



**Norma de Gestión de
la Configuración y del Cambio
del Grupo FCC**

Julio de 2025

ID	NORMA DE CONTROL DE CONFIGURACIÓN Y DEL CAMBIO	CLASIFICACIÓN	VERSIÓN	FECHA
IS_ST_05		FCC_INTERNAL	1.4	Julio 2025

Historial de Versiones				
Versión	Fecha	Autor	Detalle	Aprobador
1.0	Abril 2009	IS	Creación del Documento	Chief Information Security Officer (CISO)
	Septiembre 2019	IS	Revisión del Documento	Chief Information Security Officer (CISO)
1.1	Julio 2020	IS	Revisión del documento	Chief Information Security Officer (CISO)
1.2	Julio 2021	IS	Revisión del documento Unificación del formato con el resto de la Normativa	Chief Information Security Officer (CISO)
1.3	Mayo 2024	IS	Revisión del documento y adaptación a la normativa ISO27001:2022	Chief Information Security Officer (CISO)
1.4	Julio 2025	IS	Revisión del documento y adaptación al ENS	Chief Information Security Officer (CISO)

ID	NORMA DE CONTROL DE CONFIGURACIÓN Y DEL CAMBIO	CLASIFICACIÓN	VERSIÓN	FECHA
IS_ST_05		FCC_INTERNAL	1.4	Julio 2025

ÍNDICE

1. Introducción.....	4
1.1 Objeto.....	4
1.2 Alcance.....	4
2. Desarrollo.....	5
2.1 Principios.....	5
2.2 La Gestión de la Configuración.....	6
2.3 La Gestión del Cambio.....	7
2.4 Procedimientos.....	9
2.5 Documentación	10
3. Responsabilidades	12
4. Referencia normativa	13
4.1 Controles de la normativa ISO27001:2022 y ENS	13

ID	NORMA DE CONTROL DE CONFIGURACIÓN Y DEL CAMBIO	CLASIFICACIÓN	VERSIÓN	FECHA
IS_ST_05		FCC_INTERNAL	1.4	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

La presente Norma tiene por objeto la definición de los requisitos necesarios para la gestión y el control de la configuración y del cambio de los componentes que integran los sistemas de información del Grupo FCC.

1.2 Alcance

Esta Norma es de aplicación a los procesos de identificación, control, inventariado y verificación del estado de todos los componentes de los sistemas de información del Grupo FCC durante su diseño, desarrollo y operación.

La Norma es aplicable a todo el personal interno y colaboradores del Grupo FCC, que tenga asignadas responsabilidades en la gestión, control y uso de dichos procesos.

La gestión de la configuración y del cambio se deberá establecer, documentar, mantener y aplicar en todos los sistemas de información de FCC.

ID	NORMA DE CONTROL DE CONFIGURACIÓN Y DEL CAMBIO	CLASIFICACIÓN	VERSIÓN	FECHA
IS_ST_05		FCC_INTERNAL	1.4	Julio 2025

2. Desarrollo

2.1 Principios

- Todos los sistemas de información utilizados por el personal interno y colaboradores del Grupo FCC, independientemente de su propiedad, dispondrán del soporte y material necesario para su adecuado mantenimiento. El grupo FCC garantizará la implementación de los procesos y herramientas necesarias para cumplir con las configuraciones definidas por la presente norma (incluidas las configuraciones de seguridad) para el hardware, software, servicios y redes tanto para los sistemas recién instalados como para los sistemas operativos durante su vida útil. La adquisición e instalación de componentes software, hardware, servicios (como por ejemplo servicios en la nube) y redes que no haya sido previamente aprobada por la División de Sistemas y Tecnologías de Información, adelante DSTI, está prohibida.
- La instalación de cualquier componente en los sistemas de información de FCC deberá ser realizada de acuerdo con las especificaciones de seguridad recomendadas por el fabricante y el departamento de SI.
- La gestión de la configuración y cambios de los sistemas de información de personal interno y colaboradores del Grupo FCC deberá tener en cuenta el Procedimiento de Privacidad desde el diseño y por defecto aprobado por el Grupo.
- La gestión de la configuración y del cambio de los sistemas de información de personal interno y colaboradores del Grupo FCC deberá tener en cuenta una adecuada segregación de tareas y funciones en todas las actividades que contemple. Por este motivo, los roles asociados a la configuración y administración de componentes estarán claramente segregados.
- Los cambios de sistemas de información deberán llevarse a cabo con las medidas de seguridad necesarias, entre las que se incluye la correcta eliminación/bloqueo de datos en cumplimiento de lo establecido en el RGPD.
- La configuración y los cambios serán debidamente verificados y contrastados por personal cualificado del Grupo FCC.
- La gestión de la configuración y del cambio deberá contemplar la disponibilidad de todos los componentes de los sistemas de información del personal interno y colaboradores del Grupo FCC.
- La configuración establecida debe ser apropiadamente documentada y se debe de llevar un registro de los cambios realizados, estos registros serán custodiados de forma segura siguiendo las directrices de la Norma de Seguridad Física.

ID	NORMA DE CONTROL DE CONFIGURACIÓN Y DEL CAMBIO	CLASIFICACIÓN	VERSIÓN	FECHA
IS_ST_05		FCC_INTERNAL	1.4	Julio 2025



Figura 1: Gestión de la Configuración y el cambio

2.2 La Gestión de la Configuración

Una de las medidas de vital importancia para preservar la integridad y disponibilidad de los sistemas de información es establecer unos estrictos procedimientos de gestión de la configuración y del cambio.

Los procedimientos de gestión de la configuración deberán documentar los requisitos de seguridad y la justificación de las excepciones que se puedan dar.

Las medidas de seguridad de los sistemas de información se configurarán de la manera más restrictiva posible y en consonancia con los requisitos funcionales establecidos para cada uno de los sistemas.

2.3 La Gestión del Cambio

- Las modificaciones de seguridad, actualizaciones o parches se aplicarán únicamente cuando se hubiera aprobado su necesidad. Estos cambios procederán de fuentes confiables y serán probados antes de su despliegue en los sistemas de producción.
- Los componentes que forman un sistema de información junto con su versionado deberán de estar documentados.
- En los entornos de no producción no estará permitido el uso de datos de entornos productivos. Su utilización podrá ser aprobada por el departamento de SI siempre y cuando se garanticen que los controles de seguridad implantados proporcionan el nivel de protección adecuado al nivel de clasificación de la información tratada.
- En caso de que no fuese posible garantizar el nivel de seguridad requerido, la realización de las pruebas deberá contar con la aprobación del responsable de la

ID	NORMA DE CONTROL DE CONFIGURACIÓN Y DEL CAMBIO	CLASIFICACIÓN	VERSIÓN	FECHA
IS_ST_05		FCC_INTERNAL	1.4	Julio 2025

información correspondiente y hacer una mención expresa en el registro de aprobación de las causas del incumplimiento.

- Si se hubiese establecido un entorno de pruebas y se descubriese que no es posible garantizar el nivel de seguridad requerido, la información del Grupo FCC deberá ser adecuadamente saneada y establecer los requisitos de seguridad que garanticen que los controles proporcionan el nivel de seguridad adecuado.
- Los procedimientos de prueba de los sistemas de información del Grupo FCC incorporarán un período de funcionamiento en paralelo previo a su paso a producción.
- La sustitución o retirada de los sistemas de información y/o activos que contengan datos o información requerirá de la aceptación formal del responsable de la información y de la posterior aprobación por parte de la DSTI.
- Los sistemas de información y/o activos que contengan datos o información que hubieran sido sustituidos o retirados serán eliminados de acuerdo a los procedimientos de destrucción de soportes.
- Las modificaciones realizadas en los sistemas de información del Grupo FCC seguirán la siguiente secuencia:
 - Cada cambio se iniciará con una petición formal. Esta petición puede ser realizada por el responsable de la información o por la DSTI.
 - Antes de la aprobación de los cambios se evaluará su posible impacto en el resto de los sistemas. Esto podrá llevarse a cabo mediante un análisis basado en los procesos y no solo sobre sistemas concretos.
 - El cambio deberá ser autorizado por el responsable o propietario del Servicio de información de FCC afectado y por la DSTI.
- Las modificaciones y el alcance de los cambios se avisarán con la antelación suficiente al personal implicado para asegurar que conoce las labores que debe realizar.
- En el caso de situaciones de emergencia, las modificaciones se realizarán de acuerdo con los procedimientos operativos establecidos para tal fin, pudiendo cursarse las peticiones de cambio y configuración con posterioridad a la finalización de las actividades.
- La documentación que se realizará sobre los cambios y las instalaciones del software y hardware de sistemas deberá referirse a:
 - La gestión del proceso de cambio o instalación concreta.
 - Las acciones de cambio realizadas.

ID	NORMA DE CONTROL DE CONFIGURACIÓN Y DEL CAMBIO	CLASIFICACIÓN	VERSIÓN	FECHA
IS_ST_05		FCC_INTERNAL	1.4	Julio 2025

- Estas últimas, deberán quedar registradas en un documento, el cual contemplará como mínimo:
 - El origen del cambio.
 - El tipo y alcance de la acción.
 - Las técnicas utilizadas y la secuencia de actividades.
 - Las pruebas y sus resultados.
- Con anterioridad a todo paso al entorno productivo de cualquier cambio o modificación de los sistemas de información, se deberá de:
 - Probar de forma correcta las funcionalidades de negocio y sus capacidades de procesamiento.
 - Realizar copias de seguridad completas de los sistemas de información del Grupo FCC afectados por el cambio.
- Los elementos de los sistemas de información únicamente podrán ser sustituidos por personal autorizado, quien deberá garantizar el saneamiento y eliminación de los riesgos técnicos.
- La planificación de los mantenimientos preventivos para todos los componentes de los sistemas de información deberá tener una periodicidad determinada, pudiendo existir:
 - Mantenimientos mensuales que incluya depuración de bitácoras (logs).
 - Mantenimientos semestrales que incluyan la revisión de su configuración.
 - Mantenimientos anuales que incluyan la limpieza de los equipos.
- Los procedimientos de mantenimiento deberán incluir, como mínimo:
 - Alcance
 - Resultados
 - Tiempo
 - Personal designado para su realización
 - Procedimientos de notificación previa a los usuarios de las tareas de mantenimiento.

2.4 Procedimientos

Los procedimientos de gestión de la configuración y del cambio deberán:

ID	NORMA DE CONTROL DE CONFIGURACIÓN Y DEL CAMBIO	CLASIFICACIÓN	VERSIÓN	FECHA
IS_ST_05		FCC_INTERNAL	1.4	Julio 2025

- Definir:
 - Los responsables de la realización de las tareas de configuración y mantenimiento (segregación de funciones).
 - Los procedimientos de emergencia para la realización de tareas de configuración y mantenimiento.
 - Los procedimientos para el saneamiento de aquellos recursos que deban salir de las instalaciones del Grupo FCC por operaciones de configuración y mantenimiento.
 - Los procedimientos que aseguren que cualquier fallo en los sistemas de información sea notificado y registrado en tiempo y forma oportunos.
 - Los procedimientos que verifiquen que, tras las modificaciones a los sistemas de información, se garantiza que las características de seguridad previas a los cambios continúan funcionando adecuadamente.
 - Los procedimientos que aseguren la realización de las actividades de auditoría asociadas con los cambios en la configuración de los sistemas de información.
 - Los procedimientos que garanticen que todo el personal interno y colaboradores del grupo FCC reciben la formación necesaria para el desempeño de sus funciones sobre las funcionalidades y operaciones de los nuevos componentes.
 - Los controles para asegurar que las operaciones de configuración y mantenimiento que se realizan por empresas ajenas a FCC están en conformidad con las Marco Normativo de Seguridad de la Información del Grupo FCC y en particular con la Norma de Seguridad de Empresas Externas.
 - El alcance y nivel de monitoreo de los cambios se determinará en base a los requisitos que establezca la Política de Gestión de la Información, adicionalmente, se establecerán unas líneas base de comportamiento normal y monitorizará cualquier comportamiento anómalo.
- Identificar:
 - Los recursos profesionales y materiales necesarios para el mantenimiento en las instalaciones del Grupo FCC y fuera de las mismas.

2.5 Documentación

La documentación relativa a la gestión de la configuración y del cambio deberá contener, como mínimo:

ID	NORMA DE CONTROL DE CONFIGURACIÓN Y DEL CAMBIO	CLASIFICACIÓN	VERSIÓN	FECHA
IS_ST_05		FCC_INTERNAL	1.4	Julio 2025

- El control de versiones, que asocia los componentes del sistema con la versión apropiada. Incluyendo los cambios realizados en cada versión.
- El análisis del impacto de los cambios propuestos sobre los controles de seguridad existentes.
- Los procedimientos para:
 - Evaluar y/o aprobar los componentes de los sistemas de información antes de su paso a producción.
 - Asegurar la revisión de las funciones, controles y servicios que puedan ser potencialmente eliminados con los cambios efectuados.
 - Asegurar que los planes de contingencia y la documentación asociada se actualizan para reflejar los cambios.
 - Manejar y solucionar las posibles emergencias o el retorno a un escenario previo cuando un proceso de configuración o cambio de versión tuviese que ser cancelado.
- Los requisitos para que todas las instalaciones y modificaciones de hardware, software o firmware se realicen en conformidad con la normativa vigente en materia de propiedad intelectual e industrial.
- Los tiempos estimados de vida útil de los elementos para programar su renovación con la suficiente antelación.
- Los registros de errores derivados de la operativa de gestión deberán contener, como mínimo:
 - Nombre y versión de los sistemas involucrados.
 - Fecha y hora de la incidencia.
 - Descripción del error y de los elementos del sistema involucrados.
 - Nombre de la persona responsable de solucionar el problema.
 - Acciones correctivas realizadas.
 - Fecha y hora de la resolución de la incidencia.

3. Responsabilidades

El departamento de SI deberá:

- Definir las necesidades para un correcto control en la configuración de los sistemas de información

ID	NORMA DE CONTROL DE CONFIGURACIÓN Y DEL CAMBIO	CLASIFICACIÓN	VERSIÓN	FECHA
IS_ST_05		FCC_INTERNAL	1.4	Julio 2025

- Verificar los registros de auditoría de errores, usos no autorizados y actividad de los sistemas de información del Grupo FCC.
- Verificar la idoneidad de la documentación relacionada con los cambios de hardware, software y firmware.

La DSTI deberá:

- Aprobar los componentes, su instalación, mantenimiento y retirada.
- Realizar un análisis de impacto de los cambios en los componentes de los sistemas de información.
- Elaborar los procedimientos relativos a la instalación y control de cambios, de emergencia y vuelta atrás.
- Gestionar:
 - Los requisitos técnicos, controles y planes de prueba.
 - Las solicitudes de cambio
 - La coordinación de la implantación de los cambios aprobados.
- Monitorizar los sistemas de información de FCC para asegurar el cumplimiento de la presente Norma.
- Asegurar que los equipos de trabajo cuentan con la formación necesaria para llevar a cabo funciones de gestión de la configuración y del cambio.
- Investigar, en colaboración con el departamento de SI, los incidentes o posibles incidentes de seguridad en los sistemas de información del Grupo FCC derivados de la gestión de la configuración y el cambio, evaluando el impacto y las posibles causas.

Los Responsables de la Información deberán aprobar:

- Los cambios en la configuración de los sistemas información.
- La realización de pruebas en el caso de que no se pueda asegurar el nivel de seguridad requerido.

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	NORMA DE CONTROL DE CONFIGURACIÓN Y DEL CAMBIO	CLASIFICACIÓN	VERSIÓN	FECHA
IS_ST_05		FCC_INTERNAL	1.4	Julio 2025

ID Control ISO	Control ISO/IEC 27001:2022	Correspondencia ENS
5.15	Control de acceso	[op.acc.2] Requisitos de Acceso
5.28	Recopilación de evidencias	[op.exp.7] Gestión de Incidentes; [op.exp.9] Registro de la Gestión de Incidentes
8.9	Gestión de la configuración	[op.exp.2] Configuración de Seguridad; [op.exp.3] Gestión de la Configuración
8.16	Seguimiento de actividades	[op.mon.3] Vigilancia; [mp.s.4] Protección frente a DoS
8.32	Gestión de cambios	[op.exp.5] Gestión de Cambios