Identificación del expediente

Resolución de procedimiento sancionador núm. nº. PS 3/2023, referente a la Agència Catalana del Consum.

Antecedentes

1. En fecha 27/10/2021 tuvo entrada en la Autoridad Catalana de Protección de Datos un escrito por el cual una persona formulaba una denuncia contra la Agencia Catalana del Consumo, organismo autónomo adscrito al Departamento de Empresa y Trabajo de la Generalitat, con motivo de un presunto incumplimiento de la normativa sobre protección de datos personales.

En concreto, la persona denunciante exponía que la web de la Agencia Catalana del Consumo (en adelante, Agencia), y especialmente el formulario para presentar reclamaciones *"estaba bajo una conexión insegura"* . Manifestaba que, por tal motivo, se había dirigido al delegado de protección de datos de la Agencia, quien le habría contestado que " *no harán nada por solucionarlo hasta enero de 2022"* . A efectos de acreditar su denuncia, aportaba dos correos electrónicos:

- Un correo que la persona denunciante envió en fecha 30/09/2021 a la dirección *"Buzón LOPD"* de la Agencia (lopd.acc@gencat.cat) con el asunto *"inseguridad en formularios con datos personales"* , en el cual ponía de manifiesto, tanto lo que consideraba una conexión insegura de su web corporativa - aludiendo a la falta de un certificado seguro-, como eventuales "problemas *de filtración de datos personales cuando se estén rellenando formularios",* derivados de la carencia de un certificado seguro.

- Un correo de respuesta de la Agencia, enviado en fecha 27/10/2021 desde la dirección lopd.acc@gencat.cat a la persona aquí denunciante, en el que se señalaba lo siguiente:

  "(...) Actualmente se está haciendo la migración del portal consum.gencat.cat lo que comportará que los formularios de reclamaciones también quedarán bajo el protocolo seguro https . La previsión es que esta migración quedará completada el próximo mes de enero. En cualquier caso, es necesario tener en cuenta que los datos de los formularios se envían a nuestro gestor de expedientes mediante un servicio web. Este servicio web, que recoge los datos de los formularios y los hace llegar al gestor de expedientes, sí se encuentra bajo protocolo seguro (...)"

2. La Autoridad abrió una fase de información previa (núm. IP 434/2021), de acuerdo con lo que prevé el artículo 7 del Decreto 278/1993, de 9 de noviembre, sobre el procedimiento sancionador de aplicación a los ámbitos de competencia de la Generalidad, y el artículo 55.2 de la Ley 39/2015, de 1 de octubre, del procedimiento administrativo común de las administraciones públicas (en adelante, LPAC), para determinar si los hechos eran susceptibles motivar la incoación de un procedimiento sancionador.

Traducción automática

3. En esta fase de información, en fecha 04/11/2022 el Área de Inspección de la Autoridad realizó una serie de comprobaciones a través de Internet sobre los hechos objeto de denuncia. Así, se constató que el formulario que figuraba en la web de la Agencia, para la formulación de reclamaciones o denuncias ante esta entidad, disponía de un certificado de autenticación del sitio web (con conexión cifrada). Del resultado obtenido se levantó la correspondiente diligencia de constancia.

4. En fecha 11/11/2022 se requirió a la Agencia para que informara sobre diversas cuestiones relativas a los hechos denunciados.

5. En fecha 20/12/2022, la Agencia respondió a dicho requerimiento a través de escrito en el que exponía lo siguiente:

- Sobre si a la fecha de los hechos denunciados (27/10/2021), la web de la Agencia Catalana de Consumo no disponía de un certificado de autenticación de su sitio web corporativo (certificado SSL/TLS u otro), y no tenía implementado el protocolo https u otro protocolo de transferencia de archivos con conexiones cifradas; y si en la actualidad ya disponía de uno:

  "El 27/10/2021 el sitio web principal (consum.gencat.cat) no estaba protegido por certificado https .
  En la actualidad sí se dispone de certificado CDS consum.gencat.cat (datos debajo), migrante todo el sistema (sitio web y formularios que cuelgan) a fecha 17/11/2021.
  A continuación reproducimos la información de la captura de pantalla de puesta en producción del sistema cifrado a fecha noviembre 2021. En su caso podemos enviar información adicional en relación al certificado así como el intercambio de correos con proveedor de la aplicación durante el proceso de validación de la puesta en marcha.
  Datos del certificado generado en 2021, con validez de 1 año. (...)

  Nombre: consum.gencat.cat
  (...)
  Aplicación-
  Servicio-
  Departamento: EMT
  Tipo: SSL
  Autoridad: Sectigo

  El certificado fue renovado el pasado mes de octubre de este año 2022. El Certificado está calificado bajo CA Sectigo (los datos del certificado que se muestran a continuación son los que se pueden ver y comprobar en la página web de la Agencia).
  Datos del certificado vigente. (...)

- Sobre si durante el período de tiempo en que la Agencia no disponía de un certificado de autenticación de su sitio web, el envío y grabación de los datos personales que se efectuaba a través de los formularios web (en todo caso , de los formularios dirigidos a enviar una reclamación), se efectuaba en el marco de un certificado de autenticación del sitio web (con una conexión cifrada) y en su caso, de qué certificado se trataba, y si correspondía a un certificado calificado:

  Aunque antes de noviembre de 2021, la web GECO consum.gencat.cat no era segura

Traducción automática

(HTTP), las llamadas al sistema destino (SIC) para enviar los datos de los formularios web (entre ellos los de reclamación) siempre se son hechos por protocolo seguro (HTTPS). El servicio invocado es el siguiente:
https://empresa.extranet.gencat.cat/sicweb/AppJava/services/SicWebNvSOAP
A continuación facilitamos los datos del certificado de servicio invocado por los formularios. Hay constancia del histórico de este certificado desde 2015, actualmente renovado y con CA Sectigo hasta 2023 (captura debajo):
Nombre: empresa.extranet.gencat.cat
(...)
Aplicación-
Servicio-
DepartamentEMC
TipoSSL
AutoridadCatCert

(...)"

- En cuanto a los formularios web, sobre si durante el período de tiempo en que la Agencia no disponía de un certificado de autenticación del sitio web, cuando un usuario enviaba datos personales (formulaba una consulta, una reclamación, una queja o una denuncia, entre otros), después de haber enviado los datos, en la respuesta del servicio web correspondiente al envío figuraban datos personales:

  "La respuesta del servicio invocado por los formularios web no contiene datos personales, sólo contiene un número de expediente. Como evidencia de este punto, adjuntamos el siguiente enlace a través del cual podrá acceder al archivo xml / descriptor del servicio web que invocan los formularios: (...) "

La Agencia acompañaba su escrito de documentación diversa.

6. En fecha 13/01/2023, la directora de la Autoridad Catalana de Protección de Datos acordó iniciar un procedimiento sancionador contra la Agencia Catalana del Consumo por una presunta infracción prevista en el artículo 83.4.a), en relación con el artículo 32.1, ambos del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril, relativo a la protección de las personas físicas en cuanto al tratamiento de datos personales ya la libre circulación de éstas (en adelante, RGPD).

Este acuerdo de iniciación se notificó a dicha Agencia en fecha 13/01/2023.

En el acuerdo de iniciación se concedía a la Agencia un plazo de 10 días hábiles para formular alegaciones y proponer la práctica de pruebas que considerase convenientes para defender sus intereses.

El plazo se ha superado con creces y no se han presentado alegaciones.

Hechos probados

El sitio web principal de la Agencia Catalana del Consumo, consum.gencat.cat, durante un período de tiempo indeterminado, pero en todo caso hasta el 28/10/2021 según ha reconocido la entidad, no disponía de un certificado de autenticación de su sitio web

Traducción automática

corporativo (certificado SSL/TLS u otro), y no tenía implementado el protocolo HTTPS ni otro protocolo de transferencia de archivos con conexiones cifradas , salvo el envío y la grabación de datos que se efectuaba a través de los formularios web, que se efectuaba en el marco de un certificado de autenticación del sitio web (con una conexión cifrada).

La Agencia ha acreditado disponer de un certificado CDS emitido en fecha 28/10/2021 (renovado el 03/10/2022), y ha manifestado que en fecha 17/11/2021 hizo efectiva la migración de sus páginas web en HTTPS.

Fundamentos de derecho

1. Son de aplicación a este procedimiento lo que prevén la LPAC , y el artículo 15 del Decreto 278/1993, según lo que prevé la DT 2a de la Ley 32/2010, de 1 de octubre, de Autoridad Catalana de Protección de Datos. De conformidad con los artículos 5 y 8 de la Ley 32/2010, la resolución del procedimiento sancionador corresponde a la directora de la Autoridad Catalana de Protección de Datos.

2. De acuerdo con el artículo 64.2.f) de la LPAC y de conformidad con lo que se indica en el acuerdo de iniciación de este procedimiento, procede dictar esta resolución sin una propuesta de resolución previa, dado que la Agencia no ha formulado alegaciones en el acuerdo de iniciación. Este acuerdo contenía un pronunciamiento preciso sobre la responsabilidad imputada.

3. En relación con la conducta descrita en el apartado de hechos probados, es necesario acudir en primer lugar al artículo 32.1 del RGPD, relativo a la seguridad del tratamiento, que determina lo siguiente:

> *"1. Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, contexto y 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 las 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."*

De acuerdo con el artículo 156.2 de la Ley 40/2015, de 1 de octubre, de régimen jurídico del sector público, " *el Esquema Nacional de Seguridad tiene por objeto establecer la política de seguridad en la utilización de medios electrónicos en el ámbito de la presente Ley, y está constituido por los principios básicos y requisitos mínimos que garanticen adecuadamente la seguridad de la información tratada"* .

El Real decreto 3/2010, de 8 de enero, por el que se regulaba inicialmente, y en todo caso en el momento de los hechos imputados, el Esquema Nacional de Seguridad (ENS) en el

Traducción automática

ámbito de la Administración electrónica (a partir de lo previsto en el artículo 42 de la Ley 11/2007, de 22 de junio, ya derogada), contenía en su Anexo II las medidas de seguridad a implementar para conseguir el cumplimiento de los principios básicos y requisitos mínimos establecidos en el ENS. Entre estas medidas de seguridad, el apartado 5 contenía las *medidas de protección (mp)* , y el subapartado 5.8.2, titulado " *Protección de servicios y aplicaciones web [mp.s.2]",* establecía la obligatoriedad de utilizar certificados de autenticación del sitio web en todos los casos, es decir, tanto si era necesario establecer un nivel bajo en las medidas de seguridad, como un nivel alto, como sigue (el subrayado es nuestro):

"Los subsistemas dedicados a la publicación de información deben ser protegidos contra las
amenazas que les son propias.
a) Cuando la información tenga algún tipo de control de acceso, debe garantizarse la imposibilidad de acceder a la información obviando la autenticación, en particular tomando medidas
en los siguientes aspectos:
1º Se evitará que el servidor ofrezca acceso a los documentos por vías alternativas al protocolo determinado.
2º Se deben prevenir ataques de manipulación de URL.
3º Se previenen ataques de manipulación de fragmentos de información que se almacena en el disco duro del visitante de una página web a través de su navegador, a petición del servidor de la página, conocido en terminología inglesa como « cookies ».
4º Se deben prevenir ataques de inyección de código.
b) Se deben prevenir intentos de escalado de privilegios.
c) Se deben prevenir ataques de «cros site scripting ».
d) Se deben prevenir ataques de manipulación de programas o dispositivos que realizan una acción en representación de otros, conocidos en terminología inglesa como « proxies », y
sistemas especiales de almacenamiento de alta velocidad, conocidos en terminología inglesa
como « caches ».

Nivel BAJO

Se utilizarán "certificados de autenticación del sitio web" de conformidad con la normativa europea (...).

Nivel ALTO

Se emplearán "certificados calificados de autenticación del sitio web" .

Durante la tramitación de este procedimiento ha quedado debidamente acreditado el hecho descrito en el apartado de hechos probados, a partir de la denuncia y de los correos adjuntos presentados por la persona denunciante, pero especialmente del reconocimiento en la fase precedente por parte de la Agencia Catalana de Consumo sobre la falta de implementación de un protocolo HTTPS en la web principal durante el tiempo señalado, lo que supone un incumplimiento de la obligación prevista en el apartado 5.8.2 del ENS entonces vigente .

Traducción automática

Esto habría hecho el dicho web más vulnerable a los ataques informáticos, tales como ataques de tipo *man -in- the - middle* ("ataque de intermediario"), en que el atacante actúa como intruso entre los partos que se están comunicante. Así, podría haberse dado el caso de que una persona introdujera datos en un formulario de la web de la Agencia, a efectos de presentar una reclamación, y que lo hubiera hecho en una web que pareciera idéntica a la que esta persona estuviera visitante, pero que en realidad se tratara de una web falsa, que no correspondiera a la web oficial de la Agència Catalana del Consum.

Cabe decir que el Real Decreto 311/2022, de 3 de mayo, por el que se regula el ENS actualmente vigente, igualmente prevé en su apartado 5.8.2 que los sistemas que prestan servicios web deben ser protegidos frente a las mismas amenazas contempladas en el apartado 5.8.2 del anterior ENS.

Este hecho imputado, y ahora probado, es constitutivo de infracción, según lo previsto en el artículo 83.4.a) del RGPD, que tipifica como tal la vulneración de: " a) las obligaciones del responsable y del *encargado en tenor de los artículos 8, 11, 25 a 39, 42 y 43; "*

La conducta que aquí se aborda se ha recogido como infracción grave en el artículo 73.f) de la Ley orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales (en adelante, (LOPDGDD), en la siguiente forma:

> *f) La falta de adopción de las medidas técnicas y organizativas que sean apropiadas para garantizar un nivel de seguridad adecuado al riesgo del tratamiento, en los términos que exige el artículo 32.1 del Reglamento (UE) 2016/679 .*

4. El artículo 77.2 LOPDGDD dispone que, en el caso de infracciones cometidas por los responsables o encargados enumerados en el art. 77.1 LOPDGDD, la autoridad de protección de datos competente:

> *"(...) debe dictar una resolución que las sancione con una amonestación. La resolución establecerá asimismo las medidas que proceda adoptar para que cese la conducta o se corrijan los efectos de la infracción que se haya cometido.*
> *La resolución se notificará al responsable o encargado del tratamiento, a cuyo órgano dependa jerárquicamente, en su caso, ya los afectados que tengan la condición de interesado, en su caso."*

En términos similares a la LOPDDDD, el artículo 21.2 de la Ley 32/2010 , determina que:

> *"2. En el caso de infracciones cometidas con relación a ficheros de titularidad pública, el director o directora de la Autoridad Catalana de Protección de Datos debe dictar una resolución que declare la infracción y establezca las medidas a adoptar para corregir sus efectos ."*

Dado que en la fase precedente la Agencia acreditó, en relación con su sitio web principal, disponer de un certificado CDS emitido en fecha 28/10/2021 (renovado el 03/10/2022), y manifestó que en fecha 17/11/2021 había hecho efectiva la migración de sus páginas web a HTTPS, se considera innecesario requerir la adopción de medidas correctoras.

Resolución automática

Por todo esto, resuelvo:

1. Amonestar a la Agencia Catalana del Consumo como responsable de una infracción prevista en el artículo 83.4.a) en relación con el artículo 32.1, ambos del RGPD.

No es necesario requerir medidas correctoras para corregir los efectos de la infracción, de conformidad con lo expuesto en el fundamento de derecho 4º.

2. Notificar esta resolución a la Agencia Catalana del Consumo .

3. Comunicar la resolución al Síndic de Greuges, de conformidad con lo que prevé el artículo 77.5 del LOPDDDD.

4. Ordenar que se publique esta resolución en la web de la Autoridad (apdcat.gencat.cat) , de conformidad con el artículo 17 de la Ley 32/2010, de 1 de octubre.

Contra esta resolución, que pone fin a la vía administrativa de acuerdo con los artículos 26.2 de la Ley 32/2010, de 1 de octubre, de la Autoridad Catalana de Protección de Datos, y 14.3 del Decreto 48/2003 , de 20 de febrero, por el que se aprueba el Estatuto de la Agencia Catalana de Protección de Datos, la entidad imputada puede interponer, con carácter potestativo, un recurso de reposición ante la directora de la Autoridad Catalana de Protección de Datos Datos, en el plazo de un mes a contar desde el día siguiente de su notificación, de acuerdo con lo que prevén el artículo 123 y siguientes de la LPAC. También puede interponer directamente un recurso contencioso administrativo ante los Juzgados de lo Contencioso-Administrativo, en el plazo de dos meses a contar desde el día siguiente de su notificación, de acuerdo con los artículos 8, 14 y 46 de la Ley 29/1998, de 13 de julio, reguladora de la jurisdicción contencioso-administrativa.

Si la entidad imputada manifiesta a la Autoridad su intención de interponer recurso contencioso administrativo contra la resolución firme en vía administrativa, la resolución se suspenderá cautelarmente en los términos previstos en el artículo 90.3 de la LPAC.

Igualmente, la entidad imputada podrá interponer cualquier otro recurso que estime conveniente para defender sus intereses.

La directora,

Traducción automática