- **Procedimiento Nº: E/08765/2020**

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: Las actuaciones de inspección se inician por la recepción de un escrito de notificación de brecha de seguridad de los datos personales remitido por CUALTIS, S.L.U., *con NIF B84527977* en el que informan a la Agencia Española de Protección de Datos que, con fecha 19 de octubre de 2020, debido a un error humano el programa informático envió desde la dirección "*covid19@cualtis.com*", 3.613 emails a 190 clientes información de las personas designadas y de los trabajadores considerados como posible personal vulnerable de 30 empresas clientes.

Como consecuencia de la notificación a la División de Innovación Tecnológica de esta Agencia de una brecha de seguridad de datos personales por parte del Responsable del Tratamiento CUALTIS SLU con número de registro de entrada O00007128e2000007165 relativa a envío de datos personales a destinatarios incorrectos, se 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.

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 la brecha de seguridad de datos personales: 22 de octubre de 2020.

ENTIDADES INVESTIGADAS

Durante las presentes actuaciones se han investigado las siguientes entidades:

CUALTIS, S.L.U. (en adelante Cualtis), con NIF B84527977, en calidad de responsable del tratamiento.

RESULTADO DE LAS ACTUACIONES DE INVESTIGACIÓN

1.- Con fecha 16 de noviembre de 2020 se solicitó información a CUALTIS, S.L.U. De la respuesta recibida se desprende lo siguiente:

Respecto de la cronología de los hechos

El lunes 19 de octubre de 2020 entre las 15:50 y las 16:21, desde la dirección *"covid19@cualtis.com"* se enviaron por error un total de 3.613 emails a 190 empresas clientes (a las direcciones de correo electrónico de los representantes de estas empresas para la gestión de la valoración de trabajadores especialmente sensibles) con la información correspondiente de 30 empresas a las que prestan servicios (Nombre, email, teléfono y NIF del representante) respecto de los datos de sus

trabajadores que la organización había informado como posible personal vulnerable (nombre, NIF y puesto de trabajo), que sumaban un total de 165 trabajadores entre todas las empresas.

Esta brecha fue detectada por el personal del soporte técnico de Cualtis que supervisa las peticiones que llegan al buzón indicado para atenderlas, donde se comenzó a recibir avisos de algunas direcciones que indicaban que esa información no se correspondía con la de sus trabajadores, por lo que inmediatamente el equipo de soporte contactó con el equipo técnico de la aplicación quienes procedieron a parar el proceso automático que envía los correos a los clientes con los trabajadores pendientes de identificar el nivel de exposición al virus (covid19) para que informen y se pueda comenzar la valoración del trabajador.

La brecha fue detectada y solventado la brecha en un plazo de aproximadamente media hora.

Posteriormente se identificó la causa del problema y se resolvió la incidencia que causó la brecha.

Respecto de las causas que hicieron posible la brecha

El incidente se produjo por la subida de un paquete de software erróneo que se confundió con el que realmente estaba preparado tras la realización de las pruebas pertinentes en el entorno de *test*. En el momento del pase a producción tras la validación del paquete correcto, un error humano provocó que seleccionara el paquete de software equivocado y que éste subiera a producción, lo que causó el envío masivo de emails que fue detectado y detenido en un máximo de media hora, dando marcha a atrás al despliegue para volver a la situación adecuada.

Medidas de minimización del impacto de la brecha y resolución de la misma.

• Parada de proceso automático de envío y realización de marcha atrás al despliegue erróneo (19/10/2020 – 16:21)

• Notificación y gestión interna desde el rol de DPD y Responsable de privacidad para su investigación, análisis y gestión. (19/10/2020 – 17:00)

• Bloqueo temporal del servicio automático y atención manual de las peticiones (19/10/2020 – 17:00)

• Aviso interno a todo el personal que tenga relación con las empresas afectadas. (19/10/2020 – 18:00)

• Notificación de la incidencia a las empresas clientes de CUALTIS involucradas en el incidente (20/10/2020 – 11:56)

• Ofrecimiento a estas empresas para el envío personalizado de la información detallada de su empresa que ha sido expuesta al resto. (20/10/2020 – 11:56)

• Notificación a Agencia Española de Protección de Datos (22/10/2020 – 15:58).

• Activación de reglas en el servidor de correo electrónico para solicitar autorización al Director de Tecnología ante la detección de correos masivos a direcciones email externas. (10/11/2020 – 13:00)

• Análisis de mejoras en el proceso de subida a producción. (17/11/2020 – 18:00)

• Inclusión de la incidencia y del riesgo en el Sistema de Seguridad de la información para investigar con más detalle el evento y proponer, definir y desplegar medidas

preventivas a corto y medio plazo para evitar dichas incidencias mejorando el proceso del ciclo de vida del software.

Respecto de los datos afectados.

El número de afectados asciende a 165 trabajadores y de 30 representantes de empresas diferentes.

De los 165 trabajadores se expuso a terceros el nombre y apellidos, DNI y su puesto de trabajo, mientras que de los 30 representantes de empresas se expuso sus direcciones de correo electrónico.

Aportan copia del Modelo Comunicación realizada a los Afectados informando del incidente.

Cualtis no tiene constancia de la utilización por terceros de los datos expuestos.

Cualtis no tiene constancia de posible publicación en internet e indexación por buscadores de los datos expuestos.

Respecto de las medidas de seguridad implantadas con anterioridad la brecha

- Aportan copia del Registro de Actividad de los Tratamientos (RAT) de la actividad denominada "*Seguimiento de contactos estrechos*".
- Aportan auditoría de seguridad sobre cumplimiento RGPD y evaluación de impacto en el tratamiento de datos personales del servicio de *"Seguimiento de contactos estrechos"* (covid19), cuyo objeto consta *"Realizar la evaluación de impacto del tratamiento servicio de Seguimiento de trabajadores de contacto estrechos en los términos exigidos por el GDPR y LOPD GDD, estableciendo procedimientos documentados para posibles tratamientos posteriores, realizando una presentación del proyecto y una formación interna a implicados."*
- Aporta la documentación acreditativa de la *"Política de Seguridad*":
    - Política corporativa de tratamiento de datos personales
    - Política de seguridad de la información en ciclo de vida del software
    - Política Pública Seguridad en el desarrollo del software_privacidad.cualtis.com
- Aportan información sobre *"Procedimiento General Existente*" ante brechas de seguridad, incluyendo:
    - Instrucción General Violaciones de Seguridad
    - Procedimiento de gestión de vulneraciones críticas en tratamientos de datos personales: Gestión de incidencias de seguridad de la información
    - Política Pública: Notificación de brechas de seguridad en tratamientos de datos personales.

Respecto de las medias implementadas con posterioridad la brecha

Según manifiestan:

• Se ha implantado un circuito de integración continua del desarrollo de software para garantizar el ciclo de vida completo de un desarrollo de software y evitar errores en despliegues de software improcedentes que puedan poner el 5 peligro la seguridad de

los datos manejados por el mismo, así como garantizar la seguridad y fiabilidad de los desarrollos que suben a producción.

• Está en curso la integración del proyecto de software que causó la brecha de seguridad de la información en dicho circuito de integración continua, que debido a su reciente implantación no estaba incluido en el mismo. Mientras tanto se han adoptado medidas para detectar y evitar todo envío de información masiva a través de correo electrónico a direcciones de correo externas mediante una regla del servidor de correo que en caso de detectar estas situaciones solicita permiso para el envío al Director de Tecnologías de la información antes de ser enviado.

• Se han modificado los desarrollos involucrados que envían este tipo de correos necesarios para el funcionamiento del sistema, para que todos los envíos a las empresas vayan con copia oculta y evitar que puedan quedar visibles a otras empresas en caso de error.

• Se han adoptado medidas técnicas y organizativas para evitar, en lo posible, incidentes de seguridad como el sucedido:

- Configuración de reglas del servidor de correo para evitar envíos masivos a direcciones de fuera de la organización con información anexada que pueda originar una brecha de seguridad de la información
- Inclusión del proyecto de software que causó la brecha en el circuito de integración continua
- Adoptar herramientas de prueba automática dentro del circuito de integración continua.
- Revisión y actualización del documento de “Política de seguridad de la información en el ciclo de vida del software”, para incluir medidas adicionales en relación con la brecha.

Cualtis ha contratado a la entidad “******EMPRESA.1***” para la realización de “*Auditorías de Seguridad de la Infraestructura*”, así como de las “*Comunicaciones y Servicios Internos y Externos*” durante los próximos 3 años. Aportan certificados expedidos por la citada entidad donde se detalla:

• Alcance, metodología y pruebas de las Auditorias.

• Certificado de realización y finalización de las Auditorias.

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, consta que el origen de la brecha de seguridad de datos personales fue debido a un error humano al subir a producción un aplicativo inadecuado. No obstante, de la cronología de los hechos se desprende que Cualtis disponía de las medidas organizativas y técnicas razonables que permitieron en el breve lapso de media hora detectar la incidencia e implementar las medidas oportunas para minimizar el impacto arriba indicadas. Así, desplegó el protocolo de seguridad previamente establecido y procedió a actuar conforme con lo previsto. Entre las actuaciones llevadas a cabo por Cualtis, se debe señalar que, tras la detección y paralización del aplicativo subido por error al entorno de producción, se procedió a comunicar la incidencia a los afectados y notificar la brecha de seguridad a la AEPD. Con posterioridad, también se implantaron nuevos protocolos sobre la gestión de la información de la que es responsables al objeto de evitar la repetición de eventos similares en el futuro, encargando la elaboración de dichos protocolos a una entidad especializada.

También consta que Cualtis procedió de forma diligente a contestar todas las cuestiones planteadas por los afectados tras la comunicación de la brecha de seguridad.

Por último, cabe 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

Por lo tanto, se ha acreditado que la actuación de Cualtis, 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 CUALTIS, S.L.U., con NIF B84527977.

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