Expediente N.º: EXP202312404

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: Con fecha 16 de julio de 2023, se presentó reclamación con número de registro de entrada REGAGE23e00048055912 ante la Agencia Española de Protección de Datos contra **PIZZERÍAS CAMBALACHE, S.L.** con NIF B15203979 (en adelante, CAMBALACHE). Los motivos en que basa la reclamación son los siguientes:

La reclamante denuncia que, después de realizar un pedido el 12/05/2023 en ******EMAIL.1*** *resultando la única forma de pago disponible, la "transferencia bancaria", la cual aparece un número de cuenta y una persona titular que parecen ajenas a la empresa,* y realizar el pago mediante transferencia bancaria, se equivocó en el importe, transfiriendo una cantidad sensiblemente superior a la que ascendía su pedido. Al ir a reclamar, señala que la empresa *" se desvincula de cualquier reclamación o asunción de responsabilidad por la brecha de seguridad en su propia página web e incluso se desvincula de cualquier brecha o falla de seguridad, que resulta evidente pues la empresa tiene en su web oficial un n.º de cuenta y un titular completamente ajeno a su actividad comercial".*

Aporta dos capturas de pantalla que reflejan el correo de confirmación del pedido en el que se indicaba que el medio de pago era una transferencia bancaria.

SEGUNDO: De conformidad con el artículo 65.4 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante LOPDGDD), se dio traslado de dicha reclamación a CAMBALACHE, para que procediese a su análisis e informase a esta Agencia en el plazo de un mes, de las acciones llevadas a cabo para adecuarse a los requisitos previstos en la normativa de protección de datos.

El traslado, que se practicó conforme a las normas establecidas en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en adelante, LPACAP), fue recogido en fecha 19/09/2023 como consta en el acuse de recibo que obra en el expediente.

TERCERO: el 16/10/2023, de conformidad con el artículo 65 de la LOPDGDD, se admitió a trámite la reclamación presentada.

CUARTO: CAMBALACHE contesta a la solicitud de información de la AEPD el 20/10/2023 indicando que el 12/05/2023 se detectó la transferencia bancaria para uno de los pedidos como forma de pago pendiente", alertando al encargado de la gestión de la página web, quien confirma que se ha producido un ataque externo desactivando las formas de pago habituales, para ser suplantadas por "transferencia bancaria" a la cuenta de Bélgica: ***IBAN: BE00 0000 0000 0000 BIC/SWIFT: XXXXXXXXXXX*** cuyo titular es ***A.A.A***.

Revisando los datos del servidor y los "logs" de la web configuración del módulo de SumUp se confirma que el hacker accede al panel de administración de la página web el 12/05/2023 entre las 16:12 y las 16:50, agregando los datos de transferencia bancaria a las 16:50. No consta en los "logs" que se haya producido un acceso a la base de datos de los clientes, ni que se haya producido una exfiltración de datos. Tras el análisis realizado por el proveedor no se hallaron evidencias de la causa del incidente y se resetearon las credenciales y se revisaron los privilegios de acceso, solventando así la incidencia.

Declara CAMBALACHE que el incidente sólo afectó a dos personas y como resultado hacker obtuvo los datos identificativos de cada ordenante, así como su número de cuenta bancaria y las cantidades de dinero transferidas desde sus cuentas.

Para solucionar el incidente, se revisaron las credenciales de acceso a la administración de la página web, se han revisado permisos y se han monitorizado los procesos de pago en los siguientes días, con el objetivo de comprobar el perfecto funcionamiento del proceso de compra. y para minimizar su impacto sobre las personas afectadas, obtuvieron la explicación debida y se les restauró el importe pagado ilícitamente. Finalmente, denunció también CAMBALACHE los hechos ante la Policía Nacional.

Sobre las medidas de seguridad previas al incidente, aporta CAMBALACHE a la AEPD el registro de actividades de tratamiento completo del módulo de *"Gestión de clientes"* que comprende los activos digitales, tanto para la página web como para la app para dispositivos móviles. La seguridad está externalizada con la empresa tecnológica Hacce Soluciones TIC, S.L., de reconocida solvencia en el sector.

CAMBALACHE no realiza evaluación de impacto (EIPD o PIA), porque el tipo tratamiento no lo requiere, al tratarse de e-commerce para la adquisición de comida para recogida o entrega en domicilio, sin tratamiento de datos sensibles, ni uso de tecnologías disruptivas, por lo que no entraría dentro de las previsiones del artículo 35 del RGPD, ni de la lista publicada por la AEPD al respecto.

En cuanto a las medidas futuras, aporta CAMBALACHE el informe de su encargado de tratamiento de datos, Hacce Soluciones TIC, S.L., que propone en resumen una mayor proactividad en la implantación de las últimas medidas del fabricante y desarrollador de la tecnología web, además de las soluciones más recientes en el ámbito hardware, especialmente las relativas a la seguridad y la ciberseguridad. También planea escanear con mayor frecuencia los procesos de compra de productos para comprobar su seguridad.

CAMBALACHE, apoyándose para ello en la herramienta “Asesora Brecha”, de la web corporativa de la AEPD, considera que no es preciso notificar la brecha de seguridad a la AEPD antes del transcurso de 72 horas, al no suponer un riesgo para los derechos y libertades de las personas físicas.

FUNDAMENTOS DE DERECHO

I
Competencia

De acuerdo con las funciones que el artículo 57.1 a), f) y h) del Reglamento (UE) 2016/679 (Reglamento general de protección de datos, en adelante RGPD) confiere a cada autoridad de control y según lo dispuesto en los artículos 47 y 48.1 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.

Asimismo, el artículo 63.2 de la LOPDGDD determina que: *"Los procedimientos tramitados por la Agencia Española de Protección de Datos se regirán por lo dispuesto en el Reglamento (UE) 2016/679, en la presente ley orgánica, por las disposiciones reglamentarias dictadas en su desarrollo y, en cuanto no las contradigan, con carácter subsidiario, por las normas generales sobre los procedimientos administrativos."*

II

Cuestiones previas

Definiciones del artículo 4 del RGPD

“1) «datos personales»: toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona;

2) «tratamiento»: cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción;

7) «responsable del tratamiento» o «responsable»: la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros

determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros;

8) «encargado del tratamiento» o «encargado»: la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento;

12) «violación de la seguridad de los datos personales»: toda violación de la seguridad que ocasione 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;"

De conformidad con los apartados 1 y 2 del artículo 4 del RGPD, CAMBALACHE a través de su página web corporativa, ******EMAIL.1***, realiza tratamiento de datos de carácter personal de sus clientes, mayormente nombre, apellidos, datos de cargo, y, en su caso, dirección de entrega de la comida encargada.

De conformidad con la definición del apartado 7 del artículo 4 del RGPD CAMBALACHE es el responsable del tratamiento al ser la persona jurídica que determina los fines y medios del tratamiento indicado. En este caso, al estar externalizados tanto la gestión de la página web como la seguridad, nos encontramos con dos encargados externos por cuenta del responsable de conformidad con la definición del apartado 8 del artículo 4 del RGPD, a saber una persona física, D. ***B.B.B.,*** encargada de los sistemas informáticos en general y una persona jurídica específicamente contratada para la seguridad informática, Hacce Soluciones TIC, S.L..

Finalmente, de conformidad con la definición el apartado 12 del artículo 4 del RGPD se habría producido una violación de la seguridad de los datos personales en la página web de CAMBALACHE el 12/05/2023 entre las 16:10 y las 16:50 al suplantar un hacker los medios normales de pago de los encargos, y conseguir al acceder de manera ilícita a los datos personales de 2 clientes de CAMBALACHE, cuando utilizaron su página web corporativa para el pago de un pedido.

III

Principios relativos al tratamiento

Confidencialidad

La letra f) del artículo 5.1 del RGPD regula los principios integridad y confidencialidad:

"1. Los datos personales serán:
(…)
f) 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»)."

De conformidad con este precepto, CAMBALACHE, como responsable del tratamiento, tiene la obligación de garantizar la confidencialidad de los datos personales mediante una seguridad adecuada, incluida la protección contra el tratamiento no autorizado o ilícito.

En este caso, el hacker ha sustituido el apartado del pago de la web corporativa por otra cuenta de destino con la voluntad de estafar a los clientes de CAMBALACHE, creando la apariencia de que realizan una compra con el propio restaurante. La obtención de los datos mediante este método de phishing es una consecuencia adicional de esta acción.

Esto significa que la pérdida de la confidencialidad no se refiere a los datos personales objeto del tratamiento llevado a cabo por CAMBALACHE.

IV

Medidas de Seguridad

No obstante, como responsable del tratamiento, tiene que cumplir también lo estipulado en el artículo 32.1 del RGPD, estipula lo siguiente sobre la seguridad del tratamiento (se subraya lo aplicable al caso):

"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.

CAMBALACHE y sus encargados deben aplicar medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad contra el riesgo de phishing de los datos de los clientes que acceden a su web corporativa, garantizando la confidencialidad de que los datos recabados a través su web se recogen efectivamente por CAMBALACHE y no por terceros no autorizados. Las medidas se adoptarán en función del estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento.

V

Obligación de comunicar brechas de datos personales a la AEPD

Precisamente para garantizar la adopción de las medidas adecuadas establece el artículo 33 del RGPD con carácter general la obligación de comunicación las brechas

de datos personales a la AEPD, en su condición de autoridad de control estableciendo 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."

Como CAMBALACHE no comunicó a la AEPD la brecha de datos personales, y la AEPD tuvo conocimiento de la misma mediante la reclamación de una afectada, la AEPD solicitó información a CAMBALACHE sobre su actuación en los hechos objeto de la reclamación, siguiendo los requisitos del artículo 33 que se aplican al caso.

- Obligación de notificar la brecha a la AEPD (artículo 33.1): CAMBALACHE, apoyándose para ello la herramienta "Asesora Brecha", de la web corporativa de la AEPD, considera que no es preciso notificar la brecha de seguridad a la

AEPD antes del transcurso de 72 horas, al no suponer un riesgo para los derechos y libertades de las personas físicas.

- Descripción de naturaleza de la brecha (33.3 apartado a): el 12/05/2023 a las 20:50 desde un local de Pizzerías Cambalache se informa al encargado de informática por un pedido con "Pago por transferencia bancaria pendiente; quien informa a su vez a la empresa encargada de la seguridad a las 20:58". A las 21:07 confirma que se ha producido un ataque externo consistente en la suplantación las formas de pago habituales por "transferencia bancaria" a la cuenta de Bélgica: ***IBAN: BE00 0000 0000 0000 BIC/SWIFT: XXXXXXXXXXX*** cuyo titular es ***A.A.A.***. En ese mismo instante, se decide eliminar la parte de la configuración añadida por el atacante y dejar la página como antes del ataque, volviendo así el funcionamiento a la normalidad.

  El 12/05/2023 entre las 16:12 y las 16:50, se produjo un ataque externo a página web corporativa de CAMBALECHE, No consta en los "logs" que se haya producido un acceso a la base de datos de los clientes, ni que se haya producido una exfiltración de datos.

- Categorías y el número aproximado de interesados afectados de registros de datos personales afectados, y las categorías y el número aproximado (artículo 33.3 apartado a in fine): datos identificativos de dos (2) personas, su número de cuenta bancaria y las cantidades de dinero transferidas desde sus cuentas.

- Descripción de las posibles consecuencias de la brecha: perjuicio económico por las cantidades de dinero transferidas junto con el phishing de sus datos identificativos y su número de cuenta bancaria, con el posible mal uso futuro de esta información.

- Medidas adoptadas o propuestas por el responsable del tratamiento para poner remedio a la brecha, (artículo 33.3 c) inicio): CAMBALACHE solventó la incidencia reseteando las credenciales de acceso a la administración de la página web y se revisaron los permisos y privilegios de acceso, junto con la monitorización los procesos de pago en los siguientes días, con el objetivo de comprobar el correcto funcionamiento del proceso de compra.

- Medidas mitigadoras de los posibles efectos negativos para minimizar su impacto sobre las personas afectadas (artículo 33.3 c in fine): afirma que los afectados obtuvieron de CAMBALACHE la explicación debida y les reembolsó el importe transferido ilícitamente, aunque sólo aporta documentación de un correo electrónico a la parte reclamante informando de la incidencia con cuenta bancaria. Finalmente, denunció también CAMBALACHE los hechos ante la Policía Nacional.

- Obligación del responsable de documentar y poner a disposición de la AEPD los hechos relacionados la brecha, sus efectos y las medidas correctivas adoptadas (artículo 33.5): Aporta el informe del incidente del encargado de seguridad, así como la denuncia ante la Policía Nacional. Sobre las medidas de seguridad previas al incidente, aporta CAMBALACHE a la AEPD el registro de actividades de tratamiento completo del módulo de *"Gestión de clientes"* que

comprende los activos digitales, tanto para la página web como para la app para dispositivos móviles;

En cuanto a las medidas futuras, en el informe del encargado de seguridad CAMBALACHE, se propone en resumen una mayor proactividad en la implantación de las últimas medidas del fabricante y desarrollador de la tecnología web, además de las soluciones más recientes en el ámbito hardware, especialmente las relativas a la seguridad y la ciberseguridad. También planea escanear con mayor frecuencia los procesos de compra de productos para comprobar su seguridad.

VI
Conclusión

El ataque informático se dirige contra la web corporativa de CAMBALACHE, el atacante ha modificado su contenido y ha sustituido el apartado del pago de la web corporativa por una cuenta bancaria de destino que nada tiene ver con la empresa. El atacante se interpone entre CAMBALACHE y sus clientes con la voluntad de estafar a estos últimos y obtiene además sus datos identificativos y su número de cuenta mediante phishing.

A la vista de los hechos expuestos, procede concluir que no existen evidencias de infracción del RGPD.

Por lo tanto, en base a lo indicado en los párrafos anteriores, no se han encontrado evidencias que acrediten la existencia de infracción en el ámbito competencial de la Agencia Española de Protección de Datos.

Todo ello sin perjuicio de las posibles actuaciones posteriores que esta Agencia pudiera llevar a cabo, aplicando los poderes de investigación y correctivos que ostenta.

de acuerdo con lo señalado, por la Directora de la Agencia Española de Protección de Datos, SE ACUERDA:

PRIMERO: PROCEDER AL ARCHIVO de las presentes actuaciones.

SEGUNDO: NOTIFICAR la presente resolución a **PIZZERÍAS CAMBALACHE, S.L.** y a la parte reclamante.

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.

940-301023

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