PRODASUR

Consultores en Protección de Datos (RGPD-LOPD)

30 años 1992 2022

edor team ANDALUCÍA

Software y Servicios para Asesorías y Empresas

RGPD-LOPD

Extractos Legales relevantes 2021

DOSSIER RGPD-LOPD 2021

Protección de Datos Personales

PRESENTACIÓN:

El presente "Dossier RGPD y LOPD-GDD" tiene un carácter informativo, y es nuestra pretensión ofrecer una orientación respecto a la aplicación de la normativa de protección de datos. Son numerosas las cuestiones legales que podríamos abordar, siendo solo una mínima parte las seleccionadas.

Ofrecemos extractos sobre el RGPD y LOPD-GDD que son relevantes en el día a día para garantizar con su aplicación el cumplimiento de lo establecido en la normativa vigente y evitar posibles sanciones en materia de protección de datos.

Prodasur Software y Servicios, S.L.L es una empresa especializada en la consultoría sobre protección de datos. Seguimos las pautas marcadas por la AEPD, que nos recuerda que las empresas que tratan datos de carácter personal, deben considerar la protección de datos como un activo diferenciador para sus empresas y de responsabilidad para con sus clientes. Por eso, queremos destacar la importancia de disponer de un proyecto dirigido al cumplimiento de la normativa en materia de protección de datos: La norma nos exige el cumplimiento desde el diseño, antes de iniciar los tratamientos y de forma Proactiva. **Tener el apoyo y asesoramiento de una empresa especializada en protección de datos como es PRODASUR le puede evitar sanciones.** Nunca confíe de los servicios de consultoría de empresas que actúan bajo el famoso coste cero.

Si eres cliente de PRODASUR, aprovecha la promoción **"Plan Amigo"**.

***ver el detalle de la promoción en el folleto adjunto.**

Esperamos contribuir mínimamente en su formación, con el presente dossier que tiene una importancia más documental que noticiosa, quedando a su disposición para cuantas consultas quieras realizarnos.

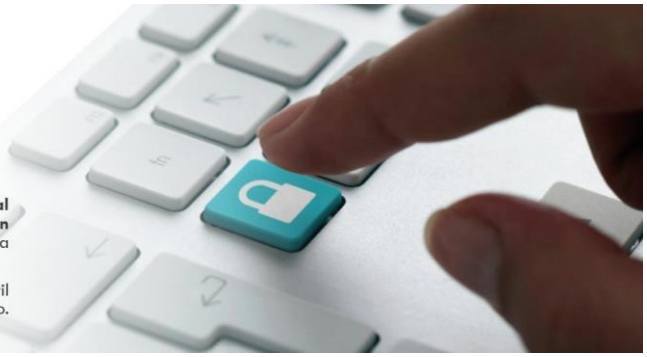
Índice

- **Análisis, tipo de infracciones y sanciones recogidas en el RGPD.**
- **Memoria AEPD 2020. Inspección de datos: Reclamaciones, Resoluciones y Multas por incumplimiento RGPD.**
- **Desafíos tecnológicos en la privacidad. Brechas de datos personales.**
- **Faqs Sobre Brechas de Seguridad.**
- **Listados trimestrales con las 10 multas más altas en España por infracción del RGPD.**

Empresa Colaboradora apep

PRODASUR está registrada en el catálogo de empresas de ciberseguridad de **INCIBE - Instituto Nacional de Ciberseguridad de España,** es miembro de **ApCpD - Asociación Profesional de Consultores en Protección de Datos** (siendo asociado su Administrador, Antonio Isidoro Aguilera Carrillo) y empresa colaboradora de **APEP - Asociación Profesional Española de Privacidad.**

PRODASUR le garantiza el servicio de consultoría contratado mediante una póliza de Responsabilidad Civil que cubre las posibles sanciones que le pudieran ser impuestas debido a deficiencias en el servicio prestado.

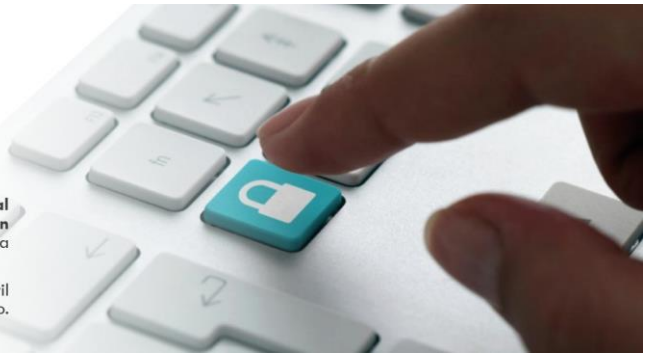


Análisis tipo de infracciones y sanciones recogidas en el RGPD

Empresa Colaboradora apep

PRODASUR está registrada en el catálogo de empresas de ciberseguridad de **INCIBE - Instituto Nacional de Ciberseguridad de España,** es miembro de **ApCpD - Asociación Profesional de Consultores en Protección de Datos** (siendo asociado su Administrador, Antonio Isidoro Aguilera Carrillo) y empresa colaboradora de **APEP - Asociación Profesional Española de Privacidad.**

PRODASUR le garantiza el servicio de consultoría contratado mediante una póliza de Responsabilidad Civil que cubre las posibles sanciones que le pudieran ser impuestas debido a deficiencias en el servicio prestado.



Análisis, Tipos de infracciones por incumplimiento del RGPD y sus correspondientes sanciones

Actualmente, las infracciones por protección de datos se dividen en 3 categorías: muy graves, graves y leves.

Las **Infracciones muy graves del RGPD** son aquellas que suponen un incumplimiento sustancial del tratamiento, tienen un plazo de prescripción de 3 años y están relacionadas con:

- El uso de los datos para una finalidad distinta a la acordada.
- Una omisión del deber de correcta información al afectado.
- La exigencia de un pago por acceder a los datos propios almacenados.
- Una transferencia internacional de información sin garantías.

En este caso se sancionará con multas administrativas que pueden alcanzar los 20 millones de euros o, en el caso de una empresa, un importe equivalente al 4% de la facturación anual.

- Quizá la sanción más conocida sea la multa de la autoridad Francesa de Protección de Datos a Google por un importe de 50 millones de euros al considerar que la información sobre el tratamiento de datos personales a disposición de los usuarios era de difícil acceso y comprensión.
- Un segundo ejemplo viene de Reino Unido, donde la autoridad inglesa (ICO) sancionó a British Airways con 204.000.000 € alegando falta de seguridad en la empresa al sufrir una brecha de seguridad y dejar destapada la información de las tarjetas de crédito de 500.000 clientes.

Las **infracciones graves del RGPD** son las que suponen una vulneración sustancial del tratamiento, tienen un plazo de prescripción de 2 años y están relacionadas con:

- Los datos de un menor recabados sin consentimiento.
- El incumplimiento de nombrar un responsable o encargado de tratamiento de datos.
- La ausencia de medidas técnicas y organizativas necesarias para una protección de datos auténtica.

En este caso se sancionará con multas administrativas que pueden llegar a un importe máximo del 2% de la facturación anual de la empresa.

- Como ejemplo de infracción grave, la AEPD sancionó a Glovo con 25.000 € por incumplimiento del artículo 34 de la LOPD GDD, que recoge de manera clara, sin lugar a interpretaciones, qué empresas deben contar necesariamente con un DPO.

Las **infracciones leves del RGPD** son el resto no contempladas anteriormente, tienen un plazo de prescripción de 1 año. Por ejemplo:

- El incumplimiento de no informar al afectado cuando lo haya solicitado
- La No transparencia de la información
- El incumplimiento por parte del encargado de sus obligaciones.

Asimismo, recoge el RGPD que, en caso de infracción leve, o si la sanción que probablemente se impusiese constituye una carga desproporcionada para una persona física, en lugar de multa podría imponerse un apercibimiento.

- Respecto a este tipo de infracciones existen numerosas sanciones:

-5.000 € a un partido político por infracción del artículo 5.1 b) del RGPD, por enviar una comunicación política sin el consentimiento expreso
-3.000 € a empresa de móviles por infracción del artículo 13 del RGPD, por no constar de Aviso Legal, ni disponer de Política de Privacidad en su página web.

1. Las infracciones más recurrentes de los ejemplos de sanciones del RGPD citadas más arriba provienen de:

- no sustentar los tratamientos llevados a cabo en una correcta base legitimadora
- no tener en cuenta los principios generales
- tener deficiencias en las medidas de seguridad

Esto tiene que servir a las organizaciones a la hora de evaluar su grado de cumplimiento, para evitarnos cuantiosas sanciones y para dotarles de una gran ventaja competitiva, pilar fundamental a la hora de contratar a un proveedor.

2. Hasta ahora España era país de la UE que más procedimientos abría, sin embargo, el importe de las multas estaba muy lejos de las de Italia, Alemania o Francia que superan los 50 millones de euros. Recientemente la AEPD, en un solo mes ha interpuesto las sanciones más elevadas de su historia a BBVA (5 millones de euros) y a Caixabank (6 millones de euros). Esto nos advierte de la posible nueva estrategia que la AEPD ha estrenado y de futuros nuevos castigos millonarios que están por venir.

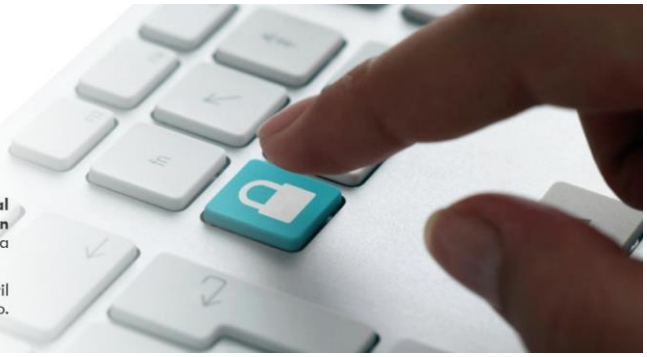
A modo de reflexión, las empresas españolas deberían tomar nota. Si Europa está sancionando con multas muy elevadas y España empieza a seguir su senda, lo lógico sería considerar muy seriamente el cumplimiento del RGPD y ponerse manos a la obra.

No dude en cumplir sus obligaciones en materia de protección de datos con la ayuda de un consultor especializado como PRODASUR

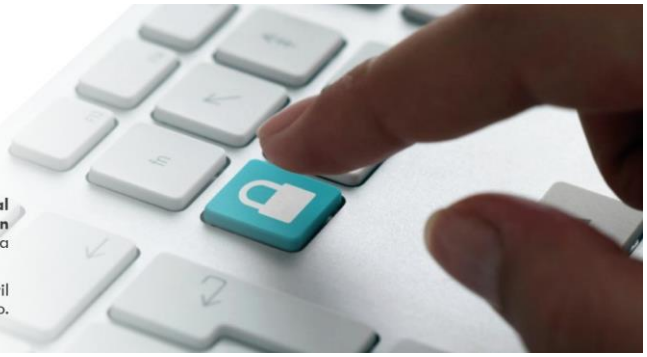
Empresa Colaboradora apep

PRODASUR está registrada en el catálogo de empresas de ciberseguridad de **INCIBE - Instituto Nacional de Ciberseguridad de España**, es miembro de **ApCpD - Asociación Profesional de Consultores en Protección de Datos** (siendo asociado su Administrador, Antonio Isidoro Aguilera Carrillo) y empresa colaboradora de **APEP - Asociación Profesional Española de Privacidad.**

PRODASUR le garantiza el servicio de consultoría contratado mediante una póliza de Responsabilidad Civil que cubre las posibles sanciones que le pudieran ser impuestas debido a deficiencias en el servicio prestado.



Memoria AEPD 2020
Inspección de datos
Reclamaciones, Resoluciones y
Multas por incumplimiento RGPD



Empresa Colaboradora

PRODASUR está registrada en el catálogo de empresas de ciberseguridad de **INCIBE - Instituto Nacional de Ciberseguridad de España,** es miembro de **ApCpD - Asociación Profesional de Consultores en Protección de Datos** (siendo asociado su Administrador, Antonio Isidoro Aguilera Carrillo) y empresa colaboradora de **APEP - Asociación Profesional Española de Privacidad.**

PRODASUR le garantiza el servicio de consultoría contratado mediante una póliza de Responsabilidad Civil que cubre las posibles sanciones que le pudieran ser impuestas debido a deficiencias en el servicio prestado.

Reclamaciones y actuaciones por iniciativa propia.

Las reclamaciones pueden plantearse directamente ante la Agencia, que es la situación más frecuente, aunque también pueden llegar a través de alguna Autoridad de Control de los Estados miembros del Espacio Económico Europeo (EEE). Dentro de los casos en los que se actúa por iniciativa propia hay que destacar las actuaciones de investigación que se realizan, cuando procede, a raíz de las notificaciones de brechas de seguridad en materia de protección de datos personales.

La siguiente tabla muestra estos datos y su comparación con los del ejercicio anterior:

Tipo de entrada	2019	2020	% relativo	Δ% anual
Reclamaciones presentadas en la AEPD	11.590	10.324	91%	-11%
Casos transfronterizos procedentes de otras AC del EEE	790	784	7%	-1%
Propia iniciativa de la AEPD (excl. brechas)	15	26	0%	73%
Notificaciones de brechas de seguridad trasladadas a la SGID	79	81	1%	3%
TOTAL	**12.474**	**11.215**	**100%**	**-9%**

Resoluciones en fase de Análisis de la Reclamación

La primera fase que se lleva a cabo en la tramitación de las reclamaciones es el análisis inicial de cada una de ellas. Comprende su clasificación, la verificación formal de su contenido y el análisis de competencia y de otras causas que afectan a su fundamento y admisibilidad. Es lo que se denomina la fase de Análisis de la reclamación. Esta fase, previa a la tramitación de cualquier procedimiento, finaliza con la inadmisión de la reclamación presentada en torno al 50% de los casos, ligeramente menor que la del año anterior, como muestra la siguiente tabla:

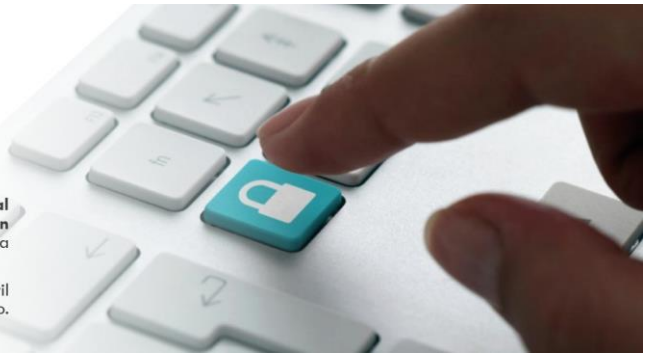
Tipo de resultado	2019	2020	% relativo	Δ% 2018/19
Resoluciones tras la fase de Análisis de la reclamación	**5.897**	**5.671**	**56%**	**-4%**
Inadmisiones a trámite*	5.820	5.522	55%	-5%
Competencia de otras AC nacionales (CGPJ, AC auton.)*	77	149	1%	94%
Resoluciones en otras fases	**5.300**	**4.396**	**44%**	**-17%**
TOTAL	**11.197**	**10.067**	**100%**	**-10%**

** Incluyen reclamaciones relacionadas con el ejercicio de derechos*

Empresa Colaboradora apep

PRODASUR está registrada en el catálogo de empresas de ciberseguridad de **INCIBE - Instituto Nacional de Ciberseguridad de España**, es miembro de **ApCpD - Asociación Profesional de Consultores en Protección de Datos** (siendo asociado su Administrador, Antonio Isidoro Aguilera Carrillo) y empresa colaboradora de **APEP - Asociación Profesional Española de Privacidad.**

PRODASUR le garantiza el servicio de consultoría contratado mediante una póliza de Responsabilidad Civil que cubre las posibles sanciones que le pudieran ser impuestas debido a deficiencias en el servicio prestado.



Tasa de reclamaciones de resoluciones

En 2020 la tasa de reclamaciones resueltas frente a reclamaciones recibidas ha aumentado un 5% respecto al año anterior. Cabe destacar esta mejora de la productividad en la resolución de reclamaciones, sobre todo si se tiene en cuenta la situación de emergencia sanitaria y de confinamiento y el empleo del teletrabajo como modo habitual de prestación de servicios. Este indicador consolida la mejora de productividad que se ha venido observando con la implantación de la política de teletrabajo de la Agencia en los últimos años. En la siguiente tabla se pueden consultar las cifras relacionadas con la tasa de resolución de reclamaciones:

Tasa de resolución de reclamaciones	2019	2020	Δ% anual
Reclamaciones resueltas en el año*	11.182	10.443	-7%
Reclamaciones pendientes de resolver al finalizar el año	3.826	3.709	-3%
Tasa de reclamaciones resueltas vs. recibidas en el año**	96%	101%	5%

** La bajada en número de reclamaciones resueltas está relacionada con la bajada en el número de reclamaciones presentadas ante la AEPD, que se ha reducido un 11%. Como se puede apreciar, se han resuelto porcentualmente un 4% más que las reclamaciones presentadas.*

*** A la vista de los datos obtenidos, se puede comprobar que se ha mejorado un 5% respecto al mismo dato del año anterior, a pesar de la situación de confinamiento y pandemia.*

Resolución en otras fases

Desde la entrada en vigor del RGPD y fundamentalmente de la LOPDGDD, se ha introducido una fase de traslado de la reclamación con la pretensión de resolver con mayor rapidez las reclamaciones, **contando con la intervención de los responsables y de los DPD que hayan designado,** en su caso. Estos traslados pueden conducir al archivo de la reclamación tras la participación del responsable o encargado del tratamiento: adoptando las medidas correctivas para solventar el posible incumplimiento y prevenir que no se produzca en el futuro, o aportando información que contribuya a clarificar la situación, de manera que se pueda determinar que no existe infracción de la normativa de protección de datos. Estos archivos no impiden que la AEPD inicie actuaciones de investigación posteriores para analizar los procedimientos implantados de acuerdo con las competencias que tiene atribuidas. La inclusión de esta nueva fase ha supuesto una gran mejora con relación a los procedimientos de trabajo anteriores. Así, casi el 80% de las resoluciones finalizan tras la fase de traslado, dando solución a los reclamantes de manera más rápida que la que se establecía con la normativa anterior.

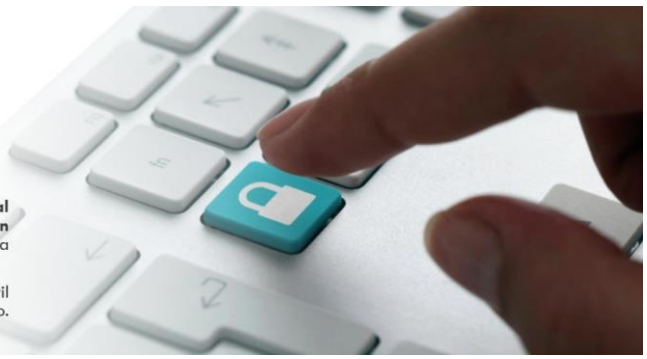
Tipo de resultado	2019	2020	% relativo	Δ% 2018/19
Resoluciones tras Traslado*	**4.197**	**3.405**	**77%**	**-19%**
Respuesta satisfactoria tras traslado al responsable o enc.	2.598	2.157	49%	-17%
Archivo por ser plena competencia de otra AC del EEE	384	414	9%	8%
Archivo provisional actuando como AC interesada en el EEE	571	451	10%	-21%
Archivo por otros motivos tras traslado	644	383	9%	-41%
Resoluciones tras Actuaciones previas de Investigación	**428**	**347**	**8%**	**-19%**
Archivo de actuaciones previas de investigación	428	347	8%	-19%
Resoluciones tras procedimiento de Ejercicio de derechos	**337**	**251**	**6%**	**-26%**
Resuelto en el procedimiento de ejercicio de derechos	337	251	6%	-26%
Resoluciones tras procedimiento Sancionador	**338**	**393**	**9%**	**16%**

** Incluyen reclamaciones relacionadas con el ejercicio de derechos*

Empresa Colaboradora apep

PRODASUR está registrada en el catálogo de empresas de ciberseguridad de **INCIBE - Instituto Nacional de Ciberseguridad de España**, es miembro de **ApCpD - Asociación Profesional de Consultores en Protección de Datos** (siendo asociado su Administrador, Antonio Isidoro Aguilera Carrillo) y empresa colaboradora de **APEP - Asociación Profesional Española de Privacidad.**

PRODASUR le garantiza el servicio de consultoría contratado mediante una póliza de Responsabilidad Civil que cubre las posibles sanciones que le pudieran ser impuestas debido a deficiencias en el servicio prestado.



Tipo de resultado	2019	2020	% relativo	Δ% 2018/19
Resuelto en procedimiento sancionador - Multa	112	172	4%	54%
Resuelto en procedimiento sancionador - Apercibimiento	139	163	4%	17%
Resuelto en procedimiento sancionador - Archivo	87	58	1%	-33%
TOTAL	**5.300**	**4.396**	**100%**	**-17%**

Reclamaciones planteadas con mayor frecuencia

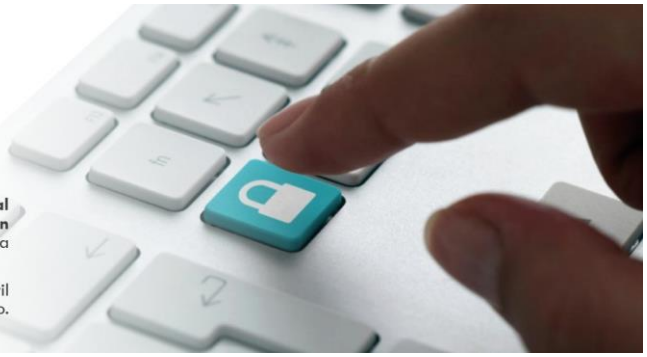
Se muestran las 10 áreas de actividad con mayor número de reclamaciones recibidas en 2020:

Reclamaciones planteadas con mayor frecuencia	2019	2020	% relativo	Δ% 2018/19
TOP 10	**8.826**	**7.751**	**75%**	**-12%**
Servicios de Internet	1.529	1.602	16%	5%
Ficheros de morosidad	1.407	1.510	15%	7%
Videovigilancia	1.415	1.189	12%	-16%
Publicidad (excepto spam)	784	681	7%	-13%
Reclamación de deudas	1.059	656	6%	-38%
Administración pública	776	503	5%	-35%
Entidades financieras/acreedoras	464	473	4%	-6%
Comercios, transporte y hostelería	508	405	4%	-20%
Sanidad	460	388	4%	-16%
Telecomunicaciones	424	380	4%	-10%
Otros	**2.764**	**2.573**	**25%**	**-7%**
TOTAL	**11.590**	**10.324**	**100%**	**-11%**

Áreas más frecuentes en procedimientos sancionadores

Se muestran las 10 áreas de actividad con mayor número de procedimientos sancionadores finalizados en 2020:

Grupo de actividad	2019	2020	% relativo	Δ% anual
TOP 10	**275**	**324**	**82%**	**18%**
Videovigilancia	106	94	24%	-11%
Servicios de Internet	58	73	19%	26%
Administración Pública	15	39	10%	160%
Telecomunicaciones	21	27	7%	29%
Comercios, transporte y hostelería	10	23	6%	130%
Publicidad a través de e-mail o teléfono móvil	32	17	4%	-47%
Comunidades de propietarios	4	14	4%	250%
Contratación fraudulenta	13	14	4%	8%
Asuntos laborales	5	13	3%	160%
Asuntos laborales	11	10	3%	-9%
Otros	**63**	**69**	**18%**	**10%**
TOTAL	**338**	**393**	**100%**	**16%**



Multas

El incremento en la cifra de sanciones impuestas denota que las cifras de gestión vuelven a aproximarse a las existentes antes de la aplicación del RGPD.

Evolución de las multas impuestas	2019	2020	Δ% anual
Número de multas	112	167	49%
Importe total	6.295.923	8.018.800	27%

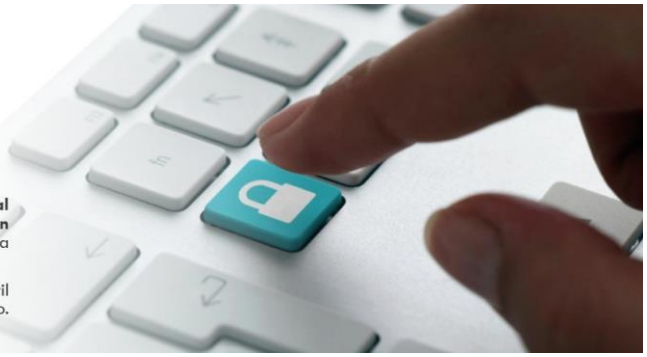
Áreas con mayor importe global de multas

Importe de multas en euros según el sector de actividad	2019	2020	% relativo	Δ% anual
Seis sectores con mayor importe global de sanciones	**1.894.021**	**7.460.900**	**93%**	**294%**
Entidades financieras/acreedoras	45.600	5.045.000	63%	10.964%
Telecomunicaciones	641.000	1.009.000	13%	57%
Contratación fraudulenta	620.620	559.000	7%	-10%
Reclamación de deudas	156.000	242.000	3%	55%
Servicios de Internet	144.300	218.900	3%	52%
Ficheros de Morosidad	286.501	387.000	5%	35%
Otros	**4.401.902**	**557.900**	**7%**	**-87%**
TOTAL	**6.295.923**	**8.018.800**	**100%**	**27%**

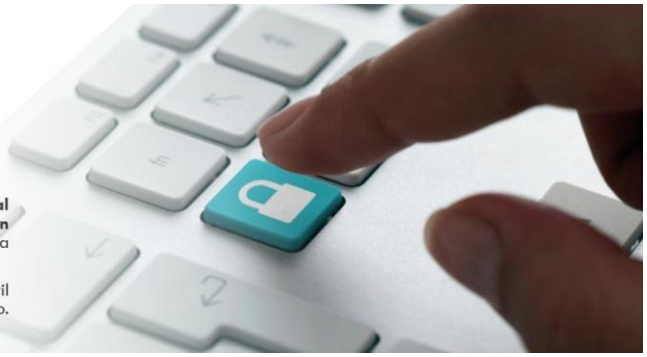
Empresa Colaboradora apep

PRODASUR está registrada en el catálogo de empresas de ciberseguridad de **INCIBE - Instituto Nacional de Ciberseguridad de España,** es miembro de **ApCpD - Asociación Profesional de Consultores en Protección de Datos** (siendo asociado su Administrador, Antonio Isidoro Aguilera Carrillo) y empresa colaboradora de **APEP - Asociación Profesional Española de Privacidad.**

PRODASUR le garantiza el servicio de consultoría contratado mediante una póliza de Responsabilidad Civil que cubre las posibles sanciones que le pudieran ser impuestas debido a deficiencias en el servicio prestado.



Desafíos tecnológicos en la privacidad. Brechas de datos personales



PRODASUR está registrada en el catálogo de empresas de ciberseguridad de **INCIBE - Instituto Nacional de Ciberseguridad de España,** es miembro de **ApCpD - Asociación Profesional de Consultores en Protección de Datos** (siendo asociado su Administrador, Antonio Isidoro Aguilera Carrillo) y empresa colaboradora de **APEP - Asociación Profesional Española de Privacidad.**

PRODASUR le garantiza el servicio de consultoría contratado mediante una póliza de Responsabilidad Civil que cubre las posibles sanciones que le pudieran ser impuestas debido a deficiencias en el servicio prestado.

Brechas de datos personales.

Una **brecha de datos personales** es un incidente de seguridad que afecta a datos de carácter personal, pudiendo producir daños sobre los derechos y libertades de las personas físicas cuyos datos son objeto del tratamiento.

No todos los incidentes de seguridad son necesariamente brechas de datos personales y no solo los ciberincidentes pueden ser brechas de datos personales. A su vez, no toda acción que suponga una vulneración de la normativa de protección de datos puede ser considerada una brecha de datos personales.

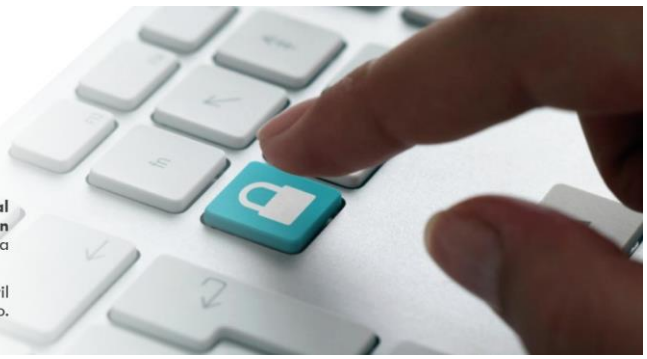
Una brecha de datos personales puede tener una serie de efectos adversos considerables en las personas, susceptibles de ocasionar daños y perjuicios físicos, materiales o inmateriales; por lo que hay que intentar evitarlas y en caso de que sucedan gestionarlas adecuadamente, especialmente cuando puedan poner en riesgo los derechos fundamentales y libertades públicas de las personas.

ANTES de que suceda, el responsable de tratamiento debe estar preparado para esta posibilidad, debe 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 SUCEDE: el responsable de 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.

Además, cuando se sufre una brecha de seguridad se debe recabar una serie de información que será muy útil para decidir qué medidas tomar y qué acciones se emprenderán para cumplir los objetivos anteriores y para valorar la necesidad de notificar a la autoridad de control y afectados.

Medio por el que se ha materializado la brecha, es decir, qué ha ocurrido: se ha perdido un dispositivo con datos personales, se ha producido un robo, se han publicado datos personales por error o se ha enviado a un destinatario equivocado, un ransomware ha cifrado un dispositivo, se ha producido una intrusión no autorizada en un sistema de información con datos personales, un empleado ha sido víctima de phishing, etc.



Origen de la brecha, si ha sido interna o externa y su intencionalidad.

Categorías de datos: si son datos básicos como credenciales o datos de contacto o si bien son categorías especiales como puedan ser datos de salud.

Volumen de datos afectados, tanto en número de registros afectados como en número de personas afectadas.

Categorías de afectados: clientes, empleados, estudiantes, abonados, pacientes, etc. Es importante identificar si se trata de colectivos vulnerables.

Información temporal de la brecha: cuándo se inició, cuándo se ha detectado y cuándo se resolvió o resolverá la brecha de seguridad.

Este apartado, proporcionan una introducción sencilla para iniciarse en la gestión de brechas de datos personales. La Guía para notificación de brechas de datos personales y las Directrices del Comité Europeo de Protección de Datos proporcionan información más completa.

Obligaciones

El Reglamento (UE) 2016/679, General de Protección de Datos establece en sus artículos 33 y 34 la obligación para las organizaciones (públicas y privadas) que actúen como responsables de tratamiento de notificar a la Autoridad de Control competente las brechas de datos personales cuando sea probable que constituyan un riesgo para los derechos y libertades de las personas.

Con carácter general, en el ámbito privado, los responsables del tratamiento afectado por la brecha deberán notificar a la Agencia Española de Protección de Datos:

-Cuando su único establecimiento esté localizado en España.
-Si tienen varios establecimientos en la Unión Europea, únicamente cuando el establecimiento principal esté localizado en España.
-Si no tienen establecimiento principal en la Unión Europea, sólo en el caso de que hayan designado un representante en España.
-Si no tienen establecimiento ni representante en la Unión Europea, en el caso de que la brecha de datos personales cuente con afectados en España.

El responsable de un tratamiento es la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros.

Los responsables de tratamiento con establecimiento principal en otro Estado Miembro de la Unión Europea, o que no tengan un establecimiento en la Unión, pero hayan nombrado un representante en otro Estado Miembro, deberán notificar a la Autoridad de Control de dicho Estado Miembro.

La notificación de una brecha de datos personales a la Autoridad de Control conforme al artículo 33 del RGPD corresponde al responsable del tratamiento. El responsable puede autorizar una persona física, representante o entidad que ejerza su representación para que realice la notificación de la brecha de datos personales ante la Autoridad de Control.

La notificación de brechas de datos personales no es un trámite dirigido a terceros ajenos al responsable de tratamiento, ni a ciudadanos o afectados por una brecha de datos personales.

En el ámbito público, con carácter general las AAPP deben notificar las brechas de datos personales a la Agencia Española de Protección de Datos a excepción del caso de las Comunidades Autónomas de Andalucía, Cataluña y País Vasco, cuando las brechas de datos personales se produzcan en entidades del sector público bajo su competencia, la Autoridad de Control a la que notificar será:

- **En el caso de Cataluña: la Autoridad Catalana de Protección de Datos (https://apdcat.gencat.cat/es/inici/) a través de su sede electrónica.**
- **En el caso del País Vasco: la Agencia Vasca de Protección de Datos mediante el correo electrónico avpd@avpd.eus**
- **En el caso de Andalucía: el Consejo de Transparencia y Protección de Datos de Andalucía a través de su ventanilla electrónica (https://www.ctpdandalucia.es/ventanilla-electronica).**

Si además es probable que la brecha de datos personales entrañe un riesgo alto para los derechos y libertades de las personas físicas, el responsable deberá comunicar la brecha a las personas cuyos datos se hayan visto afectados para que puedan tomar sus propias medidas.

El parámetro determinante para notificar una brecha de datos personales a la Autoridad de Control o comunicarla a los afectados es el nivel de riesgo. No cualquier tipo de riesgo o un riesgo para la organización, sino específicamente el riesgo para los derechos y libertades de las personas físicas afectadas por la brecha.

El plazo para notificar a la Autoridad de Control es de 72 horas desde que la organización es conocedora de la brecha.

Además, existen otras disposiciones normativas que obligan a notificar brechas de seguridad a la AEPD, como el artículo 41 de la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones a los operadores de servicios de comunicaciones electrónicas disponibles al público.

En ambos casos, las notificaciones de brechas de datos personales por parte de organizaciones se realizan de forma telemática mediante el formulario de notificaciones de brechas de datos personales disponible en la Sede Electrónica.

La organización debe reflexionar sobre lo que ha sucedido, cuáles son las consecuencias para las personas cuyos datos se han visto afectados, qué medidas de seguridad técnicas u organizativas podrían haber evitado la brecha y la conveniencia de incorporarlas, y qué acciones tomar para evitar que las personas sufran los daños potenciales y evitar que el incidente se repita.

Lo que subyace a dicha obligación de notificación es un deber más amplio y que insta al responsable a implementar un procedimiento de gestión de incidentes de seguridad que afecten a datos de carácter personal adaptado a las características del tratamiento.

La finalidad última de la notificación y comunicación de brechas de datos personales es la protección efectiva de los derechos fundamentales y libertades de las personas físicas afectadas por la brecha.

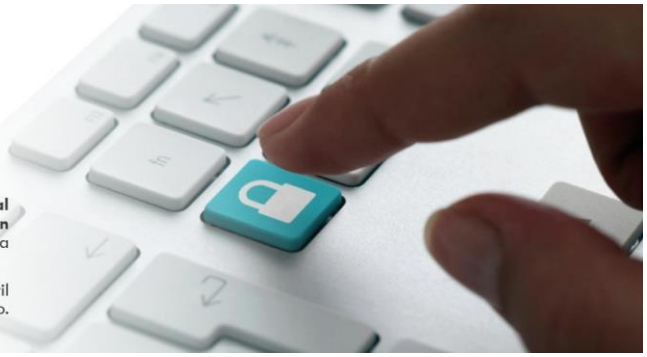
Las organizaciones que sufran una brecha de datos personales deben focalizar sus esfuerzos en evitar y mitigar las posibles consecuencias sobre los derechos fundamentales y libertades públicas de las personas afectadas.

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.

Empresa Colaboradora

PRODASUR está registrada en el catálogo de empresas de ciberseguridad de **INCIBE - Instituto Nacional de Ciberseguridad de España,** es miembro de **ApCpD - Asociación Profesional de Consultores en Protección de Datos** (siendo asociado su Administrador, Antonio Isidoro Aguilera Carrillo) y empresa colaboradora de **APEP - Asociación Profesional Española de Privacidad.**

PRODASUR le garantiza el servicio de consultoría contratado mediante una póliza de Responsabilidad Civil que cubre las posibles sanciones que le pudieran ser impuestas debido a deficiencias en el servicio prestado.



FAQ AEPD
Especial Brechas de Seguridad

Listados trimestrales con las 10 multas más altas en España por infracción del RGPD

Empresa Colaboradora

PRODASUR está registrada en el catálogo de empresas de ciberseguridad de **INCIBE - Instituto Nacional de Ciberseguridad de España,** es miembro de **ApCpD - Asociación Profesional de Consultores en Protección de Datos** (siendo asociado su Administrador, Antonio Isidoro Aguilera Carrillo) y empresa colaboradora de **APEP - Asociación Profesional Española de Privacidad.**

PRODASUR le garantiza el servicio de consultoría contratado mediante una póliza de Responsabilidad Civil que cubre las posibles sanciones que le pudieran ser impuestas debido a deficiencias en el servicio prestado.

FAQS SOBRE BRECHAS DE SEGURIDAD

¿Qué hacer ante pérdidas o robo de un dispositivo portátil?

En cuanto tengamos indicios de la pérdida o robo de un dispositivo debemos empezar a actuar lo antes posible.

En caso de que el dispositivo contenga datos de carácter personal se tendrá que, como mínimo, hacer frente a las obligaciones establecidas en los artículos 33 y 34 del RGPD. En general, el primer paso será poner el incidente en conocimiento del responsable de tratamiento para que se pueda activar el **plan de actuación**. El responsable tiene que saber exactamente qué información contenía el dispositivo y disponer de un plan de actuación para poder gestionar el incidente de seguridad.

En particular, si se trata de una brecha de seguridad que afecta a datos personales se deberá **notificar** la misma a la AEPD cuando exista un riesgo para los derechos y libertades para las personas físicas dentro del plazo de 72h desde que se conoce el incidente. Además, se deberá comunicar a los afectados cuando este riesgo sea alto.

La valoración de estas circunstancias y la decisión sobre notificar a la AEPD y a los afectados corresponde al responsable de tratamiento.

En general, para dispositivos de almacenamiento extraíbles, siempre que los dispositivos estén cifrados con un algoritmo criptográficamente fuerte, la clave de cifrado sea robusta y no se haya visto comprometida, y se disponga de una copia de seguridad de los datos, se podría considerar que la confidencialidad e integridad de los datos no están comprometidas y por tanto no es necesario notificar la brecha a la AEPD ni a los afectados, siempre y cuando el riesgo principal derive de la falta de disponibilidad de dicha información.

Para el caso de dispositivos con sistema operativo, como son teléfonos inteligentes, tabletas y ordenadores portátiles, habrá que considerar además si los mecanismos y las credenciales de autentificación de usuarios en el sistema operativo, o patrón/clave de desbloqueo en caso de teléfonos inteligentes y tabletas, son suficientemente robustas y no han sido comprometidas para tomar la decisión de notificar la brecha de seguridad.
En cualquier caso, los detalles de la brecha de seguridad deberán quedar registrados en el registro de incidentes de seguridad de la organización.

¿En qué contribuye la comunicación a los interesados?

La obligación de comunicar a los interesados establecida en el RGPD aporta un valor añadido de transparencia a las personas cuyos datos son objeto de los tratamientos, permitiendo conocer si sus datos han podido ser revelados a terceros, o han dejado de estar disponibles temporal o permanentemente. Servicios ampliamente usados como **monitor de Firefox** o **Havelbeenpwned** ponen de manifiesto la creciente preocupación de las personas por la privacidad y la demanda de transparencia en los tratamientos.

La opacidad, con la que en ocasiones se han abordado las brechas de seguridad por parte de algunas organizaciones, ha podido causar un riesgo muy elevado a los afectados al no haber sido informados y no haber podido adoptar las medidas necesarias para protegerse.

La obligación de comunicación a los interesados, además, tiene un efecto colateral muy positivo para las organizaciones, y es el servir de apoyo a aquellas políticas internas que fomentan la implantación de modelos de gestión y gobernanza de los datos efectivos y diligentes. De esta forma, el responsable obtiene un beneficio directo, ya no sólo por el cumplimiento de las obligaciones legales. El impacto sobre la **reputación** ha pasado a ser una de las mayores preocupaciones para las entidades y esta obligación permite mantener la relación de confianza que los interesados han depositado en ellas.

Las más veinte millones de comunicaciones a los interesados ejecutadas de forma proactiva por parte de responsables de tratamiento establecidos en España, según la información de las notificaciones de brechas de seguridad a la AEPD, y aproximadamente las 12.000 comunicaciones a interesados ordenadas por esta Agencia en las casi 1.500 notificaciones de brechas de seguridad recibidas en 2019, ponen de manifiesto que esta herramienta es un instrumento eficaz para la protección de los derechos y libertades de los ciudadanos.

Brechas de seguridad: ¿Cómo protegerte ante un ransomware?

Un 10% de las **notificaciones de brechas de seguridad recibidas** en la AEPD durante 2018 desde el 25 de mayo de 2018 (fecha de aplicación del RGPD) indican que el motivo de la brecha es el cifrado de equipos mediante algún tipo de **ransomware**, y en ocasiones el vector de ataque es el acceso mediante servicios de escritorio remoto.

Por eso, queremos mostrar el **caso concreto** de uno de los tipos de brecha de seguridad que se ha notificado a la AEPD con **especial incidencia en el sector privado** y dar recomendaciones para reducir el riesgo de sufrir una brecha de este tipo.

Es habitual que usuarios de pymes y grandes empresas necesiten tener acceso desde internet a un servidor o cualquier otro equipo de su red para ejecutar determinadas aplicaciones, realizar tareas de mantenimiento o de soporte. A veces, también necesitan proporcionar acceso a otras organizaciones que les prestan un servicio determinado.

Desde Windows NT 4.0, Microsoft incorpora el protocolo de escritorio remoto (Remote Desktop Protocol - RDP) que proporciona acceso remoto a la interfaz gráfica del equipo y permite resolver la necesidad anteriormente descrita. Es un servicio habitualmente usado en servidores que tienen instalado el sistema operativo Windows, aunque también se utiliza en otros sistemas operativos, para evitar tener que desplazarse físicamente donde se encuentra el equipo.

Conociendo la dirección de internet del equipo (IP o nombre DNS) y con unas credenciales válidas, se puede acceder a la interfaz gráfica del equipo que tenga habilitado el servicio y que por defecto utiliza el puerto de comunicaciones 3389 TCP.

Una práctica no recomendada, pero muy habitual por su sencillez de implementación, es redirigir los puertos en el router del proveedor de internet para permitir ese acceso remoto a algún equipo de la organización. Al permitir esta conectividad se está exponiendo un servicio normalmente protegido sólo por usuario y contraseña.

En un entorno controlado de pruebas en el que se simulen las condiciones anteriormente descritas, se puede comprobar que en menos de una hora la exposición del servicio es detectada y se realizan cientos de ataques por fuerza bruta.

La forma en la que se produce este ataque es tradicionalmente mediante phishing, en el que a través del **envío de un correo suplantando al emisor** se remite un malware como fichero adjunto que acabará cifrando los archivos del equipo. En los últimos años han cobrado una **especial importancia los ataques de tipo ransomware** en los que se busca cifrar información para posteriormente solicitar un rescate por la contraseña de descifrado. Aunque parezca una actividad en descenso, sigue siendo una gran amenaza a tener en cuenta especialmente en el caso de las pymes, uno de sus grandes objetivos.

Pero en la actualidad también se utilizan otras técnicas, como por ejemplo algunos ransomware como Crysis/Dharma o Matrix cuyo vector de entrada es precisamente el protocolo de escritorio remoto. Utilizando buscadores como **SHODAN**, encuentran equipos accesibles que tengan contraseñas débiles y usuarios por defecto habilitados como "invitado", "backup", etc. Una vez acceden al equipo proceden a deshabilitar sistemas de protección como **instantáneas de volumen o puntos de restauración** y cifran toda la información del sistema pidiendo un rescate para entregar la contraseña de descifrado.

Cuando se sufre un ataque de este tipo se suele pensar únicamente en que se ha sufrido una **brecha de disponibilidad** hasta que se consigue recuperar la información, habitualmente desde las copias de respaldo, si se dispone de ellas. Pero no siempre se tiene en cuenta que han sido comprometidos diferentes cuentas de usuario que pueden pertenecer a un dominio, que se ha podido acceder a otros equipos de la organización y conseguir credenciales diferentes a las del servidor afectado, además se desconoce si el malware ha podido enviar alguna información almacenada en nuestros sistemas hacia el exterior.

La primera medida preventiva a llevar a cabo para evitar estos ataques es **no exponer los servicios de escritorio remoto directamente a internet** mediante la redirección de puertos, al considerarse una práctica insegura.

Sería recomendable establecer al menos un servicio como **Remote Desktop Gateway**, o mejor aún implementar un sistema de **red privada virtual** (Virtual Private Network - VPN) en la que se consoliden los accesos desde el exterior. De esta manera tendremos **un único sistema expuesto que es el que deberemos vigilar con mayor diligencia**. Además, no debemos olvidar recomendaciones básicas como deshabilitar cuentas de usuario innecesarias o credenciales simples, tener los sistemas actualizados e implementar sistemas de doble autenticación.

Como medida correctiva, disponer de copias de seguridad de los datos es la medida más eficaz.

Para mayor información sobre medidas preventivas y cómo actuar ante un ransomware que haya cifrado tus dispositivos, desde la Agencia Española de Protección de Datos te recomendamos consultar la **guía sobre Ransomware** publicada por INCIBE, el **informe de buenas prácticas** del CCN-CERT y las **recomendaciones de medidas de seguridad ante ransomware** también del CCN-CERT .

Listados trimestrales con las 10 multas más altas en España por infracción del RGPD

Em cada ranking trimestral, no ha tenido en consideración los descuentos aplicados en su caso por el artículo 85 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas por reconocimiento de responsabilidad y por el pago voluntario de la multa.

En el caso de multas con la misma cuantía, se ha dado preferencia a los procedimientos sancionadores más antiguos.

1er Trimestre 2021

Multa n.° 1: 8.150.000 euros
Reclamado: Vodafone España, S.A.U.
Procedimiento Sancionador: PS/00059/2020
Infracción: Artículo 28 del RGPD en relación con el artículo 24 del RGPD. Artículo 44 del RGPD. Artículo 21 de la LSSICE. Artículo 48.1.b) de la LGT en relación con el artículo 21 del RGPD y artículo 23 de la LOPDGDD
Fecha de publicación: 11 de Marzo de 2021
Motivo de la reclamación: Durante meses, el reclamado realizó directa e indirectamente (a través de agentes comerciales) una actividad de mercadotecnia y prospección comercial mediante llamadas telefónicas y envío de e-mails y SMS que infringió distintas normas legales.

Multa n.° 2: 6.000.000 euros
Reclamado: CaixaBank, S.A
Procedimiento Sancionador: PS/00477/2019
Infracción: Artículos 13 y 14 del RGPD. Artículo 6 en relación con el artículo 7 del RGPD y artículo 6 de la LOPDGDD
Fecha de publicación: 13 de Enero de 2021
Motivo de la reclamación: Los distintos contratos y la política de privacidad utilizados por el reclamado para la recogida y tratamiento de datos personales incumplen el derecho de información de los interesados. Asimismo, las bases jurídicas del consentimiento y el interés legítimo utilizadas por el reclamado para diversos tratamientos de datos no son válidas.

Multa n.° 3: 5.000.000 euros
Reclamado: Banco Bilbao Vizcaya Argentaria, S.A.
Procedimiento Sancionador: PS/00070/2019
Infracción: Artículos 6, 13 y 14 del RGPD
Fecha de publicación: 13 de Enero de 2021
Motivo de la reclamación: El formulario de recogida de datos personales del reclamado incumplió el derecho de información de los interesados. Asimismo, las bases legales empleadas por el reclamado para el tratamiento de datos (el consentimiento y el legítimo interés), no eran válidas.

Multa n.° 4: 600.000 euros
Reclamado: Air Europa Líneas Aéreas, S.A.
Procedimiento Sancionador: PS/00179/2020
Infracción: Artículos 32.1 y 33 del RGP
Fecha de publicación: 18 de Marzo de 2021
Motivo de la reclamación: El reclamado tuvo conocimiento de una brecha de seguridad de datos personales el 17 de octubre de 2018. Sin embargo, el reclamado comunicó a la AEPD dicha brecha de seguridad el 28 de noviembre de 2018, infringiendo el plazo de 72 horas establecido por el RGPD para comunicar una brecha de seguridad a la autoridad de control. Asimismo, las medidas de seguridad técnicas y organizativas implantadas por el reclamado no eran apropiadas para garantizar un nivel de seguridad adecuado al riesgo e impedir un acceso no autorizado a los datos de los clientes.

Multa n.° 5: 250.000 euros
Reclamado: Liga Nacional de Fútbol Profesional
Procedimiento Sancionador: PS/00326/2018
Infracción: Artículo 5.1.a) del RGPD
Fecha de publicación: 20 de agosto de 2019
Motivo de la reclamación: La creación por el reclamado de una aplicación móvil que podía captar de forma indiscriminada sonido ambiente del lugar donde se encontrara el usuario. Esto podía implicar la captación de conversaciones con terceros que podrían desvelar datos personales.

Multa n.º 6: 200.000 euros
Reclamado: Vodafone España, S.A.U.
Procedimiento Sancionador: PS/00430/2020
Infracción: Artículo 6.1 del RGPD
Fecha de publicación: 11 de Febrero de 2021
Motivo de la reclamación: El reclamante manifiesta que sigue recibiendo correos electrónicos del reclamado a pesar de haber sido sancionado por estos mismos hechos en los procedimientos sancionadores PS/00278/2019 y PS/00186/2020.

Multa n.º 7: 200.000 euros
Reclamado: I-De Redes Eléctricas Inteligentes, S.A.U. (I-De)
Procedimiento Sancionador: PS/00197/2020
Infracción: Artículos 5.1.b) y c) y 6.1.b) del RGPD
Fecha de publicación: 1 de marzo de 2021
Motivo de la reclamación: El reclamado envió cartas informativas de presuntos incumplimientos contractuales de la empresa comercializadora (la reclamante), a los consumidores finales, rogándoles además que se pusieran en contacto con la entidad comercializadora para que ésta "procediera a la subsanación del problema". Es decir, el reclamado realizó un tratamiento de datos personales de los clientes del reclamante sin estar legitimado para ello, y para una finalidad distinta de la que tenía autorización.

Multa n.º 8: 150.000 euros
Reclamado: Xfera Móviles, S.A.
Procedimiento Sancionador: PS/00448/2020
Infracción: Artículos 5.1.f), 17 y 32 del RGPD y artículo 21 de la LSSI
Fecha de publicación: 9 de Marzo de 2021
Motivo de la reclamación: El reclamado continuó enviando SMS publicitarios al teléfono del reclamante (más de 60 SMS en 30 días) sin su consentimiento, y pese a que el reclamante había ejercido el derecho de supresión de sus datos personales. El reclamado también envió al reclamante SMS con información confidencial de terceras personas. Esta información permitió al reclamante acceder a datos personales y facturas de un tercero ajeno a él.

Multa n.° 9: 120.000 euros
Reclamado: Vodafone España, S.A.U.
Procedimiento Sancionador: PS/00144/2019
Infracción: Artículo 6.1 del RGPD
Fecha de publicación: 19 de septiembre de 2019
Motivo de la reclamación: El reclamado tenía contratado a nombre del reclamante varios servicios los cuales este no había contratado.

Multa n.° 10: 120.000 euros
Reclamado: Vodafone España, S.A.U.
Procedimiento Sancionador: PS/00235/2019
Infracción: Artículos 6.1.a) y 5.1.a) del RGPD
Fecha de publicación: 27 de febrero de 2020
Motivo de la reclamación: La recepción del hijo menor de edad del reclamante de una carta del reclamado en la que le comunicaba que había contraído con ellos una deuda de 93,77 euros y que en el caso de impago se procedería a su inclusión en una lista de morosos.

Conclusión:
Seis de las infracciones del ranking están relacionadas con la falta de licitud del tratamiento de datos personales (Art. 6 del RGPD).

Las sanciones a los dos bancos están relacionadas con el incumplimiento del deber de información (Arts. 13 y 14 del RGPD), que da a su vez lugar a la infracción de la licitud del tratamiento (Art. 6 del RGPD) en los casos en los que se utiliza el consentimiento como base legal para el tratamiento, al estar el consentimiento del interesado viciado por la falta de información.

Las empresas del sector de telecomunicaciones representan el 50% de las multas del ranking.

Las diez multas del actual ranking suman un total de 20.790.000 euros.

Empresa Colaboradora apep

PRODASUR está registrada en el catálogo de empresas de ciberseguridad de **INCIBE - Instituto Nacional de Ciberseguridad de España**, es miembro de **ApCpD - Asociación Profesional de Consultores en Protección de Datos** (siendo asociado su Administrador, Antonio Isidoro Aguilera Carrillo) y empresa colaboradora de **APEP - Asociación Profesional Española de Privacidad.**

PRODASUR le garantiza el servicio de consultoría contratado mediante una póliza de Responsabilidad Civil que cubre las posibles sanciones que le pudieran ser impuestas debido a deficiencias en el servicio prestado.

2º Trimestre 2021

Multa n.º 1: 8.150.000 euros
Reclamado: Vodafone España, S.A.U.
Procedimiento Sancionador: PS/00059/2020
Infracción: Artículo 28 del RGPD en relación con el artículo 24 del RGPD. Artículo 44 del RGPD. Artículo 21 de la LSSICE. Artículo 48.1.b) de la LGT en relación con el artículo 21 del RGPD y artículo 23 de la LOPDGDD
Fecha de publicación: 11 de Marzo de 2021
Motivo de la reclamación: Durante meses, el reclamado realizó directa e indirectamente (a través de agentes comerciales) una actividad de mercadotecnia y prospección comercial mediante llamadas telefónicas y envío de e-mails y SMS que infringió distintas normas legales.

Multa n.º 2: 6.000.000 euros
Reclamado: CaixaBank, S.A
Procedimiento Sancionador: PS/00477/2019
Infracción: Artículos 13 y 14 del RGPD. Artículo 6 en relación con el artículo 7 del RGPD y artículo 6 de la LOPDGDD
Fecha de publicación: 13 de Enero de 2021
Motivo de la reclamación: Los distintos contratos y la política de privacidad utilizados por el reclamado para la recogida y tratamiento de datos personales incumplen el derecho de información de los interesados. Asimismo, las bases jurídicas del consentimiento y el interés legítimo utilizadas por el reclamado para diversos tratamientos de datos no son válidas.

Multa n.º 3: 5.000.000 euros
Reclamado: Banco Bilbao Vizcaya Argentaria, S.A.
Procedimiento Sancionador: PS/00070/2019
Infracción: Artículos 6, 13 y 14 del RGPD
Fecha de publicación: 13 de Enero de 2021
Motivo de la reclamación: El formulario de recogida de datos personales del reclamado incumplió el derecho de información de los interesados. Asimismo, las bases legales empleadas por el reclamado para el tratamiento de datos (el consentimiento y el legítimo interés), no eran válidas.

Empresa Colaboradora apep

PRODASUR está registrada en el catálogo de empresas de ciberseguridad de **INCIBE - Instituto Nacional de Ciberseguridad de España**, es miembro de **ApCpD - Asociación Profesional de Consultores en Protección de Datos** (siendo asociado su Administrador, Antonio Isidoro Aguilera Carrillo) y empresa colaboradora de **APEP - Asociación Profesional Española de Privacidad.**

PRODASUR le garantiza el servicio de consultoría contratado mediante una póliza de Responsabilidad Civil que cubre las posibles sanciones que le pudieran ser impuestas debido a deficiencias en el servicio prestado.

Multa n.° 4: 1.500.000 euros
Reclamado: EDP Energía, S.A.U
Procedimiento Sancionador: PS/00236/2020
Infracción: Artículo 25 y 13 del RGPD
Fecha de publicación: 4 de mayo de 2021
Motivo de la reclamación: El reclamado carecía de mecanismos para acreditar la representación de quien efectuaba una contratación en nombre de un tercero, o para acreditar la existencia de autorización por parte del representante para prestar consentimientos en nombre del representado para otros tratamientos de datos. Asimismo, la información aportada por el Reclamado tanto telefónicamente como en sus condiciones generales no era suficientemente transparente. En particular, la información sobre el responsable del tratamiento; las finalidades y bases legitimadoras de los tratamientos de datos; los tratamientos basados en el consentimiento del interesado; y el derecho de oposición del interesado.

Multa n.° 5: 1.500.000 euros
Reclamado: EDP Comercializadora, S.A.U.
Procedimiento Sancionador: PS/00037/2020
Infracción: Artículo 25 y 13 del RGPD
Fecha de publicación: 4 de mayo de 2021
Motivo de la reclamación: El reclamado carecía de mecanismos para acreditar la representación de quien efectuaba una contratación en nombre de un tercero, o para acreditar la existencia de autorización por parte del representante para prestar consentimientos en nombre del representado para otros tratamientos de datos. Asimismo, la información aportada por el Reclamado tanto telefónicamente como en sus condiciones generales no era suficientemente transparente. En particular, la información sobre el responsable del tratamiento; las finalidades y bases legitimadoras de los tratamientos de datos; los tratamientos basados en el consentimiento del interesado; y el derecho de oposición del interesado.

Multa n.° 6: 1.000.000 euros
Reclamado: Equifax Ibérica, S.L.
Procedimiento Sancionador: PS/00240/2019
Infracción: Artículo 5.1.b) del RGPD. Artículo 6.1, en relación con el artículo 5.1.a) del RGPD. Artículos 5.1.c), 5.1.d) y 14 del RGPD.
Fecha de publicación: 26 de Abril de 2021

Motivo de la reclamación: El reclamado trató datos personales recabados de anuncios publicados por las administraciones públicas para un fin incompatible con el de los anuncios. Concretamente, la finalidad de los anuncios publicados por las administraciones era la de notificar a los interesados de que estos eran parte en un procedimiento con la administración para garantizar su derecho constitucional a la tutela judicial. La finalidad para la cual el reclamado trató estos datos personales fue la de obtener un beneficio económico prestando un servicio a terceros relacionado con la información sobre la solvencia de los afectados.

Multa n.° 7: 600.000 euros
Reclamado: Air Europa Líneas Aéreas, S.A.
Procedimiento Sancionador: PS/00179/2020
Infracción: Artículos 32.1 y 33 del RGPD
Fecha de publicación: 18 de Marzo de 2021
Motivo de la reclamación: El reclamado tuvo conocimiento de una brecha de seguridad de datos personales el 17 de octubre de 2018. Sin embargo, el reclamado comunicó a la AEPD dicha brecha de seguridad el 28 de noviembre de 2018, infringiendo el plazo de 72 horas establecido por el RGPD para comunicar una brecha de seguridad a la autoridad de control. Asimismo, las medidas de seguridad técnicas y organizativas implantadas por el reclamado no eran apropiadas para garantizar un nivel de seguridad adecuado al riesgo e impedir un acceso no autorizado a los datos de los clientes.

Multa n.° 8: 250.000 euros
Reclamado: Liga Nacional de Fútbol Profesional
Procedimiento Sancionador: PS/00326/2018
Infracción: Artículo 5.1.a) del RGPD
Fecha de publicación: 20 de agosto de 2019
Motivo de la reclamación: La creación por el reclamado de una aplicación móvil que podía captar de forma indiscriminada sonido ambiente del lugar donde se encontrara el usuario. Esto podía implicar la captación de conversaciones con terceros que podrían desvelar datos personales.

Multa n.° 9: 200.000 euros
Reclamado: Vodafone España, S.A.U.
Procedimiento Sancionador: PS/00430/2020
Infracción: Artículo 6.1 del RGPD
Fecha de publicación: 11 de Febrero de 2021
Motivo de la reclamación: El reclamante manifiesta que sigue recibiendo correos electrónicos del reclamado a pesar de haber sido sancionado por estos mismos hechos en los procedimientos sancionadores PS/00278/2019 y PS/00186/2020.

Multa n.° 10: 200.000 euros
Reclamado: I-De Redes Eléctricas Inteligentes, S.A.U. (I-De)
Procedimiento Sancionador: PS/00197/2020
Infracción: Artículos 5.1.b) y c) y 6.1.b) del RGPD
Fecha de publicación: 1 de marzo de 2021
Motivo de la reclamación: El reclamado envió cartas informativas de presuntos incumplimientos contractuales de la empresa comercializadora (la reclamante), a los consumidores finales, rogándoles además que se pusieran en contacto con la entidad comercializadora para que ésta "procediera a la subsanación del problema". Es decir, el reclamado realizó un tratamiento de datos personales de los clientes del reclamante sin estar legitimado para ello, y para una finalidad distinta de la que tenía autorización.

Conclusión:
Cuatro de las infracciones del ranking están relacionadas con la falta de información al interesado (Art. 13 del RGPD).

Cinco de las infracciones del ranking están relacionadas con la falta de licitud del tratamiento (Art. 6 del RGPD).

Las empresas sancionadas son de industrias más diversas que en los anteriores rankings: el 30% pertenecen al sector de energía, el

20% son entidades financieras y un 20% pertenecen al sector de telecomunicaciones

Las diez multas del actual ranking suman un total de 24.400.000 euros.

Empresa Colaboradora apep

PRODASUR está registrada en el catálogo de empresas de ciberseguridad de **INCIBE - Instituto Nacional de Ciberseguridad de España**, es miembro de **ApCpD - Asociación Profesional de Consultores en Protección de Datos** (siendo asociado su Administrador, Antonio Isidoro Aguilera Carrillo) y empresa colaboradora de **APEP - Asociación Profesional Española de Privacidad.**

PRODASUR le garantiza el servicio de consultoría contratado mediante una póliza de Responsabilidad Civil que cubre las posibles sanciones que le pudieran ser impuestas debido a deficiencias en el servicio prestado.

3er Trimestre 2021

Multa n.° 1: 250.000 euros
Reclamado: Liga Nacional de Fútbol Profesional
Procedimiento Sancionador: PS/00326/2018
Infracción: Artículo 5.1.a) del RGPD
Fecha de publicación: 20 de agosto de 2019
Motivo de la reclamación: La creación por el reclamado de una aplicación móvil que podía captar de forma indiscriminada sonido ambiente del lugar donde se encontrara el usuario. Esto podía implicar la captación de conversaciones con terceros que podrían desvelar datos personales.

Multa n.° 2: 120.000 euros
Reclamado: Vodafone España, S.A.U.
Procedimiento Sancionador: PS/00144/2019
Infracción: Artículo 6.1 del RGPD
Fecha de publicación: 19 de septiembre de 2019
Motivo de la reclamación: El reclamado tenía contratado a nombre del reclamante varios servicios los cuales este no había contratado.

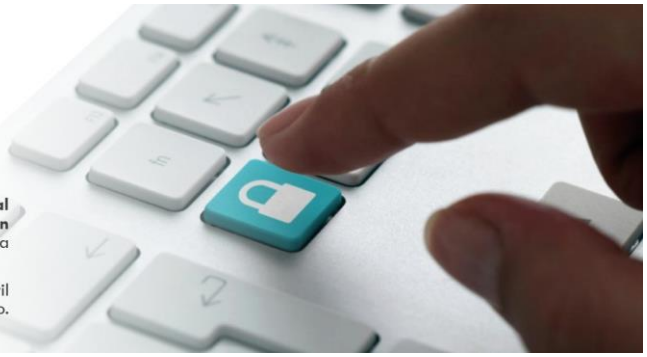
Multa n.° 3: 120.000 euros
Reclamado: Vodafone España, S.A.U.
Procedimiento Sancionador: PS/00235/2019
Infracción: Artículos 6.1.a) y 5.1.a) del RGPD
Fecha de publicación: 27 de febrero de 2020
Motivo de la reclamación: La recepción del hijo menor de edad del reclamante de una carta del reclamado en la que le comunicaba que había contraído con ellos una deuda de 93,77 euros y que en el caso de impago se procedería a su inclusión en una lista de morosos.

Multa n.° 4: 100.000 euros
Reclamado: Endesa Energía XXI, S.L.U.
Procedimiento Sancionador: PS/00074/2019
Infracción: Artículo 5.1.f) del RGPD
Fecha de publicación: 22 de mayo de 2019

Catálogo de Empresas y Soluciones de Ciberseguridad · Empresa Registrada incibe_ · ApCpD · Empresa Colaboradora apep

PRODASUR está registrada en el catálogo de empresas de ciberseguridad de **INCIBE - Instituto Nacional de Ciberseguridad de España**, es miembro de **ApCpD - Asociación Profesional de Consultores en Protección de Datos** (siendo asociado su Administrador, Antonio Isidoro Aguilera Carrillo) y empresa colaboradora de **APEP - Asociación Profesional Española de Privacidad.**

PRODASUR le garantiza el servicio de consultoría contratado mediante una póliza de Responsabilidad Civil que cubre las posibles sanciones que le pudieran ser impuestas debido a deficiencias en el servicio prestado.



Motivo de la reclamación: Un tercero contactó con el reclamado para efectuar un cambio en el contrato de suministro eléctrico en el que la reclamante figuraba como apoderada. Siguiendo las instrucciones del tercero, el reclamado modificó la ficha del contrato de la reclamante eliminando sus datos e incluyendo en su lugar los datos del tercero. Dicho tercero había sido condenado por delito de coacciones en el orden familiar, imponiéndosele orden de alejamiento de la reclamante, su domicilio o trabajo durante dos años.

Multa n.° 5: 100.000 euros
Reclamado: Vodafone España, S.A.U.
Procedimiento Sancionador: PS/00405/2019
Infracción: Artículo 6.1 del RGPD
Fecha de publicación: 3 de febrero 2020
Motivo de la reclamación: El reclamante recibió un e-mail del reclamado informándole de la facturación de una línea que el reclamante manifiesta no haber contratado.

Multa n.° 6: 100.000 euros
Reclamado: Vodafone España, S.A.U.
Procedimiento Sancionador: PS/00186/2020
Infracción: Artículo 6.1 del RGPD
Fecha de publicación: 1 de septiembre de 2020
Motivo de la reclamación: El reclamante ha vuelto a recibir en su dirección de correo electrónico un aviso de disponibilidad de factura electrónica procedente del reclamado, lo cual constituye una reincidencia de los hechos sancionados por la AEPD en el procedimiento sancionador PS/00278/2019.

Multa n.° 7: 80.000 euros
Reclamado: Orange Espagne, S.A.U.
Procedimiento Sancionador: PS/00452/2019
Infracción: Artículo 6.1 del RGPD
Fecha de publicación: 20 de julio 2020
Motivo de la reclamación: Los datos del reclamante han sido utilizados para la contratación fraudulenta de seis líneas telefónicas con el reclamado sin su consentimiento. Asimismo, a consecuencia de las distintas deudas contraídas con el reclamado, sus datos personales han sido incluidos en el fichero de solvencia patrimonial ASNEF.

Multa n.° 8: 75.000 euros
Reclamado: Vodafone España, S.A.U.
Procedimiento Sancionador: PS/00277/2019
Infracción: Artículo 5.1.f) del RGPD
Fecha de publicación: 14 de noviembre de 2019
Motivo de la reclamación: El reclamado carga los servicios contratados por el reclamante en una cuenta distinta a la facilitada por éste: la de su hijo, el cual no es cliente del reclamado. Asimismo, el reclamante manifiesta que la dirección postal que obra en los ficheros del reclamando (correspondiente a un local de su propiedad) no es la que se facilitó en el momento de la contratación.

Multa n.° 9: 75.000 euros
Reclamado: Curenergia Comercializadora de Último Recurso, S.A.U.
Procedimiento Sancionador: PS/00140/2019
Infracción: Artículo 6.1.a) del RGPD
Fecha de publicación: 4 de diciembre de 2019
Motivo de la reclamación: El reclamado ha utilizado los datos personales de la reclamante, una antigua cliente, sin su consentimiento para realizar una contratación y alta fraudulenta.

Multa n.º 10: 75.000 euros
Reclamado: EDP Comercializadora, S.A.U.
Procedimiento Sancionador: PS/00025/2019
Infracción: Artículo 6.1 del RGPD
Fecha de publicación: 7 de enero 2020
Motivo de la reclamación: El reclamado ha tratado los datos personales del reclamante (nombre, apellidos, NIF, domicilio y número de teléfono móvil) sin su consentimiento, al encontrarse dichos datos vinculados a un contrato de gas al que el reclamante es ajeno.

Conclusión:
*Siete de las infracciones falta licitud del tratamiento de datos personales (Art. 6.1 del RGPD).

Dos de las infracciones del ranking surgen por el incumplimiento del Principio de Confidencialidad (Art. 5.1.f) del RGPD).

Dos de las infracciones son por el incumplimiento del Principio de Licitud, Lealtad y Transparencia (Art. 5.1.a) del RGPD).

Empresas sector de telecomunicaciones representan el 60% de las multas del ranking.

Las diez multas del ranking suman un total de 1.095.000 euros.