- **Procedimiento Nº: E/04236/2021**

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: Como consecuencia de la notificación a la División de Innovación Tecnológica de esta Agencia de una brecha de seguridad de datos personales por parte del Responsable del Tratamiento **AYUNTAMIENTO DE ****LOCALIDAD.1*,** con número de registro de entrada ******REGISTRO.1***, que afecta a datos personales, se ordena a la Subdirección General de Inspección de Datos que valore la necesidad de realizar las oportunas investigaciones previas con el fin de determinar una posible vulneración de la normativa de protección de datos.

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 notificación, teniendo conocimiento de los siguientes extremos:

Fecha de notificación de la brecha de seguridad de datos personales: ******FECHA.1***
-Fecha de detección de la brecha: ******FECHA.2***
-Responsable: **AYUNTAMIENTO DE ****LOCALIDAD.1*** (en adelante el Ayuntamiento).

Resumen de la notificación:
(…). Aportan comunicado publicado en la web.

En la notificación adicional de fecha 12/04/2021 informan que ***(…),*** indicando que han presentado una denuncia ante la Policía Nacional y han contactado con el ***(…)***.

En la notificación adicional de 16/04/2021 indican que existen afectados ***(…)***.

La sección sindical del Ayuntamiento de Castellón del SINDICATO PROFESIONAL DE ***(…)*** ,han presentado reclamación ante esta Agencia indicando:
-Que a raíz del ciberataque que ha sufrido el Ayuntamiento han tenido conocimiento de que los atacantes han tenido acceso y descargado ***(…),*** etc.
- Que desde el Ayuntamiento no se les ha informado sobre qué datos han sido descargados, a quienes afectan y sobre las medidas a tomar al respecto.
Exigen que cada afectado sea informado de acuerdo con la situación concreta de sus datos personales, y que se justifiquen convenientemente las medidas de seguridad adoptadas.

Entidades investigadas:
Durante las presentes actuaciones se ha investigado la siguiente entidad:
AYUNTAMIENTO DE ****LOCALIDAD.1,*LOCALIDAD.1*** con CIF P1204000B.

Resultado de las actuaciones de investigación

Se constata que en el artículo de prensa, publicado en Internet por el diario ******DIARIO.1*** el 17 de abril de 2021, se ofrece una relación de la tipología de la información a la que ha accedido el diario, indicando que ha sido publicada en la ***XXXX XXX*** por el atacante al Ayuntamiento. El listado incluye como tipologías ***(…),*** entre otros. Se publican algunos trozos de documentos eliminando los datos personales, así como un documento ***(…)*** del Ayuntamiento.

Con fecha 20/04/2021 se solicitó información al responsable, recibiéndose respuesta en fecha 05/05/2021.

Con carácter previo los representantes del Ayuntamiento informan de lo siguiente:
*"Entre el pasado lunes 29 de marzo y el martes 30 del mismo mes este Ayuntamiento sufrió un ataque informático, comúnmente denominado "**XXXXXXXXX",** que afectó **(…).***
*Dicho ataque, constitutivo de una acción delictiva, coincide en el tiempo con una oleada de intrusiones de este tipo sufridas por otras Administraciones Públicas y entidades de nuestro entorno más inmediato. Desgraciadamente, y como es de sobra conocido, tales ataques han proliferado en el contexto de la pandemia producida por el COVID-19 en la que la necesidad de cumplir con la normativa sanitaria ha obligado a aumentar exponencialmente el número de empleados/as que han requerido el acceso remoto a servicios informáticos. El Ayuntamiento de *****LOCALIDAD.1** no ha sido ajeno a esta realidad, siendo necesario recurrir a modalidades de teletrabajo que permitieran mantener un nivel aceptable de prestación de los servicios municipales y, a la vez, garantizar la salud y protección de su personal.*
*Con posterioridad, los autores de dicho ilícito procedieron a la publicación en la "Dark Web" de una serie de información, indicando que la misma tenía origen en el Ayuntamiento. Todo ello con un claro ánimo lesivo para la reputación y los intereses de esta Corporación, que no son otros que los del conjunto de la ciudadanía y en particular de los vecinos y vecinas de *****LOCALIDAD.1**. Dicha publicación debe enmarcarse como el último hito de una estrategia de extorsión de la que esta Administración Pública nunca tuvo intención de participar siquiera como colaborador involuntario, tal y como se manifestó de forma clara e inequívoca desde el momento en que se detectó el ataque, informándose asimismo de esta circunstancia a la opinión pública.*
En este sentido, ante una situación inédita para este Ayuntamiento y a la vista de la extraordinaria gravedad de los hechos, esta Administración ha mostrado una actitud proactiva. A tal fin, una vez constatada la gravedad de la situación por el Ayuntamiento se activó el plan municipal de emergencias, constituyendo el órgano de coordinación previsto para las situaciones de grave riesgo, catástrofe o calamidad pública que afecten al municipio.
Además, se denunciaron los hechos ante la Policía Nacional, ampliando las denuncias en función de las nuevas revelaciones y se contactó con los organismos de asistencia en materia de ciberseguridad. Asimismo, en cumplimiento de la normativa en materia de protección de datos, se comunicaron a la Autoridad de Control tanto el incidente inicial de seguridad como las sucesivas circunstancias relevantes en relación con el mismo.
Por otro lado, este Ayuntamiento ha dispuesto lo necesario para minimizar el impacto del ciberataque en los servicios que presta a la ciudadanía y el funcionamiento de esta Administración. Asimismo, se ha mantenido una información constante a la ciudadanía

y a otros colectivos sobre la situación del ciberataque, conjugando el principio de transparencia con la necesaria cautela y discreción del proceso de investigación de un incidente de esta envergadura.
En el marco de la investigación iniciada por la Agencia Española de Protección de Datos el presente documento recoge la totalidad de actuaciones realizadas por esta Administración con la finalidad de minimizar los daños derivados del delito sufrido por este Ayuntamiento (y, por extensión, por el conjunto de la ciudadanía) y evitar su repetición. Se adjunta asimismo, documentación acreditativa de estas circunstancias.
No obstante, se informa que el presente documento se formula sin perjuicio de su posible ampliación si así se estima oportuno, toda vez que la agresividad de la intrusión impide en el momento de emisión del presente documento declarar que el incidente de seguridad se ha cerrado de forma completa. Asimismo, se hace constar que, con carácter general, la información del presente documento debe entenderse referida a fecha 3, 4 o 5 de mayo en función de la información disponible en cada caso."

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

En el presente apartado se expone un resumen cronológico de acciones que el Ayuntamiento y su personal manifiesta haber desarrollado en relación con la brecha de seguridad incluyendo las medidas de orden técnico, organizativo o de otra índole desarrolladas en este sentido, a partir de la información disponible y del conocimiento del estado de las investigaciones en cada momento. La presente cronología está actualizada a fecha 3 de mayo de 2021:

XXXXX (15.00) - Algunos usuarios del sistema informático municipal experimentan cortes en el servicio de aplicaciones corporativas. Algunos usuarios notifican que han aparecido mensajes de un aviso en el sistema antivirus, pero que el mensaje indica que ha sido detenido.
XXXXX (18.00*) -* Se detienen los cortes y se restablece normalmente el servicio.
XXXXX (1.00) - A las 1:00 del día 30 se detienen todos los servicios alojados en la infraestructura virtual.
XXXXX (7.45) - Coincidiendo con el inicio de la jornada laboral ordinaria algunos usuarios notifican que no pueden acceder a los servicios informáticos (web municipal, aplicación municipal de gestión de expedientes, plataforma de teletrabajo, acceso al correo electrónico corporativo, etc.)
XXXXX (8.00) – ***(…).***
El atacante o atacantes indican:
(…).
XXXXX (9.00) - Se contacta con la empresa contratada para el mantenimiento del hardware municipal que empieza a trabajar sobre el incidente con el equipo técnico informático municipal.
XXXXX (10.00) - Como medida inicial de contención ***(…).***
XXXXX (11.00) – ***(…)***.
Por una empresa externa ***(…).***
XXXXX (*XXXXXXX*) – Se contacta con el Delegado de Protección de Datos del Ayuntamiento (contrato de servicios con empresa externa, en adelante DPD), informándole de la posible brecha de seguridad.

XXXXX (*XXXXXXX*) - Por la Alcaldesa se informa verbalmente en la reunión del CECOPAL constituido con motivo del COVID (no confundir con el constituido al día siguiente al objeto de tratar específicamente sobre el presente incidente de seguridad) que se ha sufrido un ciberataque.
Por la Alcaldesa se informa que se va a poner en contacto con la concejala delegada de Administración Electrónica e Innovación Digital a los efectos de recabar mayor información.
XXXXX (17.30) – ***(…)***.
XXXXX (20.30) – *(…)*.
XXXXX (22.30) – *(…)*.
.
XXXXX (23.00) – ***(…)***.
XXXXX (1.00) – ***(…)***.
XXXXX (8.30) – Reunión semanal de Gerencia convocada por la Alcaldía. Asistencia de Secretaria General del Pleno, Interventor General, Asesora Jurídica, Secretario de Administración Municipal, Portavoz del Gobierno y Jefe de Gabinete de Alcaldía.
Se convoca al Director de Modernización que asiste a la reunión y expone la situación explicando que se ha sufrido ***(…).***
En la reunión se decide:
-a) Denunciar los hechos ante el CNP (se encomienda a concejala delegada de Admón.
Electrónica junto con Asesora Jurídica, Director de Modernización y Jefe SIDT).
-b) En el marco del Plan Municipal de Emergencias, la activación del CECOPAL (Centro de Coordinación Operativa Municipal) como mando único para la gestión de la emergencia bajo la dirección de 1) Alcaldesa; y participación de 2) Portavoz del Gobierno; 3) Concejala Admón. Electrónica; 4) Director de Modernización; 5) Jefe SIDT; 6) SGP; 7) Interventor General; 8) Titular Asesoría Jurídica 9) Director Servicios Urbanos; 10) Comisario Principal Policía Local; 11) Responsable de emergencias; 12) Jefa Gabinete de Comunicación; 13) Secretario Administración Municipal;
-c) Convocar Junta de Portavoces a los efectos de informar a los grupos políticos a las 14 horas.
XXXXX (11:00 aprox) Se presenta denuncia ante el CNP (asistencia de concejala delegada, Director de Modernización, Jefe SIDT y Titular Asesoría Jurídica). Aportan copia.
XXXXX (11:00) Se produce reunión del CECOPAL a los efectos de su activación, con todos los departamentos convocados por la Alcaldía
Se plantea la necesidad de afrontar la crisis con capacidad de reacción para los problemas más urgentes y se informa por las áreas participantes sus necesidades inmediatas, dando prioridad absoluta a las que se planteen por el área de seguridad y emergencias.
Se concluye:
Centrar los esfuerzos sobre las actuaciones administrativas urgentes que impliquen obligaciones ineludibles para el Ayuntamiento.
(…).
A modo de canales de comunicación: ***(…)***.
.

A continuación se producen una serie de reuniones y acciones para la gestión del incidente y restauración paulatina de los servicios que incluyen, de forma resumida, y entre otras muchas:
XXXXX Mediante reunión de la Junta de Portavoces se informa a los grupos políticos municipales. Se informa que según informaciones del CNP, se trata de ***(…)***.
XXXXX ***(…)***.
XXXXX Conjuntamente con el DPD, se comunica el incidente de seguridad a la Agencia Española de Protección de Datos, según la información disponible en ese momento.
XXXXX Reunión informativa con los/as funcionarios/as responsables administrativos de los departamentos (Jefes/as de Sección y órganos equivalentes o superiores).
XXXXX Reunión informativa con representación sindical de empleados.
XXXXX Reunión de técnicos municipales con ***(…)***.
XXXXX *(…)***.**
XXXXX Se remite una infografía sobre seguridad informática a todos/as los/as usuarios del Ayuntamiento a través de las correspondientes jefaturas ***(…)***.
XXXXX Reunión del CECOPAL, entre otros muchos temas se tratan las siguientes cuestiones***: (…).***
XXXXX El sábado 10 a las 11:45 se descubre que la información ha sido publicada ***(…)***. Diariamente se realizaba una verificación ***(…)***.
XXXXX *(…).*
XXXXX Aparecen tuits en la red social Twitter que informan de la existencia de esta información.
XXXXX Vía telefónica se contacta con ***(…)***.
XXXXX Se amplía la denuncia ante el CNP (concejala de Administración Electrónica, Director de Modernización, Jefe SIDT y Letrada Asesoría Jurídica). Se comunica a la AEPD las nuevas circunstancias de la exfiltración de información con la información disponible en el momento.
XXXXX *(…).*
XXXXX Reunión del CECOPAL, se incorpora durante la reunión la Titular de la Asesoría Jurídica, y entre otros temas se valora la viabilidad de acciones judiciales contra la publicidad de la exfiltración (publicaciones en red social Twitter) concluyendo que únicamente procede advertir del ejercicio de acciones judiciales en caso de difusión de la información publicada. Asimismo, se acuerda que en la comunicación de prensa que se realice se recuerde para general conocimiento que la información exfiltrada y referenciada en la publicación como propia del Ayuntamiento de Castelló ha sido obtenida de manera delictiva.
XXXXX ***(…)***.
A la vista de dicho análisis somero y sucinto se concluye que la intrusión potencialmente puede incluir información de gran parte de las áreas del Ayuntamiento y que aunque en el momento no se puede evaluar qué información ha sido objeto de publicación sí cabe concluir que se trata de información diversa sobre diversos ámbitos la actividad municipal.
Se decide convocar con urgencia al Delegado de Protección de Datos para una reunión a los efectos de informarle y tratar esta cuestión. Se incorpora

a la reunión la concejala delegada de Administración Electrónica e Innovación Digital.

XXXXX En reunión con el Delegado de Protección de Datos, se le informa del resultado del examen somero de los archivos. Se pone de manifiesto la importancia de comunicar esta circunstancia a la AEPD. Por el DPD se informa asimismo de que no constan precedentes de intrusiones de este nivel. Se recomienda seguir las recomendaciones del CNP.
XXXXX Reunión del CECOPAL (con la asistencia de Titular de la Asesoría Jurídica) se pone de manifiesto la necesidad de contactar con todos los organismos implicados ***(XXXXXXXXX)*** así como comunicar formalmente la brecha de seguridad a la AEPD y denunciar las nuevas revelaciones al CNP. Se advierte la inexistencia de precedentes sobre este tipo de intrusión y la conveniencia de recabar asesoramiento. Se estudia la problemática de la gestión de la comunicación a la vista del potencial número de personas afectadas y la disparidad de los datos y situaciones que podrían haberse visto comprometidos por tratarse de información que carece de una estructura lógica.
A la vista de la sensibilidad de los datos relativos a personas ***XXXXXXXXXX*** se convoca de urgencia para una reunión al concejal delegado de seguridad pública y al personal de su área a los efectos de adopción de medidas inmediatas de protección a las personas en dicha situación y cuantas otras se consideren oportunas por el área de seguridad pública y emergencias.
XXXXX Ampliación de la comunicación a la AEPD, incluyendo los datos conocidos con motivo del examen somero de los archivos. Se aumenta la calificación del riesgo para las personas afectadas (nivel alto) ***(…)***. Se adjuntan a la comunicación los comunicados oficiales publicados por el Ayuntamiento.
XXXXX Se detecta la publicación de una noticia en el medio digital “El Confidencial”. Por el departamento de comunicación del Ayuntamiento se trata de contactar con el autor de la información, sin éxito.
XXXXX Asistencia de personal del ***XXXXXX*** a dependencias municipales para ***(…)***.
XXXXX Se constituye una comisión junto con personal de ***(…)*** para la valoración del proceso de catalogación de la información (asiste Titular Asesoría Jurídica con incorporación posterior de Director de Modernización junto con personal CSIRT-CV y S2).
Por la empresa analista *(…).*
XXXXX ***(…)****.*
XXXXX Reunión Comisión Mixta revisión análisis de los datos resumiendo la situación indicando:
i) Que se trata de datos heterogéneos, de fuentes diversas y variadas (documentos pdf, fotografías, escaneos, hojas de cálculo);
ii) que no se han extraído ***(…)****;*
iii) que, además, ***(…)*** y
iv) que se debe poner de manifiesto el esfuerzo realizado por la organización para catalogar los datos.
XXXXX Reunión con empresa externa, se presentan las propuestas de la empresa en materia de cyberseguridad y, en concreto, ***(…)***.
XXXXX Reunión comisión mixta análisis datos: ***(…)***.

- Se informa por empresa externa que se ha categorizado como***.***
- Se informa ***(…),*** siendo la primera referencia en este sentido para el Ayuntamiento.
- Se plantea la posibilidad de asumir como un servicio propio a contratar por el Ayuntamiento ***(…)***.

XXXXX Reunión comisión mixta análisis datos. Se expone el estado del proceso de categorización de la información, indicándose que ***(…)***.

Respecto de las causas que hicieron posible la brecha

En el presente apartado, a modo de resumen sobre las causas posibles que han hecho posible la brecha, se incluye la relación de hechos derivado de la investigación de la intrusión según la información de la que dispone el Ayuntamiento en el momento de emisión de la contestación a esta Agencia. Informan que dicho apartado se ha laborado a partir de la información obtenida por los ***(…) .*** Indican que la presente mención sirve de muestra del agradecimiento de la Corporación a estos organismos por la asistencia prestada, de incalculable valor ante la gravedad de la situación.

Indican que se formula la presente relación de causas posibles de la brecha de seguridad a partir de la información disponible en el momento de emisión de la contestación a esta Agencia. Se informa que la presente relación de causas se emite a la vista de la información proporcionada al Ayuntamiento por ***(…)***. Advierten que, en todo caso, la presente relación está condicionada a las nuevas averiguaciones que puedan aparecer con ocasión de la investigación, desarrollada tanto desde el punto de vista técnico por el ***XXXXXXXXXX*** como por la investigación policial por parte del departamento de ciberdelito de la Policía Nacional.

Las primeras alertas tuvieron lugar el 28 de marzo 2021 y***, (…).***

La siguiente actividad sospechosa detectada se produce el lunes 29 de marzo, a las 15:22h, ***(…).***

A raíz de la actividad detectada el 29 de marzo, se produce ***(…).***

Los representantes del Ayuntamiento describen las diferentes posibilidades ***(…).***

Respecto de los datos afectados.

El Ayuntamiento una vez constatado el volumen y la complejidad de la intrusión contactó con el ***(…).***

En este sentido, advierten que la información publicada (y anunciada como de procedencia municipal) no se corresponde con información obtenida a partir de ***(…).***

Realizadas estas consideraciones previas proceden a la transcripción del informe de la empresa externa (que adjuntan):

“ […]

Indican que se está procediendo a revisar ***(…)***. No obstante, señalan que se trata de un proceso lento y tedioso por el volumen de documentos
que han sido expuestos.

Señalan que las conclusiones a las que pueden llegar actualmente, tras la revisión a alto nivel (no se desciende a revisar el contenido íntegro de cada fichero) de aproximadamente ***(…).***

Destacan la dificultad para poder identificar a cada uno de los afectados, puesto que ***(…),*** dificultando la labor del Ayuntamiento para poder notificar a los afectados sin dilación indebida, no siendo posible por consiguiente la implementación de forma inmediata de un plan de acción por parte del Ayuntamiento para proceder a dicha comunicación conforme requiere el artículo 34 RGPD.

Indican que el Ayuntamiento está a la espera de disponer de la relación de afectados con la información mínima necesaria y contrastada para habilitar un procedimiento de comunicación a los posibles interesados, con el objetivo de informar tanto del alcance en cuanto a la filtración de sus datos, como de facilitar indicaciones o recomendaciones que estos podrán llevar a cabo para mitigar posibles riesgos, además de las iniciativas que el propio Ayuntamiento está ejecutando para reducir los riesgos que se puedan producir en los derechos y libertades de los interesados.

El Ayuntamiento indica que en relación con posibles consecuencias para las personas afectadas, se informa que dicha calificación está pendiente de completar el proceso de categorización de la información publicada, y que, una vez se complete la categorización de los datos publicados en la ***XXXX-XXX*** se iniciará un proceso para la catalogación de posibles riesgos de personas afectadas, informándose en este sentido del resultado de dicha catalogación a las personas afectadas en función de la tipología de datos que pudieran haberse visto comprometidos en cada caso.

Indican que cualquier utilización fraudulenta de cualquier dato obtenido por cualquier medio y/o persona a partir de la información publicada en la ***XXX-XXXX*** tendría su origen en un ilícito penal, habiéndose advertido de esta circunstancia por el Ayuntamiento a través de sus comunicados de prensa y haciéndose constar que esta Administración ejercerá dentro de sus competencias las acciones judiciales oportunas para la protección de las personas.

Quieren hacer constar, a fin de acreditar la actitud proactiva del Ayuntamiento en relación con los riesgos expuestos que, de manera proactiva, el Ayuntamiento de ******LOCALIDAD.1*** ha encargado un ***(…)***.

Asimismo, hacen constar que el Ayuntamiento ha puesto en conocimiento inmediato del Cuerpo Nacional de Policía las revelaciones que, sucesivamente, se han ido recabando, participando asimismo en reuniones informativas con la finalidad de adoptar las medidas precisas para la protección de los derechos y libertades de las personas afectadas, teniendo en cuenta que en el momento actual no se puede concretar qué personas pueden haberse visto afectadas por la publicación.

En particular, y en relación con la mención a las personas ***XXXXXXXXXX-XX*** (14 de abril) se convocó de manera inmediata a una reunión a los responsables de la Policía Local a fin de que adoptaran las medidas precisas para la protección de dichas personas. Asimismo, con ocasión de la ampliación de la denuncia (15 de abril) se informó de esta circunstancia a la Policía Nacional. Todo ello a los efectos de la adopción de las medidas urgentes dirigidas a la protección de este colectivo de ***XXXXXXXXXXX***.

Por otro lado, indican que se ha informado a los trabajadores municipales de la conveniencia de adoptar ***(…),*** en línea con las que se venían realizando a lo largo del tiempo.

Respecto de la publicación del Diario “El confidencial”

El Ayuntamiento informa que:
- El Ayuntamiento no fue conocedor de que el medio en cuestión había tenido acceso a información exfiltrada hasta su publicación el 17 de abril.
- Enterado el Ayuntamiento de la publicación, por el servicio municipal de comunicación se trató de contactar con el medio con la finalidad de ofrecer la versión del Ayuntamiento, en el cumplimiento de la regla básica del periodismo de ofrecer la posibilidad de réplica de las partes afectadas, sin que fuera posible contactar con el medio o con el autor de la información.
- Una vez el Ayuntamiento recuperó el acceso al correo electrónico corporativo en la semana del 26 de abril, el Gabinete de Comunicación pudo constatar que se había recibido un email del autor del artículo con fecha del 14 de abril, avisando de que había tenido acceso a datos exfiltrados. Asimismo, indicaba que estaban preparando un reportaje al respecto y pedía la versión del Ayuntamiento. Ese mensaje no pudo ser recepcionado y, por tanto, tampoco contestado por parte del Ayuntamiento antes de la publicación citada porque el servicio de correo electrónico se encontraba inoperativo a causa del ciberataque.
- Se desconoce por el Ayuntamiento la forma en que por el medio en cuestión se accedió a la información publicada en la ***XXXXXXX***, si bien se advierte que por el Ayuntamiento se informó al público mediante comunicados de prensa que el origen de dicha exfiltración de información procedía de un ilícito penal con advertencia expresa de las responsabilidades en que se podía incurrir por la difusión de dicha información.

Indican que no consta que se haya utilizado por terceros los datos exfiltrados y que desde el momento en que el Ayuntamiento tuviera constancia en este sentido de cualquier utilización por terceros de los datos obtenidos a través de la brecha ejercerá cuantas acciones estén a su alcance para la protección de los derechos y libertades de las personas afectadas.

El Ayuntamiento indica que por el ***XXXXXXX*** se informa que los datos***,*** *publicados en* la ***XXXXXXX*** estuvieron accesibles desde el 11 de abril y que el 18 del mismo mes dejaron de estar accesibles en dicha ubicación. No obstante, se informa por el CSIRT-CV que con posterioridad se volvieron a publicar dichos datos. A este respecto, hacen constar que el Ayuntamiento no dispone de ninguna herramienta tecnológica o de cualquier otro tipo que impida que se realicen este tipo de publicaciones. No obstante, y tal y como se ha indicado ya, ***(…)*** en los derechos y libertades de las personas afectadas. Según la información de la que dispone el Ayuntamiento hasta el momento la publicación únicamente se ha producido en la dark web, por lo que dicha información no está accesible a personas que carezcan de conocimientos informáticos avanzados.

Manifiestan que desconocen el fundamento en que se basa la información para afirmar que la información publicada fue vista por más de 2500 personas.

Solicitada confirmación sobre las categorías de los datos exfiltrados que se publican en el artículo de El Confidencial, informan que la categorización de la información se está realizando según la metodología empleada por la empresa externa contratada tal y como se ha expuesto con anterioridad. En este sentido, indican que no es posible determinar la existencia o no de datos de la totalidad de tipologías mencionadas en la noticia, haciéndose constar además, lo laborioso y costoso del proceso de categorización de la información, no siendo posible en este momento introducir esas

variables en la metodología de catalogación de los datos (toda vez que está pendiente de catalogar algo menos del 50% de los ficheros). En cualquier caso, se informa que de los datos examinados hasta el momento sí consta información relacionada en cierto modo con las tipologías señaladas. Así y tal y como se ha expuesto en relación con el informe elaborado por la empresa externa, en la información publicada se ha detectado la existencia de datos relacionados con ***XXXXXXXXXXX.***
Manifiestan que en todo caso, cabe señalar que hasta el momento y según el proceso de categorización desarrollado por la empresa externa esta información representa los siguientes datos:

-(…)
-(…)
-(…)
-(…)
-(…)
-(…)

Respecto de la notificación realizada a las personas afectadas
El Ayuntamiento informa que, de acuerdo con lo expuesto previamente sobre el proceso de examen y categorización de los datos hasta el momento no se ha realizado ninguna notificación individualizada a los ciudadanos y ciudadanas afectadas, toda vez que no ha concluido el proceso de categorización de la información publicada que permita la identificación completa de las concretas personas afectadas.
En este sentido, señalan que el considerando 86 del Reglamento General de Protección de Datos indica que:
"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."
Los representantes del Ayuntamiento manifiestan que:
"En línea con el precepto transcrito, debe tenerse en cuenta que dicha comunicación todavía no se ha producido con la finalidad de no aumentar indebidamente la alarma social, al carecer el Ayuntamiento de la información completa sobre el alcance de la publicación, y ponderando el perjuicio que podría suponer la realización de una comunicación genérica e indiscriminada en la que se advirtiera de que se han visto comprometidos los datos de un número indeterminado de personas, sin conocer el número exacto de personas afectadas.
No debe perderse de vista que no se han encontrado antecedentes similares que permitieran establecer pautas concretas de actuación toda vez que tal y como se ha puesto de manifiesto los datos publicados proceden de fuentes heterogéneas y no responden a una estructura lógica, impidiendo que la información de las personas afectadas pueda ser explotada para su comprobación y revisión de una manera razonable. No en vano, a la vista del número de archivos incluidos en la publicación la sola identificación de las tipologías de datos afectados ya exige una labor minuciosa y extensa, tal y como ha informado la empresa que está desarrollando la empresa encargada de la categorización de los datos.

Abunda en lo anterior el hecho de que posiblemente puede haber casos en que no se podrá completar la comunicación personal a las personas afectadas por no disponer de datos de contacto de las mismas.
En este sentido, y visto que previsiblemente el número de personas resultará elevado (e, incluso que no pueda llegar a determinarse de forma exacta en su totalidad) se va a distinguir las siguientes medidas de comunicación, en el marco de un plan específico de comunicación que se elaborará al efecto:

- *La realización de notificaciones individualizadas y personales en aquellos casos en que los colectivos de personas afectadas resulten claramente identificadas y, además, se entiendan incluidos en colectivos especialmente vulnerables, tales como* ***(…).*** *En este caso, la notificación se realizará de manera individualizada a través de los servicios municipales que habitualmente se relacionan con estas personas para evitar que el tratamiento que implicará la realización de estas comunicaciones pueda generar perjuicios adicionales a sus derechos y libertades.*

- *Igualmente, en aquellos casos en que la naturaleza de los datos publicados pudiera implicar un mayor riesgo para las personas afectadas, junto a la comunicación se procederá a realizar las acciones que se determinen por las autoridades competentes (principalmente las policiales) a los efectos de proteger los derechos y libertades que pudieran verse afectadas. Todo ello sin perjuicio de aquellas medidas que, más allá de la comunicación formal se han venido disponiendo por el Ayuntamiento para la protección inmediata de las personas.*

- *Asimismo, en el caso de colectivos acotados y perfectamente individualizados (como(p.ej., en el caso de empleados/as municipales y otros usuarios/as de los servicios informáticos del Ayuntamiento) se realizarán notificaciones individuales. Todo ello sin perjuicio de las comunicaciones que ya se han venido realizando.*

- *Por último, y de conformidad con el art. 34.3 c) del Reglamento General de Protección de Datos se realizará una comunicación general para el resto de afectados cuyos datos básicos puedan haberse visto comprometidos. Está prevista la realización de una comunicación pública mediante anuncios en medios de difusión ordinarios, básicamente la página web municipal.*

- *Asimismo, en la medida que pudieran presentarse solicitudes individuales de personas solicitando información sobre sus datos, tales solicitudes serán atendida en función de los medios y la disponibilidad de acceso a la información.*

En cualquier caso, tales comunicaciones incluirán la totalidad de aspectos incluidos en la normativa de protección de datos y serán objeto de revisión previa por el Delegado de Protección de Datos de este Ayuntamiento.
Además de lo anterior, y de conformidad con lo establecido en el Reglamento General de Protección de Datos se informa que este Ayuntamiento está dispuesto a cumplir con las instrucciones o recomendaciones que, sobre este proceso de comunicación y el contenido de las mismas, pudiera plantear la Autoridad de Control.
En cualquier caso, y tal y como se ha ido exponiendo con anterioridad se informa por el Ayuntamiento:

1.- Que el no haber formulado una comunicación personal y directa a las personas afectadas no implica que no se haya informado a la opinión pública a través de los medios de comunicación y los canales oficiales de información del Ayuntamiento del alcance del ciberataque y sus dimensiones.
En este sentido, se debe poner de manifiesto, que según informa el Gabinete de Comunicación Municipal por este Ayuntamiento se han remitido 14 notas de prensa o comunicados oficiales desde el 30 de marzo hasta el 22 de abril, así como participación en ruedas de prensa, publicaciones periódicas en redes sociales oficiales, intervenciones en medios y gestiones con los medios de comunicación.
2.- Por otra parte, se han adoptado las medidas precisas para, más allá de la comunicación formal a las personas afectadas, evitar los riesgos inmediatos a las personas más vulnerables. Así, tan pronto se detectó la existencia de información publicada sobre personas ***XXXXXXXXXX*** *se procedió a comunicar esta circunstancia a la Policía Local con la finalidad de que se adoptaran las medidas inmediatas de protección a las personas.*
3.- Asimismo, a nivel interno se ha mantenido una constante comunicación a nivel interno. Así, tal y como se informa en la cronología de actuaciones municipales, se han mantenido reuniones de información con los Portavoces de los grupos políticos municipales , los miembros del Gobierno Municipal, los/as empleados/as responsables de los distintos departamentos y la representación sindical de los trabajadores/as municipales.
Asimismo, se han realizado comunicados internos informando del estado de la situación y se han incluido medidas específicas de información y concienciación (así, por ejemplo, ***(…)****. Todo ello en un contexto en que la imposibilidad del uso de las herramientas habituales de comunicación (correo electrónico corporativo, intranet) ha obligado al uso de canales informales (como p.ej****. (…)****.*
Además, el pasado 29 de abril, la concejala delegada de Administración Electrónica e Innovación Digital compareció, a solicitud propia, ante el Pleno del Ayuntamiento.
4.- Asimismo, se hace constar que, tal y como se ha informado con anterioridad, por el Ayuntamiento se ha encomendado ***(…).***
5.- Por otro lado, y en relación con las molestias que se han podido ocasionar a las personas interesadas con ocasión del incidente, por este Ayuntamiento se han adoptado una serie de medidas tendentes a reducir los perjuicios derivados de las consecuencias del ciberataque. En este sentido, una vez completada la fase de contención y tras asegurar las necesidades básicas del área de Seguridad y Emergencias se estableció la necesidad de priorizar los servicios de información y atención a la ciudadanía, permitiendo de este modo la activación de la sede electrónica y la reapertura de los servicios presenciales de atención e información. De forma adicional a lo anterior se pueden destacar las siguientes medidas:

- ***(…)***

- ***(…)***

la comunicación formal a otras Administraciones Públicas de las especiales circunstancias del Ayuntamiento a fin de acreditar eventuales incumplimientos de plazos u otras obligaciones."

Adjuntan copia del informe de la responsable del servicio municipal de comunicación con copia de los comunicados de prensa emitidos, copia de los comunicados internos informando del estado de la situación y de las medidas específicas de información y

concienciación por WhatsApp, así como de las medidas mencionadas para reducir los perjuicios que se han podido ocasionar a los ciudadanos.

Respecto de las medidas de seguridad implantadas

Con **XXXXXXX**

Los representantes del Ayuntamiento describen un conjunto de ***(…).***

El Ayuntamiento manifiesta que conoció, ***(…) XXXXXXXXXX.***

El Ayuntamiento indica que cabe inferir en este momento la opción más probable ***(…).***

El Ayuntamiento informa además que ***(…)*** este tipo de ***XXXXXXXXXX (…).***

Manifiestan que tales conclusiones están condicionadas a las nuevas averiguaciones que puedan aparecer con ocasión de la investigación, desarrollada tanto desde el punto de vista técnico por el ***XXX*** y el ***XXXXXXXX*** como por la investigación policial por parte del departamento de ciberdelito de la Policía Nacional.

Con **XXXXXXXX**
Describen las tareas desarrolladas para la recuperación del servicio, ***(…)***.

TERCERO: La reclamación interpuesta por **SINDICATO PROFESIONAL DE *XXXXXXXXX*** (en adelante, el reclamante) tiene entrada con fecha 19 de abril de 2021 en la Agencia Española de Protección de Datos. La reclamación se dirige contra el Ayuntamiento y solicitan información acerca de qué datos han sido descargados, a quienes afectan y sobre las medidas a tomar al respecto, y exigen que cada afectado sea informado, de acuerdo con la situación concreta de sus datos personales, y que se justifiquen convenientemente las medidas de seguridad adoptadas.
Dicha reclamación se incorpora al expediente previamente iniciado.

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 artículo 4 apartado 12 del 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 5 apartado 1 f) del RGPD establece que "*Los datos personales serán tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas («integridad y confidencialidad»)".*

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.

Artículo 32

"Seguridad del tratamiento

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".

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. Dicha documentación permitirá a la autoridad de control verificar el cumplimiento de lo dispuesto en el presente artículo".

Artículo 34:

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

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. L 119/52 ES Diario Oficial de la Unión Europea 4.5.2016

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."

En el presente caso, consta una brecha de seguridad de datos personales en las circunstancias arriba indicadas, categorizada como brecha de confidencialidad, al haber tenido acceso a datos personales personas no autorizadas a ello.

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.

De la documentación aportada por la entidad investigada en el curso de estas actuaciones de investigación se desprende que, con anterioridad a producirse la brecha, disponía de medidas de seguridad y organizativas preventivas razonables para evitar este tipo de incidencias, y acordes con el nivel de riesgo, pues no hay que perder de

vista la dificultad que entraña afrontar con una seguridad del 100% un ataque de tipo ***XXXXXXXXX.***

Hay que destacar la rápida actuación del Ayuntamiento desde el mismo momento en que tuvo conocimiento de los hechos, adoptando una actitud proactiva en su resolución, activando de manera inmediata el plan municipal de emergencias Se denunciaron los hechos ante la Policía Nacional y se contactó con los organismos de asistencia en materia de ciberseguridad, comunicando a la Autoridad de Control tanto el incidente inicial de seguridad como las sucesivas circunstancias relevantes en relación con el mismo.

Tras el requerimiento de información llevado a cabo por la Inspección de esta AEPD, la investigada ha informado de las nuevas medidas implementadas en orden a prevenir posibles ataques futuros, ***(…).***

No constan reclamaciones ante esta AEPD por parte de posibles usuarios afectados.

III

Por lo tanto, se ha acreditado que la actuación del Ayuntamiento, como entidad responsable del tratamiento, ha sido acorde 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 al **SINDICATO PROFESIONAL DE *XXXXXXXXX* DE LA COMUNIDAD VALENCIANA** y al **AYUNTAMIENTO DE ****LOCALIDAD.1*, ***LOCALIDAD.1** con CIF P1204000B.

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.

940-0419

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