Política de Ciberseguridad y Seguridad de la Información del Grupo FCC

Junio 2026

Historial de Versiones

Versión	Fecha	Autor	Detalle	Aprobador
1.0	Abril 2009	IS	Creación del documento	Chief Information Security Officer (CISO)
2.0	Febrero 2023	IS	Revisión del documento. Unificación del formato con el resto de Normas y nueva estructura de clasificación de la información	Chief Information Security Officer (CISO)
3.0	Mayo 2023	IS	Revisión de documentos. Adaptación a la normativa ISO/IEC 27001:2022	Chief Information Security Officer (CISO)
4.0	Enero 2024	IS	Estandarización de diagramas y actualización de plantillas de documentos de acuerdo con la nueva convención de identificadores	Chief Information Security Officer (CISO)
5.0	Junio 2026	IS	Revisión del documento y cambio de formato	Chief Information Security Officer (CISO)

ÍNDICE

1. Introducción

El presente documento forma parte del Marco Normativo de Seguridad de la Información del Grupo FCC, en el que se desarrollan 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 Política, así como su relación y dependencia con el resto de los documentos normativos.

1.1 Objeto

El objeto de la presente Política es:

- Definir los principios básicos y requisitos mínimos para el desarrollo de medidas de seguridad de los sistemas de información.
- Establecer un esquema organizativo que permita gestionar y controlar la Seguridad de la Información.
- Fortalecer la idoneidad, adecuación, eficacia de la dirección y la gestión de la Seguridad de la Información de acuerdo con las normas comerciales, legales, reglamentarias, y contractuales.

Con el fin de garantizar, de forma proporcionada, la confidencialidad, integridad, disponibilidad y auditabilidad de la información del Grupo FCC.

1.2 Alcance

Esta Política se aplicará a:

- Toda la **información** del Grupo FCC, independientemente del lugar o medio en el que se encuentre.
- Todo **el personal** que trate información del Grupo FCC.
- Toda **normativa** interna que desarrolle algún aspecto particular de la Seguridad de la Información.

2. Desarrollo

2.1 Principios de la gestión de la Seguridad de la Información

La información es un recurso estratégico para FCC, y, por tanto, se debe garantizar su adecuada protección en el desempeño de la actividad diaria y en las relaciones con entidades externas.

La Política de Ciberseguridad y Seguridad de la Información se fundamenta en los siguientes principios básicos de obligado cumplimiento, a tener siempre presentes en cualquier actividad relacionada con el tratamiento de la información:

- El Marco Normativo de Seguridad de la Información es de obligado cumplimiento para todo el personal del Grupo FCC.
- El diseño y la gestión de la Seguridad de la Información debe contemplar los objetivos estratégicos del Grupo FCC.
- La gestión de la Seguridad de la Información necesita una estructura organizativa que represente a su vez la estructura funcional que sea conocida por todo el personal y funcione como la principal referencia.
- La dimensión de la estructura de la organización de Seguridad de la Información será proporcional a las necesidades de seguridad del Grupo FCC.
- Las medidas de protección deben aplicarse en proporción al valor de los activos a proteger, los riesgos existentes y el impacto operacional, reputacional y financiero de los posibles fallos de seguridad.
- El Grupo FCC debe asegurarse de que todos los riesgos están identificados y de que se toman medidas frente a las amenazas contra la Seguridad de la Información de la que es propietario.
- La confidencialidad, integridad, disponibilidad y auditabilidad de la información deben ser preservadas durante su ciclo de vida, independientemente del medio en que esté contenida y del lugar donde se encuentre.
- La normativa interna que se implante para la protección de la información debe adecuarse a lo establecido en la normativa legal vigente.
- La información que el Grupo FCC intercambie con otras personas físicas o jurídicas deberá cumplir con el Marco Normativo de Seguridad de la Información del Grupo FCC.
- La Seguridad de la Información es responsabilidad de todo el personal interno y colaboradores de FCC, el cual debe estar adecuadamente formado para el desempeño de sus funciones.
- El estado del arte de la Ciberseguridad y la Seguridad de la Información será evaluado de forma periódica.

El Grupo FCC ha creado un Modelo de Organización de la Seguridad para asegurar el cumplimiento de los requisitos de seguridad establecidos en sus sistemas de información, basado en los siguientes apartados.

2.2 Criterios

2.2.1 Marco Normativo de Seguridad de la Información

Partiendo de la presente Política, se desarrollará el Marco Normativo de Seguridad de la Información, estructurado en los siguientes cuatro niveles:

- **Las Políticas** definirán los principios, objetivos y criterios de protección que describen la operativa de la Seguridad de la Información. Se aplicarán en el conjunto de sociedades que integran el Grupo FCC.
- **Las Normas** establecerán los requisitos que deben cumplirse para satisfacer y alcanzar los objetivos de seguridad establecidos en las Políticas. Determinan qué hay que proteger y cuál es el nivel de protección adecuado en cada caso. Se aplicarán al conjunto de sociedades que constituyen el Grupo FCC y abarcarán en su conjunto la protección de todos los entornos de los sistemas de información de la organización.
- **Los Procedimientos** describirán de forma concreta quién, cómo, dónde y cuándo se realizarán las tareas específicas para proteger los activos de información, de acuerdo con las Normas. Contendrán, por tanto, sobre todo, especificaciones técnicas para el cumplimiento de los distintos servicios o aspectos de seguridad.
- **Las Guías Técnicas** documentarán de forma explícita y detallada las tareas y acciones a realizar durante la ejecución de un procedimiento.

Las Políticas y Normas serán elaboradas por el departamento de SI, mientras que los Procedimientos y Guías técnicas, por su naturaleza operativa, serán desarrollados por los departamentos que la implanten en cada caso.

2.2.2 Clasificación de la Información

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

La Política de Gestión de la Información establece cuatro niveles de clasificación:

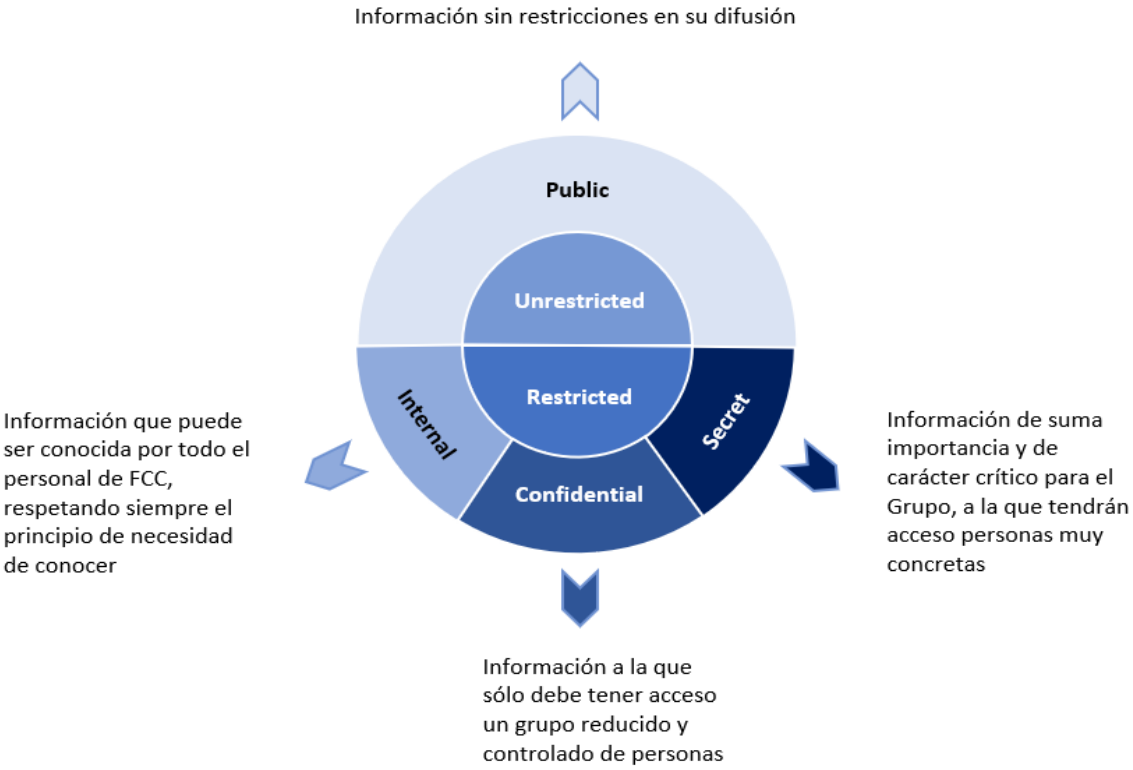

Figura 1. Esquema de clasificación de la información del Grupo FCC

2.2.3 Autorizaciones previas

El acceso a la información se justifica a través de dos vías:

- **La necesidad de conocer la información**: El personal de FCC tendrá acceso, exclusivamente, a la información que necesite conocer para el desempeño de sus funciones profesionales.
- **La habilitación personal para acceder a información Restringida**: FCC habilitará el acceso a información Restringida basándose en el criterio de confianza personal.

Ambas vías de acceso se materializarán en perfiles que permitirán ver, modificar o reproducir la información adecuada en cada caso.

2.3 Acciones

El modelo de gestión de Seguridad de la Información se basará en una serie de acciones que aseguren la confidencialidad, integridad, disponibilidad y auditabilidad de la información, así como el cumplimiento de la normativa legal vigente.

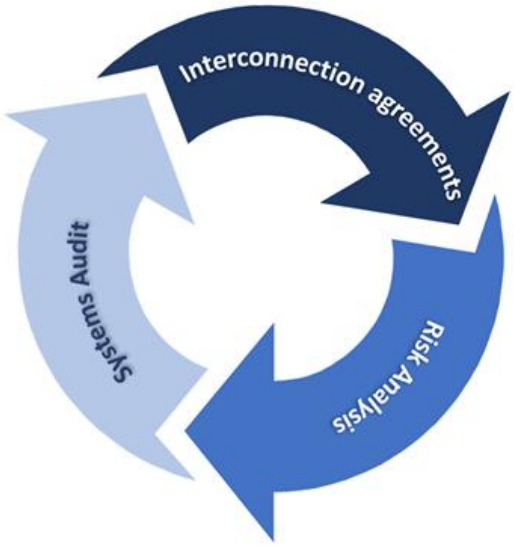

Figura 2. Acciones del modelo de seguridad

2.3.1 Acuerdos de Interconexión

Cuando se interconecten sistemas de información de FCC con diferentes tecnologías, niveles de confianza o implantación de políticas de seguridad, deberá llevarse a cabo un proceso previo de certificación que garantice el nivel adecuado de Seguridad de la Información para el nuevo sistema de información creado tras la interconexión.

El departamento de SI establecerá los criterios, condiciones y requisitos de interconexión basándose en un análisis de riesgos de los respectivos sistemas.

2.3.2 Análisis de Riesgos

El análisis y la gestión de riesgos sobre los sistemas de información se realizará para:

- Valorar los riesgos y determinar, en función de estos, qué medidas se deben aplicar.
- Categorizar y priorizar las actuaciones en materia de Seguridad de la Información.
- Consolidar un esquema de prioridades y consecuencias en caso de que se produzca un incidente de seguridad.
- Mejorar de forma continua el nivel de madurez de seguridad del grupo con motivo de reforzar la eficacia y capacidad de respuesta ante una emergencia de seguridad.
- Cumplir con las responsabilidades establecidas en el Marco Normativo del grupo FCC.
- Preparar a los negocios para cumplir con sus obligaciones legales con las autoridades y operativas y/o contractuales con sus clientes y proveedores en materia de Seguridad de la Información.

El análisis y el tratamiento de los riesgos se revisarán periódicamente.

2.3.3 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.

2.3.4 Gestión de la configuración

Como medida de importancia, es necesario definir unos procedimientos precisos con respecto a las configuraciones de seguridad en las que se incluyen: hardware, software, servicios (p.ej. Servicios Cloud) y redes. Para garantizar el cumplimiento de esta medida, se debe de tomar como referencia la Norma de Control de Configuración y Cambios.

2.4 Organización

El modelo de gestión de Seguridad de la Información del Grupo FCC se sustenta en un modelo de gobierno formado por unos órganos y roles claramente definidos, encargados de impulsar la correcta gestión de su estrategia de ciber resiliencia, reconocer las responsabilidades del personal en todos sus niveles, promover la mejora continua en la gestión de dicha estrategia, y exponer el pleno entendimiento de los riesgos a los que se enfrentan.

2.4.1 Estructura Organizativa

La Seguridad de la información del Grupo FCC se articula mediante las recomendaciones definidas por el departamento de SI.

A continuación, se presentan los comités en donde el departamento de IS tiene presencia y el rol que esta posee:

- El **Consejo de Administración** es el máximo órgano encargado de la aprobación del modelo de organización y gestión de seguridad.
- El **Comité de Ciberseguridad** actuará como máximo órgano de coordinación de la Seguridad de la Información y es el órgano encargado de comunicar la estrategia de seguridad a toda la organización. Se convocará trimestralmente, liderado por el Director de Seguridad de la Información.
- El **Comité de Control de seguridad** es el órgano encargado de coordinar y revisar el estado de seguridad en las diferentes unidades de negocio. Este comité podrá tener calidad de foro o grupo de trabajo si es necesario. Se convocará con cada una de las unidades de negocio y será liderado por un representante del departamento de SI.
- El **Comité de Coordinación TI**: Liderado por el Director de Tecnologías de la Información. Su objetivo es supervisar el estado de los proyectos de TI garantizando el cumplimiento de las recomendaciones de Seguridad de la información.
- **Privacy Board**: Liderado por el Delegado de Protección de Datos. Su objetivo es el tratamiento de las obligaciones legales en materia de protección de datos garantizando el cumplimiento de las recomendaciones de Seguridad de la información.

2.4.2 Áreas de Seguridad de la Información

La protección de la información se concretará en medidas de seguridad dirigidas a las siguientes áreas:

- Seguridad de la Información en las **Personas**, que deben cumplir una serie de requisitos para asegurar el correcto uso de la información.
- Seguridad de la Información en los **Documentos**, a lo largo de todo su ciclo de vida, con el objeto de asegurar la información que contienen.
- Seguridad de la Información en los **Sistemas de Información y Telecomunicaciones**, con el fin de asegurar la información que contienen, tratan o procesan. Antes de comenzar a procesar información del Grupo FCC, los sistemas deberán estar autorizados para ello, de acuerdo con el Marco Normativo de Seguridad de la Información del Grupo.
- Seguridad de la Información en las **Instalaciones**, con el fin de asegurar el procesado y almacenamiento de la información.
- Seguridad de la Información en poder de **Empresas Externas del Grupo**, que deberán aplicar las medidas especificadas por FCC para asegurar la información que traten como consecuencia de su participación en programas, proyectos o contratos con FCC.

3. Responsabilidades

El Grupo FCC es el propietario de la información tratada dentro de las sociedades que lo integran. FCC pone a disposición del personal y sus colaboradores determinados activos de información para cumplir con los objetivos de negocio.

Los roles y responsabilidades recaerán en comités, grupos de trabajo o unidades organizativas, según sean sus funciones:

- Los comités podrán delegar parcialmente sus funciones en aquellos subcomités o grupos de trabajo específicos que se consideren oportunos para cumplir adecuadamente con las funciones que la dirección del Grupo FCC les ha encomendado.
- El responsable de la Información será el encargado de gestionar el acceso a los activos de información, de acuerdo con el Marco Normativo de Seguridad de la Información.

Todas las responsabilidades que se asignen en materia de Seguridad de la Información deberán establecerse con claridad y evitar cualquier posible ambigüedad.

La asignación de responsabilidades se concretará en la Norma de Roles y Responsabilidades en la Seguridad de la Información de FCC.

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 de seguridad de la información	[org.1] Política de Seguridad; [org.2] Normativa de Seguridad
5.2	Funciones y responsabilidades de seguridad de la información	[org.6] Roles y responsabilidades
5.4	Responsabilidades de la dirección	[org.6] Roles y responsabilidades
5.12	Clasificación de la información	[mp.info.2] Clasificación de la información
5.15	Control de acceso	[op.acc.2] Requisitos de acceso
5.18	Derechos de acceso	[op.acc.2] Requisitos de acceso
5.19	Seguridad de la información en las relaciones con los proveedores	[op.ext.1] Contratación y ANS
5.36	Cumplimiento de políticas, reglas y normas de seguridad de la información	[org.2] Normativa de Seguridad
5.37	Procedimientos operativos documentados	[org.3] Procedimientos de seguridad
8.9	Gestión de la configuración	[op.exp.3] Gestión de la configuración de seguridad; [op.exp.4] Mantenimiento y actualizaciones de seguridad