Expediente Nº: E/02662/2018

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos ante la HACIENDA TRIBUTARIA DE NAVARRA, en virtud de denuncia presentada por UNIÓN DEL PUEBLO NAVARRO, y teniendo como base los siguientes

HECHOS

PRIMERO: Con fecha 4 de mayo de 2018, tuvo entrada en esta Agencia un escrito remitido por UNIÓN DEL PUEBLO NAVARRO, en el que expone lo siguiente:

Con fecha 20 de abril de 2018, han tenido conocimiento a través de los medios de comunicación de que se había producido un fallo de seguridad en la entidad denunciada, que provoco que durante horas los datos de contribuyentes de Navarra estuvieran expuestos al acceso por parte de terceros no autorizados.

Según se detalla en la información publicada por DIARIO de NAVARRA, de fecha 21 de abril de 2018, el sistema informático del Departamento de Hacienda, sufrió un fallo de seguridad que permitía acceder a los datos de miles de contribuyentes navarros. Dicho fallo, que se detectó tras una denuncia, ya se ha solucionado.

Un ciudadano detecto el fallo y verificó una vulnerabilidad en el sistema mediante D.N.I. y PIN. Esta persona presentó una denuncia ante la Policía Foral y puso también los hechos en conocimiento del Departamento de Hacienda, con el que colaboró en el análisis del fallo. Desde el Gobierno de Navarra aseguraron que la incidencia se solucionó en cinco horas. También se indicaba desde el Departamento de Hacienda que no había constancia de que ninguna persona se viera afectada.

El fallo consistía en que aplicando herramientas con las que se podían hacer peticiones masivas a la página web y al probar con un DNI todas las combinaciones posibles de cuatro números (PIN) se podía obtener el PIN correspondiente al DNI y así acceder a los datos.

El denunciante manifiesta que el fallo de seguridad en el sistema de identificación DNI+PIN, no solo podría afectar a los trámites en la Hacienda de Navarra, sino también a los trámites con otros departamentos u organismos del Gobierno de Navarra.

Aportan copia de la publicación de los hechos en el DIARIO DE NAVARRA de 21 de abril de 2018.

SEGUNDO: Tras la recepción de la denuncia la Subdirección General de Inspección de Datos procedió a la realización de actuaciones previas de investigación para el esclarecimiento de los hechos denunciados, teniendo conocimiento de los siguientes extremos:

Con fecha 11 de junio de 2018, la HACIENDA TRIBUTARIA DE NAVARRA ha remitido a esta Agencia la siguiente información en relación con los hechos denunciados:

1. Los hechos denunciados dieron lugar a la apertura de la incidencia de seguridad (InSeg-25), que se recibió mediante llamada telefónica al S.O.S. Navarra. Aportan copia del expediente completo de la incidencia que contiene varios documentos.
2. Según consta en el detalle de la incidencia, respecto a los HECHOS:
    a. A las 11.12 horas del día 19 de abril de 2018, se recibió una llamada en el teléfono de emergencias S.O.S. Navarra, informando de que se había detectado una vulnerabilidad en los servicios telemáticos del Gobierno de Navarra que permitía acceder a datos de terceras personas. La llamada fue derivada a la Policía Foral que recabo la información y comunicó el informe del incidente a la Dirección General de Informática, Telecomunicaciones e Innovación Pública (DGITIP) a las 11:52 horas.
    b. El Jefe de la Sección de Seguridad y Gestión del Rendimiento, en calidad de responsable de seguridad, autoriza el acceso y análisis de los registros de las aplicaciones por parte del equipo técnico de la DGITIP para comprobar los hechos.
    c. A las 13:25 horas, tras las comprobaciones técnicas, se verifica que la alerta es veraz y que la vulnerabilidad afecta a la credencial de identificación (DNI+PIN) y se inician los trabajos de implementación de la corrección. Así mismo la Sección de Seguridad estudia las medidas a adoptar para mitigar el riesgo.
    d. A las 17:21 horas se finaliza la corrección en el entorno de producción y se planifican las acciones para extraer la información necesaria que permita evaluar el impacto de posibles robos de credenciales y accesos ilegítimos.
    e. El día 20 de abril de 2018 se comprueba que la vulnerabilidad también afecta a la credencial (DNI+Clave especifica de renta) y se realizan los trabajos de corrección que finalizan a las 14:45 horas.
    f. Con fecha 24 de abril de 2018, el Jefe de Seguridad comunica la incidencia al CERT del Centro Criptológico Nacional que se registra con la referencia “***REF.1”-

g. Con fecha 25 de abril de 2018, el Jefe de Sección de Seguridad comunica la relación de personas sobre las que existe una sospecha razonable de que sus credenciales han podido verse comprometidas, analizando las trazas de auditoria.

h. Esta primera lista se refiere a los accesos realizados desde enero de 2018 hasta esa fecha y constan cuatro personas (incluida la persona denunciante) a las que inmediatamente se les revoco la credencial DNI+PIN; lo que se comunicó a los interesados mediante llamada telefónica y mediante escrito.

i. Con fecha 2 de mayo de 2018, el Jefe de Sección de Seguridad informa de que tras el análisis de los registros de accesos desde el año 2017 hasta el 11 de abril de 2018, no constan indicios que permitan fundar una sospecha sobre el compromiso de las credenciales (DNI+PIN) y (DNI+CLAVE DE RENTA) de otros usuarios diferentes de los cuatro anteriores.

j. No obstante con fecha 14 de mayo de 2018, en el informe del Director General con las conclusiones del análisis forense realizado se eleva el número de potenciales afectados a 34, en esa misma fecha se revocan las credenciales de todos ellos (29 restantes).

3. RESPECTO A LA VALORACION DE LOS HECHOS:

a. La vulnerabilidad afectaba a dos credenciales de identificación y autenticación integradas en el componente corporativo de control de accesos y representación (CAR) para el acceso a servicios telemáticos del Gobierno de Navarra. Ambas credenciales son de la modalidad de clave concertada.

b. Cuando un contribuyente, persona física, intenta acceder mediante esas credenciales, debe informar de su NIF y de la clave PIN asociada al mismo; una vez introducidos ambos, el cliente web verifica que el NIF es correcto (comprobando la letra) y a continuación se comunica con el Gobierno de Navarra para validar el PIN, comprobando que corresponde a ese NIF. En caso de que no sea correcto se pueden realizar hasta cinco intentos fallidos, en el quinto el PIN queda bloqueado.

c. No obstante, dado que la validación de la letra del NIF se realizaba en el navegador (cliente web), un usuario con los conocimientos suficientes podría eludirla y acceder al servidor con un (DNI+PIN), donde el NIF estuviera integrado únicamente por una letra y otro carácter incorrecto para el número. En este caso, el sistema no era capaz de controlar los intentos fallidos por lo que era vulnerable a un ataque de fuerza bruta, que permitía obtener de forma ilegítima las credenciales de terceras personas.

d. Para detectar aquellos usuarios que podrían haber sufrido robo de credenciales se han analizado las trazas de auditoria de CAR, entendiendo que las credenciales potencialmente comprometidas son aquellas en las que existe al menos un autoregistro en CAR de un NIF con un código de verificación incorrecto (letra incorrecta o carácter diferente de una letra). Se han encontrado 33 identificadores que cumplen esa condición.

e. Los registros “sospechosos” encontrados se refieren al periodo comprendido entre el 12 y el 19 de abril de 2018.

f. La vulnerabilidad no suponía en sí misma, la exposición no autorizada de información a terceros, pero si un riesgo alto de robo de credenciales con lo que se podía suplantar la legítima identidad de una tercera persona y acceder a su información confidencial.

g. Con el objetivo de obtener más información para detectar el acceso ilegitimo a información confidencial, se han analizado las trazas de auditoria de los 34 NIF cuyas credenciales se consideran comprometidas, obteniendo los servicios a los que han accedido desde la fecha de registro con NIF erróneo, detectando:

   Tres direcciones IP desde las que existen sospechas fundadas de que se ha realizado un ataque de fuerza bruta contra las credenciales afectadas.

   La mayoría de los accesos realizados en las fechas indicadas se refieren a la aplicación “Reimpresión IRPF” (visualización de declaraciones de IRPF de diversos años) así como el documento de datos fiscales IRPF 2017 y la carta de la campaña de la renta. En algunos casos también hay accesos a la consulta de datos de domiciliación bancaria del IRPF.

   En dos de los usuarios no existen accesos en dichas fechas, por lo que se descarta un acceso ilegitimo a su información.

   En 25 de los usuarios se han detectado accesos durante el periodo vulnerable desde las direcciones IP del ataque. En estos casos, existe un patrón más o menos constante por el que se consultan las declaraciones del IRPF de diferentes años consecutivos. El hecho de que existan estos accesos exhaustivos y desde las direcciones IP del ataque no significa necesariamente que se haya realizado un acceso ilegitimo, pero eleva las sospechas sobre la posibilidad de que haya sido así.

   En 7 de los usuarios se han detectado accesos durante las fechas vulnerables pero desde direcciones IP diferentes de las del ataque. Este hecho no permite afirmar que no hayan

existido accesos a información de forma ilegítima pero las sospechas son inferiores.

4. RESPECTO A LAS MEDIDAS CORRECTORAS APLICADAS.

   a. Se ha corregido la vulnerabilidad introduciendo los mismos controles de bloqueo del cliente web en el servidor. Los intentos fallidos que se producen a partir de un NIF correctamente formado quedan sujetos al sistema de bloqueo y los intentos fallidos a partir de un NIF incorrecto se registran en los registros de auditoría para su análisis.

   b. Así mismo, de forma adicional se han tomado las siguientes medidas:

      Planificación de auditorías técnicas de las aplicaciones afectadas.

      Planificación de proyectos para introducir un segundo factor de autenticación.

      Impulso del plan, ya existente, para la integración de los servicios del HTN en la credencial Cl@ve y progresiva extinción de la credencial DNI+PIN.

   c. Compromiso de credenciales. El 25 de abril de 2018, se procedió a revocar preventivamente las credenciales de los 5 sujetos sobre los que, en esa fecha, existían sospechas razonables de que habían podido verse afectados por un robo de credenciales. Tras la revocación se les comunico dicha circunstancia a los usuarios afectados.

      Así mismo, con fecha 14 de mayo de 2018, se procedió a revocar preventivamente las credenciales de las otras 29 personas, lo que se comunicó a los afectados.

   d. Con fecha 22 de mayo de 2’18 se remitió a los 34 usuarios potencialmente afectados una comunicación informándoles de los accesos que se habían realizado a su información, detallando el servicio accedido, la fecha y hora y el identificador IP desde el que se realizó el acceso y la información consultada, con objeto de que cada interesado pueda comprobar la legitimidad o no de dichos accesos.

5. El informe contiene un ANEXO. Sobre “Comunicación de direcciones IP”, en el que se plantea la cuestión de si es jurídicamente procedente comunicar a las personas afectadas por la eventual filtración de información confidencial, las direcciones IP desde las que se han realizado los accesos sospechosos. Esta información permite a cada

persona reconocer los accesos que ha realizado y detectar los que pueden ser ilegítimos.

Tras el análisis de diferente normativa al respecto, y lo dispuesto en el artículo 34 del nuevo Reglamento General de Protección de Datos que establece la obligación de comunicar a los interesados afectados por aquellas violaciones de seguridad de los datos personales que pueden entrañar un algo riesgo para los derechos y libertades de las personas físicas, se considera jurídicamente posible la comunicación de las direcciones IP de acceso a los afectados por la incidencia de seguridad.

6. CONCLUSIONES:
    a. Se ha constatado que la vulnerabilidad detectada por un ciudadano fue explotada, comprometiendo la credencial DNI+PIN de 34 ciudadanos y accediendo a numerosa información confidencial de los mismos.
    b. Todos los ataques por fuerza bruta se realizaron desde tres direcciones IP, en franjas temporales que no se solapan entre si y que coinciden con los días en que el propio ciudadano ha reconocido haber realizado sus pruebas para comprobar que la vulnerabilidad era explotable. Además las tres direcciones IP pueden ser relacionadas con el ciudadano ya que accede a sus propios datos a través de dos de ellas y accede a los datos de otra persona a través de una de las anteriores y de la tercera dirección IP.
    c. Por lo tanto, cabe concluir que la exposición de datos a que ha dado lugar el ataque, se circunscribe únicamente a la actividad desarrollada por el propio ciudadano que detecto la vulnerabilidad y que la comunicó al Gobierno de Navarra.
7. Por otra parte, según manifiestan, no les consta que se haya realizado la indexación por parte de buscadores de la información confidencial extraída ilegítimamente.
8. La aplicación fue diseñada y mantenida por las unidades competentes de la Dirección General de Informática, Telecomunicaciones e Innovación Pública del Departamento de Presidencia, Función Pública, Interior y Justicia del Gobierno de Navarra.

FUNDAMENTOS DE DERECHO

I

Es competente para resolver la Directora de la Agencia Española de Protección de Datos, conforme a lo establecido en el artículo 37.d) en relación con el artículo 36, ambos de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en lo sucesivo LOPD).

II

El Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos), (en lo sucesivo RGPD) indica que las violaciones de la seguridad de los datos personales pueden entrañar daños y perjuicios físicos, materiales o inmateriales para las personas físicas. Por consiguiente, tan pronto como el responsable del tratamiento tenga conocimiento de que se ha producido una violación de la seguridad de los datos personales debe, sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, notificar la violación de la seguridad de los datos personales a la autoridad de control competente, a menos que el responsable pueda demostrar, atendiendo al principio de responsabilidad proactiva, la improbabilidad de que la violación de la seguridad de los datos personales entrañe un riesgo para los derechos y las libertades de las personas físicas.

El responsable del tratamiento debe comunicar al interesado sin dilación indebida la violación de la seguridad de los datos personales en caso de que puede entrañar un alto riesgo para sus derechos y libertades, y permitirle tomar las precauciones necesarias. La comunicación debe describir la naturaleza de la violación de la seguridad de los datos personales y las recomendaciones para que la persona física afectada mitigue los potenciales efectos adversos resultantes de la violación. Dichas comunicaciones a los interesados deben realizarse tan pronto como sea razonablemente posible y en estrecha cooperación con la autoridad de control, siguiendo sus orientaciones o las de otras autoridades competentes, como las autoridades policiales. Así, por ejemplo, la necesidad de mitigar un riesgo de daños y perjuicios inmediatos justificaría una rápida comunicación con los interesados, mientras que cabe justificar que la comunicación lleve más tiempo por la necesidad de aplicar medidas adecuadas para impedir violaciones de la seguridad de los datos personales continúas o similares.

En el artículo 33 del RGPD establece la forma en que ha de notificarse una violación de la seguridad de los datos personales a la autoridad de control, determinando lo siguiente:

“1. En caso de violación de la seguridad de los datos personales, el responsable del tratamiento la notificará a la autoridad de control competente de conformidad con el artículo 55 sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, a menos que sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas. Si la notificación a la

autoridad de control no tiene lugar en el plazo de 72 horas, deberá ir acompañada de indicación de los motivos de la dilación.

2. El encargado del tratamiento notificará sin dilación indebida al responsable del tratamiento las violaciones de la seguridad de los datos personales de las que tenga conocimiento.

3. La notificación contemplada en el apartado 1 deberá, como mínimo:

a) describir la naturaleza de la violación de la seguridad de los datos personales, inclusive, cuando sea posible, las categorías y el número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados;

b) comunicar el nombre y los datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información;

c) describir las posibles consecuencias de la violación de la seguridad de los datos personales;

d) describir las medidas adoptadas o propuestas por el responsable del tratamiento para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.

4. Si no fuera posible facilitar la información simultáneamente, y en la medida en que no lo sea, la información se facilitará de manera gradual sin dilación indebida.

5. El responsable del tratamiento documentará cualquier violación de la seguridad de los datos personales, incluidos los hechos relacionados con ella, sus efectos y las medidas correctivas adoptadas. Dicha documentación permitirá a la autoridad de control verificar el cumplimiento de lo dispuesto en el presente artículo."

Por otro lado, el artículo 34 del Reglamento mencionado indica cuando es necesario informar de una violación de la seguridad de los datos personales al interesado, señalando lo siguiente:

1. Cuando sea probable que la violación de la seguridad de los datos personales entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento la comunicará al interesado sin dilación indebida.

2. La comunicación al interesado contemplada en el apartado 1 del presente artículo describirá en un lenguaje claro y sencillo la naturaleza de la violación de la seguridad de los datos personales y contendrá como mínimo la

información y las medidas a que se refiere el artículo 33, apartado 3, letras b), c) y d).

3. La comunicación al interesado a que se refiere el apartado 1 no será necesaria si se cumple alguna de las condiciones siguientes:

a) el responsable del tratamiento ha adoptado medidas de protección técnicas y organizativas apropiadas y estas medidas se han aplicado a los datos personales afectados por la violación de la seguridad de los datos personales, en particular aquellas que hagan ininteligibles los datos personales para cualquier persona que no esté autorizada a acceder a ellos, como el cifrado;

b) el responsable del tratamiento ha tomado medidas ulteriores que garanticen que ya no exista la probabilidad de que se concretice el alto riesgo para los derechos y libertades del interesado a que se refiere el apartado 1;

c) suponga un esfuerzo desproporcionado. En este caso, se optará en su lugar por una comunicación pública o una medida semejante por la que se informe de manera igualmente efectiva a los interesados.

4. Cuando el responsable todavía no haya comunicado al interesado la violación de la seguridad de los datos personales, la autoridad de control, una vez considerada la probabilidad de que tal violación entrañe un alto riesgo, podrá exigirle que lo haga o podrá decidir que se cumple alguna de las condiciones mencionadas en el apartado 3."

En el supuesto presente, la quiebra de seguridad se produjo el día 19 de abril de 2018, es decir, con anterioridad a la plena aplicación del RGPD, que se produjo el día 25 de mayo de 2018. La Hacienda Tributaria de Navarra, a pesar de no estar obligada a notificar la quiebra de seguridad detectada, al haber sucedido con anterioridad al día 25 de mayo de 2018, procedió a notificarla y a cumplir lo establecido ante esta situación en el RGPD.

La Hacienda Tributaria de Navarra ha expuesto, detalladamente, todas las actuaciones realizadas tras la detección de la quiebra de seguridad y las medidas correctoras aplicadas. Asimismo, al existir sospechas de que algunas personas podían haberse visto afectadas por un robo de credenciales, se revocaron tales credenciales y se comunicó a todos los afectados.

La Hacienda Tributaria de Navarra ha cumplido lo establecido en el RGPD, aún con anterioridad a ser plenamente aplicable el mencionado Reglamento. A excepción de la notificación en el plazo de 72 horas a esta Agencia Española de Protección de Datos, al haber podido afectar la brecha a derechos y libertades de los interesados.

III

El artículo 126.1, apartado segundo, del Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, aprobado por Real Decreto 1720/2007, de 21 de diciembre (RLOPD) establece:

"Si de las actuaciones no se derivasen hechos susceptibles de motivar la imputación de infracción alguna, el Director de la Agencia Española de Protección de Datos dictará resolución de archivo que se notificará al investigado y al denunciante, en su caso."

Por lo tanto, de acuerdo con lo señalado, por la Directora de la Agencia Española de Protección de Datos,

SE ACUERDA:

PROCEDER AL ARCHIVO de las presentes actuaciones.

NOTIFICAR la presente Resolución a la HACIENDA TRIBUTARIA DE NAVARRA y a UNIÓN DEL PUEBLO NAVARRO*.*

De conformidad con lo establecido en el apartado 2 del artículo 37 de la LOPD, en la redacción dada por el artículo 82 de la Ley 62/2003, de 30 de diciembre, de medidas fiscales, administrativas y del orden social, la presente Resolución se hará pública, una vez haya sido notificada a los interesados. La publicación se realizará conforme a lo previsto en la Instrucción 1/2004, de 22 de diciembre, de la Agencia Española de Protección de Datos sobre publicación de sus Resoluciones y con arreglo a lo dispuesto en el artículo 116 del Reglamento de desarrollo de la LOPD aprobado por el Real Decreto 1720/2007, de 21 diciembre.

Contra esta resolución, que pone fin a la vía administrativa (artículo 48.2 de la LOPD), y de conformidad con lo establecido en los artículos 112 y 123 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, los interesados podrán interponer, potestativamente, recurso de reposición ante la Directora de la Agencia Española de Protección de Datos en el plazo de un mes a contar desde el día siguiente a la notificación de esta resolución o directamente recurso contencioso administrativo ante la Sala de lo Contencioso-administrativo de la Audiencia Nacional, con arreglo a lo dispuesto en el artículo 25 y en el apartado 5 de la disposición adicional cuarta de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-Administrativa, en el plazo de dos meses a contar desde el día siguiente a la notificación de este acto, según lo previsto en el artículo 46.1 del referido texto legal.

Mar España Martí
Directora de la Agencia Española de Protección de Datos