- **Procedimiento Nº: E/01156/2020**

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: Las actuaciones de inspección se iniciaron por la recepción de un escrito de notificación de brecha de seguridad de datos personales remitido por CRUZ ROJA ESPAÑOLA (en adelante, CRE), en el que informaron a la Agencia Española de Protección de Datos del extravío de documentación durante su transporte por una empresa de mensajería (SEUR) en el itinerario entre oficina provincial de ******LOCALIDAD.1*** y oficina autonómica de ******LOCALIDAD.2*** de CRE, que contenía datos personales.

La CRE manifiesta que la incidencia no ha sido notificada a la Agencia Española de Protección de Datos dentro del plazo de las 72 horas debido a las tareas de identificación y verificación de la documentación (en soporte papel), con objeto de acreditar el extravío y, en su caso, determinar la documentación extraviada y la identidad y número de afectados con exactitud.

Aportan un informe de la incidencia y fotografía del paquete en las que se observa una caja de cartón precintada con cinta adhesiva, abierta en uno de sus vértices.

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 notificación, teniendo conocimiento de los siguientes extremos:

ANTECEDENTES

Fecha de notificación de la brecha de seguridad de datos personales: **22/01/2020**

ENTIDADES INVESTIGADAS

CRUZ ROJA ESPAÑOLA, con NIF Q2866001G con domicilio en Av. Reina Victoria 26, 28003 Madrid.

RESULTADO DE LAS ACTUACIONES DE INVESTIGACIÓN

1. Con fecha 7 de febrero de 2020 se solicitó información por la Inspección de Datos a CRE, y de la respuesta recibida se desprende lo siguiente:

   Respecto de la cronología de los hechos

   1.1. El 26 noviembre 2019, se envía desde Oficina Provincial de CRE en ******LOCALIDAD.1***, un paquete con documentación a la Oficina Autonómica de ******LOCALIDAD.2***. Dicho paquete se envía a través de la empresa de

mensajería SEUR con la que la Oficina de ******LOCALIDAD.1*** lleva años trabajando sin ninguna incidencia de gravedad. El paquete contiene la certificación del IRPF de las actividades del mes de agosto para justificar las ayudas recibidas, con copias de la entrega bienes y otros documentos de identificación de las personas usuarias (DNI/ NIE/Pasaportes) de los programas implicados.

El 29 noviembre 2019, se recibe comunicación por e-mail de la Oficina Autonómica de ******LOCALIDAD.2*** (destino) informando de que el paquete enviado ha llegado deteriorado y se ha podido perder información. La Oficina Autonómica envía fotos del estado del paquete.

El 29 noviembre 2019, desde Oficina Provincial de ******LOCALIDAD.1*** (origen) se realiza llamada telefónica a SEUR, informando de la llegada del paquete en mal estado y posible extravío de documentación. Indicamos la importancia de la localización de los documentos potencialmente extraviados. Se valoran opciones de otro tipo de servicio para este tipo de envíos.

El 29 noviembre 2019, desde Oficina Provincial de ******LOCALIDAD.1*** se vuelve a llamar telefónicamente a SEUR, para comentar el tema e indicarle nuestra preocupación. Se comenta la opción de SEUR de modelo de servicio de paquetería con mayor control del proceso llamado “Libro Control”.

El 2 diciembre 2019, se solicita a SEUR nuevo servicio de envío de documentación sensible, sistema “Libro Control”, mientras se buscan otras opciones de envío seguro con otras empresas.

El 4 diciembre 2019, el agente comercial de SEUR informa de que ya dispone de las claves de acceso para el uso del servicio “Libro Control”, envía etiquetas y nos comunica que vendrá a explicarnos el funcionamiento del nuevo servicio. Entre otras características, incluye: control en cada punto de logística, evita las cintas de transporte, dispone de bolsas herméticas que evitan la humedad y que el paquete se resienta de golpes internos.

En diciembre 2019, la información enviada para justificación contenía unos 1500 folios aproximadamente. El objetivo que se fijó fue conocer, en el menor tiempo posible, el alcance de la posible brecha de seguridad, identificando en su caso la posible documentación extraviada y las personas usuarias afectadas por ésta, ya que el paquete deteriorado contenía la mayor parte de la documentación. Durante el mes de diciembre se trabaja con las 50 Oficinas Locales recabando información sobre los documentos correspondientes a la información posiblemente extraviada, cotejándose con las copias con las que contamos y viendo, uno a uno, todos los afectados, confeccionando de esta manera una lista de personas afectadas por la documentación extraviada (recetas, documentación, certificados).

De este trabajo se determinó que el número de personas usuarias afectadas es de 60, así como se identifican los documentos concretos extraviados correspondientes a cada uno de los afectados. La información se envió en bloques agrupados por proyectos y con una portada por cada grupo, en el que se indicaban el número de usuarios por proyecto. Señalar a este respecto, que la información no se pierde en bloque, sino que llegaron varios proyectos incompletos, lo que complicó considerablemente y demoró en el tiempo la

constatación del extravío de documentación y posterior identificación de los usuarios afectados.

El 8 enero 2020, SEUR informa de que no han conseguido localizar los documentos extraviados. Se realiza una reclamación por email solicitando informe de actuaciones y explicación de las circunstancias del incidente, ya que, al tener el paquete recibido en ******LOCALIDAD.2**** cinta de precintado, la ruptura del mismo ha tenido que producirse durante el itinerario y ser conocida por sus operarios. Se solicita contactar con el responsable de logística en SEUR y tener una reunión personal con él.

El 8 enero 2020, obtienen de las oficinas locales toda la información del alcance de la brecha de seguridad, personas usuarias afectadas y los documentos extraviados de cada uno de ellos. Se comienza a redactar informe para traslado al Delegado de Protección de Datos y a la Oficina de Protección de Datos de la CRE.

El 9 enero 2020, paralelamente a la decisión de dar de alta el modo servicio de “Libro Control” en SEUR, se considera necesario disponer de un servicio que ofrezca la máxima seguridad en el envío de documentación confidencial. Aunque desde el incidente se está utilizando para envíos de este tipo el “Libro Control” de SEUR, y una vez habiendo valorado otras opciones de envíos seguros, se determina contratar con la Sociedad Estatal Correos y Telégrafos, S.A. (en adelante Correos) el servicio denominado “valija de documentación” ******LOCALIDAD.1*** - ******LOCALIDAD.2***, al ser el que aporta más garantía de seguridad. Correos contesta a la nueva solicitud de servicio, indicando que puede incluir la nueva valija solicitada dentro del acuerdo marco que tienen establecido con la sede central. Una vez recibida la información y los precios, se traslada el interés en este servicio y su contratación.

El 10 enero 2020, se fija una reunión con el Responsable de Logística en SEUR, para solicitarle explicaciones y aclaración de las circunstancias del incidente y manifestarle nuestra preocupación ante la no recuperación de los documentos. Se le solicita en dicha reunión informe de acciones y situación por parte de la empresa en este asunto.

El 15 enero 2020, se coordina con SEUR la información sobre documentación extraviada para facilitar su identificación y gestión ante el seguro.

El 16 enero 2020, se interpone denuncia ante la Policía Nacional por el extravío de datos por parte de nuestra empresa de transporte SEUR.

El 16 enero 2020, se envía al Delegado de Protección de Datos y a la responsable de la Oficina de Protección de Datos de CRE, el informe del incidente de brecha de seguridad, indicando número de casos y tipo de documentación, así como cronología de los hechos.

El 16 enero, el Delegado de Protección de Datos requiere más información del incidente, así como copia de la denuncia interpuesta y de la reclamación contra SEUR. Asimismo, solicita explicaciones sobre los motivos de la demora en la notificación del incidente e indica que es preciso notificarlo a la Agencia Española de Protección de Datos (AEPD) y comunicarlo a los usuarios afectados.

El 16 de enero, el Delegado de Protección de Datos, ante la falta de contestación de SEUR a la reclamación realizada por email el 8 de enero, nos indica que debemos realizar una reclamación formal, exigiendo explicaciones e información del incidente. Asimismo, indica que se preparará la comunicación a los afectados para que se remita desde la Oficina de ******LOCALIDAD.1***

El 16 enero 2020, se Recibe escrito de SEUR comunicando el estado de la situación, pidiendo disculpas y comunicando que seguían con la búsqueda de la documentación.

El 22 de enero 2020, se remite al Delegado de Protección de Datos y a la responsable de la Oficina de Protección de Datos de CRE, el resto de la información solicitada, confirmando número definitivo de usuarios afectados por el incidente y las medidas adoptadas para garantizar la seguridad de nuevos envíos.

El 22 de enero de 2020, el Delegado de Protección de Datos remite informe del incidente en el que incluye modelo de carta para realizar la comunicación a los usuarios afectados. Insiste en la necesidad de hacer una reclamación formal a SEUR y que informe de las gestiones realizadas a este respecto.

El 22 de enero de 2020, se notifica la brecha de seguridad a la AEPD.

El 27 enero 2020, responsables de la CRE se reúnen con el responsable de logística de SEUR y el Director de Ventas SEUR-******LOCALIDAD.1***, a los que comunican que el informe entregado es insuficiente, por lo que les solicitan por escrito la elaboración de un nuevo informe con más detalle y amplitud.

El 3 febrero 2020, se reúnen nuevamente con el responsable de logística de SEUR y el Director de Ventas SEUR-******LOCALIDAD.1***, donde entregan el informe explicando lo sucedido y respondiendo a nuestras peticiones de la pasada reunión del 27 de enero e indicando que con toda probabilidad la información extraviada ha sido destruida según sus procedimientos.

El 5 febrero 2020, se entrega a los TISE (Trabajadores Sociales) que gestionan a los usuarios afectados la entrega de comunicados escritos por la CRE para realizar entregas a cada una de las personas usuarias afectadas de la brecha de seguridad, explicando, a cada usuario, el extravío con la información concreta que le incumbe. Se indica que, a los usuarios sin hogar se les localizará y entregará en mano la notificación por no disponer de dirección postal.

El 7 febrero 2020, se envía comunicado escrito remitido por CRE a cada una de las personas usuarias afectadas por la brecha de seguridad, explicando el extravío con la información concreta por cada usuario. El modo de envío ha sido por correo certificado y con acuse de recibo a todos los usuarios afectados, exceptuando los de personas usuarias del proyecto “Personas sin Hogar”, a los que, por no disponer de dirección postal, se entregan los escritos directamente por medio de las oficinas locales que gestionan la actividad para la entrega en mano.

El 13 febrero 2020, se envía correo electrónico a todas las oficinas locales del territorio, indicando los nuevos sistemas de mensajería instaurados para el envío físico de información sensible.

Respecto de las causas que han hecho posible la incidencia

Según conversaciones mantenidas por CRE con SEUR, varias han sido las causas que han podido provocar la incidencia:

- Periodo prenavideño, en el que SEUR, según han comentado, hace frente a un importante incremento de envíos, cubriendo dicha necesidad con personal de nueva contratación.
- El embalaje deteriorado era de cartón y, aunque estaba precintado, pudiera haberse mojado o golpeado durante el manipulado y transporte.
- La documentación estaba sujeta con gomas, pero puede no haber sido suficiente para inmovilizarla dentro del embalaje.

Respecto al número y tipología de los datos afectados

El incidente ha afectado a unas 60 personas.

Los documentos desaparecidos son los siguientes:

- 50 Fotocopias de documentos de identificación: pasaporte, DNI, NIE.
- 1 Fotocopia de Libro de familia.
- 1 Fotocopia de Presupuesto dental.
- 3 Fotocopias de recetas médicas.
- 13 Fotocopias de Certificado de Empadronamiento.

Respecto a las acciones tomadas con objeto de minimizar los efectos adversos

- Intento de localizar los documentos extraviados, numerosas conversaciones con SEUR y solicitud de informes.
- Interposición de denuncia ante la Policía Nacional.
- Comunicación del incidente a las personas afectadas.

Respecto a las acciones realizadas para resolución final de la incidencia

- Paralelamente a la decisión de dar de alta el modo de “Libro Control” en SEUR para el transporte de documentación, se considera necesario tener un servicio que ofrezca la máxima seguridad en el envío de documentación confidencial. Aunque desde el incidente se está utilizando para envíos de este tipo el servicio “Libro Control” de SEUR y, una vez habiendo valorado otras opciones de envíos seguros, se determina contratar servicio de Correos denominado “valija de documentación” ******LOCALIDAD.1-***LOCALIDAD.2***, siendo el que aporta más garantía de seguridad.
- Nuevo embalaje. Envasado con bolsas impermeables para proteger los documentos de agua u otros agentes que puedan afectar a la documentación incluida, y que inmoviliza de manera más eficiente la información.
- Se solicita valorar por parte de la Oficina Autonómica reducir el envío de documentación justificativa de las ayudas en papel, ya que esta información se encuentra digitalizada en la aplicación.

- Comunicación a todas las oficinas locales del territorio, indicando los nuevos sistemas de mensajería.

Respecto de las medidas de seguridad implantadas con anterioridad a la brecha

- Aportan ficha del tratamiento "Intervención Social" en el que se incluye el tratamiento de la documentación en formato papel.
- Aportan copia del documento *"Medidas de seguridad en: sistemas informáticos oficina central, aplicaciones centrales y documentación en papel, para todas las áreas, centros y oficinas pertenecientes a CRE"* en el que se recogen las medidas de seguridad técnicas y organizativas del tratamiento de datos en formato papel. Incluye un apartado específico de las medidas a tener en cuenta respecto al transporte de documentos que contienen datos de carácter personal:

  "*1. Todos los empleados han sido informados que la documentación que contenga datos de carácter personal que requiera ser enviada fuera de la Institución, debe ser colocada en sobres o cajas cerradas, éstos deben ser precintados y debidamente cerrados evitando en todo momento que pueda quedar expuesta la documentación en el proceso de envío y transporte.*

  2. Hacer uso de transportistas y empresas de mensajería de reconocido prestigio y solvencia con los que ya viene trabajando CRE.

  3. Mantener el registro de la documentación que sale y entra de las Oficinas o Centros de CRE."
- Aportan el documento denominado *"Análisis por áreas deficiencias mas significativas. Compliance RGPD, Madrid, 04 de julio de 2018"*, del que se desprende que recoge las deficiencias detectadas en CRE para dar cumplimiento al Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 y la planificación de acciones correctoras.

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, brecha 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 art 33 del Reglamento (UE) 2016/679, de 27/04/2016 (en adelante RGPD), señala:

"Artículo 33 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.

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."

En el presente caso, consta que se produjo una brecha de seguridad de datos personales en las circunstancias arriba indicadas, categorizada como brecha de confidencialidad como consecuencia del extravío de documentación personalizada de sesenta usuarios de los servicios de la CRE durante un traslado.

De las actuaciones de investigación se desprende que la CRE disponía de medidas técnicas y organizativas preventivas a fin de evitar este tipo de incidencias. La CRE, en calidad de responsable del tratamiento, tenía contratado un servicio de traslado de documentación con la entidad SEUR y pudo detectar la posible incidencia a su llegada a destino al comprobar deterioros en la caja que los contenía y la posibilidad de que se pudieran haber extraviado parte del contenido.

Asimismo, la CRE disponía de protocolos de actuación para afrontar un incidente como el ahora analizado, lo que ha permitido la identificación, análisis y clasificación de la brecha de seguridad de datos personales así como la diligente reacción ante la

misma al objeto de notificar, comunicar, minimizar el impacto e implementar nuevas medidas razonables y oportunas para evitar que se repita la 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 las agencias colaboradoras en calidad de encargadas, así como el Delegado de Protección de Datos.

Consta también que con ocasión de la incidencia se ha procedido a implantar mejoras técnicas y organizativas, como es el cambio de empresa de transporte y asegurar las cajas de transporte de documentación de forma que se evite su deterioro ante golpes. También se ha puesto en marcha el procedimiento para el envío de documentación sensible de forma electrónica y evitar el traslado físico.

En cuanto al retraso de la notificación de la brecha de seguridad a la AEPD, se debe señalar que la propia norma señala que se deberá realizar sin dilación indebida y, de ser posible, a más tardar dentro de las 72 horas. Añade la norma que, 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. En el presente caso, la CRE justifica motivadamente el retraso como consecuencia del tiempo empleado para comprobar la efectiva pérdida de documentos en formato papel, toda vez que la documentación llegó a destino deteriorada y existía esa posibilidad. Además, era periodo vacacional de Navidad y la entidad SEUR se encontraba saturada de encargos, lo que dificultó la búsqueda de la documentación extraviada de forma sobrevenida. Una vez comprobada la ausencia de documentos era necesario identificar cuáles y cuántos usuarios podrían estar afectados. Todo ello ocasionó una demora justificada en la notificación de la brecha de seguridad a la AEPD, sin perjuicio de que esta Agencia considere mas recomendable que se hubiere realizado una notificación gradual conforme se avanza en la búsqueda de la documentación y minimización del impacto.

No constan reclamaciones ante esta Agencia de los afectados.

En consecuencia, consta que CRE disponía de medidas técnicas y organizativas razonables para evitar este tipo de incidencia y que al resultar insuficientes han sido actualizadas de forma diligente. No obstante, se sugiere, a fin de cerrar la brecha de seguridad, se elabore un Informe Final sobre la trazabilidad del suceso y su análisis valorativo, en particular, en cuanto al impacto final y mejora del procedimiento de notificación a la Autoridad de Control (AEPD). 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 causada previsiblemente por un error puntual.

III

Por lo tanto, consta que la actuación de CRE, como entidad responsable del tratamiento, ha sido acorde y proporcional 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 CRUZ ROJA ESPAÑOLA, con NIF Q2866001G y con domicilio en Av. Reina Victoria 26, 28003 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