

Política de Gestión de la Información del Grupo FCC

Junio 2026

Historial de Versiones				
Versión	**Fecha**	**Autor**	**Detalle**	**Aprobador**
1.0	Abril 2009	IS	Creación del documento	Consejo de Administración del Grupo FCC
2.0	Febrero 2021	IS	Revisión del documento. Unificación del formato con el resto de Normas y nueva estructura de clasificación de la información	Consejo de Administración del Grupo FCC
3.0	Mayo 2023	IS	Revisión de documentos. Adaptación a la normativa ISO/IEC 27001:2022	Consejo de Administración del Grupo FCC
4.0	Enero 2024	IS	Estandarización de diagramas y actualización de plantillas de documentos de acuerdo con la nueva convención de identificadores	Consejo de Administración del Grupo FCC
5.0	Julio 2025	IS	Revisión de documentos. Adaptación a la normativa ENS Nivel Medio	Consejo de Administración del Grupo FCC
6.0	Junio 2026	IS	Revisión del documento y cambio de formato	-

ÍNDICE

1. Introducción....4

1.1 Objeto....4

1.2 Alcance....4

2. Desarrollo....5

2.1 Principios de la gestión de la Información....5

2.2 Clasificación de la información....6

2.2.1 Modelo de Clasificación de la Información del Grupo FCC....7

2.3 Etiquetado de la Información....9

2.4 Gestión del Almacenamiento de la Información....10

2.4.1 Gestión específica del almacenamiento de la información Restringida....10

2.4.2 Auditoría y Sistemas de Información....10

3. Responsabilidades....11

4. Referencia normativa....12

4.1 Controles de la normativa ISO27001:2022 y ENS....12

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 del historial de versiones, revisiones y aprobaciones de la presente Política, así como su relación y dependencia con el resto de los documentos normativos.

Esta política será revisada, por lo menos, anualmente, salvo que existan circunstancias que recomienden o exijan una revisión antes de dicha fecha.

1.1 Objeto

La presente Política tiene por objeto conseguir una gestión de la información del Grupo FCC que:

- Sea eficiente y eficaz.
- Proporcione soporte a las actividades de negocio.
- Facilite la toma de decisiones.
- Asegure la confidencialidad, integridad, disponibilidad, autenticidad, trazabilidad y auditabilidad de la información.
- Sirva como compromiso de mejora continua de los sistemas de gestión de la información.
- Se ajuste al reglamento y a la legislación aplicable.

1.2 Alcance

Esta Política se aplicará a toda la información del Grupo FCC, incluida la información existente con anterioridad a su entrada en vigor.

2. Desarrollo

2.1 Principios de la gestión de la Información

- Se permitirá el acceso a la información únicamente al personal del Grupo que tenga necesidad de conocerla para el correcto desempeño de sus funciones y siempre bajo el principio de “mínimo privilegio”.
- La información se distribuirá respetando los principios de actuación de FCC y las limitaciones impuestas por criterios de seguridad, legalidad y/o privacidad.
- La información de FCC se gestionará como un recurso corporativo que da soporte a los objetivos y a las actividades de negocio.
- La gestión de la información se regirá por políticas, normas, procedimientos y guías que aseguren su confidencialidad, integridad, disponibilidad, autenticidad, trazabilidad y auditabilidad.
- La organización y el control de la información se realizará a lo largo de todo su ciclo de vida, independientemente del formato y medio en que se trate.
- Las medidas de protección aplicables a la información se incluirán en los acuerdos que regulen las relaciones entre FCC y entidades externas que requieran acceso a la misma.
- La información se clasificará y etiquetará de acuerdo con esquema de clasificación de la Información de FCC determinado por este documento y por la Norma de Seguridad de Documentos.
- Aquella información que no esté etiquetada tendrá por defecto la consideración de Información de nivel Restringido Interno.
- El responsable de la información garantizará las condiciones de seguridad requeridas según su nivel de clasificación, cuando proceda a su distribución y almacenamiento.
- El impacto potencial de un incidente definirá la necesidad de cifrar la información. La información clasificada como Restringida (Interno, Confidencial, Secreto) deberá ser protegida mediante cifrado cuando no se pueda garantizar una protección suficiente mediante otros controles, las características del cifrado vendrán determinadas por la Norma de Cifrado.
- Antes de distribuir o intercambiar cualquier información fuera del Grupo FCC, ésta deberá ser evaluada por el propietario de la información para identificar cualquier tipo de activo de nivel restringido y protegerlo aplicando las medidas estipuladas en la Guía de Manejo Seguro de la Información.
- Una vez revisada la información y aplicadas las medidas de protección apropiadas a su nivel de clasificación, la información se podrá reclasificar como de Uso Público para ser compartida fuera del grupo FCC.
- En el caso de que se divulgue o comparta por error un activo de nivel Restringido con terceros sin que el activo cuente con el nivel de clasificación adecuado, se notificará de forma inmediata el evento al departamento de SI.

2.2 Clasificación de la información

La clasificación de la información en FCC tiene como finalidad catalogar la información propiedad del Grupo o terceras partes interesadas (clientes, socios, colaboradores del Grupo, etc.) de acuerdo con su nivel de confidencialidad, considerada ésta como la sensibilidad de la información ante su potencial divulgación, para la consecución de los objetivos de negocio.

Toda información propiedad de Grupo FCC o terceras partes interesadas se deberá clasificar y etiquetar en el momento de su creación, siguiendo la Guía de Manejo Seguro de la Información.

No obstante, lo anterior, dado que la sensibilidad y/o criticidad de la información puede variar durante su ciclo de vida al tiempo que varía la necesidad o el objetivo por la que fue creada en origen, cualquier información puede ser reclasificada en cualquier momento, siguiendo asimismo el procedimiento de reclasificación de la información descrito en la Guía de Manejo Seguro de la Información.

El responsable de la información realizará de manera expresa la clasificación de la información o, en su caso, la posterior reclasificación, en función del modelo de clasificación de FCC, que se describe más abajo. Cuando la información provenga de una fuente externa, el responsable de dicha información por parte de FCC deberá reclasificar la información recibida de acuerdo con el modelo de clasificación del Grupo FCC, salvo que exista obligación expresa de aplicar los niveles de clasificación de la otra parte o la información ya haya sido previamente clasificada por la otra parte.

2.2.1 Modelo de Clasificación de la Información del Grupo FCC

FCC clasifica la información que trata tomando como criterio principal el daño potencial que podría ocasionar su difusión a personal no autorizado.

La información del Grupo FCC se clasificará en cuatro niveles:

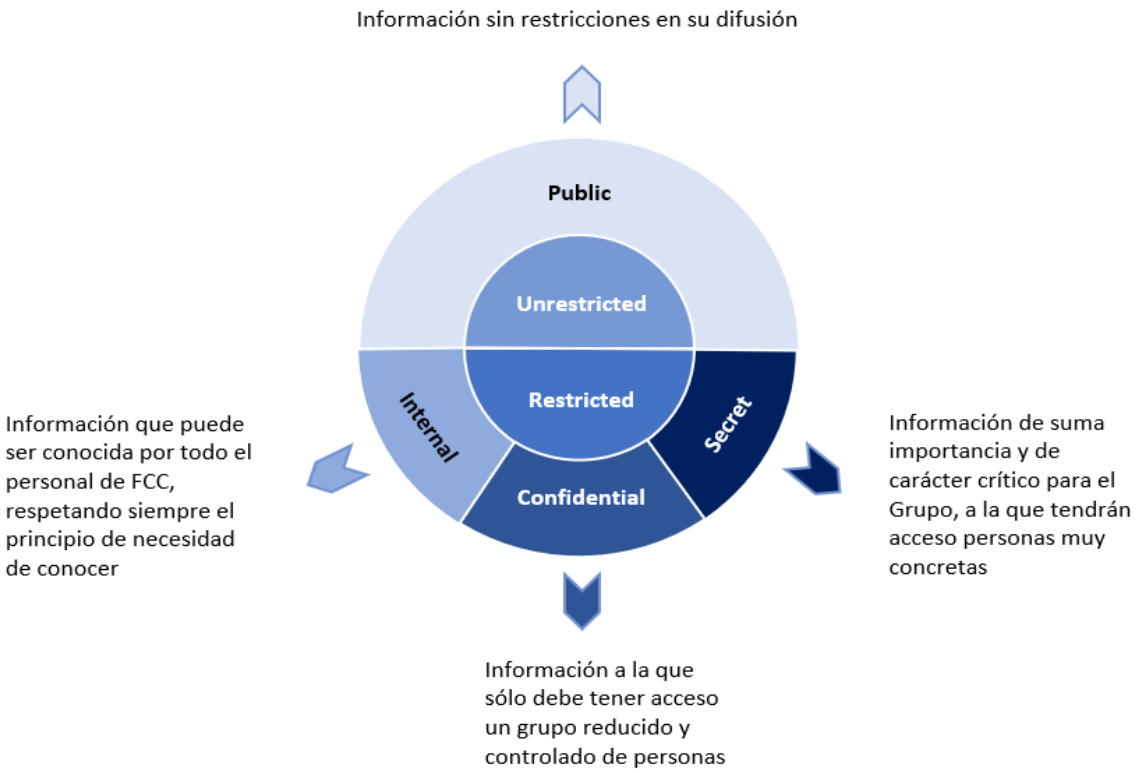


Figura 1. Esquema de clasificación de la información del Grupo FCC

- **Información de Uso Público:** información que concierne o no específicamente al Grupo FCC, que será divulgada o publicada a través de los canales oficiales y, por tanto, no requiere limitaciones de acceso. No precisa de medidas de seguridad específicas, puesto que la información está destinada a su publicación y/o divulgación sin restricciones o limitación de acceso.
- **Información de Uso Interno:** información destinada únicamente para su uso dentro de la organización, ya sea por el personal del Grupo FCC o terceras partes interesadas autorizadas por un tiempo acotado para su uso o acceso y bajo la supervisión del responsable de la información. En general, es información que si se ve comprometida no causaría una disrupción o daño reputacional significativo para el Grupo FCC o terceras partes interesadas. Precisa de medidas de seguridad que limiten su acceso por parte del personal ajeno al Grupo FCC que no requiera de dicha información para cumplir los objetivos de su colaboración con el Grupo.

Esta será la clasificación por defecto para la información de FCC no catalogada previamente.

- **Información Confidencial:** información destinada a un grupo limitado y controlado de personas. Es información que si se ve comprometida podría ser altamente perjudicial para los intereses del Grupo FCC o causar dificultades operativas para la organización, sus clientes o partes interesadas con las que colabora, incluyendo sanciones derivadas de la vulneración de los derechos de privacidad de las personas. El uso y acceso a esta información deberá estar controlado y deberá ser expresamente autorizado por el responsable de la información. El responsable de la información confidencial deberá garantizar unas medidas de seguridad adecuadas que ayuden a proteger su confidencialidad tanto fuera como dentro de la organización, limitando su acceso y distribución a un grupo controlado de personas, que cumplan estrictamente el principio de necesidad de conocer.
- **Información Secreta:** información destinada a un grupo altamente restringido de personas, que, en caso de verse comprometida, podría ocasionar la pérdida abrupta de reputación o ventajas competitivas. En general, es información de alto valor o sensibilidad, que debe contar con unas altas medidas de seguridad para asegurar su confidencialidad tanto fuera como dentro de la organización. El acceso a esta información deberá estar altamente controlado y deberá ser registrado, verificando periódicamente que se satisfacen los criterios de acceso y compartición.

El Grupo FCC, a través del departamento de SI, deberá garantizar la seguridad de la información mediante la implementación de medidas organizativas y técnicas que ayuden a asegurar la privacidad y confidencialidad de la información, de acuerdo con la clasificación de esta. Las medidas organizativas mencionadas se concentrarán en la Norma de Seguridad en documentos.

2.3 Etiquetado de la Información

Toda la información del Grupo FCC deberá estar debidamente etiquetada de acuerdo con su nivel de clasificación.

Únicamente el responsable de la información podrá proceder al etiquetado de la información de la que es responsable.

Al clasificar la información debe incorporar, independientemente del soporte en el que esté contenida la información, una de las siguientes etiquetas, excluyentes entre sí:

- Información No Restringida Uso Público: **FCC_PUBLIC**
- Información Restringida Confidencial: **FCC_CONFIDENTIAL**
- Información Restringida Uso Interno: **FCC_INTERNAL**
- Información Restringida Secreta: **FCC_SECRET**

La información no etiquetada será considerada de Uso Interno, a excepción de la archivada con anterioridad a la entrada en vigor de la presente Política. En este caso, se procederá a su clasificación cuando se desarchive.

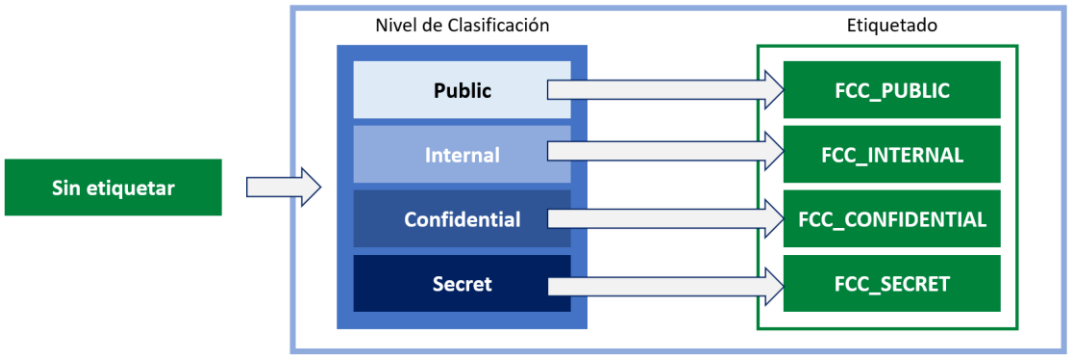


Figura 2. Esquema de etiquetado de la información del Grupo FCC

2.4 Gestión del Almacenamiento de la Información

El almacenamiento de la información se realizará de forma que asegure su confidencialidad, integridad, disponibilidad, autenticidad, trazabilidad.

Se permitirá el acceso a la información únicamente al personal que tuviera necesidad de conocerla en el desempeño de sus funciones. En el caso de externalizar la gestión del almacenamiento de la información, se fijarán en los acuerdos las medidas de seguridad mínimas aplicables y el régimen de responsabilidades derivado de la posible revelación de dicha información a terceros no autorizados.

2.4.1 Gestión específica del almacenamiento de la información Restringida

Los locales, dispositivos y/o soportes que almacenen información **Restringida**, estarán dotados de medidas de seguridad que permitan el acceso exclusivo a las personas autorizadas.

2.4.2 Auditoría y Sistemas de Información

La auditoría de sistemas permitirá conocer si la protección de la información es proporcionada y cumple con el Marco Normativo de Seguridad de la Información del Grupo FCC.

Como resultado de las conclusiones alcanzadas en la auditoría, el responsable deberá desarrollar las acciones adecuadas para la mejora de la gestión de la seguridad.

Las auditorias serán periódicas y se basarán en criterios de riesgo.

3. Responsabilidades

El **Comité de Ciberseguridad** tendrá como responsabilidades:

- Establecer los criterios generales para la clasificación y gestión de activos de información.
- Aprobar el Modelo de Clasificación y Gestión de Activos de Información.

Los **responsables de la información** tendrán como responsabilidad:

- Asegurar la correcta clasificación de la información y que las personas que tratan la información que están bajo su responsabilidad, están autorizadas para ello.

El **personal de FCC** tendrá como responsabilidad:

- Cumplir con los principios definidos en la presente Política.

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
5.1	Políticas para la seguridad de la información	[org.1] Política de Seguridad; [org.2] Normativa de Seguridad
5.9	Inventario de información y otros activos asociados	[op.exp.1] Inventario de activos; [op.pl.2] Arquitectura de Seguridad
5.12	Clasificación de la información	[mp.info.2] Calificación de la información
5.13	Etiquetado de la información	[mp.si.1] Marcado de soportes
5.14	Transferencia de la información	[org.2] Normativa de seguridad; [org.3] Procedimientos de seguridad; [op.ext.1] Contratación y ANS; [mp.s.1] Protección del correo electrónico
5.34	Privacidad y protección de datos de carácter personal	[mp.info.1] Datos personales
5.36	Cumplimiento de las políticas, y normas de seguridad de la información	[org.4] Proceso de Autorización; [op.exp.3] Gestión de la configuración de seguridad; [op.exp.4] Mantenimiento y actualizaciones de seguridad
8.10	Eliminación de la información	[mp.si.5] Borrado y destrucción
8.14	Redundancia de los recursos de tratamiento de la información	[op.cont.4] Medios alternativos
8.16	Seguimiento de actividades	[op.mon.3] Vigilancia; [mp.s.4] Protección frente a DoS