Procedimiento Nº: E/04187/2019

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: En fecha 08/04/2019 se ha recibido una declaración de brecha de seguridad notificada por el AYUNTAMIENTO de VALENCIA (en lo sucesivo AV), con NIF ***P4625200C***, relacionada con la difusión de listas de mesas electorales a través de *whatsapp.*

Según figura en la declaración a primera hora del día 08/04/2019, se ha recibido una llamada telefónica en la que una ciudadana nos ha informado que había recibido un *whatsapp* que contenía información sobre los componentes de las mesas electorales correspondientes al sorteo llevado a cabo en el Pleno de la Corporación del pasado día 02/04/2019.

Tras recibir dicha llamada y, sin solución de continuidad, se ha recibido información, desde diferentes servicios municipales y desde la propia Alcaldía sobre los mismos hechos.

Desde la Delegación de Protección de Datos Personales se han llevado a cabo acciones con el fin de identificar el posible incidente de seguridad, su clasificación, establecimiento del tipo de brecha de seguridad, valoración del alcance de la misma, medidas adoptadas y, en su caso, notificación a la AEPD.

De la información obtenida de diversos servicios municipales se desprende que:

• La información que, al parecer, se ha publicado a través de la aplicación *whatsapp*, es el fichero VLC_C75_0001_ES_VA_todos.PDF, que contiene datos.

De la información obtenida de diversos servicios municipales se desprende que:

• La información que, al parecer, se ha publicado a través de la aplicación *whatsapp*, es el fichero VLC_C75_0001_ES_VA_todos.PDF, que contiene datos personales de todos los miembros de las mesas electorales de la ciudad de València.

• Las categorías de datos que se contiene en dicho documento son: nombre y apellidos, DNI, dirección y cargo en la Mesa Electoral.

• El número de personas afectadas asciende a 8.334.

• El archivo VLC_C75_0001_ES_VA_todos.PDF ha estado en las siguientes carpetas:

\\Dades1TIC\Dades1TIC\ayun\Recursos compartidos\GENERALES 2019 (A esta carpeta pueden acceder con 16 usuarios)

\\Dades2\Dades2\ayun\SCT\NORMALDOCIC\00-REPROGRAFIA (A esta carpeta pueden acceder 12 usuarios)

\\Dades2\Dades2\ayun\Servicios_Centrales\Poblacion\MESASELECCIONESGENERALES (A esta carpeta pueden acceder 67 usuarios)

• El citado archivo también fue comunicado el mismo día del sorteo a la Junta Electoral

• Según informa el responsable de Seguridad de la Información no consta ningún ataque informático que haya expuesto dicha información a alguien desconocido a través de Internet.

En el presente caso, todo parece indicar que dicha brecha ha sido provocada por una filtración de la información, sin embargo, no existe certeza, de que haya tenido su origen en el AV, ya que la referida información fue compartida con la Junta Electoral. La severidad de la pérdida de confidencialidad es relevante dado el número de personas afectadas.

Valoración del alcance de la brecha.

En relación a las personas afectadas, cabe indicar que nos hallamos ante datos identificativos y de contacto que pueden tener como consecuencias más graves, intentos de suplantación de la identidad de las mismas.

Medidas adoptadas.

Tras conocerse la posible filtración de información se han adoptado las siguientes medidas:

Desde el servicio de tecnologías de la información se ha eliminado el citado archivo de las carpetas siguientes:

\\Dades1TIC\Dades1TIC\Ayun\Recursos compartidos\GENERALES 2019

\\Dades2\dades2\ayun\Servicios_Centrales\Poblacion\MESAS ELECCIONES

Según indican los representantes del Ayuntamiento, tras la realización de la presente comunicación a la AEPD, se va a trasladar los hechos a la Asesoría Jurídica Municipal con el fin de que se denuncien los hechos ante las autoridades que correspondan con el fin de que se investiguen los hechos y se depuren las responsabilidades que correspondan.

Con posterioridad, se han presentado escritos de reclamación por personas afectadas por la brecha de seguridad: el 07/05/2019 D. ***A.A.A.*** y Dña. ***B.B.B.***; el 13/05/2019 D. ***C.C.C.***; el 15/05/2019 D. ***D.D.D.***; el 22/05/2019 Dña. ***E.E.E.*** y el 03/06/2019 Dña. ***F.F.F.***.

SEGUNDO: A la vista de los hechos denunciados y de los documentos de los que ha tenido conocimiento esta Agencia, la Subdirección General de Inspección de Datos procedió a la realización de actuaciones para el esclarecimiento de los hechos en cuestión.

El día 02/04/2019 se procedió a celebrar el Pleno municipal relativo al sorteo para determinar la composición de las mesas electorales de los comicios del día 28/04/2019, lo que se efectúa a partir de unos números que se obtienen en dicho sorteo.

Después de un proceso informático se generaron dos archivos PDF, uno con la

lista de composición de cada mesa (titulares y suplentes) para ser comunicado a la Junta Electoral de Zona, y otros 19 archivos PDF (uno por distrito) con las notificaciones individuales a las personas elegidas.

El archivo con el listado completo para la Junta Electoral de Zona se llama VLC_C75_0001_ES_VA_todos.PDF, mientras que los otros se llaman VLC_C74_9000_D01.PDF a VLC_C74_9000_D19.PDF respectivamente.

El resultado de los procesos se colocó ese mismo día en la carpeta que usa Reprografía del ayuntamiento para proceder a su impresión (\\Dades2\dades2\ayun\SCT\NORMALDOCIC\00-REPROGRAFIA).

También se colocó en el servidor del Servicio de Tecnologías de la información y comunicación (SerTIC) (S:\Recursos Compartidos) por si hubiera que restablecer una copia para Reprografía, a la Junta Electoral (Servicio de Procesos Electorales) o al Servicio de Sociedad de la Información.

A dichos ficheros también tuvo acceso el servicio municipal de Sociedad de la Información.

Este fichero está registrado en el Registro de Actividades de Tratamiento con el nombre de PROCESOS ELECTORALES – CENSO ELECTORAL.

En fecha 05/04/2019 desde la JEZ se comunicó, telefónicamente, al Jefe del Servicio de Tecnologías de la Información y comunicación de este ayuntamiento, la existencia de una comunicación de un ciudadano en la que se indicaba que a través de la aplicación *whatsapp* estaba circulando un documento que contenía el listado de personas miembros de las mesas electorales correspondientes al sorteo llevado a cabo el día 2 de ese mismo mes. Ante dicha noticia, el Jefe del Servicio de Tecnologías de la Información y comunicación procedió, ese mismo día, a borrar el fichero que contenía los datos objeto de la filtración de todas las carpetas de la Red Local.

En fecha 06/04/2019 fue informada sobre los hechos, telefónicamente, también desde la JEZ, la Jefa del Servicio de Sociedad de la Información del este ayuntamiento.

En fecha 08/04/2019 la delegación de protección de datos tuvo conocimiento de los hechos por varias vías, una interna, a través del Servicio de Coordinación Jurídica y Procesos Electorales y otra externa, mediante comunicación telefónica efectuada por una ciudadana afectada.

A la vista de los hechos, desde la Delegación de protección de datos se interesó informe a todos los servicios municipales en los que pudo haberse tenido acceso a dicha información con el fin de intentar aclarar el alcance de la filtración y posibles orígenes de la misma.

De la información obtenida del Servicio de Tecnologías de la información y comunicación, se determinó que no se trataba de un ciberataque, sino ante una filtración o pérdida de datos por parte de alguna persona que tenía acceso a la información, si bien se desconocía si la filtración había tenido origen en el ayuntamiento o de la JEZ.

El número de personas afectadas fue de 8.334 y los datos personales se correspondían con el nombre y apellidos, DNI, dirección postal y cargo en la mesa electoral.

En fecha 16/04/2019 se formuló denuncia ante el Juzgado de Guardia de València. Se adjunta copia de la denuncia formulada.

En fecha 18/04/2019 se recibió comunicación de los Juzgados de València en al que se indicaba que había correspondiendo la instrucción al Juzgado de instrucción número 17, Diligencias Previas 692/2019 y que se había librado oficio a la Jefatura Superior de Policía a fin de que se procediera a la averiguación de los hechos denunciados e identificación de la persona autora.

En fecha 24/04/2019 se remitió comunicación de la brecha de confidencialidad a las personas afectadas siendo el contenido de la comunicación el siguiente:

Se adjunta un modelo de comunicación.

Como consecuencia de las investigaciones realizadas por la Policía, en fecha 17/05/2019 se procedió a detener a la persona presuntamente autora de los hechos, que resultó ser una persona empleada del Servicio de Tecnologías de la Información y Comunicación del Ayuntamiento de Valencia.

Como consecuencia de la identificación de la persona presuntamente autora de los hechos, desde la delegación de personal del Ayuntamiento se están estudiando las medidas disciplinarias que corresponda respecto de la persona investigada.

Por último, respecto al apartado de seguridad, cabe indicar que estamos ante un supuesto de filtración de la información por una de las personas usuarias que tenía acceso a la misma, por lo que, como se ha dicho, no se trata de un ciberataque.

Aporten ficha del Registro de Actividad correspondiente al tratamiento CENSO ELECTO-RAL: PROCESOS ELECTORALES - CENSO ELECTORAL.xlsx

Aportan copia de la Política de Seguridad aprobada por la Junta de Gobierno Local.

FUNDAMENTOS DE DERECHO

I

En virtud de los poderes de investigación y correctivos que el artículo 58 del Re-glamento (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 las quiebras de seguridad de los datos personales como aquellos incidentes que ocasionan la destrucción, pérdida o alteración accidental o ilícita de datos personales, así como la comunicación o acceso no autorizado a los mismos.

Desde el pasado 25/05/2018, la obligación de notificar a la Agencia las brechas o quiebras de seguridad que pudiesen afectar a datos personales es aplicable a cualquier responsable de un tratamiento de datos personales, lo que subraya la importancia de que todas las entidades conozcan cómo gestionarlas.

Por consiguiente, tan pronto como el responsable del tratamiento tenga conocimiento de que se ha producido una violación de la seguridad de los datos personales en el sentido señalado en el artículo 32 del RGPD debe, sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, notificar la violación de la seguridad de los datos personales a la autoridad de control competente, a menos que el responsable pueda demostrar, atendiendo al principio de responsabilidad proactiva, la improbabilidad de que la violación de la seguridad de los datos personales entrañe un riesgo para los derechos y las libertades de las personas físicas.

El responsable del tratamiento debe comunicar al interesado sin dilación indebida la violación de la seguridad de los datos personales en caso de que puede entrañar un alto riesgo para sus derechos y libertades, y permitirle tomar las precauciones necesarias. La comunicación debe describir la naturaleza de la violación de la seguridad de los datos personales y las recomendaciones para que la persona física afectada mitigue los potenciales efectos adversos resultantes de la violación.

Dichas comunicaciones a los interesados deben realizarse tan pronto como sea razonablemente posible y en estrecha cooperación con la autoridad de control, siguiendo sus orientaciones o las de otras autoridades competentes, como las autoridades policiales. Así, por ejemplo, la necesidad de mitigar un riesgo de daños y perjuicios inmediatos justificaría una rápida comunicación con los interesados, mientras que cabe justificar que la comunicación lleve más tiempo por la necesidad de aplicar medidas adecuadas para impedir violaciones de la seguridad de los datos personales continúas o similares.

También hay que señalar, que la notificación de una quiebra de seguridad no implica la imposición de una sanción de forma directa, ya que es necesario analizar la diligencia de responsables y encargados y las medidas de seguridad aplicadas.

La seguridad de los datos personales viene regulado en los artículos 32, 33 y 34 del RGPD.

En concreto el artículo 32 del RGPD *“Seguridad del tratamiento”,* establece que:

“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 artículo 33 del RGPD establece la forma en que ha de notificarse una violación de la seguridad de los datos personales a la autoridad de control, determinando 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."

Y el artículo 34 del Reglamento mencionado indica cuando es necesario informar de una violación de la seguridad de los datos personales al interesado, señalando lo siguiente:

"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 persona-les 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."

En este mismo sentido se señala en los Considerandos 85 y 86 del RGPD:

(85) Si no se toman a tiempo medidas adecuadas, las violaciones de la seguridad de los datos personales pueden entrañar daños y perjuicios físicos, materiales o inmateriales para las personas físicas, como pérdida de control sobre sus datos personales o restricción de sus derechos, discriminación, usurpación de identidad, pérdidas financieras, reversión no autorizada de la seudonimización, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, o cualquier otro perjuicio económico o social significativo para la persona física en cuestión. Por consiguiente, tan pronto como el responsable del tratamiento tenga conocimiento de que se ha producido una violación de la seguridad de los datos personales, el responsable debe, sin dilación indebida y, de ser posible, a más tardar

72 horas después de que haya tenido constancia de ella, notificar la violación de la seguridad de los datos personales a la autoridad de control competente, a menos que el responsable pueda demostrar, atendiendo al principio de responsabilidad proactiva, la improbabilidad de que la violación de la seguridad de los datos personales entrañe un riesgo para los derechos y las libertades de las personas físicas. Si dicha notificación no es posible en el plazo de 72 horas, debe acompañarse de una indicación de los motivos de la dilación, pudiendo facilitarse información por fases sin más dilación indebida.

(86) El responsable del tratamiento debe comunicar al interesado sin dilación indebida la violación de la seguridad de los datos personales en caso de que puede entrañar un alto riesgo para sus derechos y libertades, y permitirle tomar las precauciones necesarias. La comunicación debe describir la naturaleza de la violación de la seguridad de los datos personales y las recomendaciones para que la persona física afectada mitigue los potenciales efectos adversos resultantes de la violación. Dichas comunicaciones a los interesados deben realizarse tan pronto como sea razonablemente posible y en estrecha cooperación con la autoridad de control, siguiendo sus orientaciones o las de otras autoridades competentes, como las autoridades policiales. Así, por ejemplo, la necesidad de mitigar un riesgo de daños y perjuicios inmediatos justificaría una rápida comunicación con los interesados, mientras que cabe justificar que la comunicación lleve más tiempo por la necesidad de aplicar medidas adecuadas para impedir violaciones de la seguridad de los datos personales continuas o similares.

De la documentación obrante en el expediente ofrece indicios evidentes que de la brecha de seguridad provocada en los sistemas de la entidad vulnera el artículo 32 del RGPD, *Seguridad del tratamiento*, relacionada con la difusión de listas de mesas electorales a través de whatsapp, de la que tuvo conocimiento el 08/04/2019, mediante una llamada telefónica en la que una ciudadana les informaba que había recibido por dicho medio información sobre los componentes de las mesas electorales correspondientes al sorteo llevado a cabo en el Pleno de la Corporación del pasado día 02/04/2019.

En el presente caso, es de destacar que con independencia de la falla de seguridad producida las medidas técnicas y organizativas que habían sido adoptadas por el AV eran adecuadas y proporcionadas al nivel del riesgo existente que presentaba el tratamiento de datos. Las investigaciones llevadas a cabo por el Servicio de Tecnologías de la Información y Comunicación con el fin de identificar el incidente de seguridad producido, su clasificación, tipo de brecha, alcance, medidas a adoptar y su notificación a la AEPD, determinaron que no se trataba de un ciberataque sino de un filtración de la información, que las medidas implantadas y el nivel de seguridad eran adecuadas y proporcionadas para asegurar la confidencialidad de los datos, no existiendo certeza de que hubiera tenido su origen en el AV, ya que la referida información fue compartida con la Junta Electoral de Zona.

El mismo día que conocieron la brecha de seguridad la notificaron a la AEPD. Seguidamente se remitió comunicación de la brecha de confidencialidad a las personas afectadas adjuntándose el modelo de comunicación y como consecuencia de las investigaciones realizadas por la Policía, el 17/05/2019 se procedió a detener a la persona presuntamente autora de los hechos, que resultó ser una persona empleada del propio Servicio de Tecnologías de la Información y Comunicación del Ayuntamiento de Valencia.

Con posterioridad a lo que antecede se presentaron escritos de reclamación por personas afectadas por la brecha de seguridad.

III

Así las cosas, se ha acreditado que la actuación del reclamado como entidad responsable del tratamiento ha sido acorde con la normativa sobre protección de datos personales.

Por lo tanto, de acuerdo con lo señalado,

Por la Directora de la Agencia Española de Protección de Datos,

SE ACUERDA:

1. PROCEDER al **ARCHIVO** de las presentes actuaciones.

2. NOTIFICAR la presente resolución al AYUNTAMIENTO de VALENCIA, con NIF ***P4625200C***, junto con el ANEXO I y a cada uno de los reclamantes exclusivamente el ANEXO que le corresponda en el que se incluye su identificación.

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

ANEXO I

Denunciante 1: D. ***A.A.A.***
Denunciante 2: Dña. ***B.B.B.***
Denunciante 3: D. ***C.C.C.***
Denunciante 4: D. ***D.D.D.***
Denunciante 5: Dña. ***E.E.E.***
Denunciante 6: Dña. ***F.F.F.***

ANEXO II

Denunciante 1: D. ***A.A.A.***

ANEXO III

Denunciante 2: Dña. ***B.B.B.***

ANEXO IV

Denunciante 3: D. ***C.C.C.***

ANEXO V

Denunciante 4: D. ***D.D.D.***

ANEXO VI

Denunciante 5: Dña. ***E.E.E.***

ANEXO VII

Denunciante 6: Dña. ***F.F.F.***