- **Procedimiento N.º: E/03003/2020**

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 GUREAK LANEAN SA informa a la Agencia Española de Protección de datos que, con fecha ******FECHA.1***, detectaron un acceso bloqueado, tras diez intentos fallidos de inicio de sesión, desde un servidor interno de la red al servidor NAS (dispositivo de almacenamiento conectado en la red). En la revisión del incidente se comprobó que el intento de acceso fue realizado con un perfil de *Administrador* de uno de los dos dominios de la empresa y el acceso no fue ejecutado por personas de la entidad por lo que consideran que ha habido una brecha de seguridad que ha comprometido las contraseñas. En la notificación indican que puede haber unas 500 personas afectadas (clientes y proveedores) y puede haber datos económicos y de salud.

Con fecha 12 de febrero de 2020 se recibe notificación adicional remitida por GUREAK LANEAN SA en la que ponen de manifiesto que el día 9 de febrero a las 17:30 horas han detectado la creación de un usuario con perfil de *Administrador* asimismo manifiestan que se han realizado accesos utilizando también el perfil de *Administrador* del otro dominio también de la entidad y búsquedas en el directorio activo (servicio de Microsoft que almacena información acerca de los objetos de la red, entre ellos información sobre cuentas de usuarios) con accesos a datos de nombre y apellidos, cargo departamento de algunos usuarios. En esta notificación indican que puede haber 23044 registros de datos afectados.

Con fecha 12 de febrero de 2020 se reciben 11 notificaciones de brecha de seguridad en las que se pone de manifiesto que GUREAK LANEAN SA, en su calidad de encargado del tratamiento, les ha notificado el acceso no autorizado a sus servidores. Las siguientes entidades han notificado la brecha como responsables:

GUREAK GARBITASUNA SLU. Número de registros de datos afectados 674.

GUREAK BERDEA SLU. Número de registros de datos afectados 156.

GUREAK ZERBITZUGUNEAK SLU. Número de registros de datos afectados 97.

GUREAK OSTALARITZA SLU. Número de registros de datos afectados 137.

GUREAK ZERBITZU ANITZAK SLU. Número de registros afectados 203.

GUREAK ARAN SLU. Número de registros de datos afectados 56.

GERONTOLOGICO DE RENTERIA SLU. Número de registro afectados 131.

GUREAK ARABA SLU. Número de registros de datos afectados 351.

GUREAK NAVARRA SLU. Número de registros de datos afectados 181.

GUREAK IKUTTEGIA SL. Número de registros de datos afectados 123.

FUNDACION GOYENECHE DE SAN SEBASTIAN. Número de afectados 336.

GUREAK MARKETING SLU

Con fechas 12 de febrero y 3 abril de 2020 se reciben dos notificaciones de la empresa GUREAK MARKETING SLU en la que se pone de manifiesto que tuvieron conocimiento de la brecha anteriormente descrita a través del sistema informático de verificación de la compañía. En esta última notificación se aportan dos actas de la reunión extraordinaria del comité de privacidad de GUREAK MARKETING SLU de fechas 12 y 27 de febrero de 2020 sobre la brecha de seguridad

En el Acta del 12 de febrero consta que GUREAK LANEAN es una entidad del Grupo empresarial y actúa como encargado del tratamiento de GUREAK MARKETING en lo que respecta a infraestructura y tratamiento de datos y han constatado que el incidente de seguridad ha afectado a la infraestructura de esta entidad de forma similar que a la infraestructura de GUREAK MARKETING. Asimismo, informan de la existencia de la empresa INTEGRATED TECHNPLOGY SISTEM SL (en adelante ITS) como proveedor de servicios de ciberseguridad que junto con GUREAK LANEN van a elaborar un informe técnico sobre la brecha de seguridad. El número de potenciales afectados de GUREAK MARKETING asciende a 371 empleados con datos básicos, identificativos, económicos/financieros, contacto, localización y datos de salud.

En el Acta del 27 de febrero consta que se anexa el Informe elaborado por ITS con las siguientes conclusiones:

- La intrusión ha sido a través de un servidor con una configuración errónea en el Firewall (sistema informático cuya función es prevenir y proteger la red privada, de intrusiones o ataques de otras redes, bloqueándole el acceso).
- Los primeros intentos fallidos son del 30 de enero de 2020.
- Direcciones IP ubicadas en ******PAÍS.1***.
- Únicamente se ha constatado el intento de acceso a dos servidores de GUREAK MARKETING habiendo sido denegados.
- No se ha constatado que haya habido accesos efectivos o extracción de datos de GUREAK MARKETING.

En esta misma Acta también consta que se anexa un informe elaborado por GUREAK MARKETING en el que se pone de manifiesto que después de realizar las comprobaciones internas no se han producido acceso y/o extracción de datos de GUREAK MARKETING.

Con fecha 3 de julio remiten información adicional a la brecha en la que se incluye una Acta de seguimiento de fecha 26 de junio y un Informe de ITS y de GUREAK LANEAN en los que descartan el acceso y/o filtración de datos personales

Con fecha 16 y 17 de julio, todas las entidades que han notificado la brecha referenciada anteriormente han remitido una notificación completa sobre la brecha informando a la Agencia que se ha podido constatar que no ha habido acceso a datos de carácter personal.

SEGUNDO: En fecha 23 de marzo de 2020, la Directora de la Agencia Española de Protección de Datos 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, teniendo conocimiento de los siguientes extremos:

Fecha de notificación de la brecha de seguridad de datos personales: 11 de febrero de 2020.

ENTIDAD INVESTIGADA

GUREAK LANEAN SA con NIF A20044590 y domicilio en ******DIRECCIÓN.1*** (Guipúzkoa)

RESULTADO DE LAS ACTUACIONES DE INVESTIGACIÓN

Tal y como consta en la web ******URL.1***, *GUREAK es un grupo empresarial vasco que genera y gestiona oportunidades laborales estables y convenientemente adaptadas a las personas con discapacidad, prioritariamente con discapacidad intelectual en Gipuzkoa.*

1.- Con fecha 21 de mayo de 2020 se ha remitido escrito de requerimiento de información a GUREAK LANEAN SA, la cual en su escrito de contestación hace referencia al resto de las empresas del Grupo. De respuesta recibida se desprende lo siguiente:

Respecto de la empresa.

- GUREAK LANEAN es propietaria y/o administrador único de algunas de las sociedades referenciadas. Las sociedades comparten instalaciones, servicios centrales administrativos, infraestructuras, proveedores de servicios y otros, aunque son personas jurídicas independientes.
- GUREAK LANEAN tiene suscrito un contrato de prestación de servicio con cada una de las empresas en el cual GUREAK LANEAN actúa como encargado de tratamiento y el resto de las empresas que actúan como responsables de tratamiento. Han aportado contrato con GUREAK GARBITASUNA SLU de fecha 3 de enero de 2019 y manifiestan que el modelo de contrato es único (anexo 1).

  Los tratamientos que figuran corresponden, entre otros, a:

  - Mantenimiento de Sistemas Informáticos
  - Desarrollo y mantenimiento de aplicaciones

- Los sistemas de información se encuentran centralizados en las oficinas centrales del Grupo. Los centros de trabajo se encuentran interconectadas con la central con el objetivo de utilizar los servicios disponibles y centralizar la información manejada desde los centros.

  La conexión se hace a través de una línea de fibra dedicada. Esta red privada de interconexión cuenta con Firewall para securizar el acceso a Internet de todas las delegaciones.

La sede central cuenta a su vez con un Firewall con objeto de controlar los accesos de las delegaciones permitiendo sólo el acceso a los servicios necesarios, comunicaciones necesarios y securizar el acceso a internet de la Central.

Los servidores están alojados en dos CPDs

Se ha aportado como Anexo 2 información sobre la infraestructura, redes y software clasificado como CONFIDENCIAL.

- GUREAK LANEAN tiene suscrito un contrato de prestación de servicios con INTEGRATED TECHNOLOGY SYSTEMS (ITS) de fecha 25 de febrero de 2019, por el cual esta última compañía realizará el mantenimiento informático. (anexo 9)

Respecto de la cronología de los hechos y medidas tomadas para minimizar el impacto de la brecha

La entidad ha aportado Informe elaborado al efecto (anexo 3 CONFIDENCIAL) en el que figura:

- El sábado ******FECHA.1***, un equipo informático manda una alerta vía email a la dirección de soporte indicando que se han intentado varios accesos desde un servidor. El acceso ha sido bloqueado al introducir varias veces consecutivas mal la contraseña.
- El domingo 9 de febrero, un técnico de sistemas revisa la alerta con objeto de verificar el motivo por el que se está accediendo a dicho un equipo, ya que no es un acceso habitual. Al verificar que el Responsable de Seguridad de la compañía que no intentaba acceder se apaga el equipo como primera medida de prevención. También se comprueba si otros equipos han sufrido acceso en horas similares detectando intentos de acceso fallidos con un usuario administrador.

  Inmediatamente se cambia la contraseña del usuario administrador y del Responsable de Seguridad y se bloquean el resto de las cuentas de administrador en todos los sistemas.

  Se comprueba que no ha habido encriptación, pero se detecta un proceso extraño en ejecución en algunos servidores por lo que detienen inmediatamente su ejecución.

  Se detecta que uno de los servidores tiene una conexión activa fraudulenta por lo que se procede al apagado del mismo y se cierra la conexión a Internet en el Firewall como medida de precaución.

  Como medida adicional se manda un correo para que toda la organización modifique las contraseña ante la posibilidad de que hayan podido verse comprometidas.
- El lunes 10 de febrero se contacta con la empresa de seguridad ITS que lleva la gestión de los firewalls y se detecta una mala configuración en el Firewall que permitía un acceso desde el exterior. El servidor que daba acceso se encuentra apagado desde el día anterior. Se concluye que la intrusión está cerrada y no hay ninguna conexión no autorizada.

Durante toda la semana se continúa realizando un análisis forense de la intrusión y se recuperan las máquinas comprometidas.

Se vuelven a modificar las contraseñas de administrador dos veces consecutivas como medida de precaución adicional.

No se detectan accesos anómalos ni generación de usuarios fraudulentos.

- El martes 11 de febrero se obliga de nuevo a los usuarios al cambio de contraseña.
- El miércoles 12 de febrero proceden a notificar a la AEPD la brecha de seguridad debido al tipo de información que se encuentra en los servidores afectados, aunque no consta que se hayan visto comprometidos datos personales, por este motivo deciden no comunicar la brecha a los posibles afectados.

  Se decide denunciar los hechos ante la Ertzaintza (anexo 19).
- El lunes 17 de febrero se da por cerrada la intrusión y no se constata fuga de información.
- El miércoles 19 de febrero se procede a la migración del Firewall a otro.
- El jueves 9 de abril se recibe el segundo informe técnico de ITS donde se constata que después del análisis realizado no se ha producido fugas de información.
- El 28 de abril se procede a la revisión automatizada (vacuna) de todos los servidores ya revisados manualmente. No se detecta ninguna actividad inusual.

Respecto de las causas que hicieron posible la brecha

- El proveedor ITS realiza la sustitución del Firewall por un nuevo firewall.
- Este Firewall permitía el intento de conexión vía escritorio remoto con una contraseña *administrador* que se detectó que era débil y que en el hackeo se debió usar una técnica de crakeo de contraseñas y posteriormente poder conectarse al resto de los equipos.

Respecto de los datos afectados.

- Los informes forenses encargados a una empresa externa y los elaborados por los propios técnicos informáticos de GUREAK LANEAN establecen que no existen pruebas de que se hayan visto afectados ningún tipo de datos personales. Por ello consideran que no ha habido consecuencias para los posibles afectados ya que no se han extraídos datos al exterior. (Anexo 6 en el acta de fecha 12 de febrero de 2020, anexo 7 en el acta del Comité de seguridad de fecha 18 de febrero y anexo 8 en el Acta del 28 de febrero)
- GUREAK LANEAN manifiesta que la detección de la intrusión se realizó de forma temprana y el volumen de información intercambiado hacía el exterior ha sido bajo en relación con el volumen de datos existente. También en los logs de los sistemas que tienen datos de carácter personal no se han detectado accesos no habituales.
- No se ha encontrado en Internet ninguna divulgación de datos de ni tienen conocimiento de que un tercero haya accedido a datos del Grupo.

Respecto de las acciones tomadas para la resolución final de la brecha

GUREAK LANEAN ha tomado, entre otras, las siguientes actuaciones:

- Revisión de todas las reglas de firewall
- Monitorización de firewall

Información sobre la recurrencia de estos hechos y el número de eventos análogos acontecidos en el tiempo

- GUREAK LANEAN manifiestan que es la primera vez que un evento de estas características sucede en su organización. No han existido casos similares previos

Respecto de las medidas de seguridad implantadas con anterioridad la brecha

- GUREAK LANEAN ha aportado los siguientes documentos:
    - Registro de Actividades de tratamiento (anexo 10).
    - Análisis de Riesgo (anexo 11).
    - Análisis de la necesidad de evaluación de impacto (anexo 12).
    - Medidas de Seguridad basadas en la norma ISO 27002 (anexo 13).
    - Política de Seguridad de la Información (anexo 14).
    - Política de Protección de Datos (anexo 15).
    - Gestión de incidencia y brechas de seguridad (anexo 16).
    - Informe de Auditoria en el cumplimiento de la normativa de Protección de Datos de fecha 14 de diciembre de 2019 (anexo 17).

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 de

confidencialidad, como consecuencia de una mala configuración en el Firewall permitiendo el acceso desde el exterior.

De las actuaciones de investigación se desprende que, con anterioridad a la brecha de seguridad, la entidad investigada disponía de medidas de seguridad razonables en función de los posibles riesgos estimados. Aporta Registro de Actividades de Tratamiento y Análisis de Riesgo según se indica en los antecedentes y se han tomado las acciones posteriores oportunas para evitar la repetición del incidente.

Asimismo, contaba con protocolos de actuación para afrontar un incidente como el ahora analizado, lo que ha permitido de forma diligente la identificación, análisis y clasificación de la brecha de seguridad de datos personales así como la diligente reacción ante la misma al objeto de minimizar el impacto e implementar nuevas medias razonables y oportunas para evitar que se repita la incidencia en el futuro a través de la puesta en marcha y ejecución efectiva de un plan de actuación por las distintas figuras implicadas como son el responsable del tratamiento y el Delegado de Protección de Datos.

No constan reclamaciones ante esta Agencia por parte de terceros.

En consecuencia, se debe concluir que la entidad investigada disponía de medidas técnicas y organizativas razonables para evitar este tipo de incidencia y que al resultar insuficientes han sido actualizadas de forma diligente. Por último, se recomienda elaborar un Informe Final sobre la trazabilidad del suceso y su análisis valorativo, en particular, en cuanto al impacto final. Este Informe es una valiosa fuente de información con la que debe alimentarse el análisis y la gestión de riesgos y servirá para prevenir la reiteración de una brecha de similares características como la analizada, causada previsiblemente por un error puntual.

III

A la vista de las actuaciones practicadas, se ha acreditado que la actuación de GUREAK LANEAN, S.A 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 GUREAK LANEAN, S.A. con NIF A20044590 y domicilio en ******DIRECCIÓN.1*** (Guipúzkoa).

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