Procedimiento Nº: E/06442/2019
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: *REALE SEGUROS GENERALES, S.A.,* con NIF ***A78520293*** (en adelante, REALE) ha comunicado a esta Agencia que en la mañana del 18 de junio de 2019 se detectó la sustracción de tres equipos portátiles de tres empleados de una sucursal de la entidad en Barcelona. Creen que ocurrió entre la hora de finalización de la jornada y la hora de cierre del día anterior, ya que no saltó el sistema de alarma.

En la notificación de brecha de seguridad aportan copia de la denuncia interpuesta ante los Mozos de Escuadra en la que se relacionan los números de serie de los tres portátiles y en ella manifiestan que desconocen quien puede haber sido el autor porque hasta las 21:00 horas existe en la oficina tanto personal de oficina como de limpieza, y que una vez se cierra al público la oficina se activa el sistema de alarma y de videovigilancia.

En la notificación de la brecha de seguridad informan que puede haber afectado a unas 1000 personas entre las que se encuentran clientes y empleados. Las categorías de datos afectadas son : datos identificativos, de contacto, de salud, y económico-financieros.

SEGUNDO: Con fecha de 24 de junio de 2019 la Directora de la Agencia Española de Protección de Datos acuerda iniciar las presentes actuaciones de investigación en relación a una brecha de seguridad notificada por parte del REALE por lo que la Subdirección General de Inspección de Datos procedió a realizar actuaciones previas de investigación para el esclarecimiento de los hechos objeto de la reclamación, teniendo conocimiento de los siguientes extremos:

FECHAS

De la incidencia de seguridad : entre el 17 y 18 de junio de 2019

De la denuncia ante los Mossos d'Escuadra : 18 de junio de 2019

De notificación ante la AEPD : 19 de junio de 2019

ENTIDADES INVESTIGADAS

REALE SEGUROS GENERALES, S.A. con ***NIF A78520293*** con domicilio en ***C/ SANTA ENGRACIA 14 - 28010 MADRID (MADRID)***

RESULTADO DE LAS ACTUACIONES DE INVESTIGACIÓN

Respecto a los hechos

Requerida información a REALE sobre la incidencia de seguridad notificada, la entidad afectada aclara que los discos duros de los portátiles sustraídos no contenían información ni datos personales de los clientes, ya que los empleados únicamente tratan dicha información a través de aplicaciones corporativas cuyo acceso requiere autenticación mediante usuario y contraseña, sin proceder a su descarga en ningún tipo de soporte lo que incluye el disco duro local de los equipos de los empleados.

A dichas aplicaciones corporativas se accede a través del sitio web de la entidad sin que existan instalaciones de aplicaciones en los equipos de los empleados, por lo que REALE ha concluido que, teniendo presente que desde los equipos sustraídos no resulta posible el acceso directo a datos de clientes, estiman que no existen clientes de REALE afectados.

No se tiene constancia de que datos personales de afectados hayan sido accedidos por terceros ajenos.

Respecto a las medidas implementadas con anterioridad a la brecha:

REALE ha aportado a requerimiento de la Inspección de Datos la siguiente información y documentación:

- REALE mantiene medidas de seguridad física en sus oficinas consistentes en un sistema de alarma con sistema de videovigilancia que se activa al detectar movimiento o accesos no autorizados. Este sistema se encuentra activo cuando la oficina queda vacía y cerrada.

- La puerta de acceso principal de las oficinas es preciso abrirla mediante el uso de un sistema de mando a distancia.

  La oficina de REALE donde tuvo lugar la sustracción cuenta con otras cuatro puertas de emergencia, siendo la directriz que las mismas permanezcan cerradas en todo momento, salvo en caso de emergencia.

- El motivo por el cual estas medidas no sirvieron para evitar la sustracción fue un error humano involuntario que produjo que una de las puertas de emergencia se encontrara abierta en el lapso de tiempo que transcurre entre el final de la actividad laboral y la activación de la alarma.

- Con respecto las políticas y medidas de seguridad generales, REALE ha aportado copia del registro de actividades de Tratamiento y los Análisis de Riesgos relacionados con cada actividad. También ha aportado copia de la Evaluación de Impacto de una de las actividades de tratamiento.

- Los equipos de los empleados acceden a los datos de los clientes de REALE mediante aplicaciones corporativas cuyo acceso requiere autenticación mediante usuario y contraseña, sin proceder a descargas de datos en ningún tipo de soporte lo que incluye el disco duro local de los equipos de los empleados.

  Las directrices de REALE incluyen la prohibición de copiar o descargar toda o parte de la información contenida en el sistema de información web de la entidad en ningún soporte ni informático ni físico si no se dispone de autorización expresa por el equipo directivo. Aportan impresión de pantalla de la información que se muestra al usuario de las aplicaciones corporativas donde consta dicha leyenda, entre otras, como las relacionadas con la protección de los datos personales, el compromiso a guardar secreto, los accesos y su registro, las medidas de seguridad.

Respecto a las acciones emprendidas y las medidas implantadas como consecuencia de la incidencia de seguridad:

- Como consecuencia de la brecha de seguridad, se bloquearon los usuarios informáticos de los empleados cuyos portátiles fueron sustraídos y se gestionó el reseteo (o reinicialización) de sus contraseñas que permitían el acceso a la web corporativa.

- Se interpuso denuncia ante los Mozos de Escuadra. No han recibido noticias o novedades en relación con la posible investigación policial en curso.

- La Delegada de Protección de Datos (DPD) de REALE ha mantenido contactos con los empleados involucrados y los responsables territoriales, a fin de esclarecer los hechos, recabar información e impulsar la implantación de medidas de seguridad física y organizativas adicionales, a fin de evitar nuevas situaciones similares en el futuro. Aportan copia de correos electrónicos remitidos por la DPD a los empleados.

- REALE manifiesta que se encuentra valorando la implantación de las siguientes acciones:

  - Implementar mecanismos de alerta (sonoros y/o visuales) en caso de apertura indebida de las puertas de emergencia.

  - Reforzar la concienciación en cuanto a la directriz corporativa de prohibición de apertura de dichas puertas, excepto en caso de emergencia.

  - Realizar una evaluación de riesgos de seguridad física en las oficinas de la entidad para la implementación de medidas de mejora.

Aportan correo electrónico de fecha 9 de julio de 2019 que propone la revisión interna y definición de requerimientos de seguridad física en las oficinas que incluye, entre otros aspectos, los sistemas de grabación, especificando que en la actualidad solo se activan cuando el director de la sucursal o el último sale, así como la unificación y clarificación de los procedimientos y sistemas de acceso en las oficinas.

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, si bien la entidad afectada manifiesta que el posible origen de la sustracción de los equipos parte de un error humano involuntario, también pudo ser como consecuencia de una acción deliberada maliciosa tanto desde el interior como del exterior de la entidad, que en todo caso superaron las medidas de seguridad implantadas.

No obstante, se significa que la entidad afectada disponía de medidas de seguridad razonables para evitar un robo como el ahora notificado, toda vez que contaba con alarma detectora de presencia, de apertura de puertas de emergencia y de difusión de los protocolos de información a los empleados respecto de las medidas de seguridad a tener en cuenta.

Hay que añadir que de la información facilitada a esta AEPD se despende que queda descartada la posibilidad de acceso a los datos de clientes por terceros ajenos desde los equipos robados al carecer de los mismos, toda vez que los empleados acceden a los datos de los clientes desde los propios servidores web de la entidad con usuario y contraseña personalizada sin posibilidad de descargarlos en dispositivos externos de cualquier tipo.

Por último, señalar que la actuación de la entidad afectada tras detectar la quiebra de seguridad debe considerarse razonablemente diligente al iniciar sin dilación una investigación interna de los hechos y tomar las medidas cautelares arriba indicadas para minimizar los riesgos de acceso a los datos por terceros ajenos, denunciar ente los Mossos d'Escuadra el incidente e implantar nuevas medidas de seguridad de índole físico y de información a los empleados para evitar la repetición en el futuro de hechos similares.

III

Por lo tanto, se ha acreditado que la actuación del reclamado como entidad responsable del tratamiento [y como entidad encargada de la gestión del tratamiento, respectivamente], [y de la razón social 3, como entidad informante [*en relación con la*

inclusión de los datos personales del reclamante en ficheros de solvencia patrimonial y crédito], 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 ***REALE SEGUROS GENERALES, S.A.*** con ***NIF A78520293*** con domicilio en ***C/ SANTA ENGRACIA 14 - 28010 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