- **Procedimiento Nº: E/01399/2020**

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 de 10 de febrero de 2020, la Directora de la Agencia Española de Protección de Datos (en adelante, AEPD) acuerda iniciar actuaciones de investigación en relación a una brecha de seguridad de datos personales notificada por CEER CENTRO DE ESTUDIOS ENERGÉTICOS Y RADIOFÍSICOS, S.L. con NIF: B06195960 (en adelante, DPD del responsable/investigada), relativa a la sustracción de un teléfono móvil laboral con datos y fotografías de pacientes de la Clínica Dental ******CLÍNICA.1***

SEGUNDO: La Subdirección General de Inspección de Datos procedió a realizar actuaciones previas de investigación para el esclarecimiento de los hechos objeto de la notificación, teniendo conocimiento de los siguientes extremos:

FECHA DE NOTIFICACIÓN DE LA BRECHA DE SEGURIDAD:

3 de febrero de 2020

ENTIDADES INVESTIGADAS

D.ª ***A.A.A.*** (en adelante, la investigada y responsable del tratamiento de datos) con *DNI* ******NIF.1*** y domicilio en *C/* ******DOMICILIO.1***, en calidad de trabajadora autónoma prestando servicios odontológicos bajo el nombre comercial de Clínica Dental ******CLÍNICA.1***

RESULTADO DE LAS ACTUACIONES DE INVESTIGACIÓN

1. Respecto a los hechos:

- La investigada informa de que el 3 de febrero de 2020 entorno a la 1:00 horas recibe aviso de la central de alarmas contratada por su parte sobre que alguien no autorizado había entrado en la clínica odontológica que ella regenta.
- Tras ello, la investigada manifiesta que su marido se persona en la clínica en cuestión, donde dice hallar a la Policía Nacional y constatar que la cerradura ha sido forzada (según evidencia), que falta el dinero de la caja y que el teléfono móvil de la clínica ha sido sustraído.
- La investigada declara que el teléfono móvil laboral sustraído contenía datos y fotografías de pacientes de sus servicios odontológicos, entre los que señala:
    - Nombre del paciente.
    - Número de teléfono del paciente.
    - En algunos casos, fotos de incidencia en la boca del paciente (enviada por *WhatsApp* por parte de estos).

Asimismo, la investigada indica no conocer el número real de pacientes afectados al haber perdido la agenda de contactos incorporada en el propio teléfono móvil sustraído, aunque en primera instancia notifica como número aproximado unos 2.000 contactos.

- La investigada expone no tener constancia de la utilización por terceros de los citados datos personales implicados en la brecha de seguridad.
- La investigada manifiesta haber intentado anular la tarjeta SIM durante la madrugada del 3 de febrero de 2020, pero no haberlo logrado hasta las 8:00 horas de ese día, puesto que su compañía telefónica, MásMóvil, no dispone de operadores en horario nocturno.
- La investigada informa que la central de alarmas contratada dispone del vídeo captado por la cámara situada en la recepción de la clínica odontológica y que contendría imágenes del robo.
- La investigada expone que a las 9:00 horas de ese día 3 de febrero de 2020 se persona en su clínica odontológica la Policía Nacional científica en busca de huellas u otras pruebas que pudieran servir para identificar a los autores del robo.
- La investigada declara que, tras lo anterior, se puso en contacto con su DPD (CEER) para trasladarle lo acontecido y que desconoce las posibles causas que dieron lugar a que ocurriese la incidencia investigada.
- La investigada evidencia que a las 14:18 horas de ese día 3 de febrero de 2020 compareció en la comisaría de Policía Nacional del distrito de ******DISTRITO.1***, sita en ******LOCALIDAD.1***, denunciando el robo acaecido en su clínica odontológica.

2. Respecto a las medidas previas al acontecimiento de la brecha de seguridad:

- La investigada aporta un RAT (registro de actividades de tratamiento) en el que se le puede identificar como responsable del tratamiento de los datos en las actividades de clínicas dentales, de gestión de contactos, de historial clínico, de informes médicos y de gestión de clientes y/o proveedores, entre otras.
- La investigada presenta una EIPD (evaluación de impacto relativa a la protección de datos), la cual contempla un análisis de riesgos asociado al tratamiento de datos que realiza.
- La investigada certifica y prueba disponer de una instalación y conexión a central receptora de alarmas (véase el confidencial ANEXO I para más detalle) en su clínica. La investigada expone que dicha alarma estaba conectada en el momento del acceso no autorizado a la misma y corroborado con el aviso que recibe desde la central de alarmas en la fecha de los hechos.
- La investigada demuestra la existencia de cerradura en la puerta principal de la clínica donde presta sus servicios odontológicos.
- La investigada manifiesta que el teléfono móvil laboral con datos y fotografías de pacientes sustraído disponía de código PIN (*Personal Identification Number*) de cuatro números para acceso a la tarjeta SIM (*Subscriber Identity Module*, módulo de identificación del abonado) y de código de pantalla de bloqueo de seis números.

3. Respecto a las medidas posteriores al acontecimiento de la brecha de seguridad:

3.1. De carácter correctivo (reactivas para subsanar la brecha de seguridad):

- En fecha 3 de febrero de 2020, la investigada manifiesta haber procedido al bloqueo de la tarjeta SIM incorporada en el teléfono móvil laboral sustraído.
- La investigada manifiesta haber solicitado a su compañía telefónica el bloqueo del teléfono móvil laboral en cuestión por medio del código IMEI (*International Mobile Equipment Identity*, identidad internacional de equipo móvil) en fecha 3 de febrero de 2020.
- La investigada prueba disponer de un cartel informativo, con el nombre comercial bajo el que presta sus servicios odontológicos (Clínica Dental ******CLINICA.1***), en el que se informa a los pacientes de la sustracción del teléfono móvil laboral, del posterior bloqueo del terminal y de que no le consta que los datos en él incluidos hayan sido utilizados por terceros. La investigada expone haber colgado dicho cartel en la recepción de su clínica puesto que valora que es la manera en que los posibles afectados sean informados, al alegar que desconoce el número real de pacientes afectados por la incidencia.

3.2. De carácter preventivo (proactivas para evitar que se repita la brecha de seguridad):

- La investigada expone haber incorporado el requisito de que el teléfono móvil laboral pase a guardarse bajo llave.

FUNDAMENTOS DE DERECHO

I

De acuerdo con los poderes de investigación y correctivos que el artículo 58 del Reglamento (UE) 2016/679 (Reglamento general de protección de datos, en adelante RGPD) otorga a cada autoridad de control, y según lo dispuesto en el artículo 47 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.

II

En el presente caso, de las actuaciones de inspección llevadas a cabo por la inspección de esta Agencia, se desprende que las medidas de seguridad implantadas por la investigada y responsable del tratamiento de datos en la Clínica Dental ******CLÍNICA.1*** eran las razonables en relación con el registro de actividades de tratamiento y análisis de riesgos que determinó un riesgo bajo para la incidencia ahora analizada. Hay que señalar que el teléfono sustraído se encontraba en el interior de la clínica con acceso cerrado con llave y alarma conectada con central de seguridad. También disponía implantado un código de desbloqueo del terminal de seis dígitos, así

como código por defecto de desbloqueo de la tarjeta SIM, lo que impide el acceso a los datos obrantes en el terminal sustraído.

Respecto de los datos personales obrantes en el teléfono sustraído, señalar que no consta tratamiento posterior ni reclamación por los posibles afectados ante esta AEPD.

Por último, se recomienda elaborar un Informe final sobre la trazabilidad del suceso y su análisis valorativo, en particular, en cuanto al impacto final. Este Informe es una valiosa fuente de información con la que debe alimentarse el análisis y la gestión de riesgos y servirá para prevenir la reiteración de una brecha de similares características como la analizada.

III

Por lo tanto, la actuación de la investigada en calidad de responsable de los datos sustraídos del teléfono del que era titular ha sido proporcionada y diligente con la normativa sobre protección de datos personales analizada en los párrafos anteriores.

Por lo tanto, de acuerdo 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 *D.ª* ***A.A.A.*** con *DNI****: ***NIF.1*** y domicilio en *C/* ******DOMICILIO.1***

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.

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