



# Norma de Privacidad del Grupo FCC

Julio de 2025

ID	<b>NORMA DE PRIVACIDAD</b>	CLASIFICACIÓN	VERSIÓN	FECHA
IS_ST_12		FCC_INTERNAL	2.1	Julio 2025

<b>Historial de Versiones</b>				
<b>Versión</b>	<b>Fecha</b>	<b>Autor</b>	<b>Detalle</b>	<b>Aprobador</b>
<b>1.0</b>	Abril 2009	IS	Creación del Documento	Chief Information Security Officer (CISO)
	Octubre 2019	IS	Revisión del Documento	Chief Information Security Officer (CISO)
<b>1.1</b>	Julio 2021	IS	Revisión del Documento Unificación del formato con el resto de la Normativa.	Chief Information Security Officer (CISO)
<b>2.0</b>	Mayo 2024	IS	Revisión del documento y adaptación a normativa ISO27001:2022	Chief Information Security Officer (CISO)
<b>2.1</b>	Julio 2025	IS	Revisión del documento y adaptación al ENS	Chief Information Security Officer (CISO)

ID	<b>NORMA DE PRIVACIDAD</b>	CLASIFICACIÓN	VERSIÓN	FECHA
IS_ST_12		FCC_INTERNAL	2.1	Julio 2025

## ÍNDICE

<b>1. Introducción.....</b>	<b>4</b>
1.1 Objeto.....	4
1.2 Alcance.....	4
1.2.1 Geográfico.....	4
1.2.2 Material.....	4
<b>2. Seguridad de la Privacidad de Datos .....</b>	<b>5</b>
2.1 Definiciones.....	5
2.2 Valores en la Protección de Datos .....	6
2.3 Principios Generales en la Gestión de Datos Personales .....	7
2.3.1 Principio de Consentimiento .....	7
2.3.2 Principio de Información al titular de los datos.....	7
2.3.3 Principio de Proporcionalidad .....	7
2.3.4 Principio de Calidad .....	7
2.3.5 Principio de Seguridad.....	7
2.3.6 Principio de Legalidad.....	8
2.4 Directrices de Tratamiento.....	8
2.4.1 Organización y responsabilidades en materia de Privacidad .....	8
2.4.2 Tratamiento de datos sensibles.....	9
2.4.3 Contratos de Prestación de Servicios .....	10
2.4.4 Transferencia Internacional de Datos .....	10
2.4.5 Derechos de Acceso, Rectificación, Cancelación y Oposición.....	10
2.4.6 Auditorías .....	11
2.4.7 Comunicación inmediata de incidencias acaecidas en materia de Protección de Datos	11
2.4.8 Cumplimiento de la normativa de Protección de Datos vigente en cada Estado.	11
<b>3. Responsabilidades .....</b>	<b>11</b>
<b>4. Referencia normativa .....</b>	<b>11</b>
4.1 Controles de la normativa ISO27001:2022 y ENS .....	11

ID	<b>NORMA DE PRIVACIDAD</b>	CLASIFICACIÓN	VERSIÓN	FECHA
IS_ST_12		FCC_INTERNAL	2.1	Julio 2025

## 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.

### 1.1 Objeto

El objeto de la presente Norma consiste en especificar los principios y extremos básicos que deben ser observados y cumplidos en el tratamiento de Datos Personales por las Entidades del Grupo FCC.

### 1.2 Alcance

#### 1.2.1 Geográfico

Esta Norma se aplica a las Entidades que pertenecen al Grupo FCC ubicadas en cualquier Estado/País/Región del mundo (en adelante, Entidad/es FCC) que quedan comprendidas en las siguientes:

- Aquellas Entidades en las que el Grupo FCC posea la mayoría de participación.
- Aquellas Entidades que a pesar de no poseer el Grupo FCC la mayoría de participación, si ostenta la gestión de la misma.

#### 1.2.2 Material

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

ID	<b>NORMA DE PRIVACIDAD</b>	CLASIFICACIÓN	VERSIÓN	FECHA
IS_ST_12		FCC_INTERNAL	2.1	Julio 2025

## 2. Seguridad de la Privacidad de Datos

### 2.1 Definiciones

- a. «Datos Personales»: Toda información sobre una persona física identificada o identificable (el «titular, interesado o afectado»); se considerará identificable a toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social.
- b. «Tratamiento de Datos Personales» («tratamiento»): Cualquier operación o conjunto de operaciones, efectuadas o no, mediante procedimientos automatizados, y aplicadas a datos personales, como la recogida, registro, organización, conservación, elaboración o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma que facilite el acceso a los mismos, cotejo o interconexión, así como su bloqueo, supresión o destrucción.
  - «Responsable del Fichero»: La persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que sólo o conjuntamente con otros determine los fines y los medios del tratamiento de datos personales y que se registrará por su derecho nacional.
- c. En este sentido, cada Entidad del Grupo FCC será Responsable del Fichero en relación con los datos personales que gestione (p.ej. de Empleados, Clientes y Proveedores).
  - «Encargado del Tratamiento»: La persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento.
- d. «Consentimiento del Interesado»: Toda manifestación de voluntad, libre, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernan.
- e. «Datos sensibles»: Datos relativos a la salud, afiliación sindical, al origen racial o étnico, a las opiniones políticas, a las convicciones religiosas o filosóficas, así como el tratamiento de los datos relativos a la sexualidad.
- f. «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 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.

ID	<b>NORMA DE PRIVACIDAD</b>	CLASIFICACIÓN	VERSIÓN	FECHA
IS_ST_12		FCC_INTERNAL	2.1	Julio 2025

- «Cancelación de datos»: Procedimiento en virtud del cual el Responsable del Fichero cesa en el uso de los datos. La cancelación implicará la supresión o eliminación física de los datos, salvo en caso de que sea necesario conservarlos durante el plazo de prescripción de posibles responsabilidades nacidas del tratamiento. En ese caso, se conservarán previo bloqueo de los datos, consistente en la identificación y reserva de los mismos con el fin de impedir su tratamiento excepto para su puesta a disposición de las Administraciones públicas, Jueces y Tribunales. Transcurrido ese plazo deberá procederse a la supresión de los datos.

## **2.2 Valores en la Protección de Datos**

El Grupo FCC es un grupo en constante evolución que apuesta por el uso de los últimos sistemas de información y avances tecnológicos. Esto hace que, en la práctica, la información pueda ser almacenada y procesada en grandes cantidades y en poco tiempo.

Por ello, el Grupo FCC está constantemente preocupado por la confidencialidad, seguridad y buen uso de la información que gestiona en sus procesos diarios y, en concreto, de los Datos Personales de sus Empleados, Clientes y Proveedores, a los que presta especial atención.

Es por ello que, en el tratamiento de los Datos Personales, el Grupo FCC fundamenta dicho tratamiento sobre los siguientes valores:

- Transparencia y confianza respecto al tratamiento seguro de los Datos Personales en todo momento.
- Responsabilidad y compromiso en el uso de los Datos Personales basado principalmente en la confidencialidad de los mismos.
- Eficiencia en la gestión segura de los Datos Personales que se tratan en el Grupo FCC.
- Disponibilidad de los Datos Personales cuando sean necesarios y únicamente por las personas que lo necesiten por razón de sus funciones.
- Integridad de la información que evite manipulaciones no autorizadas.

ID	<b>NORMA DE PRIVACIDAD</b>	CLASIFICACIÓN	VERSIÓN	FECHA
IS_ST_12		FCC_INTERNAL	2.1	Julio 2025

## **2.3 Principios Generales en la Gestión de Datos Personales**

Cada Entidad FCC deberá gestionar los Datos Personales de acuerdo a los siguientes principios:

### **2.3.1 Principio de Consentimiento**

Los Datos Personales únicamente podrán ser objeto de tratamiento por la Entidad FCC o comunicados a otro Organismo si su titular hubiera prestado previamente su consentimiento para ello. No obstante, lo anterior, será posible el tratamiento o la comunicación de datos personales sin necesidad del consentimiento de su titular cuando así lo autorice una norma nacional o sean necesarios para la gestión y mantenimiento de un contrato.

### **2.3.2 Principio de Información al titular de los datos**

De forma previa a cualquier recogida de Datos Personales, la Entidad FCC deberá informar al titular de los mismos de manera fehaciente, como mínimo, de sus datos identificativos, de los fines de la recogida y tratamiento, de los destinatarios de datos en caso de que se deban comunicar a otras personas distintas de su titular, así como de la posibilidad de ejercer los derechos de acceso, rectificación, cancelación y oposición de los Datos Personales.

### **2.3.3 Principio de Proporcionalidad**

Los Datos Personales gestionados por la Entidad FCC, únicamente podrán ser recabados y tratados con fines determinados y explícitos y serán adecuados, pertinentes y no excesivos con relación a la finalidad para la que fueron recogidos.

### **2.3.4 Principio de Calidad**

Los Datos Personales gestionados por la Entidad FCC deberán ser reflejo de la realidad y estarán actualizados en todo momento, cancelándose los Datos Personales cuando se haya cumplido la finalidad para la que fueron recabados.

### **2.3.5 Principio de Seguridad**

La Entidad FCC deberá garantizar la confidencialidad de los Datos Personales, el acceso a los mismos únicamente por el personal autorizado y la seguridad de los mismos para lo que implantará las medidas de seguridad técnicas y organizativas necesarias en función de la tipología de Datos Personales tratados que impidan accesos no autorizados, su destrucción y/o pérdida de los mismos.

ID	<b>NORMA DE PRIVACIDAD</b>	CLASIFICACIÓN	VERSIÓN	FECHA
IS_ST_12		FCC_INTERNAL	2.1	Julio 2025

### 2.3.6 Principio de Legalidad

En todo caso y, además de lo especificado anteriormente, los Datos Personales gestionados por la Entidad FCC, deberán utilizarse de manera lícita y conforme a la finalidad por la que fueron recabados, de acuerdo con la legislación de cada Estado/País/Región y respetando los derechos y libertades de los Interesados o Afectados.

## 2.4 Directrices de Tratamiento

### 2.4.1 Organización y responsabilidades en materia de Privacidad

En materia de Privacidad, el Grupo FCC se ha dotado de una estructura organizativa con unos roles y responsabilidades definidas:

#### 2.4.1.1 ESTRUCTURA ORGANIZATIVA:

- El departamento de SI: Es la máxima figura en la gestión y coordinación de la Privacidad en todo el Grupo FCC.
- Coordinador de Protección de Datos: Es la máxima figura en la gestión y coordinación de la Privacidad en su Área de actuación.
- A los efectos de este documento, se consideran Áreas las siguientes: FCC Corporación, FCC Construcción, FCC Versia, FCC Servicios Medio Ambiente, FCC Servicios Residuos Industriales, FCC Servicios Aguas, FCC Energía y Grupo Cementos Portland Valderrivas.
- Responsable de Seguridad de la Entidad FCC: Es la máxima figura en la gestión y coordinación de la Privacidad en la Entidad FCC.

Si lo estima oportuno, el departamento de SI procederá a la creación y/o modificación de las figuras descritas anteriormente en materia de Privacidad.

#### 2.4.1.2 ROLES Y RESPONSABILIDADES:

Los roles y responsabilidades para cada una de las figuras son, como mínimo, los siguientes:

- El departamento de SI:
  - Especificar las directrices generales que se deberán observar y cumplir en materia de Privacidad en FCC.
  - Gestionar, implantar las medidas y coordinar la Privacidad en el Grupo FCC.

ID	<b>NORMA DE PRIVACIDAD</b>	CLASIFICACIÓN	VERSIÓN	FECHA
IS_ST_12		FCC_INTERNAL	2.1	Julio 2025

- Apoyar al resto de figuras en la implantación de las acciones y medidas necesarias en materia de Privacidad.
- **Coordinador de Protección de Datos:**
  - Gestionar, implantar las medidas necesarias y coordinar la Privacidad en el Área que gestiona.
  - Apoyar al departamento de SI y a los Responsables de Seguridad de las Entidades que se encuentran dentro de su Área, en el cumplimiento de las acciones necesarias en materia de Privacidad.
  - Reportar periódicamente al departamento de SI, las acciones y medidas implantadas en su Área y en las Entidades FCC que están dentro de la misma.
  - Reportar inmediatamente al departamento de SI cualquier incidencia en materia de Privacidad, así como cualquier comunicación o solicitud de información requerida desde la autoridad de control en materia de Protección de Datos.
- **Responsable de Seguridad:**
  - Gestionar, implantar las medidas necesarias y coordinar la Privacidad en la Entidad FCC de la que es Responsable.
  - Apoyar al departamento de SI, al Coordinador de Protección de Datos del Área al que pertenece su Entidad y los Responsables de Seguridad de las Entidades que se encuentran dentro de su Área, en el cumplimiento de las acciones necesarias en materia de Privacidad.
  - Reportar periódicamente al Coordinador de Protección de Datos de su Área, las acciones y medidas implantadas en su Entidad.
  - Reportar inmediatamente al departamento de SI cualquier incidencia en materia de Privacidad, así como cualquier comunicación o solicitud de información requerida desde la autoridad de control en materia de Protección de Datos.

#### **2.4.2 Tratamiento de datos sensibles**

Se prohíbe a las Entidades FCC cualquier tratamiento de Datos Personales referidos al origen racial o étnico, a las opiniones políticas, a las convicciones religiosas o filosóficas, así como el tratamiento de los datos relativos a la sexualidad.

En todo caso, para el tratamiento de datos personales de salud y de pertenencia a sindicatos, la Entidad FCC necesitará el consentimiento expreso, previo y por escrito del titular de dichos datos, salvo en los casos en los que la legislación del Estado en el que se encuentre la Entidad del Grupo FCC disponga que la prohibición establecida en el primer párrafo no pueda levantarse con el consentimiento del Interesado.

ID	<b>NORMA DE PRIVACIDAD</b>	CLASIFICACIÓN	VERSIÓN	FECHA
IS_ST_12		FCC_INTERNAL	2.1	Julio 2025

### 2.4.3 Contratos de Prestación de Servicios

En el caso de que fuera necesaria la contratación de determinados Servicios a una Entidad externa o a cualquier otra Entidad del Grupo FCC (en adelante, Encargado del Tratamiento) en virtud de la cual éste pueda/deba acceder a Datos Personales, la Entidad FCC deberá realizar las siguientes acciones:

- Elegir un Encargado del Tratamiento que tenga implantadas las medidas de seguridad necesarias acordes a la tipología de los datos que vaya a gestionar.
- Firmar de manera previa al acceso/gestión de cualquier dato, un Contrato de Prestación de Servicios en el que se establezca expresamente que el Encargado del Tratamiento sólo actúa siguiendo instrucciones de la Entidad FCC; así como que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, ni los comunicará, ni siquiera para su conservación, a otras personas.

Para la elaboración del Contrato de Prestación de Servicios, el Departamento Legal de cada Entidad FCC deberá tomar como base el modelo Contrato de Prestación de Servicios que le proporcione el Coordinador de Protección de Datos del Área al que pertenezca la Entidad FCC y dicho Departamento Legal deberá ajustarlo a las obligaciones y exigencias de la normativa nacional en cada caso. 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.

### 2.4.4 Transferencia Internacional de Datos

En caso de que la Entidad FCC deba transferir Datos Personales a otra Entidad FCC y/u Organismo Público/Privado que se encuentra en un país diferente de aquel en el que está ubicada, la Entidad FCC que pretenda exportar los datos deberá revisar y cumplir con los requisitos específicos de su normativa nacional, que podrá requerir obtener previamente la aprobación y autorización de las autoridades y reguladores de protección de datos del país en el que se encuentre la Entidad FCC que pretenda exportar los datos.

A este respecto, la Entidad FCC que pretenda transferir Datos Personales a otro país, deberá comunicarlo al Coordinador de Protección de Datos del Área al que pertenezca dicha Entidad FCC.

### 2.4.5 Derechos de Acceso, Rectificación, Cancelación y Oposición

La Entidad FCC deberá gestionar el ejercicio de solicitud de Derechos de Acceso, Rectificación, Cancelación y Oposición de los datos cumpliendo con los plazos y la forma que exija su normativa nacional vigente.

ID	<b>NORMA DE PRIVACIDAD</b>	CLASIFICACIÓN	VERSIÓN	FECHA
IS_ST_12		FCC_INTERNAL	2.1	Julio 2025

En este sentido y, a no ser que la normativa nacional vigente especifique otra cosa, el ejercicio de cualquier de los Derechos deberá ser contestado por escrito y dentro del mes para el caso de los derechos de Acceso y dentro de los 10 días hábiles a partir de la fecha en la que se recibió la notificación en el caso del resto de Derechos.

#### **2.4.6 Auditorías**

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

El departamento de SI aportará las instrucciones correspondientes de forma previa a su realización a la Entidad FCC y ésta deberá reportar al departamento de SI los resultados de la misma.

#### **2.4.7 Comunicación inmediata de incidencias acaecidas en materia de Protección de Datos**

Cualquier incidencia de seguridad relacionada con datos personales, deberá ser comunicada inmediatamente por la Entidad FCC al departamento de SI de FCC.

#### **2.4.8 Cumplimiento de la normativa de Protección de Datos vigente en cada Estado**

Esta Norma se aplicará directamente en cada una de las Entidades, y en caso de que las áreas o Entidades FCC aprueben o hayan aprobado sus propias normativas internas en materia de protección de Datos Personales, éstas no deben contradecir la presente Norma, que prevalecerá en todo caso.

Asimismo, la Entidad FCC deberá cumplir en todo caso con lo especificado por su normativa nacional en materia de Protección de Datos.

### **3. Responsabilidades**

Los roles y responsabilidades del personal al que hace referencia esta Norma se especifican en el punto *2.4.1 Organización y responsabilidades en materia de Privacidad* del presente documento.

### **4. Referencia normativa**

El presente documento ha sido revisado por el departamento de SI y su redacción toma como referencia el 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
----------------	----------------------------	---------------------

ID	<b>NORMA DE PRIVACIDAD</b>	CLASIFICACIÓN	VERSIÓN	FECHA
IS_ST_12		FCC_INTERNAL	2.1	Julio 2025

<b>5.2</b>	Roles y responsabilidades en seguridad de la información	[org.4] Proceso de Autorización
<b>5.5</b>	Contacto con las autoridades	[op.exp.7] Gestión de Incidentes
<b>5.6</b>	Contacto con grupos de interés especial	[org.1] Política de Seguridad
<b>5.19</b>	Seguridad de la información en las relaciones con proveedores	[op.ext.1] Contratación y acuerdos de nivel de servicio
<b>5.20</b>	Abordar la seguridad de la información en los acuerdos con proveedores	[op.ext.1] Contratación y acuerdos de nivel de servicio
<b>5.31</b>	Identificación de requisitos legales, reglamentarios y contractuales	[op.leg.1] Identificación de requisitos legales
<b>5.34</b>	Privacidad y protección de datos de carácter personal	[op.pdp.1] Protección de datos personales
<b>5.35</b>	Revisión independiente de la seguridad de la información	Art. 31 / Anexo III Auditoría de la Seguridad
<b>5.36</b>	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
<b>6.8</b>	Reporte de eventos de seguridad de la información	[op.exp.7] Gestión de Incidentes
<b>8.34</b>	Protección de los sistemas de información durante las pruebas de auditoría	[op.exp.2] Configuración de Seguridad; [op.exp.3] Gestión de la Configuración; [op.exp.4] Mantenimiento y Actualizaciones de Seguridad; [mp.s.2] Protección de servicios y aplicaciones Web