Norma para el Cumplimiento de los Requisitos del Reglamento General de Protección de Datos del Grupo FCC

January 2026

Historial de Versiones				
Versión	**Fecha**	**Autor**	**Detalle**	**Aprobador**
1.0	Febrero 2018	IS	Creación del Documento	Chief Information Security Officer (CISO)
	Octubre 2019	IS	Revisión del Documento	Chief Information Security Officer (CISO)
1.1	Mayo 2024	IS	Revisión del Documento Unificación del formato con el resto de la Normativa	Chief Information Security Officer (CISO)
1.2	Julio 2025	IS	Revisión del documento y adaptación a normativa ISO27001:2022 y ENS	Chief Information Security Officer (CISO)
1.3	Enero 2026	IS	Revisión del documento	Chief Information Security Officer (CISO)

INDEX

1. Introducción

El presente documento forma parte del Marco Normativo de Seguridad de la Información del Grupo FCC, que desarrolla los preceptos de obligado cumplimiento en el Grupo en materia de Seguridad de la Información.

El Marco Normativo de Seguridad es revisado y actualizado periódicamente por el departamento de Seguridad de la Información (en adelante departamento de SI), de acuerdo con lo establecido en el Documento de Gestión y Mantenimiento del Marco Normativo. Este documento contiene información sobre el historial de versiones, revisiones y aprobaciones de la presente Norma, así como su relación y dependencia con el resto de los documentos normativos. Esta norma será revisada, por lo menos, anualmente, salvo que existan circunstancias que recomienden o exijan una revisión antes de dicha fecha.

El 25 de mayo de 2016 entró en vigor el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (en adelante Reglamento General de Protección de Datos, el Reglamento o RGPD).

Desde el Dpto. Seguridad de la Información de FCC – departamento de SI (Dpto. encargado de establecer las directrices mínimas en materia de Privacidad), y para dar cumplimiento a la normativa europea en protección de datos derivada del RGPD se desarrolla la presente "**Norma**", que deberá aplicarse en cada una de las Entidades del Grupo FCC para adecuarlas a dicha normativa con la colaboración de la matriz FCC, de los Coordinadores de Protección de Datos y de toda la estructura creada al efecto.

1.1 Objeto

El objetivo de la presente Norma es trasladar a las Entidades FCC (que entren dentro del objeto de aplicación del Reglamento) las principales novedades que introduce el Reglamento, así como las acciones y los requisitos mínimos que deben ser cumplidos por cada Entidad FCC.

No obstante, el Grupo FCC podrá elaborar procedimientos que desarrollen y detallen determinados puntos de la presente Norma.

1.2 Ámbito De Aplicación

1.2.1 Geográfico

Esta Norma es de aplicación y de obligado cumplimiento por las Entidades que pertenecen al Grupo FCC ubicadas en cualquier Estado/País/Región de la Unión Europea, más concretamente:

- Aquellas Entidades en las que FCC posea la mayoría de participación (más 50%).
- Aquellas Entidades que a pesar de no poseer FCC la mayoría de participación, si ostenta la gestión o administración de esta.

1.2.2 Material

Esta Norma se aplicará a toda la información que contenga Datos Personales (en soporte papel y/o en soporte informático) responsabilidad de cada una de las Entidades FCC que se recabe, acceda, gestione, transfiera o de cualquier otra forma se trate por el personal de las Entidades FCC o sus Partners y/o Proveedores.

2. Desarrollo

2.1 Definiciones

- **«Datos personales»:** toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona.
- **«Tratamiento»:** cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción.
- **«Seudonimización»:** el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable.
- **«Fichero»:** todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica.
- **«Responsable del Tratamiento»** o **«Responsable»:** la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros. En este sentido, cada Entidad FCC será Responsable en relación con los datos personales que gestione (p.ej. de Personas trabajadoras, Clientes y Proveedores).
- **«Encargado del Tratamiento»** o **«Encargado»:** la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento.
- **«Consentimiento del interesado»:** toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen.
- **«Violación de la seguridad de los datos personales»:** toda violación de la seguridad que ocasione 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.
- **«Datos relativos a la salud»:** datos personales relativos a la salud física o mental de una persona física, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud.

- **«Coordinador en materia de protección de datos»:** Es la persona perteneciente a una Entidad del Grupo FCC, nombrada para coordinar las acciones en materia de protección de datos de un área del Grupo FCC.
- **«Responsable de seguridad de la Entidad o Entidades en materia de Protección de Datos»:** Es la persona perteneciente a una Entidad del Grupo FCC, nombrada para gestionar las acciones en materia de protección de datos de una o varias Entidades del Grupo FCC.

2.2 Novedades Relevantes Introducidas Por El Reglamento

El Reglamento establece una serie de novedades que deberán implementarse en las Entidades FCC que entren dentro del ámbito de aplicación del RGPD.

Con carácter informativo, y sin perjuicio de las efectivas medidas a implantar que se establecen en el punto 6 de la presente Norma ("Directrices mínimas en materia de Privacidad"), se exponen a continuación algunas de las novedades del RGPD:

- Se establece el principio de **"Responsabilidad Proactiva"** por el que cada Entidad FCC será responsable del correcto cumplimiento en plazo de la normativa, debiendo tener capacidad de demostrarlo en cualquier momento a través de la implantación de un sistema sólido de evidencias.
- Se fortalecen los principios aplicables al tratamiento de datos personales: licitud, lealtad y transparencia; recogidos con fines determinados, explícitos y legítimos (**«limitación de la finalidad»**); limitados a lo necesario en relación con los fines para los que son tratados (**«minimización de datos»**); exactos y actualizados («exactitud»); mantenidos de forma que se permita la identificación de los titulares de los datos durante no más tiempo del necesario para los fines del tratamiento de los datos personales (**«limitación del plazo de conservación»**); tratados de tal manera que se garantice una seguridad adecuada de los datos personales (**«integridad y confidencialidad»**).
- Se refuerza la exigencia de consentimiento. Una de las bases fundamentales para tratar datos personales es el consentimiento. El Reglamento exige que el consentimiento, con carácter general, sea libre, informado, específico e inequívoco. Para poder considerar que el consentimiento es "inequívoco", el Reglamento requiere que haya una declaración de los interesados o una acción positiva que indique el acuerdo del interesado. El consentimiento no puede deducirse del silencio o de la inacción de los ciudadanos, sino que debe existir evidencia probatoria del mismo.
- Se endurece el derecho de información obligando a la Entidad a suministrar más información con carácter previo a la recogida o registro de los datos personales de personas trabajadoras, clientes y proveedores por cualquier medio.
- Se introducen nuevos derechos a favor del titular de los datos, entre los que cabe destacar el derecho a la portabilidad de los datos que permite a los titulares solicitar a la Entidad la entrega o recuperación de esos datos en un formato que permita su traslado a otro responsable.
- Se establece la necesidad de cumplir con la protección de datos desde el diseño, que exige el cumplimiento de la protección de datos desde el inicio del servicio o desde la compra del sistema. Se promoverán las técnicas como la seudonimización (entendido como el tratamiento de datos personales de manera tal que ya no puedan atribuirse al titular del dato sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas

destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable).

- Se introduce la obligación de notificación a la Autoridad de Protección de Datos en un plazo mínimo y al titular del dato (en determinados supuestos) sobre aquellas violaciones de seguridad sobre los datos que se produzcan y que supongan riesgo de daños y perjuicios para las personas físicas. Deberán documentarse todas las violaciones de seguridad.
- Se impone la necesidad de establecer las medidas técnicas de seguridad en base a riesgos que permitan garantizar un nivel de seguridad adecuado, así como la obligación de realizar evaluaciones de impacto en protección de datos (en adelante, PIAs), siempre que sea probable que las operaciones de tratamiento, especialmente cuando se utilicen nuevas tecnologías, entrañen un alto riesgo para los derechos y libertades de las personas físicas o en los tipos de tratamientos que indique la Autoridad de Control.
- Se introduce el concepto de “derecho al olvido” para solicitar que los datos personales sean suprimidos en determinadas circunstancias.

2.3 Directrices En Materia De Protección De Datos

A continuación, se detallan las directrices mínimas que deberán ser observadas y cumplidas por cada Entidad FCC, ello sin perjuicio del cumplimiento de los requisitos exigidos por cualquier otra normativa en materia de Protección de Datos que resulte de aplicación (por derecho imperativo en el país en que esté domiciliada o ubicada la Entidad FCC).

2.3.1 Estructura de la Privacidad en FCC

Para dar cumplimiento a toda la normativa derivada del Reglamento, desde el Grupo FCC se ha creado una estructura organizativa que decida, coordine, implante y supervise en materia de protección de datos en todo el Grupo.

Dicha estructura debe estar formada, como mínimo, por:

- **Privacy Board:** Órgano multidisciplinar de máximo nivel en el Grupo FCC en materia de Privacidad. Está formado por: director Asesoría Jurídica, Directora Recursos Humanos, Director Dpto. de Auditoría Interna, Gestión de Riesgos y Cumplimiento de FCC, Director de la División de Sistemas y Tecnologías de la Información y el Coordinador Protección de Datos del Grupo FCC.
- **Coordinador de Protección de Datos del área:** Persona perteneciente a un área del Grupo FCC y designada por dicha área para impulsar, implantar, coordinar y gestionar dentro de las Entidades FCC que pertenecen a la misma, las acciones necesarias para el cumplimiento de las obligaciones en materia de Privacidad. Será a nivel nacional y / o internacional. Igualmente, podrá nombrarse un Coordinador de Protección de Datos del área para cierto/s país/es en concreto, dependiente en todo caso del Coordinador de Protección de Datos del área. A los efectos de este documento, se consideran Áreas las siguientes: FCC Corporación, FCC Construcción, FCC Servicios Medioambientales, FCC Servicios Aguas y Grupo Cementos Portland Valderrivas.
- **Coordinador de Protección de Datos adjunto:** Para la asistencia del Coordinador de Protección de Datos del área, podrán nombrarse formalmente los Coordinadores adjuntos que se estimen necesarios dentro de cada área de actividad.

- **Grupo de Trabajo:** Salvo excepción debidamente justificada al Privacy Board, dentro de cada área deberá además crearse un Grupo de Trabajo formado por responsables de los Departamentos del Grupo (responsables locales de cada Entidad, Delegación o zona) que más repercusión tienen en materia de Privacidad, por el Coordinador de Protección de Datos del área (y el/los Coordinadores adjuntos y / o del país que se hayan nombrado) y constituido con la finalidad de impulsar, coordinar, implantar, gestionar, debatir las problemáticas relativas a la protección de datos que tengan lugar dentro del área de actividad y verificar la correcta adecuación al Reglamento y a la normativa local de Protección de Datos que resulte de aplicación en las Entidades FCC que se encuentran dentro de su área de actuación.

La estructura organizativa de la Privacidad para cada una de las áreas será, en su caso, ésta:

Para conocer las funciones y responsabilidades de cada figura, véase documento “Modelo de Gobierno en materia de Privacidad”.

2.3.2 Principios Generales de Actuación

A continuación, se detallan los principios generales en materia de Privacidad que deberán observarse y cumplirse para el tratamiento de datos personales:

- Tratados de manera lícita, leal y transparente en relación con el titular de los datos (**«licitud, lealtad y transparencia»**).
- Recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines; el tratamiento ulterior de los datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos no se considerará incompatible con los fines iniciales (**«limitación de la finalidad»**).
- Adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados (**«minimización de datos»**).
- Exactos y, si fuera necesario, actualizados; se adoptarán todas las medidas razonables para que se supriman o rectifiquen, sin dilación, los datos personales que sean inexactos con respecto a los fines para los que se tratan (**«exactitud»**).
- Mantenidos de forma que se permita la identificación de los titulares durante no más tiempo del necesario para los fines del tratamiento de los datos personales; los datos personales podrán conservarse durante períodos más largos siempre que se traten exclusivamente con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, sin perjuicio de la aplicación de las medidas técnicas y organizativas apropiadas que impone el presente Reglamento a fin de proteger los derechos y libertades del interesado (**«limitación del plazo de conservación»**).
- Tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas (**«integridad y confidencialidad»**).
- Cuando el tratamiento se base en el consentimiento del titular de los datos, la Entidad FCC deberá ser capaz de demostrar que aquel consintió el tratamiento de sus datos personales. Si el consentimiento del titular se da en el contexto de una declaración escrita que también se refiera a otros asuntos, la solicitud de consentimiento se presentará de tal forma que se distinga claramente de los demás asuntos, de forma inteligible y de fácil acceso y utilizando un lenguaje claro y sencillo.

2.3.3 Aspectos Organizativos

A nivel organizativo, habrá que realizar, como mínimo, las siguientes acciones:

2.3.3.1 Establecimiento y Nombramiento del Modelo de Gobierno en Materia de Privacidad en cada área

Dentro de cada una de las áreas de actividad habrá que diseñar y nombrar formalmente un Modelo de Gobierno en materia de Privacidad, que deberá contar al menos con un Coordinador de Protección de Datos del área de actividad (nacional y/o internacional). De forma complementaria, dentro de cada área podrán nombrarse los Coordinadores Adjuntos y /o de país que se estimen necesarios.

En todos los casos deberá existir un nombramiento formal y quedar bien definidas las funciones y responsabilidades asumidas por cada uno de los cargos nombrados.

Deberá informarse de los nombramientos hechos, así como cualquier cambio que se haga en el Modelo de Gobierno (bien sea cambios en responsabilidades, nombramientos, etc.) al Coordinador de Protección de Datos del área y al departamento de SI.

2.3.3.2 Control e Inventario actualizado de Entidades FCC de cada área

Cada Coordinador de Protección de Datos de área deberá llevar el control de las Entidades FCC que haya en su área en cada momento (y a las que aplique la presente Norma), para que las directrices de protección de datos se apliquen sobre las mismas, y de cara a eventuales inspecciones o auditorías.

Para ello, deberá mantenerse actualizada la herramienta de gestión de protección de datos de cada área, incorporando las nuevas Entidades FCC que se creen o adquieran y dando de baja aquellas entidades que han desaparecido o están fuera del control de FCC.

2.3.3.3 Obligación de Evidenciar el Correcto Cumplimiento del Reglamento

Con base en los principios de Responsabilidad Proactiva y de cara a posibles inspecciones o auditorías, deben quedar evidenciados todos los aspectos que conciernen a tratamientos de datos de carácter personal, al correcto cumplimiento de la normativa, así como las medidas correctoras que se apliquen.

Es decir, deben quedar evidenciadas y custodiadas por cada una de las Entidades FCC todas las actuaciones, políticas, medidas e incluso las reuniones mantenidas (mediante acta) para la llevanza y aplicación de esta Norma y demás acciones concernientes a protección de datos a las que el Grupo FCC quede obligado por la normativa vigente.

2.3.4 Aspectos Legales

En lo que respecta a los aspectos legales, habrá que realizar, como mínimo, las siguientes acciones:

2.3.4.1 Registros de actividades de tratamiento

En cada Entidad FCC habrá que identificar e inventariar todos los puntos en que se realicen tratamientos de datos de carácter personal de cara a la adecuación de los mismos al RGPD.

Dicho inventario de tratamientos será además la base sobre la que crear el Registro de las Actividades de Tratamientos que se exige el Reglamento en su artículo 30.

Dicho Registro deberá contener, como mínimo, la información recogida en el art. 30 RGPD.

Será responsabilidad de cada Coordinador de Protección de Datos de área la buena llevanza y mantenimiento actualizado, de una manera diligente, de los Registros de Actividades de Tratamiento de datos personales.

2.3.4.2 Clausulado

Habrá que revisar y actualizar conforme a los requisitos que exige el RGPD las cláusulas y/o contratos en materia de Protección de Datos que se utilicen en cada Entidad FCC (cláusulas/contratos de Personas trabajadoras, de Clientes y de Proveedores).

Para ello, siempre se tomarán como base aquellos modelos de cláusulas/contratos proporcionados por la departamento de SI. Dichos modelos deberán ser revisados conforme a los requisitos exigidos por la normativa de Protección de Datos que resulte de aplicación.

En concreto:

PERSONAS TRABAJADORAS

Todas las Entidades FCC deberán regularizar conforme al RGPD (y los requisitos que puedan ser establecidos por la normativa de Protección de Datos que resulte de aplicación) las cláusulas de información y consentimiento en materia de Protección de Datos de todas las personas trabajadoras actuales.

Asimismo, respecto a las futuras personas trabajadoras, las Entidades FCC deberán hacer firmar una cláusula de información y consentimiento conforme a los requisitos del RGPD (y los requisitos que puedan ser establecidos por la normativa de Protección de Datos que resulte de aplicación).

CLIENTES

Todas las Entidades FCC deberán regularizar conforme al RGPD (y los requisitos que puedan ser establecidos por la normativa de Protección de Datos que resulte de aplicación) las cláusulas de información y consentimiento en materia de Protección de Datos de todos los clientes actuales.

Asimismo, respecto a los futuros clientes, las Entidades FCC deberán hacer firmar una cláusula de información y consentimiento conforme a los requisitos del RGPD (y los requisitos que puedan ser establecidos por la normativa de Protección de Datos que resulte de aplicación).

PROVEEDORES

En el caso de que fuera necesaria la contratación de una aplicación y/o Servicios a una Entidad externa o a cualquier otra Entidad del Grupo FCC (en adelante, Proveedor) en virtud de la cual, éste pueda/deba acceder/tratar Datos Personales, la Entidad FCC deberá elegir a un Proveedor que ofrezca garantías suficientes para aplicar medidas técnicas y organizativas apropiados, de manera que el tratamiento sea conforme con los requisitos del Reglamento y se firme de manera previa al acceso/gestión de cualquier dato un Contrato de Prestación de Servicios en el que se establezca expresamente el contenido mínimo que marca el art. 28 RGPD (y los requisitos que puedan ser establecidos por la normativa de Protección de Datos que resulte de aplicación). Para la elaboración del Contrato de Prestación de Servicios, cada Entidad FCC deberá tomar como base el modelo de Contrato de Prestación de Servicios que le proporcione el Coordinador de Protección de Datos del área al que pertenezca la Entidad FCC.

Todo Contrato de Prestación de Servicios que se firme con un Encargado del Tratamiento deberá ser comunicado inmediatamente al Coordinador de Protección de Datos del área al que pertenezca la Entidad FCC y almacenado correctamente por el área.

Asimismo, en todas las “Request For Proposal” (RFP) y/o solicitudes de oferta que se elaboren, se deberá incluir una cláusula de Protección de Datos conforme a los requisitos del RGPD. El modelo de esta será proporcionado por el Coordinador de Protección de Datos del área.

Con relación a los contratos vigentes con Proveedores cuya fecha de finalización sea anterior a mayo de 2018 se establece lo siguiente: En principio, no se existe ninguna obligación en base al Reglamento, porque dichos contratos ya deberían tener la cláusula de Protección de Datos que cumpla con la normativa vigente. No obstante, lo anterior, aquellos contratos que estén en esta situación, pero se prevea realizar una prórroga de su vigencia, SÍ deberán ser regularizados conforme al Reglamento.

Respecto a los contratos vigentes con Proveedores cuya fecha de finalización sea posterior a mayo de 2018: Se deberá gestionar la firma de la cláusula de Protección de Datos que, como mínimo, cumplirá con los requisitos recogidos en el art. 28 RGPD (y los requisitos que puedan ser establecidos por la normativa de Protección de Datos que resulte de aplicación). Se deberá tomar como base el modelo Cláusula de Protección de Datos que le proporcione el Coordinador de Protección de Datos del área al que pertenezca la Entidad FCC.

2.3.4.3 Cumplimiento con la normativa en materia de protección de datos vigente en el país en que se encuentre domiciliada/ubicada la entidad FCC

Asimismo, cada Entidad FCC deberá cumplir, además de lo exigido por el RGPD, aquellas otras disposiciones de cualquier otra normativa en materia de Protección de Datos que resulte de aplicación por derecho imperativo en el país en que se encuentre domiciliada/ubicada dicha Entidad.

2.3.5 Aspectos Técnicos

2.3.5.1 Inventario de Sistemas de Información

En cada entidad FCC habrá que identificar e inventariar todos los sistemas de información (internos y externos) a través de los cuales se traten/gestionen datos de carácter personal de cara a la adecuación de estos y de sus medidas de seguridad conforme al Reglamento.

2.3.5.2 Análisis de Riesgos y Evaluación de impacto sobre la Privacidad

Teniendo en cuenta el estado de la técnica, los costes de aplicación, 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, la Entidad FCC aplicará las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros:

- La seudonimización y el cifrado de datos personales (en algunos casos);
- La capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento. También el sistema de información deberá garantizar la portabilidad de datos, esto es, cumplir con las medidas técnicas que permitan dar respuesta a un ejercicio de un derecho de portabilidad de datos mediante el cual el interesado tendrá derecho a recibir los datos personales que le incumban, facilitados a FCC en un formato estructurado, de uso común y lectura mecánica y a transmitirlos a otro responsable del tratamiento.
- La capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico;
- Un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

Este sentido, todos los sistemas de información utilizados en el Grupo FCC deberán ser objeto de un análisis de riesgos que permita identificar las medidas de seguridad que sean necesarias conforme a lo anteriormente detallado.

Asimismo, conforme a lo establecido en el art.35 del Reglamento, siempre que desde alguna Entidad FCC vaya a realizarse un tratamiento de datos de carácter personal que, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas, se realizará, antes del tratamiento, una Evaluación del Impacto (PIA) en materia de Privacidad de dicho tratamiento en la protección de datos personales.

En todo caso, un PIA deberá realizarse siempre que el tratamiento de datos personales consista en: una evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado, como la elaboración de perfiles; un tratamiento a gran escala de las categorías especiales de datos a que se refiere el artículo 9 del RGPD; o una observación sistemática a gran escala de una zona de acceso público.

Tanto los análisis de riesgos como las Evaluaciones de Impacto sobre la Privacidad (PIAs) que se realicen el Grupo FCC se harán conforme a la Metodología de evaluación de riesgos que será aprobada por el Privacy Board.

2.3.5.3 Auditorías para verificar el Cumplimiento

Las Entidades FCC deberán realizar auditorías periódicas (internas o externas) a fin de verificar el correcto cumplimiento de la presente Norma, de las directrices establecidas y de las medidas de seguridad implantadas.

De forma previa a su realización, el departamento de SI aportará las instrucciones correspondientes a su realización a la Entidad FCC y ésta deberá reportar al departamento de SI los resultados de esta.

2.3.5.4 Notificar violaciones de Seguridad relacionadas con Datos Personsales

La Entidad FCC notificará de forma inmediata, por escrito y sin perjuicio de aquellas notificaciones que fueran necesarias a la correspondiente Autoridad de Control, al Director de Seguridad de la Información de FCC (sdseguridad@fcc.es), la existencia de cualquier “Violación de Seguridad” en el sentido de toda violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita, la pérdida y la alteración, la revelación o el acceso no autorizados, de datos personales transmitidos, conservados o tratados de otra forma o la comunicación o acceso no autorizados a dichos datos, incluyendo la información exigida en el RGPD y demás normativa que resulte de aplicación.

2.3.5.5 Consulta previa a Coordinadores de Protección de Datos del Área

Siempre que desde alguna Entidad FCC vaya a iniciarse un nuevo proyecto, contratarse una nueva aplicación o realizarse alguna actividad (ya sea comercial, de marketing, publicitaria, o de cualquier tipo) que pueda entrañar tratamiento de datos de carácter personal habrá que consultar previamente a los Coordinadores de Protección de datos del área correspondiente, el impacto de dicha actividad o proyecto en la protección de datos.

2.4 Implantación

Esta Norma deberá cumplirse en su totalidad a partir del 25 de mayo de 2018, fecha en que es de aplicación el contenido del Reglamento General de Protección de Datos. No obstante, la implantación de medidas deberá comenzar con antelación suficiente como para poder cumplir todas las disposiciones del RGPD cuando sea de aplicación.

3. Responsabilidades

Tal y como establece el Código Ético de FCC, todas las personas trabajadoras son responsables de conocer y cumplir las leyes y normativas internas. En cualquier caso, el Grupo FCC pondrá a su disposición los medios necesarios para que conozcan y comprendan sus obligaciones.

Asimismo, cada Entidad FCC (cualquiera que sea su forma jurídica) es la responsable de cumplir con las obligaciones y requisitos exigidos por el Reglamento Europeo de Protección de Datos, por la normativa local de Protección de Datos que resulte de aplicación y con las decisiones e instrucciones remitidas por el departamento de SI sobre dicha materia. Esta responsabilidad se extenderá más allá de la fecha de entrada en vigor del RGPD.

De forma general, cada Entidad FCC es responsable, como mínimo, de:

- La correcta adecuación y cumplimiento (en plazo) de las obligaciones establecidas por el Reglamento y la normativa local de Protección de Datos que resulte de aplicación, así como derivadas de esta Normativa.
- Establecer un sistema sólido de evidencias que le permita demostrar a posteriori su correcto cumplimiento.
- Comunicar al Coordinador de Protección de Datos del área cualquier cambio societario que pueda tener reflejo en gestión de la Privacidad. Dicha comunicación habrá de ser con carácter previo a la realización efectiva.
- Afrontar las sanciones económicas que les sean impuestas por la Autoridad de Control en caso de incumplimiento de las exigencias del Reglamento y de la normativa local de Protección de Datos que resulte de aplicación.

El legislador ha aumentado considerablemente la cuantía de las sanciones económicas. Se prevé, en caso de incumplimiento o cumplimiento defectuoso, la imposición de sanciones administrativas cuyo importe puede llegar a alcanzar los 20.000.000€ o el 4% del volumen de negocio total anual global del ejercicio financiero anterior (optándose por la de mayor cuantía**)**, en el caso de infracciones muy graves, además del correspondiente daño reputacional.

4. Referencia normativa

El presente documento ha sido revisado por el departamento de SI y su redacción toma como referencia a las siguientes normativas:

- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE
- Conjunto de directrices de Seguridad de la Información del Grupo FCC, desde una perspectiva jurídica, técnica y organizativa.
- Estándar internacional ISO27001:2022 y ENS.

4.1 Controles de la normativa ISO27001:2022 y ENS

ID Control ISO	Control ISO/IEC 27001:2022	Correspondencia ENS
5.1	Políticas para la seguridad de la información	[org.1] Política de Seguridad; [org.2] Normativa de Seguridad
5.2	Roles y responsabilidades en seguridad de la información	[org.4] Proceso de Autorización
5.24	Planificación y preparación de la gestión de incidentes de seguridad de la información	[op.exp.7] Gestión de Incidentes
5.25	Evaluación y decisión sobre eventos de seguridad de la información	[op.exp.7] Gestión de Incidentes
5.26	Respuesta a incidentes de seguridad de la información	[op.exp.9] Registro de la Gestión de Incidentes
5.28	Recopilación de evidencias	[op.exp.7] Gestión de Incidentes; [op.exp.9] Registro de la Gestión de Incidentes
5.31	Identificación de requisitos legales, reglamentarios y contractuales	[op.leg.1] Identificación de requisitos legales
5.34	Privacidad y protección de datos de carácter personal	[op.pdp.1] Protección de datos personales
5.36	Cumplimiento de las políticas, reglas y normas de seguridad de la información	[org.4] Proceso de Autorización; [op.exp.3] Gestión de la Configuración; [op.exp.4] Mantenimiento y Actualizaciones de Seguridad
5.37	Documentación de procedimientos operativos	[org.3] Procedimientos de Seguridad

6.3	Concienciación, educación y formación	[mp.per.3] Concienciación; [mp.per.4] Formación
6.8	Reporte de eventos de seguridad de la información	[op.exp.7] Gestión de Incidentes
8.10	Eliminación de la información	[mp.si.5] Borrado y destrucción
8.11	Enmascaramiento de datos	[mp.info.1] Datos personales
8.12	Prevención de fugas de datos	[mp.com.1] Perímetro seguro; [mp.com.2] Protección de la confidencialidad; [mp.si.2] Criptografía; [mp.eq.3] Protección de dispositivos portátiles
8.24	Uso de criptografía	[op.exp.10] Protección de claves criptográficas; [mp.si.2] Criptografía; [mp.info.3] Firma electrónica