20210210, Nota Informativa, Pacto Digital.

En virtud de mis compromisos contractuales, seguidamente quiero participaros de la propuesta que ha lanzado la AEPD hace unos días sobre la posibilidad de unirse al denominado Pacto Digital.

El pasado 28 de enero se celebró el día mundial de protección de datos, con ese motivo, la Agencia Española de Protección de Datos ha lanzado el PACTO DIGITAL PARA LA PROTECCIÓN DE LAS PERSONAS, una iniciativa que tiene como objetivo promover un compromiso firme con la privacidad en las políticas de sostenibilidad y los modelos de negocio de las organizaciones, compatibilizando el derecho fundamental a la protección de datos con la innovación, la ética y la competitividad empresarial.

Esta iniciativa está orientada a reforzar el derecho a la protección de datos a la vez que se promueve la innovación y la sostenibilidad. El desarrollo del proyecto ha contado con la colaboración de algunas de las principales organizaciones empresariales, fundaciones, asociaciones de medios de comunicación y grupos audiovisuales, y está abierto a las organizaciones quieran asumir los compromisos reflejados en la carta de adhesión.

El PACTO DIGITAL PARA LA PROTECCIÓN DE LAS PERSONAS promueve la privacidad como un activo para organizaciones públicas y privadas. Entre los principios que se recogen se encuentra impulsar la transparencia para que los ciudadanos conozcan qué datos se están recabando y para qué se emplean, promover la igualdad de género y la protección de la infancia y las personas en situación de vulnerabilidad, o garantizar que las tecnologías eviten perpetuar sesgos o aumentar las desigualdades existentes, evitando la

discriminación algorítmica por razón de raza, procedencia, creencia, religión o sexo, entre otras.

Mediante la adhesión al PACTO DIGITAL, las entidades se comprometen a implantar los principios y recomendaciones recogidas en el mismo, así como a difundir entre sus empleados y usuarios el Canal prioritario para solicitar la eliminación urgente de contenidos sexuales y violentos en internet, así como otros recursos y herramientas para ayudar a la concienciar sobre el valor de la privacidad y la importancia del tratamiento de los datos personales.

La información y la posibilidad de unirse al Pacto Digital (mediante solicitud a través de la Sede Electrónica de la AEPD con Certificado Digital) se puede encontrar en el siguiente enlace: https://www.aepd.es/es/pactodigital

Considero que unirse al Pacto Digital puede ser una buena oportunidad para implementar estrategias éticas adecuadas en nuestras organizaciones, dotándolas, al mismo tiempo, de un distintivo de calidad que puede ser muy relevante.

Con casi total seguridad, al Pacto Digital se irán sumando un gran número de entidades públicas y privadas, por lo que no estaría de más que pensaran seriamente en la posibilidad de unirse a él.

Bajo estas líneas, adjunto el documento del Pacto Digital al completo.

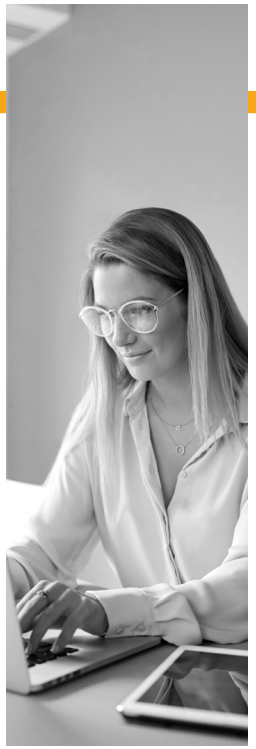
En todo caso, y como siempre, quedo a vuestra disposición para aclarar cualquier duda sobre la cuestión comentada.

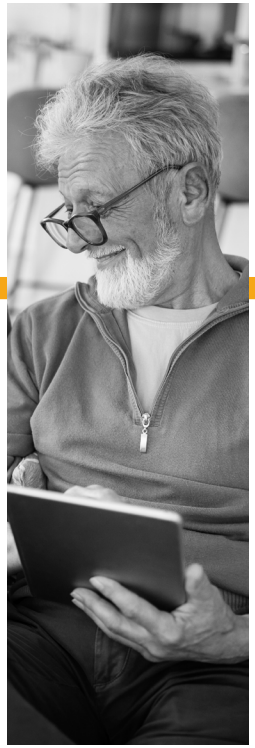
Hecho conforme a mi leal saber y entender, en Manilva a 10 de febrero de 2021,

Salvador Zotano Sánchez

(Delegado de Protección de Datos Certificado 19-ADK0101 conforme al Esquema AEPD-DPD)

agencia española protección datos





Pacto Digital para la protección de las personas

ÍNDICE

PRESENTACIÓN

La Agencia Española de Protección de Datos (AEPD) presentó en 2019 el documento Marco de Responsabilidad Social, con un Plan de acción de 103 iniciativas en ámbitos como la educación y los menores, la igualdad de género, la innovación y el emprendimiento, el medio ambiente, el buen gobierno y la transparencia, y los trabajadores y trabajadoras. Estas iniciativas están plenamente alineadas con los Objetivos de Desarrollo Sostenible (ODS) de la Agenda 2030, especialmente los ODS 5, 12, 16 y 17.

Nuestro compromiso con la Sociedad nace de nuestra propia razón de ser como organismo público que tiene como misión tutelar un derecho fundamental. Partiendo de esta premisa, adquirimos una responsabilidad con la ciudadanía y con los sujetos obligados que se plasma en nuestro Marco de Responsabilidad Social bajo dos conceptos clave:

- Combatir la violencia en internet, especialmente contra las mujeres.

- Favorecer la innovación en el terreno de la privacidad y de la protección de datos, de modo que ésta no sea un obstáculo para el desarrollo de la economía digital.

Entre las medidas para combatir la violencia digital, destaca la creación del Canal prioritario para solicitar la retirada urgente en Internet de contenidos sexuales o violentos.

Se trata de una iniciativa pionera a nivel mundial con el que la Agencia pretende proporcionar a la ciudadanía una respuesta institucional rápida y eficaz a la problemática de la violencia digital, cada vez más habitual y con un fuerte impacto sobre la vida privada de las víctimas de este tipo de conductas, especialmente mujeres y jóvenes, pero también en otras situaciones especialmente graves, como el racismo y la homofobia.

Medidas similares se han promovido también en el entorno empresarial, donde también se pueden deducir otras posibles responsabilidades, como pueden ser las derivadas de la omisión de medidas de prevención o protección o por no evaluar adecuadamente los riesgos laborales para las personas trabajadoras.

Estas acciones son un ejemplo evidente de enfoque preventivo y de responsabilidad proactiva que establece el Reglamento General de Protección de Datos. El RGPD opta por una doble estrategia de prevención y de flexibilización que hacen necesario un cambio de mentalidad en el modo de cumplimiento.

En este contexto ha de enmarcarse la iniciativa que ha puesto en marcha esta Agencia, encaminada a promover la adhesión a un gran pacto por la convivencia ciudadana en el ámbito digital bajo la denominación de **PACTO DIGITAL PARA LA PROTECCIÓN DE LAS PERSONAS**, en el que se pone en valor la privacidad como un activo para las organizaciones públicas y privadas.

Con esta iniciativa queremos reforzar los derechos en el entorno digital, y concienciar a la vez de que junto a un derecho puede existir también una obligación. Para ello, es necesario que todos los actores implicados en el ámbito digital, la ciudadanía y las organizaciones, sean conscientes de las consecuencias que puede suponer en la vida de la persona afectada la difusión de contenidos especialmente sensibles y también las responsabilidades en que pueden incurrir aquellos que los difunden (civiles, penales, administrativas y, en su caso, educativas y laborales).

Entrando ya en el alcance concreto de la iniciativa que estamos impulsando, cabe señalar que su adhesión supone asumir una serie de compromisos que figuran relacionados a lo largo de los tres grandes documentos que la integran.

Mediante la **Carta de Adhesión**, la entidad firmante se compromete, de una parte, a implantar en sus respectivas organizaciones los principios y recomendaciones contemplados en los otros dos documentos que conforman el contenido del Pacto, y, de otra, como compromisos adicionales, a difundir entre su personal, usuarios y usuarias el Canal prioritario para solicitar la eliminación urgente de contenidos sexuales y violentos en internet, así como otros recursos y herramientas que la AEPD ha puesto a disposición de los sectores público y privado y de la ciudadanía para ayudar a la sensibilización sobre el valor de la privacidad y la importancia del tratamiento de los datos personales, también en el entorno laboral. Herramientas y recursos con los que queremos extender nuestra política de tolerancia cero frente a los casos de violencia digital a todas las organizaciones comprometidas.

En general, se busca que las entidades adheridas a esta iniciativa asuman un compromiso firme en sus políticas de sostenibilidad y en sus respectivos modelos de negocio, y ello no sólo por tratarse de un derecho fundamental de las personas que, como tal, hay que proteger adecuadamente, sino también, y al mismo tiempo, por considerarse cada vez más como un activo de las propias organizaciones públicas y privadas y como un elemento distintivo de la competitividad.

El segundo documento **-Compromiso por la responsabilidad en el ámbito digital-** contiene las obligaciones específicas de las organizaciones en el ámbito digital, impulsando su difusión en su organización y ante terceros.

Es importante destacar que no se pretende que las organizaciones adheridas asuman más obligaciones de las que legalmente le corresponden, sino de precisar un compromiso específico en el ámbito digital que debe ser objeto de una especial diligencia por parte de las organizaciones firmantes.

Como correlato de estas obligaciones, el documento pasa a enumerar las responsabilidades en que podrán incurrir las personas firmantes en caso de incumplimiento de las mismas, especialmente las conductas relacionadas con la llamada "violencia digital": de carácter administrativo por infracción de la normativa de protección de datos o de la normativa laboral y de prevención de riesgos; civiles y penales, e incluso disciplinarias en el ámbito educativo por la realización de conductas como el acoso al alumnado.

Finalmente, el documento incorpora algunos principios que, desde la perspectiva de la ética y la protección de datos, la llamada ética digital, deberían tenerse especialmente en cuenta a la hora de diseñar e implantar los nuevos desarrollos tecnológicos. Entre los principios éticos más significativos relacionados con la privacidad estarían los relativos a impulsar la mayor transparencia posible para que los usuarios y usuarias conozcan qué datos se están recabando, cuándo se registran y para qué se emplean; promover la igualdad de género, la protección de la infancia, de las víctimas y de las personas en situación de vulnerabilidad, o garantizar que las tecnologías eviten perpetuar los sesgos o aumentar las desigualdades existentes, evitando la discriminación algorítmica por razón de raza, procedencia, creencia, religión o sexo, entre otras.

El tercer documento que integra la presente iniciativa de la AEPD es el **Decálogo de buenas prácticas en privacidad para medios de comunicación y organizaciones con canales de difusión propios**, con el que la Agencia quiere promover la lucha contra la violencia digital tanto entre los medios de comunicación como con todas aquellas organizaciones que disponen de canales de difusión propios para informar sobre temas de interés para sus públicos, ya sea mediante sus redes sociales o con revistas o boletines corporativos.

Por último, se incluye un **Anexo** con la relación de más de cien **herramientas, guías, materiales y recursos** que la AEPD ha puesto a disposición de la ciudadanía y de los responsables para promover un mayor conocimiento y facilitar un mejor cumplimiento de la normativa de protección de datos.

Para afrontar con garantías un reto de este calado resulta imprescindible tejer alianzas con las principales asociaciones, fundaciones y organizaciones empresariales y del tercer sector, en las que, desde el primer momento, no hemos encontrado más que una plena disposición a adherirse a esta iniciativa y a participar de forma activa en su definición y contenido.

En reciprocidad, desde la Agencia hemos sido totalmente receptivos a incorporar cuantas sugerencias y comentarios nos han hecho llegar, y creemos que los documentos reflejan fielmente los objetivos que nos marcamos cuando acordamos poner en marcha esta iniciativa estratégica para posicionar a la Agencia y a sus grupos de interés en la primera línea de la lucha contra la violencia digital.

En consecuencia, no podemos más que dar las gracias a las organizaciones que se adhieran a la presente iniciativa por el apoyo y la confianza que han depositado en nuestra institución.

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

01 CARTA DE ADHESIÓN

La entidad firmante declara públicamente su compromiso con las personas a través del derecho fundamental a la protección de sus datos y su privacidad, tanto de sus clientes y/o usuarios como de su personal, y con un uso responsable y ético de las tecnologías, para lo que promoverá desde su ámbito de actuación cuantas iniciativas posibiliten dicho objetivo.

En consecuencia, mediante la presente **CARTA**, la entidad firmante se adhiere:

- Al documento **"Compromiso por la Responsabilidad en el Ámbito Digital"**, en el que se contienen las obligaciones específicas de las organizaciones en el ámbito digital y las responsabilidades en que podrán incurrir ante el eventual incumplimiento de las mismas, impulsando su difusión en el seno de su organización y ante terceros, para promover las condiciones adecuadas de convivencia desde el respeto a la privacidad en el entorno digital.

- Al **Decálogo de buenas prácticas en privacidad para medios de comunicación y organizaciones con canales de difusión propios**.

Asimismo, asume los siguientes COMPROMISOS en favor de la protección de los datos personales y la privacidad, la innovación y la sostenibilidad:

- A difundir, en función de los medios disponibles, la información sobre el Canal Prioritario que ha puesto en marcha la Agencia Española de Protección de Datos para ayudar a la ciudadanía en los casos urgentes y graves de violencia digital, y a fomentar las buenas prácticas para evitar la violencia digital, que afecta mayoritariamente a las niñas y mujeres.

- A promover un entorno laboral libre de acoso, especialmente en el ámbito digital, oponiéndose frontalmente al uso y difusión de datos personales que supongan tratamientos ilícitos de datos que pudieran socavar el derecho a la privacidad de sus empleados y empleadas. Los principios de igualdad, dignidad, no discriminación y el derecho a la integridad física y moral son principios jurídicos universales, consagrados en la Constitución Española, que asigna a los poderes públicos la obligatoriedad de promover las condiciones necesarias para que la igualdad y no discriminación sean efectivas. Para ello, impulsará las Recomendaciones de la AEPD para la prevención del acoso sexual digital en el ámbito laboral.

- A promover la innovación y la transformación digital desde un enfoque basado en los principios de la ética, la responsabilidad y la transparencia, en relación con aquellos productos y servicios que lleven a cabo tratamientos masivos de datos, tanto en el número de personas como en la extensión de los datos recogidos de cada persona, en especial los que incluyan Inteligencia Artificial (IA).

- A establecer directrices de teletrabajo que sean respetuosas con la privacidad, en particular de los propios empleados y empleadas, que garanticen la mínima intrusión en su esfera personal.

- A difundir, en su ámbito de actuación, en función de los medios disponibles, los recursos, cuya relación se adjunta a la presente Carta, que la AEPD ha puesto a disposición de los sectores público y privado y de la ciudadanía para ayudar a la sensibilización sobre el valor de la privacidad y la importancia del tratamiento de los datos personales, y garantizar su respeto.

- A impulsar campañas informativas, en función de los medios disponibles, destinadas a la formación y sensibilización en materia de privacidad y protección de datos personales, a fin de reducir las desigualdades en el ámbito digital ('brecha digital'), especialmente en los sectores más vulnerables de la población.

- A promover campañas de sensibilización digital a menores para lograr que éstos hagan un uso equilibrado y responsable de los dispositivos digitales y de los servicios de la sociedad de la información a fin de garantizar el adecuado desarrollo de su personalidad. Para prevenir los riesgos de un uso abusivo de los mismos, se ponen a disposición los recursos y materiales cuya relación se adjunta.

- A incorporar la protección de los datos personales a la hora de diseñar las políticas de sostenibilidad y responsabilidad social, incluyendo actuaciones orientadas específicamente a garantizar el cumplimiento de este derecho fundamental como activo de las organizaciones públicas y privadas y como elemento distintivo de la competitividad. En este sentido, se considera una buena práctica el hecho de incluir en los Principios de Negocio Responsable o el Código Ético de la compañía, la oposición categórica a cualquier práctica que sugiera conductas o prácticas de acoso laboral, sexual y por razón de discriminación también en el entorno digital (acoso digital o ciberacoso).

La Asociación Española de Fundaciones (AEF), las fundaciones y otras entidades del tercer sector, atendiendo especialmente a su misión social en función de los medios y disponibilidades existentes, valoran y estiman positivamente las iniciativas que la AEPD lleva a cabo en materia de servicio, defensa y protección en favor de la sociedad y en especial hacia los segmentos menos favorecidos de nuestro entorno; la AEPD lo tendrá especialmente en cuenta en el seguimiento y aplicación de esta iniciativa, que requiere la adaptación de estos compromisos a las necesidades y características de estas entidades.

La validez de este compromiso es de un año, con renovación automática, salvo desistimiento de la entidad adherida.

02 COMPROMISO POR LA RESPONSABILIDAD EN EL ÁMBITO DIGITAL

La protección de las personas en relación con el tratamiento de datos personales es un derecho fundamental.

La Constitución española garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen. Como derecho fundamental distinto reconoce el derecho a la autodeterminación informativa o libertad informática, que es el derecho a la protección de datos personales, complementario del anterior, pero que no se reduce sólo a los datos íntimos, sino que abarca todos aquellos que identifiquen o permitan la identificación de la persona, pudiendo servir para la confección de su perfil ideológico, racial, sexual, económico o de cualquier otra índole, o que sirvan para cualquier otra utilidad que en determinadas circunstancias constituya una amenaza para el individuo (STC 292/2000).

Los principios de igualdad, dignidad, no discriminación y el derecho a la integridad física y moral son principios jurídicos universales, consagrados en la Constitución Española, que asigna a los poderes públicos la obligatoriedad de promover las condiciones necesarias para que la igualdad y no discriminación sean efectivas.

El artículo 8, apartado 1, de la Carta de los Derechos Fundamentales de la Unión Europea y el artículo 16, apartado 1, del Tratado de Funcionamiento de la Unión Europea establecen que toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan.

El Reglamento General de Protección de Datos -Reglamento (UE) 2016/679 (RGPD)- y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD) configuran conjuntamente el desarrollo del derecho fundamental a la protección de datos de carácter personal.

La mayor novedad que presenta el Reglamento europeo es la evolución de un modelo basado en el control, fundamentalmente de carácter formal, del cumplimiento de la normativa de protección de datos a otro que descansa en el principio de responsabilidad activa, que exige una previa valoración por el responsable o por el encargado del tratamiento del riesgo que pudiera generar el tratamiento de los datos personales para, a partir de esa valoración, adoptar las medidas que procedan.

Así, con carácter general, el responsable deberá aplicar medidas adecuadas y eficaces y poder demostrar la conformidad de las actividades de tratamiento con la normativa aplicable (RGPD y LOPDGDD), incluida la eficacia de las medidas adoptadas, que se revisarán y actualizarán cuando sea necesario.

Dichas medidas deberán tener en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento, así como el riesgo para los derechos y libertades de las personas físicas (artículos 24.1 RGPD y 28 LOPDGDD).

El responsable del tratamiento deberá adoptar, por tanto, una actitud proactiva, incorporando el valor de la privacidad en su actividad ordinaria, garantizando el cumplimiento de este derecho como un activo de la organización y un elemento distintivo de competitividad en el mercado.

Para el pleno desarrollo del derecho fundamental a la protección de los datos personales y a la privacidad, las organizaciones firmantes asumen el compromiso de cumplir con especial diligencia las siguientes obligaciones

OBLIGACIONES ESPECÍFICAS EN EL ÁMBITO DIGITAL

Informar a los usuarios y usuarias sobre el tratamiento de sus datos y el ejercicio de sus derechos

Las organizaciones deberán informar de forma clara y sencilla sobre los aspectos más importantes del tratamiento de sus datos, identificando quién los trata, con qué base jurídica, para qué finalidad, y sobre la forma de ejercer sus derechos. No podrá denegarse el ejercicio de estos derechos en el caso de que la persona quiera ejercitarlos por un procedimiento o cauce diferente al que se le ofrezca (artículos 13 y 14 RGPD y 11 LOPDGDD).

En particular,
promoverán informar de forma destacada a los usuarios y usuarias sobre las medidas y herramientas para garantizar su privacidad.

Aplicar los principios relativos al tratamiento

Las organizaciones deberán aplicar en el tratamiento de los datos de clientes, su personal, proveedores, ciudadanos y ciudadanas los principios de licitud, lealtad, transparencia, limitación de la finalidad, minimización, exactitud, limitación del plazo de conservación, integridad, confidencialidad y responsabilidad proactiva, con el alcance dado a los mismos por el artículo 5 del RGPD.

Garantizar la licitud del tratamiento

Las organizaciones estarán obligadas a garantizar la licitud del tratamiento de los datos de clientes, su personal, ciudadanos y ciudadanas sobre la base de alguna de las causas contempladas en el artículo 6 y también, en caso de categorías especiales de datos personales (datos de salud, de carácter político o sindical, relativos a la vida sexual, etc.), en su artículo 9, ambos del RGPD.

Designar un Delegado de Protección de Datos (DPD)

Las organizaciones privadas deberán designar, en los supuestos legalmente exigibles, y las entidades del sector público, en todo caso, a una persona como Delegado/a de Protección de Datos que cuente con la debida cualificación, garantizándole los medios necesarios para el ejercicio de sus funciones de manera independiente, debiendo comunicar la designación a la Agencia Española de Protección de Datos (artículos 37 a 39 RGPD, y 34 a 36 LOPDGDD). En particular, se prestará especial atención en designar como DPD a quienes acrediten la cualificación y la capacitación profesional que se requieren para su desempeño.

Se promoverá especialmente la designación de Delegados/as de Protección de Datos en los casos en que no resulte legalmente obligatorio, siempre que las circunstancias del tratamiento así lo aconsejen y la entidad disponga de los recursos para ello. La organización ofrecerá todo el apoyo necesario al DPD para que pueda atender en las mejores condiciones las reclamaciones que le dirijan los ciudadanos y ciudadanas cuando opten por esta vía antes de plantear una reclamación ante la AEPD, o en los casos en que la AEPD decida su traslado a la persona responsable con carácter previo a su admisión a trámite (artículo 65.4 LOPDGDD).

Aplicar la privacidad “desde el diseño” y “por defecto”

Las organizaciones deberán aplicar, tanto a la hora de determinar los medios de tratamiento como en el momento del propio tratamiento, es decir, “desde el diseño”, medidas técnicas y organizativas apropiadas, e integrar las garantías necesarias en el tratamiento, a fin de cumplir eficazmente las obligaciones legales y proteger los derechos de las personas afectadas (artículo 25.1 RGPD).

Asimismo, promoverán la aplicación de las medidas técnicas y organizativas apropiadas para garantizar que, por defecto, sólo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento. Esta obligación se aplicará a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad (artículo 25.2 RGPD).

El incumplimiento de estas obligaciones específicas, podrá dar lugar a las siguientes responsabilidades en el ámbito digital.

RESPONSABILIDADES EN EL ÁMBITO DIGITAL

PERSONAS ADULTAS

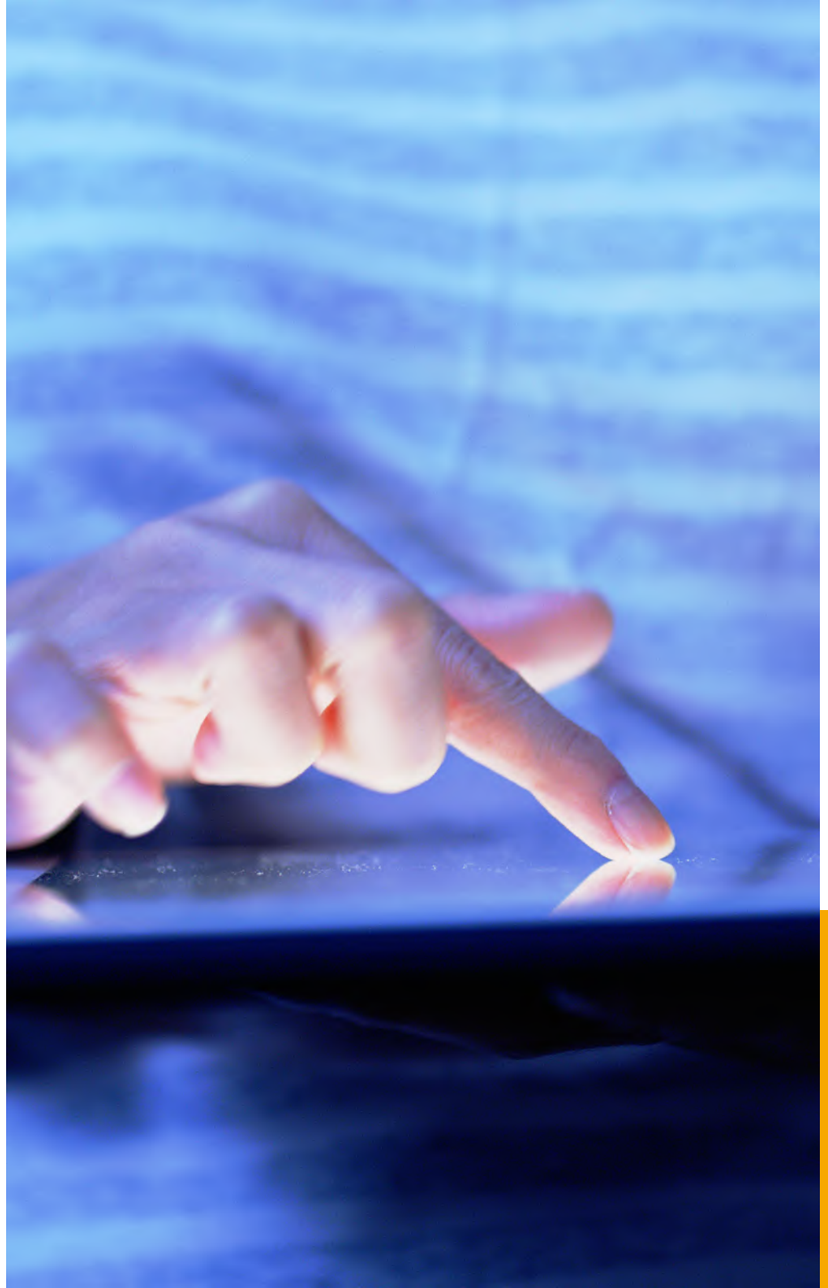
Responsabilidad administrativa por infracción de la normativa de protección de datos

Entre los hechos que constituirían una infracción a la normativa de protección de datos y que serían, por tanto, susceptibles de sanción, se encuentran:

- No facilitar la información que permita a las personas usuarias conocer quién y para qué tratarán sus datos personales.
- Conseguir los datos personales de una persona de manera ilícita, engañosa o fraudulenta, en particular, mediante la suplantación de la identidad.
- Utilizar los datos de carácter personal de una persona o comunicarlos a terceros sin una base jurídica que lo permita, en particular si se trata de datos sensibles como la ideología, religión, creencias, origen étnico, salud, vida y orientación sexual.
- Utilizar los datos de carácter personal de una persona para fines distintos e incompatibles de aquellos para los que fueron recogidos.

Las víctimas de violencia de género gozan de especial protección que alcanza a la utilización, acceso y difusión de sus datos personales, a fin de evitar verse expuestas a nuevos riesgos de dicha naturaleza.

En particular, la difusión de datos especialmente sensibles de una persona física (en contenidos tales como imágenes, audios o videos de carácter sexual o violento que permitan identificarla) publicados a través de los diferentes servicios de internet sin consentimiento, se considera un tratamiento ilícito de datos personales y, por tanto, puede constituir una infracción de la normativa de protección de datos sancionable por la Agencia Española de Protección de Datos con multas que en los casos más graves pueden alcanzar los 20 millones de euros o el 4% del volumen global de facturación de la compañía (art. 83.5 RGPD).



Responsabilidad civil

Los ciudadanos y ciudadanas podrían tener que indemnizar a la persona afectada por los daños y perjuicios, materiales y morales, que se deriven de su conducta ilícita en materia de protección de datos personales (artículos 82 RGPD; 1.101 y 1.902 Código civil).

Los padres, tutores, acogedores y guardadores legales o de hecho podrían tener que responder igualmente por los daños y perjuicios causados por sus hijos y tutelados menores con sus dispositivos móviles (artículo 1.903 Código Civil).

Para un conocimiento más detallado de los delitos en los que se puede incurrir y de su alcance, consultar la Guía de Protección de Datos y prevención de delitos

Responsabilidad Penal

La evolución de las tecnologías de la información y la comunicación y la extensión de su uso a través de los servicios y aplicaciones de Internet, como redes sociales, mensajería instantánea o correo electrónico en dispositivos inteligentes, ha llevado a que se utilicen como un cauce habitual no sólo para la comisión de infracciones en materia de protección de datos, sino también hechos tipificados como delitos. Expresiones como ciberacoso, ciberbullying, sexting, grooming, phishing, pharming o carding, que cada vez nos resultan más familiares, son términos en inglés que identifican situaciones de acoso, amenazas, coacciones, revelación de secretos, delitos sexuales, violencia de género o estafas.

El código penal tipifica determinadas conductas en el ámbito digital como delitos, como los que atentan a la integridad moral, de descubrimiento y revelación de secretos, de amenazas, coacciones, acoso; calumnias e injurias, de violencia de género, suplantación de identidad, o de daños informáticos, entre otros.

Responsabilidad disciplinaria por infracción en el entorno laboral

Para la empresa

– Infracciones en materia de relaciones laborales

La Ley sobre Infracciones y Sanciones en el Orden Social tipifica como infracciones muy graves:

> *"Los actos del empresario que fueren contrarios al respeto de la intimidad y consideración debida a la dignidad de los trabajadores" (artículo 8.11).*

> *"El acoso sexual, cuando se produzca dentro del ámbito a que alcanzan las facultades de dirección empresarial, cualquiera que sea el sujeto activo de la misma" (artículo 8.13).*

> *"El acoso por razón de origen racial o étnico, religión o convicciones, discapacidad, edad y orientación sexual y el acoso por razón de sexo, cuando se produzcan dentro del ámbito a que alcanzan las facultades de dirección empresarial, cualquiera que sea el sujeto activo del mismo, siempre que, conocido por el empresario, éste no hubiera adoptado las medidas necesarias para impedirlo" (artículo 8.13 bis).*

Las infracciones muy graves se sancionan por la Inspección de Trabajo y Seguridad Social con multas que van desde 6.251 a 187.515 euros.

– Infracciones en materia de prevención de riesgos laborales

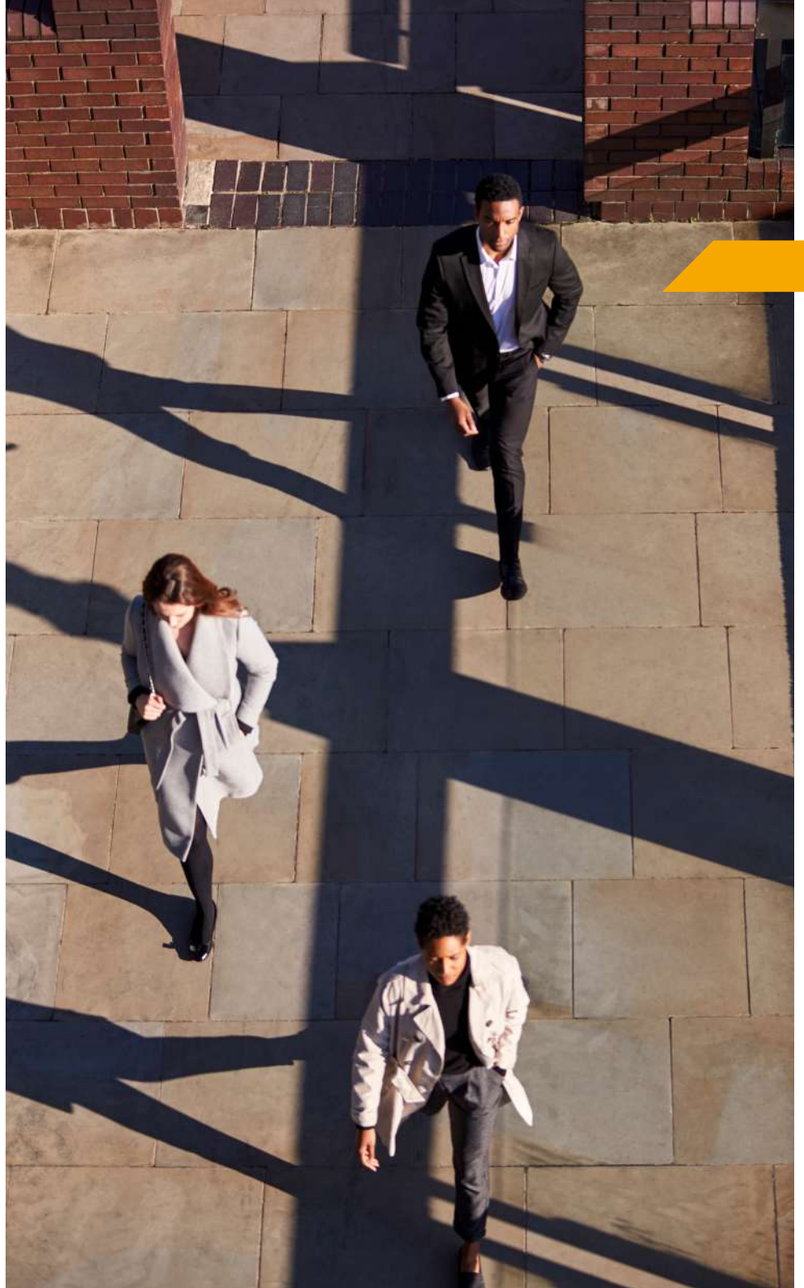
Asimismo, se tipifican como infracciones graves:

> *"No llevar a cabo las evaluaciones de riesgos y, en su caso, sus actualizaciones y revisiones, así como los controles periódicos de las condiciones de trabajo y de la actividad de los trabajadores que procedan, o no realizar aquellas actividades de prevención que hicieran necesarias los resultados de las evaluaciones, con el alcance y contenido establecidos en la normativa sobre prevención de riesgos laborales" (artículo 12.1.b).*

Las infracciones graves se sancionan por la Inspección de Trabajo y Seguridad Social con multas que van desde 626 a 6.250 euros.

– Infracciones en materia de igualdad

Finalmente, hay que hacer referencia a la responsabilidad que se deriva en virtud de lo que establece la Ley Orgánica 3/2007, de 22 de marzo, para la igualdad efectiva de mujeres y hombres que, en sus artículos 45 y 46, establece la obligación de que las empresas que reúnan ciertos requisitos (más de 50 trabajadores, cuando así lo establezca el convenio colectivo o lo acuerde la autoridad laboral en un procedimiento sancionador) dispongan de un plan de igualdad que contenga un conjunto de medidas tendentes a alcanzar la igualdad de trato y oportunidades entre mujeres y hombres, así como a eliminar la discriminación por razón de sexo. Mediante el Real Decreto-Ley 6/2019, de 1 de marzo, se establecieron nuevas obligaciones, en especial en lo relativo a la constitución, características y condiciones para la inscripción y acceso al Registro de Planes de Igualdad.



Para los empleados y empleadas

Los trabajadores podrán ser sancionados por incumplimientos laborales, de acuerdo con la graduación de faltas y sanciones establecidas en las disposiciones legales o en los convenios colectivos aplicables, que, en caso de faltas muy graves, pueden llegar incluso al despido disciplinario (artículo 58 del Estatuto de los Trabajadores).

En el caso de personal funcionario, puede implicar el traslado, suspensión de funciones o incluso la separación del servicio (artículos 93 y siguientes del Estatuto Básico del Empleado Público).

MAYORES DE 14 Y MENORES DE 18 AÑOS

Responsabilidad administrativa por infracción de la normativa de protección de datos

La responsabilidad por hechos constitutivos de infracción a la normativa de protección de datos es aplicable, con la misma extensión y alcance indicados anteriormente, cuando son cometidos por mayores de 14 años, edad en la que, conforme establece la LOPDGDD, pueden prestar el consentimiento para el tratamiento de sus datos personales y ejercitar sus derechos en materia de protección de datos. Es además la edad en la que se responde por infracciones penales reguladas en la Ley Orgánica 5/2000, de responsabilidad penal de los menores.

– Responsabilidad civil

La responsabilidad de los menores de edad se gradúa por la edad. Así, los daños y perjuicios, tanto materiales como morales, causados a terceros originados por menores de edad, pero mayores de 14 años, dan lugar a la exigencia de responsabilidad civil con arreglo al siguiente esquema:

- Los padres o tutores responden de manera solidaria cuando los daños y perjuicios se deriven de conductas tipificadas como delito.

- Los padres o tutores responden igualmente cuando los daños y perjuicios se deben a actos que no sean delitos cometidos por quienes están bajo su guarda (culpa “in vigilando”), pero que se produzcan como consecuencia de una infracción a la normativa de protección de datos, con independencia de la responsabilidad administrativa en que por tal infracción se haya podido incurrir.

– Responsabilidad penal

La Ley Orgánica 5/2000, reguladora de la responsabilidad penal de los menores (LORPM) se aplica a las conductas tipificadas como delitos o faltas en el Código Penal o en leyes penales especiales cometidas por menores de edad entre 14 y 17 años.

Entre las medidas que, conforme al artículo 7 de la citada ley orgánica, se pueden imponer por los Jueces de Menores están el internamiento; el tratamiento ambulatorio; la asistencia a un centro de día para realizar actividades de apoyo, educativas, formativas, laborales o de ocio; la permanencia de fin de semana en el domicilio o en un centro; la libertad vigilada, etc.

– Responsabilidad disciplinaria en el ámbito educativo

En el ámbito educativo también dan lugar a responsabilidad disciplinaria, cuando se producen en los centros escolares, conductas como el acoso al alumnado, su intimidación, humillación, las ofensas graves, su discriminación, o de violencia realizadas a través de las redes sociales y servicios equivalentes en internet y que en ocasiones responden a alguno de los delitos antes expuestos.

La Ley Orgánica 2/2006, de Educación, recoge entre los principios del sistema educativo:

- La transmisión y puesta en práctica de valores que favorezcan la libertad personal, la responsabilidad, la ciudadanía democrática, la solidaridad, la tolerancia, la igualdad, el respeto y la justicia, así como que ayuden a superar cualquier tipo de discriminación.
- La educación para la prevención de los conflictos y para la resolución pacífica de los mismos, así como la no violencia en todos los ámbitos de la vida personal, familiar y social.
- El desarrollo de la igualdad de derechos y oportunidades y el fomento de la igualdad efectiva entre hombres y mujeres.

En desarrollo de estos principios, las Comunidades Autónomas han aprobado normas que regulan la convivencia en los centros educativos en las que se contempla la imposición de medidas correctivas que van desde la amonestación verbal, o el apercibimiento por escrito, a la suspensión del derecho de asistencia al centro o la expulsión del alumno o alumna.

– Responsabilidad laboral de los mayores de 16 años y menores de 18

Los mayores de 16 años y menores de 18 tienen capacidad para contratar la prestación de sus trabajos con arreglo a los artículos 6 y 7 del Estatuto de los Trabajadores (siempre que vivan de forma independiente, con consentimiento de sus padres o tutores, o con autorización de la persona o institución que les tenga a su cargo) y, en esa medida, les es de aplicación idéntica responsabilidad que a las personas trabajadoras mayores de edad.

MENORES DE 14 AÑOS RESPONSABILIDAD CIVIL

Los menores de 14 años carecen de responsabilidad penal, pero no por ello dejan de responder de los daños y perjuicios materiales y morales causados por sus actos.

La responsabilidad civil por los daños y perjuicios causados por menores de 14 años es exigible a los padres o tutores que los tengan bajo su guarda (culpa “in vigilando”).

– Responsabilidad disciplinaria en el ámbito educativo

Los menores de 14 años tienen la misma responsabilidad disciplinaria que la que se recoge en el anterior tramo de edad.

COMPROMISO CON LA INNOVACIÓN, LA PROTECCIÓN DE DATOS Y LA ÉTICA

La privacidad ha de entenderse como un valor, no como una mercancía que puede ser objeto de monetización.

La responsabilidad digital está estrechamente vinculada con el respeto por los derechos humanos. Así, respetar la privacidad, la intimidad y la confidencialidad de los datos personales, pero también promover la toma de decisiones libre e informada y la equidad, la transparencia y la rendición de cuentas son condiciones necesarias para evitar las prácticas discriminatorias, los usos no deseados (y también encubiertos), así como posibles asimetrías y vulnerabilidades, y en especial la toma de decisiones desde la opacidad.

La convergencia de tecnologías como por ejemplo la IA, el Big Data, el Internet de las Cosas, la biometría, el blockchain, el 5G o el uso de datos genéticos debe aplicarse de forma responsable analizando de forma anticipada los riesgos y los eventuales impactos que puedan tener en las personas destinatarias (individuos, colectivos, sociedad en su conjunto).

Resulta, pues, necesaria la toma de decisiones ética anticipando escenarios que puedan generar riesgos para la privacidad, en especial el de reidentificación, y que aumentan a medida que las tecnologías emergentes convergen.

Para ello, se considera una práctica recomendable fomentar la formación en ética y privacidad de los distintos agentes implicados, en especial aquellos que programan algoritmos y que toman decisiones, así como la alfabetización digital con carácter transversal.En particular, los nuevos desarrollos tecnológicos deberán tener especialmente en cuenta los siguientes principios:

- Impulsar la mayor transparencia posible para que los usuarios y usuarias conozcan qué datos se están recabando, cuándo se registran y para qué se emplean. Para alcanzar un nivel significativo de transparencia, las personas deberán contar con acceso a sus datos personales de un modo sencillo y fácil de utilizar.
- Promover la igualdad de género, la protección de la infancia, de las víctimas y de las personas en situación de vulnerabilidad.
- Garantizar que las tecnologías eviten perpetuar los sesgos o aumentar las desigualdades existentes, evitando la discriminación algorítmica por razón de raza, procedencia, creencia, religión, sexo o cualquier otra razón.
- Realizar la mínima intrusión en la vida e intimidad de las personas, garantizando un tratamiento proporcional y necesario que preserve las libertades individuales.
- Implementar mecanismos de verificación, validación y acreditación que garanticen un tratamiento leal y la rendición de cuentas.

La ética de la IA persigue proteger valores como la dignidad, la libertad, la democracia, la igualdad, la autonomía del individuo y la justicia frente al gobierno de un razonamiento mecánico.

En especial, la perspectiva ética de la Inteligencia Artificial (IA), como una parte de la “ética digital”, es uno de los aspectos que más inquietud despierta. La ética de la IA persigue proteger valores como la dignidad, la libertad, la democracia, la igualdad, la autonomía individual y la justicia frente al gobierno de un razonamiento mecánico.

Una Inteligencia Artificial confiable y centrada en el ser humano ha de cumplir con siete requisitos clave: acción y supervisión humanas, solidez técnica y seguridad, gestión de la privacidad y los datos, transparencia, diversidad, no discriminación y equidad, bienestar social y ambiental y rendición de cuentas.

Estos requisitos deben ser evaluados a lo largo de todo el ciclo de vida de un sistema de IA de forma continua y considerarse el posible impacto colateral de dichos tratamientos en un entorno social, más allá de las limitaciones concebidas inicialmente de propósito, de duración en el tiempo y de extensión.

En particular, un aspecto crítico de los sistemas de IA es el de la posible existencia de sesgos y en aceptar, sin espíritu crítico, los resultados de una IA como ciertos e inamovibles, asumiendo un “principio de autoridad” derivado de las expectativas creadas por dichos sistemas. En definitiva, orientar la innovación y la toma de decisiones desde la perspectiva del respeto a la privacidad y bajo los principios de la ética y la responsabilidad digital, constituye un compromiso que debemos garantizar para las generaciones futuras.

03 DECÁLOGO DE BUENAS PRÁCTICAS

DECÁLOGO DE BUENAS PRÁCTICAS EN PRIVACIDAD PARA MEDIOS DE COMUNICACIÓN Y ORGANIZACIONES CON CANALES DE DIFUSIÓN PROPIOS

El artículo 17 del Convenio de Estambul recoge que los Estados animarán al sector privado, al sector de las tecnologías de la información y de la comunicación y a los medios de comunicación, respetando la libertad de expresión y su independencia, a participar en la elaboración y aplicación de políticas, así como a establecer líneas directrices y normas de autorregulación para prevenir la violencia contra la mujer y reforzar el respeto de su dignidad. Asimismo, especifica que se promoverán las capacidades de los menores y su entorno familiar y educativo para hacer frente a los contenidos degradantes de carácter sexual o violento.

Los principios de igualdad, dignidad, no discriminación y el derecho a la integridad física y moral son principios jurídicos universales, consagrados en la Constitución Española, que asigna a los poderes públicos la obligatoriedad de promover las condiciones necesarias para que la igualdad y no discriminación sean efectivas. En particular, en el ámbito específico de la no discriminación por razón de sexo, la Ley Orgánica 3/2007, de 22 de marzo, para la Igualdad Efectiva de Mujeres y Hombres, en su artículo 48, apartado 1, dispone a este respecto que "*Las empresas deberán promover condiciones de trabajo que eviten el acoso sexual y el acoso por razón de sexo y arbitrar procedimientos específicos para su prevención y para dar cauce a las denuncias o reclamaciones que puedan formular quienes hayan sido objeto del mismo.*"

Las nuevas tecnologías y los servicios que estas ofrecen proporcionan innumerables ventajas. No obstante, en ocasiones se utilizan como vía para extender y amplificar la violencia que tiene lugar en el mundo offline, tratando de fomentar la humillación pública de las víctimas y dañando de forma grave su privacidad. En este contexto tienen lugar diferentes formas de ciberviolencia o violencia digital, dirigidas en su mayor parte contra las mujeres, los menores de edad, las personas discriminadas por su orientación sexual o raza, las personas con discapacidad o enfermedad grave o en riesgo de exclusión social. Así, es cada vez más frecuente que se publiquen en Internet o se difundan a través de las redes sociales contenidos sexuales o violentos que tienen como víctimas estos colectivos.

Este decálogo forma parte de la "Carta de Adhesión: Por un Pacto Digital para la protección de las personas", elaborada por la Agencia Española de Protección de Datos. Mediante esta Carta de Adhesión, la Agencia quiere intensificar las relaciones tanto con los medios de comunicación como con todas aquellas organizaciones que disponen de canales de difusión propios para informar sobre temas de interés para sus públicos. El objetivo final es fomentar la privacidad de las víctimas y concienciar de manera global sobre la existencia del Canal prioritario para solicitar la retirada de contenidos -textos, audios, fotografías o vídeos- sexuales o violentos difundidos sin el consentimiento de las personas que aparecen en ellos.

01. Los firmantes de la Carta se abstendrán de identificar de forma alguna a las víctimas de agresiones, hechos violentos o de contenido sexual en sus informaciones o de publicar información de la que, con carácter general, pueda inferirse su identidad cuando se trate de personas sin relevancia pública.

Todo ello sin perjuicio de que las personas no públicas puedan verse involucradas en hechos noticiables, en cuyo caso la cobertura informativa será la necesaria para dar adecuado cumplimiento al derecho a la información, atendiendo a las peculiaridades de cada caso.

02. Las informaciones difundidas por los medios no incluirán imágenes innecesarias desde el punto de vista puramente informativo, ya sea de forma cualitativa o cuantitativa, evitándose por tanto la repetición sistemática de las imágenes.

03. La Agencia Española de Protección de Datos tiene deber de confidencialidad y no facilitará información alguna sobre las víctimas o las personas que, sin serlo, han puesto en conocimiento de la Agencia la difusión de esos contenidos sensibles a través del Canal prioritario. Tampoco se pondrá en contacto con las víctimas o con aquellos que han denunciado los hechos para comunicarles un posible interés de los medios de comunicación en entrevistarlos.

04. La AEPD respetará la protección de datos de los denunciados si fueran personas físicas, salvo que ellos mismos lo hubieran hecho público. Una vez finalizado el procedimiento, las informaciones publicadas destacarán la sanción impuesta a quien grabó o difundió las imágenes, como herramienta pedagógica.

05. Cuando los firmantes de la Carta de Adhesión ofrezcan información sobre difusión digital de contenidos violentos, tratarán de advertir, en la medida de las posibilidades de cada medio, sobre la responsabilidad disciplinaria, civil, penal y administrativa que podrían acarrear este tipo de conductas.

06. Los firmantes no disculparán o justificarán de forma alguna al agresor que ha difundido contenidos sensibles de terceros sin consentimiento. El desconocimiento de la ley no es un atenuante. La grabación voluntaria de imágenes de contenido sexual no ampara la difusión posterior de las mismas si esta se realiza sin consentimiento de todos los intervinientes en dichas imágenes.

07. En las informaciones que aborden la difusión de contenido sexual o violento de víctimas de ciberviolencia o violencia digital a través de internet se incorporará de forma sistemática una referencia al Canal Prioritario de la Agencia Española de Protección de Datos en la medida de las posibilidades de cada medio.

08. En los contenidos publicados en internet que traten de violencia digital también se destacará que todas las personas afectadas por la difusión de dichos contenidos pueden efectuar la denuncia correspondiente a través del Canal Prioritario para solicitar la retirada de los contenidos, aunque no sean los denunciantes los que aparezcan en las imágenes, audios o textos.

09. En el caso de que un medio de comunicación llegase a conocer la identidad de una posible víctima de violencia digital se abstendrán de publicar o difundir imágenes o contenidos que haya obtenido directamente de las redes sociales de las que sea usuaria la víctima, así como de realizar valoraciones a partir de esas imágenes. Las imágenes provenientes de dichas redes sociales que hayan sido previamente difundidas a través de cualesquiera medios serán utilizadas respetando las reglas y principios anteriormente establecidos.

10. Las medidas mencionadas en el punto anterior serán aplicables aunque los perfiles de las redes sociales de la víctima se encontrasen en abierto.

Tú también
#PuedesPararlo
con el
#CanalPrioritario

Canal Prioritario **FAQ's**

04 ANEXO

RELACIÓN DE HERRAMIENTAS, GUÍAS, MATERIALES Y RECURSOS DE LA AEPD PARA CIUDADANOS Y RESPONSABLES

CIUDADANOS

- Sección Preguntas Frecuentes (FAQs)
- Guía para el ciudadano
- Conoce tus derechos y cómo ejercerlos
- Información sobre el derecho a la supresión de datos personales (derecho “al olvido”)
- ¿Qué derechos tengo para proteger mis datos personales? (infografía)
- ¿Cómo elimino fotos y vídeos de internet?
- Guía de privacidad y seguridad en internet (contenidos divisibles)
- Guía de protección de datos y prevención de delitos
- Fichas de protección de datos y prevención de delitos
- Protección de datos en vacaciones (infografía)
- Site videovigilancia. Guía, fichas y consejos
- Novedades para los ciudadanos sobre la nueva LOPDGDD
- Novedades de la Ley Orgánica 3/2018, para los ciudadanos (Vídeo)
- Privacidad, datos personales y aplicaciones para encontrar pareja (Blog)
- Fotos y vídeos no tan privados (Blog)
- Videos “Protege tus datos en internet”
- Cuatro pasos para deshacerte de tu móvil de forma segura (Blog)
- Seguridad en tus contraseñas (Blog)

EDUCACIÓN Y MENORES

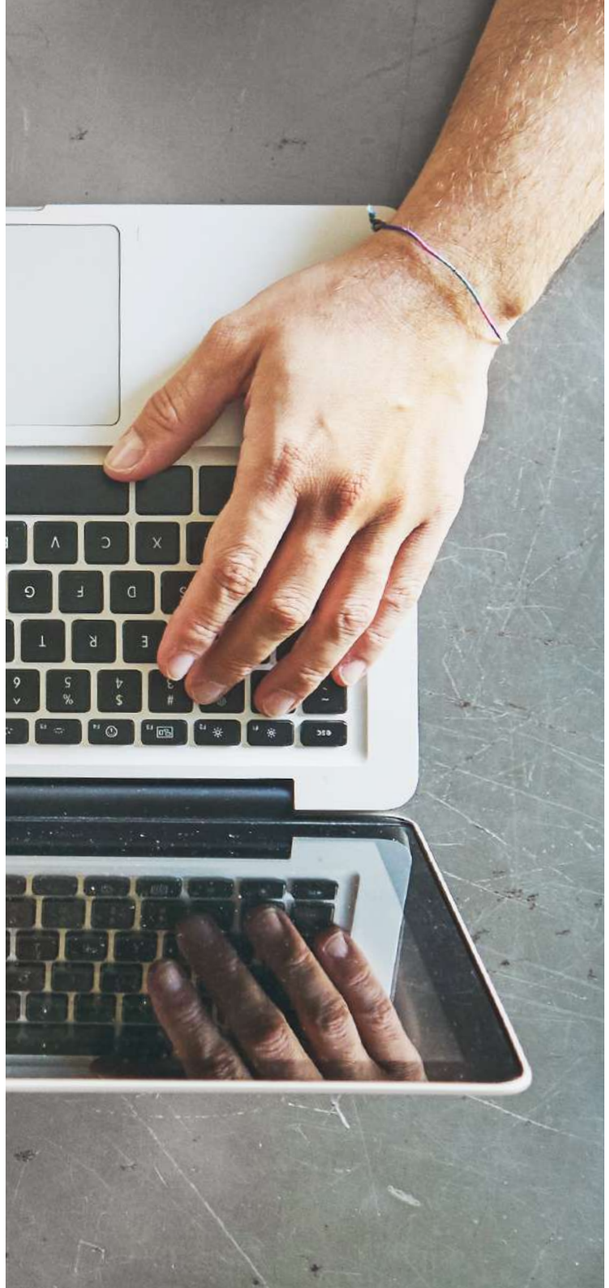
- Espacio de educación y menores
- Tú decides en Internet (cómic)
- Videos “Tú controlas en internet”
- Videos “Historias para concienciar a los menores”
- Videos “Talleres para familias sobre menores y su cibermundo”
- Guía “Sé legal en internet”
- Guía “Enséñales a ser legales en Internet”
- “No te enredes en Internet”
- “Guíales en internet”
- ¿Sabes qué es?
- Conocimiento y habilidades en el ámbito de las TIC
- Infografía “Protege sus datos en la vuelta a clase”
- Guía de protección de datos para centros educativos
- Blog: ¿Puedo publicar en redes sociales el vídeo de la salida escolar de mis hijos/as?
- Decálogo seguridad en las Redes Sociales (Fuente: CCN)
- Protección del menor en Internet. Recomendaciones para padres y tutores (infografía)
- Inspección sectorial sobre servicio de cloud en el sector educativo
- Informe sobre la utilización por profesores y alumnos de sistema ajenos a las plataformas educativas
- **AseguraTIC** (web del Instituto Nacional de Tecnologías Educativas y Enseñanza del Profesorado -INTEF-, que integra los recursos, en instituciones públicas y entidades privadas) dirigidos a la comunidad educativa en materia de educación digital
- **NOOC “Menores y seguridad en la red”**, en colaboración con el INTEF y el Instituto Nacional de Ciberseguridad (INCIBE) del que están previstas nuevas ediciones (https://intef.es/). Los trabajos seleccionados están accesibles a través de estos 2 enlaces:
  - #MenorSeguroEnRed
  - Menores y seguridad en la red trabajos destacados

VIOLENCIA DE GÉNERO. RECURSOS PARA AYUDAR A COMBATIR LA VIOLENCIA DIGITAL

- Canal prioritario para comunicar la difusión de contenido violento o sexual en internet y solicitar su retirada
- ¿Cómo puedo comunicar la difusión de imágenes sensibles? (infografía)
- Consultas frecuentes sobre este canal
- ¿Sabías que difundir vídeos de contenido sexual o violento puede tener consecuencias administrativas, civiles y penales?
- Espacio web de ayuda a la protección de la privacidad de las víctimas de violencia de género
- Recomendaciones para la protección de datos en las políticas de prevención del acoso digital
- Marco de actuación de la AEPD en materia de igualdad de género
- Protocolo de actuación frente al acoso sexual y por razón de sexo en la AEPD
- Protocolo de actuación frente al acoso laboral en la AEPD

CONSUMO, COMERCIO ONLINE Y PUBLICIDAD

- Guía y Fichas sobre Compra segura en internet
- Infografía sobre compra segura en internet
- Vídeo – Recomendaciones para la compra segura en internet
- Infografía sobre Juguetes conectados
- La época de 'regalos inteligentes (BLOG)
- Decálogo para la adaptación al RGPD de las políticas de privacidad en internet
- Cómo evitar la publicidad no deseada
- Cómo evitar la publicidad no deseada (infografía)
- Cómo evitar la publicidad no deseada (vídeo)



CONTRATACIÓN DE SERVICIOS PÚBLICOS Y MOROSIDAD

- Preguntas frecuentes (FAQs) sobre contratación irregular y morosidad
- Guía para la presentación de quejas y reclamaciones en el ámbito de las telecomunicaciones

SALUD

- Decálogo de protección de datos para el personal sanitario y administrativo
- Guía para pacientes y usuarios de la sanidad

ÁMBITO LABORAL

- Sección Preguntas Frecuentes
- Comunicado sobre la información acerca de tener anticuerpos de la COVID-19 para la oferta y búsqueda de empleo
- Valoración del programa de teletrabajo 2019

PROTECCIÓN DE DATOS Y COVID-19

INFORMES Y COMUNICADOS

- Informe sobre tratamientos de datos en relación con el COVID-19
- Preguntas frecuentes dirigidas tanto a ciudadanos como a empresas y otros sujetos obligados al cumplimiento de la normativa de protección de datos
- Comunicado de la AEPD en relación con webs y apps que ofrecen autoevaluaciones y consejos sobre el coronavirus.
- Comunicado de la AEPD sobre apps y webs de autoevaluación del COVID-19
- Recomendaciones para proteger los datos personales en situaciones de movilidad y teletrabajo
- Comunicado AEPD en relación con la toma de temperatura por parte de comercios, centros de trabajo y otros establecimientos
- El uso de las tecnologías en la lucha contra el COVID-19
- Informe sobre el uso del reconocimiento facial para exámenes
- Monitorización remota de datos fuente en ensayos clínicos
- Comunicado de la AEPD sobre la información acerca de tener anticuerpos de la COVID-19 para la oferta y búsqueda de empleo

BLOG DE LA AEPD

- Tratamientos de datos personales en situaciones de emergencia
- Brechas de seguridad: El Top 5 de las medidas técnicas que debes tener en cuenta
- Notificación de brechas de seguridad de los datos personales durante el estado de alarma
- Campañas de phishing sobre el COVID-19

DOCUMENTOS COMITÉ EUROPEO DE PROTECCIÓN DE DATOS

- Directrices 04/2020 sobre el uso de datos de localización y herramientas de rastreo de contactos en el contexto de la pandemia de COVID 19
- Directrices 03/2020 sobre el tratamiento de datos relativos a la salud con fines de científica en el contexto del brote de COVID 19

RESPONSABLES Y ENCARGADOS DEL TRATAMIENTO

- Decálogo de recursos de ayuda de la AEPD
- Guía para el responsable de tratamiento de datos personales
- Guía para el cumplimiento del deber de informar
- Directrices para la elaboración de contratos entre responsables y encargados del tratamiento
- Guía práctica de análisis de riesgos para el tratamiento de datos personales
- **FACILITA RGPD.** Herramienta de ayuda para empresas que realicen tratamientos de datos personales de escaso riesgo para el cumplimiento del RGPD
- **FACILITA_EMPRENDE.** Herramienta de análisis de riesgos para emprendedores
- **GESTIONA EIPD.** Herramienta de análisis de riesgos y evaluaciones de impacto
- Guía práctica para las evaluaciones de impacto en la protección de datos personales
- Modelo de informe de Evaluación de Impacto en la Protección de Datos para AAPP
- Listas de tipos de tratamientos de datos que requieren EIPD (art 35.4)
- Lista orientativa de tipos de tratamientos de datos que no requieren una evaluación de impacto relativa a la protección de datos (art 35.5)
- Guía de Privacidad desde el Diseño
- Guía para la gestión y notificación de brechas de seguridad
- Cómo gestionar una fuga de información en un despacho de abogados
- Guía para clientes que contraten servicios de Cloud Computing
- Orientaciones para prestadores de servicios de Cloud Computing
- Código de buenas prácticas en proyectos de big data
- La K-anonimidad como medida de la privacidad
- Orientaciones y garantías en los procedimientos de anonimización de datos personales
- Guía de drones y protección de datos
- Orientaciones para la aplicación provisional de la disposición adicional séptima de la LOPDGDD
- Guía sobre el uso de las cookies

aepd agencia española protección datos

www.aepd.es

@aepd_es