- Expediente N.º: EXP202301217

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos y teniendo como base los siguientes:

HECHOS

PRIMERO: Con fecha 23 de enero de 2023, tiene entrada en la División de Innovación Tecnológica de esta Agencia la notificación de una brecha de seguridad de datos personales por parte del responsable de tratamiento EDISTRIBUCIÓN REDES DIGITALES, S.L. (en adelante ERD o entidad notificante) relativa a la publicación en un repositorio de internet de credenciales de acceso a una base de datos que contiene CUPS y datos de consumo.

El resumen de los datos contenidos en la notificación es el siguiente:

- Descripción de lo ocurrido: ***(…)***

- Encargado del tratamiento: ENGINEERING INGEGNERIA INFORMATICA S.P.A (en adelante EII)

- Fecha de detección de la brecha: 20 de enero de 2023

- Fecha de inicio de la brecha: 10 de enero de 2023 (fecha exacta)

- Fecha de finalización de la brecha: 20 de enero de 2023

- Brecha de confidencialidad

- Número de afectados según notificación: 12.000.000

- Tipología de los datos según notificación: Datos básicos (Ej: nombre, apellidos, fecha de nacimiento)

- Indican que no han comunicado la brecha a los afectados.

- No indican afectados en otros países.

SEGUNDO: Con fecha 31 de enero de 2023, la Directora de la Agencia Española de Protección de Datos instó a la Subdirección General de Inspección de Datos (SGID) a iniciar las actuaciones previas de investigación a las que se refiere el artículo 67 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, LOPDGDD) para investigar a EDISTRIBUCIÓN REDES DIGITALES, S.L., ENGINEERING INGEGNERIA INFORMATICA S.P.A y ENGINEERING INGEGNERIA INFORMATICA SPAIN S.L., en

relación con los siguientes hechos:

Tras los requerimientos de información solicitados tanto al responsable del tratamiento ERD (con fechas 28 de marzo de 2023 y 28 de julio de 2023) como a la sede española del encargado del tratamiento EII (con fecha 28 de julio de 2023), se ha obtenido la siguiente documentación:

o Escrito procedente de ERD, de fecha 21 de abril de 2023. que incluye los siguientes anexos:

- Documento número 1: Escritura de apoderamiento (Págs. 18-40)
- Documento número 2: Primer informe de valoración realizado con fecha 23 de enero de 2023 tras la reunión mantenida por las áreas de ******ÁREA.1, ***ÁREA.2, ***ÁREA.3, ***ÁREA.4***. (Págs. 41-46)
- Documento número 3: Segundo informe de valoración de la Brecha realizado con fecha 1 de febrero de 2023. (Págs. 47-52)
- Documento número 4: Intercambio de comunicaciones internas. (Págs. 53-55)
- Documento número 5: Justificante de presentación de notificación de la brecha de seguridad. (Págs. 56-63)
- Documento número 6: Comunicación interna remitida al Delegado de Protección de Datos en la que se pone de manifiesto que no había constancia de que se hubiera producido el acceso a los datos personales incluidos en el servidor FTP (Págs. 64-65)
- Documento número 7: Procedimiento “Sistemas de Información de Medidas Eléctricas. Ficheros para el intercambio de información de medida (Versión 40, octubre de 2022)” (Págs. 66-317)
- Documento número 8: Correo electrónico remitido ***(…)***. (Págs. 318-321)
- Documento número 9: Credenciales de acceso al servidor FTP (Págs. 322-323)
- Documento número 10: Muestra de los ficheros logs obtenidos como resultado del análisis de todos los accesos registrados en el servidor FTP durante el 1 y el 24 de enero de 2023. (Págs. 324-330)
- Documento número 11: Acreditación de que no se ha encontrado en internet ningún tipo de referencia a la publicación de los datos incluidos en el servidor FTP en el periodo comprendido entre el 1 de enero y el 1 de abril de 2023. (Págs. 331-332)
- Documento número 12: Confirmación del servicio ***(…)*** de que no se han publicado en internet los datos incluidos en el servidor FTP. (Págs. 333-335)
- Documento número 13: Copia del Registro de Actividades del Responsable del tratamiento, relativo al tratamiento “MED - curva carga comercializadoras” (Págs. 336-346)
- Documento número 14: Copia del Registro de incidentes que ERD donde puede apreciarse registrado el incidente “Información publicada en repositorio público de Github” (Págs. 347-348)
- Documento número 15: Análisis de riesgo realizado (Págs. 349-353)
- Documento número 16, Evaluación de Impacto del tratamiento donde se ha producido la violación de seguridad de los datos personales (Págs. 354-490)
- Documento número 17: Contrato de desarrollo, mantenimiento y soporte de software con EII, con fecha 24 de diciembre de 2018. (Págs. 491-509)
- Documento número 18: copia de las comunicaciones intercambiadas con EII.

(Págs. 510-514)

- Escrito procedente de ERD, de fecha 11 de agosto de 2023, que incluye los siguientes anexos:

  - Documento número 1: Acreditación de actividades de formación y concienciación entre los empleados de EII, en relación con la importancia del cumplimiento de buenas prácticas que garanticen la seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental. (Pág. 15)
  - Documento número 2, Análisis de riesgos al completo sobre el sistema Exabeat. (Pág. 20)
  - Documento número 3: Política núm. 1097 “Normas de comportamiento para personas digitales”. (Pág. 21)
  - Documento número 4: Anexo IX: Manual sobre la Gestión de Incidentes de Seguridad que forma parte del Procedimiento Organizativo 2393 de protección de datos personales. (Pág. 53)
  - Documento número 5: Procedimiento Organizativo 2484 de seguimiento de implantación de medidas correctivas asociadas a los incidentes de seguridad. (Pág. 70)
  - Documento número 6: Evidencia del inicio del proceso de análisis del incidente de seguridad, una vez se detectó la afectación de datos de carácter personal y se recopiló toda la información necesaria para la correcta valoración de la situación y sus potenciales efectos. (Pág. 76)
  - Documento número 7: Evaluaciones del riesgo sobre los derechos y libertades de los Interesados afectados. (Pág. 78)
  - Documento número 8: Registro del incidente de seguridad. (Pág. 89)
  - Documento número 9: Justificante de notificación ante la Agencia Española de Protección de Datos de la Brecha de seguridad. (Pág. 108)
  - Documento número 10: Procedimiento organizativo 36: Desarrollo de Soluciones y Gestión de Entregas (en adelante “OP36”) que describe la entrega, mejora o reparación de soluciones de TI, garantizando la cobertura integral del ciclo de vida global del software desarrollado, incluidas las actividades de gestión de entregas, tanto desde el punto de vista de las aplicaciones, como de las infraestructuras. (Pág. 190)
  - Documento número 11: Ejemplo de la puesta a disposición de la normativa interna a través de una red interna denominada “Intranet” para el acceso de los empleados internos del grupo empresarial al que pertenece ERD. (Pág. 272)
  - Documento número 12: Convocatorias de las sesiones formativas impartidas a los proveedores relacionadas, concretamente, con el cumplimiento de la OP36 del grupo empresarial al que pertenece ERD. (Pág. 274)
  - Documento número 13: Listado de repositorios que ERD permite utilizar a EII. (Pág. 281)

- Escrito procedente de EII, de fecha de 17 de agosto de 2023, que incluye los siguientes anexos:

  - Documento número 1: RGP01_0_Regolamento_uso_risorse_aziendali. (Pág. 7)

- Documento número 2: Communication channel e-mail . (Pág. 30)
- Documento número 3: ISM04 Policy Sicurezza Infraestructture IT di Gruppo . (Pág. 34)
- Documento número 4: ISM04_e Group IT Infraestructure ***ÁREA.1 Policy. (Pág. 41)
- Documento número 5: ISM04A01 Misure e Presidi Protocolli di rete. (Pág. 48)
- Documento número 6: ISM04A01_e ***ÁREA.1 Measures and Controls Network Protocols. (Pág. 54)
- Documento número 7: Capturas portal de empleados con la información de EXABEAT. (Pág. 59)
- Documento número 8: Procedimientos para el Deploy. (Pág. 61)
- Documento número 9: Declaración-08-23. (Pág. 77)
- Documento número 10: Normativa empleados_ENGINEERING. (Pág. 79)
- Documento número 11: Infografía Gestión Brechas_ ENGINEERING INGEGNERIA INFORMATICA SPAIN, SL. (Pág. 92)
- Documento número 12: Infografía Procedimiento Derechos_ ENGINEERING INGEGNERIA INFORMATICA SPAIN, SL. (Pág. 94)
- Documento número 13: Infografía Política Protección de Datos_ENGINEERING INGEGNERIA INFORMATICA SPAIN, SL. (Pág. 96)
- Documento número 14: Certificado Prodat Adecuación RGPD_ENGINEERING INGEGNERIA INFORMATICA SPAIN, SL. (Pág. 98)
- Documento número 15: Normativa Empleados_ENGINEERING_IS. (Pág. 100)

Respecto de la empresa

La entidad notificante ERD es una sociedad limitada de nacionalidad española. Se trata de una gran empresa filial de grupo con 2.562 empleados fijos y 53 empleados no fijos y un volumen de ventas de más de 1.000.000.000 euros, perteneciente al Grupo Económico: ENEL SPA - ITALIA.

ERD es una empresa cuya actividad corresponde a la Distribución de energía eléctrica.

ERD tiene como proveedor a Amazon AWS y a EII en calidad de encargado del tratamiento.

.- Amazon Web Services (en adelante AWS) es una plataforma de servicios de nube que proporciona una variedad de servicios de infraestructura, entre otros, almacenamiento, bases de datos, …

.- EII es la empresa principal de un grupo de ingeniería especializado en servicios de ingeniería informática. El grupo tiene sede en España a través de la empresa ENGINEERING INGEGNERIA INFORMATICA SPAIN, S.L.

GitHub es una plataforma para alojar proyectos (código fuentes de aplicaciones y herramientas).

Respecto de la cronología de los hechos. Acciones tomadas con objeto de minimizar los efectos adversos y medidas adoptadas para su resolución final

A continuación, se describen de manera cronológica y detallada los hechos ocurridos en torno a la Brecha junto con las evidencias aportadas:

. - 10 de enero de 2023:

(…).

. - 11 de enero de 2023:

- Se elimina el repositorio de Github

- (…).

. - 12-17 de enero de 2023: ***(…).***

. - 17 de enero de 2023: ***(…).***

. - 17-20 de enero de 2023: ***(…)***.
Se confirma que el incidente ha tenido lugar como consecuencia de un fallo humano.

. - 20 de enero de 2023:

- Se detecta que el servidor FTP se utilizaba para compartir información entre ERD y las compañías comercializadoras, en el que se incluía el CUPS y las curvas de carga horaria de los puntos de suministro ubicados en la red de ERD.

- Comienzan los trabajos para determinar las implicaciones de la publicación de dicha información incluida en el servidor FTP y analizar las medidas de seguridad que se debían adoptar para mitigar los posibles efectos derivados de dicha publicación.

. - 23 de enero de 2023:

- Se realiza una valoración del incidente. (Valoración aportada)

- Notificación de la brecha.

. - 25 de enero de 2023:

- Fin del reseteo de las contraseñas comprometidas que estaban incluidas en el servidor FTP.

- Análisis de todos los registros de acceso al servidor FTP afectado: se concluye que no hay constancia de que se haya producido el acceso a los datos personales incluidos en el servidor FTP.

. - 1 de febrero de 2023:

- Segunda valoración del incidente (Valoración aportada)

- Notificación desde AEPD: la brecha se incorpora al registro de notificaciones.

Tras revisar los informes elaborados por el DPD, las comunicaciones internas entre el equipo del DPD y las distintas áreas implicadas en la resolución de la Brecha, los intercambios de correo electrónicos, los logs y la documentación aportada, se corroboran los hechos cronológicos expuestos anteriormente.

ERD indica las medidas en respuesta al incidente y las soluciones implantadas, enumeradas en las valoraciones del incidente por parte del DPD que se han aportado como evidencia*:*

(…)

De la misma forma, en paralelo por parte de EII:

. (…).

Respecto al análisis de los logs de acceso al servidor FTP presuntamente comprometido, ERD especifica en su primer escrito de respuesta:

(…)

Se han cotejado las credenciales de acceso aportadas documentalmente con el listado de los logs de todos los accesos registrados en el servidor FTP durante el 1 y el 24 de enero de 2023 y se ha confirmado que los accesos fueron internos.

Respecto de las causas que hicieron posible la brecha

Tal y como ERD especifica en su escrito de respuesta, el día 10 de enero de 2023 uno de los programadores noveles de EII, "*realizó una copia de parte del código fuente de EXABEAT, con el objetivo de familiarizarse con el funcionamiento de dicho sistema realizando modificaciones y pruebas del software de EXABEAT sin interferir con el funcionamiento de la versión en "producción"*".
[…]

"*Conviene poner de manifiesto que* ***(…).***

Adicionalmente, existen repositorios como Github, que pueden ser utilizados por cualquier persona para alojar proyectos personales. Estos repositorios públicos pueden ser además configurados tanto con acceso restringido, como de acceso público."

El programador de EII "*realizó la copia de los códigos fuente en un repositorio de Github que inadvertidamente había dejado configurado con acceso público, quedando el código fuente de EXABEAT visible por terceros*. *En este sentido, cabe señalar que, como parte de un código fuente,* ***(…)****.*

(…)

Por su parte, EII indica:

"El incidente de seguridad que tuvo lugar consistió en un error humano, por la falta de cumplimiento de las normas de la empresa, que (entre otras) prohíben el uso, durante las funciones laborales, de software y servicios de uso personal. En cualquier caso, una vez que se tuvo conocimiento del suceso, ese mismo día, la empresa inmediatamente aplicó las medidas necesarias para poner fin al incidente, (…)"

Consultada EII por el motivo por el cual el programador novel utilizó un repositorio público como Github en vez de usar los repositorios protegidos de trabajo de los que dispone EII para poder realizar modificaciones de prueba, EII explica que:

(…)

Por otra parte, ERD (…) proporciona el listado de repositorios que ERD permite utilizar a EII, (…).

Respecto de los datos afectados

(…)

ERD aporta el Procedimiento "Sistemas de Información de Medidas Eléctricas. Ficheros para el intercambio de información de medida (Versión 40, octubre de 2022)".

Respecto del contrato de encargado del tratamiento

El responsable ERD aporta copia del Contrato de desarrollo, mantenimiento y soporte de software con EII en cuya cláusula 9 se especifica el tratamiento de datos de carácter personal, actuando esta entidad en calidad de responsable y EII como encargada del tratamiento.

El objeto del contrato es la prestación de los servicios de desarrollo y mantenimiento de aplicaciones de los sistemas y procesos de ENEL con cobertura en España.

(…)

Las obligaciones del Encargado de tratamiento establecen:

- Apartados a) y b) - "Utilizar los datos personales solo para la finalidad objeto del contrato y Garantizar que las personas encargadas del tratamiento lo hacen de acuerdo con las instrucciones del responsable del Tratamiento" (RGPD art. 28.3.a)

- Apartado e) - "No subcontratar con ningún tercero sin la previa autorización escrita del responsable del tratamiento"

- Apartados g) y h) - "Mantener el deber de secreto respecto a los datos de carácter personal a los que haya tenido acceso en virtud del contrato, incluso después de que finalice su ejecución y Garantizar que las personas autorizadas para tratar datos personales se comprometan, de forma expresa y por escrito, a respetar la confidencialidad y a cumplir las medidas de seguridad correspondientes, de las que

hay que informarles convenientemente" (RGPD art. 28.3.b)

- *Apartado q)* - Referencia a medidas de seguridad (RGPD art. 28.3.c)

(el subrayado ha sido incorporado por la Agencia)

Respecto de las medidas de seguridad implantadas

(…)

EII aporta el documento "RGP01_0_Regolamento_uso_risorse_aziendali" (Normas de uso de los recursos de la empresa) dirigido a regular toda la actividad y los comportamientos que tienen que ver con dispositivos laborales y el acceso a los recursos disponibles en la red (conexiones de datos, repositorios, red de intranet e internet, correo electrónico, telefonía fija y móvil).

Entre otras, en este documento se establece lo siguiente (Se añade la traducción desde el italiano, idioma base del documento):

. – (…)
[…]"

También se ha aportado la acreditación de actividades de formación y concienciación entre los empleados de EII, en relación con la importancia del cumplimiento de buenas prácticas que garanticen la seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental.

1.- Realización de una Formación Elearning sobre "Concienciación RGPD Básica", por parte de todos los empleados

2.- Puesta a disposición de diferentes infografías, en materia de brechas de seguridad y política de privacidad en la intranet corporativa.

3.- Firma de un documento, llamado Normativa de Protección de Datos para el personal laboral y colaboradores de EII en el que se recoge la información en materia de protección de datos, el deber de confidencialidad y secreto, y las medidas de seguridad obligatorias para todos los trabajadores/colaboradores. EII refiere que este documento se actualiza anualmente.

(…)

ERD aporta el análisis de riesgo realizado, en el que se evalúan satisfactoriamente las medidas de seguridad adoptadas en el sistema EXABEAT relativas al incidente y se aprecia el estado de cumplimiento de los aspectos relacionados con el tratamiento de los datos de CUPS y de la curva de carga horaria de los clientes.

ERD también proporciona la Evaluación de Impacto del tratamiento donde se ha producido la violación de seguridad de los datos personales, así como el Registro

de Actividades del tratamiento y el Registro de incidentes donde se ha registrado el incidente “Información publicada en repositorio público de Github”.

(…)

Se revisa el contrato y se confirma por parte del Encargado la obligación del deber de secreto y compromiso de confidencialidad.

(…)

Aporta un anexo con la comunicación que se envía al personal en este aspecto, que contiene correos electrónicos y capturas de la intranet informando sobre temas de ciberseguridad y avisando sobre el incidente de seguridad ocurrido. También proporciona las políticas de seguridad tanto en italiano como en inglés.

(…)

Respecto de la notificación con posterioridad a las 72 horas

ERD indica que, tal como se ha expuesto en el orden cronológico de los hechos, fue el día 20 de enero de 2023 cuando se detectó que el servidor FTP***, (…)***, lo cual requería una valoración del impacto en los derechos y libertades de los interesados.

Con anterioridad a esa fecha, únicamente se había podido determinar que en el repositorio Github se había publicado una copia del código fuente del aplicativo EXABEAT de ERD, no pudiéndose conocer entonces si dicha publicación no autorizada había supuesto un acceso a datos personales y un riesgo para los derechos y libertades de los afectados.

ERD notificó la brecha de datos personales a la División de Innovación Tecnológica de esta Agencia con fecha 23 de enero de 2023.

Respecto de la comunicación a los afectados

En la notificación a esta Agencia respecto de la brecha de confidencialidad, ERD informa que “*no se comunicará a los afectados por la brecha de datos personales”*.

ERD basa esta decisión en el cálculo del nivel de riesgo para los derechos y libertades de las personas físicas afectadas por la brecha, según la Guía para la notificación de brechas de datos personales (mayo 2021), tal como especifica en las valoraciones del incidente por parte del DPD aportadas como evidencia:

Volumen:	*Registros de 12,4 Millones de clientes*	*5*
Tipología de datos	*Datos no sensibles*	*1*
Impacto	*Externo*	*6*
Riesgo:	*5 x (1 x 6)*	***30***

La versión de la guía indica que hay que comunicar a los interesados cualquier

brecha que cumpla simultáneamente las siguientes circunstancias:

• Riesgo con valor cuantitativo superior a 40.
• Ante la coincidencia de dos circunstancias cualitativas (Marcadas en la guía en albero).

La Guía para la notificación de brechas de datos personales, en su versión de junio de 2021, indica que:

"No será necesaria la comunicación a los afectados cuando:

• El responsable ha tomado medidas técnicas y organizativas adecuadas que evitan los riesgos anteriores, minimizan los daños a los derechos y libertades y/o los hacen reversibles.
• El responsable ha tomado con posterioridad a la brecha de datos personales las medidas de protección que mitiguen total o parcialmente el posible impacto para los afectados y garanticen que ya no hay posibilidad de que el alto riesgo para sus derechos y libertades se materialice. Por ejemplo, mediante la identificación y puesta en marcha inmediatamente de medidas como la revocación, cancelación o bloqueo de credenciales de acceso o certificados digitales comprometidos, o mediante el restablecimiento de los servicios y copias de seguridad de los datos de forma que no puedan comprometerse otros datos personales.

La herramienta Comunica-Brecha RGPD ofrece ayuda a los responsables de tratamiento para la toma de decisiones en cuanto a la obligación de comunicar una brecha de datos personales a los afectados."

Información sobre la recurrencia de estos hechos y número de eventos análogos acontecidos en el tiempo

ERD señala que "*en ningún caso el propio servidor FTP o los datos que contenía fueron directamente publicados en Github,* ***(…).*** *En todo caso, los datos del servidor FTP no se han publicado en fuentes externas, así como tampoco se ha detectado que terceros hubieran accedido a esta información.*

El área de Seguridad del Grupo Endesa únicamente ha registrado y documentado un evento similar debido a un incidente ocurrido, con fecha 30 de abril de 2018, que supuso la publicación de ficheros de información interna en un repositorio público de Github".

FUNDAMENTOS DE DERECHO

I
Competencia

De acuerdo con las funciones que el artículo 57.1 a), f) y h) del Reglamento (UE) 2016/679 (Reglamento general de protección de datos, en adelante RGPD) confiere a cada autoridad de control y según lo dispuesto en los artículos 47 y 48.1 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en lo sucesivo LOPDGDD), es competente para

resolver estas actuaciones de investigación 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
Cuestiones previas

En el presente caso, de acuerdo con lo establecido en el artículo 4.1 del RGPD, consta la realización de un tratamiento de datos personales por parte de ERD.

ERD realiza esta actividad en su condición de responsable del tratamiento, dado que es quien determina los fines y medios de tal actividad, en virtud del artículo 4.7 del RGPD.

El artículo 4 apartado 12 del RGPD define, de un modo amplio, las "violaciones de seguridad de los datos personales" como "*todas aquellas violaciones de la seguridad que ocasionen la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos"*.

En el presente caso, consta una brecha de seguridad de datos personales en las circunstancias arriba indicadas, categorizada como una brecha de confidencialidad.

Hay que señalar que la identificación de una brecha de seguridad no implica la imposición de una sanción de forma directa por esta Agencia, ya que es necesario analizar la diligencia de responsables y encargados y las medidas de seguridad aplicadas.

La seguridad de los datos personales viene regulada en los artículos 32, 33 y 34 del RGPD, que regulan tanto la seguridad del tratamiento, la notificación de una violación de la seguridad de los datos personales a la autoridad de control, así como la comunicación al interesado, respectivamente.

III
Seguridad del tratamiento

El artículo 32 del RGPD estipula lo siguiente:

"1. Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los 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 los 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.

2. Al evaluar la adecuación del nivel de seguridad se tendrán particularmente en cuenta los riesgos que presente el tratamiento de datos, en particular como consecuencia de la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.

3. La adhesión a un código de conducta aprobado a tenor del artículo 40 o a un mecanismo de certificación aprobado a tenor del artículo 42 podrá servir de elemento para demostrar el cumplimiento de los requisitos establecidos en el apartado 1 del presente artículo.

4. El responsable y el encargado del tratamiento tomarán medidas para garantizar que cualquier persona que actúe bajo la autoridad del responsable o del encargado y tenga acceso a datos personales solo pueda tratar dichos datos siguiendo instrucciones del responsable, salvo que esté obligada a ello en virtud del Derecho de la Unión o de los Estados miembros."

En el presente caso, en el momento de producirse la brecha de seguridad, no consta que el ERD y EII no dispusiese de medidas de seguridad razonables en función de los posibles riesgos estimados.

Las medidas tomadas por ERD en respuesta al incidente y las soluciones implantadas se consideran adecuadas:

• ***(…)***

De la misma forma, en paralelo por parte del encargado de tratamiento EII:
. – (…).

La brecha tuvo lugar debido a un error humano de uno de los programadores noveles del encargado de tratamiento EII, que realizó una copia del código fuente de EXABEAT (Sistema centralizado de gestión de medidas) en un repositorio de Github que inadvertidamente había dejado configurado con acceso público, quedando el código fuente de EXABEAT visible por terceros.

El código fuente de EXABEAT ***(…)***, por lo que en un primer momento se descarta cualquier potencial acceso externo a dicho aplicativo.

El 20 de enero de 2023 se detecta que, entre las credenciales publicadas, se

encuentran las de un servidor FTP al que se puede acceder desde internet y que contiene el CUPS y las curvas de carga horaria de los puntos de suministro ubicados en la red de ERD. Se valora el incidente y se notifica a la AEPD con fecha 23 de enero de 2023.

ERD ha proporcionado evidencias de que todos los accesos al servidor FTP presuntamente comprometido se han llevado a cabo desde entornos internos del grupo empresarial de ERD como consecuencia del uso habitual y lícito de los sistemas y que en ningún caso se ha producido un acceso no autorizado o la utilización irregular de los datos incluidos en el servidor FTP por parte de terceros.

También ha aportado acreditación de que no se ha encontrado en internet ningún tipo de referencia a la publicación de los datos incluidos en el servidor FTP en el periodo comprendido entre el 1 de enero y el 1 de abril de 2023.

EII reconoce que el incidente de seguridad consistió en un error humano, por la falta de cumplimiento de las normas de la empresa.

Se ha comprobado que las normas internas de EII prohíben el uso de software y servicios de uso personal y se han acreditado las actividades de formación y concienciación entre los empleados de EII: Realización de Formación sobre "Concienciación RGPD Básica", puesta a disposición de diferentes infografías y firma de la Normativa de Protección de Datos para el personal laboral y colaboradores de EII, en el que se recoge la información en materia de protección de datos, el deber de confidencialidad y secreto, y las medidas de seguridad obligatorias para todos los trabajadores/colaboradores.

Se ha confirmado ***(...)*** que los repositorios que ERD permite utilizar a EII no son repositorios de acceso público.

En consecuencia, no existen evidencias de no que se ha actuado de forma diligente una vez conocida la brecha de seguridad y que las medidas adoptadas con posterioridad al incidente aquí analizado no fueron adecuadas.

IV
Notificación de quiebra de seguridad

El Artículo 33 del RGPD establece lo siguiente:

"1. En caso de violación de la seguridad de los datos personales, el responsable del tratamiento la notificará a la autoridad de control competente de conformidad con el artículo 55 sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, a menos que sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas. Si la notificación a la autoridad de control no tiene lugar en el plazo de 72 horas, deberá ir acompañada de indicación de los motivos de la dilación.

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

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

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

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

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

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

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

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

En el presente caso, consta que ERD sufrió una brecha de seguridad de los datos personales en fecha 10 de enero de 2023, siendo detectada el día 20 de enero de 2023 y notificada a esta Agencia 3 días más tarde.

En consecuencia, la entidad responsable del tratamiento de datos cumplió lo que determina el artículo 33 del RGPD al notificar en el plazo establecido tras detectar la brecha de seguridad.

V

Comunicación de una violación de la seguridad de los datos personales al interesado

La comunicación de una violación de la seguridad de los datos personales al interesado está regulada en el artículo 34 del RGPD, según el cual:

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

2. La comunicación al interesado contemplada en el apartado 1 del presente artículo describirá en un lenguaje claro y sencillo la naturaleza de la violación de la seguridad de los datos personales y contendrá como mínimo la información y las medidas a que se refiere el artículo 33, apartado 3, letras b), c) y d).

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

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

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

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

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

ERD no ha comunicado a los afectados por la brecha de datos personales. Esta decisión se basa en el cálculo del nivel de riesgo para los derechos y libertades de las personas físicas afectadas por la brecha; valoraciones que han realizado y aportado, según la Guía para la notificación de brechas de datos personales (mayo 2021).

VI
Conclusión

Por lo tanto, en base a lo indicado en los párrafos anteriores, no se han encontrado evidencias que acrediten la existencia de infracción en el ámbito competencial de la Agencia Española de Protección de Datos.

De conformidad con lo señalado, por la Directora de la Agencia Española de Protección de Datos, SE ACUERDA:

PRIMERO: PROCEDER AL ARCHIVO de las presentes actuaciones.

SEGUNDO: NOTIFICAR la presente resolución a EDISTRIBUCIÓN REDES DIGITALES, S.L., y a ENGINEERING INGEGNERIA INFORMATICA SPAIN S.L.

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 según lo preceptuado por el art. 114.1.c) de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, y de conformidad con lo establecido en los arts. 112 y 123 de la citada Ley 39/2015, de 1 de octubre, los interesados podrán interponer, potestativamente, recurso de reposición ante la Directora de la Agencia Española de Protección de Datos en el plazo de un mes a

contar desde el día siguiente a la notificación de esta resolución o directamente recurso contencioso administrativo ante la Sala de lo Contencioso-administrativo de la Audiencia Nacional, con arreglo a lo dispuesto en el artículo 25 y en el apartado 5 de la disposición adicional cuarta de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-Administrativa, en el plazo de dos meses a contar desde el día siguiente a la notificación de este acto, según lo previsto en el artículo 46.1 de la referida Ley.

940-301023

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