Expediente N.º: EXP202207931

RESOLUCIÓN DE PROCEDIMIENTO SANCIONADOR

Contenido

Del procedimiento instruido por la Agencia Española de Protección de Datos y en base a los siguientes

ANTECEDENTES

PRIMERO: Notificación de brecha de seguridad de datos personales.

Con fecha 27/05 y 27/06/2022, se notificó a la División de Innovación Tecnológica de esta Agencia una brecha de seguridad de los datos personales remitida por la **DIRECCIÓN GENERAL DE COORDINACIÓN DE ESTUDIOS** como responsable del tratamiento **(SECRETARÍA DE ESTADO DE SEGURIDAD-MINISTERIO DEL INTERIOR)** con NIF S2800109G (en adelante, reclamada).

En los escritos-formularios recibidos sobre la notificación de la brecha, se informa de lo siguiente:

En el de 27/05/2022, según el formulario: "*notificación inicial*" "*a los efectos de cumplimiento con el plazo de notificación establecida en el RGPD. En el plazo máximo de 30 días se notificará información adicional. En caso contrario, la autoridad de control considerará esta notificación COMPLETA*", se indica, entre otras circunstancias:

-Ha consistido en el robo de un portátil y un pendrive corrompido con información de actuaciones policiales que se estaban utilizando para estudios de "*prevención y detección de delitos*", sin que estuvieran los datos cifrados de forma segura, anonimizados o protegidos de forma que fuesen ininteligibles para quien haya podido tener acceso, y se puede identificar a las personas.

- En tipos de afectados: Datos básicos (Ej.: nombre, apellidos, fecha de nacimiento), Imagen (Fotos o vídeos), DNI, NIE, Pasaporte y/o cualquier otro documento identificativo, sobre condenas e infracciones penales, datos de localización, de contacto, de salud (otros datos de salud).

-En ¿cuántas personas han visto sus datos afectados por la brecha?, se indica 5.000, de un volumen total de personas sobre las que se recogen datos de 500.000. En respuesta a si hay miembros de colectivos vulnerables, como supervivientes de violencia de género o en riesgo de exclusión social-, y menores se indica que sí, si bien en la ampliación de información producida el 27/06/2022 se indica que no para ambos colectivos

-En la pregunta ¿Considera que ha tomado todas las acciones posibles y da por resuelta la brecha?, indica que No.

-En cuanto a si se ha comunicado la brecha a las personas afectadas, se indica que "*no serán informadas*".

- "*Se ha puesto el incidente en conocimiento de las autoridades policiale*s", por considerar que existe delito.

-El responsable del tratamiento es la DIRECCIÓN GENERAL DE COORDINACIÓN Y ESTUDIOS (DGCE), encuadrada en actividad de "*seguridad*", dependiente de la Secretaría de Estado de Seguridad (SES), y la SUBDIRECCIÓN GENERAL DE SISTEMAS DE INFORMACIÓN Y COMUNICACIONES PARA LA SEGURIDAD (SGSICS), adscrita directamente a la SES.

-Como "fecha de detección de la brecha, entendida como la fecha en la que el responsable tiene la certeza de que se han visto afectados *datos personales*", que consta en el formulario, indica 26/05/2022, y en "*¿Conoce la fecha en la que se inició?",* indica 4/05/2022, la de la sustracción del ordenador portátil.

En el apartado: *"¿se ha producido el incidente por algún fallo de deficiencia o incumplimiento de medidas de seguridad implementadas?*", se indica que sí.

Como diferencia entre el primero y el segundo comunicado de la brecha, en el segundo, de 27/06/2022, a diferencia del primera, indica que si considera que ha tomado todas las acciones posibles y da por resulta la brecha el 24/06/2022.

Acompaña al escrito de 27/06/2022 un INFORME que firma el DPD de la DGCE, en nombre de este, según refiere, sin fecha, titulado: "*INCIDENTE BRECHA SEGURIDAD TRATAMIENTO DATOS PERSONALES PDYRH (personas desaparecidas y restos humanos)*". Como antecedentes explica que a la notificación inicial de 27/05/2022, se

recibió el 30/05/2022 una comunicación de la AEPD en la que se consideraba que la información proporcionada no era completa, porque sigue en curso una investigación por parte del responsable del tratamiento sobre la brecha para determinar las causas circunstancias y alcance". Se otorgaba un plazo para completar la información máximo de 30 días, y se advertía que "*expirado el plazo, se valoraría la brecha con la información que obrara, sin perjuicio de las acciones que se puedan emprender*."

El informe amplía la notificación de la brecha. Se indica, en síntesis:

-La SES y sus órganos directivos dependientes, disponen de procedimiento de actuación para cuando se materializa una brecha. Tras la entrada en vigor de la Orden INT/424/2019, de 10/04 sobre política de seguridad de la información, remitió el 2/12/2020 a todos los organismos para los que está designado el DPD de la SES, la actuación formal a llevar a cabo cuando se produjese una violación de seguridad de datos personales, incluyendo la actualización de la aprobación de la LO 7/2021 de 26/05, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales (LO 7/2021 en lo sucesivo), a través del traslado de 15/02/2022 de un nuevo procedimiento. Manifiestan adjuntar ANEXO 1, si bien no figura.

-Explica las competencias y entidades que dependen de la SES, de acuerdo con la regulación de la estructura orgánica, y la Orden INT 429/2019 de 10/04 por la que se aprueba la política de seguridad de la información. Añade que en los hechos también se ve involucrada la SUBDIRECCIÓN GENERAL DE SISTEMAS DE INFORMACIÓN Y COMUNICACIONES PARA LA SEGURIDAD, (SGSICS).

Explica y detalla las competencias de la DGCE, en la que se encuadran diversas áreas. A tal efecto:

-Fomentar la participación y colaboración de la Universidad e instituciones y personalidades investigadoras en el desarrollo de las actividades y funciones que le corresponden, (art 5 bis y 1.6 del Real Decreto 146/2021, de 9/03, por el que se modifica el Real Decreto 139/2020, de 28/01 por el que se establece la estructura orgánica básica de los departamentos ministeriales, y el Real Decreto 734/2020 de 4/08, por el que se desarrolla la estructura orgánica básica del Ministerio del Interior). Para ello, cuentan con el "*ÁREA DE "VIOLENCIA DE GÉNERO, ESTUDIOS Y FORMACIÓN" (VGEF*)" en la que se "*formaliza la participación de técnicos, científicos y alumnos en prácticas en proyectos, actuaciones y actividades de la Secretaría de Estado de Seguridad."*

-La gestión centralizada para la coordinación efectiva y permanente del sistema de personas desaparecidas, a través del CENTRO NACIONAL DE DESAPARECIDOS (XXXX), adscrito al ÁREA DEL SISTEMA ESTADÍSTICO Y ATENCIÓN DE LAS VÍCTIMAS (SEAV).

-También detalla las funciones de la SGSICS, que ostenta competencia sobre seguridad de los sistemas de la información.

-Indica que el incidente de seguridad se produjo sobre actuaciones llevadas a cabo por el XXXX, que quedan amparadas por el tratamiento del fichero *PDyRH***,** cuyo responsable

del tratamiento es la DGCE. Aporta la información de su contenido inscrito en el Registro de actividades de tratamiento (RAT) dentro de la LO 7/2021, constando:

1. finalidad: "*actividades de tratamiento necesarias para la averiguación de la identidad de personas desaparecidas y cadáveres/ restos humanos sin identificar con el fin de detectar, prevenir e investigar delitos, de forma que se implemente la colaboración entre las fuerzas y cuerpos de seguridad tanto nacionales como autonómicas."*

2. *Legitimación del tratamiento: Ley Orgánica 2/1986 de 13 de marzo, de Fuerzas y Cuerpos de Seguridad, Ley de Enjuiciamiento criminal y artículo 11 de la Ley Orgánica 7/2021*"

3. "*origen de los datos*": "*diligencias policiales, personas desaparecidas, Nombre, apellidos, DNI, sexo, fecha de nacimiento, lugar de nacimiento, domicilio, descripción física, datos biométricos, datos genéticos, fotografías. Imágenes de impresiones dactilares y fotografías importadas desde el fichero de DNI. Denunciantes: Nombre, apellidos, DNI, sexo, fecha de nacimiento, lugar de nacimiento, domicilio y teléfono*."

-Manifiesta que:

1. "*Los trabajos para los que eran necesarios los datos personales iban dirigidos a desarrollar una herramienta predictiva de estimación de riesgo de desapariciones denominada SERDESVI -Sistema de Estimación de Riesgo de Desaparición Violenta- que se utilizaría para prevenir o detectar ilícitos penales en estos casos*".

2. *"La persona causante del incidente no es personal del Ministerio del Interior, es un investigador (colaborador) dentro de la estructura de la DGCE con diversos "status" jurídicos en el desarrollo de esta y otras herramientas similares. Dicho colaborador, tenía firmado un documento de confidencialidad y seguridad de la información*".

-En la parte III, final, del mismo informe, titulada: "*comunicación del incidente y posible brecha*", indica:

*"El colaborador que sufrió el robo lo comunicó al **"(…)**" (no detalla cual en concreto) el 4/05/2022", "sin especificar el contenido de la información que podría contenerse en los dispositivos sustraídos". "El día 6/05/2022, tras serle requerida más información", "amplió la denuncia y señaló que en el dispositivo podría contenerse información policial".*

Tras esta revelación, el DEPARTAMENTO DE ATENCIÓN A PUESTOS DE USUARIO (CAU) informó acerca de estos hechos al ÁREA DE INFRAESTRUCTURA Y SEGURIDAD TIC de la SGSICS, que inició una investigación con objeto de aclarar las circunstancias de la sustracción del dispositivo, recabándose para ello toda la información disponible acerca de los hechos ocurridos. "*Dada la dificultad de acreditar qué información contenían los dispositivos sustraídos, en el momento que se determinó que tenían datos personales se procede a comunicar con el DPD de la SES y con el responsable del tratamiento (RTR) de la DGCE. La comunicación de incidente de seguridad que podría constituir una "Brecha de Protección de Datos", fue trasladada al DPD de la SES, el 26/05/2022, a las 10.50 horas."*

"*Conforme a las instrucciones del RTR, la DGCE, al no estar clarificados varios extremos, el jueves día 26, se procede a pedir información a las ÁREAS (VGEF y SEAV) que podían ser las que gestionaban el o los tratamientos que han podido dar lugar a la brecha*". Esas áreas, "*de las que dependerían funcionalmente los tratamientos PDYRH, SISTEMA VioGén y FORMACION y ACTIVIDADES de cooperación educativa con Universidades*.

"*El mismo día 26, el responsable solicitó al DPD de la Secretaría de Estado para que, en el marco de sus funciones, valorase los hechos que se han puesto en su conocimiento y colaborase en la determinación de las posibles vulnerabilidades y mejoras a llevar a cabo para subsanar lo ocurrido y prevenir que se pudiera volver a materializar un peligro de ese tipo. En base a lo cual, requiere a todos los afectados para que, el lunes siguiente, día 30 mayo, se entrevisten con el mismo a tales efectos.*

Los jefes de área afectadas responden al requerimiento de información a través de comunicación con el DPD".

"*En correspondencia con la información trasladada por el Área VGEF, únicamente se desprende que el incidente no ha afectado a ningún tratamiento de dicha Área, si bien, la persona que ha causado el incidente estaba encuadrado en el "ÁREA DE FORMACIÓN Y ESTUDIOS"*, y "*De la información remitida por el Área SEAV, se puede valorar un resumen de la brecha y aplican desde el primer momento las primeras medidas para subsanar posibles vulnerabilidades e incrementar el nivel de seguridad del tratamient*o."

"*El responsable del Tratamiento, a través de este DPD, conforme a lo establecido legal y procedimentalmente, realiza una primera comunicación por brecha de seguridad de datos el mismo día 27 de mayo a las 14.06 horas*".

"*Los datos sustraídos que se trataban con la finalidad de desarrollar la herramienta citada, provenían de diligencias policiales y contenían datos básicos, imagen, documentos de identidad, sobre infracciones penales y condenas, datos de localización y datos de salud. A día de hoy, tras comprobar la documentación exacta*, **(…),** *cabe señalar que en la información sustraída no figuraban datos biométricos ni datos de menores."*

"…*la SES implementa en todos los ordenadores de sus usuarios (**…**), tanto portátiles como PC de sobremesa, esto es, el equipo cuenta con la solución **(…)** y la solución **XXX** del fabricante **XXXXXXX** denominada **XXXXX**. Los registros obtenidos de las consolas de ambas soluciones indican que las últimas comunicaciones establecidas por el equipo sustraído tuvieron lugar minutos antes de la hora en la que el usuario refiere que le fue sustraído el dispositivo el día **XX/XX**/2022, en el caso de **XXXXXXX** a las 19:39:17 horas y en el caso de **XXXXXX** a las 19:11:00 con el usuarios **XXXXX** logado, no volviéndose a registrar ninguna otra comunicación desde dicho momento hasta el día de hoy, lo que indica que quien hubiera sustraído el dispositivo no lo ha conectado a Internet desde entonces, dado que de otro modo los agentes instalados en el equipo de las soluciones de protección de **XXXXXX** mencionadas, hubieran enviado un reporte automáticamente a sendas consolas de administración*."

"*Indica que no existe constancia de que se haya materializado perjuicio alguno que afecte a los derechos de los interesados*" y que se "*han analizado todos los flujos de*

datos contenidos en los tratamientos referidos diseñándose un sistema basado en el incremento de las medidas de protección técnicas y organizativas en todas las actividades de tratamiento en relación con las personas implicadas en cada una de ellas y en la propia información que se maneja. Desarrollándose un sistema que no permite en ningún caso acceso a datos que no se encuentren totalmente anonimizados por parte del personal externo que desarrolle su labor en la DGCE".

Consideran que el tratamiento queda al amparo de la Ley Orgánica 7/2021, por lo que considera que: "*El responsable del tratamiento entiende que la comunicación a las personas interesadas debe omitirse al entender que comunicarla impediría que se llevasen a cabo las indagaciones e investigaciones policiales en curso, causaría un perjuicio grave a la seguridad pública y es necesaria para proteger los derechos y libertades de terceras personas*."

SEGUNDO: Actuaciones previas de investigación 11/07/2022.

Con fecha 11/07/2022, la Directora de la AEPD como consecuencia de la notificación de la brecha de datos personales comunicada, instó de la Subdirección General de Inspección de Datos a la realización de actuaciones previas de investigación para el esclarecimiento de los hechos en cuestión, en virtud de las funciones asignadas a las autoridades de control en el artículo 57.1 y de los poderes otorgados en el artículo 58.1 del Reglamento (UE) 2016/679 (Reglamento General de Protección de Datos, en adelante RGPD), y de conformidad con lo establecido en el Título VII, Capítulo I, Sección segunda, de la LOPDGDD, teniendo conocimiento de los siguientes extremos:

Con fecha 16/09/2022, se solicitó a la DGCE:

1-Procedimiento interno comunicación brechas de seguridad

En su escrito, indica la existencia de un procedimiento interno para la comunicación de brechas de seguridad (adaptado a la Ley Orgánica 7/2021) que aportaba como anexo I, al mismo, no localizándose dicho adjunto. Se solicita copia de este.

Con fecha 6/10/2022, respondió la Delegación de protección de Datos de la SES, acompañando diversos anexos de distintos órganos de la SES.

Aporta copia de "*protocolo interno para la gestión de brechas*", fecha de entrada en vigor 14/03/2022, con actualización a la LO 7/2021, figurando una versión anterior de 27/11/2020. En el mismo, se indica entre otros aspectos:

- "*Habrá que determinar si la brecha de seguridad detectada supone un riesgo para los derechos y libertades de los afectados. Este paso es clave, ya que marca la diferencia en cuanto a si se tiene que notificar el problema de seguridad a la AEPD o no. Para saber si el ataque supone un riesgo, habrá que analizar si entra en uno de los criterios y ejemplos recogidos en el considerando 75 del RGPD o en las Directrices 01/2021 del CEPD"*, sobre ejemplos de notificación de violaciones de la seguridad de los datos personales, adoptadas el 14/12/2021

- "*El responsable del tratamiento deberá establecer un registro en el cual se recojan el lugar, día y hora de detección de la violación de seguridad, así como también los sistemas, datos y equipos que se han visto afectados. Una vez resuelta la brecha se deberá también incluir en el citado registro la solución o los procedimientos establecidos para reparar o mitigar el problema de seguridad*."

- "*1. Cuando notificar: Tan pronto como el responsable del tratamiento tenga conocimiento de que se ha producido una brecha de datos personales debe efectuar la correspondiente notificación a la Autoridad de Control competente, cuando sea probable que la brecha constituya un riesgo para los derechos y libertades de las personas. En su caso, debe realizarse sin dilación y a más tardar en las 72 horas siguientes, computando también las horas trascurridas durante fines de semana y festivos*."

- "4. *Quién debe notificar: Cuando un responsable de tratamiento tenga la constancia de que una brecha de datos personales pueda suponer un riesgo para los derechos y libertades de las personas físicas, deberá notificar a la Agencia Española de Protección de datos*."

- "*La notificación de una brecha de datos personales a la autoridad de control le corresponde al responsable del tratamiento conforme al artículo 33 del RGPD, el artículo 39 de la LOPDP (LO 7/21)…"*

- "*El responsable informará necesariamente a su delegado de Protección de Datos el cual le podrá asesorar y auxiliar en el proceso*."

-También existe un apartado de "*comunicación a los afectados*", entre los que se anota: "*En el caso de tratamiento donde se aplique la Ley Orgánica 7/2021, de 26/05, la comunicación al interesado podrá aplazarse, limitarse u omitirse con sujeción a las condiciones y por los motivos previstos en su artículo*."

2-Copia del registro de incidentes actualizado documentando la violación de seguridad.

Aporta la copia del ANEXO II: archivo que, al abrirlo, titula: "*ampliación información sustracción portátil*", versión 3/10/2022 de la SGSICS, que tiene encomendada la gestión, administración y seguridad TIC de la infraestructura tecnológica con la que el Ministerio del Interior presta sus servicios. En este informe se responde también a otras cuestiones planteadas en otros párrafos requeridos por el Servicio de Inspección.

Se afirma que el día 6/05/2022, el CAU informó al ÁREA DE SEGURIDAD TIC DE LA SGSICS de la "*sustracción de un equipo portátil perteneciente al Ministerio del Interior, asignado al personal que presta sus servicios en la sede de la SES, en Calle* ******DIRECCIÓN.1****, de Madrid*.", y que iniciaron una investigación.

Indica que aporta como "*copia del registro de incidentes actualizado documentando la violación de seguridad*:"

 Doc.1.- Extracción del registro y seguimiento de la incidencia en el gestor de incidencias de esta Subdirección (herramienta de ticketing JIRA). No figura en este anexo II, sino que se halla dentro del Anexo IV (que contiene varios documentos de distintas procedencias) en este caso, remitido aparte por la misma SGSICS titulado "*Informe de*

seguridad sobre la sustracción de un ordenador portátil perteneciente Centro Nacional de Desaparecidos" y se trata de un e mail desde la SGSICS de 9/05/2022, 10: 48, indica: "*Asunto CAU 2019 se abre JIRA en Seguridad de sistemas debido a robo portátil HP*". Le precede otro del mismo día en el que igualmente envía la ampliación de la denuncia de 6/05/2022.

 Doc.2.- Extracción del registro de la incidencia en la herramienta de ***(…)***. No figura en este anexo II, ni se aprecia en ninguno de los enviados.

 Doc.3.- Extracción del registro de la incidencia en la herramienta de ***(…).*** No figura en este anexo II, ni se aprecia en ninguno de los enviados.

3-Relación de la persona física que disponía del portátil y el dispositivo USB sustraído (con la información de carácter personal), se solicita acreditación documental de su vinculación con la (DGCE), aportando copia de posibles convenios, contratos u otros instrumentos jurídicos existentes para la formalización de este personal externo encargado de tratamiento, así como los acuerdos de confidencialidad firmados.

Manifiesta que aporta copia de información facilitada por el ÁREA DEL SISTEMA ESTADÍSTICO Y ATENCIÓN A LAS VÍCTIMAS, (SEAV) en concreto en anexo "*contrato*" número expediente ***21***/027 que refiere:

-Copia de PLIEGO DE PRESCRIPCIONES TÉCNICAS "*para la contratación de investigación científica sobre la creación y validación de una herramienta predictiva y de valoración del riesgo de desaparición con desenlace fata*l", de 31/03/2021, (firma DGCE). Consiste (punto 1, objeto) en una *"revisión, lectura, vaciado de datos y análisis de información documentada en una muestra de 2000 atestados por desaparición de personas en diferentes puntos. El estudio de datos documentales de una muestra significativa de desapariciones (2000) seleccionada por los funcionarios emplazados en el XXXX a través del sistema* PDyRH *(personas desaparecidas y restos humanos sin identificar).*

Se explorará la potencial utilidad de las variables identificadas para crear:

a) un modelo de denuncia, recogida de información ante casos de desaparición estandarizado y con soporte empírico
b) una herramienta predictiva del escenario o tipo de desaparición más probable y de valoración de riesgo de desenlace fatal, y
c) una guía ejecutiva de la respuesta inicial de actuación policial basada en la evidencia."

Todo ello con la finalidad de validar la actual clasificación de escenarios de desapariciones, de identificar nuevos indicadores, y de avanzar en la capacidad predictiva". "*Todos los casos han de estar cerrados y esclarecidos policialmente e integrados en el Sistema de Personas Desaparecidas y Restos Humanos sin identificar (*PDyRH*). Supone como trabajo:*

a) La recopilación y estudio pormenorizado de toda la documentación policial, psicosocial y criminológica de cada caso.

b) La sistematización de la información recopilada en una base de datos creada a tal efecto, así como el análisis de los datos."

En "*equipo de trabajo"*, se indica que el adjudicatario contará necesariamente con un investigador principal.

En el punto 3: "*Por parte de la Secretaría de Estado de Seguridad – Dirección General de Coordinación y Estudios – Centro Nacional de Desaparecidos y Área de Estudios, se designará a un Coordinador del estudio, que mantendrá la interlocución que sea necesaria con el equipo de trabajo que designe la Institución adjudicataria a efectos de propiciar la máxima coordinación entre las tareas y actividades a desarrollar*."

"7. NORMAS DE SEGURIDAD Y CONTROL
Todo el personal que, por parte de la Institución adjudicataria, intervenga en los trabajos, deberá someterse a las normas de seguridad, control y régimen interior de los centros y dependencias policiales y penitenciarias en las que tengan que trabajar."

La cláusula 8.2: *"confidencialidad y protección de datos sobre los datos relacionados con la actividad de la Administración que haya de suministrarse".* Se indica que la adjudicataria*: "únicamente tratará los datos de carácter personal a los que tenga acceso conforme a las instrucciones de la Coordinación del estudio y no los aplicará a fin distinto".*

"*9. OBLIGACIONES DE LA ADMINISTRACIÓN*
• Facilitar la selección de los casos a revisar.
• Facilitar el acceso del personal investigador a la documentación policial de los implicados en los casos objeto de estudio.

• Facilitar el acceso del personal a todas las dependencias del Ministerio del Interior en donde tengan que trabajar, sin perjuicio del control debido por razones de seguridad.

El plazo de ejecución es de un máximo de 5 meses.

- Copia de *PLIEGO DE CLÁUSULAS Administrativas PARTICULARES, contrato de servicios "abierto simplificado", con referencia en el punto 27 a "seguridad y confidencialidad",* y en el 28 a *"tratamiento de datos personales" en la que se reconoce el acceso a casos en los que hay implicadas personas físicas en calidad de autores de delitos y víctimas.* Se indica que la entidad contratista tendrá la consideración de *"encargado del tratamiento"* y entre otras, que deberá *"aplicar medidas que garanticen la seguridad de los datos."*

"En la ejecución de las prestaciones del contrato se consideran los siguientes datos de carácter personal, responsabilidad de la entidad contratante, quien facilitará los datos que sean necesarios al contratista:

- Los datos de carácter personal seleccionados por la entidad contratante.

- Los datos de carácter personal que figuran en las diligencias policiales y los aportados en entrevistas a los propios agentes de las Fuerzas y Cuerpos de Seguridad.

- Los datos de carácter personal que se obtengan durante las entrevistas a víctimas y autores de delitos.

En todo caso:

- La entidad contratante tendrá la consideración de responsable del tratamiento.

- El contratista tendrá la consideración de encargado del tratamiento de estos datos y no se considerará que se produce comunicación de datos.

a) El encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento, no los aplicará o utilizará con fin distinto al que figure en dicho contrato, ni los comunicará, ni siquiera para su conservación, a otras personas. Manteniendo en todo momento la debida confidencialidad de los datos.

b) El encargado del tratamiento deberá adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.

c) Una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos al responsable del tratamiento, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento.

- En el caso de que el encargado del tratamiento destine los datos a otra finalidad, los comunique o los utilice incumpliendo las estipulaciones del contrato, será considerado también responsable del tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente

-En el punto 17, como condiciones medioambientales, se indica que: "*la prestación de servicios se realizará utilizando medios informáticos evitando el soporte físico papel excepto en casos imprescindibles*"

-copia de la formalización de contrato con Fundación de la Universidad Autónoma de Madrid, adjudicado el 23/06/2021.

-copia de factura expedida el 13/12/2021.

4- En relación con el desarrollo de la herramienta predictiva para la que era necesario los datos personales sustraídos, se solicita información sobre su funcionamiento, aportándose detalles de los tipos de datos personales que se necesita como entrada para entrenar los algoritmos, los que se necesitan para validación o prueba, así como detalles de la predicción que realiza y el uso que se haría de la misma, indicando también la existencia de elaboración de perfiles.

Manifiesta el escrito respuesta, que se adjunta información facilitada por el Área de Sistema Estadístico y Atención a las Victimas (SEAV) Anexo III. Este anexo, del XXXX, responde a varias de las cuestiones del requerimiento de la inspección, y figura firmada en 4/10/2022. Tras encuadrar su dependencia de la DGCE, que su creación fue por

Instrucción de 2/2018 de 5/02, y sus funciones, detalla que en 2019 puso en marcha un estudio "*para establecer métodos fiables y eficaces de valoración de riesgo, que permitan ayudar a los investigadores policiales a orientar las investigaciones desde el momento en que se recibe una denuncia por desaparición*." "*Con apoyo de personal universitario, previamente se creó un grupo de trabajo para determinar los factores que influyen en que una persona desaparezca, con el objetivo de llegar a la creación de una herramienta eficaz, que permita a los investigadores estimar el escenario más probable ante una nueva denuncia por desaparición, así como el tipo de desenlace más probable*."

El contrato de 2021 es una continuación de dicho trabajo. Refiere el apartado 11 de la "*memoria justificativa"* en la que se incluye el tratamiento de datos por parte del adjudicatario, se indica el acceso a datos relacionados con víctimas de delitos de desapariciones y autores de delitos.

Informa que el 1/07/2021 se adjudicó el contrato a la ***(…).***

Manifiesta que de conformidad con el apartado 5 del Pliego de prescripciones técnicas, para la contratación del servicio se preveía personal investigador, y la Universidad *contrató a* D. ***A.A.A.*** (INVESTIGADOR COLABORADOR IC en lo sucesivo) y a ***B.B.B.*** (***XX*** en lo sucesivo) para dirigir el trabajo en las instalaciones del XXXX. También se menciona la confidencialidad y la protección de datos en los que hayan de suministrarse al adjudicatario para la realización de los servicios convenidos, extensible a los colaboradores del adjudicatario, que suscribirán el compromiso de confidencialidad.

La Fundación procedió a la contratación del equipo de trabajo para el desarrollo de dicha herramienta.

"*Los documentos necesarios por el equipo de investigación para el estudio y desarrollo del contrato objeto de licitación, fueron requeridos a las Fuerzas y Cuerpos de Seguridad (FCS) por el XXXX, siendo remitidos al email oficial creado al efecto* ******EMAIL.1****, cuenta securizada y gestionada por la SGSICS." El uso de este correo se encuadra, por las finalidades a las que se dedica, dentro de la Sección de normativa y estudios del XXXX, al que solamente tiene acceso su jefe. Recepcionados los documentos, éstos eran almacenados en la* ***"XXXXX"*** *oficial securizada de la SGSICS, denominada* ***XXXXXX****. "El funcionamiento de este espacio, está securizado, y el acceso* ***(…)***."

"*El procedimiento para visualizar los documentos era como a continuación se explica:*

Cuando el equipo de investigación requería de alguna documentación, el ***XXXXXXXXX*** *en un equipo de sobremesa (PC) de la sala dispuesta para el desarrollo del trabajo en la sede del* ***XXXXX****, accedía a la nube y únicamente se les mostraban los documentos necesarios para el estudio que demandaban diariamente, volviendo a cerrar la nube y dejándoles la documentación para su análisis y estudio. Los equipos informáticos que utilizaba el equipo de investigación eran los proporcionados por la* ***XXXX*** *con las medidas de acceso de seguridad establecidas. Es de significar que para* ***(…)****, gestionados y securizados por* ***la SGSICS****. Los terminales informáticos utilizados para el acceso a* ***XXXXXXX****, por el equipo de investigación, eran del tipo de* ***(…)*** *propiedad de la Secretaría de Estado de Seguridad, gestionados y controlados por la* ***XXXXX***.

Una de las cláusulas del contrato del *pliego de prescripciones técnicas,* 8.2.2., indica que la adjudicataria deberá garantizar el cumplimiento de los requisitos establecidos por la normativa de protección de datos personales, en relación con los datos de carácter personal a los que vaya a tener acceso*:*

 "*Únicamente tratará los datos de carácter personal a los que tenga acceso conforme a las instrucciones de la Coordinación del estudio, y no los aplicará o utilizará con fin distinto. "*

El 13/12/2021, la ***(…)***, da por finalizado el contrato, haciendo entrega del trabajo realizado por el equipo de investigación multidisciplinar, no teniendo el XXXX, a partir de esa fecha, más relación de negocio jurídico con la *Fundación* ni con los investigadores del equipo de trabajo. Se emitió en su día (13/12/2021) la factura.

"*La herramienta predictiva resultante (aplicación) está implementándose en el Sistema PDyRH, como apoyo para la toma de decisiones de los investigadores".*

"*Por informaciones posteriores recibidas, que fueron recogidas en el primer informe al DPD de la SES mencionado, se informaba que se había podido conocer que por el anterior **(…)**, Estudios y Formación (**…**), se permitió la extracción y alojamiento de documentos en un portátil oficial, sin conocimiento de los funcionarios que habían participado en el proceso de creación de la herramienta predictiva. Estos extremos no fueron conocidos por los responsables del XXXX hasta el día posterior a la sustracción de la mochila en la que, entre otros efectos, se encontraba el ordenador portátil adjudicado a dicho responsable, en el que en ese momento tuvieron noticias de que el **XXXXXXXX**, D. **XX**, había almacenado información en dicho ordenador portátil, propiedad de la SES, que utilizaba –según sus propias manifestaciones– para otros usos particulares, y que sacaba de las instalaciones sin ningún control, y que lo llevaba haciendo desde fechas sin determinar. Todo ello, igualmente, era desconocido por los responsables del XXXX*."

5-Copia del REGISTRO DE OPERACIONES del sistema de información que trata los datos personales (según lo especificado en el art. 33 de la Ley Orgánica 7/2021).

En concreto, el registro de aquellas operaciones relacionadas con la consulta y comunicación de los datos personales a la persona encargada de tratamiento, víctima de los dispositivos sustraídos.

La Delegación de protección de datos señala en su respuesta:

"*La información específica que ha producido el incidente de seguridad y la brecha de protección de datos personales no se extrajo de un sistema de información y por lo tanto no se pueden aportar registros desde el sistema **XXXXX** o cualquier otro". Se aporta información en el anexo XXX sobre la extracción primaria de los datos, si bien, se desconoce cuál fue el proceso organizativo o técnico por el que los datos acabaron en poder de la persona que sufrió la sustracción. A día de hoy, el registro de operaciones como tal no se ha implementado en los sistemas de información en su totalidad. Sí se acreditan las dimensiones de seguridad más la autenticación y la trazabilidad, si bien, no se incorpora aún en los registros automatizados la inclusión de la justificación, nombre de*

la persona o la identidad de los destinatarios para las operaciones indicadas en el artículo 33 de la LOPDP (recogida, alteración, consulta, comunicación, incluidas las transferencias, y combinación o supresión). "
Hay que señalar que tal anexo XXX no figura.

-Amplía la información en el ya citado Informe de 3/10/2022 de la SGSICS **XXXXXXX**, que indica:

"*Según comunicó a esta Subdirección, el personal interlocutor del XXXX, el disco duro del ordenador portátil sustraído contenía una extracción de PDyRH del año 2019 (base de datos) de la que en esta Subdirección no se tiene ninguna constancia acerca de su existencia ni origen.*

"*Sin embargo, acerca de esta extracción se hace necesario realizar las siguientes aclaraciones: El sistema PDyRH recoge los datos de los cadáveres y restos humanos sin identificar investigados por las Fuerzas y Cuerpos de Seguridad españoles, así como todas las denuncias de personas desaparecidas, información con la que el sistema posteriormente realiza una comparativa. En caso de hallar alguna coincidencia se comunica a los Cuerpos implicados y se inicia un protocolo de colaboración. El sistema cuenta con tres entornos: Producción con seis servidores de aplicaciones y dos servidores de base de datos,* ***XXXXXXX*** *con* ***XXXXXXXXX*** *de aplicaciones y* ***XXXXXXXXX*** *de base de datos y* ***XXXXXXX****, con* ***XXXXXX*** *dedicado al proyecto. La información que se almacena en el sistema PDyRH es la obtenida a través de los campos habilitados en la aplicación, que se extrae de los atestados policiales de forma automatizada o manual en el caso de que el sistema policial no se encuentre integrado con el sistema PDyRH. Los atestados en ningún caso se encuentran ni en los servidores de aplicaciones de PDyRH ni en base de datos. De este modo en el sistema PDyRH únicamente existen campos con datos de la denuncia e información estructurada que complementa y se cruza para su comparación, permaneciendo almacenados los atestados en los sistemas policiales correspondientes".*

Afirman que la SGSICS tiene la siguiente responsabilidad con respecto a este sistema PDyRH:

1. Definición del modelo de datos, desarrollo y mantenimiento del sistema.
2. Habilitación de accesos a usuarios de Fuerzas y Cuerpos de Seguridad.
3. Gestión de incidencias.

Menciona los distintos Cuerpos y Fuerzas de Seguridad del Estado que tienen acceso a dicha aplicación, y, "*además, a base de datos, el personal autorizado del XXXX, responsable del tratamiento de datos*."

Los usuarios se conectan a la aplicación a través de una red dedicada y segura, denominada "*Red Policial*" (red administrada por la SGSICS)".

En la SGSICS no consta que se haya dirigido petición en ningún momento por parte del responsable del tratamiento, solicitando una extracción de datos de la aplicación ni de la base de datos de PDyRH que pudiera corresponder con la información contenida en el dispositivo sustraído.

Tampoco se tiene constancia, ni ninguna evidencia o alerta de que este sistema informático, haya sufrido ninguna brecha de seguridad.

Para lo cual se adjuntan los logs de la aplicación y de la BBDD del 21 al 30/11/2021 y se pone a disposición el resto de los logs almacenados para cualquier consulta que se estime oportuna.

Por otra parte, debe reseñarse que el día 30/11/2021, desde esta Subdirección fue atendida una petición formulada por el jefe de Área de Estudios, Área de Violencia de Género, Estudios y Formación de la Dirección General de Coordinación y Estudios, referida a la extracción de atestados policiales del sistema *VioGén* y no, así como consta en la información facilitada por el interlocutor de XXXX, relativa a PDyRH, siendo atendida, al proceder del departamento del responsable de los datos.

Dado que la información solicitada no radicaba en base de datos del sistema, si no que en la base de datos solo figuran apuntes a las rutas donde se alojan el resto documentos, las operaciones realizadas fueron las siguientes:

Con fecha 26/11/2021, se solicitó por el área responsable del Sistema *VioGén*, personalmente y por correo electrónico a través del jefe de Área de Estudios y Formación, autorizado previamente por quien en el correo se nombra como "***XX***", copia de los atestados policiales del año 2019. Esto se recoge del hilo de correo electrónico que figura como evidencia 10 del informe original de este incidente. Se incluye como ANEXO II.

"*Dado el volumen de atestados a recuperar, 62.409, varios de ellos dañados y ante la imposibilidad de extraerlos directamente desde la propia aplicación VioGén (entorno web) desde SGSICS se les ofreció la posibilidad de realizar la extracción de dichos atestados directamente desde el servidor"* y *"extraer los ficheros seleccionados mediante herramienta SFTP*". "*Está operativa no dejaba auditoría en la aplicación web VioGén*." "*Para constancia y comprobación, como Doc. 4 se adjunta registro de auditoría de la fecha en la que se realizó la extracción*." Indica que "*lo que se registra en la auditoría de la aplicación es:*

Listado de denuncias y hechos asociados a cada denuncia, con información de "identificación de víctima y autor del caso, y consulta de ficha de denuncia, -no del fichero con el atestado -aunque puede estar presente enlace a dicho fichero si lo tuviera para ser descargado sin constar que lo haga en su caso."

"*Tras realizarse la extracción fue entregada en mano en las instalaciones de la SGSICS en El Pardo, al jefe de Área de Estudios y Formación el 30/11/2021*." conteniendo los atestados referidos en el documento anexo referenciado como Doc. 5.

No se recibe ni el documento 4, ni el 5 que aparece citado.

-Por su parte, en ANEXO III, procedente del XXXX de 4/10/2022, se responde, entre otros puntos, a este, no con lo que se le cuestiona sino con referencia al registro de actividades del tratamiento, reiterando que la actividad de tratamiento afectada por el robo del portátil del Ministerio del Interior es la actividad "*Sistema de Personas Desaparecidas y Restos*

Humanos Sin Identificar" (PDyRH), y reitera el contenido del mismo que ya figuraba en el informe de la DGCE que acompaña a la segunda notificación de la brecha.

Manifiesta que "*No obstante, ha quedado constatado que en el portátil no solo existía información personal extraída del sistema PDyRH (donde se almacenan datos de personas desaparecidas y restos humanos* sin identificar junto a las denuncias de desaparición que llegan a las FCSE), sino que también existía otra información sensible de carácter policial, como atestados policiales de desapariciones y homicidios ya esclarecidos, audios y videos de testimonios familiares, víctimas, agresores y otro material policial relacionado con las investigaciones. Para dar soporte al tratamiento de esta información para la realización de estudios científicos han procedido a actualizar el RAT, a fecha 12/09/2022, incluyendo la nueva actividad denominada SES-ESTUDIOS, detallando su estructura.

6- En relación con la investigación interna que se realizó sobre el incidente, se solicita:

o Copia de la documentación existente en la denuncia que formuló la persona víctima de la sustracción (tanto al Área de la que dependía como al CAU en los días 4 y 6/05/2022.
o Copia de la documentación obtenida por el Área de Infraestructuras y Seguridad TIC (de la SGSICS) en el transcurso de la investigación del incidente (que inició tras los nuevos datos aportados por la víctima el día 6/05/2022).
o Copia de la documentación remitida por las Áreas que gestionaban los posibles tratamientos que dieron lugar a la brecha (Áreas VGEF y SEAV), tras la solicitud realizada el 26/05/2022 con carácter de urgencia y siguiendo las instrucciones del Director General de Coordinación y Estudios.

Responde que se adjunta en ANEXO IV, que contiene diversos documentos, una parte realizada por la SGSICS, que aporta:

-Copia que acredita la primera denuncia interpuesta por el usuario ante la Policía Nacional el 4/05/2022. En la misma se indica "*que el dicente pertenece al Ministerio de Interior-Centro Nacional de Desaparecidos*", que entre los efectos que contenía la mochila, había unas carpetas con el logo del "*XXXX*" conteniendo información de terceras personas de carácter policial", "*reseña que el ordenador tiene clave de acceso y contenía archivos con información confidencial*", que no puede aportar el número de serie del ordenador pero que realizará una ampliación para aportar más datos.

-En la denuncia de ampliación del 6/05/2022, proporciona los datos de identificación de marca y modelo del ordenador y número de serie, añade como objetos, un pendrive de color amarillo, indicando que "*el ordenador no dispone de clave de acceso como manifestó en un primer momento por lo que cualquier persona podría tener acceso a la información*".

Acompaña la SGSICS un "*Informe de seguridad sobre la sustracción de un ordenador portátil perteneciente Centro Nacional de Desaparecidos*" enlazando con el ANEXO II referido en el punto SEGUNDO, si bien este ANEXO 4 es más amplio, aunque carece de fecha

Indica que el equipo portátil del Ministerio de Interior estaba asignado al personal que presta sus servicios en la sede de la SES, ******DIRECCIÓN.1*** de Madrid y que de la investigación iniciada a partir del día 6/05/2022, el portátil se encontraba en poder de ***XX***,

persona que desarrollaba proyectos en el XXXX, describe, marca, modelo y núm. de serie, y que "*no disponía de clave de acceso por lo que cualquier persona podía acceder a la información*.", disco duro de 500 GB y memoria RAM de 8 GB, e identificación del hostname-nombre por el que se identifica al equipo- y tenía configurado el usuario "***XXXXX***" con privilegios de administrador y "*cuya cuenta carecía de contraseña*", tampoco existía contraseña de arranque BIOS (que hubiera impedido ser iniciado por cualquier persona que no conociera dichas credenciales). El disco duro de 500GB no se encontraba cifrado, "*por lo que el acceso a la información contenida es completamente libre con solamente encender el dispositivo*".

Afirman que el equipo fue adjudicado inicialmente por la SGSICS (el 29/11/2018) a D. ***C.C.C.*** (***XX*** en lo sucesivo) que, era en aquel momento, jefe de ***(…)*** -de la DGCE, pero que en el momento del robo ya no prestaba los servicios en el departamento. Posteriormente, el 2/12/2019, el ordenador fue remaquetado por el departamento de Atención a Puestos de Usuarios de la SGSICS, sin que exista ningún otro registro relativo a nueva adjudicación ni intervención sobre el ordenador sustraído hasta la fecha.

"*Según informan desde el XXXX, el equipo se encontraba bajo la responsabilidad de otro Facultativo de Policía Nacional del Área* ***XXXXX".*** (al que identifican con nombre y apellidos- y que resulta ser el actual jefe de ***XXXXXXXX***).

Afirman que el equipo sustraído formaba parte de una partida inicial de 6 portátiles solicitados en el año 2017 para unas actividades internas de formación que requerían disponer de portátiles con el usuario administrador habilitado y sin credenciales y, que fueron entregados para ser utilizados exclusivamente en el interior de la sede. Que posteriormente fue asignado al jefe de Área de VGEF en fecha 29/11/2018, pero que en cualquier caso estaba destinado a su uso interior de las dependencias del Área. En el sistema gestor de incidencias de la SGSICS figura un registro introducido por parte del CAU al respecto, que reza:

"*Recibidos los equipos. Una vez terminado el curso quedan 5 portátiles en el armario esperando su recogida. Siguiendo indicaciones de* ***XXXXX,*** *un portátil se le ha asignado al* ***C.C.C..*** "*Abro otra mantis con este hecho****.*** Saludos***, XXXXX."***

"*El propósito y utilización del ordenador portátil era el desarrollo de tareas de investigación científica y de una herramienta predictiva desde 2018, tareas que eran desempeñadas por* ***XX*** *bajo la supervisión del personal del XXXX, "sin persona concreta bajo cuya responsabilidad desarrollara estas tareas*."

Afirman que en la SGSICS-***XXXXX***, no constaba la existencia de autorización para sacar el ordenador de la sede y que el propio usuario D. ***XX*** había afirmado que no tenía conocimiento de que esto no se podía hacer, y que no recuerda si cuando se incorporó en 2017 le dijeron que no podía sacarlo de la sede.

Manifiestan que "*Según consta por la documentación firmada por* ***XX****, en el equipo sustraído existía un usuario configurado de acceso a la red Wifi SES****XXXXXX WLAN_****XXXX****, destinada a cubrir la necesidad de acceso a Internet a través de dispositivos inalámbricos de los usuarios que trabajan en la sede de la SES "****XXXXXX***", donde se ubica el Centro Nacional de Desaparecidos. Aporta copia en evidencia 8 firmada el 24/06/2021, si bien no se contiene referencia alguna al equipo para el que se

solicita. También se asocian las "*normas específicas de seguridad de la información en el uso de la red wifi SES**XXXXXX** en el ámbito de la SES*" en la que se indica que "*está destinada al servicio de personal del Gabinete de Coordinación y estudios para la Seguridad en su sede de **XXXXXXXX** y su acceso está restringido a los usuarios que desempeñen sus funciones en dicha sede*. *Puntualmente, los usuarios ajenos a la SES podrán ser habilitados para hacer uso de esta conexión, siempre que las necesidades de su trabajo o función lo requieran*".

A través de la aplicación ***XXX*** -open web Access- haciendo uso de la conexión a Internet, accedía al buzón de correo ******EMAIL.1***, que era compartido con otros usuarios de semejante perfil al suyo dentro del XXXX. Se ha procedido a deshabilitar el usuario de acceso a la citada web.

Se afirma que el ordenador sustraído no tenía acceso al dominio de la SES donde podía existir información sensible, ya que esto sólo se podía hacer desde ***(…)*** a los que se le aplicaban políticas de seguridad específicas como el bloqueo de puestos USB

Se afirma que en la SGSICS no tienen constancia del modo en que la información contenida en el equipo sustraído fue proporcionada al usuario, afirmando que corresponde al funcionario responsable del propio usuario el control de sus funciones y de la información que se le proporciona. También afirman que en ningún momento se les solicitó desde la XXXX ni de la persona adjudicataria del ordenador, medidas para la protección de la información ni del dispositivo en su traslado o uso de información de carácter policial o conteniendo datos de carácter personal fuera de las dependencias de SES.

La SGSICS afirma que el usuario D. ***XX*** no aparece registrado en las aplicaciones corporativas de gestión de usuarios del Ministerio del Interior ("***…***") y por tanto no cuenta con un usuario individualizado y unívoco de los dominios de la Secretaría de Estado, donde pudiera existir información sensible. *Afirman que este es el motivo por el que no existe un documento firmado por el usuario o por su responsable asignado*, informándole sobre la normativa de buenas prácticas aplicables a su puesto de trabajo. Aunque afirman que *sí existe documento de Acuerdo de Confidencialidad por parte del XXXX* firmado por el usuario con fecha 14/12/2017, aportan un escrito (evidencia 7), con la mención en una sola hoja, logo de la SES, de "*4. protocolo de firma: "he leído el acuerdo relativo a la política de confidencialidad de la Subdirección, y acepto su contenido en los términos aquí expresados*" sin que figuren estos, sin conocer los términos. Indica que desde la SGSICS no se tenía constancia de ello (se les envió por el XXXX por e mail el 17/05/2022).

Desde la SGISCS se afirma que, según manifestaciones obtenidas por parte de los responsables del XXXX y del propio D. ***XX*** , *este usuario no tiene en la actualidad relación contractual con el Ministerio del Interior*, *sino que realiza tareas de desarrollo de una herramienta predictiva como parte de un proyecto de **XXXXXXXX** del Instituto de **(…)*,** (al que pertenece el usuario) y que si bien existe convenio general de formación entre UAM y SES, no se tiene constancia de que pudiera estar trabajando bajo el amparo del citado convenio a través de la formalización de un acuerdo o cláusula de colaboración. No obstante, con la información que dispone el departamento de atención a puestos de usuario de la SGSICS, la SES contrató el 11/06/2019 con la UAM la revisión y

análisis de casos de desaparición de etiología violenta, y posteriormente, con fecha 23/06/2021, la contratación con la ***XXXXXXX*** de la UAM para la creación y validación de una herramienta predictiva y de valoración de riesgo de desaparición con desenlace fatal.

En relación con la *información comprometida* con el portátil se afirma que, según manifiestan los propios responsables del XXXX, la información contenida en el disco duro era la siguiente:

1. 1140 atestados policiales esclarecidos sobre desapariciones de distinta etología utilizados para ***XXXXXXXXX.***
2. 800 atestados policiales esclarecidos sobre desapariciones utilizados para ***XXXXXXXXX.***
3. 60 atestados policiales esclarecidos sobre homicidios con diligencias de investigación de la Policía Judicial e inspecciones oculares técnico policial.
4. Entrevistas grabadas con agentes de la Policía Judicial, familiares y entorno cercano de víctimas y agresores, así como videos grabados con estos últimos en prisión.
5. Extracción de la base de datos de *PDyRH* del año ***XXXX***.
6. Base de datos utilizada para la elaboración del trabajo: "***XXXXXXXXX*** *de casos*".
7. Base de datos utilizadas para la elaboración del trabajo publicado: "***(…)*****".**
8. Bases de datos utilizada la construcción del ***XXXXXXXXX,*** e informe técnico sobre su construcción.

Según manifestación de D. ***XX***, entre los dispositivos de almacenamiento sustraídos había uno de ellos "*etiquetado con CEPOL que contenía información personal*". "*Otro de los pendrives estaba corrupto y era inaccesible. El resto de los pendrives, según el usuario, estaban vacío*s". En las carpetas amarillas que también fueron sustraídas con documentación en papel, según primeras manifestaciones del usuario, contenía información policial, no obstante, estas manifestaciones fueron corregidas posteriormente en la segunda denuncia afirmándose que contenían facturas a nombre de ***XXX*** relativas a los viajes en el marco del proyecto en el que trabajaba y no información sensible de carácter policial.

La propia SGSICS afirma que, tras la investigación interna realizada, se concluye con la existencia de varias deficiencias que surgieron tanto a nivel técnico como operacional y organizativo, en concreto afirman textualmente las siguientes:

A nivel organizativo afirman que:

1. No consta la designación de un funcionario responsable directo de D. ***XX*** como usuario externo que desempeñaba su trabajo en el XXXX,

2. No consta que se informara al usuario de la normativa que aplica a su puesto de trabajo, de las acciones que está autorizado a llevar a cabo y de las que no está autorizado a realizar con los medios y recursos que se ponían a su disposición. Tampoco consta la aceptación y conocimiento del usuario de dichas normas, cumplimentando el protocolo de firma y ratificado por su responsable en la SES.

A nivel operacional:

1. No consta cómo, por quien, y bajo que precepto le fue entregada al usuario la información contenida en el dispositivo sustraído.

2. Se permitió la salida de dispositivos en los que se contiene información de nivel alto o incluso crítico, y máxime cuando el dispositivo que la contiene carecía de medidas de protección básicas o elementales que la hiciera inaccesible por personal no autorizado.

3. El usuario permaneció en un establecimiento público con un dispositivo con información confidencial y sin adoptar unas medidas de vigilancia adecuadas.

A nivel técnico:

1. Los usuarios configurados en el equipo sustraído eran el usuario "***XXXXXXXX***" y el usuario "***XXXXX***" que contaba con privilegios de administración y que carecía de contraseña de acceso. El dispositivo carecía de medidas de protección pasiva como la contraseña en la BIOS, el cifrado del disco duro o la existencia de particiones de disco protegidas por cifrado.

2. Además del propio usuario al que le fue sustraído el ordenador, existían, según información de atención puestos a usuarios, un total de tres usuarios genéricos (Becarios 1, 2 y 3 respectivamente) con acceso a recursos del dominio **XXX**-mir.es y compartiendo buzón de correo ******EMAIL.1***, lo que no permite la trazabilidad de las acciones.

3. Entiende se ha de comunicar a la AEPD.

Por parte de la SGSICS, se adjunta las siguientes evidencias:

-Copia del documento interno, evidencia 3 "*Movimiento de Material*" del CAU que acredita la asignación del portátil el 29/11/2018, por "*fallo del que tenía asignado*". Sobre la configuración del mismo no figura ninguna anotación.

-Evidencia 4: "*histórico actuación sobre equipo sustraíd*o", de 2017 a 2019. Se aprecia que se configuró por primera vez en 2017, y se volvió a plataformar en 2019.

-Evidencia 5: "*remaquetación del equipo sustraído*", figurando *"usuario del equipo con privilegios de administrador*",

-Evidencia 6, con cuatro anotaciones, del 13 al 20/12/2017, una de ellas "*ticket de configuración usuario* ***XXXXXXXX*** *con permisos administrador y sin contraseña en cada portátil", del 13, y figurado en la última "recibidos los equipos, una vez terminado el curso quedan 5 equipos en el armario del despacho de* ***XXXXXX****, esperando su recogida. Siguiendo indicaciones de P…, un portátil se le ha asignado al* ***XXXXXXX****.*"

Como evidencia 9, "*consolas de* ***XXXXXXXXX***", aporta captura de pantallas de registros "***(…)***" en las que se ve el día 4/05/2022 que la última conexión figura antes de producirse la suspensión, sin que haya habido ninguna con posterioridad.

Como evidencia número 10, captura de pantalla con el correo electrónico enviado por D. ***XX*** (jefe de ***(…),*** dirección c/ ******DIRECCIÓN.2***)" el viernes 26/11/2021 con el contenido

siguiente relacionado con el traspaso de la información contenida en el portátil robado en mayo 2023:

“Hola equipo.

*Esta mañana hemos tenido reunión con SAS y con una universidad en VioGén (como ya sabíais) y **XX** ha dado luz verde a hacer estos estudios de atestados y de casos del 2019. Os he llamado a todos, pero no me cogéis. ¿Qué tal os viene que me pase el lunes por la mañana a partir de las 10:00 h. para hacer las extracciones de datos? Me acompañaría el becario de la **XXXXXXXX** que las va a procesar, para llevárselas en un portátil, que nos corre algo de prisa. Sería recuperar la extracción de todos los casos del 2019 a un año de seguimiento (y ya veríamos si de paso llevarnos las del 2020, ahora que estamos casi a final de año) y los atestados que se puedan sacar (si son 40.000 mejor).*

-Refiere medidas y acciones “*encaminadas a mejorar las medidas de seguridad preventivas” por parte del área de estudios de violencia de género, como encargada de los alumnos en prácticas, centralizando la gestión del personal alumno, con listados para incrementar el control, revisión de los convenios actualizados, gestión del uso físico de los espacios de las salas comunes de trabajo y asignación de un tutor responsable, revisión y mejora de cláusulas de confidencialidad del personal que accede a datos con una guía de comportamientos específicos y buenas prácticas, guías para el uso de los recursos (aportan copia de la cláusula, de las buenas prácticas) . Revisión periódica de las actuaciones*

“*Significar, que, el transcurso del tiempo desde la notificación de la sustracción hasta la remisión de este informe ha sido el tiempo necesario para aclarar e identificar el alcance del incidente y la información sensible que ha podido ser expuesta*”

En el mismo **XXXXXXXX**, que contiene diversa documentación, se aporta informe del responsable del SISTEMA ESTADÍSTICA Y ATENCIÓN A VICTIMAS, (SEAV) al DPD, fechado el 27/05/2022.

En este informe, el jefe del Área SEAV afirma que en cuanto tuvo constancia de lo sucedido, lo puso en conocimiento del propio director de la DGCE mediante el envío de correo electrónico en fecha 5/05/2022 a las 14:25. Este hecho queda acreditado con la aportación de la captura de pantalla del propio correo electrónico del responsable del ***(…),*** que contenía el siguiente texto (con copia a tres personas):

“A.A.A., buenos días:

*... Ayer por la tarde le sustrajeron al **XXXXXXX … (XXXX**) su mochila en el interior de un bar de Madrid. Interpuso denuncia…En el interior de la mochila portaba …el ordenador HP del trabajo facilitado por la SGSICS, si bien, al no ser personal del Ministerio, no tenía clave asignada en su usuario (si en la parte del administrador), así como documentación del **XXXX** en papel y en Pendrives. Tanto la información contenida en soporte físico como digital está relacionada con el trabajo que ha estado realizando estos últimos años sobre la herramienta predictiva del riesgo, incluidos atestados policiales.*
Estamos en contacto con la SGSICS para dar de alta la incidencia del ordenador…el asunto lo estamos gestionando conjuntamente con Estudios del Área de Violencia de

Género, Estudios y Formación para, entre otras cosas, revisar y mejorar los procedimientos de seguridad que debe utilizar el personal de la Universidad que trabaja con nosotros. Te seguiré informando, si hay alguna otra novedad al respecto. Se indica expresamente que

- A esta SGSICS, el mismo día 5/05, se le participó verbalmente quedando la referencia en el aplicativo informático.

-El ***XXXX*** emitió el 10/05/22 un informe dirigido al responsable del fichero ***XXXXXX*** sobre la sustracción con documentación sensible a un ***XXXXXXXXXX.***

En el informe se afirma que hasta el día 5/05/2022, se desconocía, tanto por parte del jefe de Área SEAV como del jefe de Servicio del ***XXXX***, que el ***XXXXXXXXXX*** de la UAM que desarrollaba trabajos para el ***XXXX*** hacía uso de un portátil oficial no solo para los trabajos del área relacionados con estudios tutelados por el Área VGEF, sino también para su uso personal y privativo.

En el informe se afirma que los datos que se encontraban en el portátil eran 2000 atestados sobre personas desaparecidas con desenlace fatal de distintos Cuerpos de Seguridad y de casos ya juzgados. En concreto, se afirma que el portátil contenía, según las indagaciones del XXXX:

- Atestados policiales sobre desapariciones de personas esclarecidas tanto de Policía Nacional y Guardia Civil como de las Policías Autonómicas Mossos d'Esquadra y Policía Foral de Navarra. También contenía bases de datos en las que se encontraba almacenada la información de los atestados anteriormente referidos.

- Atestados policiales sobre homicidios esclarecidos policial y judicialmente y asociados a una denuncia por desaparición, tanto de Policía Nacional como de Guardia Civil. También contenía bases de datos en las que se encontraba grabada la información de los atestados anteriormente referidos, así como grabaciones de entrevistas en audio y video con los implicados en los casos (víctimas, agresores o familiares de estos entre otros aspectos).

- Bases de datos, extracciones anuales de *PDyR*H, manuscritos de trabajos de investigación, memorias justificativas de proyectos, cuadros de justificación de gastos, y otros aspectos de administración y control.

En el informe se afirma que los datos personales afectados pertenecían a sujetos sobre los que se denunció su desaparición y tuvieron desenlace fatal, sobre los autores condenados e ingresados en prisión, y sobre familiares y otras personas de su entorno, desconociéndose el alcance del número de personas afectadas puesto que no se contaba con respaldo del contenido del portátil.

En relación con las consecuencias estimadas, se afirma que en caso de acceder a la información contenida en el ordenador por personas que puedan interpretar el contenido de la información, las consecuencias serían impredecibles, puesto que algunos de los atestados que se conocen, por las propias declaraciones de D. ***XX*** son de casos muy mediáticos (pero ya juzgados).

El jefe del Área SEAV afirma que la cronología de los hechos fue la siguiente:

-El 4/05/2022 se produjo la sustracción del portátil propiedad de la SES (SGSICS) que estaba asignado por el Área VGEF al ***XXXXXXXX*** D***. XX***. A las 22:54 horas, este mismo ***XXXXXXX*** interpuso denuncia ante Policía Nacional.

-"*el 26/05/2022 se recibió en las áreas VGEF y SEAV un correo por parte del DPD de la SES solicitando la redacción de informe sobre lo sucedido y les adjuntaba el informe ya redactado por parte de la SGSICS a raíz de su investigación interna*". En relación con este correo se responde por parte del área SEAV con las siguientes imprecisiones que habían detectado en el informe adjuntado y que había redactado la SGSICS:

- Que el portátil no estaba asignado al ***XXXX*** tal y como se afirmaba por parte de la SGSICS, ya que no fue hasta el 5/05/2022 cuando se tuvo constancia en esta área que el ***XXXXXXX*** tenía asignado portátil oficial con información policial.

- Que el portátil estaba asignado a D. ***C.C.C.***, componente del área de ***(…)***, el cual causó baja en la DGCE mediante resolución de fecha de 1/02/2022 sin que la SGSICS hiciera nada con los dispositivos que esta persona tenía asignados, y que las medidas no han de ser solicitadas por los usuarios sino de oficio por los responsables de la seguridad informatica SGSICS

- Que la labor de supervisión del trabajo del ***XXXXX*** D. ***XX*** compete en exclusiva al área VGEF, al igual que para cualquier otro personal de universidades.

- En el informe se afirma que la actividad de D. ***XX*** en la SES se puede sintetizar:

-Lleva colaborando con VGEF y SEAV desde 2017 y debido a sus capacidades y cualificaciones se decidió que su tesis doctoral versara sobre la mencionada herramienta predictiva del riesgo que ayudara a los investigadores en los casos de desapariciones, estando a la supervisión de D. ***XX*** hasta su fecha de cese.

-El 11/06/2019 se contrató con ***XXXX*** para realizar revisión pormenorizada de casos de desaparición de etiología violenta en España, trabajo que recopilaba atestados y entrevistas con agentes, entorno de la víctima y agresor.

-El 23/06/2021, se licitó "*contrato para la creación y validación de una herramienta predictiva y valoración del riesgo de desaparición con desenlace fatal*". Este contrato se adjudicó a la ***XXXX*** en julio de 2021, con una duración de 6 meses, finalizándose los servicios en diciembre de 2021.

-Que posteriormente, D. ***XX*** ha continuado desarrollando trabajos para el XXXX, como ejemplo se afirma que en ***XXXXXXXX*** representó al XXXX en la conferencia de ***XXXXX*** "***(…)***", y asiste a ponencias de formación.

-Por parte del área SEAV se afirma que los documentos necesarios para el equipo de investigación fueron solicitados desde el XXXX a las Fuerzas de Seguridad siendo remitidos al email oficial creado al efecto y al que según afirman tenía acceso exclusivamente el jefe del XXXX (******EMAIL.2***). No obstante, según afirmación de la

SGSICS, el usuario D***. XX*** también tenía acceso a este buzón de correo y era compartido por otros usuarios de semejante perfil.

-Por parte del área SEAV, se afirma que el 13/12/2021, la XXXX dio por finalizado el contrato haciendo entrega del trabajo. Afirman que a partir de esta fecha el *XXXX* no tiene más relación de negocio jurídico con esta Fundación, ni con los investigadores contratados. En el momento de la entrega y previa a la emisión de la factura se incidió en la obligación de la destrucción de cualquier dato personal al que se hubiese tenido acceso. Afirman que la herramienta predictiva está implementándose en el sistema *PDyRH* como apoyo a la toma de decisiones de los investigadores y en virtud del plan estratégico del XXXX (según se indica en el mismo la implantación está prevista para el primer semestre de 2023).

-Por parte del área SEAV, se afirma que se había tenido conocimiento de que el anterior responsable del ***XXXXXXXX*** permitió la extracción y alojamiento de documentos en un portátil oficial sin conocimiento de los funcionarios que habían participado en el proceso de creación de la herramienta predictiva, y que esto no fue conocido ni por el área SEAV ni por el XXXX hasta el día posterior al robo del portátil, fecha en la que tuvieron noticias de que el ***XXXXXX*** *D.* ***XX*** había almacenado información en dicho portátil propiedad de la SES y que según sus propias manifestaciones también utilizaba para otros usos particulares y que sacaba de las instalaciones sin ningún control.

-Por parte del área SEAV se afirma textualmente: *"en caso de acceder a la información contenida en el ordenador por personas que puedan interpretar el contenido de la información, las consecuencias serían impredecibles, puesto que algunos de los atestados que se conocen, por las propias declaraciones de* ***XX***, *son de casos muy mediáticos, pero ya juzgados. Es decir, no se refieren a investigaciones vigentes".*

-En la documentación recibida, se afirma por parte del área SEAV, que se había permitido por el anterior jefe del ***XXXXXXXX*** la extracción y alojamiento de documentos en un portátil oficial y que estos extremos no fueron conocidos por los responsables del ***XXXX*** hasta el día posterior a la sustracción del portátil. Se afirma que ni por parte de los responsables de la SEAV ni por parte de los responsables del XXXX se tenía constancia de que el ***XXXXXXX*** de la UAM D***. XX*** , que desarrollaba trabajos para el ***XXXX*** a través de la ***XXXX***, hacía uso de un portátil oficial no solo para los trabajos del área ***XXXX*** sino que también era utilizado para sus clases en la Universidad, para su trabajo en la tesis doctoral y otros usos privativos y que según afirmación del propio ***XXXXXXX*** nadie le advirtió desde su incorporación en 2017 que no podía hacerlo.

En la documentación recibida, se afirma por parte del área SEAV, que según las propias declaraciones voluntarias que les había formulado el usuario D. ***XX*** ,el disco duro del portátil contenía al menos la siguiente información:

1. Atestados policiales sobre desapariciones de personas esclarecidas tanto de Policía Nacional y Guardia Civil como de las Policías Autonómicas Mossos d'Esquadra y Policía Foral de Navarra. También contiene bases de datos en las que se encontraba grabada la información de los atestados anteriormente referidos.

2. Atestados policiales sobre homicidios esclarecidos policial y judicialmente y asociados a una denuncia por desaparición, tanto de Policía Nacional como de Guardia

Civil. También contiene bases de datos en las que se encuentra grabada la información de los atestados anteriormente referidos, así como grabaciones de entrevistas en audio y video con los implicados en los casos (víctimas, agresores o familiares de estos entre otros aspectos).

3. Extracciones anuales del sistema de personas desaparecidas ***XXXXXXXX***.

4. También contenía dos carpetas con material relacionado con la información anterior y que fue utilizado con fines de docencia e investigación científica.

7- Relación de las medidas de seguridad preventivas para garantizar la protección de los datos personales afectados por la brecha, así como también acreditación del Análisis de Riesgos realizado para concluirlas. En concreto aquellas medidas destinadas a:

o Garantizar el control de acceso a los dispositivos y el control de los usuarios.

o Garantizar el control de soportes de almacenamiento con datos personales, y en concreto de aquellos que podían ser utilizados fuera de las instalaciones del Ministerio.

Responde que se adjunta información facilitada por la SGSICS Anexo II en la que señala que las medidas con las que la SGSICS protege los dispositivos portátiles administrados son las que se enumeran a continuación:

1. Herramienta ***XXXXXXXXXXX*** para detección y bloqueo de amenazas, análisis heurístico, escaneos semanales programados, políticas de control de aplicaciones instaladas, políticas de control de dispositivos que se conecten a portátiles, prevención de malware, políticas de control de acceso a web y cortafuegos para controlar el acceso de las aplicaciones de los portátiles a internet.

2. Herramienta ***XXXXXXXXX*** para neutralizar amenazas desconocidas por ***XXXXXXX*** e impedir la ejecución de ficheros maliciosos a partir de listas negras de ***XXXXXX***.

3. Protección de acceso a la ***XXXX*** mediante contraseña.

4. Para los soportes de almacenamiento destinados a ser utilizados fuera de las instalaciones del Ministerio, se procede al ***(…)***.

Con respecto al equipo sustraído, afirman que estaba incluido en una partida de seis equipos portátiles solicitados a la SGSICS para ser utilizados únicamente durante formaciones de carácter interno y que necesitaban disponer de menos seguridad dada las características de estos cursos, que posteriormente fue adjudicado el 29/11/2018 al Jefe de ***XXXXXXX*** en sustitución del que tenía por avería,(consta en documento anexo referencia 7) pero que, tanto el equipo averiado como el adjudicado, estaban destinados a su uso interior de las dependencias del Área VGEF, y que no se informó a la SGSICS por parte de la DGCE del uso del dispositivo con información policial fuera de las dependencias de la SES. Dadas las características propias de los cursos, estos equipos fueron configurados con el usuario administrador habilitado para su uso por las personas que los utilizaran y sin credenciales de acceso de usuario. Esta petición consta en el gestor de incidencias de la SGSICS con número de referencia ***XXXXX*** que se adjunta como Doc. 6.

"*Respecto a las medidas adoptadas por la SGSICS para la protección de los soportes de almacenamiento destinados a ser utilizados fuera de las instalaciones del Ministerio, se procede al* ***(…)****.*

En este punto hay que señalar que dado que por parte los responsables del Centro adjudicatario del equipo, no se informó ni se solicitó en ningún momento de la SGSICS medidas para la protección de la información ni del dispositivo en su traslado o uso de información de carácter policial o conteniendo datos de carácter personal fuera de las dependencias de Secretaría de Estado de Seguridad, el portátil sustraído carecía de cifrado de disco y de contraseña en la BIOS.

El Inspector indica como observación "*No se acredita el análisis de riesgos llevado a cabo ni por la propia DGCE como responsables de tratamiento ni por la SGSICS como responsables de garantizar la seguridad de los dispositivos*."

Se adjunta información facilitada por la SGSICS, Anexo II

8- Relación de todas aquellas medidas de seguridad reactivas (técnicas y organizativas) implantadas tras la detección de la brecha, y en concreto aquellas relacionadas con el cifrado y la anonimización de la información.

Responde que se adjunta información facilitada por la SGSICS Anexo II. En la misma, se indica:

"en coordinación con la DGCE, se procedió a la revisión y actualización de los procedimientos y medidas técnicas y organizativas de seguridad dando resultado el documento actualizado "Cláusula de Confidencialidad y Normativa de Buenas Prácticas", remitiéndose por parte del Área VGEF correo para que lo complete el personal externo (alumnos en prácticas) para asegurar que este documento fuese recibido, firmado y devuelto al Área para su custodia, y la petición de una relación actualizada de los alumnos de prácticas, en la que se consigne la fecha de inicio y fin de las mismas. Aporta copia del correo."

En la documentación recibida, anexo III del XXXX, se afirma que, como responsables de todas las acciones que realizan los alumnos en prácticas de la DGCE, se han revisado los protocolos de seguridad existentes y se ha procedido de forma inmediata a definir una serie de acciones para mejorar las medidas de seguridad:

1. Centralización de la gestión del personal alumno en prácticas (manteniendo un listado actualizado de convenios, acciones de gestión del uso físico de espacios para mejorar el control del personal).

2. Revisión y mejora de la cláusula de confidencialidad y documento de buenas prácticas en el uso de recursos y procedimientos de actuación ante pérdidas de información, con objeto de mejorar concienciación del personal que accede a datos protegidos y ofrecer guía de comportamientos que reduzcan el riesgo de brechas.

Revisión periódica por parte de la VGEF para mejora de los controles

1. Para controlar la salida de información se ha prohibido el uso o limitación de acceso a las instalaciones mediante teléfonos móviles, portátiles o dispositivos de almacenamiento. Para facilitar la custodia de estos se ha solicitado la habilitación de un armario.

2. Las personas externas que realicen trabajos en las instalaciones del XXXX:

3. Sólo tendrá acceso a datos seudonimizados por código y únicamente el funcionario responsable del externo tendrá acceso a los datos de correlación.

4. Los trabajos se realizan desde portátil oficial facilitado por el XXXX, siendo imposible la extracción de datos y que no podrá salir de las instalaciones

"*con respecto, a las medidas de tipo técnico, se siguen estrictamente las pautas marcadas por la Subdirección General de Sistemas de Información y Comunicaciones para la Seguridad (SGSICS), organismo que según el RD 734/2020 de 4/08, es el competente en esta materia*. "

Aporta anexo VI de la DGCE de 24/06/2022, dirigido a SGSICS en el que le solicita la colaboración y cooperación para revisar distintas medidas de seguridad técnicas y organizativas de su propia Dirección General, y de sus áreas que se están llevando a cabo, mencionándolas de modo que garanticen un nivel adecuado, otro de la misma fecha, dirigido al jefe del área SEAV, que gestiona varios ficheros el tratamiento de datos personales de los que la Dirección General es la responsable, le solicita la colaboración y cooperación para revisar el tratamiento del fichero PDYRH y colabore con la SGSICS para revisar los niveles de riesgo y las medidas de seguridad, considerando distintas y variadas que enumera.

El mismo tipo de escrito, se dirige a la jefa del Área de violencia de género, estudios y formación

9- Copia de la Evaluación de Impacto de protección de datos, en relación con las actividades de tratamiento afectadas por la brecha, o justificación del motivo por el que no se considera necesario realizarla, en su caso.

Respondió la propia Delegación de protección de datos que: "*No se ha realizado una evaluación de impacto del tratamiento PDyRH, puesto que la situación que dio origen a la brecha no derivó del tratamiento de datos formal o del sistema de información que le da soporte. No obstante, se han revisado, analizado y complementado legalmente todas y cada una de las actividades de tratamiento que se llevan a cabo en las Áreas afectadas, cuya documentación se acompaña dando respuesta a las preguntas precedentes*".

En la documentación recibida, ANEXO V, también se adjunta la respuesta dada el 26/09/2022, titulada: "síntesis *de las medidas reactivas adoptadas en el área de violencia de género estudios y formación sobre Protección de Datos de carácter personal-Estudios*.", por el JEFE DE ÁREA VGEF en contestación a la carta recibida por parte del Director de la DGCE y acreditada en el punto anterior, del análisis- De esta respuesta, se extrae:

Se afirma que dado que la recopilación, almacenamiento y tratamiento de datos son necesarios para realizar medidas de investigación científica para la elaboración de estudios e informes que permitan actualizar el conocimiento sobre los distintos aspectos de la criminalidad que faciliten su prevención y detección, así como una adecuada formación de los profesionales. se han revisado los protocolos de seguridad y procedimientos de tratamiento de la información

Las actuaciones realizadas han sido:

1. El soporte legal de las actividades de investigación se relaciona en la cumplimentación de las nuevas actividades de tratamientos: "*SES-ESTUDIOS*" y "*SES-TRATAMIENTOS ACCIONES INVESTIGACIÓN CIENTÍFICA*" publicitados en el Registro de Actividades de Tratamiento (RAT) del Departamento Ministerial. La finalidad es la realización de estudios científicos sobre criminalidad orientados a la prevención y detección de los delitos y en general contribuir en la mejora de la política de seguridad pública.

2. Se ha elaborado el Informe de Evaluación de Impacto en la Protección de datos (EIPD).

3. Se ha revisado y mejorado la Cláusula de Confidencialidad y Buenas Prácticas

4. También se ha procedido a implementar acciones para la gestión del uso físico de los espacios por parte del personal externo colaborador,

5. Asignación de un tutor responsable para los alumnos en prácticas, como figura de referencia y enlace con Estudios en caso de dudas o incidencias de los alumnos.

6. Normas generales de acceso y permanencia en el edificio. Normas de acceso lógico, uso responsable de los sistemas de información, traslado de activos e incidentes de información.

7. Guía de uso responsable de los recursos, destacando pautas para el buen uso de los sistemas de información, el uso responsable del correo electrónico y del acceso a Internet, la propiedad intelectual y el procedimiento de actuación ante las posibles pérdidas de información. Todo ello, cuando existan permisos específicos para estas acciones.

8. Elaboración de una ficha individual de personas externas colaboradoras en la que consta el detalle de las personas físicas, autorizaciones y accesos.

9. Se afirma que está previsto el seguimiento de todas las actuaciones mencionadas, que serán revisadas periódicamente al objeto de mantener actualizado el mapa de riesgos y mejora de los controles previamente definidos.

En ANEXO IV, figura también un documento que refiere, sin fecha y sin referencia de autor, añadiendo a lo anterior que "*por parte de Estudios de esta área de VGEF, encargados de coordinar todas las acciones relativas a los alumnos en prácticas, han revisado tras la brecha los protocolos de seguridad existentes, procediéndose también de*

forma inmediata a definir una serie de acciones reactivas encaminadas a mejorar las medidas de seguridad existente, en concreto:"

1. Se ha centralizado la gestión del personal alumno en prácticas, se mantendrán listados actualizados de alumnos, lo que permitirá incrementar el control y la monitorización:

2. Se procederá a la revisión de convenios de forma que se pueda acceder únicamente a través de convenios actualizados con las Universidades pertinentes y cumpliendo plazos establecidos.

10- En relación con el Esquema Nacional de Seguridad:

o Descripción de los sistemas de información afectados por la brecha y su categoría de seguridad.

o Copia de la Declaración de Aplicabilidad que contiene la relación de medidas implantadas en los sistemas de información afectados por la brecha.

o Copia del informe de la última auditoría realizada en los sistemas de información afectados por la brecha para verificar el cumplimiento de los requerimientos del ENS.

Se responde con la información se adjunta por la SGSICS, ANEXO II.

Manifiestan, que la información sustraída y proporcionada por parte de esta Subdirección correspondía únicamente al sistema de seguimiento integral de los casos de violencia de género *VioGén*. Especifica:

- las "*categorías de interesados*":

"*Personas que sean víctimas de hechos susceptibles de ser tipificados como violencia de género y las personas incursas en procedimientos judiciales e investigaciones judiciales relacionadas con esos mismos hechos*."

-la descripción: "*categorías datos personales*": antecedentes penales de los presuntos autores y situación penitenciaria de los mismos, relativa a la concesión de permisos o la puesta en libertad (condicional o definitiva) de los internos que se encuentren sujetos a medidas judiciales de alejamiento o prohibición de comunicación con la víctima. Así como todos aquellos que se encuentren condenados a penas o medidas alternativas diferentes al ingreso en prisión. Datos de carácter identificativo: DNI/NIF/pasaporte/, así como otros documentos de identidad, fotografía, domicilios, teléfonos, correo electrónico, vehículos. Datos de características personales: Datos de filiación, personas relacionadas, fecha y lugar de nacimiento, sexo, nacionalidad, situación laboral, datos de salud, profesión, nivel educativo y estado civil. Datos de carácter asistencial y de apoyo a las víctimas que figuren en los expedientes que elaboren los diferentes servicios y órganos que presten servicio a las víctimas de violencia de género.

Sobre la declaración de aplicabilidad que contiene la relación de medidas implantadas en los sistemas de información afectados por la brecha, señalan que "*dado que el sistema VioGén se trata de un sistema policial no contemplado en el ámbito de aplicación del*

Real Decreto 3/2010, de 8/01, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica (ENS), al no corresponder con un sistema mencionado en el artículo 2 de la Ley 11/2007, de 22/06, de acceso electrónico de los ciudadanos a los servicios públicos, y como quiera que hasta la nueva publicación del ENS (mayo 2022) no se recogía con expresa mención los referidos sistemas dentro del ámbito de aplicación del ENS, es en estos momentos, en base a la nueva redacción del ENS, que se está procediendo a la elaboración del Plan de Seguridad con medidas ajustadas al nuevo ENS. No existe por tanto Declaración de Aplicabilidad referida al sistema *VioGén* basada en el ENS.

Sobre la copia del informe de la última auditoría realizada en los sistemas de información afectados por la brecha para verificar el cumplimiento de los requerimientos del ENS, se manifiesta que se adjunta anexo referenciado como Doc. 9 la última auditoría realizada al sistema *VioGén, si bien no es aportada,* y reiteran que no tienen responsabilidad con respecto a la información restante que estaba almacenada en el portátil robado, como por ejemplo la perteneciente al sistema PDyRH.

1. Información actualizada respecto de si tiene conocimiento de la utilización por terceros de los datos personales obtenidos a través de la brecha.

Manifiesta el responsable de tratamiento que no tiene constancia hasta la fecha de la utilización por terceros de los datos personales filtrados en el portátil.

De la documentación recibida en respuesta a nuestro requerimiento también se acredita que este mismo día 24/06/2022 el director de la DGCE envió otra carta dirigida tanto al jefe de Área SEAV, al jefe de Área VGEF, y al subdirector General de la SGSICS con el siguiente contenido:

“De conformidad con los trabajos llevados a cabo derivados del incidente de seguridad materializado el pasado día 04 de mayo, siguiendo las recomendaciones y el criterio del delegado de Protección de Datos de la Secretaría de Estado de Seguridad….

Es necesario que revise todo el flujo de datos y tratamientos realizados en el fichero PDYRH de manera que se analicen y se documenten todas las actividades llevadas a cabo, de forma que, cumpliendo los principios generales de tratamiento, en el caso de entenderse necesarias, se incluyan en la documentación oportuna y se publiciten conforme a la legislación aplicable. Del mismo modo, en coordinación con la Subdirección General de Sistemas de Información y Comunicaciones para la Seguridad, en la parte que les competa, se revisen en base a los posibles niveles de riesgo todas medidas de seguridad técnicas y organizativas de modo que garantice un nivel adecuado de protección para los datos personales.

En concreto, salvo en los supuestos legalmente autorizados, se debe impedir en todo caso, que personas de carácter externo que colaboren con su Área en el desarrollo de cualquier actividad, posean el estatus que tengan en base al instrumento jurídico oportuno, puedan acceder a datos que no estén previamente anonimizados o pseudo-anonimizados, utilicen cuentas de correos oficiales (genéricas o personales), o usen o se relacionen con terceros a través de cualquier herramienta tecnológica que pueda llevar a error sobre sus funciones o cometidos en este organismo (correo electrónico, repositorio compartido, etc.)

Tampoco podrán acceder a informaciones que no sean ineludibles para sus cometidos y cualquier actuación en ese campo deberá ir guiada por el principio de "necesidad de conocer".

Como medidas de seguridad específicas que se debe comprobar que se están llevando a cabo en estos casos, al menos, se encontrarán las siguientes:

1. *Este personal externo, en concreto si está realizando alguna práctica de formación, debe estar supervisado singularmente por personal que acredite qué está haciendo, cómo lo está haciendo, dónde lo está haciendo y para quién lo está haciendo. De manera que en todo momento se pueda garantizar cuál es la labor concreta que está desempeñando.*
2. *Se debe controlar **(…)** de este personal de las instalaciones.*
3. *Se debe proporcionar el **(…)**, no permitiéndose el acceso a zonas o áreas no habilitadas para este personal.*
4. *No utilización de los **(…)** que se extenderá desde el acceso hasta la desconexión.*
5. *No podrán usar **(…)** más que para desarrollar sus cometidos, no permitiéndose el acceso a ninguna página, desarrollo o sistema que no se corresponda con su actividad.*
6. *No podrán utilizar **(…)** relacionada con sus cometidos.*
7. *No utilización de **(…)** de ningún tipo.*
8. *No conexión de **(…)**, deberá hacerse con supervisión de la SGSICS.*
9. *No utilización de **(…).***
10. *No utilización de **(…)** y/o contenga datos de carácter personal.*
11. *No utilización, uso o cualquier actividad basada en **(…)** fuera de las instalaciones.*

Del mismo modo, se reitera la necesidad de que todo su personal esté informado y concienciado en materia de protección datos, incidiéndose en las obligaciones de comunicación de incidentes o brechas de seguridad conforme a los protocolos establecidos para todos los organismos que dependen de la Secretaría de Estado de Seguridad. En todo caso, cualquier incidente de seguridad que afecta a datos de carácter personal debe ser comunicado al responsable de Tratamiento correspondiente y al DPD en el plazo más breve posible y siempre dentro de las 72 horas desde que se tenga conocimiento. Lo que le comunico a los efectos citados, rogando trasladen todas las actuaciones que se lleven a cabo al DPD de la Secretaría de Estado de Seguridad para su análisis y valoración.

En ANEXO III del XXXX de 4/10/2022, se indica que no se tiene noticia de la utilización por terceros sin autorización de los datos personales almacenados en dicho ordenador.

11) En fecha 6/02/2023, se solicitó requerimiento de información dirigido a la ***XXXXXX*** de la Universidad Autónoma de ***XXXXXX*** (***XXXX***), adjudicataria del contrato firmado con la SES. En fecha 22/02/2023, se recibe respuesta con la siguiente información:

-La ***XXXX*** resultó adjudicataria del contrato de investigación expediente 000000***XX***P027, para lo cual se contrató a D. ***XX***, *a instancia* de la propia SES, debido a que ya venía trabajando con los datos objeto del contrato y tenía experiencia en su análisis y a D.ª ***XX.*** Aporta copia de los contratos de trabajo de ambos trabajadores con fecha de firma 30/06/2021.

-Afirman que se acordó con la SES, que el personal adscrito a este contrato realizaría todos los trabajos en las dependencias sitas en la calle ******DIRECCIÓN.2*** de Madrid y con equipos informáticos propiedad de la SES, puesto que la información objeto del estudio tenía la consideración de datos especialmente protegidos. Afirman que no se realizaron trabajos fuera de las instalaciones de la SES ni con equipos propios de los investigadores, ni de la ***XXXX***. Por lo tanto, a la finalización del contrato no procedía la destrucción o devolución de los datos personales por hallarse en equipos que no era titularidad de la ***XXXX***.

-Afirman que los datos nunca fueron extraídos de los equipos de la SES y que desconocen cómo fue posible que el día 4/05/ 2022, un portátil con datos sensibles fuera robado al citado usuario. Afirman que esta situación no puede vincularse con la actuación de la ***XXXX*** como adjudicataria, puesto que el contrato finalizó el 31/12/2021 y no se mantuvo ninguna vinculación posterior con ninguno de los contratados. Aportan documento que enviaron a las dos personas contratadas notificando la finalización del contrato para dicha fecha, "*quedando rescindida la relación laboral desde esta fecha*"

-Afirman que en ningún momento la Dirección General de Coordinación y Estudios comunicó a la ***XXXX*** a la finalización del contrato (ni tampoco a los dos investigadores autorizados para la ejecución de los servicios) la obligación de destruir los datos, ni tampoco en momentos previos al abono de la factura. También se afirma que se desconoce en qué dispositivo se encontraban los datos que fueron sustraídos en fecha 4/05/ 2022.

-Afirman que el responsable del contrato no facilitó en ningún momento a los investigadores de la ***XXXX***, ni a la propia ***XXXX***, documentación, políticas o información relativa a las medidas técnicas y organizativas que debían cumplir los investigadores en la ejecución del contrato.

-Afirman que todo el personal de la ***XXXX*** recibe en el momento de su incorporación una documentación relativa al tratamiento de datos personales y formación en la materia. Como prueba de ello aportan el documento *Política de Seguridad de la* ***XXXX*** y el documento *"Compromiso de Confidencialidad de Empleados*" firmado por los investigadores contratados para dicho contrato, ***(…)*** *el* 30/06/2021. De este último documento destaca el siguiente contenido:

"… Usted asume el compromiso de guardar secreto profesional respecto de los datos personales, datos sobre los clientes, estrategias comerciales y organizativas e industriales, y cualquier otra información a la que tenga acceso con el motivo de las funciones asignadas, dicha obligación subsistirá en cumplimiento del artículo 32 del RGPD, aun después de finalizar relación laboral.

Bajo ningún concepto usted debe incorporar a los sistemas informáticos su información de carácter personal...

Asimismo, de conformidad con el artículo 32 del RGPD, como empleado se compromete a cumplir con las normas internas de seguridad que afectan al desarrollo de sus funciones, así como el uso de los equipos informáticos, correo electrónico demás aplicaciones a las que va a tener acceso. De igual modo, como parte necesaria tiene la

responsabilidad y el deber de realizar los programas formativos y aplicar los procedimientos y normas que se le comuniquen a tal efecto".

-Aportan copia del Registro de Actividades de Tratamiento para los contratos adjudicados entre los años 2020 y 2023 como encargados de tratamiento.

-Aportan la designación del delegado de Protección de Datos y la comunicación de este ante esta Agencia.

TERCERO: Inicio de procedimiento sancionador.

Con fecha 8/05/2023, se acordó por la Directora de la AEPD:

"INICIAR PROCEDIMIENTO SANCIONADOR a ***(...)****, con NIF* ***XXXXXXXX****, por la presunta infracción del del RGPD en los siguientes artículos:*

-25 del RGPD, de conformidad con el artículo 83.4.a) del RGPD, calificada como grave a efectos de prescripción en el artículo 73.d) de la LOPDGDD.

-32 del RGPD, de conformidad con el artículo 83.4.a) del RGPD, calificada como grave a efectos de prescripción en el artículo 73.f) de la LOPDGDD.

-33 del RGPD, de conformidad con el artículo 83.4.a) del RGPD, calificada como leve a efectos de prescripción en el artículo 74.m) de la LOPDGDD.

-34 del RGPD, de conformidad con el artículo 83.4.a) del RGPD, calificada como leve a efectos de prescripción en el artículo 74.ñ) de la LOPDGDD.2

"a los efectos previstos en el art. 64.2 b) de la ley 39/2015, de 1/10, del Procedimiento Administrativo Común de las Administraciones Públicas, (en lo sucesivo, LPACAP), las sanciones que pudieran corresponder serían de un apercibimiento por cada infracción, sin perjuicio de lo que resulte de la instrucción."

CUARTO: Alegaciones al acuerdo de inicio.

Frente al acuerdo de inicio, con fecha 29/12/2023, se recibieron alegaciones, manifestando:

1-Ha tenido entrada un escrito de notificación formal del acuerdo de inicio del PS/00128/2023, dirigido al Ministerio del Interior, nif ***XXXXXXXXX***, "*al no tener constancia de la recepción de la notificación del acuerdo de apertura, firmado electrónicamente por la directora de la AEPD el 8/05/2023*", "*por lo que procedemos de nuevo a su remisión",* manifestando que "*de lo cual no se ha tenido constancia en la SES, la DGCE ni en ninguno de sus órganos o unidades dependientes*."

Manifiesta que todo ello, cuando la comunicación de la brecha y el titular de los tratamientos se corresponden con el órgano directivo señalado de la DGCE, con nif propio: ***XXXXXXXXX***, también de la SES. Con base a que su DGCE tiene la

responsabilidad del tratamiento, así se indica en el RAT, como órgano directivo de la SES, que ejerce las competencias legalmente atribuidas, y que de acuerdo con el artículo 28.1 de la Ley 40/2015 de 1/10, solo pueden ser declarados responsables los que resulten responsables de las infracciones, estima que no puede atribuírsele al Ministerio del Interior en su conjunto la responsabilidad ni la conducta de la comisión objeto del expediente. Se "*hace necesaria la modificación del acuerdo de inicio de procedimiento para el ejercicio de la potestad sancionadora, so perjuicio de entender el procedimiento nulo pleno derecho de conformidad con el contenido del artículo 47 de la Ley 39/2015, de 1/10, del Procedimiento Administrativo Común de las Administraciones Públic*as."

Señala que anteriormente, en actuaciones previas, también se remitió requerimiento de información al NIF del Ministerio del Interior el 16/09/2022, y fue contestado por la DGCE el 6/10/2022.

2-Considera que el periodo de las actuaciones previas habría sido sobrepasado, tanto en la fecha de la firma del acuerdo de inicio, como cuando la comunicación es legalmente efectiva, mediante la notificación que se produce el 20/12/2023. "*Resultaría oportuna la formulación de una nueva iniciación del periodo de investigación y en virtud del resultado, la formulación de un nuevo acuerdo de inicio del procedimiento sancionador*", pues en caso contrario, se podría entender nulo, de conformidad con el artículo 47 de la LPACAP.

3-Estima que el tratamiento de datos se estaba realizando "*directamente por una autoridad competente dentro del -ámbito de aplicación del artículo 4 de la citada LO 7/2021, el mismo era necesario y que la finalidad del mismo era la prevención y la posible detección de ilícitos penales"*, por lo que se difiere del parecer de la AEPD de aplicar el RGPD, y no la LO 7/21. Aplicar el razonamiento expuesto, "*haría materialmente imposible desarrollar herramientas* policiales propias *por los órganos del Departamento para las Fuerzas y Cuerpos de Seguridad o el resto de a las autoridades competentes, puesto que el artículo 6.2 de la LO 7/21 no permite la cesión a entidades que no sean consideradas competentes salvo previsión con norma de ley interna o de la UE*". Las operaciones se estaban llevando a cabo por las áreas de la DGCE con la finalidad de lograr una herramienta técnica para prevenir y detectar delitos.

4-Sobre la imputación del artículo 25 del RGPD, manifiesta que "*los tratamientos que resultaron afectados, ya se encontraban incluidos como ficheros declarados e inscritos en la orden INT/1911/2007 de 26/06: "violencia doméstica y de género" en el Ministerio del Interior, y posteriormente en la orden INT/1202/2011 de 4/05*", en la que consta como responsable del fichero la SES.

5-Manifiesta que "*No son tratamientos nuevos con posibilidad de privacidad por diseño y por defecto desde una planificación previa a la realización efectiva de las operaciones puesto que se encontraban vigentes y en funcionamiento desde hacía décadas. Las medidas de seguridad estaban implantadas conforme al contenido del entonces aplicable, el Real Decreto 1720/2007, de 21/12, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13712, de protección de datos de carácter personal*."

6-Sobre la conducta atribuida como infracción del artículo 32 del RGPD, indica que da por reproducidas las medidas de respuesta y control comunicadas a la AEPD en las actuaciones previas.

Resume las medidas se seguridad implantadas indicando que se han reforzado las medidas técnicas aplicando políticas *Zerotrust* por defecto, diseñando un puesto de trabajo con mayores medidas de seguridad y un control centralizado a través de "*microsoft endpoint configuration Manager"*, que permite realizar un seguimiento constante de la situación de seguridad del parque informático y actuar de manera inmediata en caso de detecciones de incidencias de seguridad. Específicamente, refiere:

"*-**(…)**:*

*1. **XXXXXXX** en el arranque*

*2. Usuario y Contraseña del **XX***

*-Todos los equipos cumplen con la política de seguridad: Actualización y control de software instalado, para ello se usa la funcionalidad de **Itune de M365**, con la cual **(…).***

*Despliegue de **XXXXXXXXXX** Configuration **XXXXXXXXXXXXXX** con los siguientes objetivos:*

1. *Detectar actividad **XXXXXXXX** de usuarios y dispositivos **(…)**.*

2. *Proteger el **(…)**.*

3. Obtener información clara y en tiempo real de la escala de tiempo de los ataques para responder con rapidez.

4. *Monitorizar múltiples puntos de entrada a través de la integración con **(…).***

*-Despliegue por GPO de **(…)**.*"

7-Sobre la conducta del posible incumplimiento del artículo 33 del RGPD, artículo 38 de la LO 7/21, al considerarse leve, debería entenderse prescrita. Añade que la comunicación la realizó el responsable de manera inmediata después de que la unidad técnica que investigaba el incidente comprobó que podrían verse implicados datos de carácter personal.

8- Sobre la conducta del posible incumplimiento del artículo 34 del RGPD, artículo 39 de la LO 7/21, al considerarse leve, debería entenderse prescrita. Añade que el tratamiento que daba cobertura a estas actuaciones queda en el ámbito de la LO 7/21, por lo que ene aplicación del artículo 39.5 no procedía realizar la comunicación.

FUNDAMENTOS DE DERECHO

I Competencia

De acuerdo con los poderes que el artículo 58.2 del Reglamento (UE) 2016/679 (Reglamento General de Protección de Datos, en adelante RGPD), otorga a cada autoridad de control y según lo establecido en los artículos 47, 48.1, 64.2 y 68.1 de la Ley Orgánica 3/2018, de 5/12, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, LOPDGDD), es competente para iniciar y resolver este procedimiento la Directora de la Agencia Española de Protección de Datos.

Asimismo, el artículo 63.2 de la LOPDGDD determina que: *"Los procedimientos tramitados por la Agencia Española de Protección de Datos se regirán por lo dispuesto en el Reglamento (UE) 2016/679, en la presente ley orgánica, por las disposiciones reglamentarias dictadas en su desarrollo y, en cuanto no las contradigan, con carácter subsidiario, por las normas generales sobre los procedimientos administrativos."*

II Caducidad del procedimiento

En el acuerdo de inicio de indicaba*: "El procedimiento tendrá una duración máxima de 9 meses a contar desde la fecha del acuerdo de inicio o, en su caso, del proyecto de acuerdo de inicio. Transcurrido ese plazo se producirá su caducidad y, en consecuencia, el archivo de actuaciones; de conformidad con lo establecido en el artículo 64 de la LOPDGDD."*

El artículo 63 de la LOPDGD que se enmarca en el título VIII *"procedimientos en caso de posible vulneración de la normativa de Protección de Datos*" señala:

"1. Las disposiciones de este Título serán de aplicación a los procedimientos tramitados por la Agencia Española de Protección de Datos en los supuestos en los que un afectado reclame que no ha sido atendida su solicitud de ejercicio de los derechos reconocidos en los artículos 15 a22 del Reglamento (UE) 2016/679, así como en los que aquella investigue la existencia de una posible infracción de lo dispuesto en el mencionado reglamento y en la presente ley orgánica.

2. Los procedimientos tramitados por la Agencia Española de Protección de Datos se regirán por lo dispuesto en el Reglamento (UE) 2016/679, en la presente ley orgánica, por las disposiciones reglamentarias dictadas en su desarrollo y, en cuanto no las contradigan, con carácter subsidiario, por las normas generales sobre los procedimientos administrativos."

El acuerdo de inicio se firmó el 8/05/2023, y transcurrido el plazo para su resolución, que hubiera acontecido el 8/02/2024, no había tenido lugar. Aplicando el artículo 21.1 de la LPACAP, resulta:

"*1. La Administración está obligada a dictar resolución expresa y a notificarla en todos los procedimientos cualquiera que sea su forma de iniciación.*

En los casos de prescripción, renuncia del derecho, caducidad del procedimiento o desistimiento de la solicitud, así como de desaparición sobrevenida del objeto del procedimiento, la resolución consistirá en la declaración de la circunstancia que concurra en cada caso, con indicación de los hechos producidos y las normas aplicables."

Considerando los efectos previstos en el artículo 25 de la misma norma, que indica:

"*1. En los procedimientos iniciados de oficio, el vencimiento del plazo máximo establecido sin que se haya dictado y notificado resolución expresa no exime a la Administración del cumplimiento de la obligación legal de resolver, produciendo los siguientes efectos:*

b) En los procedimientos en que la Administración ejercite potestades sancionadoras o, en general, de intervención, susceptibles de producir efectos desfavorables o de gravamen, se producirá la caducidad. En estos casos, la resolución que declare la caducidad ordenará el archivo de las actuaciones, con los efectos previstos en el artículo 95.", que indica:

"3*. La caducidad no producirá por sí sola la prescripción de las acciones del particular o de la Administración, pero los procedimientos caducados no interrumpirán el plazo de prescripción.*

En los casos en los que sea posible la iniciación de un nuevo procedimiento por no haberse producido la prescripción, podrán incorporarse a éste los actos y trámites cuyo contenido se hubiera mantenido igual de no haberse producido la caducidad. En todo caso, en el nuevo procedimiento deberán cumplimentarse los trámites de alegaciones, proposición de prueba y audiencia al interesado."

De conformidad con lo señalado, la Directora de la Agencia Española de Protección de Datos

RESUELVE:

PRIMERO: Declarar la caducidad del procedimiento iniciado a la **DIRECCIÓN GENERAL DE COORDINACIÓN DE ESTUDIOS (SECRETARÍA DE ESTADO DE SEGURIDAD-MINISTERIO DEL INTERIOR)** con NIF S2800109G por las infracciones de los artículos 25, 32, 33 y 34 del RGPD.

SEGUNDO: NOTIFICAR la presente resolución a **DIRECCIÓN GENERAL DE COORDINACIÓN DE ESTUDIOS (SECRETARÍA DE ESTADO DE SEGURIDAD-MINISTERIO DEL INTERIOR)** con NIF S2800109G.

TERCERO: COMUNICAR la presente resolución al DEFENSOR DEL PUEBLO, de conformidad con lo establecido en el artículo 77.5 de la LOPDGDD.

CUARTO: De conformidad con lo establecido en el artículo 50 de la LOPDGDD, la presente Resolución se hará pública una vez haya sido notificada a los interesados.

Contra esta resolución, que pone fin a la vía administrativa conforme al art. 48.6 de la LOPDGDD, y de acuerdo con lo establecido en el artículo 123 de la LPACAP, 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 13/07, 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 de la referida Ley.

Finalmente, se señala que conforme a lo previsto en el art. 90.3 a) de la LPACAP, se podrá suspender cautelarmente la resolución firme en vía administrativa si el interesado manifiesta su intención de interponer recurso contencioso-administrativo. De ser éste el caso, el interesado deberá comunicar formalmente este hecho mediante escrito dirigido a la Agencia Española de Protección de Datos, presentándolo a través del Registro Electrónico de la Agencia [https://sedeagpd.gob.es/sede-electronica-web/], o a través de alguno de los restantes registros previstos en el art. 16.4 de la citada Ley 39/2015, de 1/10. También deberá trasladar a la Agencia la documentación que acredite la interposición efectiva del recurso contencioso-administrativo. Si la Agencia no tuviese conocimiento de la interposición del recurso contencioso-administrativo en el plazo de dos meses desde el día siguiente a la notificación de la presente resolución, daría por finalizada la suspensión cautelar.

938-16012024

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