suspende la sesión a las 16 horas y 59 minutos).

(Se reanuda la sesión a las 17 horas y 15 minutos).

SRA. PRESIDENTA (Sra. Aranburu Bergua): Se reanuda la Comisión de Hacienda y Política Financiera. Turno de réplica ahora para el señor Consejero y la señora Consejera y el señor Sagüés. Como a ustedes les parezca más oportuno. ¿Empieza la señora Consejera? Sí.

SRA. CONSEJERA DE PRESIDENCIA, FUNCIÓN PÚBLICA, INTERIOR Y JUSTICIA (Sra. Beaumont Aristu): Únicamente transmito lo mismo que hacemos siempre en la Comisión de Presidencia, al menos, cuando he estado yo, que es que, en este receso, hemos intentado agrupar un poco las cuestiones que se han planteado que en algún caso se han repetido con otras expresiones para poderlas contestar. Esperamos acertar y que no quede nada en el tintero. Va a intervenir, entonces, en primer lugar, el señor Sagüés a los efectos de contestar a las preguntas más técnicas y luego ya cerraremos la comparecencia el Consejero Aranburu y yo.

SR. DIRECTOR GENERAL DE INFORMÁTICA, TELECOMUNICACIONES E INNOVACIÓN PÚBLICA (Sr. Sagüés García): Kaixo berriro. Creo que lo que procede es volver a contar varias cosas de las que he contado porque está claro que no han quedado claras. Es evidente que no lo he hecho bien, porque lo que quería transmitir no ha quedado claro y se ha repetido varias veces.

Quizás no me he detenido en definir lo que es un análisis forense. Es verdad que sobre eso he pasado un poco rápido. Entonces, ¿qué es el análisis forense? Creo que vulnerabilidad sí que ha quedado claro lo que es, el ataque también, pero ¿qué es el análisis forense?

En los sistemas de información de Gobierno de Navarra o de cualquier gran organización, lo que se hace es recoger, les voy a llamar trazas. Recoger trazas es recoger qué es lo que ha pasado en ese sistema de información a lo largo del tiempo. Se almacenan gigas y gigas de información todos los meses con qué es lo que ha pasado y quién ha accedido, desde qué dirección IP, a qué hora, etcétera. Eso es lo que permite, después, tener una trazabilidad de qué es lo que ha pasado. Entonces, cuando nosotros o cualquier otra organización detecta un problema o quiere mejorar uno de sus sistemas de información, lo que hace es analizar las trazas y ver qué es lo que pasa, cuánta gente accede a esta hora, cuánta gente accede a esta otra, para cosas que no tienen que ver con ataques informáticos, pero es bueno tener esa información porque te permite mejorar. Es en este punto, en esa trazabilidad, en la que precisamente nos concedieron este premio a principios de este año. Precisamente, Gobierno de Navarra es puntero, voy a decir, en trazabilidad. Tiene un sistema muy bueno, apoyado en este nuevo antivirus y apoyado en lo que se ha desarrollado en la Dirección General.

Entonces, un análisis forense es analizar esas trazas en busca de la información que se está buscando. En este caso, tenemos un ataque. El ataque explota una vulnerabilidad. Esta vulnerabilidad se explota de una manera concreta. La manera que he descrito, no sé si con acierto o con demasiada superficialidad, pero se explota de una manera concreta. Entonces, lo que hacen los técnicos de la Dirección General es analizar las trazas, no después ni en el momento del ataque, sino desde hoy hasta cuando tengamos trazas. En este caso, hasta 2007. Es hasta donde tenemos trazas. Antes no hay registros. El analizar las trazas nos permite garantizar –aquí siempre la garantía estoy hablando del 99,99, vale, porque hay esa duda, pero yo creo que tenemos la garantía, porque tenemos las trazas– que esta forma de explotar esta vulnerabilidad no había ocurrido antes. La única vez que alguien hace un ataque de fuerza bruta sobre el sistema de credenciales DNI+PIN es en el periodo en el que la persona que posteriormente pone en comunicación de Gobierno de Navarra esta vulnerabilidad está haciendo sus pruebas.

Aquí, alguno ha preguntado por qué lo hace. Pues yo también me lo pregunto. ¿Por qué lo hace? Esto es una actividad deportiva, prácticamente, es decir, voy a ver si consigo romperlo. No lo digo en broma, ¿eh? Es así. Se enseña en la universidad y el que tú sepas hacer eso como informático garantiza que cuando te toca programar los sistemas de información, tengas las cautelas y tengas el conocimiento suficiente para evitar este tipo de ataques. Es una disciplina en sí.

Entonces, tenemos una vulnerabilidad que se explota de una manera concreta. Comprobamos, de manera fehaciente, que esa forma concreta de explotar esta vulnerabilidad no ha ocurrido en el pasado y, por lo tanto, podemos garantizar que así ha sido. Con esto, el señor Garmendia ha dicho que no podemos, porque ha habido muchos ataques, cuando decimos que garantizamos, garantizamos lo que acabo de decir: para esta vulnerabilidad y de esta forma concreta. No decimos que no haya otras vulnerabilidades o que no se hayan podido explotar en el pasado o que se exploten en el futuro de otras formas. Es un poco lo que he querido decir.

Creo que eso es, por encima de todo, lo que no ha quedado claro en la presentación anterior y ahí espero haberlo aclarado ahora y si no, háganme gestos y lo intento de nuevo. Yo creo que esa es un poco la idea.

Respondiendo al señor Garmendia, cuando en el informe técnico decimos que nos lo encontramos así o que nos lo encontramos, en un momento pone «se encontró con», en ningún caso, y si no queda claro lo digo ahora, estoy intentando decir que como estaba así, que esto es una cosa del pasado... Creo que en mi intervención y siempre que me ha tocado venir aquí, soy bastante cuidadoso en eso. No intento decir «mira, la culpa es del anterior». Creo que no va por ahí. Y cuando decimos encontramos, nos encontramos en el informe, nos estamos refiriendo a que el ciudadano nos lo comunique y, por lo tanto, nos encontramos con esto. No me refiero a nada más que a eso. No va más atrás lo que queríamos decir.

En relación con la intervención del señor Sánchez de Muniáin, sobre la comunicación que se ha hecho, sobre si debería haberse comunicado, yo creo que eso sí que lo he explicado con bastante claridad. La comunicación que se ha hecho es exactamente la que marcaba la ley en tiempo y en forma y, además, muy rápido. Otra cosa es esa pregunta que queda en el aire y creo que es una pregunta lícita y a ver si consigo aclararla sobre si hay que comunicar a la ciudadanía, hacer una nota de prensa diciendo «había una vulnerabilidad en los sistemas de

Gobierno de Navarra». Es una pregunta lícita, me parece que es correcto. La realidad sobre las vulnerabilidades en Gobierno de Navarra, cuando las corregimos, es que corregimos vulnerabilidades todos los meses. Corregimos cientos de vulnerabilidades. Es así. Cada vez que reprogramamos, volviendo a ese término, un sistema de información, en esa reprogramación, en esas mejoras que se introducen, se cierran puertas que en un principio no se conocían, y que cuando lo mejoras, resulta que las detectas y las corriges. Y cada vez que hacemos una reprogramación de un sistema o mejoramos un sistema, obviamente no decimos «cuidado, fíjate, aquí ocurría...», porque realmente estaríamos todos los días diciendo que hay una vulnerabilidad.

Otra cosa es cuando una vulnerabilidad se explota y tenemos conocimiento de que ha obtenido datos de manera ilícita, ha bloqueado datos... En ese caso, es lógico que tengamos que comunicarlo, en primer lugar, a los afectados. Pero la alarma esa que probablemente haya surgido en relación con este tema es otra cuestión, es diferente, porque no es que los datos estuvieran expuestos y se han quedado en el aire, sino que una persona ha visto cómo acceder a este sistema, nos lo ha comunicado y lo hemos corregido muy rápido. Los datos no están expuestos seis horas, están expuestos quince años. Y están expuestos, y siento decirlo así, pero están expuestos ahora por alguna vulnerabilidad que no conocemos.

Cuando el Gobierno de Navarra, cuando yo voy a la Comisión Sectorial de Administración Electrónica, Gobierno de Navarra –y lo digo también para que tengamos esa tranquilidad, entre comillas– estamos muy arriba en relación con nuestros pares en el Estado en seguridad informática. Lo estamos. Creo que lo he dicho. Históricamente lo estábamos y ahora seguimos estándolo. Para nada comparto la visión del señor Garmendia de que lo tenemos esto dejado, para nada la comparto y creo que los hechos lo avalan. Entonces, un poco en relación con la comunicación. Creo que hay que discernir entre haber dejado los datos expuestos o que hubiera una vulnerabilidad, porque las hay y se detectó, se corrigió y se comunicó en tiempo y en forma a los afectados y al Centro Criptológico Nacional, que es lo que había que hacer.

No voy a entrar al detalle, pero ha habido vulnerabilidades muy graves en Gobierno de Navarra, ha habido bloqueos de información en Gobierno de Navarra, ha habido muchas cosas en Gobierno de Navarra históricamente. Creo que tampoco es justo decir que esta es la más grave de todas las que ha habido, pero, con eso, no quiero decir que no sea grave, porque he venido aquí a asumir esa responsabilidad y lo tengo claro, ¿eh?

Y yo creo que con eso básicamente respondo a la parte más técnica, si quieren, de las preguntas que se han hecho y cedo la palabra a los Consejeros.

SRA. CONSEJERA DE PRESIDENCIA, FUNCIÓN PÚBLICA, INTERIOR Y JUSTICIA (Sra. Beaumont Aristu): Nuevamente, por completar la información que acaba de aportar el Director General y, singularmente, por responder alguna pregunta que se me ha hecho directamente a mí, que creo que son cinco.

La primera, por el señor Sánchez de Muniáin, para aclarar quién dice la verdad: ¿el Jefe de Policía Foral en su informe o el Director General de Informática en el suyo, por lo que respecta a la expresión denuncia sí o no? Vamos a ver, eso usted lo extrae de la publicación en *Diario de Navarra* el 21 de abril que hablaba de una denuncia ante Policía Foral. Luego lo extrae de ahí, hombre, sí, lo extrae de ahí porque es el único sitio en que se ha hablado de eso y así lo formuló usted en la solicitud de pregunta a la Consejera Ollo, que la respondió el Consejero

Aranburu. Pero usted también lo ha calificado de aparente contradicción. Efectivamente es que es solo una aparente contradicción. Dicen los dos la verdad. El informe de Policía Foral se refiere a que no hay una denuncia formal, efectivamente, en Policía Foral. Lo que ocurrió fue una llamada al 112, el 112 lo deriva al CMC de Policía Foral y CMC a la Dirección General de Informática y Telecomunicaciones y, a continuación, esa Dirección General a Hacienda. Ese es el recorrido que tuvo este asunto. Por lo tanto, es absolutamente intrascendente la expresión denuncia, llamada, aviso, pedir auxilio, pedir socorro... Las llamadas al 112 son muy variadas en ese sentido.

Y, en relación con esa cuestión, el señor Garmendia dice: «Hay que conocer la traza de ese recorrido, de eso que comenzó con una llamada al 112». Entenderán ustedes que, primero, no nos lo han pedido y, segundo, no les vamos a facilitar tampoco la identidad de la persona que llamó al 112 y, precisamente, por la protección de datos. Precisamente por la protección de datos no se la vamos a facilitar.

Esa persona puede ser héroe, puede ser villano o villana, puede ser que le tengamos que dar las gracias, puede ser que le abramos un expediente porque hizo lo que no debía. Eso lo estamos viendo, pero que quede claro que no vamos a facilitar la identidad de esa persona, porque no debemos. Estaríamos incumpliendo precisamente con lo que todos queremos proteger.

El señor Sánchez de Muniáin también dice: «¿Cómo es posible que sin tener seguridad de que eso estaba funcionando bien y que era tan vulnerable el sistema del DNI+PIN se extendiera por orden foral de la Consejera para su uso para otras funciones o servicios?». Cuando dicté la orden foral extendiendo la posibilidad, como mera posibilidad, solamente, para que cada departamento decidiera, «yo que tengo una línea de subvenciones en tal materia de turismo o que tengo que conceder licencias de pesca, o que tengo entre mis atribuciones tal cuestión», pues es ofertar esa posibilidad que existía para el uso por cada departamento. Cada departamento asume y ve si eso es suficiente o es insuficiente. Por ahora, sinceramente, no hemos detectado ningún problema en ningún sentido.

El señor Garmendia también dice: «Es que están haciendo ustedes todo mal, van con mucho retraso, no han nombrado al Delegado de Protección de Datos». El Reglamento nos obligaba y hemos cumplido, con crear la figura del Delegado de Protección de Datos por un Decreto Foral que está aprobado, está publicado en el Boletín Oficial, tras haber debatido bastante en el Gobierno, haber visto cómo lo han hecho en otras comunidades autónomas. Su adscripción era propio que lo fuera a la Dirección General de Informática, era propio que lo fuera a la de Presidencia, era propio que lo fuese a los Servicios de Estadística, que en nuestro Gobierno dependen de Hacienda. Después de ver todo eso, nos pareció que lo propio era que no podía mezclarse en el gallinero quien tiene que controlar, a su vez, y que lo propio es que estuviese en Presidencia. Así se ha aprobado. No hemos todavía designado a la persona nominativamente. Estamos en eso. Lo haremos muy próximamente. Pero lo que tiene que quedar claro es que desde que creamos esa figura como Dirección de Servicio adscrita a la Dirección General de Presidencia, la Directora General de Presidencia ejerce, de hecho, las funciones de Delegada de Protección de Datos en estrecha colaboración con la Dirección General de Informática, Telecomunicaciones e Innovación Pública.

Y, por último, creo que no me olvido de nada de lo que se me ha planteado a mí, el señor García es el que ha insistido fundamentalmente, aunque también el señor Sánchez de

Muniáin. Sí, yo asumo mi responsabilidad. La ha asumido el Director General de Informática que fue designado por el Gobierno a mi propuesta y, consecuentemente, la responsabilidad política es mía.

SR. CONSEJERO DE HACIENDA Y POLÍTICA FINANCIERA (Sr. Aranburu Urtasun): Voy a cerrar, simplemente, porque tampoco tengo grandes cosas que decir. Ya se ha explicado todo y yo creo que se ha contestado a las preguntas y a las dudas que quedaban.

Creo que se me ha atribuido a mí alguna especie de acreditación negativa de que nunca se había producido alguna cosa de estas. Yo eso no lo dije. A mí, en la rueda de prensa, me pasaron la nota. Lo que dije es que expliqué cómo había sido la vulnerabilidad, más o menos, en los términos que se ha dicho, algo un poco más chapuceramente, pero dije que lo que se había hecho era analizar y que nos había costado tiempo porque hasta la semana pasada no se pudo terminar –esto es una rueda de prensa que hice a primeros de mayo–, que se han revisado once años y que más no se podía, y que desde 2007 hasta la actualidad se ha rechazado cualquier tipo de incidencia, es decir, que no había habido ninguna filtración ni ninguna captación de datos por este motivo. Eso es un poco lo que yo transmití. Yo, por supuesto, no puedo decir que no haya habido vulnerabilidades, filtraciones en estos últimos años, porque, además, todos ustedes saben que tengo la condición de funcionario de Hacienda y hemos vivido situaciones de vulnerabilidades que darían para anécdotas y para escribir un libro, pero no es el momento, porque tampoco tengo pruebas, pero sí que se podrían comentar a lo largo de otra jornada, en otro momento.

En todo caso, por terminar, sí que precisamente y basándome o valiéndome de esta experiencia, creo que los controles de seguridad, al menos en el Departamento de Hacienda, en estos últimos años, se han reforzado. No hay motivo para la alarma. Todos los protocolos de los que yo hasta hace tres años era usuario se están reforzando de una manera exponencial. No se pueden hacer idea de qué manera se están controlando las cosas, lo cual a mí me da mucha tranquilidad como Consejero y como ciudadano. Y, por lo tanto, en este momento y por este tema que no va más allá del hueso ese que comentaba el señor Araiz, yo creo que lo que hay que hacer es felicitar a los técnicos de la Dirección General de Informática por la labor hecha en este episodio. Pues sin más. Eskerrik asko.

SRA. PRESIDENTA (Sra. Aranburu Bergua): Pues solo queda ya agradecer a los presentes, al señor Consejero de Hacienda y Política Financiera, a la señora Consejera de Presidencia, Función Pública, Interior y Justicia, al señor Sagüés y a todo el equipo que ha acompañado, por su presencia en esta Comisión y por todas las explicaciones aportadas, y dado que no hay más puntos que tratar, se levanta la sesión.

(Se levanta la sesión a las 17 horas y 32 minutos).