**Procedimiento Nº: E/07210/2019**
940-0419

## RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos y teniendo como base los siguientes

## HECHOS

**PRIMERO:** Las actuaciones de inspección se inician por la recepción de un escrito de notificación de quiebra de seguridad remitido por NESTLÉ ESPAÑA SA (en adelante NESTLÉ) en el que informan a la Agencia Española de Protección de Datos que, con fecha 5 de julio de 2019, han tenido conocimiento de un incidente de seguridad por el cual se podía acceder a datos de terceros.

En la fecha mencionada un usuario que había recibido una *newsletter* animando a darse de alta en un club *on line* de NESTLÉ (Club embajadores) y poder participar en un acto promocional, informa que al clicar en el enlace facilitado en la *newsletter* se accede a datos personales de terceros registrados en una base de datos de NESTLÉ.

Adjunto a la notificación se ha aportado un escrito en el que se pone de manifiesto que puestos en contacto con el usuario éste les remite unos videos con los datos de terceros a los que ha tenido acceso desde un fichero cuyo responsable es NESTLÉ y la información accesible corresponde a datos personales de padres y de menores de tres años y datos de salud (embarazo, gestación, condición genética, estado de salud…) por lo que deciden realizar una comunicación a los interlocutores (Agencia de marketing OGILVY) solicitando de forma inmediata la inhabilitación del acceso a la Base de Datos de NESTLÉ.

Con fecha 16 de julio de 2019, NESTLÉ remite a esta Agencia una notificación adicional en la que se adjunta un informe emitido por OGLIVY en el que se informa que el 27 de junio se realizó una actualización en el portal web de NESTLÉ, para permitir un acceso más rápido a las páginas, por la cual a los usuarios que mantenían activa una función (*Remember Me*) se generaba un *token* temporal que agilizaba el acceso. El problema estuvo en que el *token* se almacenaba en la *caché* y al acceder un usuario si la *caché* no estaba vacía utilizaba este *token* para el acceso. OGLIVY considera que el impacto potencial es de unos 116 usuarios (la base de datos contiene 510.000 usuarios) y que tiene constancia de que hay 14 afectados. En el informe también se indica que se modificó la gestión del *token* y se resolvió la incidencia en 1 día.

**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 reclamación, teniendo conocimiento de los siguientes extremos:

## ANTECEDENTES

Fecha de notificación de quiebra: 8 de julio de 2019

## ENTIDADES INVESTIGADAS

***NESTLÉ ESPAÑA, S.A. con NIF A08005449 con domicilio en AVDA. DELS PAISOS CATALANS 25-51 - 08950 ESPLUGUES DE LLOBREGAT (BARCELONA)***

## RESULTADO DE LAS ACTUACIONES DE INVESTIGACIÓN

1 Con fecha 1 de agosto de 2019 se remite requerimiento de información a NESTLÉ y de la respuesta recibida en fecha 21 de agosto se desprende:

Respecto de la empresa

- NESTLÉ tiene suscritos contratos con las empresas OGILVY ONE WORLWIDE SA (en adelante OGILVY) y KONECTA BTO SL (en adelante KONECTA).
- El contrato con OGILVY, de fecha 12 de marzo de 2019, responde a la prestación de servicios para tratamiento y gestión de las distintas bases de datos de NESTLÉ con datos personales de consumidores y/o usuarios interesados en acciones promocionales.

  El contrato con KONECTA, de fecha 10 de junio de 2019, responde a la prestación de servicio para la atención a los suscriptores de NESTLÉ en diversos canales.

Respecto de la cronología de los hechos. Medidas realizadas para minimizar el impacto de la incidencia

- El día 29 de junio de 2019 se activó una funcionabilidad que provocó un comportamiento anómalo en las funcionalidades "*en caché*" y "*recuérdame*".

  La función "*recuérdame*" facilita el acceso rápido a la web a usuarios ya registrados asignándoles un código de identificación (*token*) que se almacena en el equipo del usuario de tal manera que permite el acceso a servicios de la web sin necesidad de utilizar credenciales.

  La función *"caché"* guarda en el sistema páginas visitadas recientemente.

  El error consistió en que se almacenó en *caché* no solo las páginas visitadas por un usuario sino también su *token.*

  El 5 de julio, NESTLÉ tuvo conocimiento de una posible anomalía a través de un usuario que lo comunicó en la sección de consulta de la web de NESTLÉ. La entidad contactó inmediatamente con el usuario, el cual remitió unos videos con las capturas de pantallas a las que había tenido acceso el sábado 6 de julio a las 22:25. NESTLÉ también contactó con la empresa OGILY encargada del tratamiento donde se había producido la incidencia.

  NESTLÉ ha aportado copia de las comunicaciones con los usuarios que detectaron la incidencia. En relación con estas comunicaciones NESTLÉ manifiesta que hubo una comunicación de un usuario el 27 de junio de 2019 a las 14:49 donde se hacía referencia al incidente de seguridad pero

pasó inadvertida en KONECTA, también hubo otra comunicación el 28 de junio a las 14:33 y KONECTA la remitió a OGILVY el cual consideró que había habido un cruce de datos erróneo por lo que procedió a contestar de forma genérica al usuario. Asimismo, hubo dos comunicaciones el 5 de julio y 8 de julio que se encontraban en la cola de gestión y fueron localizadas el 10 de julio una vez detectada la incidencia.

- El 8 de julio visualizaron los videos comprobando que se accedía a una base de datos cuyo responsable es NESTLÉ, por lo que se declaró el incidente como brecha de seguridad e inmediatamente se procedió a bloquear la web donde se había producido la incidencia, y desactivar el acceso a la base de datos (a las 14:09 del 8 de julio). También se procedió a notificar a la Agencia Española de Protección de Datos.
- El incidente fue solucionado por OGILVY a las 1:31 del 9 de julio de 2019. La solución consistió en utilizar una plataforma externa de almacenamiento de tal manera que el *token* no se asociara a las páginas almacenadas en *cache.*
- Asimismo se suspendieron todas las comunicaciones a usuarios de la base de datos afectada el 11 de julio de 2019 (brecha de confidencialidad).
- Durante los días 16 y 17 desde OGILVY se restauraron los datos de los usuarios que habían sido modificados utilizando las copias de respaldo (brecha de integridad).
- El servicio se reestableció para los usuarios el 17 de julio de 2019.
- NESTLÉ ha aportado copia de las comunicaciones mantenidas con OGILVY donde figuran las acciones inmediatas tomadas. Copia del correo remitido al *Cyber Security Operations Center* del Grupo NESTLÉ con el *reporting informations Securtiy Events* y el remitido a la *Data Protección Office de NESTLÉ* en Suiza.

Respecto de los datos afectados

- El acceso al perfil privado no es automático en la web afectada, por ello algunos usuarios al detectar que la identificación (saludo con nombre) no era la correcta lo reportaron a NESTLÉ.
- Los datos que figuran en el perfil privado son:
    - Datos identificativos: nombre y apellidos, fecha de nacimiento, dirección de mail, género, teléfono, dirección postal, situación de gestación (SI/NO), hijos menores de 3 años (SI/NO), fecha de nacimiento de los hijos, género, nombre.
    - Condición genética o estado de salud: embarazada (SI/NO)
- NESTLÉ considera que potencialmente podría haber 116 usuarios afectados aunque no identificados. No obstante, se modificaron los datos de 10 usuarios y tiene evidencias de que 5 personas accedieron a datos de otros usuarios ya que lo reportaron.

- NESTLÉ remitió un correo electrónico el 12 de julio de 2019 a las 5 personas que reportaron el incidente informando de los hechos y de su solución en pocas horas.
- No han remitido ninguna comunicación a los posibles afectados ya que el número ha sido calculado estadísticamente y se ignora si efectivamente ha habido más afectados y, en su caso, se desconoce su identidad.
- NESTLÉ manifiesta que no tienen constancia de la utilización posterior por terceros de los datos de los afectados y que no se ha podido producir indexación dado que el incidente se ha producido en el área privada previa identificación del usuario que no permite acceder los motores de búsqueda.

Respecto de las medidas de seguridad implantadas con anterioridad al incidente

- NESTLÉ ha aportado copia del Análisis de Riesgos y Evaluación de impacto sobre el tratamiento de datos origen del incidente ("*BD CONSUMIDOR INFANT NUTRITUION*").
- NESTLÉ ha aportado copia de la ficha del Registro de actividades correspondiente al tratamiento *BD CONSUMIDOR INFANT NUTRITUION* en el que se integran los datos recabados en la web afectada por la incidencia.
- NESTLÉ ha aportado copia del "Procedimiento de actuación ante Brechas de seguridad"
- La entidad OGILVY encargada del tratamiento y gestión de las distintas bases de datos de NESTLÉ, tiene relacionadas en el contrato de prestación de servicios las medidas de seguridad implantadas (Anexo I del contrato -Documento 2-). Entre las medidas figura:
    - OGILVY dispone de un sistema de gestión de la seguridad de la información certificado con el estándar ISO/IEC 27001.
    - Tienen implantado un sistema de identificación inequívoca y personalizada para cada usuario.
    - El acceso es por usuario y contraseña con un sistema que permite el acceso únicamente a los recursos necesarios para el servicio. La frecuencia de modificación es alta. Disponen de un procedimiento de asignación, distribución y almacenamiento (cifrado) que garantiza la confidencialidad e integridad.
    - Disponen de un mecanismo que impide el intento reiterado de accesos no autorizados.
    - Procedimiento de actuación ante brechas de seguridad.
- La entidad KONECTA dispone también de certificación ISO/IEC 27001.
- NESTLÉ manifiesta que las medidas de seguridad no se han visto afectadas ya que ha sido un error en la programación.

Respecto de las medias implementadas con posterioridad a la incidencia

NESTLÉ manifiesta que se van a implantar, entre otras, las siguientes medidas:

- Revisión de todos los procesos donde consten datos personales antes de cambiar las versiones de los Sistemas de Información.
- Excluir páginas con datos personales de la *caché.*
- Establecimiento de reglas automatizadas basadas en contenidos de mensajes y/o palabras para que se redirecciones al buzón del especialista correspondiente de la compañía.
- Chequeos periódicos de los canales de entrada.
- Establecer un canal exclusivo de comunicación para incidentes de seguridad.

## FUNDAMENTOS DE DERECHO

**I**

De acuerdo con los poderes de investigación y correctivos que el artículo 58 del Reglamento (UE) 2016/679 (Reglamento general de protección de datos, en adelante RGPD) otorga a cada autoridad de control, y según lo dispuesto en el artículo 47 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en lo sucesivo LOPDGDD), es competente para resolver estas actuaciones de investigación la Directora de la Agencia Española de Protección de Datos.

**II**

El RGPD define, de un modo amplio, las "violaciones de seguridad de los datos personales" (en adelante 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."

En el presente caso, consta que se produjo una quiebra de seguridad de datos personales en las circunstancias arriba indicadas, categorizada como brecha confidencialidad por el acceso, a través del sitio web de NESTLÉ, a datos de terceros ajenos, y como brecha de integridad al haber sido posible la modificación de los datos de los afectados restableciéndose la integridad a través de la restauración de una copia de seguridad previa.

No obstante, también consta que NESTLÉ disponía de medidas técnicas y organizativas para afrontar un incidente como el ahora analizado, lo que ha permitido tras una reclamación externa la identificación, análisis y clasificación de la brecha de seguridad de datos personales así como la diligente reacción ante la misma al objeto de notificar, comunicar y minimizar el impacto e implementar las medias razonables oportunas para evitar que se repita en el futuro a través de la puesta en marcha de un plan de actuación previamente definido por las figuras implicadas del responsable del tratamiento.

No hay constancia de la utilización posterior por terceros de los datos de los afectados y que se haya podido producir indexación dado que el incidente se ha producido en el área privada previa identificación del usuario que no permite acceder los motores de búsqueda.

También debe valorase la adopción de medidas técnicas y de gestión al objeto de comprobar y en su caso mejorar la calidad de las aplicaciones de gestión de datos personales.

El informe final tras el seguimiento y cierre sobre la brecha y su impacto es una valiosa fuente de información con la que debe alimentarse el análisis y la gestión de riesgos futuros. El uso de esta información servirá para prevenir la reiteración del impacto de una brecha.

**III**

Por lo tanto, se ha acreditado que la actuación del reclamado 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 a ***NESTLÉ ESPAÑA, S.A.*** con NIF ***A08005449*** y con domicilio en ***AVDA. DELS PAISOS CATALANS 25-51 - 08950 ESPLUGUES DE LLOBREGAT (BARCELONA)***

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