Identificación del expediente

Resolución de procedimiento sancionador núm. PS 35/2022, en lo referente a Indra Sistemas, SA.

Antecedentes

1 . En fechas 05/10/2021, 06/10/2021, 07/10/2021, y 26/10/2021 tuvieron entrada en la Autoridad Catalana de Protección de Datos, hasta seis denuncias (dos de ellas por remisión de la Agencia Española de Protección de Datos) formuladas de forma separada por personas ciudadanas contra la Autoridad del Transporte Metropolitano (en adelante, la ATM), y una denuncia formulada contra la Sociedad Catalana para la Movilidad, SA, (en adelante, SocMobilitat), con motivo de un presunto incumplimiento de la normativa sobre protección de datos personales.

En concreto, las personas denunciantes se quejaban de que en fecha 05/10/2021 se había detectado una vulnerabilidad de seguridad en el portal T-mobilitat.atm.cat, (https://t-mobilitat.atm.cat) que debería permitido el acceso por parte de terceros a sus datos personales allí registrados, facilitados para darse de alta como usuarios de la nueva tarjeta T-Mobilitat (nombre y apellidos, DNI, dirección postal y correo electrónico). Asimismo, se quejaban de que la vulnerabilidad detectada permitía la modificación de la información de los usuarios allí contenida.

Para justificar los hechos denunciados, las personas denunciantes aportaban la siguiente documentación:

-Captura de pantalla del hilo del tuit publicado por un ciudadano en fecha 05/10/2021 (a las 15:39 h) donde se muestra la brecha de seguridad y la forma en que se podía acceder a la información de terceras personas, y se indicaba los pasos a seguir (https://twitter.com (...)).

-Noticia publicada en los medios de comunicación en fecha 05/10/2021 " *Un error en la web de la T-Mobilitat deja al descubierto datos de los usuarios".*

- Tuits publicados por T-Mobilitat en su canal en fechas 05/10/2021, y 06/10/2021, respectivamente, en relación al incidente objeto de denuncia:

" *Hemos detectado un error operativo en la web de la T-Mobilitat, en etapa de pruebas. El fallo ha permitido durante tiempo limitado el acceso a datos no sensibles. La ATM abrirá un expediente informativo a la empresa responsable de este desarrollo web* " (05/10/2021 a las 17:00 h).

" *El acceso a la web T-mobilitat.cat en esta fase de pruebas ha quedado suspendido temporalmente. Hemos decidido realizar, con la Agencia de Ciberseguridad, un análisis exhaustivo para descartar cualquier otra vulnerabilidad no detectada* ." (06/10/2021 a las 18:00 h).

2. La Autoridad abrió una fase de información previa, de acuerdo con lo que prevé el artículo 7 del Decreto 278/1993, de 9 de noviembre, sobre el procedimiento sancionador de aplicación a los ámbitos de competencia de la Generalidad , y el artículo 55.2 de la Ley 39/2015, de 1 de octubre, del procedimiento administrativo común de las administraciones

públicas (en adelante, LPAC), para determinar si los hechos eran susceptibles de motivar la incoación de un procedimiento sancionador, y las personas presuntamente responsables.

3. La ATM, en cumplimiento de lo que prevé el artículo 33 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril, relativo a la protección de las personas físicas en lo que se refiere al tratamiento de datos personales ya la libre circulación de éstos (en adelante, RGPD), y en su condición de responsable de tratamiento notificó a esta Autoridad en fecha 06/10/2021, la violación de seguridad de los datos sufridos (NVS 86/ 2021), consistente en la vulnerabilidad detectada en el portal T-mobilitat.atm.cat, que comprometió datos personales de los usuarios allí registrados. Las actuaciones llevadas a cabo en el marco de la notificación de dicha violación de seguridad (NVS 86/2021) se incorporaron en la fase de información previa abierta con motivo de las denuncias presentadas ante la Autoridad por los mismos hechos.

4. En la fase de información previa, en fecha 15/11/2021 se requirió la ATM para que diera cumplimiento a lo siguiente:

- Por un lado que informara si se disponía de nueva información que modificara en algún aspecto las manifestaciones efectuadas, en el marco de la notificación a la Autoridad de la violación de seguridad, en relación con el resultado del análisis sobre el incidente efectuado por la Agencia de Ciberseguridad, y recogido en el "informe sobre la vulnerabilidad de seguridad detectada en el portal T-mobilitat.atm.cat el 05/10/2021", y en su anexo, y en concreto respecto a :

"Cronología de la incidencia
El día 5 de octubre de 2021 a las 15:39 un ciudadano publica en Twitter una vulnerabilidad detectada en el portal T-mobilitat.atm.cat
A las 16:24 ATM indica la vulnerabilidad al proveedor SOC Movilidad.
Se convoca un comité técnico urgente para revisarla y proceder a su mitigamiento.
A las 16.40 se mitiga la vulnerabilidad.

"Acceso a datos
Los datos comprometidos son el nombre, apellidos e identificador de usuario, no de la palabra de paso de entrada en el portal web. Recalcar que no ha habido afectación en los datos ubicados en los Sistemas Centrales del sistema T-movilidad sino únicamente en aquellos correspondientes al portal web. Tampoco se ha producido afectación a la integridad de los datos.
El alcance de los datos comprometidos ha sido confirmado por la Agencia de Ciberseguridad de Cataluña como conclusión del análisis de datos que han realizado en base a la información proporcionada por ATM (Ver Anexo 1).
El volumen de datos comprometidos es de 2.161 registros, de los que 1.046 son internos de test del sistema.

Causa de la vulnerabilidad
En la infraestructura de tecnología Liferay del portal T-mobilitat.atm.cat había quedado configurado el usuario, contraseña, y la posibilidad nativa de entrar que viene por defecto del fabricante.
De esta forma se podía acceder desde Internet a las páginas de configuración del propio portal y entrar con el usuario por defecto.

Acciones de mitigación realizadas
Las siguientes acciones se han realizado sobre la infraestructura de tecnología Liferay del portal T-mobilitat.atm.cat:
• Dejar sólo un usuario administrador y cambiarle la contraseña.
• Desconectar la posibilidad nativa de entrar en Liferay .
• Comprobar a través de un script que no se ha modificado contenido alguno del portal. En este caso se ha confirmado que no ha habido ninguna modificación."

-Por otra parte, que confirmara si la violación de seguridad de los datos sufrida, se habría producido en el marco de un encargo encomendado a la Sociedad Catalana para la Movilidad, SA. En caso de respuesta afirmativa, aportara copia del contrato de encargado de tratamiento suscrito con dicha entidad.

5. En fecha 22/11/2021, la ATM respondió al anterior requerimiento, a través de escrito en el que exponía lo siguiente:

- Que no se había producido ninguna modificación, respecto a la información aportada en la notificación de la violación de seguridad, que "era correcta y se ajustaba a la realidad de los hechos ocurridos."

- Que la violación de seguridad, se produjo en el marco de un encargo encomendado a la Sociedad Catalana para la Movilidad SA. "

Se adjuntaba el contrato de encargo del tratamiento suscrito entre la ATM (responsable del tratamiento) y SocMobilitat (encargado del tratamiento) el 30/09/2021 para la prestación de servicios para la fase de implantación y gestión de la T-Movilidad.

6 . De acuerdo con los antecedentes que se han relacionado hasta aquí y con el resultado de las actuaciones de indagación llevadas a cabo en el marco de la información previa, que engloba tanto las denuncias interpuestas contra la ATM (a las que se asignó nº IP 394/2021, 395/2021, 400/2021, 403/2021, 431/2021 y 432/2021) como la denuncia interpuesta contra Soc Movilidad (a la que se asignó nº IP 397/20 la Directora de esta Autoridad acordó en fecha 10/01/2022 iniciar un procedimiento sancionador contra el encargado del tratamiento Soc Mobilitat (PS (...)), por la presunta vulneración del principio de seguridad de los datos en el despliegue del portal T-Mobilitat y consiguiente vulneración de su confidencialidad, y de acuerdo con el régimen de responsabilidad en materia de protección de datos previsto en el artículo 28.10 del RGPD, que prevé que el encargado del tratamiento es responsable ante la autoridad de control, de las presuntas vulneraciones de la normativa de protección de datos que puedan cometerse en el desarrollo del encargo que incumplan lo establecido en el encargo. Este acuerdo de iniciación se notificó a la entidad imputada en fecha 17/01/2022.

7. En fecha 04/02/2022, SocMobilitat formuló alegaciones al acuerdo de iniciación aportando junto con su escrito documentación diversa. Entre esta documentación, el contrato de encargado de tratamiento suscrito entre SocMobilitat e Indra Sistemas SA (en adelante, Indra), en fecha 30/09/2021 para la prestación de servicios técnicos en el marco del Proyecto Tecnológico T-mobilitat adjudicado a SocMobilitat (documento núm.2), entre los que, y según manifiesta, el despliegue del portal T-mobilitat, y el "Informe jurídico en relación a la brecha de seguridad del portal extranet de T-Mobilitat" (documento núm.6).

8 . A la vista de las alegaciones formuladas, y del análisis de la documentación aportada por la entidad imputada, en fecha 26/04/2022 se requirió a SocMobilitat la aportación de documentación adicional, más concretamente:

-Copia de los contratos de prestación de servicios para la fase de implantación y de gestión para la T-Mobilitat suscritos entre SocMobilitat e Indra en fecha 21/07/2014, y de sus posteriores modificaciones o adendas, a las que hacía referencia el contrato de encargado del tratamiento suscrito entre SocMobilitat e Indra en fecha 30/09/2021 (cláusula 2a: "Condiciones y finalidades del tratamiento" :

> *2. Condiciones y finalidades del tratamiento*
> *2.1 "El tratamiento consistirá en las prestaciones técnicas dentro del Proyecto tecnológico de la T-Movilidad atribuidas y asumidas por INDRA en los contratos de prestación de servicios para la fase de implantación para la T-movilidad y en el de prestación de servicios para la fase de gestión para la T-Movilidad suscritos entre SOC MOVILIDAD e INDRA en fecha 21 de julio de 2014 y sus posteriores modificaciones addendas."*

-Copia de la evaluación o del análisis de riesgos efectuado por SocMobilitat con respecto al tratamiento de datos derivado de las prestaciones técnicas encomendadas a Indra en dichos contratos. Al respecto, en el contrato de encargado del tratamiento se hacía constar lo siguiente:

> "7. Obligaciones del encargado del tratamiento (...)
> *"7.5. Seguridad del Tratamiento*
> *El encargado del Tratamiento implantará las Medidas apropiadas respecto a la seguridad del Tratamiento, que se correspondan con las de la Administración contratante y que se ajusten al Esquema Nacional de Seguridad (NIVEL BÁSICO)." (...).*

9 . En fecha 03/05/2022 la entidad SocMobilitat dio cumplimiento a dicho requerimiento y aportó copia de los contratos de prestación de servicios para la implantación y gestión de la T-Mobilitat suscritos entre SocMobilitat e Indra en fecha 21/07/2014 y de sus modificaciones, y copia del análisis de riesgos.

En dichos contratos de prestación de servicios para la implantación y gestión de la T-Mobilitat suscritos entre SocMobilitat e Indra en fecha 21/07/2014, consta como tarea asignada a Indra el despliegue del portal web de la T-mobilitat.

10 . Del análisis de toda la documentación aportada por SocMobilitat en la tramitación del procedimiento sancionador (...), se constató que los hechos que motivaron su incoación, es decir, la vulneración del principio de seguridad de los datos en el despliegue del portal T-Mobilitat y consiguiente vulneración de su confidencialidad, por falta de aplicación de determinadas medidas de seguridad, era imputable a Indra Sistemas, SA en el marco del contrato de encargo del tratamiento de datos personales suscrito entre SocMobilitat (adjudicataria del contrato y encargada del tratamiento) e Indra (socia accionista de SocMobilitat y subencargada del tratamiento), para la prestación de servicios en la fase de implantación y de gestión de la T-movilidad.

En este sentido, en el contrato de encargo del tratamiento de datos personales suscrito entre SocMobilitat e Indra en fecha 30/09/2021 se estipulaban las medidas de seguridad que Indra debía adoptar para la prestación objeto de encargo:

"7. Obligaciones del encargado del tratamiento (...)

"7.5. Seguridad del Tratamiento
El encargado del Tratamiento implantará las Medidas apropiadas respecto a la seguridad del Tratamiento, que se correspondan con las de la Administración contratante y que se ajusten al Esquema Nacional de Seguridad (***NIVEL BÁSICO*** *).*

En todo caso, el Encargado deberá implantar mecanismos para:
a. Garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de Tratamiento.
b. Restaurar la disponibilidad y acceso a las Datos personales de forma rápida, en caso de incidente físico o técnico.
c. Verificar, evaluar y valorar de forma regular, la eficacia de las medidas técnicas y organizativas implantadas para garantizar la seguridad del tratamiento.
d. Seudonimizar y cifrar las Datos personales, en su caso.

En conjunto, deberá adoptar todas aquellas otras medidas que, teniendo en cuenta el conjunto de tratamientos que lleva a cabo, sean necesarias para garantizar un nivel de seguridad adecuado al riesgo." (...).

Dicho esto, las medidas de seguridad que se vulneraron en la configuración del portal de la T-movilidad, que propiciaron que el acceso quedara abierto, ya su vez, accesible a terceros, son de nivel básico (apartado 4.1.2 "Arquitectura de la Seguridad"),4.2 relativo al control de acceso, y apartado 4.3.2 relativo a la "configuración de seguridad") del Esquema Nacional de Seguridad (ENS) aprobado por Real Decreto 3/2010, al que se hace referencia a ello.

A la vista de todo lo anterior y de conformidad con el artículo 20.1.c) del Decreto 278/1993, de 9 de noviembre, sobre el procedimiento sancionador de aplicación a los ámbitos de competencia de la Generalidad de Cataluña, en fecha 27 /05/2022, la Directora de la Autoridad Catalana de Protección de Datos acordó sobreseer el procedimiento núm. (...) iniciado contra SocMobilitat, al considerar que no se podía atribuir a SocMobilitat la responsabilidad de la falta de aplicación de las medidas técnicas apropiadas para garantizar la seguridad de los datos objeto de tratamiento, dado que la adopción de los mismos medidas de seguridad, y en concreto las de nivel básico, era una obligación que correspondía a Indra, como subencargado del tratamiento, tal y como se estipula en el contrato de encargo del tratamiento de datos personales suscrito en fecha 30/09/ 2021 entre SocMobilitat e Indra. En la misma resolución de sobreseimiento se acordó incoar un expediente sancionador a Indra Sistemas, SA, a fin de determinar su presunta responsabilidad en la falta de aplicación de medidas técnicas de nivel básico en la implantación del portal web T-mobilitat, exigidas por SocMobilitat, que propició que terceras personas pudieran acceder a los datos personales de los usuarios allí registrados.

En este sentido, debe tenerse en cuenta que el régimen de responsabilidad en materia de protección de datos establecido en el artículo 28.10 del RGPD, al que antes se ha hecho referencia, es también aplicable al subencargado del tratamiento, de acuerdo con lo que dispone el artículo 28.4 del RGPD y 70.1.b) LOPDGDD (que se considera, en todo caso, un

encargado del encargado del tratamiento), y, por tanto, es también responsable, ante la autoridad de control, de las presuntas vulneraciones de la normativa de protección de datos que pueda cometer en el desarrollo del encargo que incumplan lo establecido en el encargo.

11. En fecha 01/06/2022, se inició, por el Acuerdo de la directora de la Autoridad Catalana de Protección de Datos, el presente procedimiento sancionador contra Indra, por una presunta infracción prevista en el artículo 83. 4 .a), en relación con el artículo 32.1; todos ellos del RGPD. Este acuerdo de iniciación se notificó a la entidad imputada en fecha 02/06/2022.

En el acuerdo de iniciación se concedía a la entidad imputada un plazo de 10 días hábiles para formular alegaciones y proponer la práctica de pruebas que considerase convenientes para defender sus intereses.

12. En fecha 15/06/2022, Indra formuló alegaciones al acuerdo de iniciación .

13 . En fecha 09/09/2022, la instructora de este procedimiento formuló una propuesta de resolución, por la que proponía que la directora de la Autoridad Catalana de Protección de Datos impusiera a Indra una multa de 25.000 euros como responsable, de una infracción prevista en el artículo 83.4.a) en relación con el artículo 32.1, en lo que se refiere al principio de seguridad de los datos, ambos del RGPD.

Esta propuesta de resolución se notificó en fecha 10/09/2022 y se concedía un plazo de 10 días para formular alegaciones.

14. En fecha 22/09/2022, la entidad imputada presentó un escrito de alegaciones a la propuesta de resolución.

Hechos probados

En fecha 30/09/2021 la Sociedad Catalana para la Movilidad, SA, formalizó un contrato de encargado del tratamiento con la sociedad Indra Sistemas, SA, para la prestación de servicios en la fase de implantación y gestión de la T-movilidad (entre otros, el despliegue del portal T-movilidad).

La ejecución de este contrato, comportaba que Indra accedía y gestionaba los datos personales de los usuarios de la T-Mobilitat, y se le exigía la adopción de medidas de nivel básico del ENS.

En el marco de este encargo, el subencargado del tratamiento, Indra, no aplicó medidas técnicas de seguridad de nivel básico exigidas por SocMobilitat, dado que al configurar el control de acceso al portal web de la T-Mobilitat no se modificó la contraseña que por defecto asigna el fabricante de la infraestructura de tecnología “Liferay” al administrador (credencial de acceso pública), de tal modo que el acceso quedaba abierto, ya su vez, accesible a terceros, medida que ENS exige para los sistemas categorizados de nivel básico.

Así pues, desde la puesta en marcha del portal T-Mobilitat (a las 08:00 del día 04/10/2021), hasta las 16:40 h del día 05/10/2021, cualquier persona podía acceder a través de internet en las páginas de configuración del portal web T-mobilitat, y en la información personal de

terceros allí contenida, así como modificarla, si se introducía la contraseña o paso de paso que por defecto asigna el fabricante de la infraestructura de tecnología "Liferay" (software utilizado para la gestión de las tarjetas t-Movilidad) al administrador. En concreto los datos personales de los usuarios a los que se accedió eran: nombre y apellidos, identificador de usuario, y al propio hecho que habían solicitado la nueva tarjeta T-Mobilitat.

Así, consta acreditado el acceso por parte de un tercero a dichos datos en fecha 05/10/2021 a las 15:39 h (ciudadano/usuario del portal que publicó el tuit).

Fundamentos de derecho

1. Son de aplicación las previsiones de la Ley 39/2015, de 1 de octubre, del procedimiento administrativo común de las administraciones públicas (LPAC) , y el artículo 15 del Decreto 278/1993, de acuerdo con la DT 2ª de la Ley 32/2010, de 1 de octubre, de la Autoridad Catalana de Protección de Datos. La resolución del procedimiento sancionador corresponde a la directora de la Autoridad Catalana de Protección de Datos , de conformidad con los artículos 5 y 8 de la Ley 32/2010.

2. La entidad imputada ha formulado alegaciones tanto en el acuerdo de iniciación como en la propuesta de resolución. En esta resolución se analiza el conjunto de estas alegaciones.

2.1. Sobre la accesibilidad al sistema por terceros.

Indra esgrime que reconoce que al configurar el control de acceso al portal web de la T-Mobilitat, no modificó la contraseña que por defecto asigna el fabricante de la infraestructura de tecnología "Liferay" al administrador, pero niega que esto fuera lo que provocase que, desde la puesta en marcha del portal T-movilidad hasta las 16:40 h del día 05/10/2021, el acceso al portal quedara abierto, y que cualquier persona pudiera acceder a través de internet en la información allí registrada.

En este sentido, Indra defiende, como ya exponía en las alegaciones al acuerdo de incoación, que desde el momento de la puesta en marcha del portal web, había implementado un sistema de identificación y autenticación de usuarios protegido con credenciales, y que si bien es cierto que el acceso había quedado configurado con la posibilidad nativa de entrar con las credenciales que vienen por defecto del fabricante, estas credenciales estaban bajo el control exclusivo del usuario administrador, y vuelve a reiterar que lo que provocó que dejaran de estar bajo su control exclusivo fue la actuación maliciosa de un tercero que, aprovechándose de sus conocimientos informáticos, vulneró las medidas de seguridad implementadas por Indra, y mediante pruebas de penetración no autorizadas adivinó la contraseña, accedió a los datos reservados de ATM, e hizo públicas las credenciales del administrador a través de las redes sociales, momento a partir del cual las credenciales dejaron de estar bajo el control exclusivo del usuario administrador, y el acceso al sistema quedó abierto.

Al respecto, cabe decir, cómo se analizará con detalle en la próxima alegación y cómo ya se ponía de manifiesto en la propuesta de resolución, que no se puede admitir que el sistema de identificación y autenticación implementado por Indra estuviera protegido con credenciales que estaban bajo el control exclusivo del administrador, y que lo que ocasionó que la puerta de entrada al sistema quedara abierta fuera la actuación de un tercero que vulneró dicho sistema, teniendo en cuenta que es un hecho no discutido que, por descuido o

error, se había dejado activada (o no se había retirado) la contraseña estándar asignada por defecto por el fabricante al administrador (extremo, se insiste, reconocido por Indra), de tal modo que cualquier persona podía entrar con dicha contraseña, sin que, por tanto, el administrador tuviera en ningún momento el "control exclusivo" sobre dicha contraseña, como sostiene Indra, pues es evidente que desde el momento en que éstas eran de carácter público (publicadas en la documentación técnica del fabricante y accesibles en internet por cualquier persona), el administrador no tenía ningún control sobre las mismas.

Por eso no puede prosperar la alegación esgrimida por Indra en el sentido de que lo que provocó que el acceso quedara abierto y accesible a terceros, fue la vulneración de las medidas de nivel básico implementadas por Indra, en tanto que no se puede sostener que tuviera implementadas dichas medidas, cuando el sistema de control de acceso no disponía de un sistema de autenticación de usuarios protegido con credenciales configuradas por el propio administrador, a fin de garantizar que sólo podían acceder a los datos las personas autorizadas.

Por último hay que recordar que, como ya se puso de manifiesto por parte de la persona instructora en la propuesta de resolución, la imputación a Indra en el presente procedimiento no deriva del hecho de que se haya materializado un acceso a los datos por parte de un tercero no autorizado, sino que la conducta que se le imputa es no haber implementado las correspondientes medidas de seguridad en la configuración del control de acceso al portal web para garantizar la confidencialidad de los datos allí registrados y asegurar su protección frente a intentos de accesos indebidos, y en concreto medidas de nivel básico del ENS que le fueron expresamente exigidas por SocMobilitat en el contrato de encargo suscrito en fecha 30/09/2021.

2.2. Sobre el incumplimiento de las medidas de seguridad por parte de Indra.

2.2.1 El deber de preservar la confidencialidad mediante la implementación de las medidas técnicas adecuadas.

Las alegaciones formuladas por Indra, se centran exclusivamente en discutir la aplicación de las medidas de seguridad correspondientes al ENS, y obvia toda referencia a las obligaciones que dimanen directamente del RGPD, el eje central del conjunto de la normativa de protección de datos, más concretamente, a la obligación de mantener la confidencialidad de los datos personales que se tratan, que es un deber recogido como principio rector en el artículo 5.1 f) del RGPD, invocado de forma constante tanto en el acuerdo de incoación como en la propuesta de resolución, y que impone que los datos deben ser:

> tratados *de tal modo que se garantice una adecuada seguridad de las datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas («integridad y confidencialidad »)* "

Esta obligación se ve reforzada en el art. 32.1 del RGPD, cuyo incumplimiento se imputa en el presente procedimiento:

> 1. *Teniendo en cuenta el estado de la técnica, las costas de aplicación, y la naturaleza, el alcance, el contexto y las fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas*

físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros:

b) la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento (...) ".

En relación a esta obligación no es una cuestión que esté en discusión, que la obligación de garantizar la confidencialidad de los datos personales mediante la aplicación de las adecuadas medidas de seguridad , se recogió expresamente en el propio contrato de encargado del tratamiento suscrito entre SocMobilitat e Indra, es decir, Indra, debía implementar las medidas de seguridad correspondientes al nivel básico del ENS, y llevar a cabo las acciones indispensables para garantizar en todo momento la confidencialidad de la información tratada, lo que no hizo cómo se analiza en los siguientes subapartados. Como tampoco es discutible que cambiar la contraseña que había por defecto en el software de gestión de "Liferay", no supone ir más allá del estado de la técnica actual ni conlleva costes de implementación significativos.

En este marco, el objeto del ENS es, justamente, "asegurar el acceso, **integridad** , disponibilidad, autenticidad, **confidencialidad,** trazabilidad y conservación de las datos, informaciones y servicios utilizados en medios electrónicos que gestionan en el ejercicio de sus competencias ". (art. 1.2).

Efectuadas con carácter previo estas consideraciones, se analizan a continuación los argumentos esgrimidos por Indra para intentar justificar que, en la configuración del control de acceso al portal web de la T-movilidad, cumplió con las medidas de seguridad de nivel básico exigidas por SocMobilitat.

2.2.2 El deber de que el control de acceso sea efectivo mediante el uso de claves secretas (contraseñas).

Una de las principales alegaciones de Indra, como ya se avanzaba en el punto 2.1 de esta resolución, consiste en asegurar que contaba con un sistema de control de acceso adecuado ya que "Ninguna de estas normas [*cita* previamente una serie de normas de antecedentes y coetáneas en el ENS] *establece expresamente qué se entiende por proteger el sistema de modo que nadie acceda a los recursos sin autorización, más allá de citar la necesidad de configurar un sistema de autenticación basado, por ejemplo, en usuario y contraseña* [...]".

Sin embargo, cuando reconoce Indra, se está haciendo referencia a la necesidad de que el sistema de acceso se base en la combinación de usuario y contraseña ya se está especificando la naturaleza de la protección que se exige. Pues "contraseña" implica, según la definición de la RAE "una *seña* ***secreta*** *que permite el acceso a algo, a alguien oa un grupo de personas* ***antes inaccesible*** ".

De hecho, este mismo carácter secreto también se establece en la página 4 " Guía de Seguridad de las TIC CCN-STIC 821. Apéndice V: Normas de creación y uso de contraseñas NP40": " *Es especialmente importante mantener el carácter secreto de la contraseña. No debe entregarse ni comunicarse a nadie. En caso de haber tenido necesidad de hacerlo, el usuario deberá proceder a cambiarla de forma inmediata* ". Se trata de un

instrumento particularmente válido como medio de interpretación del ENS, dado que las instrucciones técnicas del CCN-STIC están expresamente previstas para este fin en el propio ENS (apartado 7º del Anexo II).

En otros términos, para que un sistema de autenticación pueda considerarse mínimamente efectivo como protección, es necesario que exija un usuario y una contraseña entendida como una información secreta. Por tanto, en ningún caso el sistema implementado por Indra podía ser considerado válido en la medida en que no cumplía con algo esencial como era que la contraseña fuera secreta, ya que al ser la que incorporaba por defecto el fabricante era públicamente accesible.

La medida 4.1.2 "Arquitectura de seguridad [op.pl.2]" del ENS indica que también para los sistemas de categoría básica habrá que detallar un sistema de identificación y autenticación de usuarios, y la medida 4.2 "Control de acceso. [op.acc]" detalla las características indispensables tanto de la identificación [op.acc.1] como de la autenticación [op.acc.5]; ambas medidas (4.1.2 y 4.2), citadas expresamente en el acuerdo de incoación y la propuesta de resolución.

La imputación fáctica a Indra consiste justamente en haber omitido el deber de cambiar la contraseña que el fabricante establecía por defecto en la funcionalidad Liferay. En consecuencia, resulta especialmente trascendente y clarificador todo lo referido específicamente a la autenticación de usuarios.

Ciertamente, la medida "4.1.2 Arquitectura de seguridad [op.pl.2]" establece distintas opciones para la identificación y autenticación de usuarios, entre ellas las "contraseñas". En cualquier caso, si se opta por la opción del uso de contraseñas es inherente al mismo concepto, tal y como se ha expuesto, que la misma tenga carácter "secreto"; característica que, como es obvio, se incumple si se trata de una contraseña que un determinado fabricante incorpora por defecto en sus soluciones, pues esa contraseña es conocida por múltiples clientes de la misma solución y puede incluso, como en éste caso, haberse hecho pública a través de internet.

El apartado 4.2.5 que trata específicamente la autenticación refuerza asimismo la conclusión de que el mantenimiento (no cambio) de una contraseña que se encuentra en una solución tecnológica por defecto por parte del fabricante incumple el ENS. Y es que sea cual sea la opción utilizada para la autenticación de usuarios, debe cumplirse con el fin de garantizar su "seguridad" que (i) " 1. Las credenciales se activarán una vez estén bajo ***el control efectivo del usuario*** ", y (ii) ***Las credenciales estarán bajo el control exclusivo del usuario.*** **"** Ninguno de estos dos requisitos inexcusables se satisfacen, se insiste, si se trata de contraseñas que por defecto había implementado el fabricante de la correspondiente solución tecnológica, pues las credenciales en ningún momento están bajo el control exclusivo del usuario en la medida que se trata de una clave conocida por terceros (otros adquirentes de la solución, el propio productor de la misma, quien tenga acceso por internet, etc.).

En términos más llanos, el propio RGPD y, en un grado mayor de concreción el ENS, lo que establecen es que -entre otras dimensiones - es necesario proteger la confidencialidad de la información. Esto se logra principalmente estableciendo mecanismos de acceso (puerta) de tal modo que únicamente pueda acceder a la información quien esté autorizado para hacerlo (quien tenga la llave para abrir la puerta). Este mecanismo de protección sería ineficaz si

estas claves fueran conocidas por todos (fabricante, internautas, otros compradores de la solución, etc.). Es evidente que ni del RGPD ni del ENS se puede extraer la conclusión de que una situación como la descrita pueda ser válida, dado que confrontaría directamente con el propósito perseguido de protección de la confidencialidad y, además, iría en contra del que cuando se definen particularmente las medidas de autenticación se exige: contraseñas como algo intrínsecamente secreto y, por tanto, de control "exclusivo" por parte del usuario. Exigir colocar una puerta que pudiera abrir cualquiera no tendría ningún sentido práctico más allá de generar una mera apariencia de seguridad cuando ésta es inexistente.

En resumen, el uso de contraseña como medio de autenticación requiere que la información utilizada sea "secreta" ya que es una propiedad que le es inherente, porque si la contraseña es conocida se incumple el requisito de que esta información/clave esté bajo el control exclusivo del usuario.

2.2.3 La aplicación integral de la obligación de establecer un eficaz control de acceso.

La última de las alegaciones planteada por Indra con el fin de intentar sostener que no habría incumplido las medidas de seguridad de nivel básico exigidas, consiste en apuntar que la obligación de que la contraseña sea secreta y bajo el control exclusivo del usuario no resultaría de aplicación en la medida en que: (i) únicamente estaría previsto por los "equipos" y que, (ii) teniendo en cuenta – a su juicio – que los equipos no tienen software, esta obligación no resultaría de aplicación a el asunto objeto del expediente puesto que Liferay es un software.

Con carácter preliminar debe contextualizarse que, tal y como ya se ha expuesto, la obligación de protección de la confidencialidad se proyecta por todos los tratamientos de protección de datos en virtud del RGPD y, en consecuencia, no depende de qué elemento técnico concreto se utilice para llevar a cabo el tratamiento. Similarmente, las medidas indicadas del ENS (4.1.2 y 4.2 – y singularmente el 4.2.5.-) hacen referencia de forma consistente al conjunto del sistema de información ya sus propios recursos:

> 4.1.2 " *La Seguridad del sistema será objeto de un planteamiento integral detallando, al menos, los siguientes aspectos* [...]"
>
> 4.2 " *El control de acceso cubre el conjunto de actividades preparatorias y ejecutivas para que una determinada entidad, usuario o proceso, pueda, o no, acceder a un recurso del sistema para realizar una determinada acción* "
>
> 4.2.5 " *Los mecanismos de autenticación frente al sistema* [...]"

Se constata que estas exigencias no son susceptibles de verse alteradas en función de la naturaleza específica de que elemento específico se utilice. De hecho, teniendo en cuenta que Indra asume que Liferay es en cualquier caso un componente del sistema (pág. 10 de las alegaciones al acuerdo de incoación), las medidas 4.1.2 y 4.2 -y singularmente la 4.2. 5- le serían indudablemente de aplicación. Más cuando, justamente en relación con los "componentes del sistema, el apartado 4.2.2 Requisitos de acceso [op.acc.2] refuerza la importancia de controlar los accesos justamente a los distintos componentes del sistema (apartado c):

c *) Particularmente se controlará el acceso a los componentes del sistema ya sus archivos o registros de configuración.* ”

En consecuencia, esta alegación no puede desvirtuar las consideraciones expuestas en los dos subapartados precedentes. Y esto porque Liferay forma parte del sistema, que el propio ENS se encarga de definir en su anexo IV como el “ *Conjunto organizado de recursos para que la información se pueda recoger, almacenar, procesar o tratar, mantener, usar, compartir, distribuir, poner a disposición, presentar o transmitir* .” Es decir, que cuando las medidas indicadas se refieren a la protección del sistema de la información implica el aseguramiento del conjunto de recursos que se utilizan para llevar a cabo el tratamiento de la información incluido el software (Liferay).

Dicho de otra forma, es incorrecto afirmar que el cambio de contraseñas sólo afecta a una tipología específica “equipos”, cuando la protección de la información tiene una vocación de ser integral en el sentido de que la protección del conjunto del sistema pasa, obviamente, para asegurar el conjunto de elementos que lo conforman (uno de ellos, según Indra, el software) y, tal y como se ha explicado en los dos subapartados anteriores, la protección de la confidencialidad, y las obligaciones específicas del ENS , conllevan necesariamente cambiar las contraseñas que pudieran haber instaladas por defecto por parte del fabricante .

En definitiva, la imputación de la infracción a Indra de incumplir la normativa de protección de datos ni incurre ni puede hacerlo en una interpretación extensiva de ningún concepto específico, puesto que la obligación de que las contraseñas sean secretas y bajo el control de el usuario no presenta ninguna dependencia sobre qué elemento se trate (hardware o software...), únicamente que forme parte del sistema que trate la información.

A pesar de que entrar a dar respuesta al resto de alegaciones formuladas por Indra no resultaría necesario a partir de la anterior consideración, se estima oportuno hacerlo con un ánimo, nuevamente, de completitud y, también, para evidenciar la incorrección de su planteamiento.

Así, Indra apunta que es necesario efectuar una separación entre equipos y software situándolos como conceptos antagónicos. Nada más lejos de la realidad. La RAE define “equipo” como “Conjunto de aparatos constituido por una computadora y sus periféricos” y “computadora [electrónica]” como “Máquina electrónica que, mediante determinados programas, permite almacenar y tratar información y resolver problemas de diversa índole” .

Es decir, de nuevo, afirma que es inherente a “equipo” que existan programas para que se puedan llevar a cabo funciones informáticas/electrónicas vinculadas al tratamiento de datos.

Se llega a la misma conclusión de analizar la propia medida apuntada en el marco de este expediente “4.3.2 Configuración de Seguridad [op.exp.2]”, consistente en la obligación de retirar las contraseñas estándar de los “equipos ” con carácter previo a su entrada a producción. Pues la existencia de una contraseña en un entorno informático, como es el caso, implica la presencia de un software que permita justamente contrastar si la contraseña introducida es válida o no.

Así pues, el error de base de carácter técnico en la alegación de Indra conduce también a que la interpretación indebidamente reduccionista que intenta efectuar pierda cualquier sentido, ya no sólo estructural (Liferay es un elemento del sistema), sino también material

(no es posible contraponer software a equipo puesto que el software constituye un aspecto esencial de cualquier equipo informático).

Retornando al principio de este subapartado, incluso por el caso erróneo de que alguien considerase que "equipo" es algo antagónico a "software", cabe recordar que Indra asume que el software en cualquier caso es un "componente del sistema", de tal forma que las obligaciones que se establecen a nivel de sistema le son, sin lugar a dudas, de aplicación. Así, cuando el RGPD y el ENS (art. 1.2) exigen que se proteja la confidencialidad de la información y cuando el ENS especifica que es necesario establecer un control de acceso a nivel de sistemas (4.2.op.acc) es claro que tal obligación se proyecta también hacia el programa Liferay.

Desde un punto de vista material, defender lo contrario equivale a sostener que la confidencialidad se encuentra adecuadamente preservada aunque las contraseñas para acceder como administrador al software -y por tanto para poder efectuar los cambios de máxima trascendencia- sean conocidas por parte de los fabricantes, otros compradores y por internautas en general.

Y, desde una óptica jurídica, asumir la posición de Indra contravendría el propio espíritu y funcionalidad última de la norma así como múltiples preceptos como los indicados e, incluso, otros que recogen ese mismo espíritu: protección de acceso remoto [op.acc.7] *"que nadie accederá a recursos sin autorización. "*

En definitiva, todas y cada una de las medidas específicas a las que ha hecho referencia la instrucción de este expediente tienen carácter "básico", y le eran exigibles a Indra, teniendo en cuenta que en el contrato de encargo suscrito con SocMobilitat se recogía expresamente la obligación de implementar en todo caso las medidas de seguridad que correspondieran a un sistema de categoría básica.

2.3 Sobre la ausencia de culpabilidad.

En la línea de lo anterior, Indra esgrime que de mantenerse la imputación efectuada en la propuesta de resolución, se estaría sancionando a Indra por la materialización de un acceso indebido por un tercero, y no por la falta de aplicación de medidas de seguridad, es decir, se estaría considerando que la seguridad de los datos es una obligación de resultados y no de medios, por lo que carecería el elemento de culpabilidad necesario en su conducta para poder exigirle responsabilidades en la infracción que se le imputa, tal y como dispone el artículo 28 de la Ley 40/2015 de Régimen Jurídico del Sector Público y la jurisprudencia que invoca.

Al respecto, cabe poner de manifiesto en primer lugar que, efectivamente, se coincide con la entidad imputada en la que el principio de culpabilidad, es decir, la necesidad de que exista dolo o culpa en la acción punitiva, es plenamente aplicable al derecho administrativo sancionador. Ahora bien, de acuerdo con lo que ya se ha dicho de forma reiterada en esta resolución, la conducta de vulneración de seguridad de los datos que se imputa a Indra es, precisamente, la falta de implementación de barreras de seguridad exigidas por SocMobilitat para proteger la confidencialidad de los datos registrados en el portal web, y es algo no discutido que el sistema entró en fase de producción con datos reales de usuarios, dejando activadas las credenciales que venían por defecto del fabricante.

Así pues, está claro que en tanto que Indra no implementó medidas de seguridad de nivel básico que le eran exigibles, en su condición de subencargada del tratamiento, incumplió la obligación establecida en el artículo 32.1 del RGPD de proteger la seguridad de los datos, y ésta sin duda es una obligación de medios, siendo pues, responsable de la infracción que se le imputa en este procedimiento, porque su comisión se materializó con independencia de las actuaciones llevadas a cabo por el tercero para acceder en los datos tratados. Dicho de otra forma, la comisión de la infracción sería también imputable a Indra aunque no se hubiera producido el acceso indebido de este tercero.

En resumen, el elemento objetivo del tipo infractor del artículo 83.4.a) del RGPD, se perfecciona desde el momento en que el sistema entró en fase de producción y no implementó medidas de carácter técnico y organizativo necesarias que garantizaran la seguridad de los datos de carácter personal y evitara su alteración, pérdida, tratamiento o acceso no autorizado, y más concretamente medidas de nivel básico, de acuerdo con lo previsto en el citado artículo 32.1 de el RGPD y el contrato que estipulaba las obligaciones de Indra.

Y tampoco resulta admisible su argumento de que el sistema se encontraba en un entorno de pruebas, y que fue el responsable o el encargado de tratamiento, pero en ningún caso Indra, quien ordenó que entrara en producción. Y esto porque se trataba de un entorno de pruebas llevado a cabo por Indra con datos reales de usuarios que estaban expuestos en internet (portal extranet), y las pruebas de software con datos personales constituyen igualmente un tratamiento sujeto a las obligaciones que establece el RGPD y, evidentemente, también las establecidas en el artículo 32.1 del RGPD en lo que respecta a la seguridad de los datos.

En resumen, Indra tenía el deber de cumplir con las obligaciones de seguridad estipuladas en el contrato suscrito con SocMobilitat y actuar con la diligencia necesaria para que la seguridad de los datos personales no se viera comprometida, garantizando que sólo accedían a los datos tratados personas autorizadas, lo que le obligaba a establecer un mecanismo que permitiera la identificación de forma inequívoca y personalizada de cualquier usuario que intentara acceder al sistema de información, circunstancias que no se cumplían en el presente caso, en que, ya fuera por descuido o por “un error operativo”, como se decía en los Tuits publicados por T-Mobilitat en su canal en fechas 05/10/2021 y 06/10/2021 (antecedente 1º), no se modificó la contraseña de carácter público que por defecto asigna el fabricante al administrador, en la fase de pruebas de la implementación de la tarjeta de la T-movilidad, lo que comportó una puerta abierta a la información contenida en la plataforma.

Al respecto hay que hacer referencia a la doctrina jurisprudencial que sostiene que no se requiere una conducta dolosa del infractor, sino que es suficiente la simple negligencia o incumplimiento de los deberes que la Ley impone a las personas responsables de archivos o del tratamiento de datos de extremar la diligencia..." (Sentencia de la Audiencia Nacional de 12/11/2010, recurso n. 761/2009).

En la misma línea se pronuncia el Tribunal Supremo, entre otros, en la sentencia de 25/01/2006, dictada también en el ámbito de protección de datos, cuando afirma que “el principio de culpabilidad consiste en la falta de diligencia observada por la entidad recurrente al tratar de forma automatizada una fecha relativa a la ideología del denunciante, resultando irrelevantes las invocaciones que se hacen (...) acerca de la ausencia de intencionalidad oa la existencia del error, y eso por cuanto el elemento culpabilístico del tipo sancionador

aplicado concurre cuando se incluye la expresada fecha sobre la ideología, no siendo precisa la concurrencia de una intencionalidad específica tendente a revelar datos privados del afectado".

En definitiva, a fin de determinar la concurrencia del elemento culpabilístico no es necesario que los hechos infractores se hayan producido con dolo o intencionalidad, sino que es suficiente que haya intervenido negligencia o falta de diligencia en el cumplimiento de las obligaciones que le son exigibles legalmente, como sería el supuesto aquí analizado, en el que ni siquiera implementó medidas de seguridad de nivel básico que le habían sido concretamente exigidas por vía contractual. Y, es decir, este deber de diligencia es máximo cuando se realizan actividades que afectan a derechos fundamentales, como es el derecho a la protección de datos de carácter personal.

Así lo ha declarado la Sentencia de la Audiencia Nacional de 05/02/2014 (recurso n. 366/2012) dictada en materia de protección de datos, que sostiene que la condición de responsable de tratamiento de datos personales "impone un deber especial de diligencia a la hora de llevar a cabo el uso o tratamiento de las datos personales o su cesión a terceros, en lo que concierne al cumplimiento de los deberes que la legislación sobre protección de datos establece para garantizar los derechos fundamentales y las libertades públicas de las personas físicas, y especialmente su honor e intimidad personal y familiar, cuya intensidad se encuentra potenciada por la relevancia de los bienes jurídicos protegidos por aquellas normas."

En el presente caso, la falta de diligencia es evidente ante el hecho indiscutido de que se dejó configurado el acceso al portal web con la contraseña que viene por defecto del fabricante cuando se estaban tratando datos de usuarios reales, lo que constituye un claro incumplimiento de sus obligaciones en cuanto a las medidas de seguridad que tenía el deber de implementar, y que es imputable a Indra , aunque derive de un error humano de un trabajador, de acuerdo con el sistema de responsabilidad previsto en el RGPD, y particularmente en el artículo 70 del LOPDDDD, en el que se establece que la responsabilidad por las infracciones a la normativa de protección de datos recae, entre otros, sobre los responsables, o en su caso, sobre los encargados de los tratamientos, y no sobre su personal.

En conclusión, en el presente caso es clara la concurrencia del elemento culpabilístico en la conducta de Indra, exigido por la normativa y la jurisprudencia para poder exigirle responsabilidades en la comisión de la infracción imputada en el presente procedimiento sancionador, atendida su carencia de diligencia en el cumplimiento de las obligaciones que le eran exigibles.

2.4 Sobre la adopción de medidas inmediatas.

Al respecto, Indra esgrime que una vez tuvo conocimiento de la vulnerabilidad, que fue publicada a las 15:39 h del mismo día 05/10/2021 en las redes sociales, procedió de forma inmediata a solucionar el incidente.

En este sentido, Indra pone de manifiesto que en tan sólo 61 minutos desde que se tuvo conocimiento del escape de datos, bloqueó "cualquier acceso por parte de terceros no autorizados", y llevó a cabo las siguientes acciones sobre la infraestructura de tecnología Liferay del portal T-movilidad, para mitigar las posibles consecuencias adversas para las personas afectadas, y eliminar los riesgos de nuevos accesos, y en concreto:

• Se dejó sólo un usuario administrador y se le cambió la contraseña.
• Se desconectó la posibilidad nativa de entrar en Liferay.
• Se realizó una auditoría de análisis de gestión de contenidos de Liferay, para verificar el total de contenidos del portal y ordenarlos por fecha de modificación. *De esta forma se pudo certificar que durante el período de tiempo en las que se accedió al portal como administrador hasta que se mitigó la incidiencia, no se realizó ninguna modificación sobre ningún contenido* .

Al respecto, cabe poner de manifiesto que las actuaciones llevadas a cabo por parte de Indra de forma inmediata y en cuanto tuvo conocimiento del incidente, no permiten desvirtuar la infracción que se le imputa por la vulneración de la seguridad de las datos, si bien se tienen en cuenta como circunstancia atenuante en la cuantificación de la sanción, de acuerdo con el análisis que se realiza en el fundamento de derecho 5º de esta resolución, y despliegan efectos en cuanto al hecho de que en el presente procedimiento no deba exigirse la adopción de medidas correctoras para corregir los efectos de la infracción cometida.

2.5 Sobre la carencia de daños y perjuicios.

Por último, en el apartado de conclusiones, y como última alegación para justificar su solicitud de sobreseimiento del procedimiento, Indra esgrime que el incidente de seguridad que se produjo no habría tenido consecuencias negativas para las personas afectadas, es decir, que no se habrían generado daños y perjuicios.

Al respecto, cabe decir que entre los elementos objetivos que conforman el tipo infractor previsto en el artículo 83.4.a) del RGPD no se incluye la necesidad de que la persona titular de los datos, en relación a los cuales se ha producido la infracción, considere vulnerada su privacidad o intimidad. El tipo sólo requiere , como se ha dicho, la falta de adopción de las medidas técnicas y organizativas para garantizar un nivel de seguridad adecuado al riesgo del tratamiento, en los términos exigidos en el artículo 32.1 del RGPD.

En cualquier caso, cabe recordar que en el presente expediente sancionador constan hasta siete denuncias de personas que han entendido vulnerada la privacidad de sus datos a raíz de la infracción imputable a Indra.

Por todo lo expuesto hasta aquí, no pueden tener éxito las alegaciones formuladas por la entidad imputada a la propuesta de resolución.

3 . En relación con la conducta descrita en el apartado de hechos probados, relativa a la falta de aplicación de las medidas de seguridad de nivel básico exigidas para garantizar un nivel de seguridad adecuado al riesgo, es necesario acudir, como se ha dicho, a el artículo 32.1 del RGPD, que dispone que:

"1. Teniendo en cuenta el estado de la técnica, las costas de aplicación, y la naturaleza, el alcance, el contexto y las fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros:

a) la seudonimización y el cifrado de datos personales;

b) la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento;
c) la capacidad de restaurar la disponibilidad y el acceso a las datos personales de forma rápida en caso de incidente físico o técnico;
d) un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento."

Como se ha dicho también, respecto a la conducta descrita en los hechos probados, se considera que Indra ha vulnerado medidas de seguridad, de nivel básico, del Esquema Nacional de Seguridad (ENS) aprobado por Real Decreto 3/2010, y aplicable a Indra, de acuerdo con la disposición adicional primera de la LOPDDDD (Medidas de seguridad en el ámbito del sector público), por razón del contrato de encargo firmado con SocMobilitat, que le fueron exigidas en dicho contrato. Y en concreto se vulneraron las medidas que se detallan a continuación:

1. El apartado 4.1.2 *"Arquitectura de Seguridad"* del Anexo II ("Medidas de Seguridad") del ENS, determina lo siguiente:

La seguridad del sistema será objeto de un planteamiento integral detallando, al menos, los siguientes aspectos:
Categoría BÁSICA
a) (…)
d) Sistema de identificación y autenticación de usuarios:

1. Uso de claves concertadas, contraseñas, tarjetas de identificación, biometría, u otras de naturaleza análoga.
(...)

2. El apartado 4.2 relativo al control de acceso, determina lo siguiente:

"El control de acceso cubre el conjunto de actividades preparatorias y ejecutivas para que una determinada entidad, usuario o proceso, pueda, o no, acceder a un recurso del sistema para realizar una determinada acción.

El control de acceso que se implante en un sistema real será un punto de equilibrio entre la comodidad de uso y la protección de la información. En sistemas de nivel Bajo, se primará la comodidad, mientras que en sistemas de nivel alto se primará la protección.

En todo control de acceso se requerirá lo siguiente :
a) Que todo acceso esté prohibido, salvo concesión expresa.
b) Que la entidad quede identificada singularmente [op.acc.1].
c) Que la utilización de los recursos esté protegida [op.acc.2].
d) Que se definan para cada entidad los siguientes parámetros: a qué se necesita acceder, con qué derechos y bajo esa autorización [op.acc.4].
e) Serán diferentes las personas que autoricen, usen y controlen el uso [op.acc.3].
f) Que la identidad de la entidad quede suficientemente autenticada [op.acc.5].
g) Que se controle tanto el acceso local ([op.acc.6]) como el acceso remoto ([op.acc.7]).

Con el cumplimiento de todas las medidas indicadas se garantizará que nadie accederá a recursos sin autorización. Además, quedará registrado el uso del sistema ([op.exp.8]) para poder detectar y reaccionar a cualquier fallo accidental o deliberado.

Cuando se interconecten sistemas en los que la identificación, autenticación y autorización tengan lugar en diferentes dominios de seguridad, bajo distintas responsabilidades, en los casos en que sea necesario, las medidas de seguridad locales se acompañarán de los correspondiente acuerdos de colaboración que delimiten mecanismos y procedimientos para la atribución y ejercicio efectivos de las responsabilidades de cada sistema ([op.ext]).”

3. Y por último, el apartado 4.3.2 relativo a la “Configuración de Seguridad”, que determina lo siguiente:

“Se configurarán los equipos previamente a su entrada en operación, de forma que:
a) Se retiran cuentas y contraseñas estándar.
b) Se aplicará la regla de "mínima funcionalidad": (…)”

Así pues, en caso de que nos ocupa ha quedado acreditado que el subencargado del tratamiento, Indra, no aplicó medidas técnicas de nivel básico, exigidas por SocMobilitat para garantizar un nivel de seguridad adecuado al riesgo (tendentes a evitar que a estos datos pudieran acceder personas no autorizadas), dado que al configurar el control de acceso al portal web de la T-Movilidad, no se modificó la contraseña que por defecto asigna el fabricante de la infraestructura de tecnología “Liferay” al administrador, de tal modo que el acceso quedaba abierto, ya su vez, accesible a terceros.

Este hecho recogido en el apartado de hechos probados constituye la infracción prevista en el artículo 83.4.a) del RGPD, que tipifica como tal la vulneración de “las obligaciones *del responsable y del encargado a tenor de los artículos 8, 11, 25 a 39, 42 y 43”* , entre las que se encuentra la prevista en el artículo 32.1 del RGPD.

Dicho esto, la conducta que aquí se aborda se ha recogido como infracción grave en el artículo 73.f) de la LOPDDDD, en la siguiente forma:

"f) La falta de adopción de las medidas técnicas y organizativas que sean apropiadas para garantizar un nivel de seguridad adecuado al riesgo del tratamiento, en los términos que exige el artículo 32.1 del Reglamento (UE) 2016/679."

4 . En el contrato de encargado del tratamiento suscrito entre SocMobilitat e Indra, como se ha dicho también, se estipulaba, que Indra debía adoptar las medidas de nivel básico del ENS para garantizar un nivel de seguridad adecuado al riesgo, y así se hacía constar lo siguiente:

“7. Obligaciones del encargado del tratamiento (...)
“7.5. Seguridad del Tratamiento
*El encargado del Tratamiento implantará las Medidas apropiadas respecto a la seguridad del Tratamiento, que se correspondan con las de la Administración contratante y que se ajustan al Esquema Nacional de Seguridad (**NIVEL BÁSICO**).*
En todo caso, el Encargado deberá implantar mecanismos para:
a. Garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de Tratamiento.

b. Restaurar la disponibilidad y acceso a las Datos personales de forma rápida, en caso de incidente físico o técnico.
c. Verificar, evaluar y valorar de forma regular, la eficacia de las medidas técnicas y organizativas implantadas para garantizar la seguridad del tratamiento.
d. Seudonimizar y cifrar las Datos personales, en su caso.
En conjunto, deberá adoptar todas aquellas otras medidas que, teniendo en cuenta el conjunto de tratamientos que realiza, sean necesarias para garantizar un nivel de seguridad adecuado al riesgo.
La documentación relacionada con la gestión de los riesgos, incluyendo el resultado de las auditorías periódicas que se realicen, puede ser solo solicitada en cualquier momento por el responsable del Tratamiento."

A este respecto, el apartado décimo del artículo 28 del RGPD, dispone lo siguiente:

10. Sin perjuicio de lo dispuesto en los artículos 82, 83 y 84, si un encargado del tratamiento infringe el presente Reglamento al determinar los fines y medios del tratamiento, se le considerará responsable del tratamiento en lo que se refiere a dicho tratamiento ."

Esto es también aplicable al subencargado del tratamiento, de acuerdo con lo que dispone el artículo 28.4 del RGPD y 70.1.b) LOPDGDD (que se considera, en todo caso, un encargado del encargado del tratamiento), y , por tanto, es también responsable, ante la autoridad de control, de las presuntas vulneraciones de la normativa de protección de datos que pueda cometer en el desarrollo del encargo (prestaciones técnicas encomendadas), y en concreto de la falta de aplicación de las medidas de nivel básico exigidas en el mismo encargo, en la configuración del portal de acceso a la T-Mobilitat, sin necesidad de requerir, como se ha dicho, la adopción de ninguna medida correctora, ya que Indra ha acreditado haber tomado las medidas adecuadas para solucionar el incidente de seguridad detectado en la plataforma.

5. Al no incluirse la entidad Indra Sistemas SA, en ninguno de los sujetos previstos en el artículo 77.1 del LODGDD, resulta de aplicación el régimen sancionador general previsto en el artículo 83 del RGPD.

El artículo 83.4 del RGPD prevé para las infracciones allí previstas, se sancionen con una multa administrativa de 10.000.000 de euros como máximo, o tratándose de una empresa, de una cuantía equivalente al 2% como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía.

Dicho esto, corresponde determinar la cuantía de la multa administrativa que procede imponer. Según lo establecido en el artículo 83.2 del RGPD, y también de conformidad con el principio de proporcionalidad consagrado en el artículo 29 de la Ley 40/2015, corresponde imponer la sanción de 23.500 euros (veintitrés mil cinco -cientos euros). Esta cuantificación de la multa, en un importe minorado respecto a lo propuesto por la instructora del procedimiento, tras considerar que no concurre una de las circunstancias agravantes contempladas en la propuesta de resolución, se basa en la ponderación de los criterios agravantes y atenuantes que a continuación se indican:

Como criterios atenuantes, se observa la concurrencia de las siguientes causas:

– La naturaleza, gravedad y duración de la infracción (art.83.2.a).

- Haber realizado medidas inmediatas para corregir los efectos de la infracción.

- La falta de intencionalidad (art.83.2.b) RGPD).

- La falta de constancia de la obtención de beneficios como consecuencia de la infracción (art. 83. 2. k) RGPD y 76.2.c) LOPDGDD).

No resultan de aplicación otros criterios atenuantes invocados por Indra en su alegación quinta, en concreto la atenuante prevista en el artículo 83.2.g) del RGPD, y la prevista en el art.76.2.d) de la LOPDDDD, en tanto que, con respecto al primero, la naturaleza de datos afectados ya se ha tenido en cuenta a la hora de aplicar la atenuante prevista en el art.83.2.a) del RGPD, y que, en lo que se refiere al segundo, la actuación de un tercero no ha tenido ninguna incidencia en la comisión de la infracción que aquí se imputa, como ya se ha dicho de forma reiterada.

Por otro lado, como criterio agravante, hay que tener en cuenta el siguiente elemento :

- La vinculación de la actividad de Indra con la realización de tratamientos de datos personales, al tener como actividad principal la prestación de servicios de consultoría en diferentes ámbitos, que implica el tratamiento de datos personales en las operaciones y proyectos que ejecuta para los sus clientes (como consta en la web https://www.indracompany.com/es/indra/privacidad-proteccion-datos).

Sin embargo, no resulta de aplicación el criterio agravante contemplado en la propuesta de resolución referente al artículo 83.2.e) del RGPD, en tanto que ha quedado acreditado que la entidad sancionada con anterioridad, era Indra BMB Servicios Digitales SL , que tiene personalidad jurídica independiente de la entidad aquí imputada, lo que debe comportar la reducción de la cuantía de la sanción propuesta por la persona instructora.

Por todo esto, resuelvo:

1 . Imponer a Indra Sistemas, SA la sanción consistente en una multa de 23.500.- euros (veintitrés mil quinientos euros), como responsable de una infracción prevista en el artículo 83.4.a) en relación con el artículo 32.1, ambos del RGPD, sin necesidad de requerir medidas correctoras de acuerdo con lo expuesto en el fundamento de derecho cuarto.

2 . Notificar esta resolución a Indra Sistemas, SA.

3 . Ordenar que se publique esta resolución en la web de la Autoridad (apdcat.gencat.cat), de conformidad con el artículo 17 de la Ley 32/2010, de 1 de octubre.

Contra esta resolución, que pone fin a la vía administrativa de acuerdo con los artículos 26.2 de la Ley 32/2010, de 1 de octubre, de la Autoridad Catalana de Protección de Datos, y 14.3 del Decreto 48/2003 , de 20 de febrero, por el que se aprueba el Estatuto de la Agencia Catalana de Protección de Datos, la entidad imputada puede interponer, con carácter potestativo, un recurso de reposición ante la directora de la Autoridad Catalana de Protección de Datos Datos, en el plazo de un mes a contar desde el día siguiente de su notificación, de acuerdo con lo que prevén el artículo 123 y siguientes de la LPAC. También

puede interponer directamente un recurso contencioso administrativo ante los Juzgados de lo Contencioso-Administrativo, en el plazo de dos meses a contar desde el día siguiente de su notificación, de acuerdo con los artículos 8, 14 y 46 de la Ley 29/1998, de 13 de julio, reguladora de la jurisdicción contencioso-administrativa.

Si la entidad imputada manifiesta a la Autoridad su intención de interponer recurso contencioso administrativo contra la resolución firme en vía administrativa, la resolución se suspenderá cautelarmente en los términos previstos en el artículo 90.3 de la LPAC.

Igualmente, la entidad imputada podrá interponer cualquier otro recurso que estime conveniente para defender sus intereses.