- **Procedimiento Nº: E/10681/2019**

940-0419

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: Las actuaciones de inspección se inician por la recepción de un escrito de notificación de quiebra de seguridad de datos personales (en adelante quiebra de seguridad) remitido por la entidad UNMEQUI UNIVERSAL MEDICO QUIRURGICA, S.A (en adelante UNMEQUI) con NIF: A28026003, en el que informan a la Agencia Española de Protección de Datos (en adelante AEPD) que el 23/10/2019, en el momento de la recogida de los contenedores blindados que garantizan que no se puede acceder a su contenido, el personal de la empresa Cartón y Papel Reciclado, S.A. detectó que los contenedores habían sido forzados. Inmediatamente se comunicó al Delegado de Protección de Datos la incidencia y acto seguido se procedió a la sustitución/reparación de los contenedores y a la constitución de un comité de investigación.

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

ANTECEDENTES

Fecha de notificación de quiebra: 25 de octubre de 2019

ENTIDADES INVESTIGADAS

UNMEQUI UNIVERSAL MÉDICO QUIRURGICA, S.A. con NIF A28026003 con domicilio en VELAZQUEZ, nº 124, 28006 Madrid.

RESULTADO DE LAS ACTUACIONES DE INVESTIGACIÓN

1. Con fecha 17 de diciembre de 2019 se requiere información a UNMEQUI y de la respuesta recibida se desprende:

   Respecto de la cronología de los hechos

   22/10/2019. El personal de la empresa Cartón y Papel Reciclado, S.A., accede al Centro de UNMEQUI con intención de llevar a cabo la recogida mensual de los contenedores blindados. En ese momento, detecta que las cerraduras de dos contenedores están rotas. Inmediatamente, informa a la Dirección Médica de UNMEQUI y ésta solicita a la empresa de destrucción que repare las cerraduras.

23/10/19. Siguiendo el Protocolo de Recogida y Destrucción de Documentación, el Departamento de Gestión, Calidad y Medioambiente informa del suceso al Departamento Jurídico para que estudie la gravedad del incidente, se abra una incidencia y se tomen las medidas oportunas según el RGPD. Aportan copia del Protocolo de recogida y destrucción de documentación.

El Departamento Jurídico remite el mail de la incidencia al Delegado de Protección de Datos (en adelante, DPD).

El DPD mantiene una reunión con los Departamentos de Gestión, Calidad y Medioambiente y Jurídico.

Se crea un Comité de investigación compuesto por los siguientes responsables:

1. El Responsable de Seguridad.
2. Director de UNMEQUI.
3. Asesor jurídico.
4. Jefe del Departamento de Seguridad y Sistemas.
5. Delegado de Protección de Datos.

24/10/2019. El DPD registra la incidencia y la evalúa conforme al Procedimiento de Gestión de Brechas y Metodología de Análisis de Riesgos del Responsable.

25/10/2019.

- Se sustituyen los contenedores por unos nuevos.
- Se cambia de ubicación del contenedor de Urgencias.
- Se notifica la brecha de seguridad ante la Agencia Española de Protección de Datos.

Respecto de las causas que han originado la incidencia:

Los contenedores de destrucción confidencial de la información se instalaron como medida de seguridad con el objeto de mitigar un riesgo inicial identificado en el análisis de riesgos para garantizar la destrucción de manera segura de la información confidencial.

Uno de los contenedores estaba ubicado en el departamento de Administración, zona de acceso restringido únicamente al personal, y el otro contenedor estaba ubicado en el Hospital, en la zona de Urgencias, donde se deposita la documentación de los departamentos de admisión, caja, recepción y radiología.

Manifiestan que se aplicaron todas las medidas de seguridad necesarias para evitar un acceso indebido a la documentación antes de su destrucción.

La incidencia se debe a un ataque malicioso.

Número de clientes afectados por la incidencia.

UNMEQUI no tiene constancia de que la incidencia haya afectado a ningún paciente ni usuario.

Tipología de los datos afectados.

Los documentos que se tiran en los contenedores pertenecen al departamento de Administración y a la zona de Urgencias.

Los datos que figuran en los documentos depositados en los contenedores son datos identificativos, económicos, financieros y de salud.

Descripción detallada de las acciones tomadas con objeto de minimizar los efectos adversos

- Sustitución de los contenedores.
- Cambio de ubicación del contenedor de urgencias.

Durante las semanas posteriores se ha llevado a cabo un seguimiento de la incidencia.

Acciones realizadas para la resolución final de la incidencia

23/10/2019.

Creación de un Comité de investigación.

24/10/2019.

- Análisis de la brecha.
- Valoración de la gravedad.
- Valoración del riesgo para los afectados.
- Registro de la brecha.

25/10/2019.

- Sustitución de los contenedores.

- Cambio de ubicación del contenedor de urgencias.

- Notificación de la brecha de seguridad ante la Agencia Española de Protección de Datos.

Respecto de la seguridad de los tratamientos de datos con anterioridad a la incidencia.

UNMEQUI ha llevado a cabo una adecuación de los procedimientos de destrucción de documentación confidencial al Reglamento General de Protección de Datos (RGPD) y a la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD) implementado un Sistema Interno de Gestión de Protección de Datos, realizando la identificación, revisión y adecuación de los tratamientos de la Organización en los que había implicados datos de carácter personal.

Como resultado de dicho proceso de adecuación al RGPD y a la LOPDGDD, UNMEQUI elaboró una serie de documentos que conforman el sistema de gestión de la Organización, que se encuentra compuesto, entre otros, según manifiesta su representante, por los siguientes:

- Registro de actividades de tratamiento.

- Análisis de riesgos previos de todos y cada uno de los tratamientos de datos.

- Cláusulas informativas a los interesados y de legitimación de cada tratamiento.

- Inventario de empleados con acceso al sistema de información para realizar los tratamientos de datos personales, así como evaluación de cumplimiento de las medidas de seguridad efectivamente implantadas.

- Evaluaciones de impacto relativas a la protección de datos de tratamientos calificados con un riesgo alto a los derechos y libertades de los interesados.

- Plan de formación.

- Procedimiento de gestión de brechas de seguridad.

- Procedimiento de atención de derechos de los interesados.

- Procedimiento de información.
- Procedimiento de videovigilancia.
- Procedimiento de contratación de terceros.
- Protocolo de recogida y destrucción de documentación.
- Política de seguridad.

Además, la Organización cuenta con un seguro de Responsabilidad Civil en materia de protección de datos.

Aportan copia del Registro de Actividad de los tratamientos relativos al incidente.

Aportan copia del Análisis de Riesgo sobre todos los tratamientos, así como la EIPD realizada sobre el tratamiento Historia Clínica Electrónica.

Aportan copia del Procedimiento de Brechas de Seguridad de datos personales.

Aportan informe de Política de Seguridad

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

El RGPD define, de un modo amplio, las "violaciones de seguridad de los datos personales" (en adelante quiebra de seguridad) 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."*

El artículo 33 del RGPD señala lo siguiente:

"Notificación de una violación de la seguridad de los datos personales a la autoridad de control

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."

En el presente caso, consta una quiebra de seguridad de datos personales en las circunstancias arriba indicadas, categorizada como una brecha de confidencialidad, como consecuencia del supuesto acceso indebido al contenido de los contenedores de destrucción de documentos.

De las actuaciones de investigación se desprende que la entidad UNMEQUI disponía con anterioridad a la incidencia de razonables medidas técnicas y organizativas preventivas a fin de evitar este tipo de incidencias y acordes con el nivel de riesgo.

Asimismo, la entidad UNMEQUI disponía de protocolos de actuación para afrontar un incidente como el ahora analizado, lo que ha permitido de forma diligente la identificación, análisis y clasificación del incidente de seguridad de datos personales así como la diligente reacción ante la misma al objeto de notificar, minimizar el impacto e implementar nuevas medias razonables y oportunas para evitar que se repita la supuesta incidencia en el futuro a través de la puesta en marcha y ejecución efectiva de un plan de actuación por las distintas figuras implicadas como son el responsable del tratamiento y el Delegado de Protección de Datos.

No constan reclamaciones ante esta Agencia de personas afectadas.

En consecuencia, consta que la entidad UNMEQUI, en calidad de responsable del tratamiento afectado, disponía de forma previa de medidas técnicas y organizativas razonables en función del nivel de riesgo para evitar este tipo de incidencia. No obstante, se recomienda la realización de un informe final sobre el incidente notificado. 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 ahora analizada.

III

Por lo tanto, se ha acreditado que la actuación de UNMEQUI en calidad de responsable del tratamiento ha sido acorde y proporcionada 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 UNMEQUI UNIVERSAL MÉDICO QUIRURGICA, S.A., con NIF A28026003 y con domicilio en la calle Velázquez nº 124, 28006 Madrid.

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