

Asertrucks

De: Asertrucks <asertrucks@asertrucks.es>
Enviado el: martes, 18 de junio de 2019 11:46
Asunto: Brechas de seguridad de datos personales: qué son y cómo actuar

Seguimiento:

Destinatario	Lectura
andresnr@manuelrey.com	Eliminado: 24/06/2019 10:28
ANTONIO ESTEVE (aesteve@motortarrega.com)	
Asertrucks	
AUPASA CAMIONES	Leído: 18/06/2019 11:55
'AUTOS BUENOS AIRES GALICIA (abgalicia@gmail.com)'	
AZUDAUTOS (GER-FORM)	
AZUDAUTOS VENTAS	
'CAMIONSA'	
EXTREMEÑA DE CAMIONES	
EXTREMEÑA DE CAMIONES	
FERNANDO AGON	
FERNANDO AGON S.L. (pedro)	
FERNANDO AGON, S.L.	Eliminado: 04/09/2019 16:52
fran@fernandoagon.com	Leído: 18/06/2019 11:51
FRANCISCO ORTEGA (juan@grupo-alvarez.net)	Leído: 18/06/2019 16:23
GONSOLI LORCA	
'GUADARRAMA CAMIONES'	
'MANUEL REY'	
'MANUEL REY'	
'MOTORISA'	
PEDRO GUTIERREZ LIEBANA	
PEDRO GUTIERREZ LIEBANA	
'R1 GAMA CAMIONES 2010,S.L.'	
SANTISTEBAN V.I.	
SERCASA	
SERCASA (CALIDAD Y TACOGRAFO)	
SIGFREDO MORENO (smoreno@r1gama.com)	
SR. JUAN JOSÉ ACOSTA ACOSTA (juanjoseacosta@grupoacosta.org)	
TALAUTO	Leído: 18/06/2019 12:15
TALAUTO	
'TALLERES CRAF'	Leído: 18/06/2019 22:57
TALLERES CRAF	Leído: 18/06/2019 19:00
'TALLERES SCORA'	
'TALLERES SCORA'	Leído: 28/06/2019 16:12
'V.I. TALLERES PASTOR'	Leído: 18/06/2019 13:03
VALAUTO	
'VEHINSA'	Leído: 19/06/2019 12:31

Destinatario

Lectura

VEINLUC

'VEINLUC'



RED DE RENAULT TRUCKS

Att. Sr. Director Gerente

Madrid, 18 de junio de 2019.

Ref: R/129-19

Estimado asociado,

Adjunto remito información que nos ha hecho llegar D. Agustín Pérez (Apemar) sobre las brechas de seguridad de datos personales.

Cualquier aclaración al respecto, por favor, póngase en contacto con Asertrucks.

Atentamente

Almudena Díaz
Secretaria General
ASERTRUCKS
Telf: 91.350.31.56

De: APEMAR [mailto:agustin.perez@apemag.es]

Enviado el: martes, 18 de junio de 2019 10:20

Para: APEMAR

Asunto: Brechas de seguridad de datos personales: qué son y cómo actuar

Estimado Colaborador:

Mediante el presente comunicado pretendemos aclarar qué es una **brecha de seguridad de datos personales**, cómo debe una organización prepararse para afrontarlas, qué hacer si sucede y en qué casos hay que notificar a la AEPD y a los afectados.

- **¿QUE ES UNA BRECHA DE SEGURIDAD DE DATOS PERSONALES?**

Es un incidente de seguridad que afecta a datos de carácter personal. Este incidente puede tener un origen accidental o intencionado y además puede afectar a datos tratados digitalmente o en formato papel. En general, se trata de un suceso que ocasione destrucción, pérdida, alteración, comunicación o acceso no autorizado a datos personales.

- **¿QUE HACER?**

ANTES: el responsable del tratamiento debe estar preparado para esta posibilidad, establecer quién y qué acciones se ejecutarán en caso de producirse. Para ello, lo primero es ser consciente de qué datos personales se están tratando, con qué medios y los riesgos que puede haber. Así, una parte muy importante es implementar mecanismos que permitan detectar las brechas de seguridad de datos de carácter personal.

SI SUCEDER: el responsable del tratamiento debe poner en marcha el plan de actuación, concretando tareas específicas que permitan resolver la brecha, minimizar sus consecuencias y evitar que vuelva a suceder en el futuro.

- **NOTIFICACION A LA AEPD Y COMUNICACION A LOS AFECTADOS**

Ante el suceso de una brecha de seguridad, el responsable del tratamiento debe valorar las posibles consecuencias sobre los afectados y su severidad. Una brecha de seguridad puede producir daños en la reputación de los afectados, limitar sus derechos, producir pérdidas financieras, discriminación, etc. y además puede producir estos efectos con diferentes grados de severidad, por lo que debemos pensar en los beneficios que aporta el que los afectados sean conscientes de que esa brecha se ha producido.

Para realizar esta valoración correctamente es de suma importancia **tener el registro de actividades de tratamiento y el análisis de riesgo previamente elaborado y actualizado.**

Si la brecha de seguridad constituye un riesgo para los derechos y las libertades de las personas se debe notificar ante la AEPD en un plazo máximo de 72 horas desde que se tenga constancia a través del enlace habilitado en la Sede electrónica. En cualquier caso, en la línea de proactividad y transparencia que marca el RGPD siempre es recomendable notificar ante la AEPD una brecha de seguridad en los datos personales que sufra un responsable del tratamiento.

Para rellenar el formulario es muy útil tener de antemano clara la información relevante para la brecha que se ha destacado anteriormente.

Si además entraña un alto riesgo deberá comunicarse sin dilación indebida a los afectados a través del medio que se suela utilizar para comunicarse con ellos, con un lenguaje claro y sencillo. Esto permitirá que los afectados puedan reaccionar cuanto antes y tomar las medidas oportunas, porque en dicha comunicación se les deberá explicar claramente lo sucedido y las medidas recomendadas para que puedan minimizar o eliminar las consecuencias negativas que pueda tener la brecha sobre ellos.

En el caso que la brecha la sufra un encargado del tratamiento, este debe informar al responsable del tratamiento, que tendrá que valorar si notifica ante la AEPD y comunicar a los afectados. En todo caso, los detalles sobre las responsabilidades del responsable y encargado ante una brecha de

seguridad deben quedar expresamente detalladas en el contrato mediante el cual se establece el encargo del tratamiento.

Independientemente de si se ha notificado a la AEPD o no, o si se ha informado a los afectados, debemos llevar un **registro de las brechas de seguridad** que suframos, en el que se justifique las decisiones que se han tomado. **Este documento puede ser exigible en cualquier momento por parte de la AEPD.**

- **CONCLUSIONES**

Con el marco establecido por el Reglamento General de Protección de Datos y la Ley Orgánica 3/2018 se promueve una cultura para la gestión diligente de los datos personales por parte de los encargados y responsables del tratamiento. Por un lado, esta nueva cultura de tratamiento de brechas de seguridad debe permitir minimizar el impacto sobre los afectados, estableciendo mecanismos para que puedan ser conscientes y puedan tomar medidas. Por otro lado, tan importante como solucionar una brecha de seguridad y minimizar las consecuencias sobre los afectados, es aprender de ella, y determinar qué ha fallado en los procedimientos de gestión de la información. Para ello, forma parte del principio de responsabilidad proactiva documentar en detalle la brecha y las acciones tomadas para gestionarla y prevenirla en el futuro.

Para ampliar información sobre cómo actuar ante una brecha de seguridad y qué aspectos deben estar planificados con anterioridad, puedes consultar la guía de la AEPD [Guía de gestión y notificación de brechas de seguridad](#).

Confiamos en que la información facilitada sea de su utilidad y quedamos a su entera disposición por si precisan de alguna aclaración al respecto.

Saludos cordiales.

Agustín Pérez Martínez
Socio - Director
Telf.: 91 463 89 78 - 620 268 360
Email: agustin.perez@apemag.es
www.apemag.es



Este documento se dirige exclusivamente a su destinatario. Puede contener información confidencial sometida a secreto profesional y su divulgación está prohibida en virtud de la legislación vigente. Se informa que, si no es usted el destinatario o la persona autorizada por el mismo, que la información contenida en este mensaje es reservada y su utilización o divulgación con cualquier fin está prohibida. Si ha recibido este documento por error, le rogamos que nos lo comunique por teléfono, o e-mail y proceda a su destrucción.

Su e-mail nos consta como contacto profesional y/o suscriptor y su utilización tiene como fin facilitarle información legal de interés y/o agilizar la comunicación y prestación de servicios. APEMAR Servicios Profesionales para Redes, S.L. no realiza envíos no solicitados de e-mail o similares sin consentimiento del destinatario, por lo tanto, si no desea recibir más comunicaciones, puede darse de baja de esta base de datos llevando a cabo los siguientes pasos: 1) Presionar "Responder" 2) Eliminar el asunto y en su lugar poner "BAJA" 3) Presionar "Enviar". Así mismo, le informamos que puede ejercer en cualquier momento sus derechos de acceso, rectificación, supresión, oposición, limitación al tratamiento y a la portabilidad de los datos dirigiéndose por escrito, concretando su solicitud y acompañando fotocopia del D.N.I. o de otro documento oficial de identificación personal a APEMAR Servicios Profesionales para Redes, S.L. (C/ Rueda, 42 7ªA – 28011 Madrid).

Por favor tenga en cuenta la conservación del medioambiente antes de imprimir este e-mail. EL MEDIOAMBIENTE ES COSA DE TODOS.