EVALUACIÓN DE IMPACTO

ASOCIACIÓN ESPAÑOLA PARA LA PRIVACIDAD DIGITAL (ASOCIACIONEPD)

1. Datos Generales **3**

Datos del Responsable: 3

Datos del Representante: 3

Datos del Delegado de Protección de Datos: 4

2. Introducción **4**

3. Evaluación de la necesidad y proporcionalidad de las operaciones de tratamiento **5**

4. Evaluación de los riesgos **6**

5. Medidas previstas para afrontar los riesgos **8**

6. Necesidad de efectuar la consulta previa **8**

Objeto de la consulta 8

Obligación de realizar una consulta previa. 8

7. Consultas a los Colectivos Afectados **9**

8. Ciclo de vida del dato personal **9**

NOTAS: **11**

1.https://firebase.google.com/terms **11**

2.https://firebase.google.com/terms/data-processing-terms **11**

3.https://firebase.google.com/terms/crashlytics-app-distribution-data-processing-term/ **11**

4.https://cloud.google.com/terms/data-processing-terms **12**

9. GESTIÓN DE BRECHAS DE SEGURIDAD **13**

Tipologías de brechas de seguridad 13

Definiciones básicas de conceptos relacionados 13

Notificación de la brecha de seguridad a la Autoridad de Control **14**

Cuándo notificar a la AEPD **16**

Plazos para notificar la brecha de datos a la AEPD **16**

Quién debe notificar las brechas de datos a la AEPD **17**

Comunicación de la brecha a los afectados. **17**

Cuándo comunicar a los interesados afectados **17**

Plazos para notificar la brecha de datos a los interesados afectados **17**

Quién debe comunicar las brechas de datos a los interesados afectados **18**

10. EVALUACIÓN DETALLADA DE LA NECESIDAD Y PROPORCIONALIDAD DEL TRATAMIENTO **18**

Consideraciones iniciales sobre la evaluación de la necesidad y 19

proporcionalidad del tratamiento 19

Contenido fundamental de la evaluación de la necesidad y proporcionalidad del tratamiento 20

JUICIO DE IDONEIDAD 20

JUICIO DE NECESIDAD 21

JUICIO DE PROPORCIONALIDAD EN SENTIDO ESTRICTO 21

Decisión final sobre la evaluación de la necesidad y proporcionalidad 23

11. CONCLUSIONES Y RECOMENDACIONES **23**

Conclusiones **23**

Recomendaciones 24

Actualización del proceso de la Evaluación de Impacto 24

12. MEMORANDO DEL DELEGADO DE PROTECCIÓN DE DATOS **25**

Visión del DPO/DPD 25

Revisión de los resultados y realimentación de la EIPD 26

Conclusiones y recomendaciones del DPO/dpd al responsable del tratamiento. 28

13. REFERENCIAS **28**

ANEXOS **29**

A. Actividades de Tratamiento **29**

USUARIOS INSCRITOS EN LA LISTA STOP PUBLICIDAD 29

B. Listado de Riesgos Detectados **32**

C. Listado de Medidas de Protección **40**

D. Documentación complementaria **52**

1. Algunas cuestiones fundamentales sobre la EIPD 52

2. Algunas preguntas y cuestiones relativas al modelo global de práctica de la evaluación e implantación de una EIPD – PIA. 53

E. Aplicación de medida de seguridad **70**

1. Niveles de riesgo y posibles medidas técnicas y organizativas aplicables 71

2. Posibles medidas de seguridad para los diferentes niveles de riesgo 71

F. INVENTARIO DE HARDWARE Y SOFTWARE 76

Inventario hardware 76

Inventario software 79

1. Datos Generales

Datos del Responsable:

NIF/CIF: G42631564

Nombre o R. Social: ASOCIACIÓN ESPAÑOLA PARA LA PRIVACIDAD DIGITAL (ASOCIACINEPD)

Actividad: Actividades de organizaciones empresariales, profesionales y patronales

Dirección Postal: Calle Médico Temístocles Almagro, N.18, Lc-2

Código Postal: 03300 **Localidad:** Orihuela

Provincia: Alicante **País:** España

Teléfono: 965306309 **Fax:**

Correo Electrónico: dpo@asociacionepd.es

Página Web: www.asociacionepd.es

Datos del Representante:

NIF/CIF: 74176803D

Nombre o R. Social: José Manuel de Ramón Rodríguez

Dirección Postal: Calle Médico Temístocles Almagro, N.18, LO-2

Código Postal: 03300 **Localidad:** ORIHUELA

Provincia: ALICANTE **País:** España

Teléfono: 965306309

Correo Electrónico: presidente@asociacionepd.es

Datos del Delegado de Protección de Datos:

NIF/CIF: 29005859F

Nombre o R. Social: Alberto Giménez Rodríguez

Dirección Postal: Calle Médico Temístocles Almagro, N.18, LO-2

Código Postal: 03300 **Localidad:** ORIHUELA

Provincia: ALICANTE **País:** España

Teléfono: 965306309 **Fax:**

Correo Electrónico: dpo@asociacionepd.es

2. Introducción

El tratamiento objeto de la presente Evaluación de Impacto es:

USUARIOS INSCRITOS EN LA LISTA STOP PUBLICIDAD

El Reglamento Europeo de Protección de Datos incorpora para los responsables la obligación de preparar un registro de tratamientos y un análisis básico de riesgos que los mismos pueden implicar.

Pero además de esta previsión, el artículo 35 plantea la obligación de elaborar un documento adicional relativo a la evaluación del impacto cuando el tratamiento entrañe o pueda entrañar un alto riesgo para los derechos y libertades de las personas físicas, en particular si utiliza nuevas tecnologías o debido a su naturaleza, alcance, contexto o fines.

En nuestro caso, se puede considerar la necesidad de realizar la evaluación de impacto en base al alcance de usuarios inscritos (Art. 35.1

Aunque el tratamiento objeto no se incluye en ninguno de los casos previstos en este mismo artículo 35, a saber:

− cuando se lleve a cabo una evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas físicas o que les afecten significativamente de modo similar;

− cuando se lleve a cabo un tratamiento a gran escala de categorías especiales de datos o de datos personales relativos a condenas e infracciones penales;

− en los casos de observación sistemática a gran escala de una zona de acceso público.

3. Evaluación de la necesidad y proporcionalidad de las operaciones de tratamiento

Aunque no nos encontramos ante supuestos de tratamiento que se consideran de alto riesgo para los derechos de los interesados, decidimos realizar un Informe de Evaluación de Impacto. En el presente caso, la necesidad de llevar a cabo este tratamiento y la legitimación que alega el responsable para el mismo puede justificarse de la siguiente manera de acuerdo con los criterios indicados:

− Idoneidad: se considera que el tratamiento es idóneo para conseguir el objetivo propuesto.

- Objetivo: exclusión publicitaria
- Tratamiento: inscripción de usuarios interesados
    1) Nombre y apellidos
    2) Número de identificación personal (DNI, NIE, Pasaporte)
    3) Email
    4) Fecha de Nacimiento
    5) Dirección Postal
    6) Tipo de representación y justificación, en su caso

− Necesidad:

El tratamiento es necesario y no existe otra forma de realizarlo para conseguir el objetivo propuesto.

- Necesidad: Inscripción de usuarios, con nombre y apellidos y verificación mediante email. Aportar datos personales sobre medios que se pretenden excluir de la actividad publicitaria.

− Proporcionalidad:

Las actividades de tratamiento son proporcionales a las finalidades previstas.

- Finalidad del tratamiento: exclusión publicitaria.
- Proporcionalidad: Aportación de datos a excluir
    1. Dirección Postal
    2. Números de teléfono
    3. Dirección e-mail
    4. Identificaciones de redes sociales
    5. Identificaciones para aplicaciones de mensajería

En el anexo **Actividad del Tratamiento** se especifica su legitimación y proporcionalidad en relación a sus finalidades.

De acuerdo con el análisis de riesgos realizado en relación a este tratamiento, se puede concluir que la evaluación de los riesgos para los derechos y libertades de los interesados, queda configurada de acuerdo con los siguientes parámetros:

− Identificación de amenazas y riesgos:

Las amenazas sobre el tratamiento pueden proceder de diferentes causas: desastres naturales, errores y fallos humanos, ataques intencionados a nivel informático (por ejemplo, hacking) o físico (por ejemplo, acceso a almacenes de datos, ordenadores, etc), incumplimiento normativo referido al periodo de retención, ausencia de base legal que legitime el tratamiento…).

− Posibles consecuencias de alguna de estas formas de amenaza:

- Vulneración de la confidencialidad de los datos, que se ve afectada cuando existe un acceso no permitido a los mismos;
- Vulneración de la integridad de los mismos, cuando se modifican o alteran por vías no autorizadas;
- Vulneración de la disponibilidad, que dejará de existir para los datos en caso de su eliminación.

4. Evaluación de los riesgos

Se ha de valorar y estimar la probabilidad y el impacto de que el riesgo se materialice. El concepto de riesgo inherente, hace referencia al riesgo intrínseco de cada actividad, sin tener en cuenta las medidas implementadas para limitarlo. Este concepto de riesgo inherente implica conjugar, por una parte, la exposición que se da tanto a la operación de tratamiento en particular y, por otra, la probabilidad de que la amenaza asociada al riesgo se materialice.
De acuerdo con los criterios orientativos facilitados por la Agencia de Protección de Datos, el cálculo del riesgo inherente se realiza mediante la siguiente fórmula:
Riesgo = Probabilidad x Impacto

a) Sobre la probabilidad:
Siguiendo las orientaciones facilitadas por la Agencia de Protección de Datos, las opciones sobre el cálculo de la probabilidad de que el riesgo se produzca será la siguiente:

• Despreciable: La posibilidad de ocurrencia es muy baja.

• Limitada: La posibilidad de ocurrencia es baja.

• Significativa: La posibilidad de ocurrencia es alta.

• Máxima: La posibilidad de ocurrencia es muy elevada.

b) Sobre el impacto de los daños en caso de materializarse la amenaza:
Siguiendo las orientaciones facilitadas por la Agencia de Protección de Datos, los niveles de impacto generados por la realización de los riesgos sobre los derechos de los interesados, serán los siguientes:

• Despreciable: El impacto es muy bajo

• Limitado: El impacto es bajo

• Significativo: El impacto es alto

• Máximo: El impacto es muy alto

Los daños que pueden generar estos impactos pueden ser de distintos tipos: daños físicos o sobre la integridad física, daños materiales que pueden generar pérdidas económicas, de empleo, etc, y daños morales, por ejemplo, depresión o situaciones de acoso.

El listado de los riesgos resultantes de esta evaluación se detalla en el Anexo B. **Listado de Riesgos Detectados**.

A partir de la evaluación de riesgos realizada, se concluye que el nivel de riesgo para este tratamiento es moderado. En consecuencia, se describe a continuación el plan de acción diseñado para garantizar la protección de los derechos de las personas interesadas, y que incluye las medidas de control a implantar para gestionar los riesgos. Estas medidas pueden ser de tipo legal, organizativo o técnico.
De acuerdo con los criterios mantenidos por la Agencia de Protección de Datos, existen las siguientes formas de afrontar el riesgo para reducir la probabilidad de que se produzca o su nivel de impacto:

• **Retención del riesgo:**

Si el nivel de riesgo inherente es inferior al nivel de riesgo considerado como aceptable, no existe necesidad de implementar controles adicionales.

• **Transferencia del riesgo:**

Consiste en compartir un riesgo con una organización externa, por ejemplo, una aseguradora, que será quien afronte sus consecuencias.

• **Anulación del riesgo:**

En los casos de riesgo muy elevado, la forma más contundente de eliminar el riesgo es abandonar la actividad de tratamiento que lo implica.

• **Reducción del riesgo:**

Para reducir el nivel de riesgo, se deben establecer medidas de control que reduzcan los niveles de probabilidad y/o impacto asociados al riesgo inherente.
El riesgo residual, es decir, el que afecta a este tratamiento una vez diseñadas e implementadas estas medidas de seguridad puede quedar configurado como riesgo residual Bajo.

5. Medidas previstas para afrontar los riesgos

Las medidas de control a implementar para gestionar los riesgos quedan detalladas en el anexo C **Listado de Medidas de Protección**.

6. Necesidad de efectuar la consulta previa

Objeto de la consulta

Cuando el resultado del informe de evaluación de impacto concluye con la existencia de un riesgo elevado, el responsable debe poner en marcha el procedimiento de Consulta Previa a la Autoridad de Control para que acepte o no la posibilidad de este tratamiento. No siendo el caso de la presente.

El proceso de consulta previa tiene como objeto presentar ante la Autoridad de Control Nacional Competente (Agencia Española de Protección de Datos - AEPD)un tratamiento que sea conforme con el RGPD UE, que tenga obligación o se haya valorado la oportunidad, o conveniencia, de realizar una EIPD por parte del responsable del tratamiento (Asociación Española para la Privacidad Digital), pero que entrañe un nivel de riesgo residual para los derechos y libertades de los ciudadanos que podría resultar inaceptable.

Obligación de realizar una consulta previa.

Debe consultarse a la Autoridad de Control sobre la procedencia de una actividad de tratamiento, y siempre antes de iniciarla, cuando una evaluación de impacto relativa a la protección de datos muestra que, en ausencia de garantías, medidas de seguridad y mecanismos destinados a mitigar los riesgos, dicho tratamiento entrañaría un alto riesgo para los derechos y libertades de las personas físicas, y el responsable del tratamiento considera que el riesgo no puede mitigarse por medios razonables en cuanto a tecnología disponible y costes de aplicación **(Considerando 94 del RGPD UE 2016/679)**.

En el presente caso que nos ocupa, el resultado del informe de EIPD concluye con la existencia de un nivel de riesgo residual bajo para los derechos y libertades de los ciudadanos, puesto que se han aplicado las medidas de protección necesarias para mitigar los potenciales riesgos detectados en la Evaluación de Impacto en la Protección de Datos **(EIPD-PIA: apartado evaluación de los riesgos y anexo listado de riesgos detectados)**.
En consecuencia, de todo ello se desprende la no necesidad y la no obligación legal de llevar a cabo esta Consulta Previa a la AEPD, por motivos objetivos y obvios recogidos y expuestos en el presente informe de EIPD-PIA. Puesto que no se dan las condiciones legales exigidas por el ***artículo 36.1 del RGPD UE 2016/679*** para realizar esta consulta.

7. Consultas a los Colectivos Afectados

Cuando el proyecto corporativo tenga efectos sobre sectores amplios de la población o pueda generar desconfianza por parte de los afectados, es importante obtener la visión de las personas o colectivos afectados.
Las consultas con las partes afectadas, tanto internas como externas, son un tema que puede resultar delicado pero que es importante para el correcto desarrollo de una EIPD.

Se puede obtener la opinión general de **estos terceros (Usuarios de la Lista Stop Publicidad)** mediante cuestionarios, reuniones o grupos de trabajo, sin que sea necesario revelar detalles excesivos sobre nuevos productos o servicios o revelar secretos comerciales o tecnológicos.
Las consultas son importantes para obtener la visión de personas u organizaciones que no están implicadas en el proyecto corporativo y que, por ello, lo pueden observar desde una perspectiva más amplia, poniendo de manifiesto riesgos que no son tan evidentes o pueden pasar desapercibidos para los que trabajan o están cercanos al mismo.

Por otro lado, la Asociación Española para la Privacidad Digital es totalmente consciente de que la consulta con las personas físicas cuyos datos personales van a ser tratados es recomendable pues, por una parte, posibilitará que la entidad (la Asociación) conozca las preocupaciones de los mismos y, por otra, dotará al proyecto corporativo de transparencia.
El apartado 9 del artículo 35 del RGPD UE, establece que **"cuando proceda"** en una EIPD deberá recabarse la opinión de los interesados o de sus representantes en relación con el tratamiento previsto, sin embargo, no precisa cuáles serán los supuestos o situaciones en que procede realizar esta consulta a los afectados/interesados.

8. Ciclo de vida del dato personal

Dejar constancia fehaciente de que para tratamientos complejos, en los que la principal fuente de riesgo proviene de la sensibilidad, la extensión de los datos, las formas de recogida de éstos o su comunicación a terceros, es recomendable realizar un análisis global del ciclo de vida del dato. El análisis del ciclo de vida supone considerar, para un conjunto o categoría de datos, las distintas etapas de su vida, desde su recogida o generación hasta su destrucción. En el caso que nos ocupa en este momento, la descripción del ciclo de vida de los datos es un análisis complementario al análisis estructurado del tratamiento.
Una aproximación inicial y elemental al estudio del ciclo de vida de los datos puede estructurar el mismo en las etapas detalladas a continuación:

- Recogida/Generación
- Registro
- Uso
- Comunicación
- Finalización

Recogida/Generación (CAPTURA DE DATOS):
Se trata del proceso de obtención de datos para su tratamiento. La Asociación Española para la Privacidad Digital procede a la obtención de datos a través de formularios web.

Registro (CLASIFICACIÓN/ALMACENAMIENTO):
La Asociación viene a establecer categorías y asignarlas a los datos para su almacenamiento, organización, estructuración, conservación o adaptación en los archivos, bases de datos o sistemas de información.
Cumpliendo todo ello con la implantación de las medidas de seguridad correspondientes según el nivel de riesgo aplicable, contempladas por la normativa europea de protección de datos (RGPD UE).

Uso (TRATAMIENTO):
Asimismo el responsable del tratamiento procede a englobar la operación o conjunto de operaciones realizadas sobre datos personales o conjunto de datos personales, fundamentalmente y de manera prácticamente exclusiva mediante procedimientos automatizados, con relación a su modificación, extracción, consulta o utilización. Se contempla la posibilidad técnica de que dichos procedimientos sean excepcionalmente o habitualmente poco frecuentes y de naturaleza manual.

Comunicación a un tercero (CESIÓN O TRANSFERENCIA DE DATOS A UN TERCERO PARA SU TRATAMIENTO):
La Asociación no procede a comunicar datos personales a terceros. Según el artículo 4.10 del RGPD UE se entiende por tercero: "la persona física o jurídica, autoridad pública, servicio u organismo distinto del interesado, del responsable del tratamiento, del encargado del tratamiento y de las personas autorizadas para tratar los datos personales bajo la autoridad directa del responsable o encargado". Los resultados de las consultas, efectuadas por los obligados a consultar y autoridad en la materia, serán de tipo positivo/negativo sobre el dato o conjunto de datos consultados.

La ASOCIACIÓN ESPAÑOLA PARA LA PRIVACIDAD DIGITAL ha externalizado determinados servicios contratando en algunos casos a proveedores o empresas con sede fuera de la UE y del EEE respecto al tratamiento en calidad de responsable de tratamiento: LISTA STOP PUBLICIDAD, a efectos de la normativa de protección de datos implica transferencias internacionales de datos.

1) La ASOCIACIÓN ESPAÑOLA PARA LA PRIVACIDAD DIGITAL utiliza los servicios de Google como prestador de servicios externos para alojar la LISTA STOP PUBLICIDAD, siendo Google encargado de tratamiento. A continuación se detalla la relación a efectos de protección de datos entre Google LLC y la ASOCIACIÓN ESPAÑOLA PARA LA PRIVACIDAD DIGITAL.
La infraestructura de LISTA STOP PUBLICIDAD está desarrollada y alojada en Google Firebase. Firebase es un servicio contratado con Google entendiendo por tal a Google LLC (anteriormente conocida como Google Inc.), Google Ireland Limited, Google Asia Pacific Pte. Ltd., o cualquier otra entidad que controle directa o indirectamente, esté controlada por Google LLC o esté bajo control común con Google LLC.
La transferencia internacional de datos se fundamenta en un Acuerdo de procesamiento de datos (Ver NOTA 1) suscrito entre Google y ASOCIACIÓN ESPAÑOLA PARA LA PRIVACIDAD DIGITAL (Revisado y aceptado el 20 de julio de 2022) que incluye Cláusulas contractuales tipo de la UE adoptadas por la Comisión en base al Artículo 46.2.c) del RGPD en relación con la Decisión de Ejecución (UE) 2021/914 de la Comisión de 4 de Junio de 2021 relativa a las cláusulas contractuales tipo para la transferencia de datos personales a terceros países de conformidad con el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo siendo el exportador de datos y responsable de tratamiento la ASOCIACIÓN ESPAÑOLA PARA LA PRIVACIDAD DIGITAL y el importador de datos y encargado de tratamiento Google.

La base de datos de Firebase cuyo responsable es la ASOCIACIÓN ESPAÑOLA PARA LA PRIVACIDAD DIGITAL utiliza los siguientes servicios proporcionados por Firebase:

Firebase Hosting: proporciona alojamiento a https://listastoppublicidad.es/ (Ver NOTA 2)

Firebase Crashlytics herramienta que utiliza Firebase para los informes de fallos/incidencias de https://listastoppublicidad.es/ (Ver NOTA 3)

Cloud Firestore, Cloud Functions for Firebase, Cloud Storage for Firebase, Firebase Authentication: son servicios de Firebase y están sujetos a las Condiciones del servicio de Google Cloud Platform son "Servicios" y/o "Software" y están sujetos a las Condiciones específicas del servicio de Google Cloud Platform que forman parte de las Condiciones del servicio de Google Cloud Platform. (Ver NOTA 4)

NOTAS:

1.https://firebase.google.com/terms

2.https://firebase.google.com/terms/data-processing-terms

3.https://firebase.google.com/terms/crashlytics-app-distribution-data-processing-term/

4.https://cloud.google.com/terms/data-processing-terms

2) Proveedor verificación identidad: TWILIO. Twilio SMS APIs: Twilio es una plataforma de comunicación en la nube que nos permite verificar la identidad a través de SMS. La ASOCIACIÓN ESPAÑOLA PARA LA PRIVACIDAD DIGITAL incorpora la doble autentificación en base a un interés legítimo en virtud del art. 6.1. f) del RGPD para mejorar la seguridad de nuestros servicios y para garantizar el cumplimiento de la normativa de protección de datos. El proveedor es Twilio Ireland Limited, Irlanda. Twilio Ireland Limited, sociedad registrada en la República de Irlanda, con domicilio social en 25-28 North Wall Quay. Twilio es un grupo multinacional (haz click aquí para ver empresas del grupo TWILIO). En este contexto Twilio realiza transferencias internacionales de datos.

La ASOCIACIÓN ESPAÑOLA PARA LA PRIVACIDAD DIGITAL ha suscrito un contrato de encargado de tratamiento de datos (Acuerdo de procesamiento de datos) con Twilio que garantiza el cumplimiento de la normativa de protección de datos.

La legalidad de las transferencias entre Twilio y la ASOCIACIÓN ESPAÑOLA PARA LA PRIVACIDAD DIGITAL se fundamenta en base a las Cláusulas contractuales tipo de la UE contenidas en el Acuerdo de procesamiento de datos suscrito entre ambas partes.

Twilio tiene procesadores externos (subprocesadores) (puede consultarlos en este enlace https://www.twilio.com/legal/sub-processors) Sitio web: https://www.twilio.com/de/authy-static. Más información y privacidad: https://www.twilio.com/legal/tos y https://www.twilio.com/legal/privacy.

Finalización (SUPRESIÓN/DESTRUCCIÓN):
El responsable del tratamiento ha articulado debidamente procesos de limitación del uso de los datos personales, incluyendo el bloqueo de los datos (según lo previsto en el artículo 32.2 de la LOPD GDD 3/2018), la supresión y la destrucción de datos. Así:

- Para los menores de 14 años que fueron inscritos por representante se prevé que al cumplir los 14 años se inicie automáticamente un proceso de bloqueo (de la inscripción por representante), posterior cancelación o supresión (silencio del mayor de 14 años al efecto), y definitiva destrucción, por el transcurso de los plazos determinados en el sistema a efectos de obligaciones legales del responsable del tratamiento.
- Para discapacitados inscritos por representantes se contempla la necesidad de acreditar el cambio de estado, cuestionar la representación inicial que originó la inscripción en el sistema o proceder a la cancelación por el representante que inicialmente inscribió al afectado, procediendo al bloqueo por rectificación o supresión, cancelación y destrucción definitiva tras el transcurso de los plazos determinados en el sistema a efectos de obligaciones legales del responsable del tratamiento.
- Para los fallecidos inscritos por representantes se contempla cuestionar la representación inicial que originó la inscripción en el sistema o proceder a la

cancelación por el representante que inicialmente inscribió al afectado, procediendo al bloqueo por rectificación o supresión, cancelación y destrucción definitiva tras el transcurso de los plazos determinados en el sistema a efectos de obligaciones legales del responsable del tratamiento.

- Para los mayores de 14 años inscritos sin representante el sistema permite que el propio inscrito rectifique o cancele, los datos de inscripción y los aportados para la exclusión publicitaria, de forma inmediata. Iniciándose un proceso automático de bloqueo y cancelación o supresión definitiva, respetando los plazos determinados en el sistema a efectos de obligaciones legales del responsable del tratamiento.

9. GESTIÓN DE BRECHAS DE SEGURIDAD

Tipologías de brechas de seguridad

La Asociación Española para la Privacidad Digital a la hora de evaluar el nivel de riesgo de una brecha de seguridad de datos personales, conforme a criterios de la AEPD procede a determinar su tipología, es decir determina a qué dimensión o dimensiones de seguridad de los datos personales ha afectado la brecha. Dichas dimensiones son la confidencialidad, la disponibilidad y la integridad. Comentar que el responsable del tratamiento (la Asociación) tiene en consideración que una misma brecha de seguridad de datos personales puede afectar a más de una dimensión dependiendo de las circunstancias particulares en cada caso.

Definiciones básicas de conceptos relacionados

Confidencialidad: Una brecha de seguridad afecta a la confidencialidad cuando los datos personales de un tratamiento han podido ser accedidos por terceros sin permiso, incluyendo cuando los datos son filtrados. Esto incluye, por ejemplo, los casos de intrusión en sistema de información con acceso y/o exfiltración de datos personales, el envío de datos personales por error, la pérdida de dispositivos o documentación con datos personales, malware de tipo ransomware con exfiltración de datos, etc.
Es importante indicar que en la plataforma corporativa web de la Asociación, los datos personales que pudieren verse afectados por una violación de la seguridad de los datos están totalmente cifrados o encriptados de forma segura, anonimizados y protegidos de forma que sean inintilegibles para quien haya tenido acceso a dichos datos o lo pueda tener en el futuro. De esta manera, las consecuencias de la brecha de confidencialidad quedarán en gran medida mitigadas, reduciendo o incluso anulando los riesgos derivados del incidente.

Disponibilidad: Una brecha afecta a la disponibilidad de los datos personales cuando han estado inaccesibles de forma temporal o permanente para quien legítimamente debe poder tratarlos o acceder a ellos. Esta situación puede ocurrir por sucesos que afecten a los datos personales en sí mismos o también por sucesos que afecten a los sistemas utilizados para su tratamiento. Por ejemplo, incluye casos de cifrado de datos o de los sistemas de información causado por malware de tipo ransomware o la imposibilidad de acceder a un almacenamiento de datos (acceso físico o lógico).
Procede señalar que el responsable del tratamiento ha articulado medidas técnicas y organizativas, para poder determinar que la disponibilidad se puede recuperar o está en vías de recuperación, puesto que obviamente recuperar los datos y sistemas de tratamiento es la vía para mitigar el daño que pueden producir este tipo de brechas de datos personales. Para la consecución de tal objetivo o fin la Asociación ha establecido estrategias y procedimientos de recuperación ante situaciones de este tipo, incluyendo procedimientos de copias de seguridad y de respaldo de datos personales, recuperación ante incidentes y estrategias de gobernanza de los datos personales.
Integridad: Una brecha afecta a la integridad cuando se han alterado los datos personales de forma ilegítima y el tratamiento de esos datos personales puede causar daños a los afectados. Como puede ser el caso de un tercero que ha modificado en la base de datos de la organización la información relativa a los datos bancarios de los Clientes que se utilizan para el cobro del servicio prestado a los mismos.
Conviene indicar claramente que la Asociación Española para la Privacidad Digital, cuando se producen brechas de seguridad de datos personales de integridad, ésta procede a determinar si el tratamiento de los datos supuestamente alterados ilegítimamente puede causar o ha causado algún daño a los afectados y en su caso si el daño se puede revertir.
Como conclusión final de este apartado, sería oportuno reproducir el contenido del **artículo 32.1 b) del RGPD UE** que estipula lo indicado a continuación:
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:
(...)
b) ***la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento".***

Notificación de la brecha de seguridad a la Autoridad de Control

Con independencia de la necesidad de notificar a la AEPD sobre una brecha de datos personales, el responsable del tratamiento conforme al contenido del artículo 33.5 del RGPD UE y en base al principio de responsabilidad proactiva consagrado en el artículo 5.2 del RGPD UE y en el Considerando 85 del RGPD UE, reconoce su obligación de documentar cualquier brecha acaecida en su caso, incluidos los hechos relacionados con la brecha, sus efectos y las medidas correctivas adoptadas (medidas de protección). Por lo tanto, si llegado el caso se produjere alguna incidencia de entidad, alguna violación de la seguridad de los datos o alguna brecha de seguridad de datos personales, la Asociación Española para la Privacidad Digital, estará en condiciones de cumplir con su obligación legal y de aportar toda la documentación necesaria y requerida por la Autoridad de Control, a tales efectos.
En el caso de ser necesario, la notificación contemplada en el apartado 1º del artículo 33 del RGPD UE 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.
El responsable del tratamiento (la Asociación) a la hora de evaluar el riesgo de una brecha de seguridad tiene en cuenta y presente en todo momento **los siguientes factores**:

- Tipo de brecha de datos personales
- Naturaleza, carácter sensible y el volumen de datos personales
- Facilidad de identificación de las personas
- Gravedad de las consecuencias para los derechos y libertades de las personas
- Características particulares del responsable del tratamiento
- Número de personas afectadas
- Consideraciones generales

Cuándo notificar a la AEPD

El responsable del tratamiento (la Asociación) conforme al artículo 33 del RGPD UE, tan pronto como tenga conocimiento de que se ha producido una brecha de datos personales procederá a efectuar la correspondiente notificación a la AEPD, siempre y cuando sea probable que la brecha constituya un riesgo para los derechos y libertades de las personas. En el hipotético caso de que se produjera tal brecha de seguridad de datos personales, la Asociación la realizará sin dilación y a más tardar en las **72 horas** siguientes al momento de producirse o acaecer dicha brecha de datos, computando también las horas transcurridas durante fines de semana y festivos.
El criterio seguido por la Asociación Española para la Privacidad Digital para determinar si un incidente ha producido "una brecha de datos personales" se recoge en el propio RGPD: "toda violación 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 de carácter personal".

Es importante señalar que no es obligatorio legalmente notificar todas las brechas de seguridad dado que el RGPD UE prevé una excepción a esta obligación cuando, conforme al principio de responsabilidad proactiva, el responsable del tratamiento pueda garantizar que es improbable que la brecha de seguridad de datos personales en cuestión entrañe un riesgo para los derechos y las libertades de las personas físicas o de los ciudadanos.

Plazos para notificar la brecha de datos a la AEPD

El RGPD establece que el responsable del tratamiento notificará las brechas de datos personales a la Autoridad de Control sin dilación indebida y a más tardar dentro de la 72 horas desde que se tenga constancia de la brecha de seguridad de datos personales.
El plazo de 72 horas empieza a calcularse desde el instante en que el responsable del tratamiento tenga constancia de que el incidente de seguridad ha afectado a datos personales, incluyendo las horas transcurridas durante fines de semana y días festivos.
Corresponde al encargado del tratamiento notificar al responsable del tratamiento sin dilación indebida las brechas de seguridad de datos personales de las que tenga constancia. Para la notificación del encargado al responsable, el RGPD no establece un plazo de tiempo concreto y se limita a indicar que debe realizarse dilación indebida.

Quién debe notificar las brechas de datos a la AEPD

Corresponde en el caso de acaecimiento de una brecha de seguridad, a la Asociación Española para la Privacidad Digital como responsable del tratamiento, notificará a la AEPD las brechas de datos de las que tenga constancia, cuando éstas puedan suponer un riesgo para los derechos y libertades de las personas físicas.
El encargado del tratamiento que ha sido objeto de la brecha de datos personales únicamente podrá notificar en nombre del responsable del tratamiento (la Asociación) si así lo tiene establecido en un contrato o vínculo legal de similar índole.

Comunicación de la brecha a los afectados.

En primer lugar dejar constancia de que los interesados afectados son las personas
físicas cuyos datos personales se han visto afectados por una brecha de seguridad comprometiendo la confidencialidad, integridad y/o disponibilidad de esos datos, y quienes pueden sufrir las consecuencias.
En el seno de la organización (la Asociación) se ha establecido un proceso de gestión de brechas de seguridad de datos personales, que incluye un procedimiento para llevar a cabo la comunicación de dicha brecha de datos a los interesados afectados, concretando la información a la que hace referencia el **artículo 34 del RGPD UE**, incluyendo los plazos concretos adecuados para llevar a cabo la comunicación.

Cuándo comunicar a los interesados afectados

El artículo 34 del RGPD UE estipula que cuando sea probable que la brecha de datos personale entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento comunicará la brecha de datos personales a los afectados sin dilación indebida.
Consecuentemente, la Asociación Española para la Privacidad Digital tan pronto como tenga constancia de la brecha de datos personales procederá a valorar el riesgo para las personas afectadas y determinará la necesidad de comunicar la brecha de datos a los afectados. En caso de que el riesgo se determine como alto, la comunicación a los afectados se realizará a la mayor brevedad posible.

Plazos para notificar la brecha de datos a los interesados afectados

El RGPD UE no establece un plazo concreto para la comunicación a los afectados, pero sí indica que deberá realizarse sin dilación indebida.
La Asociación Española para la Privacidad Digital es consciente y tiene presente en todo momento que en el caso de producirse una brecha de seguridad, cualquier dilación en la comunicación a los afectados le puede restar efectividad, por lo que una comunicación a destiempo puede llegar teóricamente a tener el mismo efecto que una comunicación no realizada. Por tanto, la Asociación Española para la Privacidad Digital como responsable del tratamiento, en el hipotético caso de que produjere un retraso en la comunicación inmediata a los interesados cuando ésta sea necesaria, procederá a justificar debidamente dicho retraso.

Quién debe comunicar las brechas de datos a los interesados afectados

La comunicación de una brecha de datos personales a las personas afectadas conforme al artículo 34 del RGPD UE corresponde al responsable del tratamiento (la Asociación).
El encargado del tratamiento que ha sido objeto de la brecha de datos personales únicamente podrá comunicar dicha brecha de seguridad a los afectados si así lo tiene establecido en un contrato o vínculo legal con la Asociación Española para la Privacidad Digital.
En cualquier caso, la Asociación deberá ser previamente informada sobre la ocurrencia de la brecha de datos personales y sobre todos los detalles relevantes como establece el artículo 33.2 del RGPD UE, pues le corresponde decidir sobre la necesidad de comunicar la brecha de datos personales a los afectados.

10. EVALUACIÓN DETALLADA DE LA NECESIDAD Y PROPORCIONALIDAD DEL TRATAMIENTO

Necesidad y proporcionalidad del tratamiento

El principio de "minimización de datos" establece que los datos personales serán "adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que serán tratados". Durante la definición del mismo, consideramos qué datos son estrictamente necesarios para realizar las actividades de tratamiento en función de las finalidades previstas por la Asociación Española para la Privacidad Digital.
De la misma manera, todas las acciones que el tratamiento incluya deben ser necesarias y proporcionales a las finalidades previstas. Si tomamos como base el **considerando 39 del RGPD UE**, procedemos a tener en cuenta los siguientes aspectos para evaluar la necesidad del tratamiento:
1. Los datos personales sólo se deben tratar si la finalidad del tratamiento no se puede hacer razonablemente por otros medios, o sea, sin tratar datos de carácter personal.
2. Las finalidades tienen que estar definidas de manera determinada, explícita y legítima.

3. Cualquier tratamiento de datos personales tiene que ser lícito y leal. Este concepto tiene relación con el análisis de las finalidades establecidas en el tratamiento y su supuesto legitimador.
4. Los datos personales tienen que ser adecuados, pertinentes y limitados a lo necesario para los fines para los cuales se tratan.
5. El plazo de conservación de los datos tiene que limitarse a un mínimo estricto. Consideramos que la proporcionalidad tiene que ver con evaluar si la finalidad que se persigue se puede conseguir por otros medios, por ejemplo: utilizando otros datos, reduciendo el universo de personas afectadas (de manera cuantitativa o cualitativa), haciendo uso de otras tecnologías menos invasivas o bien aplicando otros procedimientos o medios de tratamiento (modificando los inicialmente previstos), etc.
Las Autoridades de Protección de Datos con frecuencia determinan que para comprobar si un tratamiento supone una medida restrictiva de un derecho fundamental, este debe superar los tres puntos o componentes del llamado **principio de proporcionalidad**.
En efecto, de conformidad con la doctrina jurisprudencial del TC (Tribunal Constitucional), la constitucionalidad de cualquier medida restrictiva de derechos fundamentales viene determinada por la estricta observancia del principio de proporcionalidad. Dicho principio ha sido recogido por las SSTC 66/1995, 55/1996, 207/1996, 37/1998 y la STC 98/2000. A los efectos que aquí importan, basta con recordar que dichas sentencias de manera sintetizada, determinan que para comprobar si una medida restrictiva de un derecho fundamental supera el juicio de proporcionalidad, es necesario constatar si cumple los tres requisitos o condiciones siguientes: si tal medida es susceptible de conseguir el objetivo propuesto (juicio de idoneidad); si, además, es necesaria, en el sentido de que no exista otra medida más moderada para la consecución del tal propósito con igual eficacia (juicio de necesidad); y, finalmente, si la misma es ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto (juicio de proporcionalidad en sentido estricto).

Consideraciones iniciales sobre la evaluación de la necesidad y proporcionalidad del tratamiento

• Los datos recogidos o recabados:

Por la **Asociación Española para la Privacidad Digital** se van a usar exclusivamente para la finalidad declarada (inclusión en el sistema de exclusión publicitaria), y no para ninguna otra no informada ni incompatible con la legitimidad de su uso (principio de limitación de la finalidad). Por lo tanto se obtienen de las personas interesadas o de sus representantes (usuarios inscritos en la Lista Stop Publicidad) los datos de carácter personal estrictamente necesarios o fundamentales, para cumplir con las finalidades legítimas previstas.

• La finalidad:

Que se pretende cubrir por parte del **responsable del tratamiento** requiere obviamente de todos los datos a recabar y para todas las personas interesadas o sus representantes (principio de minimización de datos). Solamente se obtienen y se utilizan los datos personales indispensables para la consecución de la finalidad inicial.

• Las tecnologías utilizadas:

Para el tratamiento de datos son adecuadas para la finalidad establecida desde el punto de vista del cumplimiento de los principios básicos o fundamentales de la privacidad. Desde el principio de la creación de la plataforma web de **la Asociación**, en todo momento se han tenido en cuenta los principios fundamentales de la protección de datos desde el diseño y por defecto. Todo ello conforme a lo estipulado por el artículo 25 del RGPD UE.

• Plazos de conservación de los datos personales:

La Asociación no los mantiene más tiempo del necesario para las finalidades del tratamiento (principio de limitación del plazo de conservación). Los datos son conservados el tiempo estrictamente imprescindible. El interesado o afectado puede en cualquier momento, ejercitar su derecho a la supresión de los datos y a retirar el consentimiento libremente prestado previamente.

Contenido fundamental de la evaluación de la necesidad y proporcionalidad del tratamiento

Hay que dejar constancia de que una de las exigencias del artículo 35 del RGPD UE con relación a la EIPD, es la que aparece en el artículo 35.7 b) del RGPD UE, es decir, la obligación de que se realice "una evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento en cuanto a su finalidad".
La Asociación Española para la Privacidad Digital, como paso previo antes de abordar esta evaluación de la necesidad y proporcionalidad de los tratamientos, ha procedido a consultar las directrices del CEPD, las resoluciones o informes jurídicos de la AEPD, o la doctrina jurisprudencial, donde pueden recogerse o existir evaluaciones de tratamientos que guarden similitud con los de la Asociación Española para la Privacidad Digital en función de la naturaleza, ámbito, contexto o fines del tratamiento y que permitan identificar los límites a los que el tratamiento en cuestión ha de sujetarse.
Este principio de proporcionalidad, llevado a la evaluación de la necesidad y proporcionalidad del tratamiento, se traduce en realizar una ponderación atendiendo a tres criterios: juicio de idoneidad, juicio de necesidad, y juicio de proporcionalidad en sentido estricto.

JUICIO DE IDONEIDAD

En relación con este primer juicio el responsable del tratamiento ha determinado que los tratamientos son adecuados para los fines que se persiguen. Los tratamientos dan respuesta a determinadas carencias, demandas, exigencias, obligaciones y oportunidades objetivas y consiguen los objetivos propuestos con la eficacia suficiente.

En este juicio de idoneidad la Asociación ha procedido a evaluar si las propuestas de tratamientos, tal y como están planteadas, alcanzan la eficacia necesaria para cumplir los fines que persiguen. Respecto a la mencionada eficacia, el responsable del tratamiento la ha demostrado de forma objetiva, para lo cual ha realizado la:
1. Definición del umbral de efectividad del tratamiento: La Asociación ha establecido de forma objetiva, cualitativa y basada en evidencias, cuál es el umbral de efectividad que se debería alcanzar para cumplir con los fines del tratamiento. Según cálculos

objetivos estimados y aproximados existe un margen de error del 7% en un valor resultado, y una detección de un 93% de casos.
2. Evaluación de la efectividad de la propuesta de tratamiento: La Asociación ha evaluado de forma objetiva, cualitativa y basada en evidencias, la efectividad de los tratamientos, tal y como se han planteado, verificando al mismo tiempo que se dan respuesta a las necesidades planteadas y en toda su extensión.

JUICIO DE NECESIDAD

En relación con el segundo juicio el responsable del tratamiento ha determinado que la finalidades perseguidas no pueden alcanzarse de otro modo menos lesivo o invasivo, es decir, no existe por tanto unos tratamientos alternativos que sean igualmente eficaces para el logro de las finalidades perseguidas.

La Asociación para llevar a cabo este juicio de necesidad ha seguido los pasos que indicamos a continuación:
1. Determinación de la relevancia de los fines del tratamiento: Ha evaluado que los fines del tratamiento tienen la importancia suficiente para ser abordados con un tratamiento de riesgo inicial moderado y de riesgo residual bajo (**Actividad de Tratamiento Lista Stop Publicidad**).
2. Verificación de la adecuación de las operaciones de tratamiento: Ha verificado de que cada una de las operaciones concretas del tratamiento está orientada a cumplir con los fines del tratamiento de una forma objetivamente demostrable.
3. Justificación de la configuración actual del tratamiento: Ha evaluado que no existen otros tratamientos, que ya están en curso o que se podrían plantear, que resuelven los fines declarados sin incurrir en un alto riesgo, incluso aunque sea necesario introducir alguna modificación para cumplir los fines perseguidos.

JUICIO DE PROPORCIONALIDAD EN SENTIDO ESTRICTO

En relación con el tercer y último juicio el responsable del tratamiento ha verificado que la gravedad del riesgo del tratamiento para los derechos y libertades, y su intromisión en la privacidad, es adecuada al objetivo perseguido y proporcionada a la urgencia y gravedad de esta. El responsable del tratamiento asimismo ha procedido a ponderar el beneficio para el interés general alcanzado con el tratamiento y los derechos de los sujetos cuyos datos se ven afectados, sin que ésta pueda suponer la negación absoluta del derecho a la protección de datos y vaciar de su contenido esencial.
La Asociación para realizar este juicio de proporcionalidad en sentido estricto, y una vez acreditada la idoneidad y necesidad del tratamiento, ha llevado a cabo los siguientes pasos:
1. **Identificación del grado de impacto del tratamiento en los derechos y libertades:**
Ha determinado de forma detallada, las limitaciones o intrusiones a los derechos y libertades que pueden suponer los tratamientos para el interesado/afectado. Esta evaluación se ha procedido a realizar previamente, en la determinación de los factores de riesgo que constan en el apartado Evaluación de los riesgos. Concluyendo como resultado final un nivel de riesgo global bajo.
2. **Identificación y descripción de medidas compensatorias:**

Ha detallado debidamente los controles establecidos en el diseño del tratamiento para disminuir dicho impacto. Esta evaluación se ha procedido a realizar previamente, en la determinación de las medidas de protección para mitigar los posibles riesgos detectados que constan en el apartado Medidas previstas para afrontar los riesgos. Concluyendo como resultado final un nivel de riesgo residual bajo.

3. **Identificación de los beneficios del tratamiento:**

La Asociación Española para la Privacidad Digital ha procedido a determinar las ventajas y beneficios, que de forma objetiva y con evidencias, conlleva o tiene el tratamiento de datos para los interesados o afectados, siendo éstos considerados de forma individual y como colectivo en su conjunto. Considerándose por lo tanto también el beneficio social.

En relación con las actividades de tratamiento: **usuarios inscritos en la Lista Stop Publicidad,** el responsable del tratamiento se ha cerciorado con total seguridad y con hechos evidentes de que los beneficios potenciales de las actividades de tratamiento mencionadas son incuestionables y totalmente reales, dada su trascendencia social, puesto que los sistemas de exclusión publicitaria tienen prevista su creación por el artículo 23 de la LOPD GDD 3/2018.

Dicho artículo 23 LOPD GDD estipula lo siguiente:

"1. Será lícito el tratamiento de datos personales que tenga por objeto evitar el envío de comunicaciones comerciales a quienes hubiesen manifestado su negativa u oposición a recibirlas. A tal efecto, podrán crearse sistemas de información, generales o sectoriales, en los que solo se incluirán los datos imprescindibles para identificar a los afectados. Estos sistemas también podrán incluir servicios de preferencia, mediante los cuales los afectados limiten la recepción de comunicaciones comerciales a las procedentes de determinadas empresas".

4. **Confirmación de existencia de identidad en la calidad de la información utilizada:**

Ha evaluado que existe simetría en la información analizada para el juicio de ponderación, por lo tanto, el nivel de análisis con relación al impacto es igual al nivel alcanzado en base a la información proporcionada respecto de las ventajas.

5. **Análisis BDB (Balance Daño-Beneficio):**

La Asociación Española para la Privacidad Digital ha procedido a evaluar de forma totalmente objetiva y evidente, si los beneficios para los interesados y la sociedad en su conjunto, previamente determinados, compensan y justifican el impacto para los derechos y libertades de las personas afectadas identificados en el apartado Evaluación de los riesgos. El resultado de la evaluación objetiva ha sido totalmente positivo. Derivándose en su conjunto más beneficios que perjuicios para los afectados o interesados titulares de los datos personales objeto de tratamiento.

Claramente se desprende del análisis de las finalidades legítimas, a las que obedecen la creación de las actividades de tratamiento de las que es titular la Asociación Española para la Privacidad Digital, que el beneficio general para la ciudadanía del tratamiento de datos incluidos en dichas actividades de tratamiento es absolutamente innegable y provechoso socialmente hablando.

Decisión final sobre la evaluación de la necesidad y proporcionalidad

La evaluación de la necesidad, y la proporcionalidad debe conducir a la toma de una decisión sobre si el tratamiento es viable o, por el contrario, no lo es de acuerdo a la forma en que está planteado.

En el presente caso que nos ocupa, toda la información recopilada a lo largo del informe de Evaluación de Impacto en la Protección de Datos, nos conduce a que el análisis de la evaluación de la necesidad y proporcionalidad del tratamiento, arroja o desprende como conclusión final que los tratamientos de datos personales, incluidos en las distintas actividades de tratamiento de las cuales es titular el responsable del tratamiento (la Asociación), son legítimos y conformes a derecho, cumpliendo de manera escrupulosa con todos y cada uno de los principios rectores más importantes en materia de protección de datos personales, contemplados por el artículo 5 del RGPD UE 2016/679.

Consideramos que al estar la Asociación Española para la Privacidad Digital en condiciones de poder demostrar y justificar la necesidad y la proporcionalidad de los tratamientos de datos, incluidos los tratamientos de alto riesgo o de las operaciones de tratamiento que pudieran formar parte de éstos, se desprende consecuentemente que está legitimada o habilitada para poder avanzar en la EIPD - PIA.

En el proceso de realizar la evaluación de la necesidad y la proporcionalidad tenemos la certeza de que el responsable del tratamiento (la Asociación), ha procedido a proporcionar las evidencias adecuadas, a registrar y a guardar toda la información relevante para llevar a cabo dicho análisis y plasmar en un informe final todo el proceso de la evaluación realizada con sus oportunas conclusiones.

11. CONCLUSIONES Y RECOMENDACIONES

Conclusiones

De la información y de la documentación recogida a lo largo del presente Informe de Evaluación de Impacto en la Protección de Datos (**EIPD-PIA**), tanto en sus distintos apartados como en los anexos correspondientes, se puede concluir que el responsable del tratamiento (Asociación Española para la Privacidad Digital) ha implementado correctamente las obligaciones principales que incorpora el Reglamento General Europeo de Protección de Datos (**RGPD UE 2016/679**) y la Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales (**LOPD GDD 3/2018**), a efectos de garantizar la protección de los derechos de las personas en relación al tratamiento de sus datos personales.

Respecto al resultado final de la gestión del riesgo para los derechos y libertades fundamentales de los ciudadanos (personas físicas afectadas o interesadas) en materia de protección de datos, hay que dejar constancia de que tras la detección de una serie de riesgos potenciales, se han aplicado las medidas de protección oportunas para mitigar lo máximo posible dichos riesgos detectados.

En relación con la gestión del riesgo y lo mencionado anteriormente, hay que decir que respecto a la ***afectación estimada del riesgo*** la probabilidad de

que se materialice el riesgo es despreciable. Siendo asimismo el impacto o gravedad del riesgo en caso de producirse.

Y respecto a la ***efectividad de la medida de protección*** hay que mencionar que la probabilidad del riesgo tras aplicar la medida de protección es despreciable. Siendo asimismo el impacto del riesgo tras aplicar la medida de protección despreciable.
En relación a la determinación del riesgo, es muy importante señalar que el responsable del tratamiento, tras realizar la EIPD, ha obtenido como resultado que tanto el ***nivel de riesgo global***, como el ***nivel de riesgo residual*** tras aplicar las oportunas medidas de protección es bajo.
En referencia en el caso particular de que proceda la posible Consulta Previa a la AEPD conforme al **artículo 36 del RGPD UE**, nos remitimos a la recogido en el apartado correspondiente sobre la Necesidad de Consulta Previa. Argumentando en dicho apartado que no se considera a efectos legales obligatoria o necesaria por los motivos expuestos en tal apartado.

Recomendaciones

Estas recomendaciones identifican impactos o riesgos evitables, y cómo se pueden eliminar o reducir a un nivel más aceptable.
El equipo de trabajo que ha llevado a cabo o ha realizado la EIPD decide hacerle a la Asociación Española para la Privacidad Digital (responsable del tratamiento), las siguientes recomendaciones:

- Evaluación continua en el tiempo de los riesgos para los derechos y libertades fundamentales de los ciudadanos (interesados/afectados) en materia de protección de datos de carácter personal. Ya que una detección temprana de nuevos riesgos para la privacidad de las personas, es fundamental para que cuando se les hayan aplicado las medidas de protección necesarias para poder mitigar en la medida de lo posible los mencionados nuevos riesgos, estas medidas protectoras sean eficaces y cumplan su objetivo y su fin último de proteger a las personas de una intrusión en la esfera o el ámbito de su Privacidad personal.

Actualización del proceso de la Evaluación de Impacto

El equipo que ha realizado la EIPD es consciente y tiene presente que muchos proyectos experimentan cambios antes de que finalmente se implementen. A medida que avanza el proyecto, la EIPD debería ser revisada y actualizada o revisada si los desarrollos en el diseño o implementación del proyecto crean nuevos impactos de privacidad que no se habían considerado anteriormente.

Cuándo los cambios a los que se ha hecho mención anteriormente son sustanciales y derivan en nuevos impactos significativos en la privacidad que no fueron considerados en un momento anterior por la EIPD realizada, puede ser recomendable iniciar una nueva EIPD, siguiendo los pasos correspondientes.

12. MEMORANDO DEL DELEGADO DE PROTECCIÓN DE DATOS

Visión del DPO/DPD

El delegado de protección de datos de la Asociación Española para la Privacidad Digital, por imperativo legal, en base al artículo 39.1 c) del RGPD UE 2016/679 ha sido solicitado para llevar a cabo y ofrecer el asesoramiento acerca de la Evaluación de Impacto relativa a la Protección de Datos y para supervisar su aplicación conforme con el artículo 35 del RGPD UE.

Es muy importante ***dejar constancia fehaciente*** de que el DPO de la Asociación responsable del tratamiento, ha participado adecuadamente en el proceso de la EIPD desde la posición y funciones que exigen los artículos 38 y 39 del RGPD UE a dicho responsable del tratamiento.

En relación a los posibles riesgos derivados del tratamiento de datos, para los derechos y libertades fundamentales en materia de protección de datos de las personas físicas, he de expresar y manifestar que la Asociación Española para la Privacidad Digital, ha realizado en mi opinión una valoración bastante real y aproximada de los riesgos potenciales que pueden implicar la ejecución del proyecto corporativo del responsable del tratamiento. Estos potenciales riesgos vienen recogidos con detalle en el Anexo B sobre Listado de Riesgos Detectados, incluido en el Informe final de la EIPD.

Tras un estudio exhaustivo y pormenorizado del análisis realizado por parte de la Asociación Española para la Privacidad Digital, en relación con la probabilidad y la gravedad (impacto) de los riesgos para los derechos y libertades de las personas afectadas, se llega a la conclusión final de que el responsable del tratamiento ha determinado dicha probabilidad y gravedad con referencia directa a la naturaleza, el alcance, el contexto y los fines del tratamiento de datos. Todo ello conforme a lo previsto por el **considerando 76 del RGPD UE**.

Respecto a las potenciales consecuencias negativas que el tratamiento de datos pueda suponer para los interesados, hay que señalar que los riesgos para los derechos y libertades de las personas físicas, de gravedad (impacto) y probabilidad despreciables, pueden deberse al tratamiento de datos que pudieran provocar daños y perjuicios físicos, materiales o inmateriales, en particular en los casos en los que el tratamiento pueda dar lugar a problemas de discriminación, usurpación de identidad o fraude, pérdidas financieras, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, reversión no autorizada de la seudonimización o cualquier otro perjuicio económico o social significativo; en los casos en los que se prive a los interesados de sus derechos y libertades o se les impida ejercer el control

sobre sus datos personales; en los casos en los que se evalúen aspectos personales, en particular el análisis o la predicción de aspectos referidos al comportamiento o hábitos en la navegación web por parte del usuario, con el fin de crear o utilizar perfiles personales; en los casos en los que se traten datos personales de personas vulnerables, en particular niños; o en los casos en los que el tratamiento implique una gran cantidad de datos personales y afecte a un gran número de interesados.

También es importante señalar que si el responsable del tratamiento no toma a tiempo medidas adecuadas, las violaciones de la seguridad de los datos personales pueden entrañar daños y perjuicios físicos, materiales o inmateriales para las personas físicas, como pérdida de control sobre sus datos personales o restricción de sus derechos, discriminación, usurpación de identidad, pérdidas financieras, reversión no autorizada de la seudonimización, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, o cualquier otro perjuicio económico o social significativo para la persona física en cuestión. Por consiguiente, tan pronto como el responsable del tratamiento tenga conocimiento de que se ha producido una violación de la seguridad de los datos personales, el responsable debe, sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, notificar la violación de la seguridad de los datos personales a la autoridad de control competente, a menos que el responsable pueda demostrar, atendiendo al principio de responsabilidad proactiva, la improbabilidad de que la violación de la seguridad de los datos personales entrañe un riesgo para los derechos y las libertades de las personas físicas.
Si dicha notificación no es posible en el plazo de 72 horas, debe acompañarse de una indicación de los motivos de la dilación, pudiendo facilitarse información por fases sin más dilación indebida.

Revisión de los resultados y realimentación de la EIPD

La revisión de una EIPD y su implementación por un tercero independiente como puede ser en este caso por el DPO puede ayudar a asegurar que la misma se ha llevado a cabo adecuadamente y sus recomendaciones implementadas.
Existe la posibilidad de la revisión por parte del DPD del informe final; siendo una tercera persona independiente a la organización o entidad que lo ha elaborado.
Todo ello puede traer consigo beneficios considerables, en lo que se refiere a la transparencia y la confiabilidad del mencionado informe, que al ser valorado y analizado por un tercero, éste puede emitir una opinión con relación al mismo objetiva, y realista de su alcance y contenido, sin las sospechas derivadas del interés que sobre dicho informe final, puede tener el propio responsable del tratamiento, si finalmente lo somete a examen por sus propios recursos y medios.

Si no se lleva a cabo una revisión independiente, sigue habiendo un beneficio para la entidad responsable del tratamiento, al realizar y al mismo tiempo documentar un examen interno, abordando la implementación de las medidas de mitigación y evitación de los riesgos detectados, y que se concretan en las recomendaciones contenidas en el mencionado informe final de EIPD.
Una vez que se han obtenido los resultados de la EIPD, y se han implantado las medidas correctoras y de mejora adoptadas por la alta dirección de la entidad, tal como recomienda la Agencia Española de Protección de Datos, procede que se verifique de manera adecuada la revisión y comprobación de su implantación real y de su eficacia. Tarea de la cual ha procedido a ocuparse el DPO de la Asociación.
De tal objetivo, se desprende que lo decisivo, en todo caso, radica en que cualquier evaluación periódica, y la actualización del modelo EIPD, pase por la constitución de las suficientes garantías y la seguridad jurídica necesaria que garanticen que efectivamente dicho modelo se adapta y ajusta a las necesidades de la Asociación, y mantiene plenamente, la eficacia para la función por la cual fue constituido.
Es importante señalar, que en esta primera revisión de los resultados de la EIPD por parte del DPO, no se ha procedido a introducir, ni a la aprobación de ninguna modificación derivada a consecuencia de las conclusiones obtenidas en el informe final del proyecto de EIPD.
Constituye una cuestión trascendente, que dentro de los planteamientos y de la normativa o regulación que se aplique o se lleve a cabo, que se determine por la propia entidad (la Asociación), la forma en que se va a realizar la EIPD, y la consiguiente actualización en su caso del nuevo modelo sugerido, en este caso por el DPO, a los efectos de que el mismo responda de una manera eficaz a las finalidades por las cuales dicho modelo EIPD ha sido establecido.

En relación a la periodicidad, debe tenerse en cuenta que la actualización y evaluación del modelo EIPD es conveniente que se lleve a cabo al menos cada dos o tres años, dando con ello cumplimiento a las finalidades de asegurar su implementación y efectividad, no siendo obstáculo que por circunstancias importantes y suficientemente justificadas la revisión del sistema se lleve a efecto en cualquier otro plazo, que a juicio de la propia Asociación, le reporte unas ventajas adicionales en su modelo de gestión y funcionamiento.

Tal como sugiere la **Agencia Española de Protección de Datos (AEPD)**, es necesario, examinar el proyecto una vez operativo para verificar que los riesgos detectados se han abordado correctamente, y que no existen otros nuevos que en su momento pasaron desapercibidos o que han surgido posteriormente, lo que llevaría aparejada una nueva iteración de las fases de la EIPD.

Dicha Autoridad de Control Nacional Competente (AEPD), no sólo pretende que la EIPD tenga una incidencia especial en las primeras fases del tratamiento, sino que el debido control sobre el mismo se prolongue y dilate sobre todo el ciclo de vida y de su permanencia en la entidad responsable del tratamiento, así lo afirma, cuando a tal efecto, señala expresamente lo siguiente: "*Por ello, una Evaluación de Impacto, aunque tiene una importancia y un protagonismo especial en las fases iniciales de un proyecto, es un proceso que acompaña al sistema de información, producto o servicio durante todo su ciclo de vida*".

Conclusiones y recomendaciones del DPO/dpd al responsable del tratamiento.

Se desprende de todo la información revisada que obra en la documentación incluida en el Informe de EIPD (apartados y anexos), que la Asociación Española para la Privacidad Digital como responsable del tratamiento, cumple correctamente con las principales obligaciones que recoge el RGPD UE 2016/679 (Reglamento General de Protección de Datos) y la LOPD GDD 3/2018 (Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales), con la legítima pretensión de hacer efectiva la protección de los derechos de los ciudadanos en materia de protección de datos de carácter personal. Todo ello, conforme a lo estipulado por el artículo 35 del RGPD UE.

Dejar constancia asimismo, de que el Informe de EIPD, se ajusta al **Modelo del Informe de EIPD para el sector privado de la Agencia Española de Protección de Datos - AEPD, versión de marzo de 2022).**
Por último el DPO, como recomendación final quiere recordarle a la Asociación Española para la Privacidad Digital que el principio de responsabilidad proactiva que el RGPD UE incorpora en su artículo 24, le obliga a mantener este nivel de cumplimiento a lo largo del tiempo y adaptarlo a las circunstancias cambiantes que puedan concurrir en cada momento, por lo que se recomienda la revisión y actualización en su caso del presente Informe de EIPD cada dos o tres años y, en todo caso, siempre que se produzca alguna modificación en la estructura del tratamiento de datos que pueda implicar cambios sustanciales en la política de protección de datos personales a tales efectos.

13. REFERENCIAS

Procedemos en este apartado a señalar una relación exhaustiva de los documentos utilizados en la ejecución de la EIPD por el equipo de trabajo.
Dichos documentos son los siguientes:

• Considerandos y articulado del RGPD UE 2016/679.

• Articulado de la LOPD GDD 3/2018.

• Informe jurídico de la AEPD sobre el principio de proporcionalidad (2019-09/informe-juridico-rgpd-grabacion-de-imagenes-y-voz-proporcionalidad.pdf)

• Modelo AEPD de informe de evaluación de impacto en la protección de datos (EIPD) para el sector privado. Versión de marzo 2022.

• Guía AEPD para una evaluación de impacto en la protección de datos personales. AEPD - 2014.

• Guía AEPD práctica para las evaluaciones de impacto en la protección de los datos sujetas al RGPD.

• AEPD - Gestión del riesgo y evaluación de impacto en tratamientos de datos personales. Versión Junio 2021.

• AEPD - Guía para la notificación de brechas de datos personales. Versión Mayo de 2021.

• Grupo Protección de Datos artículo 29 - CEPD -
Directrices sobre la evaluación de impacto relativa a la protección de datos (EIPD) y para determinar si el tratamiento "entraña probablemente un alto riesgo" a efectos del Reglamento (UE) 2016/679. WP 248 rev.01.

• Grupo de Trabajo sobre Protección de Datos del artículo 29 - CEPD. Directrices sobre la notificación de las violaciones de la seguridad de los datos personales de acuerdo con el Reglamento 2016/679. WP 250 rev.01.

• Doctrina Jurisprudencial del Tribunal Constitucional (SSTC) sobre el principio de proporcionalidad:
1. STC 66/1995
2. STC 55/1996
3. STC 207/1996
4. STC 37/1998
5. STC 98/2000

ANEXOS

A. Actividades de Tratamiento

Se describen a continuación las operaciones de tratamiento desarrolladas por el responsable, identificando los datos tratados, intervinientes, terceros, sistemas implicados y demás información vinculada al tratamiento.

USUARIOS INSCRITOS EN LA LISTA STOP PUBLICIDAD

DATOS RECOGIDOS PARA LA INSCRIPCIÓN
Datos de carácter identificativo

- Número de identificación (DNI /NIF/NIE/ PASAPORTE)
- Nombre y apellidos
- Dirección (postal, electrónica)
- Teléfono
- Fecha de nacimiento

DATOS RECOGIDOS PARA LA EXCLUSIÓN PUBLICITARIA

- Dirección postal
- Dirección electrónica
- Números de teléfono fijo y móvil
- Dirección email
- Identificación en redes sociales
- Identificación en aplicaciones de mensajería

FINALIDAD
Descripción detallada de la finalidad y usos previstos:

INSCRIPCIÓN EN LA LISTA STOP PUBLICIDAD, EXCLUSIÓN DE CANALES DE PUBLICIDAD, GESTIÓN DE LA LISTA STOP PUBLICIDAD, DATOS DERIVADOS DE LA AUDITORÍA DEL CUMPLIMIENTO DEL REGLAMENTO DE USO DE LA LISTA STOP PUBLICIDAD Y DEL CUMPLIMIENTO NORMATIVO.

ORIGEN Y PROCEDENCIA DE LOS DATOS
Procedencia de los datos

− El propio interesado o su representante

Colectivos o Categorías de interesados

− Usuarios inscritos

− Asociados o miembros

− Padres o tutores

SISTEMA DE TRATAMIENTO
Tipo de Sistema de Tratamiento

− Automatizado

CONSERVACIÓN DE LOS DATOS
Plazo de conservación previsto en función de los diferentes escenarios:
Mientras el sistema de lista esté en funcionamiento:

· **Finalización** (SUPRESIÓN/DESTRUCCIÓN):

El responsable del tratamiento ha articulado debidamente procesos de limitación del uso de los datos personales, incluyendo el bloqueo de los datos (según lo previsto en el artículo 32.2 de la LOPD GDD 3/2018), la supresión y la destrucción de datos. Así:

- Para los **menores de 14 años que fueron inscritos por representante** se prevé que al cumplir los 14 años se inicie automáticamente un proceso de bloqueo (de la inscripción por representante), posterior cancelación o supresión (silencio del mayor de 14 años al efecto), y definitiva destrucción,

por el transcurso de los plazos determinados en el sistema a efectos de obligaciones legales del responsable del tratamiento.

- Para **discapacitados inscritos por representantes** se contempla la necesidad de acreditar el cambio de estado, cuestionar la representación inicial que originó la inscripción en el sistema o proceder a la cancelación por el representante que inicialmente inscribió al afectado, procediendo al bloqueo por rectificación o supresión, cancelación y destrucción definitiva tras el transcurso de los plazos determinados en el sistema a efectos de obligaciones legales del responsable del tratamiento.
- Para los **fallecidos inscritos por representantes** se contempla cuestionar la representación inicial que originó la inscripción en el sistema o proceder a la cancelación por el representante que inicialmente inscribió al afectado. procediendo al bloqueo por rectificación o supresión, cancelación y destrucción definitiva tras el transcurso de los plazos determinados en el sistema a efectos de obligaciones legales del responsable del tratamiento.
- Para **mayores de 14 años que fueron inscritos sin representante** el sistema permite causar baja en el sistema en cualquier momento, tanto para la inscripción como para los datos aportados y que se pretende excluir de la publicidad. Con la baja cursada por el mismo usuario se inicia automáticamente un proceso de bloqueo de los datos de la inscripción, y posterior cancelación o supresión, aunque la definitiva e irreversible destrucción de los datos personales se produce automáticamente por el transcurso de los plazos determinados en el sistema a efectos de obligaciones legales del responsable del tratamiento.

UBICACIÓN

Nombre: ASOCIACIÓN ESPAÑOLA PARA LA PRIVACIDAD DIGITAL **NIF/CIF:** G42631564
Dirección: Calle Médico Temístocles Almagro, N.18, Lc-2
Localidad: Orihuela **Código postal:** 03300
Provincia: Alicante **País:** España
Teléfono: 965306309 **Fax:** **E-mail:** dpo@asociacionepd.es

CESIÓN O COMUNICACIÓN DE DATOS
Categorías de Destinatarios de Cesiones

No se prevén cesiones.

LEGITIMACIÓN Y JUSTIFICACIÓN DEL TRATAMIENTO

Conforme a lo estipulado por el RGPD 2016/679 UE, la legitimación del tratamiento es el consentimiento libremente prestado por el interesado o afectado (artículo 6. 1. a) RGPD). Asimismo la legitimación del tratamiento tiene fundamento en la existencia de intereses legítimos perseguidos por el responsable del tratamiento, cuya satisfacción es necesaria para llevar a cabo el tratamiento de datos (artículo 6. 1. f) RGPD), en base a lo estipulado por el artículo 23 (sistemas de exclusión publicitaria) de la LOPD GDD 3/2018.

Las operaciones de tratamiento desarrolladas en relación a la finalidad del fichero o tratamiento son adecuadas y necesarias. Dichas operaciones de tratamiento cumplen con el principio de proporcionalidad, al derivarse de éstas más beneficios para el responsable que perjuicios para el afectado o interesado.
En el presente caso, la necesidad de llevar a cabo este tratamiento y la legitimación que alega el responsable para el mismo puede justificarse de la siguiente manera de acuerdo con los criterios indicados:
* Idoneidad: se considera que el tratamiento es idóneo para conseguir el objetivo propuesto
* Necesidad: el tratamiento es necesario y no existe otra forma de realizarlo para conseguir el objetivo propuesto
* Proporcionalidad: las actividades de tratamiento son proporcionales a las finalidades previstas

Más información detallada en el apartado de Evaluación de la necesidad y proporcionalidad del tratamiento.

B. Listado de Riesgos Detectados

Nivel de riesgo global calculado: Bajo

- **1. Descripción del Riesgo:**

Acceso y corrección: Las personas no pueden acceder y corregir fácilmente su información personal.

Clasificación de Riesgo: Otro
Afectación Estimada del Riesgo:

• Probabilidad de que se materialice este riesgo: Despreciable

• Impacto o Gravedad en caso de producirse: Despreciable

- **2. Descripción del Riesgo:**

Accesos no autorizados a datos personales.
Clasificación de Riesgo: Deber de Secreto
Afectación Estimada del Riesgo:

• Probabilidad de que se materialice este riesgo: Despreciable

• Impacto o Gravedad en caso de producirse: Despreciable

- **3. Descripción del Riesgo:**

Anonimato y seudonimato: La información personal del individuo NO se recogerá cuando no se requiera (por ejemplo, para proporcionar información).
Clasificación de Riesgo: Otro
Afectación Estimada del Riesgo:

• Probabilidad de que se materialice este riesgo: Despreciable

• Impacto o Gravedad en caso de producirse: Despreciable

- **4. Descripción del Riesgo:**

Calidad de la información: La mala calidad de la información puede conducir a decisiones inapropiadas que tienen un impacto negativo en las personas afectadas.
Clasificación de Riesgo: Otro
Afectación Estimada del Riesgo:

• Probabilidad de que se materialice este riesgo: Despreciable

• Impacto o Gravedad en caso de producirse: Despreciable

- **5. Descripción del Riesgo:**

Carecer de los mecanismos y procedimientos necesarios para detectar cuándo debe notificarse la creación, modificación o cancelación de un tratamiento de datos personales a la AEPD o a la autoridad de protección de datos competente.
Clasificación de Riesgo: Notificación de los Tratamientos
Afectación Estimada del Riesgo:

• Probabilidad de que se materialice este riesgo: Despreciable

• Impacto o Gravedad en caso de producirse: Despreciable

- **6. Descripción del Riesgo:**

Carencia de procedimientos y herramientas para la comunicación de rectificaciones, cancelaciones
u oposiciones a los cesionarios de los datos personales.
Clasificación de Riesgo: Derechos ARCO RGPD
Afectación Estimada del Riesgo:

• Probabilidad de que se materialice este riesgo: Despreciable

• Impacto o Gravedad en caso de producirse: Despreciable

- **7. Descripción del Riesgo:**

Carencia de procedimientos y herramientas para la gestión de los derechos de los afectados.
Clasificación de Riesgo: Derechos ARCO RGPD
Afectación Estimada del Riesgo:

• Probabilidad de que se materialice este riesgo: Despreciable

• Impacto o Gravedad en caso de producirse: Despreciable

- **8. Descripción del Riesgo:**

Deficiencias en la protección de la confidencialidad de la información.
Clasificación de Riesgo: Seguridad
Afectación Estimada del Riesgo:

• Probabilidad de que se materialice este riesgo: Despreciable

• Impacto o Gravedad en caso de producirse: Despreciable

- **9. Descripción del Riesgo:**

Deficiencias organizativas en la gestión del control de accesos.
Clasificación de Riesgo: Seguridad
Afectación Estimada del Riesgo:

• Probabilidad de que se materialice este riesgo: Despreciable

• Impacto o Gravedad en caso de producirse: Despreciable

- **10. Descripción del Riesgo:**

Deficiencias técnicas en el control de accesos que permitan que personas no autorizadas accedan y sustraigan datos personales.
Clasificación de Riesgo: Seguridad
Afectación Estimada del Riesgo:

• Probabilidad de que se materialice este riesgo: Despreciable

• Impacto o Gravedad en caso de producirse: Despreciable

- **11. Descripción del Riesgo:**

Dificultades para conseguir la portabilidad de los datos personales a otros entornos una vez finalizado el contrato.
Clasificación de Riesgo: Tratamientos por Encargo
Afectación Estimada del Riesgo:

• Probabilidad de que se materialice este riesgo: Despreciable

• Impacto o Gravedad en caso de producirse: Despreciable

- **12. Descripción del Riesgo:**

Dificultades para garantizar la legitimidad de la recogida y la cesión de datos personales provenientes de terceros.
Clasificación de Riesgo: Legitimación de los Tratamientos y Cesiones de Datos Personales
Afectación Estimada del Riesgo:

• Probabilidad de que se materialice este riesgo: Despreciable

• Impacto o Gravedad en caso de producirse: Despreciable

- **13. Descripción del Riesgo:**

Dificultar la revocación del consentimiento o la manifestación de la oposición a un tratamiento o cesión.
Clasificación de Riesgo: Legitimación de los Tratamientos y Cesiones de Datos Personales
Afectación Estimada del Riesgo:

• Probabilidad de que se materialice este riesgo: Despreciable

• Impacto o Gravedad en caso de producirse: Despreciable

- **14. Descripción del Riesgo:**

Dificultar o imposibilitar el ejercicio de los derechos de los afectados.
Clasificación de Riesgo: Derechos ARCO RGPD
Afectación Estimada del Riesgo:

• Probabilidad de que se materialice este riesgo: Despreciable

• Impacto o Gravedad en caso de producirse: Despreciable

- **15. Descripción del Riesgo:**

Divulgación: La desidentificación de la información personal antes de la divulgación no puede impedir la reidentificación.
Clasificación de Riesgo: Otro
Afectación Estimada del Riesgo:

• Probabilidad de que se materialice este riesgo: Despreciable

• Impacto o Gravedad en caso de producirse: Despreciable

- **16. Descripción del Riesgo:**

En el entorno web, ubicar la información en materia de protección de datos (políticas de privacidad, cláusulas informativas) en lugares de difícil localización o diseminada en diversas secciones y
apartados que hagan muy difícil su acceso conjunto y detallado.
Clasificación de Riesgo: Transparencia de los Tratamientos
Afectación Estimada del Riesgo:

• Probabilidad de que se materialice este riesgo: Despreciable

• Impacto o Gravedad en caso de producirse: Despreciable

- **17. Descripción del Riesgo:**

Enriquecer los datos personales de forma no prevista en las finalidades iniciales y sin la información adecuada a los afectados al realizar una interconexión con otras bases de datos de la organización o de terceros, en particular, la re-identificación de información disociada.
Clasificación de Riesgo: Legitimación de los Tratamientos y Cesiones de Datos Personales
Afectación Estimada del Riesgo:

• Probabilidad de que se materialice este riesgo: Despreciable

• Impacto o Gravedad en caso de producirse: Despreciable

- **18. Descripción del Riesgo:**

Existencia de errores técnicos u organizativos que propicien la falta de integridad de la información, permitiendo la existencia de registros duplicados con informaciones diferentes o contradictorias, lo que puede derivar en la toma de decisiones erróneas.
Clasificación de Riesgo: Calidad de los Datos
Afectación Estimada del Riesgo:

• Probabilidad de que se materialice este riesgo: Despreciable

• Impacto o Gravedad en caso de producirse: Despreciable

- **19. Descripción del Riesgo:**

Existencia de incentivos para obtener la información ilícitamente por su valor (económico, político, social, laboral, etc.) para terceros no autorizados.
Clasificación de Riesgo: Seguridad
Afectación Estimada del Riesgo:

• Probabilidad de que se materialice este riesgo: Despreciable

• Impacto o Gravedad en caso de producirse: Despreciable

- **20. Descripción del Riesgo:**

Falta de conocimiento experto sobre protección de datos y de canales de comunicación con los afectados.
Clasificación de Riesgo: General
Afectación Estimada del Riesgo:

• Probabilidad de que se materialice este riesgo: Despreciable

• Impacto o Gravedad en caso de producirse: Despreciable

- **21. Descripción del Riesgo:**

Falta de diligencia (o dificultad para demostrarla) en la elección de encargado de tratamiento.
Clasificación de Riesgo: Tratamientos por Encargo
Afectación Estimada del Riesgo:

• Probabilidad de que se materialice este riesgo: Despreciable

• Impacto o Gravedad en caso de producirse: Despreciable

- **22. Descripción del Riesgo:**

Falta de formación del personal sobre las medidas de seguridad que están obligados a adoptar y sobre las consecuencias que se pueden derivar de no hacerlo.
Clasificación de Riesgo: Seguridad
Afectación Estimada del Riesgo:

• Probabilidad de que se materialice este riesgo: Despreciable

• Impacto o Gravedad en caso de producirse: Despreciable

- **23. Descripción del Riesgo:**

Garantías insuficientes para el uso de datos personales con fines históricos, científicos o estadísticos.
Clasificación de Riesgo: Calidad de los Datos
Afectación Estimada del Riesgo:

• Probabilidad de que se materialice este riesgo: Despreciable

• Impacto o Gravedad en caso de producirse: Despreciable

- **24. Descripción del Riesgo:**

Gestión deficiente de las subcontrataciones e insuficiente control sobre encargados y subcontratistas y, en particular, dificultades para comprobar o supervisar que el encargado y los subcontratistas cumplen las instrucciones y, especialmente, las medidas de seguridad.
Clasificación de Riesgo: Tratamientos por Encargo
Afectación Estimada del Riesgo:

• Probabilidad de que se materialice este riesgo: Despreciable

• Impacto o Gravedad en caso de producirse: Despreciable

- **25. Descripción del Riesgo:**

Impedir la utilización anónima de un determinado producto o servicio cuando la identificación del usuario no resulta indispensable.
Clasificación de Riesgo: Legitimación de los Tratamientos y Cesiones de Datos Personales
Afectación Estimada del Riesgo:

• Probabilidad de que se materialice este riesgo: Despreciable

• Impacto o Gravedad en caso de producirse: Despreciable

- **26. Descripción del Riesgo:**

Imposibilidad de atribuir a usuarios identificados todas las acciones que se llevan a cabo en un sistema de información.
Clasificación de Riesgo: Seguridad
Afectación Estimada del Riesgo:

• Probabilidad de que se materialice este riesgo: Despreciable

• Impacto o Gravedad en caso de producirse: Despreciable

- **27. Descripción del Riesgo:**

Inexistencia de contrato o elaboración de un contrato incorrecto que no refleje todos los apartados necesarios y las garantías adecuadas.
Clasificación de Riesgo: Tratamientos por Encargo
Afectación Estimada del Riesgo:

• Probabilidad de que se materialice este riesgo: Despreciable

• Impacto o Gravedad en caso de producirse: Despreciable

- **28. Descripción del Riesgo:**

Inexistencia del responsable de seguridad o deficiente definición de sus funciones y competencias.

Clasificación de Riesgo: Seguridad
Afectación Estimada del Riesgo:

• Probabilidad de que se materialice este riesgo: Despreciable

• Impacto o Gravedad en caso de producirse: Despreciable

- **29. Descripción del Riesgo:**

No definición o deficiencias en los procedimientos para comunicar al responsable el ejercicio de los derechos de los interesados realizados ante los encargados de tratamiento.
Clasificación de Riesgo: Tratamientos por Encargo
Afectación Estimada del Riesgo:

• Probabilidad de que se materialice este riesgo: Despreciable

• Impacto o Gravedad en caso de producirse: Despreciable

- **30. Descripción del Riesgo:**

Notificación de la obtención de la información: La notificación de la obtención de la información puede no ser accesible para todos los interesados o afectados, por ejemplo, aquellos procedentes de diversos orígenes culturales y lingüísticos.
Clasificación de Riesgo: Otro
Afectación Estimada del Riesgo:

• Probabilidad de que se materialice este riesgo: Despreciable

• Impacto o Gravedad en caso de producirse: Despreciable

- **31. Descripción del Riesgo:**

Notificación de obtención de la información: El responsable del tratamiento podría no proporcionar el aviso de obtención de la información a todos los individuos, por ejemplo, aquellos que utilizan canales de comunicación no estándar.
Clasificación de Riesgo: Otro
Afectación Estimada del Riesgo:

• Probabilidad de que se materialice este riesgo: Despreciable

• Impacto o Gravedad en caso de producirse: Despreciable

- **32. Descripción del Riesgo:**

Obtención de la información: La información personal podría ser recolectada sin un propósito claro, lo que podría aumentar el riesgo de usos no autorizados y divulgaciones.
Clasificación de Riesgo: Otro
Afectación Estimada del Riesgo:

• Probabilidad de que se materialice este riesgo: Despreciable

• Impacto o Gravedad en caso de producirse: Despreciable

- **33. Descripción del Riesgo:**

Obtención, uso o divulgación: El consentimiento para la recopilación, uso o divulgación de información puede no ser válida.
Clasificación de Riesgo: Otro
Afectación Estimada del Riesgo:

• Probabilidad de que se materialice este riesgo: Despreciable

• Impacto o Gravedad en caso de producirse: Despreciable

- **34. Descripción del Riesgo:**

Obtener un consentimiento dudoso, viciado o inválido para el tratamiento o cesión de datos personales.
Clasificación de Riesgo: Legitimación de los Tratamientos y Cesiones de Datos Personales
Afectación Estimada del Riesgo:

• Probabilidad de que se materialice este riesgo: Despreciable

• Impacto o Gravedad en caso de producirse: Despreciable

- **35. Descripción del Riesgo:**

Pérdida de competitividad del servicio derivada de los daños reputacionales causados por una deficiente gestión de la privacidad de las personas.
Clasificación de Riesgo: General
Afectación Estimada del Riesgo:

• Probabilidad de que se materialice este riesgo: Despreciable

• Impacto o Gravedad en caso de producirse: Despreciable

- **36. Descripción del Riesgo:**

Pérdidas económicas y daños reputacionales derivados del incumplimiento de legislaciones sectoriales con incidencia en la protección de datos personales a las que pueda estar sujeto el responsable del tratamiento.
Clasificación de Riesgo: General
Afectación Estimada del Riesgo:

• Probabilidad de que se materialice este riesgo: Despreciable

• Impacto o Gravedad en caso de producirse: Despreciable

- **37. Descripción del Riesgo:**

Pérdidas económicas, pérdida de clientes y daños reputacionales derivados de la carencia de medidas de seguridad adecuadas o de la ineficacia de las mismas, en particular, cuando se producen pérdidas de datos personales.
Clasificación de Riesgo: General
Afectación Estimada del Riesgo:

• Probabilidad de que se materialice este riesgo: Despreciable

• Impacto o Gravedad en caso de producirse: Despreciable

- **38. Descripción del Riesgo:**

Recoger datos personales sin proporcionar la debida información o de manera fraudulenta o no autorizada (cookies, ubicación geográfica, comportamiento, hábitos de navegación, etc...).
Clasificación de Riesgo: Transparencia de los Tratamientos
Afectación Estimada del Riesgo:

• Probabilidad de que se materialice este riesgo: Despreciable

• Impacto o Gravedad en caso de producirse: Despreciable

- **39. Descripción del Riesgo:**

Redactar la información en materia de protección de datos en un lenguaje oscuro e impreciso que impida que los afectados se hagan una idea clara y ajustada de los elementos esenciales que deben conocer para que exista un tratamiento leal de sus datos personales.
Clasificación de Riesgo: Transparencia de los Tratamientos
Afectación Estimada del Riesgo:

• Probabilidad de que se materialice este riesgo: Despreciable

• Impacto o Gravedad en caso de producirse: Despreciable

- **40. Descripción del Riesgo:**

Seguridad de la información: El responsable del tratamiento u organización no tiene estándares básicos de seguridad de la información en su lugar.
Clasificación de Riesgo: Otro
Afectación Estimada del Riesgo:

• Probabilidad de que se materialice este riesgo: Despreciable

• Impacto o Gravedad en caso de producirse: Despreciable

- **41. Descripción del Riesgo:**

Seguridad de la información: La información se guarda en dispositivos de almacenamiento extraíbles o externos, aumentando el riesgo de pérdida accidental de información personal.
Clasificación de Riesgo: Otro
Afectación Estimada del Riesgo:

• Probabilidad de que se materialice este riesgo: Despreciable

• Impacto o Gravedad en caso de producirse: Despreciable

- **42. Descripción del Riesgo:**

Solicitar datos o categorías de datos innecesarios para las finalidades del nuevo sistema, producto o servicio.
Clasificación de Riesgo: Calidad de los Datos
Afectación Estimada del Riesgo:

• Probabilidad de que se materialice este riesgo: Despreciable

• Impacto o Gravedad en caso de producirse: Despreciable

- **43. Descripción del Riesgo:**

Tratar datos personales cuando no es necesario para la finalidad perseguida.
Clasificación de Riesgo: Legitimación de los Tratamientos y Cesiones de Datos Personales
Afectación Estimada del Riesgo:

• Probabilidad de que se materialice este riesgo: Despreciable

• Impacto o Gravedad en caso de producirse: Despreciable

- **44. Descripción del Riesgo:**

Uso de identificadores que revelan información del afectado.
Clasificación de Riesgo: Seguridad
Afectación Estimada del Riesgo:

• Probabilidad de que se materialice este riesgo: Despreciable

• Impacto o Gravedad en caso de producirse: Despreciable

- **45. Descripción del Riesgo:**

Uso o divulgación: Los individuos pueden ser sorprendidos o molestos por un uso secundario o revelación, resultando en quejas de privacidad y/o publicidad negativa.
Clasificación de Riesgo: Otro
Afectación Estimada del Riesgo:

• Probabilidad de que se materialice este riesgo: Despreciable

• Impacto o Gravedad en caso de producirse: Despreciable

- **46. Descripción del Riesgo:**

Utilizar cookies de seguimiento u otros mecanismos de rastreo sin obtener un consentimiento válido tras una información adecuada.
Clasificación de Riesgo: Legitimación de los Tratamientos y Cesiones de Datos Personales
Afectación Estimada del Riesgo:

• Probabilidad de que se materialice este riesgo: Despreciable

• Impacto o Gravedad en caso de producirse: Despreciable

- **47. Descripción del Riesgo:**

Violaciones de la confidencialidad de los datos personales por parte de los empleados de la organización.
Clasificación de Riesgo: Deber de Secreto
Afectación Estimada del Riesgo:

• Probabilidad de que se materialice este riesgo: Despreciable

• Impacto o Gravedad en caso de producirse: Despreciable

C. Listado de Medidas de Protección

Riesgo residual tras aplicar las medidas de protección: Bajo

1.- Medida de Protección: Comunicación auditable y clara de las responsabilidades del personal en relación con el cumplimiento de las políticas y las medidas de seguridad así como de las sanciones aparejadas al incumplimiento de las mismas.

Categoría: Reducción del riesgo
Riesgo por el que se adopta esta medida:
Falta de formación del personal sobre las medidas de seguridad que están obligados a adoptar y sobre las consecuencias que se pueden derivar de no hacerlo.
Efectividad Estimada de la Medida:

• Probabilidad del riesgo tras aplicar esta medida: Despreciable

• Impacto del riesgo tras aplicar esta medida: Despreciable

2.- Medida de Protección: Comunicación auditable y clara de las responsabilidades del personal en relación con el cumplimiento de las políticas y las medidas de seguridad así como de las sanciones aparejadas al incumplimiento de las mismas.

Categoría: Reducción del riesgo
Riesgo por el que se adopta esta medida:
Existencia de incentivos para obtener la información ilícitamente por su valor (económico, político,
social, laboral, etc.) para terceros no autorizados.
Efectividad Estimada de la Medida:

• Probabilidad del riesgo tras aplicar esta medida: Despreciable

• Impacto del riesgo tras aplicar esta medida: Despreciable

3.- Medida de Protección: Construir canales seguros y con verificación de identidad para la distribución de información de seguridad (códigos de usuario, contraseñas, etc...).

Categoría: Reducción del riesgo
Riesgo por el que se adopta esta medida:
Deficiencias organizativas en la gestión del control de accesos.
Efectividad Estimada de la Medida:

• Probabilidad del riesgo tras aplicar esta medida: Despreciable

• Impacto del riesgo tras aplicar esta medida: Despreciable

4.- Medida de Protección:
Construir canales seguros y con verificación de identidad para la distribución de información de seguridad (códigos de usuario, contraseñas, etc...).

Categoría: Reducción del riesgo
Riesgo por el que se adopta esta medida:
Deficiencias técnicas en el control de accesos que permitan que personas no autorizadas accedan y sustraigan datos personales.
Efectividad Estimada de la Medida:

• Probabilidad del riesgo tras aplicar esta medida: Despreciable

• Impacto del riesgo tras aplicar esta medida: Despreciable

5.- Medida de Protección:
Definición de procedimientos de gestión y puesta en marcha de herramientas que garanticen la comunicación de rectificaciones, cancelaciones y oposiciones a las organizaciones a las que se hayan cedido los datos personales de que se trate.

Categoría: Reducción del riesgo
Riesgo por el que se adopta esta medida:
Carencia de procedimientos y herramientas para la comunicación de rectificaciones, cancelaciones
u oposiciones a los cesionarios de los datos personales.
Efectividad Estimada de la Medida:

• Probabilidad del riesgo tras aplicar esta medida: Despreciable

• Impacto del riesgo tras aplicar esta medida: Despreciable

6.- Medida de Protección:
El responsable del tratamiento tiene que asegurarse de que el aviso de recaudación de datos sea coherente y accesible en todos los métodos de recolección, incluidos formularios impresos, formularios en línea y por teléfono. Hay que proporcionar una notificación posterior a la obtención de la información en la que no sea posible notificar antes o en el momento de dicha obtención.

Categoría: Reducción del riesgo
Riesgo por el que se adopta esta medida:
Notificación de obtención de la información: El responsable del tratamiento podría no proporcionar el
aviso de obtención de la información a todos los individuos, por ejemplo, aquellos que utilizan
canales de comunicación no estándar.
Efectividad Estimada de la Medida:

• Probabilidad del riesgo tras aplicar esta medida: Despreciable

• Impacto del riesgo tras aplicar esta medida: Despreciable

7.- Medida de Protección:
Establecer mecanismos de registro de acciones sobre los datos personales o logging así como herramientas fiables y flexibles de explotación de los ficheros de auditoría resultantes.

Categoría: Reducción del riesgo
Riesgo por el que se adopta esta medida:

Imposibilidad de atribuir a usuarios identificados todas las acciones que se llevan a cabo en un
sistema de información.
Efectividad Estimada de la Medida:

• Probabilidad del riesgo tras aplicar esta medida: Despreciable

• Impacto del riesgo tras aplicar esta medida: Despreciable

8.- Medida de Protección:
Establecer mecanismos y procedimientos de concienciación sobre la obligación de guardar secreto sobre los datos personales que se conozcan en el ejercicio de las funciones profesionales.
Categoría: Reducción del riesgo
Riesgo por el que se adopta esta medida:
Accesos no autorizados a datos personales.
Efectividad Estimada de la Medida:

• Probabilidad del riesgo tras aplicar esta medida: Despreciable

• Impacto del riesgo tras aplicar esta medida: Despreciable

9.- Medida de Protección:
Establecer mecanismos y procedimientos que garanticen el control sobre las actividades de los subcontratistas que puedan elegir un encargado de tratamiento.
Categoría: Reducción del riesgo
Riesgo por el que se adopta esta medida:
Gestión deficiente de las subcontrataciones e insuficiente control sobre encargados y subcontratistas y, en particular, dificultades para comprobar o supervisar que el encargado y los
subcontratistas cumplen las instrucciones y, especialmente, las medidas de seguridad.
Efectividad Estimada de la Medida:

• Probabilidad del riesgo tras aplicar esta medida: Despreciable

• Impacto del riesgo tras aplicar esta medida: Despreciable

10.- Medida de Protección:
Establecer mecanismos y procedimientos que permitan resolver de una manera rápida y eficaz los errores que se hayan podido cometer.
Categoría: Reducción del riesgo
Riesgo por el que se adopta esta medida:
Existencia de errores técnicos u organizativos que propicien la falta de integridad de la información,
permitiendo la existencia de registros duplicados con informaciones diferentes o contradictorias, lo
que puede derivar en la toma de decisiones erróneas.
Efectividad Estimada de la Medida:

• Probabilidad del riesgo tras aplicar esta medida: Despreciable

• Impacto del riesgo tras aplicar esta medida: Despreciable

11.- Medida de Protección:
Establecer medidas técnicas y organizativas que garanticen la portabilidad.
Categoría: Reducción del riesgo
Riesgo por el que se adopta esta medida:
Dificultades para conseguir la portabilidad de los datos personales a otros entornos una vez

finalizado el contrato.

Efectividad Estimada de la Medida:

• Probabilidad del riesgo tras aplicar esta medida: Despreciable

• Impacto del riesgo tras aplicar esta medida: Despreciable

12.- Medida de Protección:

Establecer procedimientos para la revisión sistemática y obligatoria de los distintos formularios de recogida de datos personales que garanticen el cumplimiento de la política de privacidad, la homogeneidad de la información y, en particular, que se ofrezca la información adecuada.

Categoría: Reducción del riesgo

Riesgo por el que se adopta esta medida:

Recoger datos personales sin proporcionar la debida información o de manera fraudulenta o no
autorizada (cookies, ubicación geográfica, comportamiento, hábitos de navegación, etc...).

Efectividad Estimada de la Medida:

• Probabilidad del riesgo tras aplicar esta medida: Despreciable

• Impacto del riesgo tras aplicar esta medida: Despreciable

13.- Medida de Protección:

Establecer procedimientos que garanticen que siempre que se recurre a un encargado de tratamiento se firma el correspondiente contrato en los términos establecidos por la legislación de protección de datos.

Categoría: Reducción del riesgo

Riesgo por el que se adopta esta medida:

Inexistencia de contrato o elaboración de un contrato incorrecto que no refleje todos los apartados
necesarios y las garantías adecuadas.

Efectividad Estimada de la Medida:

• Probabilidad del riesgo tras aplicar esta medida: Despreciable

• Impacto del riesgo tras aplicar esta medida: Despreciable

14.- Medida de Protección:

Establecimiento de sanciones disuasorias para los empleados que violen la confidencialidad de los datos personales y comunicación clara y completa de las mismas.

Categoría: Reducción del riesgo

Riesgo por el que se adopta esta medida:

Violaciones de la confidencialidad de los datos personales por parte de los empleados de la
organización.

Efectividad Estimada de la Medida:

• Probabilidad del riesgo tras aplicar esta medida: Despreciable

• Impacto del riesgo tras aplicar esta medida: Despreciable

15.- Medida de Protección:

Estructurar y proporcionar la información sobre los tratamientos de datos personales en varios niveles fácilmente accesibles por los afectados y valorar la utilización de iconos u otros sistemas
gráficos para facilitar su comprensión.

Categoría: Reducción del riesgo
Riesgo por el que se adopta esta medida:
En el entorno web, ubicar la información en materia de protección de datos (políticas de privacidad,
cláusulas informativas) en lugares de difícil localización o diseminada en diversas secciones y
apartados que hagan muy difícil su acceso conjunto y detallado.
Efectividad Estimada de la Medida:

• Probabilidad del riesgo tras aplicar esta medida: Despreciable

• Impacto del riesgo tras aplicar esta medida: Despreciable

16.- Medida de Protección:
Evitar el uso de cookies u otros mecanismos de rastreo y monitorización. En caso de que se utilicen, preferir las menos invasivas (cookies propias frente a cookies de terceros, cookies de sesión frente a cookies permanentes, periodos cortos de caducidad de las cookies, etc...).
Categoría: Reducción del riesgo
Riesgo por el que se adopta esta medida:
Utilizar cookies de seguimiento u otros mecanismos de rastreo sin obtener un consentimiento válido
tras una información adecuada.
Efectividad Estimada de la Medida:

• Probabilidad del riesgo tras aplicar esta medida: Despreciable

• Impacto del riesgo tras aplicar esta medida: Despreciable

17.- Medida de Protección:
Evitar el uso de identificadores ligados a elementos de autenticación, como números de tarjetas de crédito o similares, ya que favorecen el fraude en la identificación e incluso la suplantación de identidad.
Categoría: Reducción del riesgo
Riesgo por el que se adopta esta medida:
Uso de identificadores que revelan información del afectado.
Efectividad Estimada de la Medida:

• Probabilidad del riesgo tras aplicar esta medida: Despreciable

• Impacto del riesgo tras aplicar esta medida: Despreciable

18.- Medida de Protección:
Formación apropiada del personal sobre protección de datos en el sector específico de que se trate.
Categoría: Reducción del riesgo
Riesgo por el que se adopta esta medida:
Pérdidas económicas y daños reputacionales derivados del incumplimiento de la legislación sobre protección de datos personales.
Efectividad Estimada de la Medida:

• Probabilidad del riesgo tras aplicar esta medida: Despreciable

• Impacto del riesgo tras aplicar esta medida: Despreciable

19.- Medida de Protección:
Formación apropiada del personal sobre protección de datos en el sector específico de que se trate.
Categoría: Reducción del riesgo
Riesgo por el que se adopta esta medida:

Pérdidas económicas y daños reputacionales derivados del incumplimiento de legislaciones
sectoriales con incidencia en la protección de datos personales a las que pueda estar sujeto el
responsable del tratamiento.

Efectividad Estimada de la Medida:

• Probabilidad del riesgo tras aplicar esta medida: Despreciable

• Impacto del riesgo tras aplicar esta medida: Despreciable

20.- Medida de Protección:

Formación apropiada del personal sobre protección de datos en el sector específico de que se trate.

Categoría: Reducción del riesgo

Riesgo por el que se adopta esta medida:

Pérdida de competitividad del producto o servicio derivada de los daños reputacionales causados por una deficiente gestión de la privacidad de las personas.

Efectividad Estimada de la Medida:

• Probabilidad del riesgo tras aplicar esta medida: Despreciable

• Impacto del riesgo tras aplicar esta medida: Despreciable

21.- Medida de Protección:

Formación apropiada del personal sobre protección de datos.

Categoría: Reducción del riesgo

Riesgo por el que se adopta esta medida:

Pérdidas económicas, pérdida de clientes y daños reputacionales derivados de la carencia de medidas de seguridad adecuadas o de la ineficacia de las mismas, en particular, cuando se producen pérdidas de datos personales.

Efectividad Estimada de la Medida:

• Probabilidad del riesgo tras aplicar esta medida: Despreciable

• Impacto del riesgo tras aplicar esta medida: Despreciable

22.- Medida de Protección:

Formación apropiada del personal sobre protección de datos.

Categoría: Reducción del riesgo

Riesgo por el que se adopta esta medida:

Falta de conocimiento experto sobre protección de datos y de canales de comunicación con los afectados.

Efectividad Estimada de la Medida:

• Probabilidad del riesgo tras aplicar esta medida: Despreciable

• Impacto del riesgo tras aplicar esta medida: Despreciable

23.- Medida de Protección:

Hay que asegurarse de que el aviso de recopilación está disponible en una variedad de formatos y un rango apropiado de idiomas para el grupo objetivo.

Categoría: Reducción del riesgo

Riesgo por el que se adopta esta medida:

Notificación de la obtención de la información: La notificación de la obtención de la información puede no ser accesible para todos los interesados o afectados, por ejemplo, aquellos procedentes de diversos orígenes culturales y lingüísticos.

Efectividad Estimada de la Medida:

• Probabilidad del riesgo tras aplicar esta medida: Despreciable

• Impacto del riesgo tras aplicar esta medida: Despreciable

24.- Medida de Protección:
Hay que asegurarse de que el responsable del tratamiento ha identificado y documentado claramente los propósitos para los que va a recopilar y utilizar información personal y que la personas que forman parte de la organización son conscientes de estos propósitos.

Categoría: Reducción del riesgo
Riesgo por el que se adopta esta medida:
Obtención de la información: La información personal podría ser recolectada sin un propósito claro, lo que podría aumentar el riesgo de usos no autorizados y divulgaciones.
Efectividad Estimada de la Medida:

• Probabilidad del riesgo tras aplicar esta medida: Despreciable

• Impacto del riesgo tras aplicar esta medida: Despreciable

25.- Medida de Protección:
Hay que comprobar la fiabilidad de las herramientas utilizadas para recopilar o procesar información personal. Hay que considerar el establecimiento de controles periódicos de herramientas y procedimientos para el procesamiento de datos humanos. También hay que identificar y documentar los procedimientos para la frecuencia con la que la información personal será revisada y actualizada.

Categoría: Reducción del riesgo
Riesgo por el que se adopta esta medida:
Calidad de la información: La mala calidad de la información puede conducir a decisiones
inapropiadas que tienen un impacto negativo en las personas afectadas.
Efectividad Estimada de la Medida:

• Probabilidad del riesgo tras aplicar esta medida: Despreciable

• Impacto del riesgo tras aplicar esta medida: Despreciable

26.- Medida de Protección:
Hay que considerar si el responsable del tratamiento puede usar información que no identifique a las personas. Si es necesario distinguir entre diferentes personas, el responsable del tratamiento tiene que considerar si puede usar seudónimos en su lugar.

Categoría: Reducción del riesgo
Riesgo por el que se adopta esta medida:
Anonimato y seudonimato: La información personal del individuo se recogerá cuando no se requiera (por ejemplo, para proporcionar información).
Efectividad Estimada de la Medida:

• Probabilidad del riesgo tras aplicar esta medida: Despreciable

• Impacto del riesgo tras aplicar esta medida: Despreciable

27.- Medida de Protección:
Hay que controlar el uso de dispositivos portátiles de almacenamiento a través de políticas de organización y de controles técnicos.

Categoría: Reducción del riesgo
Riesgo por el que se adopta esta medida:
Seguridad de la información: La información se guarda en dispositivos de almacenamiento extraíbles o externos, aumentando el riesgo de pérdida accidental de información personal.

Efectividad Estimada de la Medida:

• Probabilidad del riesgo tras aplicar esta medida: Despreciable

• Impacto del riesgo tras aplicar esta medida: Despreciable

28.- Medida de Protección:
Hay que identificar cómo los procedimientos de acceso y corrección pueden hacerse más sencillos. Hay que considerar la existencia del derecho a proporcionar a las personas acceso rutinario a su información personal.

Categoría: Reducción del riesgo
Riesgo por el que se adopta esta medida:
Acceso y corrección: Las personas no pueden acceder y corregir fácilmente su información personal.
Efectividad Estimada de la Medida:

• Probabilidad del riesgo tras aplicar esta medida: Despreciable

• Impacto del riesgo tras aplicar esta medida: Despreciable

29.- Medida de Protección:
Hay que realizar más consultas con los interesados para probar las expectativas de la comunidad acerca de sus usos y divulgaciones propuestas. Hay que considerar si es posible buscar consentimiento para usos secundarios y divulgaciones.

Categoría: Reducción del riesgo
Riesgo por el que se adopta esta medida:
Uso o divulgación: Los individuos pueden ser sorprendidos o molestos por un uso secundario o revelación, resultando en quejas de privacidad y/o publicidad negativa.
Efectividad Estimada de la Medida:

• Probabilidad del riesgo tras aplicar esta medida: Despreciable

• Impacto del riesgo tras aplicar esta medida: Despreciable

30.- Medida de Protección:
Hay que revisar el proceso por el cual el responsable del tratamiento planea buscar el consentimiento. Hay que asegurar que el consentimiento será verdaderamente voluntario, informado, actual y específico, y dado por una persona con la capacidad de dar su consentimiento.

Categoría: Reducción del riesgo
Riesgo por el que se adopta esta medida:
Obtención, uso o divulgación: El consentimiento para la recopilación, uso o divulgación de información puede no ser válido.
Efectividad Estimada de la Medida:

• Probabilidad del riesgo tras aplicar esta medida: Despreciable

• Impacto del riesgo tras aplicar esta medida: Despreciable

31.- Medida de Protección:
Hay que revisar los postulados de la seguridad de la información e identificar qué pasos adicionales debe tomar el responsable del tratamiento para asegurar la protección de la información personal.

Categoría: Reducción del riesgo
Riesgo por el que se adopta esta medida:
Seguridad de la información: El responsable del tratamiento u organización no tiene estándares básicos de seguridad de la información en su lugar.
Efectividad Estimada de la Medida:

• Probabilidad del riesgo tras aplicar esta medida: Despreciable

• Impacto del riesgo tras aplicar esta medida: Despreciable

32.- Medida de Protección:
Hay que revisar los procedimientos de des-identificación para asegurar que se eliminen los detalles suficientes para que el destinatario de la información no pueda volver a identificarlo o combinarlo con otra información para establecer la identidad de un individuo.

Categoría: Reducción del riesgo
Riesgo por el que se adopta esta medida:
Divulgación: La desidentificación de la información personal antes de la divulgación no puede impedir la reidentificación.
Efectividad Estimada de la Medida:

• Probabilidad del riesgo tras aplicar esta medida: Despreciable

• Impacto del riesgo tras aplicar esta medida: Despreciable

33.- Medida de Protección:
Implantar políticas de privacidad claras, concisas y fácilmente accesibles por los afectados, en formatos estandarizados, y con uniformidad en todos los entornos de la organización.

Categoría: Reducción del riesgo
Riesgo por el que se adopta esta medida:
Redactar la información en materia de protección de datos en un lenguaje oscuro e impreciso que impida que los afectados se hagan una idea clara y ajustada de los elementos esenciales que deben conocer para que exista un tratamiento leal de sus datos personales.
Efectividad Estimada de la Medida:

• Probabilidad del riesgo tras aplicar esta medida: Despreciable

• Impacto del riesgo tras aplicar esta medida: Despreciable

34.- Medida de Protección:
Implantar sistemas que permitan a los afectados acceder de forma fácil, directa y con la apropiada seguridad a sus datos personales, así como ejercitar sus derechos.

Categoría: Reducción del riesgo
Riesgo por el que se adopta esta medida:
Dificultar o imposibilitar el ejercicio de los derechos de los afectados.
Efectividad Estimada de la Medida:

• Probabilidad del riesgo tras aplicar esta medida: Despreciable

• Impacto del riesgo tras aplicar esta medida: Despreciable

35.- Medida de Protección:
Implantar sistemas que permitan a los afectados acceder de forma fácil, directa y con la apropiada seguridad a sus datos personales, así como ejercitar sus derechos.

Categoría: Reducción del riesgo
Riesgo por el que se adopta esta medida:
Carencia de procedimientos y herramientas para la gestión de los derechos de los afectados.
Efectividad Estimada de la Medida:

• Probabilidad del riesgo tras aplicar esta medida: Despreciable

• Impacto del riesgo tras aplicar esta medida: Despreciable

36.- Medida de Protección:
Incluir en el contrato de encargo la obligación de comunicar al responsable las peticiones de ejercicio de los derechos de los interesados.

Categoría: Reducción del riesgo
Riesgo por el que se adopta esta medida:
No definición o deficiencias en los procedimientos para comunicar al responsable el ejercicio de los
derechos ARCO RGPD realizados ante los encargados de tratamiento.
Efectividad Estimada de la Medida:

• Probabilidad del riesgo tras aplicar esta medida: Despreciable

• Impacto del riesgo tras aplicar esta medida: Despreciable

37.- Medida de Protección:
Instalar herramientas de hardware o software que ayuden a una gestión eficaz de la seguridad y los compromisos u obligaciones legales de la organización en el área de la protección de datos personales.
Categoría: Reducción del riesgo
Riesgo por el que se adopta esta medida:
Deficiencias en la protección de la confidencialidad de la información.
Efectividad Estimada de la Medida:

• Probabilidad del riesgo tras aplicar esta medida: Despreciable

• Impacto del riesgo tras aplicar esta medida: Despreciable

38.- Medida de Protección:
Nombramiento del responsable de seguridad y establecimiento por parte de la dirección de sus funciones, competencias y atribuciones en el desarrollo y gestión de los proyectos.
Categoría: Reducción del riesgo
Riesgo por el que se adopta esta medida:
Inexistencia del responsable de seguridad o deficiente definición de sus funciones y competencias.
Efectividad Estimada de la Medida:

• Probabilidad del riesgo tras aplicar esta medida: Despreciable

• Impacto del riesgo tras aplicar esta medida: Despreciable

39.- Medida de Protección:
Nombrar un Delegado de Protección de Datos o Data Protection Officer (que dependiendo del tamaño de la organización será una persona o un departamento interno o externo) para ocuparse de todas las cuestiones relativas a la privacidad dentro de la organización y contar con asesoramiento cualificado. Si se procede a este nombramiento, el Delegado de Protección de Datos puede hacerse cargo también de la interlocución con los afectados.
Categoría: Reducción del riesgo
Riesgo por el que se adopta esta medida:
Incorporación tardía de los expertos en protección de datos (en particular, del delegado de
protección de datos o DPO) al proyecto o definición deficiente de sus funciones y competencias.
Efectividad Estimada de la Medida:

• Probabilidad del riesgo tras aplicar esta medida: Despreciable

• Impacto del riesgo tras aplicar esta medida: Despreciable

40.- Medida de Protección:
Permitir el uso anónimo de los servicios y productos cuando no sea necesaria la identificación de las personas.
Categoría: Reducción del riesgo

Riesgo por el que se adopta esta medida:
Impedir la utilización anónima de un determinado producto o servicio cuando la identificación del usuario no resulta indispensable.
Efectividad Estimada de la Medida:

• Probabilidad del riesgo tras aplicar esta medida: Despreciable

• Impacto del riesgo tras aplicar esta medida: Despreciable

41.- Medida de Protección:
Revisar de forma exhaustiva los flujos de información para detectar si se solicitan datos personales que luego no son utilizados en ningún proceso.
Categoría: Reducción del riesgo
Riesgo por el que se adopta esta medida:
Tratar datos personales cuando no es necesario para la finalidad perseguida.
Efectividad Estimada de la Medida:

• Probabilidad del riesgo tras aplicar esta medida: Despreciable

• Impacto del riesgo tras aplicar esta medida: Despreciable

42.- Medida de Protección:
Revisar de forma exhaustiva los flujos de información para detectar si se solicitan datos personales que luego no son utilizados en ningún proceso.
Categoría: Reducción del riesgo
Riesgo por el que se adopta esta medida:
Solicitar datos o categorías de datos innecesarios para las finalidades del nuevo sistema, producto o servicio.
Efectividad Estimada de la Medida:

• Probabilidad del riesgo tras aplicar esta medida: Despreciable

• Impacto del riesgo tras aplicar esta medida: Despreciable

43.- Medida de Protección:
Revisar las posibilidades que ofrece la legislación de protección de datos para permitir el tratamiento de datos personales y asegurar que este encaja en alguna de ellas.
Categoría: Reducción del riesgo
Riesgo por el que se adopta esta medida:
Carecer de una legitimación clara y suficiente para el tratamiento o la cesión de datos personales.
Efectividad Estimada de la Medida:

• Probabilidad del riesgo tras aplicar esta medida: Despreciable

• Impacto del riesgo tras aplicar esta medida: Despreciable

44.- Medida de Protección:
Revisar las posibilidades que ofrece la legislación de protección de datos para permitir el tratamiento de datos personales y asegurar que este encaja en alguna de ellas.
Categoría: Reducción del riesgo
Riesgo por el que se adopta esta medida:
Obtener un consentimiento dudoso, viciado o inválido para el tratamiento o cesión de datos
personales.
Efectividad Estimada de la Medida:

• Probabilidad del riesgo tras aplicar esta medida: Despreciable

• Impacto del riesgo tras aplicar esta medida: Despreciable

45.- Medida de Protección:

Revisar las posibilidades que ofrece la legislación de protección de datos para permitir el tratamiento de datos personales y asegurar que este encaja en alguna de ellas.

Categoría: Reducción del riesgo

Riesgo por el que se adopta esta medida:

Dificultades para garantizar la legitimidad de la recogida y la cesión de datos personales
provenientes de terceros.

Efectividad Estimada de la Medida:

• Probabilidad del riesgo tras aplicar esta medida: Despreciable

• Impacto del riesgo tras aplicar esta medida: Despreciable

46.- Medida de Protección:

Seleccionar encargados de tratamiento que proporcionen garantías suficientes de cumplimiento de los contratos y de la adopción de las medidas de seguridad estipuladas a través, por ejemplo, de su adhesión a posibles códigos de conducta o a esquemas de certificación homologados y de acreditada solvencia.

Categoría: Reducción del riesgo

Riesgo por el que se adopta esta medida:

Falta de diligencia (o dificultad para demostrarla) en la elección de encargado de tratamiento.

Efectividad Estimada de la Medida:

• Probabilidad del riesgo tras aplicar esta medida: Despreciable

• Impacto del riesgo tras aplicar esta medida: Despreciable

47.- Medida de Protección:

Si es necesario, buscar asesoramiento experto.

Categoría: Reducción del riesgo

Riesgo por el que se adopta esta medida:

Dificultar la revocación del consentimiento o la manifestación de la oposición a un tratamiento o cesión.

Efectividad Estimada de la Medida:

• Probabilidad del riesgo tras aplicar esta medida: Despreciable

• Impacto del riesgo tras aplicar esta medida: Despreciable

48.- Medida de Protección:

Si es necesario, buscar asesoramiento experto.

Categoría: Reducción del riesgo

Riesgo por el que se adopta esta medida:

Carecer de los mecanismos y procedimientos necesarios para detectar cuándo debe notificarse la
creación, modificación o cancelación de un tratamiento de datos personales a la AEPD o a la
autoridad de protección de datos competente.

Efectividad Estimada de la Medida:

• Probabilidad del riesgo tras aplicar esta medida: Despreciable

• Impacto del riesgo tras aplicar esta medida: Despreciable

49.- Medida de Protección:

Siempre que sea posible, utilizar datos anónimos o disociados.

Categoría: Reducción del riesgo

Riesgo por el que se adopta esta medida:
Garantías insuficientes para el uso de datos personales con fines históricos, científicos o
estadísticos.
Efectividad Estimada de la Medida:

• Probabilidad del riesgo tras aplicar esta medida: Despreciable

• Impacto del riesgo tras aplicar esta medida: Despreciable

50.- Medida de Protección:
Verificar la legitimidad de la interconexión de datos prevista.
Categoría: Reducción del riesgo
Riesgo por el que se adopta esta medida:
Enriquecer los datos personales de forma no prevista en las finalidades iniciales y sin la información
adecuada a los afectados al realizar una interconexión con otras bases de datos de la organización
o de terceros, en particular, la re-identificación de información disociada.
Efectividad Estimada de la Medida:

• Probabilidad del riesgo tras aplicar esta medida: Despreciable

• Impacto del riesgo tras aplicar esta medida: Despreciable

D. Documentación complementaria

1. Algunas cuestiones fundamentales sobre la EIPD

A la hora de elaborar un proyecto de Evaluación de Impacto en un tratamiento de protección de datos, es necesario que demos respuesta a una serie de cuestiones fundamentales, entre las que se encuentran las siguientes:

1.1• **¿El proyecto involucrará la recopilación de nueva información sobre individuos?:**
Si. La estrictamente necesaria para cumplir con las finalidades legítimas perseguidas por la Asociación. También es posible la rectificación de datos previamente aportados. Los datos recabados son el nombre y los apellidos, el número de identificación personal, la dirección postal, la dirección e-mail, el número de teléfono y los identificadores en Redes Sociales y aplicaciones de mensajería instantánea.

1.2• **¿El proyecto obligará a los individuos (interesados/afectados) a proporcionar información sobre ellos mismos?:**
Sí. Solamente la información personal esencial y precisa para poder prestarles el servicio de lista de exclusión publicitaria.

1.3• **¿Se dará a conocer información sobre individuos a organizaciones o personas que no hayan tenido acceso rutinario a la información?:**
No se tienen previstas cesiones de datos personales.

1.4• **¿El responsable del tratamiento está utilizando información sobre individuos para un propósito que no se utiliza actualmente, o de una manera que no se**

utiliza actualmente?:
No se utiliza información para propósitos distintos a los actuales, ni se tiene previsto hacerlo.

1.5• **¿El proyecto implica el uso de nueva tecnología que podría ser percibida como intrusión en la privacidad, por ejemplo biométrica o reconocimiento facial?:**
No, en ningún caso se tienen previstas dichas tecnologías.

1.6• **¿El proyecto dará lugar a que la Asociación tome decisiones o tome acciones contra individuos de una manera que podría tener un impacto significativo en ellos?:**
No, en ningún momento del tiempo.

1.7• **¿Es particularmente probable que la información acerca de determinadas personas suscite inquietudes o expectativas de privacidad?:**
No, dentro de lo considerado como razonable dada la naturaleza de los datos personales aportados por los interesados o afectados y del ciclo de vida de los datos aportados.

1.8• **¿El proyecto requiere que la Asociación se ponga en contacto con las personas que pueden encontrar el tratamiento de datos como intrusivo?**:
No, en ningún momento, puesto que el tratamiento que se va a llevar a cabo cumple con todos los principios relativos al tratamiento consagrados en el artículo 5 del RGPD UE 2016/679. Además no se procede al tratamiento de datos especialmente protegidos o sensibles y se dispone del consentimiento inequívoco, explícito, expreso del interesado o afectado, para proceder al tratamiento automatizado de dichos datos de carácter personal.

1.9• **¿Se requiere una revisión periódica de la seguridad de los datos?:**

Si bien no es en este caso legalmente obligatoria la realización de Auditorías de Medidas de Seguridad en materia de protección de datos, el Responsable del Tratamiento lleva a cabo dichas Auditorías con una periodicidad temporal bienal, salvo que se produzcan modificaciones sustanciales en el tratamiento de datos o en los sistemas de información utilizados por la Asociación, que obliguen o recomienden llevarlas a cabo con una periodicidad temporal menor a dos años.

1.10• **¿Es necesaria una revisión técnica de Impacto de Calidad/Seguridad Técnica?:**

Los procesos técnicos de ejecución de los sistemas de información implementados por el Responsable del Tratamiento, están sujetos a continuas revisiones de naturaleza técnica, para la verificación del correcto funcionamiento de dichos procesos. En caso de observarse alguna anomalía se procede a su corrección de manera efectiva e inmediata. Por lo que todos los activos que forman parte del sistema de información, están sometidos continuamente a procesos de revisión y mantenimiento técnico por profesional informático especializado en la materia.

2. Algunas preguntas y cuestiones relativas al modelo global de práctica de la evaluación e implantación de una EIPD – PIA.

Apartado número 1º. Legitimación de los tratamientos

1. ¿Se cuenta con el consentimiento libre, específico, inequívoco e informado de los afectados para el tratamiento de sus datos personales?: Sí
2. ¿El tratamiento de los datos responde a una relación contractual?: Si
3. ¿Se han establecido medidas de garantía y salvaguardia para limitar los efectos del tratamiento sobre los afectados?: Sí
4. En el caso de que el tratamiento se base en el consentimiento del afectado,¿existen mecanismos para probar que se ha prestado en los términos que marca la ley y para que se pueda ejercer la revocación del mismo?: Sí
5. ¿Tiene establecida claramente cuál es la base legal de los tratamientos que realiza y ha documentado de alguna forma el modo en que la ha establecido?: Sí
6. Si alguno de los tratamientos que realiza está basado en el consentimiento de los interesados, ¿ha verificado que ese consentimiento reúne los requisitos que exige el RGPD?: Sí
7. En caso contrario, ¿ha encontrado otra base legal adecuada para estos tratamientos?: Sí

Apartado número 2º. Transferencias Internacionales de datos

1 ¿Se van a transferir datos personales fuera de España?: Sí

2 ¿Es el país de destino un miembro del Espacio Económico Europeo?: No

3. Si no es así, ¿es un país declarado adecuado por la Comisión Europea o por el director/directora de la AEPD?:No

4 ¿Las transferencias se llevan a cabo mediante garantías adecuadas, a través de los instrumentos jurídicos reconocidos a este fin por el artículo 46 del RGPD UE?: Si

5 En caso contrario, ¿se puede aplicar alguna de las excepciones previstas por el RGPD UE en su artículo 49?: No procede

Apartado número 3º. Calidad de los datos

1. ¿Se recogen sólo los datos personales estrictamente necesarios para las finalidades de las que se trate?: Sí. Aquellos datos personales que se recaben sólo se podrán recoger para su tratamiento, así como someterlos al mismo, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y finalidades determinadas, explícitas y legítimas para las que fueron obtenidos. Estos datos no se emplearán para finalidades distintas para las que fueron recogidos.
2. ¿Se recaban los datos de forma leal y transparente?: Sí. Es obligación legal del responsable del tratamiento tomar las medidas oportunas para facilitar al interesado toda la información recogida o contemplada por el artículo 13 del RGPD UE.
3. ¿Se usan los datos para finalidades distintas o incompatibles con las establecidas y comunicadas al afectado?: No. Los datos de carácter personal

objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos.

4. ¿Existen mecanismos de actualización de la información y de verificación de dicha actualización?: Sí. Los datos son exactos y están actualizados en caso que sea necesario y se adoptan todas las medidas razonables para que esta modificación se pueda llevar sin dilación alguna y por tanto que los datos dejen de ser inexactos con respecto a los fines para los que se tratan. El responsable del tratamiento aplica las medidas técnicas y organizativas apropiadas a fin de garantizar y demostrar que el tratamiento realizado cumple con lo dispuesto en el RGPD UE.
5. ¿Se contempla la posibilidad de suprimir los datos personales de oficio, cuando ya no sean necesarios para la finalidad o finalidades para las que se recogieron?: Sí. En el supuesto de que los datos personales resultaran ser inexactos, en todo o en parte, o incompletos, serán suprimidos y sustituidos de oficio por los correspondientes datos rectificados o completados, sin perjuicio de las facultades que se les confieren a los interesados/afectados de rectificación y supresión. También serán suprimidos de oficio cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados. La supresión dará lugar al bloqueo de los datos, el cual consiste en su identificación y reserva con el fin de impedir su tratamiento, excepto para su puesta a disposición de las Administraciones Públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades que deriven del tratamiento, durante el plazo de prescripción de éstas o atendiendo a la prescripción de las sanciones administrativas derivadas del tratamiento. Cumplido el plazo deberá procederse a sus supresiones. La supresión no procederá cuando los datos deban conservarse durante los plazos previstos en las disposiciones aplicables o, en su caso, en las relaciones contractuales entre la entidad (**Asociación Española para la Privacidad Digital**) responsable del tratamiento y el afectado o interesado que justificaron el tratamiento de datos. Como ocurre con la **Actividad de Tratamiento Clientes Obligados a la Consulta**, respecto a la cual, existirá la obligación legal de conservar los datos personales de los Clientes Obligados a la Consulta durante un periodo temporal de 5 años, por posible ejercicio de la responsabilidad civil de naturaleza contractual por parte de la Asociación
6. ¿Se definen los plazos de conservación de los datos personales?: Sí. Los datos de carácter personal son conservados durante el tiempo que pueda exigirse algún tipo de responsabilidad derivada de una relación u obligación jurídica o de la ejecución de un contrato o de la aplicación de medidas precontractuales solicitadas por el interesado titular de los datos personales. Transcurrido este período en su caso, los datos sólo podrán ser conservados previa disociación de los mismos, sin perjuicio de la anteriormente mencionada, **obligación de bloqueo**.
7. ¿Existen procedimientos para determinar que se han cumplido los plazos máximos de conservación de los datos personales?: Sí. Automatizada

8. ¿Se conservan los datos personales de tal manera que puedan ejercerse por parte de los interesados/afectados los derechos personalísimos en materia de protección de datos, contemplados por la normativa europea (RGPD UE 2016/679) y nacional (LOPD GDD 3/2018) de protección de datos?: Sí.
9. ¿En el caso de que se proceda a disociar los datos personales, se utilizan procedimientos que garantizan la irreversibilidad del proceso y la imposibilidad de reidentificar a los titulares de los datos (Afectados/Interesados)?: Sí. Todo ello a través de procesos técnicos informáticos de cifrado/encriptado, debidamente incorporados e integrados en la plataforma web de la Asociación

Apartado número 4º. Deber de Secreto

1. ¿Se forma adecuadamente a todas las personas que tratan datos de carácter personal de la obligación de guardar secreto sobre los datos que conozcan en el ejercicio de sus funciones?: Sí
2. ¿Se les informa adecuadamente de sus obligaciones y de las consecuencias de no hacerlo?: Sí
3. ¿Queda constancia de dicha información?: Sí, por escrito.

Apartado número 5º. Tratamiento de datos por encargado

1. ¿Se han realizado los análisis necesarios de manera diligente para elegir un encargado del tratamiento que ofrezca las garantías adecuadas?: Sí. El responsable del tratamiento vela por que el encargado del tratamiento reúna las garantías necesarias para el cumplimiento de lo dispuesto en el RGPD UE.
2. ¿Se regula la relación entre el responsable y el encargado en un contrato (escrito o acordado electrónicamente con las garantías que establece la legislación aplicable)?: Sí. La realización de tratamientos por cuenta de terceros está regulada en un contrato que consta por escrito o en formato electrónico, estableciéndose expresamente que el encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento.
3. ¿Se han adoptado medidas para verificar el cumplimiento de las condiciones contractuales y de las medidas de seguridad por parte del encargado y de los posibles subcontratistas?: Sí. Respecto a los subencargados del tratamiento, el RGPD estipula que cuando un encargado del tratamiento recurra a otro encargado del tratamiento para llevar a cabo determinadas actividades de tratamiento por cuenta del responsable del tratamiento, se impondrán a este otro encargado del tratamiento, mediante contrato u otro acto jurídico establecido con arreglo al Derecho de la Unión o de los Estados miembros, las mismas obligaciones de protección de datos que las estipuladas en el contrato u otro acto jurídico entre el responsable y el encargado (artículo 28.4 RGPD UE).

4 ¿Se estipula en el contrato de encargado del tratamiento que los datos no serán comunicados a otras personas?: Sí. En el mismo contrato se indica que el encargado del tratamiento no aplicará los datos personales o los utilizará con fin distinto al que figure en dicho contrato, ni los comunicará, ni siquiera para su conservación, a otras personas.

5 ¿Se estipulan las medidas de seguridad que deberá adoptar el encargado del tratamiento?: Sí. En el contrato de encargado del tratamiento se recogen las medidas de seguridad relativas a lo establecido en el artículo 32 del RGPD UE y que el encargado del tratamiento está obligado a implementar.

6 ¿Se regula el destino de los datos a la finalización de la prestación de que se trate (destrucción, devolución al responsable o comunicación a otro encargado designado por el responsable)?: Sí. Una vez cumplida la prestación contractual, los datos deberán ser destruidos o devueltos al responsable del tratamiento, al igual que cualquier soporte o documentos en que conste algún dato personal objeto de tratamiento. Conforme al RGPD UE, a elección del responsable, el encargado suprimirá o devolverá todos los datos personales una vez finalice la prestación de los servicios de tratamiento, y suprimirá las copias existentes a menos que se requiera la conservación de los datos en virtud del Derecho de la Unión o de los Estados miembro.

7 ¿Se informa al encargado de que en caso de que destine los datos personales a otra finalidad, los comunique o incumpla el contrato será considerado responsable del tratamiento y podrá incurrir en el régimen sancionador del RGPD y de la LOPD GDD?: Sí. Se estipula en el contrato de encargado del tratamiento, que en el caso de que el encargado del tratamiento destine los datos a otra finalidad, los comunique o los utilice incumpliendo las estipulaciones del contrato, será considerado también responsable del tratamiento, respondiendo de las infracciones en que hubiere incurrido personalmente.

8 ¿Existe una cesión por que el encargado del tratamiento establece un nuevo vínculo con los afectados?: No. Puesto que no se establece un nuevo vínculo entre quien accede a los datos y el interesado, por lo que no se considerará comunicación o cesión de datos el acceso de un tercero a los datos cuando éste sea necesario para la prestación de un servicio al responsable del tratamiento.

9 Si existen o van a existir subcontrataciones, ¿se cuenta con la autorización del responsable del tratamiento?: Sí. En el caso que nos ocupa, la contratación se efectuará siempre en nombre y por cuenta del responsable del tratamiento.

10 ¿Se ajusta el subencargado del tratamiento (subcontratista) a las instrucciones del responsable del tratamiento?: Sí, en todo momento.

11 ¿Se formaliza un contrato entre el encargado del tratamiento y el subencargado del tratamiento en los términos del contrato inicial?: Sí. Teniendo en cuenta que la nueva relación jurídica entre las partes, viene regulada conforme a lo establecido en el Artículo 28.4 del RGPD UE.

12 Si el encargado del tratamiento presta sus servicios en los locales del responsable o bien accede remotamente a los datos personales sin posibilidad de copiarlos o incluirlos en sus sistemas, ¿se ha reflejado este hecho en el Registro de Actividades de Tratamiento del responsable?: Sí.

13 ¿Se ha comprometido el personal del encargado a cumplir las medidas de seguridad establecidas por el responsable?: Sí. El personal del encargado se

compromete al cumplimiento de las medidas de seguridad recogidas o contempladas en el contrato de encargado del tratamiento y en el Registro de Actividades de Tratamiento del encargado del tratamiento.

14 En el caso de que la prestación no implique acceso a datos, ¿se recoge expresamente la prohibición de acceder a datos personales y la obligación de secreto sobre aquellos que el encargado incidentalmente hubiera podido conocer?: Sí. Cuando se trata de personal ajeno, el contrato de encargado del tratamiento recoge expresamente la prohibición de acceder a los datos personales y la obligación de secreto respecto a los datos que el mencionado personal hubiera podido conocer con motivo de la prestación del servicio por parte del encargado del tratamiento.

15 Si el servicio se presta en los locales del encargado del tratamiento, ¿se ha incluido este hecho en su RAT (Registro de Actividades de Tratamiento), así como la identidad del responsable del tratamiento?: Sí.

16 ¿Ha desarrollado el encargado del tratamiento el RAT correspondiente o completado el que ya tuviera con la información referida al encargo recibido?: Sí.

17 ¿El responsable del tratamiento ha previsto como valorar si los encargados con los que haya contratado o vaya a contratar operaciones de tratamiento ofrece garantías suficientes de cumplimiento del RGPD UE 2016/679?: Sí. El responsable del tratamiento elige únicamente encargados que ofrezcan garantías suficientes para aplicar medidas técnicas y organizativas apropiadas, de tal manera que el tratamiento sea conforme con los requisitos del RGPD UE y garantice la protección de los derechos fundamentales del interesado o afectado.

18 ¿Contiene los contratos de encargo que actualmente tenga suscritos la **Asociación Española para la Privacidad Digital** todos los elementos que prevé el RGPD UE?: Sí. Todo ello conforme a los requisitos contemplados por el artículo 28.3 del RGPD UE.

Apartado número 6º. Información y derechos

1 ¿Se adoptan las medidas necesarias para garantizar el carácter personalísimo (verificación de la identidad o, en su caso de la validez de la representación otorgada a un tercero) del ejercicio de los derechos?: Sí. Para el ejercicio de los derechos de los interesados será necesario que el afectado acredite su identidad. Los derechos serán denegados cuando la solicitud sea formulada por persona distinta del afectado y no se acreditase que la misma actúa en representación de aquél.

2 ¿Se han adoptado medidas para acreditar la representación en casos de minoría de edad, incapacidad o fallecimiento?: Sí. Cuando el afectado se encuentre en situación de incapacidad o minoría de edad que le imposibilite el ejercicio personal de estos derechos, podrán ejercitarse por su representante legal, en cuyo caso será necesario que acredite tal condición.

3 ¿Se ha previsto el ejercicio de los derechos mediante representante voluntario y la forma de acreditar dicha representación?: Sí. Para el caso de que se ejerzan a través de representante voluntario, éste deberá estar expresamente designado

para el ejercicio del mismo. Deberá constar claramente acreditada la identidad del representado, mediante la aportación de copia de su DNI o documento equivalente (con datos exclusivamente necesarios), y la representación conferida por aquél.

4 ¿Se ha habilitado un medio sencillo y gratuito para el ejercicio de los derechos?: Sí. Se concede al interesado un medio sencillo y gratuito para el ejercicio de los derechos personalísimos en materia de protección de datos personales.

5 ¿Se conservan los datos personales de tal forma que permitan el fácil y rápido ejercicio de los derechos?: Sí. Conforme establece la normativa europea de protección de datos (RGPD UE).

6 ¿Se han implantado las medidas y procedimientos adecuados para garantizar el ejercicio de los derechos en los plazos marcados por la ley?: Sí. Todo ello conforme a lo estipulado por el artículo 12.3 del RGPD UE 2016/679.

7 En el caso de que el responsable del tratamiento utilice encargados del tratamiento, ¿les ha instruido para que les den traslado de cualquier ejercicio de derechos que reciba?: Sí. Cuando los afectados ejerciten sus derechos ante un encargado del tratamiento y solicitasen el ejercicio de su derecho ante el mismo, dicho encargado del tratamiento dará traslado de la solicitud al responsable, a fin de que por el mismo se resuelva dicha solicitud.

8 ¿Se han implantado las medidas y procedimientos adecuados para que siempre se proporcione una respuesta a los ciudadanos que ejercen tales derechos?: Sí. El responsable del tratamiento contestará la solicitud que se le dirija en todo caso, con independencia de que figuren o no datos personales del afectado en sus ficheros o actividades de tratamiento.

9 ¿Se han implantado medidas y procedimientos para responder a los requerimientos de la AEPD en el marco de los procedimientos de tutela de derechos de afectados?: Sí. En todo caso, conforme recoge la normativa vigente en materia de protección de datos personales.

10 ¿Existen mecanismos y procedimientos para informar a los posibles cesionarios de datos personales de las rectificaciones o supresiones realizadas?: Sí. En el caso de que los datos rectificados o suprimidos hubieran sido cedidos previamente, el responsable del tratamiento procederá a comunicar dicha rectificación o supresión efectuada al cesionario, para que éste, en el plazo máximo temporal de un mes contado desde la recepción de dicha comunicación, proceda asimismo a rectificar o suprimir los datos personales del interesado titular de los datos.

11 En el caso del derecho de acceso, ¿se ofrece toda la información que establece la Ley en los formatos adecuados y legibles sin tener que recurrir a medios adicionales para su interpretación?: Sí. Todo ello conforme a lo contemplado por el articulado de la normativa europea y nacional de protección de datos personales (RGPD UE 2016/679 y LOPD GDD 3/2018).

12 En el caso del derecho de supresión, ¿se conservan los datos personales durante los plazos previstos por las disposiciones aplicables o en las relaciones contractuales y solo por esos plazos?: Sí. La supresión no procederá cuando los datos de carácter personal deban ser conservados durante los plazos previstos

en las disposiciones aplicables o, en su caso, en las relaciones contractuales entre la persona o entidad responsable del tratamiento y el interesado que justificaron el tratamiento de los datos.

13 ¿Se mantienen los datos bloqueados a disposición de las Administraciones Públicas (AA.PP.), los Jueces y Tribunales durante el plazo de prescripción de responsabilidades?: Sí. La supresión dará lugar al bloqueo de los datos, conservándose únicamente a disposición de las Administraciones Públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento, durante el plazo de prescripción de éstas, transcurrido el cual deberá procederse a la supresión.

14 La información que se proporciona a los interesados, ¿está presentada de forma clara, concisa, transparente y de fácil acceso?: Sí. Para las personas físicas afectadas queda totalmente claro que se están recogiendo, utilizando, consultando o tratando de otra manera datos de carácter personal que les conciernen, así como la medida en que dichos datos son o serán tratados.

15 ¿Contiene esa información todos los elementos que prevé el RGPD UE?: Sí. De manera detallada y exhaustiva, conforme a lo estipulado por los artículos 13, 14 y 15 del mencionado RGPD.

16 ¿Dispone el responsable del tratamiento de mecanismos para el ejercicio de derechos visibles, accesibles y sencillos por parte de las personas afectadas?: Sí. Se han articulado mecanismos y se han arbitrado fórmulas para facilitar al afectado el ejercicio de sus derechos, incluidos los mecanismos para solicitar y, en su caso, obtener de forma gratuita, en particular, el acceso a los datos personales y su rectificación o supresión, así como el ejercicio del derecho de oposición.

17 ¿Pueden ejercerse los derechos personalísimos por vía electrónica?: Sí. El responsable del tratamiento proporciona los medios necesarios para que las solicitudes se presenten por medios electrónicos, puesto que en el presente caso que nos ocupa, los datos de carácter personal de los interesados se tratan por medios electrónicos.

18 ¿El responsable del tratamiento tiene establecidos procedimientos o mecanismos que le permitan verificar la identidad de quienes solicitan el ejercicio del derecho de acceso o ejercen los demás derechos de afectados?: Sí. El responsable del tratamiento utiliza todas las medidas razonables para verificar de forma efectiva la identidad de los interesados que ejercitan los derechos de afectados reconocidos por la normativa europea y nacional vigente en materia de protección de datos personales.

19 ¿El responsable del tratamiento tiene establecidos procedimientos que le permitan responder a los ejercicios de los derechos en los plazos previstos por el RGPD UE?: Sí. El responsable del tratamiento ha articulado los mecanismos necesarios, para responder a las solicitudes de los interesados sin dilación indebida y a más tardar en el plazo de un mes, y para explicar sus motivos en caso de que no fuera a atender dichas solicitudes.

20 ¿Ha valorado el responsable del tratamiento si sería necesaria la colaboración de los encargados del tratamiento para responder a las solicitudes de los

interesados y, si es así, ha previsto incluir esta colaboración en los contratos de encargo?: Sí. El responsable del tratamiento ha formalizado en el contrato o acto jurídico la posibilidad de que el encargado asista al responsable del tratamiento, teniendo en cuenta la naturaleza del tratamiento, a través de medidas técnicas y organizativas apropiadas, siempre que sea posible, para que el responsable del tratamiento pueda cumplir con su obligación de responder a las solicitudes que tengan por objeto el ejercicio de los derechos de los interesados/afectados.

21 En particular, ¿tiene el responsable previstos mecanismos para atender a posibles ejercicios del derecho a la limitación del tratamiento, de forma que los datos afectados puedan ser conservados sin ser objeto de las operaciones de tratamiento que corresponderían?: Sí. Manteniendo, en su caso los datos debidamente bloqueados
temporalmente.

22 ¿Ha valorado el responsable del tratamiento si los tratamientos de datos que realiza pueden ser objeto del derecho a la portabilidad?: Sí, puesto que conforme a lo estipulado por el artículo 20 del RGPD UE, pueden ser objeto de portabilidad los siguientes tratamientos:

- Cuando el tratamiento esté basado en el consentimiento lícito por parte del interesado para el tratamiento de sus datos personales para uno o varios fines.
- Cuando esté basado en un contrato en el que el interesado es parte, para la ejecución de dicho contrato o para la aplicación a petición del interesado de medidas precontractuales.
- Cuando el tratamiento se efectúe por medios automatizados.

23 En caso afirmativo, ¿ha previsto procedimientos o mecanismos para poder atender a este derecho y proporcionar los datos al interesado (o a otro responsable) en un formato estructurado, de uso común y susceptible de lectura mecánica?: Sí. Puesto que el responsable del tratamiento es conocedor, de que el interesado tiene derecho a recibir los datos personales que le incumban, que haya facilitado a un responsable del tratamiento, en un formato estructurado, de uso común y lectura mecánica, y a transmitirlos a otro responsable del tratamiento sin que lo impida el responsable del tratamiento al que se los hubiera facilitado.

Apartado número 7º. Seguridad general por niveles de riesgos

1 ¿Se ha llevado a cabo la clasificación e identificación de los distintos niveles de riesgos (bajo, moderado, elevado/muy alto) aplicables a todos y cada uno de los ficheros o actividades de tratamiento de datos personales?: Sí. El responsable del tratamiento tiene implantadas las medidas de seguridad acordes con el nivel de riesgo aplicable en su caso, que establecen o recogen la normativa europea de protección de datos (RGPD UE).
Las medidas de seguridad que corresponden, según el **nivel de riesgo** aplicable al tratamiento en cuestión, son de índole técnica y organizativa, quedando plasmadas en el Registro de Actividades de Tratamiento (**RAT**) del responsable,

el cual se ajusta a la normativa de protección de datos vigente, la cual será de obligado cumplimiento para todos aquellos con acceso a datos de carácter personal.

2 ¿Se garantiza que las medidas de seguridad para el acceso a datos personales a través de **redes de telecomunicaciones** garantizan el mismo nivel de seguridad conforme al nivel de riesgo aplicable en su caso, que el existente en el **entorno local**?: Sí. Las medidas de seguridad exigibles a los accesos a datos personales a través de redes de telecomunicaciones, garantizan un nivel de seguridad en relación con el nivel de riesgo aplicable equivalente al establecido para el acceso en modo local.

3 ¿Existe un procedimiento para gestionar las autorizaciones para la salida de dispositivos portátiles que contienen datos personales fuera de los locales del responsable del tratamiento?: Sí. No obstante no ha sido necesario hasta el momento actual, el régimen de trabajo fuera de las instalaciones del responsable con dispositivos portátiles que contengan datos de carácter personal. En el caso de que se almacenen datos personales en dispositivos portátiles y éstos se traten fuera de los locales del responsable del tratamiento, la Asociación Española para la Privacidad Digital, emitirá una autorización específica previa. Y en todo caso se garantizará el nivel de seguridad conforme al nivel de riesgo aplicable, que corresponde al tipo de fichero o de actividad de tratamiento. Esto se fijará en el RAT (Registro de Actividades de Tratamiento) y podrá establecerse para un usuario o para un perfil de usuarios y determinando un período de validez para las mismas.

4 ¿Cumplen las copias de trabajo y los/las ficheros/actividades de tratamiento temporales las medidas de seguridad que les corresponden según su nivel de riesgo aplicable al caso concreto?: Sí. En el hipotético caso de que se proceda a la creación de ficheros temporales o copias de documentos exclusivamente para la realización de trabajos temporales o auxiliares, éstos/éstas cumplirán escrupulosamente con todas las medidas de seguridad en materia de protección de datos, recogidas o contempladas por la normativa vigente europea de protección de datos personales (RGPD UE 2016/679), según o acorde al nivel de riesgo aplicable al caso concreto en cuestión.

5 ¿Se destruyen una vez han dejado de ser necesarios?: Sí. De tal manera que todo fichero temporal o toda actividad de tratamiento temporal o toda copia de trabajo temporal, será borrado o destruido una vez que deje de ser necesario para los fines que ocasionaron su creación.

6 ¿Se ha elaborado el Registro de Actividades de Tratamiento (RAT)?: Sí. Conforme a lo establecido en el artículo 30 del RGPD UE 2016/679.

Apartado número 8º. Seguridad de actividades de tratamiento automatizadas (nivel de riesgo bajo)

1 ¿Se han definido claramente en el Registro de Actividades de Tratamiento las funciones y obligaciones de los usuarios que acceden a los sistemas de información que contienen datos personales?: Sí. Entre otros documentos los usuarios tienen firmadas las Normas Internas de Uso de Sistemas de Información.

2 ¿Se han establecido los procedimientos necesarios para que todo el personal conozca las medidas de seguridad que les afecta y que debe implantar?: Sí. Se les ha informado de dichas medidas de seguridad a implantar.

3 ¿Se ha creado un registro de incidencias y un procedimiento para su gestión?: Sí. Está debidamente creado el registro y su procedimiento. También, el responsable del tratamiento ha procedido a diseñar un sistema informático de valoración de brechas de seguridad de datos o de violaciones de seguridad de los datos, para su posible comunicación a la Autoridad de Control Nacional Competente (AEPD).

4 ¿Se ha difundido este procedimiento para conocimiento general de todo el personal?: Sí. Todo el personal es conocedor de dicho procedimiento.

5 ¿Se ha asegurado que cada usuario acceda únicamente a los datos personales que son necesarios para sus funciones?: Sí. En base, en todo momento al principio de Minimización de Datos.

6 ¿Existe una relación actualizada de perfiles con estas autorizaciones y los mecanismos para su actualización?: Sí. Estando debidamente registrada dicha relación, en el Registro de Actividades de Tratamiento del responsable del tratamiento.

7 ¿Existen medidas para evitar que un usuario acceda a recursos con permisos distintos de los autorizados?: Sí. En base, a procedimientos automatizados de identificación y autenticación.

8 ¿Está claramente delimitado y consignado en el Registro de Actividades de Tratamiento el personal autorizado para gestionar estos permisos?: Sí. De forma totalmente transparente.

9 ¿Existen medidas adecuadas para identificación, inventario, control de acceso y autorización de la salida de soportes?: Si. Estando todo ello detallado en el Registro de Actividades de Tratamiento del responsable del tratamiento.

10 ¿Se han adoptado las medidas adecuadas para evitar la sustracción, pérdida o acceso indebido a la información durante su transporte?: Sí. En todo momento se tutelan de manera efectiva los soportes informáticos, además de estar protegidos con sistemas de seguridad, a través de procedimientos de identificación y autenticación.

11 ¿Existen medidas para evitar que los soportes desechados contengan datos personales que puedan ser recuperados?: Sí. Todos los soportes informáticos desechados, son sometidos a procesos de borrado seguro de la información, a través de los métodos de destrucción física del soporte, de desmagnetización o de sobreescritura de la información.

12 ¿Existen medidas para garantizar la correcta identificación y autenticación de los usuarios de forma inequívoca y personalizada?: Sí. También está implantada la medida de seguridad de limitación del intento de acceso reiterado no autorizado a los sistemas de información.

13 ¿Existe un procedimiento seguro de asignación, distribución y almacenamiento de contraseñas?: Sí.

14 ¿Existen procedimientos para el cambio periódico de las contraseñas al menos una vez al año?: Sí.

15 ¿Existen mecanismos de realización de copias de seguridad y de recuperación de la información que contienen?: Sí. Además se realizan con una periodicidad temporal diaria.
16 ¿Se verifica cada seis meses el correcto funcionamiento de estos sistemas?: Sí.
17 Si se realizan pruebas con datos reales, ¿se garantiza que se protegen con las medidas de seguridad acordes con su nivel de riesgo aplicable?: Sí.
18 ¿Se asegura que se hace una copia con carácter previo a su utilización?: Sí.

Apartado número 9º. Seguridad de actividades de tratamiento automatizadas (nivel de riesgo moderado). Además de las de nivel de riesgo bajo, las detalladas a continuación

1 ¿Se ha designado un Responsable de Seguridad?: Sí. Se ha hecho constar en el Registro de Actividades de Tratamiento, en el cual se ha procedido a designar al Presidente el señor D. José Manuel de Ramón Rodríguez, como persona que ostenta dicho cargo (Responsable de Seguridad). El Responsable de Seguridad se encargará de coordinar y controlar las medidas definidas en el RAT. No obstante dejamos constancia que la responsabilidad seguirá correspondiendo al Responsable del Tratamiento, no a la persona designada.
2 ¿Se realizan auditorías de control de cumplimiento del RGPD y auditorías de medidas de seguridad en materia de protección de datos bienales o cada vez que se produzcan modificaciones sustanciales en los sistemas de información? Sí. Emitiéndose los correspondientes y respectivos informes de Auditoría RGPD y LOPD GDD. La Asociación Española para la Privacidad Digital a partir del nivel de riesgo moderado, lleva a cabo, al menos cada dos años, una Auditoría externa en los sistemas de información e instalaciones de tratamiento y almacenamiento de datos personales.

3 ¿Se ha establecido un sistema de registro de entrada y salida de soportes y documentos?: Sí. Se ha procedido a establecer un sistema de registro de entrada de soportes que permita, directa o indirectamente, conocer el tipo de soporte o documento, la fecha y hora, el emisor, el número de documentos o soportes, incluidos en el envío, el tipo de información que contienen, la forma de envío y la persona responsable de la recepción que deberá estar debidamente autorizada. Del mismo modo, se dispone de un sistema de registro de salida de soportes que permita, directa o indirectamente, conocer el tipo de documento o soporte, la fecha hora, el destinatario, el número de documentos o soportes incluidos en el envío, el tipo de información que contienen, la forma del envío y la persona responsable de la entrega que deberá estar debidamente autorizada.
4 ¿Existe un mecanismo que limite la posibilidad de intentar reiteradamente el acceso no autorizado al sistema de información?: Sí. El responsable del tratamiento(Asociación) ha establecido un mecanismo automatizado que limite dicha posibilidad.
Así de esta manera se podrá evitar los accesos no autorizados por parte de terceros ajenos a la entidad, a los sistemas de información de la Asociación Española para la Privacidad Digital.
5 ¿Existe control de acceso físico a los locales donde están ubicados los equipos

físicos que dan soporte a los sistemas de información?: Sí. El responsable del tratamiento ha definido una política de protección de datos, de tal manera que exclusivamente podrá acceder a los lugares físicos que den soporte a los sistemas de información, aquella persona autorizada en el RAT.

6 ¿Existen procedimientos para consignar en el registro de incidencias los mecanismos de recuperación que haya sido necesario ejecutar?: Sí. Dejar constancia de que la entidad responsable del tratamiento (Asociación), ha procedido a consignar en el mencionado registro de incidencias, los procedimientos realizados de recuperación de los datos, indicando igualmente la persona que ejecutó el proceso, los datos restaurados y, en su caso, qué datos han sido necesarios grabar manualmente en el proceso de recuperación. Asimismo procede comentar que para la ejecución de procesos de recuperación de datos, se cuenta o se dispone de la autorización por escrito de la Asociación Española para la Privacidad Digital (responsable del tratamiento).

Apartado número 10º. Seguridad de actividades de tratamiento automatizadas (nivel de riesgo elevado/muy alto). Además de las de nivel de riesgo bajo y moderado, las detalladas a continuación

1 ¿Existen procedimientos y herramientas para cifrar los soportes durante su distribución fuera de los locales del responsable del tratamiento?: Sí. No obstante, hay que dejar bien claro, que en principio no se va a proceder a la distribución fuera de los locales del responsable del tratamiento, de soportes informáticos que contengan datos de carácter personal para un nivel de riesgo elevado/muy alto.

2 ¿Y para los dispositivos portátiles o móviles?: Sí. Asimismo dejamos constancia por escrito, de que los dispositivos portátiles o móviles, en ningún momento van a salir fuera de las instalaciones del responsable del tratamiento (Asociación Española para la Privacidad Digital). En cualquier caso, si en algún momento del tiempo dichos dispositivos fuesen necesarios de que salieran fuera de las instalaciones del responsable del tratamiento, por protocolo de protección de datos, se procederá a cifrar/encriptar con un software específico para ello, el contenido de la información de los mencionados dispositivos portátiles o móviles, que pudieren contener datos de carácter personal para un nivel de riesgo elevado/muy alto.

3 ¿Se conservan las copias de respaldo y los procedimientos de recuperación de los datos en lugar diferente de aquel en que se encuentran los equipos informáticos que los tratan?: Sí. Las copias de seguridad y de respaldo están ubicadas en la NUBE de Google LLC.

4 ¿Se conservan al menos durante dos años, un registro de los accesos que se realizan al sistema de información?: Sí. Los accesos están debidamente registrados en un informe informatizado de registros de accesos a datos con nivel de riesgo elevado/muy alto.

5 ¿Permite dicha información identificar el registro accedido en caso de que el acceso se haya permitido?: Sí. De manera totalmente inequívoca.

6 ¿Se han establecido procedimientos que impidan la desactivación de este registro de accesos?: Sí. Dicho procedimiento está permanentemente activo en

el tiempo, obedeciendo en todo momento al principio de Responsabilidad Proactiva por parte del responsable del tratamiento. Todo ello en base a lo estipulado por el artículo 24 del RGPD UE.

7 ¿Se han establecido procedimientos para que el responsable de seguridad revise al menos una vez al mes el registro de accesos?: Si. Aunque la aplicación de dicha medida de seguridad es para un nivel de riesgo elevado/muy alto.

8 Si los datos se transmiten a través de redes públicas de telecomunicaciones o redes inalámbricas, ¿se procede al cifrado de los datos?: Sí. Todo el tráfico del flujo de datos personales de las personas afectadas/interesadas, a través de la plataforma web de la Asociación Española para la Privacidad Digital, está debidamente cifrado/encriptado, conforme a lo previsto por el RGPD UE.

Apartado número 11º. Medidas de responsabilidad proactiva

1 ¿Ha hecho la Asociación Española para la Privacidad Digital una valoración de los riesgos que los tratamientos que desarrolla implican para los derechos y libertades de los ciudadanos?: Sí. De manera totalmente objetiva la entidad responsable del tratamiento, ha procedido a ponderar la probabilidad y la gravedad del riesgo para los derechos y libertades de los interesados/afectados, las cuales (probabilidad y gravedad) se han determinado con referencia a la naturaleza, el alcance, el contexto y los fines del tratamiento de datos. Así, de este modo se consigue o se logra averiguar si las operaciones de tratamiento de datos suponen o implican un riesgo o si éste es elevado/muy alto.

2 ¿El responsable del tratamiento ha determinado qué medidas de responsabilidad activa corresponden a su situación de riesgo y cómo debe aplicarlas?: Sí. La Asociación Española para la Privacidad Digital ha adoptado políticas internas y ha aplicado medidas que cumplen en particular con los principios de protección de datos personales desde el diseño y por defecto. Dichas medidas consisten entre otras en:

- Reducir al máximo el tratamiento de datos personales.
- Seudonimizar o cifrar/encriptar lo antes posible los datos personales.
- Dar transparencia a las funciones y al tratamiento de datos personales, permitiendo a los interesados supervisar el tratamiento de los datos y al responsable del tratamiento crear y mejorar elementos de seguridad.
- Alentar al programador de la plataforma web (incluida la Lista de exclusión publicitaria Stop Publicidad) de la Asociación Española para la Privacidad Digital, para que al desarrollar, diseñar, seleccionar y usar aplicaciones y servicios que están basados en el tratamiento de datos personales para cumplir su función, tenga presente y en cuenta de manera permanente el derecho fundamental reconocido constitucionalmente a la protección de datos de carácter personal. También se ha concienciado al técnico programador, de que se asegure, con la debida atención al estado de la técnica actual, de que el responsable del tratamiento está en condiciones de cumplir con sus obligaciones legales en materia de protección de datos personales.

3 ¿Ha previsto el responsable del tratamiento cómo establecer el registro de

actividades de tratamiento (RAT) en el seno de la Asociación Española para la Privacidad Digital?: Sí. La Asociación lleva un registro de las actividades de tratamiento efectuadas bajo su responsabilidad. Dicho registro de actividades de tratamiento contiene de manera detallada toda la información legal recogida o establecida por el artículo 30 del RGPD UE 2016/679.

4 ¿Ha previsto la Asociación quién se encargará de mantener actualizado el registro de actividades de tratamiento (RAT)?: Sí. Se encargará de ello una empresa externa especializada en asesoramiento jurídico en materia de protección de datos personales denominada B. Energy, S.L. – nombre comercial: Admindatos. Dicha mercantil actúa legalmente en calidad de encargada del tratamiento.

5 ¿Ha revisado el responsable del tratamiento las medidas de seguridad que aplica a sus tratamientos a la luz de los resultados del análisis de riesgo de los mismos?: Sí. Además adicionalmente, la Asociación lleva a cabo una Auditoría de Medidas de Seguridad en materia de Protección de Datos, con una periodicidad temporal bianual o bienal. Complementariamente se emite el correspondiente informe de Auditoría RGPD.

6 ¿Ha valorado la Asociación suficientemente la posibilidad de introducir medidas de seguridad adicionales en función del tipo de tratamiento o del contexto en que se realiza?: Sí. El responsable del tratamiento a la hora de evaluar la adecuación del nivel de riesgo aplicable, ha tenido particularmente en cuenta los riesgos que presenta cada 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 personales.

7 Atendiendo al tipo de tratamiento que realiza la Asociación, ¿ha establecido ésta mecanismos para identificar con rapidez la existencia de violaciones de la seguridad de los datos o de brechas de seguridad en el ámbito de la protección de los datos personales?: Sí. El responsable del tratamiento toma a tiempo medidas adecuadas, para evitar en la medida de lo posible, teniendo en cuenta el estado de la técnica y de la tecnología existente en el tiempo presente, que las violaciones de la seguridad de los datos personales puedan entrañar daños y perjuicios físicos, materiales o inmateriales para las personas físicas, como pérdida de control sobre sus datos personales o restricción de sus derechos, discriminación, usurpación de identidad, pérdidas financieras, reversión no autorizada de la seudonimización, daño para la reputación, pérdida de confidencialidad de datos sujetos al deber de secreto, o cualquier otro perjuicio económico o social significativo para la persona física en cuestión.

En el hipotético caso del acaecimiento de una brecha de seguridad, el responsable del tratamiento tan pronto como tenga conocimiento de que se ha producido una violación de la seguridad de los datos personales, notificará sin dilación indebida y, de ser posible, a más tardar 72 horas después de que se haya tenido constancia de ella, la violación de la seguridad de los datos personales a la autoridad de control competente (Agencia Española de Protección de Datos – AEPD), a menos que la Asociación esté en condiciones de

poder demostrar, atendiendo al principio de responsabilidad proactiva, la improbabilidad de que dicha violación de la seguridad de los datos entrañe un riesgo para los derechos y las libertades de las personas físicas. Si dicha notificación no fuese posible en el plazo de 72 horas, el responsable del tratamiento acompañará la documentación pertinente con indicación de los motivos de la dilación.

8 ¿Tiene el responsable del tratamiento previstas medidas de reacción frente a los diferentes tipos de quiebras de seguridad, incluidos los procedimientos para evaluar el riesgo que puedan suponer para los derechos y libertades de los afectados?: Sí. La Asociación ha adoptado medidas de protección técnica y organizativa apropiadas y estas medidas se aplican a todos los datos personales que puedan ser afectados por la violación de la seguridad de los datos, en particular aquellas que hagan ininteligibles los datos personales para cualquier persona que no esté autorizada a acceder a ellos, como el cifrado/encriptado. Asimismo la Asociación, está en condiciones reales de adoptar medidas ulteriores a la brecha de seguridad que garanticen que ya no exista la probabilidad de que se concretice el alto riesgo para los derechos y libertades del interesado a que se refiere el artículo 34.1 del RGPD UE 2016/679.

9 ¿Ha establecido el responsable del tratamiento procedimientos para notificar las violaciones de seguridad de los datos a las autoridades de protección de datos y, si fuera necesario a los interesados/afectados?: Sí. Existe un procedimiento claro, estructurado y normalizado, para que en caso de ser necesario notificar por vía telemática las brechas de seguridad de los datos personales a la AEPD y en su caso a las personas afectadas/interesadas. Dicho procedimiento incluye toda la información necesaria recogida y contemplada por los artículos 33 y 34 del RGPD UE 2016/679.

10 ¿Dispone el responsable del tratamiento de un registro o herramienta similar en que pueda documentar los incidentes de seguridad que se produzcan, aunque no sean notificados a las autoridades de protección de datos?: Sí. La Asociación dispone de un documento electrónico sobre valoración de brechas de seguridad RGPD y de otro documento electrónico para registrar las incidencias en materia de protección de datos que se produzcan, para así de esta manera poder documentar cualquier tipo de violación de la seguridad de los datos personales, incluidos los hechos relacionados con dicha brecha, sus efectos y las medidas correctivas adoptadas. De tal manera que dicha documentación permitirá a la autoridad de control competente (AEPD) verificar el cumplimiento de lo estipulado por los artículos 33 y 34 del RGPD UE 2016/679.

11 ¿Ha valorado la Asociación si los tratamientos que realiza requieren una Evaluación de Impacto sobre la Protección de Datos porque supongan un alto riesgo para los derechos y libertades de los interesados?: Sí. Puesto que cuando sea probable que un tipo de tratamiento, en particular si se utilizan nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento estará obligado legalmente a realizar, antes del tratamiento, una

evaluación del impacto de las operaciones de tratamiento en la protección de datos personales. Dejar constancia de que conforme al RGPD UE una única evaluación (EIPD) podrá abordar una serie de operaciones de tratamiento similares que entrañen altos riesgos similares (artículo 35.1 RGPD UE).

12 ¿Dispone la Asociación de una metodología para la realización de la EIPD?: Sí. Dicha Evaluación de Impacto en la Protección de Datos incluye como mínimo los siguientes aspectos:

• Una descripción sistemática de las operaciones de tratamiento previstas y de los fines del tratamiento, inclusive, cuando proceda el interés legítimo perseguido por el responsable del tratamiento;

• Una evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento con respecto a su finalidad;

• Una evaluación de los riesgos para los derechos y libertades de los interesados/afectados;

• Las medidas previstas para afrontar los riesgos, incluidas garantías, medidas de seguridad y mecanismos que garanticen la protección de los datos personales.

11.13 Según el tipo de tratamiento que realiza y los resultados del análisis de riesgos
previo, ¿la Asociación viene obligada legalmente a nombrar un Delegado de Protección de Datos (DPO)?: Sí. Puesto que las actividades principales del responsable del tratamiento pueden consistir en operaciones de tratamiento que, en razón de su naturaleza, alcance y/o fines, requieran una observación habitual y sistemática de interesados/afectados a gran escala (artículo 37.1 b) RGPD UE 2016/679).

14 ¿Ha establecido la Asociación los criterios para seleccionar al Delegado de Protección de Datos y, en particular, para valorar sus cualificaciones profesionales y sus conocimientos?: Sí. El DPO ha sido designado atendiendo a sus cualidades profesionales y, en particular a sus conocimientos especializados del Derecho y la práctica en materia de protección de datos y a su capacidad para desempeñar las funciones indicadas en el artículo 39 del RGPD UE 2016/679.

15 El puesto de DPO tal y como está configurado en la entidad (Asociación Española para la Privacidad Digital), ¿respeta los requisitos de independencia en el ejercicio de las funciones, posición en el organigrama, ausencia de conflicto de intereses y disponibilidad de los recursos necesarios establecidos por el RGPD?: Sí. El responsable del tratamiento garantiza que el DPO no recibe ninguna instrucción en lo que respecta al desempeño de sus funciones. El DPO rinde cuentas directamente al más alto nivel jerárquico del responsable del tratamiento.

El DPO mantiene en todo momento el secreto o la confidencialidad en lo que respecta al desempeño de sus funciones, de conformidad con el Derecho de la Unión o de los Estados miembros.

El DPO desempeña otras funciones y cometidos. No obstante el responsable del

tratamiento garantiza que dichas funciones y cometidos no dan lugar a conflicto de intereses.

16 ¿Ha hecho la Asociación pública la designación del DPO y sus datos de contacto y los ha comunicado a la autoridad de protección de datos nacional?: Sí. El responsable del tratamiento ha publicado debidamente en la página web corporativa de la Asociación, los datos de contacto del DPO y asimismo los ha comunicado por vía telemática a la Agencia Española de Protección de Datos (AEPD).

17 ¿Ha establecido el responsable del tratamiento procedimientos para que los interesados/afectados puedan contactar con el DPO?: Sí. Los interesados podrán ponerse en contacto con el DPO por lo que respecta a todas las cuestiones relativas al tratamiento de sus datos personales y al ejercicio de sus derechos al amparo de la normativa europea de protección de datos (RGPD UE 2016/679) y de la normativa española de protección de datos (LOPD GDD 3/2018). Las comunicaciones podrán realizarse principalmente por vía electrónica (email), por vía telefónica, y por vía postal en caso de no ser posible por medios electrónicos.

E. Aplicación de medida de seguridad

El artículo 24 del Reglamento Europeo de Protección de Datos obliga tanto al responsable como al encargado de tratamiento a adoptar las medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento de datos personales es conforme con dicho Reglamento. Tales medidas deberán ser determinadas en cada caso atendiendo a la naturaleza, el ámbito, el contexto y los fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad que el tratamiento de sus datos personales pueda implicar para los derechos y libertades de los interesados.

De acuerdo con esta previsión, el responsable aplicará toda una serie de garantías teniendo en cuenta el estado de la técnica, el coste de aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, de manera que se pueda asegurar que solo son objeto de tratamiento los datos personales necesarios específicos para cada tratamiento, se conserven durante el plazo mínimo necesario y se garantice su confidencialidad. Igualmente estas medidas garantizan que los datos personales no sean accesibles sin la intervención de una o varias personas físicas.

Las medidas técnicas y organizativas aplicadas por el responsable en relación a los datos objeto del presente tratamiento son las siguientes en función del nivel de riesgo y la gravedad de las consecuencias generadas en caso de violación de seguridad que han sido valoradas en el preceptivo informe de análisis riesgo elaborado por el responsable.

1. Niveles de riesgo y posibles medidas técnicas y organizativas aplicables

Nivel de riesgo bajo:
Cualquier tratamiento de datos personales obliga a incorporar un mínimo de medidas de seguridad básicas.
Nivel de riesgo moderado:
Determinado por la existencia de una probabilidad media de vulneración de derechos de los interesados así como de una gravedad media de los daños generados por tal vulneración.
Nivel de riesgo elevado o muy alto:
Un nivel elevado o un nivel muy alto de riesgo para los derechos y libertades de las personas físicas en relación al tratamiento de sus datos personales puede venir producido por diversas situaciones, por ejemplo, cuando el tratamiento implica la evaluación sistemática y exhaustiva de aspectos personales basado en un tratamiento automatizado, como la elaboración de perfiles, y en base al que se tomen decisiones con efectos jurídicos para sus titulares, o el tratamiento a gran escala de categorías especiales de datos o la observación sistemática a gran escala de zonas de acceso público.

2. Posibles medidas de seguridad para los diferentes niveles de riesgo

(AUT): Aplicable a ficheros con tratamiento automático o mixto.
(MAN): Aplicable a ficheros con tratamiento manual o mixto.
Registro de Actividades de Tratamiento

- **Ámbito de aplicación. (AUT/MAN)**
- **Medidas, normas, procedimientos reglas y estándares de seguridad. (AUT/MAN)**
- **Funciones y obligaciones del personal. (AUT/MAN)**
- **Estructura y descripción de ficheros y sistemas de información. (AUT/MAN)**
- **Procedimiento de notificación, gestión y respuesta ante incidencias. (AUT/MAN)**
- **Procedimiento de realización de copias de respaldo y recuperación de datos. (AUT/MAN)**
- **Medidas para el transporte de soportes y documentos. (AUT/MAN)**
- **Medidas para la destrucción de documentos y soportes o reutilización. (AUT/MAN)**
- **Tratamiento de datos por cuenta de terceros. (AUT/MAN)**
- **Identificación del responsable de seguridad. (AUT/MAN)**
- **Controles periódicos de verificación del cumplimiento. (AUT/MAN)**
- **Medidas a adoptar en caso de reutilización o desecho de soportes. (AUT/MAN)**

Personal
- **Funciones y obligaciones de usuarios y perfiles de usuarios claramente definidas y documentadas.**
(AUT/MAN)

**Difusión entre el personal de las normas que les afecten y de las consecuencias por
incumplimiento.
(AUT/MAN)**
Funciones de control y autorizaciones delegadas. (AUT/MAN)

Incidencias
**Registrar tipo de incidencia, momento en que se ha producido, persona que la notifica,
persona a la que se comunica y efectos derivados y medidas correctoras.
(AUT/MAN)**
**Procedimiento de notificación y gestión de las incidencias y violaciones de seguridad a la Agencia e interesados
(AUT/MAN)**
**Registrar realización de procedimientos de recuperación de los datos, persona que lo ejecuta, datos restaurados y grabados manualmente.
(AUT)**
Autorización por escrito del responsable del fichero para su recuperación. (AUT)

Control de Acceso
**Cada usuario accederá únicamente a recursos que precise para el desarrollo de sus funciones.
(AUT/MAN)**
**Relación actualizada de usuarios y perfiles de usuarios y los accesos autorizados para cada uno de ellos.
(AUT/MAN)**
Mecanismos que eviten el acceso a recursos con derechos distintos de los autorizados. (AUT/MAN)
Conceder, alterar o anular permisos de acceso exclusivamente por personal autorizado. (AUT/MAN)
**Iguales condiciones para personal ajeno al responsable del fichero, con acceso a los
recursos.
(AUT/MAN)**
**Control de acceso físico a los lugares donde se hallen instalados los equipos físicos que den soporte a los sistemas de información.
(AUT)**

Gestión de Soportes y Documentos
**Identificar el tipo de información que contienen. Sistema de etiquetado.
(AUT/MAN)**
Inventario. (AUT/MAN)
Acceso restringido al personal autorizado al almacén de soportes. (AUT/MAN)
**Salida de soportes, incluido e-mail, autorizada por el responsable del fichero.
(AUT/MAN)**

Medidas para el transporte de soportes y documentos, dirigidas a evitar la sustracción, pérdida o acceso indebido.
(AUT/MAN)
Medidas para la destrucción o borrado de documentos y soportes que eviten su acceso posterior o recuperación.
(AUT/MAN)
Medidas optativas de identificación de soportes que dificulten su identificación por personas no autorizadas.
(AUT/MAN)
Registro de entrada y salida de soportes. (AUT)
Identificación de soportes que dificulten su identificación por personas no autorizadas. (AUT)
Cifrado de datos en la distribución de soportes. (AUT)
Cifrado de datos en dispositivos portátiles cuando se encuentren fuera de las instalaciones del responsable.
(AUT)

Identificación y Autenticación
Procedimientos de identificación y autenticación de los usuarios. (AUT)
Se establecerá un mecanismo que permita la identificación de forma inequívoca y personalizada de todo usuario y la verificación de que está autorizado.
(AUT)
Procedimientos de asignación, distribución y almacenamiento que garantice su confidencialidad e integridad.
(AUT)
Periodicidad con que se cambian las contraseñas que no podrá ser superior a un año. (AUT)
Almacenamiento ininteligible de contraseñas activas. (AUT)
Límite de intentos reiterados de acceso no autorizado al sistema de información.
(AUT)

Copias de Seguridad y Respaldo
Procedimiento de copia de respaldo, al menos semanal. (AUT)
Procedimiento para la recuperación de datos que garanticen su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción.
(AUT)
Procedimiento de grabación manual para ficheros parcialmente automatizados.
(AUT)
Verificar cada seis meses la correcta definición, funcionamiento y aplicación de los procedimientos de realización de copias de respaldo y recuperación de los datos.
(AUT)
Prohibición de pruebas con datos reales, salvo que se asegure el nivel de seguridad
correspondiente al tratamiento realizado.
(AUT)

Previamente a pruebas con datos reales, realizar copia de seguridad. (AUT)
Copia de respaldo de los datos y procedimientos de recuperación de los mismo en un lugar diferente del que se encuentren los equipos informáticos que los tratan, que deberá cumplir las medidas de seguridad exigidas o utilizar elementos que garanticen la integridad y recuperación de la información.
(AUT)

Registro de Accesos
Registrar usuario, fecha y hora, fichero accedido, tipo acceso y registro accedido.
(AUT)
Control del responsable de seguridad. Revisión 1 vez al mes y elaboración de un informe mensual de las revisiones y problemas detectados.
(AUT)
Conservación del registro durante 2 años. (AUT)
Excepción: Si responsable del fichero es persona física y sólo él tiene acceso y trata los datos personales.
(AUT)

Telecomunicaciones
Transmisión de datos a través de redes públicas o redes inalámbricas, cifrando los datos o utilizando cualquier otro mecanismo que garantice que la información no sea inteligible o manipulada por terceros.
(AUT)

Criterios de Archivo
De acuerdo con los criterios previstos en su respectiva legislación. En su defecto los fijará el responsable del fichero.
(MAN)
Garantizar la correcta conservación, localización y consulta de la información.
(MAN)
Posibilitar el ejercicio de los derechos de acceso, rectificación, cancelación y oposición al tratamiento.
(MAN)

Dispositivos de Almacenamiento
Los dispositivos de almacenamiento deberán disponer de mecanismos que obstaculicen su apertura y si sus características físicas no lo permiten, el responsable del fichero o tratamiento adoptará medidas que impidan el acceso de personas no autorizadas.
(MAN)

Custodia de Soportes
Cuando no se hallen en los dispositivos de almacenamiento la persona al cargo deberá custodiar la documentación e impedir en todo momento que pueda ser accedida por persona no autorizada.

(MAN)

Almacenaje de Información

Los armarios, archivadores u otros elementos en los que se almacenen los ficheros no automatizados con datos de carácter personal deberán encontrarse en áreas en las que el acceso esté protegido con puertas de acceso dotadas de sistemas de apertura mediante llave u otro dispositivo equivalente.
(MAN)
Dichas áreas deberán permanecer cerradas cuando no sea preciso el acceso a los documentos incluidos en el fichero.
(MAN)
Si, atendidas las características de los locales de que dispusiera el responsable del fichero o tratamiento, no fuera posible cumplir lo establecido en el apartado anterior, el responsable adoptará medidas alternativas que, debidamente motivadas, se incluirán en el documento de seguridad.
(MAN)

Copia o Reproducción

La generación de copias o la reproducción de los documentos únicamente podrá ser
realizada bajo el control del personal autorizado en el documento de seguridad.
(MAN)
Deberá procederse a la destrucción de las copias o reproducciones desechadas de forma que se evite el acceso a la información contenida en las mismas o su recuperación posterior.
(MAN)

Acceso a Documentos

El acceso a la documentación se limitará exclusivamente al personal autorizado.
(MAN)
Se establecerán mecanismos que permitan identificar los accesos realizados en el caso de documentos que puedan ser utilizados por múltiples usuarios.
(MAN)
El acceso de personas no incluidas en el párrafo anterior deberá quedar adecuadamente registrado de acuerdo con el procedimiento establecido al efecto en el documento de seguridad.
(MAN)

Traslado de Documentos

Siempre que se proceda al traslado físico de la documentación contenida en un fichero, deberán adoptarse medidas dirigidas a impedir el acceso o manipulación de la información objeto de traslado.
(MAN)

F. INVENTARIO DE HARDWARE Y SOFTWARE

Inventario hardware

Código: DDE001	Tipo de Hardware: Disco Duro Externo	
S.O.:	Descripción: Copias de Respaldo de datos	
Fabricante: TOSHIBA	Modelo: USB 3.0 HARD DRIVE	Fecha: 01-07-2022
Uso: Privado.		
Dispositivo Portátil: Si		
Sistema de Cifrado:		
Sistema de Etiquetado: Alfanumérico.		

Código: IMM001	Tipo de Hardware: Impresora Multifunción	
S.O.:	Descripción:	
Fabricante: EPSON	Modelo: WORKFORCE WF-7710	Fecha: 01-07-2022
Uso: Compartido.		
Dispositivo Portátil: No		
Sistema de Cifrado:		
Sistema de Etiquetado:		

Código: IMM003	Tipo de Hardware: Impresora Multifunción	
S.O.:	Descripción: Nueva Impresora	
Fabricante: EPSON	Modelo: WorkForce - WF-7830	Fecha: 01-07-2022
Uso: Compartido.		
Dispositivo Portátil: No		
Sistema de Cifrado:		
Sistema de Etiquetado:		

Código: OPE001	Tipo de Hardware: Ordenador Personal	
S.O.: WINDOWS 10	Descripción: Ordenador de Alberto	
Fabricante: Clónico	Modelo:	Fecha: 01-07-2022
Uso: GESTION INTEGRAL.		
Dispositivo Portátil: No		
Sistema de Cifrado:		
Sistema de Etiquetado:		

Código: OPE002	Tipo de Hardware: Ordenador Personal	
S.O.: Windows 10	Descripción: Ordenador de José Manuel de Ramón	
Fabricante: CLÓNICO	Modelo:	Fecha: 01-07-2022
Uso: Compartido.		
Dispositivo Portátil: No		
Sistema de Cifrado:		
Sistema de Etiquetado:		

Código: OPE003	Tipo de Hardware: Ordenador Personal	
S.O.: Windows 10	Descripción: Ordenador de Maribel	
Fabricante: Clónico	Modelo:	Fecha: 01-07-2022
Uso: Compartido.		
Dispositivo Portátil: No		
Sistema de Cifrado:		
Sistema de Etiquetado:		

Código: OPE006	Tipo de Hardware: Ordenador Personal	
S.O.: WINDOWS 10	Descripción: SALA DE JUNTAS - LOCAL 1	
Fabricante: MINIX	Modelo: –	Fecha: 01-07-2022
Uso: COMPARTIDO. LOCAL 1		
Dispositivo Portátil: No		
Sistema de Cifrado:		
Sistema de Etiquetado:		

Código: OTR001	Tipo de Hardware: Otro	
S.O.:	Descripción: Destructora de documentación.	
Fabricante: REXEL	Modelo: RDS2270	Fecha: 01-07-2022
Uso: Destrucción de documentación.		
Dispositivo Portátil: No		
Sistema de Cifrado:		
Sistema de Etiquetado:		

Código: OTR002	Tipo de Hardware: Otro	
S.O.:	Descripción: Centralita Telefonía VO IP	
Fabricante: GRANDSTREAM	Modelo: GXP 2100	Fecha: 01-07-2022
Uso: Gestión administrativa (telefonía VO IP).		
Dispositivo Portátil: No		
Sistema de Cifrado:		
Sistema de Etiquetado:		

Código: OTR003	Tipo de Hardware: Otro	
S.O.: SANGOMA	Descripción: CENTRALITA VOIP - LOCAL 1	
Fabricante: SANGOMA	Modelo: ASTERIK	Fecha: 01-07-2022
Uso: COMPARTIDO. LOCAL 1		
Dispositivo Portátil: No		
Sistema de Cifrado:		
Sistema de Etiquetado:		

Código: OTR006	Tipo de Hardware: Otro	
S.O.:	Descripción: EXTENSION DE VO IP - LOCAL 1	
Fabricante: YEALINK	Modelo: T236	Fecha: 01-07-2022
Uso: COMPARTIDO. LOCAL 1		
Dispositivo Portatil: SI		
Sistema de Cifrado:		
Sistema de Etiquetado: ALFANUMÉRICO.		

Código: SER001	Tipo de Hardware: Servidor	
S.O.: MV WARE ESX I	Descripción: LOCAL 1	
Fabricante: H.P.	Modelo: PROLIANT ML-330	Fecha: 02-01-2019
Uso: PRIVADO. LOCAL 1		
Dispositivo Portatil: No		
Sistema de Cifrado:		
Sistema de Etiquetado:		

Código: SER002	Tipo de Hardware: Servidor	
S.O.: WINDOWS SERVER 2012 R2	Descripción: CONTROLADOR DE DOMINIO - LOCAL 1	
Fabricante: MV WARE	Modelo: -------	Fecha: 02-01-2019
Uso: COMPARTIDO. LOCAL 1		
Dispositivo Portatil: No		
Sistema de Cifrado:		
Sistema de Etiquetado:		

Código: SER003	Tipo de Hardware: Servidor	
S.O.: WINDOWS 7	Descripción: ESCRITORIO REMOTO - LOCAL 1	
Fabricante: MV WARE	Modelo: ---	Fecha: 02-01-2019
Uso: COMPARTIDO. LOCAL 1		
Dispositivo Portatil: No		
Sistema de Cifrado:		
Sistema de Etiquetado:		

Código: SER004	Tipo de Hardware: Servidor	
S.O.: WINDOWS SERVER 2012 R2	Descripción: COPIAS DE SEGURIDAD - LOCAL 1	
Fabricante: H.P.	Modelo: MICROSERVER	Fecha: 02-01-2020
Uso: PRIVADO. LOCAL 1		
Dispositivo Portatil: No		
Sistema de Cifrado:		
Sistema de Etiquetado:		

Inventario software

Aplicación	Versión	Fabricante	Fecha
3CX Phone	2012	3CX Ltd.	01-07-2022
Aplicación ProDAG 4	4.11	AG Ediciones	01-07-2022
FIREBASE	2022	GOOGLE LLC	01-07-2022
Moodle	1.9.7.	Moodle tm	01-07-2022
PLUGIN FETCH	2022	¿?	01-07-2022
Página Web LISTASTOPPUBLICIDAD	2022	¿?	01-07-2022
SANGOMA S.O. CENTRALITA VOIP	¿?	¿?	01-07-2022
Tecnópolis Gestión	10.7.5.133	Tecnópolis software S.L.L.	01-07-2022
Tecnópolis Gestión	10.7.5.133	Tecnópolis Software S.L.L.	01-07-2022
Windows	10 PRO	MICROSOFT	01-07-2022
Windows	7	Microsoft Corporation	02-01-2019
Windows Server	2012 R2	Microsoft Corporation	02-01-2019

En Orihuela (Alicante) a 31 de agosto de 2022

EIPD: ASOCIACIÓN ESPAÑOLA PARA LA PRIVACIDAD DIGITAL

Firma en nombre de la entidad responsable del tratamiento
D.: José Manuel de Ramón Rodríguez
Cargo: Presidente de la Asociación Española para la Privacidad Digital
Correo electrónico: presidente@asociacionepd.es
Teléfono: 676455441 - 655489888

Firma del Delegado de Protección de Datos
D.: Alberto Giménez Rodríguez
Correo electrónico: dpo@asociacionepd.es
Teléfono: 633187315 - 655489888