Norma de

Empresas Externas

del Grupo FCC

Julio de 2025

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

ÍNDICE

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 proteger la confidencialidad, integridad, autenticidad, trazabilidad, disponibilidad y auditabilidad de la información de FCC cuando es tratada por empresas externas y colaboradores de Grupo (en adelante, Empresas Externas y colaboradores) durante la duración de su relación contractual.

1.2 Alcance

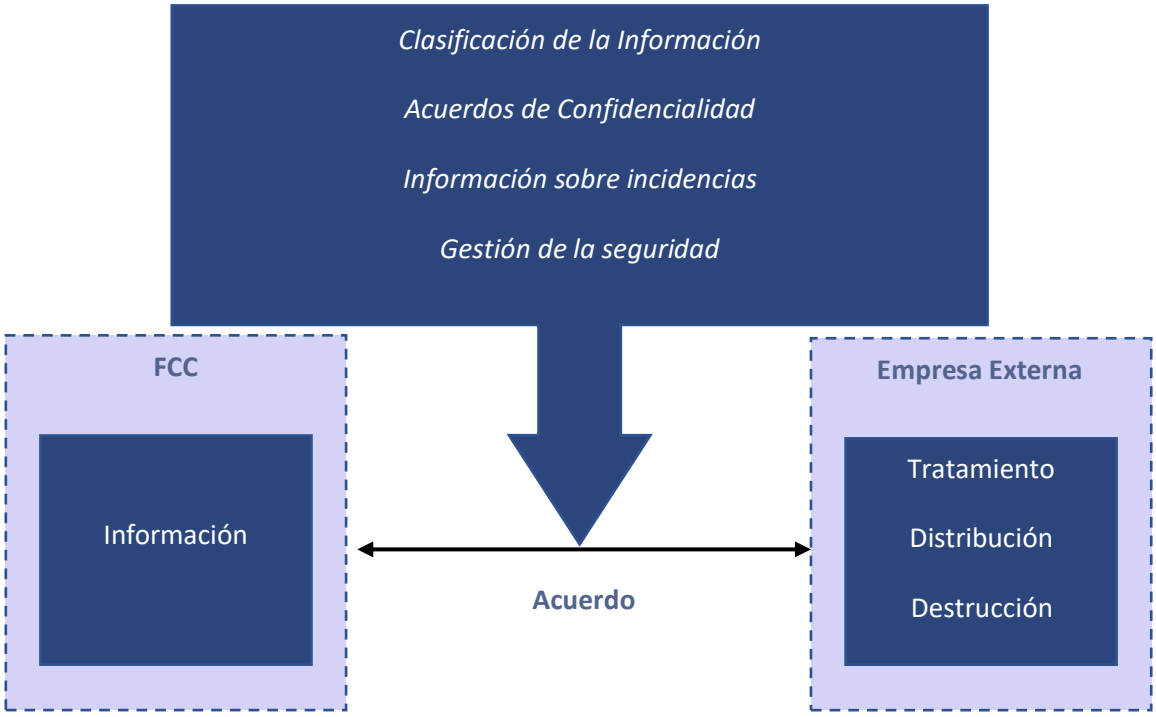
Esta Norma es de aplicación a toda la Información del grupo FCC tratada por Empresas Externas y colaboradores que tuvieran la necesidad de acceder a ella como consecuencia de su participación en programas, proyectos o acuerdos con el Grupo FCC.

2. Desarrollo

2.1 Principios

- El acceso a información del Grupo FCC por personal perteneciente a Empresas Externas vendrá autorizado por su necesidad de conocerla.
- El acceso a información del Grupo FCC por personal perteneciente a Empresas Externas que requieran acceso a determinada información clasificada como Secreto o Confidencial será preciso, además, disponer de una Habilitación Personal de Seguridad.

- Las Empresas Externas deberán aplicar a la información de FCC las medidas de protección determinadas por FCC, en atención al nivel de confidencialidad de la misma.
- Requerirá de autorización expresa de FCC:
    - La distribución de Información Restringida a terceros por parte de Empresas Externas.
    - La desclasificación o reclasificación de la información de FCC tratada por Empresas Externas.
    - La reutilización de herramientas desarrolladas por los colaboradores durante sus servicios al grupo.
- Las Empresas Externas no podrán destinar la información de FCC a un fin diferente al establecido en el acuerdo que rija la colaboración.
- El tratamiento de información de FCC deberá respetar la legislación vigente en materia de privacidad y protección de datos.
- Los programas, proyectos o acuerdos que impliquen el tratamiento de información restringida, no entrarán en vigor hasta que no cumplan con los principios establecidos en la presente Norma.
- La subcontratación por parte de Empresas Externas de un servicio o parte de él queda prohibida, salvo que FCC lo autorice de forma expresa, de acuerdo con los siguientes criterios:
    - El contenido de los servicios a subcontratar y la identificación de la empresa subcontratada deberán estar recogidos en la oferta o contrato que se firme entre FCC y la Empresa Externa.
    - El tratamiento de la Información de FCC por parte del subcontratista se deberá ajustar a lo dispuesto en la presente Norma.



2.2 Instrucciones Específicas De Seguridad

El Responsable de la Contratación, junto con la Dirección de Seguridad de la Información y Gestión de Riesgos, determinará la necesidad de establecer un documento específico sobre las instrucciones de seguridad de cada proyecto, programa o acuerdo.

Los acuerdos con Empresas Externas, donde se trate información de FCC, deberán contemplar como mínimo:

- Los métodos y procedimientos de gestión, clasificación, tratamiento y salvaguarda de la información.
- Las medidas de seguridad derivadas de la aplicación de la legislación vigente.
- Las obligaciones de seguridad aplicables en la subcontratación de tareas en favor de terceras empresas.
- La obligación de que las Empresas Externas faciliten, a requerimiento de FCC, información sobre el personal que accede a la Información de FCC.
- El compromiso por parte de las Empresas Externas de informar en tiempo y forma de las incidencias o incidentes de seguridad que se puedan producir.
- La obligación, por parte de las Empresas Externas, de destruir o devolver a FCC toda su información una vez concluya la colaboración. En caso de destrucción, las Empresas Externas deberán presentar un certificado que acredite la completa destrucción irreversible de la información.

2.3 Servicios Gestionados De Tecnologías De La Información

Los procesos de tecnologías de la información que vayan a ser gestionados por Empresas Externas deberán estipular expresamente en el contrato, la necesidad de que FCC conozca y apruebe:

- Los procedimientos operativos de seguridad que lleve aparejada la prestación de los servicios gestionados.
- Las medidas de seguridad adoptadas en las instalaciones donde se preste el servicio.
- Las medidas de seguridad establecidas para las comunicaciones entre centros si hubiese conexiones con instalaciones externas al Grupo.
- Las métricas e indicadores de seguridad que permitan evaluar los niveles de confidencialidad, integridad, disponibilidad, autenticidad, trazabilidad y auditabilidad ofrecidos por los servicios.
- La posibilidad de realizar auditorías de seguridad en los sistemas desde donde se realice el servicio gestionado.

2.4 Uniones Temporales De Empresas

Las Uniones Temporales de Empresas, Agrupaciones de Interés Económico y otros tipos de sociedades que se gestionen conjuntamente con terceros ajenos al Grupo, estarán afectadas por los principios de actuación y las responsabilidades que indica la presente Norma.

2.5 Acuerdos De Confidencialidad

Las Empresas Externas que traten Información de FCC estarán obligadas a guardar secreto sobre la misma, comprometiéndose a no divulgarla, publicarla, o ponerla a disposición de terceros no autorizados. Estas obligaciones subsistirán aun después de finalizar sus relaciones con FCC por un periodo de cinco años, como se indica en el anexo de esta Norma.

Se suscribirán los contratos de confidencialidad que figuran en los anexos de la presente Norma.

2.6 Distribución De La Información

La distribución de la Información de FCC se realizará de acuerdo con los criterios establecidos en la presente Norma.

La protección de la información deberá contemplar que su soporte, transporte y almacenamiento se corresponden con el nivel de clasificación de la información distribuida.

Los registros deberán garantizar la trazabilidad de las acciones realizadas durante la distribución de la información.

2.7 Destrucción De La Información

La destrucción de la Información de FCC que esté en poder de Empresas Externas deberá tener en cuenta las siguientes consideraciones:

- La necesidad de que el proceso de destrucción se realice asegurando la confidencialidad de la manipulación y la imposibilidad de que la información sea recuperada o reconstruida.
- La certificación de que la destrucción ha sido realizada siguiendo los criterios establecidos por FCC.

2.8 Trabajo en modalidad no presencial de colaboradores prestadores de servicios

El presente apartado tiene como objetivo establecer unas instrucciones de obligado cumplimiento por parte de los colaboradores prestadores de servicios cuando desempeñen su trabajo en modalidad no presencial.

Se deberá asegurar en todo momento la disponibilidad, confidencialidad, integridad y auditabilidad de toda la información del Grupo FCC que trate un colaborador. Para ello:

- Se deberá asegurar que el lugar desde donde se realice el trabajo no presencial debe contar con unas condiciones óptimas y mínimas de seguridad tanto físicas como lógicas.
- Se contará con garantías suficientes para realización de copias de backup y continuidad de las actividades del servicio prestado
- Se deberá almacenar la información únicamente en recursos corporativos y siempre aplicando las medidas de seguridad propias a su nivel de clasificación.

- La empresa colaboradora deberá proporcionar dispositivos adecuados con unas medidas de seguridad apropiadas para realizar de forma segura el teletrabajo. En el caso de disponer de un dispositivo personal se deberá cumplir con los requisitos de seguridad del Grupo FCC.
- Los accesos remotos se basarán en el principio de mínimo privilegio y el principio de necesidad de conocer, de forma que sólo se pueda acceder a lo mínimo indispensable para garantizar el desempeño de las funciones que necesita realizar la persona que accede.
- Se deberá acceder a los recursos del Grupo FCC únicamente desde conexiones seguras proporcionadas o autorizadas por el Grupo.
- Se deberá establecer y comunicar las condiciones del trabajo no presencial (horario, lugar de trabajo, nivel de clasificación de la información, etc.).
- Se ostentará el derecho de monitorización y supervisión sobre los dispositivos remotos para asegurar la correcta continuidad de las actividades en cumplimiento con el Marco Normativo de Seguridad de la Información del Grupo FCC.
- Una vez finalizado el trabajo del colaborador en modalidad no presencial, se deberá anular la autorización a los recursos del Grupo FCC, los derechos de acceso y se deberá destruir la información vinculada al servicio prestado.

3. Responsabilidades

El Responsable de la contratación tendrá como funciones:

  - Incluir el ”Anexo – Requisitos de Seguridad de la Información” en los acuerdos que subscriba con empresas externas.

- Revisar periódicamente el cumplimiento de los requisitos de seguridad incluidos en el contrato.
- Establecer el procedimiento de evaluación correspondiente para la evaluación del nivel de madurez en seguridad de los proveedores en base a la naturaleza del servicio.
- Asegurarse de que dichas empresas y sus instalaciones estén capacitadas para proteger la Información de FCC.
- Garantizar que se cumplen las medidas de seguridad cuando se desempeñe el trabajo en modalidad no presencial.

- La gestión y registro de las Habilitaciones Personales de Seguridad que sean necesarias para la realización del programa, proyecto o acuerdo en el que participe el personal de Empresas Externas.
- Informar inmediatamente a las Empresas Externas sobre cualquier cambio que se produzca en los niveles de seguridad de la información puesta a su disposición.
- Informar a la Dirección de Seguridad de la Información y Gestión de Riesgos Tecnológicos de FCC de las posibles pérdidas, totales o parciales, o revelaciones de la información puesta a disposición de Empresas Externas.

El Responsable de la Información tendrá como funciones:

- Autorizar la distribución de la información a personal de las Empresas Externas, así como al de las que éstas subcontraten
- Autorizar la desclasificación o reclasificación de la información del Grupo FCC que esté en poder de Empresas Externas.
- Conocer los controles de seguridad implantados para la información del Grupo FCC tratada por Empresas Externas.

Las Empresas Externas que tratan Información del Grupo FCC deberán:

- Garantizar la protección de la información del Grupo FCC que traten.
- Notificar al Responsable de la Contratación las incidencias e/o incidentes que afecten a la confidencialidad, integridad, disponibilidad y auditabilidad de la misma.
- Trasladar el conocimiento a aquellos terceros con los que subcontrate el tratamiento de Información del Grupo FCC de las medidas establecidas en la presente Norma.
- Garantizar los requisitos de terminación segura de la relación contractual con FCC, incluyendo:
    - Desaprovisionamiento de los derechos de acceso a la información del grupo FCC.
    - Manejo de la información.
    - Determinación de los derechos de propiedad intelectual desarrollado durante el servicio.
    - Portabilidad de la información en caso de cambio de proveedor.
    - Gestión de registros.
    - Devolución de activos.
    - Eliminación segura de información y otros activos.

- Requisitos continuos de confidencialidad.

La Dirección de Seguridad de la Información y Gestión de Riesgos Tecnológicos deberá:

- Investigar cualquier indicio de pérdida o revelación no autorizada de la Información del Grupo FCC tratada por Empresas Externas.
- Definir y aprobar los medios de distribución y destrucción que aseguren un nivel mínimo de protección de la información de FCC tratada por Empresas Externas.
- Verificar las instalaciones y los procedimientos de seguridad aplicados por las Empresas Externas en el tratamiento de información de FCC.
- Supervisar que se cumplen los acuerdos, en materia de seguridad, cuando se desempeñe el trabajo en modalidad no presencial.

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
5.15	Control de acceso	[op.acc.2] Requisitos de acceso
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
5.19	Seguridad de la información en las relaciones con los proveedores	[op.ext.1] Contratación y acuerdos de nivel de servicio
5.20	Abordar la seguridad de la información en los acuerdos con proveedores	[op.ext.1] Contratación y acuerdos de nivel de servicio
5.22	Seguimiento, revisión y gestión de cambios de servicios en proveedores	[op.ext.2] Gestión diaria
6.7	Trabajo a distancia	[org.2] Normativa de Seguridad; [mp.per.2] Deberes y Obligaciones