

- **Expediente N°: E/09935/2020**

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: Con fecha 2 de diciembre de 2020, la Subdirección General de Inspección de Datos recibió para su valoración un escrito de notificación de brecha de seguridad de los datos personales remitido por BELDEN IBERIA S.L. con NIF B84125574 (en adelante, BELDEN), y un escrito de notificación de brecha de seguridad de los datos personales remitido por GRASS VALLEY SPAIN, S.A. con NIF A82773664 (en adelante, GRASS VALLEY), recibido ambos en fecha 25 de noviembre de 2020, en los que se informa a la Agencia Española de Protección de Datos:

- BELDEN IBERIA SL informa que, con fecha 12 de noviembre de 2020, el equipo de Tecnología de la Información del Grupo BELDEN (...).

(...).

Puede haber afectados y notificaciones de brecha en diversos países europeos.

- GRASS VALLEY SPAIN S.A. manifiesta tener constancia de una violación de datos que afecta a sus antiguos propietarios el Grupo BELDEN (pertenecían a dicho Grupo hasta julio de 2020).

SEGUNDO: La Subdirección General de Inspección de Datos procedió a la realización de actuaciones previas de investigación para el esclarecimiento de los hechos en cuestión, en virtud de los poderes de investigación otorgados a las autoridades de control en el artículo 57.1 del Reglamento (UE) 2016/679 (Reglamento General de Protección de Datos, en adelante RGPD), y de conformidad con lo establecido en el Título VII, Capítulo I, Sección segunda, de la LOPDGDD, teniendo conocimiento de los siguientes extremos:

Respecto de la empresa

- Tal y como consta en Internet, Belden Inc. es un fabricante estadounidense de soluciones de transmisión de señales, incluyendo la creación de redes, conectividad y productos de cable.
- El Grupo Belden es un grupo de sociedades internacional cuya sede central está radicada en Estados Unidos. Por lo que respecta a la Unión Europea, su principal centro de actividad se sitúa en los Países Bajos, con las sociedades siguientes: Belden CDT European Shared Services B.V., Belden Europe BV y Belden Wire & Cable BV.

- Grupo Belden se encuentra actualmente en proceso de tramitación de la aprobación de sus Normas Corporativas Vinculantes (*Binding Corporate Rules*). Se trata de un proyecto que comenzó en 2019 y actualmente Grupo Belden está finalizando la solicitud ante la Autoridad Holandesa de Protección de Datos, que ha aceptado actuar en calidad de autoridad principal.
 - Los principales servidores de Grupo Belden (...)
 - Al ser una empresa estadounidense con un establecimiento principal en la Unión Europea ubicado en Holanda, la incidencia de seguridad notificada tiene carácter transfronterizo, motivo por el cual se ha realizado consultas en el “Sistema de Información del Mercado Interior” (en lo sucesivo IMI), regulado por el Reglamento (UE) nº 1024/2012, del Parlamento Europeo y del Consejo, de 25 de octubre de 2012 (Reglamento IMI) y que tiene como objeto favorecer la cooperación administrativa transfronteriza, la asistencia mutua entre los Estados miembros y el intercambio de información, sin obtener constancia de la existencia de ninguna anotación relativa a BELDEN IBERIA SL y GRASS VALLEY SPAIN SA. Dichas consultas se realizaron desde la Inspección de Datos, en fecha 11 de diciembre de 2020.
- Asimismo, y con fecha 19 de abril de 2021 se consulta nuevamente el Sistema IMI sin obtener constancia de anotaciones respecto del Grupo Belden.
- No obstante, la empresa manifiesta haber remitido una notificación de este incidente a la Autoridad Holandesa de Protección de Datos.
- Grupo Belden es la propietaria de los sistemas y se ocupa por sí misma de su mantenimiento, sin que, por consiguiente, tenga ningún contrato relevante con terceros.
 - GRASS VALLEY SPAIN S.A. fue propiedad del Grupo Belden hasta julio de 2020.
 - En su escrito de 31 de agosto de 2021, GRASS VALLEY SPAIN S.L. manifiesta a esta Agencia que (...).

Respecto de la cronología de los hechos. Acciones tomadas con objeto de minimizar los efectos adversos y medidas adoptadas para su resolución final

El informe técnico del ataque fue elaborado a nivel global para todas las entidades del Grupo Belden y, por tanto, no es exclusivo de Belden Iberia.

- El 12 de noviembre de 2020, el equipo del departamento de Tecnologías de la Información (TI) de Grupo Belden (...).
- El 13 de noviembre (...).
- (...).
- Tras la brecha de seguridad de los datos, Grupo Belden procedió a la contratación de una empresa externa para adoptar las medidas de contención a medio y largo plazo. Entre ellas:
 - o (...).
 - o (...).
 - o (...).
 - o (...).
 - o (...).
 - o (...).

Respecto de las causas que hicieron posible la brecha

- En la auditoría realizada por la empresa externa se considera que (...).
- (...).
- (...).

Respecto de los datos afectados

- Grupo Belden manifiesta que los datos posiblemente exfiltrados corresponden a: (...).
 - (...)
 - (...)
 - (...)
- A este respecto, han aportado copia de las comunicaciones.
- (...)
 - (...)

Respecto de la Seguridad del tratamiento de datos con anterioridad y posterioridad a la brecha

- Grupo Belden manifiesta que (...)
- (...)
- (...):
 - o (...).
 - o (...).
 - o (...).
 - o (...).
 - o (...).
 - o (...).
 - o (...).
 - o (...).
 - o (...).
 - o (...).
 - o (...).
 - o (...).
 - o (...).
 - o (...).
 - o (...).
- (...).
- (...):
 - o (...).
 - o (...).
 - o (...).
 - o (...).
 - o (...).
 - o (...).
 - o (...).
 - o (...).
 - o (...).
- (...):
 - o (...).
 - o (...).

Respecto de la notificación con posterioridad a las 72 horas

Grupo Belden manifiesta que Belden Iberia, por su condición de entidad no operativa, no cuenta con certificado digital y que tuvieron complicaciones imprevistas para realizar la notificación de brecha de seguridad a la AEPD a través de la sede electrónica, al no contar con el certificado. Por ello, se adoptaron medidas expeditas para presentar físicamente la notificación, pero las restricciones relacionadas con el COVID causaron demoras que no podían preverse y que son ajenas a Belden Iberia.

Todas las entidades de Grupo Belden fueron informadas de la brecha de seguridad de los datos inmediatamente. Asimismo, Grupo Belden se aseguró de que todas las Autoridades de Protección de Datos de los países donde es preceptivo comunicar las brechas de seguridad de datos fueran informadas de la brecha a la mayor brevedad posible y, en todo caso, dentro del plazo establecido en cada país. Tras las citadas comunicaciones, varias autoridades de protección de datos se han puesto en contacto con Grupo Belden y pueden confirmar que las autoridades de protección de datos británica, canadiense (de Alberta), sueca, danesa y vietnamita han cerrado la investigación sin ninguna crítica y sin recomendar ninguna actuación adicional.

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

Belden manifiesta que no se ha vuelto a replicar la brecha de seguridad de los datos desde que Belden descubriera la misma e implantara las medidas de contención.

FUNDAMENTOS DE DERECHO

I

Competencia

En virtud de los poderes que el artículo 58.2 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (RGPD) reconoce a cada autoridad de control, y según lo establecido en los artículos 47 y 48 de la LOPDGDD, investigación la Directora de la Agencia Española de Protección de Datos es competente para iniciar y resolver este procedimiento.

II

Cuestiones previas

En el presente caso, de acuerdo con lo establecido en el artículo 4.1 del RGPD, consta la realización de un tratamiento de datos personales, toda vez que BELDEN realiza, entre otros tratamientos, el almacenamiento de los siguientes datos personales de personas físicas, tales como: nombre, domicilio, fecha de nacimiento, entre otros.

BELDEN realiza esta actividad en su condición de responsable del tratamiento, dado que es quien determina los fines y medios de tal actividad, en virtud del artículo 4.7 del RGPD.

El artículo 4 apartado 12 del RGPD define, de un modo amplio, las “violaciones de seguridad de los datos personales” (en adelante brecha 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 una brecha de seguridad de datos personales en las circunstancias arriba indicadas, categorizada como una brecha de confidencialidad, al haber accedido un tercero a los servidores empresariales en la sede central del Grupo, habiéndose producido una exfiltración de datos de empleados y exempleados.

Hay que señalar que la identificación de una brecha de seguridad no implica la imposición de una sanción de forma directa por esta Agencia, ya que es necesario analizar la diligencia de responsables y encargados y las medidas de seguridad aplicadas.

La seguridad de los datos personales viene regulada en los artículos 32, 33 y 34 del RGPD, que regulan tanto la seguridad del tratamiento, la notificación de una violación de la seguridad de los datos personales a la autoridad de control, así como la comunicación al interesado, respectivamente.

III

Artículo 32 del RGPD

El Artículo 32 “*Seguridad del tratamiento*” del RGPD establece:

“1. Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros:

- a) la seudonimización y el cifrado de datos personales;*
- b) la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento;*
- c) la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico;*
- d) un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.*

2. Al evaluar la adecuación del nivel de seguridad se tendrán particularmente en cuenta los riesgos que presente el tratamiento de datos, en particular como consecuencia de 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.

3. La adhesión a un código de conducta aprobado a tenor del artículo 40 o a un mecanismo de certificación aprobado a tenor del artículo 42 podrá servir de elemento

para demostrar el cumplimiento de los requisitos establecidos en el apartado 1 del presente artículo.

4. El responsable y el encargado del tratamiento tomarán medidas para garantizar que cualquier persona que actúe bajo la autoridad del responsable o del encargado y tenga acceso a datos personales solo pueda tratar dichos datos siguiendo instrucciones del responsable, salvo que esté obligada a ello en virtud del Derecho de la Unión o de los Estados miembros”.

En el presente caso, de la documentación aportada por BELDEN en el curso de estas actuaciones de investigación no se desprende que, con anterioridad a la brecha de seguridad, BELDEN careciera de medidas de seguridad razonables en función de los posibles riesgos estimados.

Asimismo, no existen evidencias de que no hubiera actuado de forma diligente una vez conocida la brecha de seguridad, ni que las medidas adoptadas con posterioridad al incidente aquí analizado no fueran adecuadas.

Tampoco constan reclamaciones ante esta Agencia por parte de terceros, relacionadas con la presente brecha de seguridad.

IV

Artículo 5.1.f) del RGPD

El artículo 5.1.f) “*Principios relativos al tratamiento*” del RGPD establece:

*“1. Los datos personales serán:
(...)*

f) tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas («integridad y confidencialidad»).”

En el presente caso, consta que los datos personales de los afectados, obrantes en la base de datos de BELDEN, fueron indebidamente expuestos a un tercero, que había accedido a información confidencial que contenía datos de carácter personal.

No obstante, cabe recordar que la mera identificación de una brecha de seguridad por parte de esta Agencia no implica la comisión de una infracción en materia de protección de datos, ya que es necesario analizar la diligencia de responsables y encargados y las medidas de seguridad aplicadas.

Tal como se ha expuesto anteriormente, de los hechos que se deducen del expediente administrativo, no se desprende que, con anterioridad a la brecha de seguridad, BELDEN, careciera de medidas de seguridad razonables en función de los posibles riesgos estimados ni que no se hubiera actuado de forma diligente una vez conocida la brecha de seguridad, ni que las medidas adoptadas con posterioridad al incidente aquí analizado no fueran adecuadas.

Al respecto, el artículo 28 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público dispone que: *“Sólo podrán ser sancionadas por hechos constitutivos de infracción administrativa las personas físicas y jurídicas, (...) que resulten responsables de los mismos a título de dolo o culpa”*.

En el presente caso, no ha quedado acreditado que BELDEN hubiera actuado de forma negligente ni, mucho menos, con dolo por su parte, por tanto, no cabe entender que se hubiera producido una infracción del artículo 5.1.f) RGPD.

V

Artículo 33 del RGPD

El artículo 33 *“Notificación de una violación de la seguridad de los datos personales a la autoridad de control”* del RGPD dispone:

“1. En caso de violación de la seguridad de los datos personales, el responsable del tratamiento la notificará a la autoridad de control competente de conformidad con el artículo 55 sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, a menos que sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas. Si la notificación a la autoridad de control no tiene lugar en el plazo de 72 horas, deberá ir acompañada de indicación de los motivos de la dilación.

2. El encargado del tratamiento notificará sin dilación indebida al responsable del tratamiento las violaciones de la seguridad de los datos personales de las que tenga conocimiento.

3. La notificación contemplada en el apartado 1 deberá, como mínimo:

- a) describir la naturaleza de la violación de la seguridad de los datos personales, inclusive, cuando sea posible, las categorías y el número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados;*
- b) comunicar el nombre y los datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información;*
- c) describir las posibles consecuencias de la violación de la seguridad de los datos personales;*
- d) describir las medidas adoptadas o propuestas por el responsable del tratamiento para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.*

4. Si no fuera posible facilitar la información simultáneamente, y en la medida en que no lo sea, la información se facilitará de manera gradual sin dilación indebida.

5. El responsable del tratamiento documentará cualquier violación de la seguridad de los datos personales, incluidos los hechos relacionados con ella, sus efectos y las medidas correctivas adoptadas. Dicha documentación permitirá a la autoridad de control verificar el cumplimiento de lo dispuesto en el presente artículo”.

En el presente supuesto, se ha notificado la brecha de seguridad en un plazo superior a las 72 horas desde que se tuvo conocimiento de que se había producido, pero se han acreditado correctamente los motivos de tal dilación, toda vez que BELDEN, por su condición de entidad no operativa, no contaba con certificado digital y tuvieron complicaciones imprevistas para realizar la notificación de brecha de seguridad a la AEPD a través de la sede electrónica, al no contar con el certificado. Por ello, se adoptaron medidas expeditas para presentar físicamente la notificación, pero las restricciones relacionadas con el COVID causaron demoras que no podían preverse y que son ajenas a BELDEN.

VI

Artículo 34 del RGPD

El artículo 34 “Comunicación de una violación de la seguridad de los datos personales al interesado” del RGPD establece:

“1. Cuando sea probable que la violación de la seguridad de los datos personales entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento la comunicará al interesado sin dilación indebida.

2. La comunicación al interesado contemplada en el apartado 1 del presente artículo describirá en un lenguaje claro y sencillo la naturaleza de la violación de la seguridad de los datos personales y contendrá como mínimo la información y las medidas a que se refiere el artículo 33, apartado 3, letras b), c) y d).

3. La comunicación al interesado a que se refiere el apartado 1 no será necesaria si se cumple alguna de las condiciones siguientes:

- a) el responsable del tratamiento ha adoptado medidas de protección técnicas y organizativas apropiadas y estas medidas se han aplicado a los datos personales afectados por la violación de la seguridad de los datos personales, en particular aquellas que hagan ininteligibles los datos personales para cualquier persona que no esté autorizada a acceder a ellos, como el cifrado;*
- b) el responsable del tratamiento ha tomado medidas ulteriores que garanticen que ya no exista la probabilidad de que se concrete el alto riesgo para los derechos y libertades del interesado a que se refiere el apartado 1;*
- c) suponga un esfuerzo desproporcionado. En este caso, se optará en su lugar por una comunicación pública o una medida semejante por la que se informe de manera igualmente efectiva a los interesados.*

4. Cuando el responsable todavía no haya comunicado al interesado la violación de la seguridad de los datos personales, la autoridad de control, una vez considerada la probabilidad de que tal violación entrañe un alto riesgo, podrá exigirle que lo haga o podrá decidir que se cumple alguna de las condiciones mencionadas en el apartado 3.”

BELDEN aporta copia de la comunicación enviada a los usuarios afectados, de acuerdo con lo establecido en el citado artículo 34 RGPD.

Cabe destacar que no consta ante esta Agencia reclamación alguna sobre la brecha de seguridad objeto del presente expediente.

VII Conclusión

Por lo tanto, en base a lo indicado en los párrafos anteriores, no se han encontrado evidencias que acrediten la existencia de infracción en el ámbito competencial de la Agencia Española de Protección de Datos.

Así pues, 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 BELDEN IBERIA S.L.

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.

940-051121

Mar España Martí
Directora de la Agencia Española de Protección de Datos