- **Procedimiento Nº: E/01996/2020**

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: La entidad NH HOTEL GROUP S.A. (en adelante NH) notifica a esta Agencia (AEPD) una violación de la seguridad de los datos personales (en adelante quiebra de seguridad) tras la recepción el 11/02/2020 de un email en el departamento de seguridad de la entidad con relación a un acceso no autorizado a información contenida en un buzón de correo titularidad de NH con el que se gestionan peticiones de información general de los servicios de uno de sus hoteles.

Indican que a raíz de ello iniciaron un proceso de investigación, verificando con fecha 18/02/2020 que se había producido una incidencia de seguridad consistente en accesos a varios buzones de correo electrónico con el objeto de acceder a la plataforma de EXPEDIA (entidad virtual establecida en Estados Unidos de América) donde se gestionan las reservas realizadas a través de esa OTA (Online Travel Agency).

En la notificación de brecha de seguridad se indica la existencia de unos 29.459 afectados y que las categorías de datos son:

- Datos básicos.
- DNI, NIE y/o Pasaporte.
- Datos económicos o financieros.
- Datos de contactos.

Los representantes de NH han manifestado en la notificación de brecha de seguridad que los afectados no serán informados ya que el acceso a los buzones de NH se ha realizado con el fin de acceder a la plataforma de un tercero y extraer información económica de una entidad, y por ello los datos de particulares no eran objeto de intento de acceso por parte del tercero no autorizado, no habiéndose tenido constancia de reclamación alguna de estos titulares de tratamientos no autorizados.

Con fecha de 03/03/2020 la directora de la AEPD acordó iniciar actuaciones de investigación para 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:

ANTECEDENTES

Fecha de notificación de la quiebra de seguridad: 21/02/2020.

ENTIDADES INVESTIGADAS

NH HOTEL GROUP S.A. con NIF A28027944 con domicilio en SANTA ENGRACIA 120, 7 PLANTA - 28003 MADRID (MADRID)

RESULTADO DE LAS ACTUACIONES DE INVESTIGACIÓN

1.- Adjuntos a la notificación de quiebra constan un informe ejecutivo y un informe de incidencia. En el informe ejecutivo se resume:

"El 18 de febrero de 2020, el departamento de seguridad de NH Hotel Group recibe una notificación de un posible compromiso de cuentas empresariales de los Hoteles de la cadena en la extranet de Expedia. Estos accesos se realizaron en algunas cuentas que los Hoteles de NH tienen en la plataforma de Expedia para la gestión de las reservas realizadas a través de esa OTA (Online Travel Agency).

Los datos facilitados por Expedia en este momento inicial, fueron:

- *Un listado que contenía, al menos, 22 cuentas genéricas de hoteles NH en la extranet de Expedia.*
- *Accesos a estas cuentas de Expedia desde direcciones IP inusuales (En este caso pertenecientes a Rumanía)*
- *Datos sobre la forma de acceso a estas cuentas, los cuales habían sido realizados mediante los reseteos de las contraseñas de acceso a la plataforma de Expedia. Estos reinicios de contraseña se notificaban a la cuenta de correo electrónico que Expedia tenía asociada a cada identificador de usuario, que en la mayoría de los casos corresponde una dirección de correo electrónico cuya nomenclatura se crea a partir del nombre comercial del hotel seguido de @nh-hotels.com.*
- *El acceso a las cuentas de la extranet de Expedia podría suponer un acceso a todos los datos de reservas de los hoteles de NH que se realizan en esta plataforma incluidos los detalles de las tarjetas de crédito de los clientes (que se encuentran tokenizadas por Expedia) y tarjetas de la propia agencia (tarjetas de crédito virtuales).*
- *Las cuentas afectadas fueron bloqueadas por parte de Expedia en su plataforma.*

Los análisis realizados por parte de NH, teniendo en cuenta la información aportada por Expedia, nos han permitido comprobar que el acceso a las cuentas de Expedia en nombre de NH se ha producido porque, a su vez, se había producido un compromiso de las cuentas de email genéricas de Hoteles NH. Estas cuentas de email genéricas son:

nhcollectionpresident@nh-hotels.com
nhcollectionportarossa@nh-hotels.com
nhvillasanmauro@nh-hotels.com
nhpueblafinsa@nh-hotels.com
nhnice@nh-hotels.com
nhberlinalexanderplatz@nh-hotels.com
nhberlinpotsdamerplatz@nh-hotels.com

nhfrankfurtmesse@nh-hotels.com
nhpraguecity@nh-hotels.com
nhlatino@nh-hotels.com
nhdanubecity@nh-hotels.com
nhbrusselslouise@nh-hotels.com
nhgrazcity@nh-hotels.com
nhtoulouseairport@nh-hotels.com
nhcuritibathefive@nh-hotels.com
nhvalledorado@nh-hotels.com
nhbarcelonastadium@nh-hotels.com
nhciudadreal@nh-hotels.com
nhcornella@nh-hotels.com
nhoberhausen@nh-hotels.com
nhkloesterlenoerdlingen@nh-hotels.com
nhmuenchenairport@nh-hotels.com

- *Las cuentas de correo tenían establecida una contraseña débil, que no cumplía con la política de seguridad de NH.*

- *A través del control no autorizado de estas cuentas, se ha obtenido acceso a la extranet de Expedia solicitando el reseteo de la contraseña que se recibía en la cuenta comprometida.*

- *Actualmente NH está trabajando en identificar si puede haber otras cuentas susceptibles de estar comprometidas, diferentes a las aportadas por Expedia.*

Las tareas de contención relacionadas con el incidente han sido:

- *Cambio de la contraseña de todas las cuentas de email de NH comprometidas, vía telefónica, y forzando el cumplimiento de unos requisitos de seguridad que incluyen:*

  - *Longitud de al menos 7 caracteres.*
  - *Mayúsculas.*
  - *Minúsculas.*
  - *Caracteres especiales.*
  - *Números.*
  - *Tener en cuenta histórico de contraseñas anteriores para evitar repeticiones.*

- *Los requisitos anteriores ya estaban implantados y eran obligatorios en el momento de establecer una nueva contraseña días antes de que ésta quedara caducada. Se detectó que en el caso de que una contraseña estuviese caducada y fuese reiniciada por el personal de soporte informático quedaba invalidada la opción de tener en cuenta el histórico, por lo que los usuarios podían volver a poner las contraseñas utilizadas con anterioridad. Esta medida ya se ha corregido y se ha hecho extensible a todas las cuentas de correo de la compañía para evitar que se pueda volver a reproducir.*

- *Se han deshabilitado los protocolos EWS, IMAP, POP, ActiveSync, Outlook Mobile y SMTP de las cuentas genéricas de todos hoteles, (tanto las comprometidas como no comprometidas).*

- *Se han cambiado las cuentas de correo asociadas a las cuentas de la Extranet de Expedia afectadas.*
- *Se está implementando una medida de control a las cuentas por acceso de geolocalización, que permitirán evitar accesos a las cuentas genéricas desde localizaciones distintas a donde esté el Hotel, es decir, sólo desde la IP del Hotel se podrá acceder al correo electrónico genérico del propio hotel."*

Entre las cuentas de correo comprometidas se encuentran algunas que parecen corresponder a hoteles NH ubicados en países de la Unión Europea. En la notificación de brecha de seguridad se observa que, en el apartado de implicaciones transfronterizas, se encuentran marcadas las casillas correspondientes a los siguientes Estados miembros de la UE, en los que pudiera haber sujetos afectados por la brecha: Alemania, Republica Checa, Austria, Francia, Italia, Luxemburgo, Polonia y Bélgica.

Por ello se crea y activa un caso de Consulta Informal por art. 60 del RGPD en el IMI (Sistema de Información del Mercado Interior) que se envía a las Autoridades de control de los Estados miembros mencionados.

2.- Respecto de la empresa.

NH ha publicado en su página web que durante el año 2019 tuvo: 1.718,3 millones de euros de ingresos, un beneficio de gestión (GOP) de 649,5 millones de euros y un beneficio neto de 90,0 millones de euros (Según Cuenta de Pérdidas y Ganancias-Actividad Recurrente hasta EBITDA).

3.- Respecto de la cronología de los hechos

- 11 de febrero de 2020: NH recibe una notificación sobre la posible brecha de seguridad.

- 18 de febrero de 2020: NH comprueba que la incidencia comunicada mediante correo del día 11/02/2020 consiste en una incidencia de seguridad con posible impacto en los datos de la compañía.

- 21 de febrero de 2020: se recibe notificación de brecha de seguridad en la AEPD

4.- Respecto de las causas que hicieron posible la brecha

Como han informado los representantes de NH en el informe ejecutivo adjunto a la notificación de brecha, las cuentas de correo de NH tenían establecida una contraseña débil, que no cumplía con la política de seguridad de NH. Una vez ganado el control no autorizado de estas cuentas de correo, se obtuvo acceso a la extranet de Expedia, solicitando el restablecimiento de la contraseña de acceso a la plataforma de EXPEDIA, y recibiéndose la nueva contraseña en la cuenta de correo de NH comprometida.

5.- Respecto de los datos afectados.

Se ha solicitado información y documentación a NH sobre los datos de tarjetas de crédito de los clientes de la entidad que pudieron ser accedidos como consecuencia de la brecha, en concreto información sobre los datos de las tarjetas bancarias de los Clientes de NH que han sido accedidos. De la respuesta recibida se desprende lo siguiente:

"En relación con esta solicitud de información, NH manifiesta que, la brecha de seguridad se centra en accesos por parte de terceros a cuentas de correo electrónico corporativas, que son usadas por los hoteles de la cadena, a fin de gestionar las reservas de los clientes finales de NH, no hay gestión de pagos en las cuentas de correo comprometidas.

De acuerdo con lo manifestado en el párrafo anterior, en estas cuentas de correo comprometidas, no hay datos económicos de los clientes finales. Los accesos a los datos económicos de los clientes finales, de haberse producido, no han podido hacerse a través de las cuentas de email comprometidas.

Por este motivo, no podemos facilitarle a esta Agencia ningún dato de los mencionados, porque no se contienen en las direcciones de email comprometidas.

No obstante lo anterior, en estas cuentas de correo comprometidas en contadas ocasiones algunas Agencias de Viajes online o bien Agencias de Viaje físicas envían datos de sus tarjetas de crédito o débito corporativas, para realizar pagos de reservas realizadas a nombre de estas entidades jurídicas. De haberse producido algún acceso a datos económicos por parte de terceros no autorizados, se habrían realizado en relación con estas tarjetas.

NH es una entidad sujeta al cumplimiento de la normativa de PCI Compliance, encontrándose actualmente certificada en esta norma, como puede ser verificado por medio del certificado actual de cumplimiento de esta norma que se adjunta como Documento 1.

Adicionalmente, y dado el compromiso de cumplimiento normativo adquirido por parte de NH, se envían a los trabajadores del grupo recordatorios sobre la obligatoriedad de que los datos económicos de los clientes y en especial los datos de las tarjetas de los mismos se encuentren en el entorno seguro diseñado por NH, esto es, en la burbuja de PCI Compliance. Se adjuntan como Documento 2 los emails recordatorios de la obligatoriedad de uso de la burbuja de PCI Compliance y sobre la obligatoriedad de realizar un curso general cuyo contenido son las normas de PCI Compliance aplicables a los datos económicos de los clientes.

De acuerdo con lo anterior, NH dispone de un entorno seguro y que cumple con los estándares PCI para el tratamiento tokenizado de las tarjetas de crédito y débito, tanto de los clientes personas físicas como de los clientes personas jurídicas, pero al margen de los procedimientos implementados, algunas entidades comunican los datos de sus tarjetas corporativas a través del email.

Por lo tanto, los datos de las tarjetas expuestas contienen el nombre y los datos de estas Agencias de Viajes, bien físicas u online, pero no contienen los datos

económicos de las personas físicas a cuyo nombre se abonaba la reserva pagada.“

Aportan como documento 1 copia de un documento titulado “Attestation of Compliance for Onsite Assessments – Service Providers” emitido por PCI (Payment Card Industry) Security Standars Council a nombre de NH. Aportan también como documento 2 copia de los correos electrónicos referidos. Ambos documentos obran en las actuaciones de inspección.

6. Respecto de las medidas de seguridad implantadas con anterioridad la brecha

NH informa que los tratamientos de datos en los que están involucrados los datos relativos a tarjetas de crédito o débito, tras el análisis de riesgos realizado, no ha supuesto la necesidad de realizar Evaluaciones de Impacto sobre la Privacidad, como así puede ser verificado en el Análisis de Riesgos (AR).

Aportan copia del AR realizado por NH, así como un documento titulado “Procedimiento de Evaluación de Riesgo Inherente y del Impacto en la Privacidad de las Actividades de Tratamiento”.

En relación con las medidas de seguridad implementadas con anterioridad a la brecha, reiteran que, como manifestaban en la comunicación inicial de la brecha, con relación a las cuentas de correo electrónico se tenía implementada la siguiente política de contraseñas:

- Longitud de al menos 7 caracteres.
- Mayúsculas.
- Minúsculas.
- Caracteres especiales.
- Números.

7. Respecto de las medias implementadas con posterioridad la brecha

Según informan los representantes de NH:

Se detectó que en el caso de que una contraseña estuviese caducada y fuese reiniciada por el personal de soporte informático los empleados podían solicitar una de las contraseñas que o bien estaban en el histórico o bien fuera parecida a las anteriores pero con una pequeña modificación de los patrones de la contraseña, es decir, que los usuarios podían volver a poner las contraseñas utilizadas con anterioridad. Teniendo en cuenta el incidente de seguridad, el departamento técnico de NH corrigió de inmediato esta posibilidad para evitar que se puedan repetir contraseñas previas.

La posibilidad de que las contraseñas se repitieran fue el motivo por el que los patrones de las mismas se repetían y no cumplían con los requisitos establecidos por NH. Por este motivo NH modificó de inmediato esta posibilidad dando instrucciones al departamento de soporte de que, en ningún caso los usuarios podían volver a establecer contraseñas que no cumplieran con la política establecida con la entidad.

Como se indica en el resumen ejecutivo aportado por NH:

- *Se han deshabilitado los protocolos EWS, IMAP, POP, ActiveSync, Outlook Mobile y SMTP de las cuentas genéricas de todos hoteles, (tanto las comprometidas como no comprometidas).*

- *Se han cambiado las cuentas de correo asociadas a las cuentas de la Extranet de Expedia afectadas.*

- *Se está implementando una medida de control a las cuentas por acceso de geolocalización, que permitirán evitar accesos a las cuentas genéricas desde localizaciones distintas a donde esté el Hotel, es decir, sólo desde la IP del Hotel se podrá acceder al correo electrónico genérico del propio hotel.*

A fecha abril de 2020 NH realiza inspecciones en las 362 cuentas genéricas de correo electrónico de sus hoteles. Esta entidad informa que se ha puesto de manifiesto que no se ha producido ninguna otra intromisión en el resto de las cuentas de correo electrónico de los Hoteles. Es decir, informan que las cuentas comprometidas fueron las 22 inicialmente comunicadas por NH, no habiendo existido más intromisiones no autorizadas.

Adicionalmente, el 18 de febrero de 2020 se comunicó el cambio de todas las contraseñas de las cuentas de correo electrónico de los hoteles a los directores de todos los centros NH.

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

En el presente caso, hay que partir de dos actuaciones de NH diferenciadas.

La primera, referida al propio incumplimiento interno de la seguridad en las claves de acceso a las cuentas de correo corporativas, que es precisamente el origen de la incidencia ahora analizada. Al respecto, se significa que NH ya ha implantado las medidas adecuadas para corregir el protocolo de reseteo o caducidad de las claves de acceso añadiendo el requisito de tener en cuenta histórico de contraseñas anteriores para evitar repeticiones. También NH ha suprimido determinados protocolos de comunicaciones para todas las cuentas de correo de NH, actualizado las claves de acceso e implantación de listas “blancas” de direcciones IP para el acceso a los buzones de correo electrónico.

La segunda, referida a la posibilidad de que la incidencia haya permitido el acceso por terceros ajenos a datos personales de los clientes de NH. En este sentido, del análisis de la documentación aportada tal acceso no consta acreditado. Tampoco constan

reclamaciones de clientes y los datos de los medios de pago estaban encriptados. No obstante, y de forma casual, es cierta la posibilidad del acceso a datos de medios de pago de OTA´s -entidades jurídicas- quedando, por lo tanto, al margen del ámbito de aplicación del RGPD.

En cuanto a las cuentas de correo comprometidas que parecen corresponder a hoteles NH ubicados en países de la Unión Europea, esta AEPD activó un caso de Consulta Informal por art. 60 del RGPD en el IMI (Sistema de Información del Mercado Interior) que se envía a las Autoridades de control de los Estados miembros mencionados. Sólo respondió la CNIL (Autoridad francesa de protección de datos) en el sentido de que se le informe sucintamente del resultado de la actuación dictada por esta Agencia.

En consecuencia, corregidos los defectos en la seguridad del sistema de información de NH indicados en los antecedentes, habiendo dispuesto NH una conducta proactiva para la minimización de los efectos e implantado medidas adicionales para evitar la repetición de hechos similares se acuerda el archivo de actuaciones.

Por último señalar, que la documentación generada de todo el proceso de detección, contención, respuesta, recolección y custodia de evidencias ante una posible brecha de seguridad de los datos personales es importante de cara a comunicaciones a las posibles partes interesadas tanto de carácter interno o externo, y para la elaboración de un informe final que tras su análisis permita extraer conclusiones. Este informe final, elaborado tras el seguimiento y cierre de este tipo de incidentes 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 de hechos similares.

III

En el presente caso, consta que NH actuó con la diligencia debida para minimizar el impacto a los posibles afectados e implantó nuevas medidas de seguridad proporcionales al riesgo evaluado para evitar la repetición de incidentes similares en el futuro.

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 NH HOTEL GROUP S.A., con NIF A28027944 y con domicilio en SANTA ENGRACIA 120, 7 PLANTA - 28003 MADRID (MADRID).

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