Norma de Seguridad en Documentos 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 del formato con el resto de la Normativa.	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)
3.0	Julio 2025	IS	Revisión del documento y adaptación a la normativa ENS nivel medio	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 establecer las medidas de protección aplicables a los documentos que contengan información del Grupo FCC con el fin de asegurar la confidencialidad, integridad, disponibilidad, autenticidad, trazabilidad y auditabilidad de dicha información a lo largo del ciclo de vida de estos.

1.2 Alcance

Esta Norma se aplica a todos aquellos documentos que contengan información de del grupo, independientemente del lugar donde se sitúen, su localización y soporte.

En adelante, con la expresión “documento”, se hace referencia a aquéllos que contengan información cuya propiedad sea del Grupo FCC.

2. Desarrollo.

2.1 Principios

- Los documentos deberán protegerse desde una perspectiva integral, contemplando todas las etapas que se suceden a lo largo de su ciclo de vida y con independencia del formato, del soporte o de los medios que se utilicen.
- Las medidas de protección organizativas y técnicas que se aplicarán a los documentos, serán proporcionables al nivel de riesgo de la información que contienen y al nivel de clasificación de esta, de acuerdo con lo indicado en la Política de Gestión de la Información del Grupo FCC.
- Todo documento deberá ser accesible, únicamente, por personas que tengan necesidad de conocer la información contenida en los mismos. Si la información es Restringida, deberá ser necesario disponer de una Habilitación Personal de Seguridad.
- Todo documento que contenga información Restringida, en concreto, Confidencial y Secreta, deberá estar cifrado en cualquiera de los estados en los que se encuentre, ya sea en reposo y/o en tránsito, siguiendo las medidas indicadas en la Norma de Criptografía.

- El tratamiento de los documentos por parte de colaboradores deberá ser realizado en conformidad con la Norma de Empresas Externas al Grupo.
- En aquellos documentos que contengan información con diferentes niveles de clasificación, se aplicarán las medidas específicas de cada nivel. En caso de que esto no sea posible, deberán aplicarse las medidas de seguridad asociadas al nivel de clasificación más restrictivo.

2.2 Etiquetado

- Todos los documentos que contengan Información de FCC, con independencia de su formato y medio de soporte, deberán identificar el nivel de clasificación asignado a la información que contienen mediante la incorporación, de forma clara y visible, de una de las siguientes etiquetas excluyentes entre sí:
  - **FCC_SECRET**
  - **FCC_CONFIDENTIAL**
  - **FCC_INTERNAL**
  - **FCC_PUBLIC**
- Los documentos etiquetados como **"FCC_SECRET"** deberán incorporar una portada que claramente indique este nivel de clasificación y la lista de distribución autorizada, de forma que se impida, sin abrirlo, ver el contenido del documento.
- Los documentos no etiquetados con el nivel de clasificación de la Información que contienen serán considerados de Uso Interno, a excepción de aquellos que estuvieran archivados con anterioridad a la entrada en vigor de la presente Norma. En este caso, se procederá a su clasificación cuando se desarchive.

2.3 Almacenamiento

- Únicamente podrán ser almacenados aquellos documentos que contengan información necesaria para el cumplimiento de los objetivos de negocio del Grupo FCC.
- No se podrán almacenar documentos que contravengan la legislación vigente, el orden público, la moral y las buenas costumbres.
- La información deberá almacenarse en soportes o dispositivos que aseguren su tratamiento dentro del entorno tecnológico empleado por el Grupo FCC. Evitando así, que cualquier obsolescencia tecnológica del soporte o cualquier filtración de su contenido, pueda crear una indisponibilidad de la información.
- Cuando el almacenamiento de la información se realice de forma externalizada se deberán fijar en el acuerdo suscrito entre el Grupo FCC y el proveedor los puntos referentes a las medidas de seguridad a aplicar por el proveedor, el régimen de responsabilidades y los criterios recogidos en la Norma de Seguridad en Empresas Externas del Grupo FCC.
- El acceso a los datos se basará en el principio del mínimo privilegio y siguiendo las medidas descritas en la Norma de Control de accesos.
- El responsable de los documentos que contenga Información Restringida deberá mantener una relación actualizada de personas con acceso autorizado al mismoToda

información restringida deberá ser custodiada, almacenada y conservada del resto de la información.

- La información restringida deberá estar custodiada en lugares con medidas de seguridad adecuadas, quedando descartados armarios y/o habitaciones no protegidas por llave o carpetas de red públicas compartidas para soportes digitales.
- La información restringida no deberá ser expuesta o abandonada, deberá estar siempre bajo custodia de una persona con acceso autorizada o destruida adecuadamente en caso de que ya no sea necesaria. En caso de que cualquier información se extravié se deberá informar al Responsable de la Información.
- La información restringida disponible en un soporte digital deberá ser cifrada siempre que sea posible.
-

2.4 Distribución

- Los documentos que contengan Información No Restringida, podrán ser distribuidos a todas aquellas personas que tuvieran necesidad de conocer, sin requerir la previa autorización de su responsable.
- En consonancia con la Norma de Empresas Externas del Grupo FCC, cuando la gestión de documentos fuera externalizada, los acuerdos que regulen dicha prestación de servicios deberán incluir un compromiso de confidencialidad y no revelación extensiva a todo el personal dependiente del proveedor externo que interviniera en la prestación del servicio.
- En la distribución de documentos a cualquier tercero ajeno al Grupo, se deberá incluir en los acuerdos, la obligación del receptor de implantar las medidas de seguridad que el Grupo FCC estime oportunas atendiendo a los niveles de clasificación de la información contenida en dichos documentos.
- La distribución de documentos se realizará a través de medios que aseguren:
    - La recepción inequívoca por el destinatario o personal autorizado por éste.
    - La confidencialidad, integridad autenticidad y trazabilidad de la información.
- Todo documento restringido que se distribuya por un canal digital deberá usar métodos de cifrado. Para dicho tipo de distribución se evitará siempre que sea posible el uso de correo electrónico.
- Evitar el uso de impresoras, empleando solo aquellas específicas y pertenecientes al Grupo FCC recogiendo los documentos tras su impresión
- La información Restringida que estuviera registrada en documentos debidamente etiquetados deberá distribuirse en soportes que no contengan etiquetas que hagan referencia expresa al nivel de clasificación de la información contenida.
- Se empleará correo certificado con acuse de recibo y con entrega en mano siempre que se distribuya información restringida mediante un soporte físico. Para dicho proceso se deberá emplear un sobre opaco y el acuso de recibo deberá ser recibido y archivado.
- Se deberá eliminar toda información adicional contenida en campos ocultos, metadatos, comentarios, revisiones anteriores, etc. Se exceptuarán aquellos casos en los que dicha información sea pertinente para el receptor del documento.

2.5 Destrucción

- Para la destrucción de los documentos se emplearán medios que aseguren que la información quede irreconocible e irrecuperable, manteniendo durante todas las acciones la confidencialidad de la información contenida en los mismos.
- En el caso de externalizar en proveedores especializados la destrucción de los documentos, se deberá incluir en los acuerdos que se suscriban un compromiso de confidencialidad y no revelación extensiva a todo el personal dependiente del colaborador que, de forma directa o indirecta, interviniera en la prestación, con independencia de los requisitos adicionales que imponga la legislación vigente en función de la naturaleza de la información que contuvieran.
- Cuando la destrucción de la información esté externalizada, el acuerdo realizado entre ambas empresas deberá exigir a la empresa prestadora del servicio un certificado de garantía de destrucción de los documentos, en el que acredite la completa eliminación de la información contenida en los mismos.
- Para cada uno de los niveles de clasificación de la información deberán desarrollarse procedimientos que detallen los criterios seguros de destrucción de esta.
- El transporte hasta el lugar donde vaya a llevarse a cabo la destrucción de los documentos deberá realizarse de forma que asegure que durante el traslado no se producen sustracciones, pérdidas o filtraciones de dicha información.
- Cuando se trate de documentos electrónicos que contengan datos de carácter personal, la distribución se realizará cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que dicha información no sea inteligible ni manipulada durante su transporte.
- En ningún caso se podrá autorizar la eliminación ni se podrá proceder a la destrucción de documentos, en tanto subsista su valor probatorio de derechos y obligaciones de las personas físicas o jurídicas, o que no hayan transcurrido los plazos que la legislación vigente establezca para su conservación.

3. Responsabilidades

El departamento de SI deberá:

- Desarrollar los criterios de seguridad para el etiquetado de los documentos.
- Aprobar y/o definir los medios de distribución y de destrucción de los documentos.
- Verificar los procedimientos de seguridad de los documentos.
- Asegurar la existencia de medidas de seguridad adecuadas al nivel de clasificación de la información y del tipo de soporte utilizado.
- Garantizar la existencia de recursos informativos acerca de los niveles de etiquetado y seguridad de documentos.

La División de Sistemas y Tecnologías de la Información deberá:

- Asegurar que la información almacenada en documentos electrónicos está disponible para su utilización en los medios de tratamiento vigentes en cada momento.

Los responsables de la Información deberán, para sus sistemas:

- Verificar los procedimientos de identificación y autenticación de acceso.
- Conocer los controles implantados para la seguridad de los documentos.

Los usuarios deberán:

- Informar, de la forma más detallada posible, de las incidencias encontradas en materia de documentos de información.

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.

4.1 Controles de la normativa ISO27001:2022 y ENS

ID Control ISO	Control ISO/IEC 27001:2022	Correspondencia ENS
5.9	Inventario de información y otros activos asociados	[op.exp.1] Inventario de activos; [op.pl.2] Arquitectura de Seguridad
5.10	Uso aceptable de la información y otros activos asociados	[org.2] Normativa de Seguridad; [org.3] Procedimientos de Seguridad; [mp.si.3] Custodia
5.11	Devolución de activos	[org.2] Normativa 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
7.10	Soportes de almacenamiento	[mp.si.1] Marcado de soportes; [mp.si.2] Criptografía; [mp.si.3] Custodia; [mp.si.4] Transporte; [mp.si.5] Borrado y destrucción
8.10	Eliminación de la información	[mp.si.5] Borrado y destrucción

Anexo I Acciones recomendadas por clasificación de la información

	Información general	PÚBLICO	INTERNO	CONFIDENCIAL	SECRETO
1.	**CREACIÓN**				
1.1	Marcado/etiquetado de la información				
1.1.1	Historial de cambios Nombre del documento Resumen de cambios Fecha de los cambios	X	X	X	X
1.1.2	Tabla de auditorías Autor (Departamento + Fecha de elaboración) Responsable de la aprobación (Comité + Fecha de elaboración)		X	X	X
1.1.3	Clasificación y estado del documento	X	X	X	X
1.1.4	Responsable / Administrador del documento	X	X	X	X
1.1.5	Control de distribución		X	X	X
2	**ALMACENAMIENTO**				
2.1	Control de accesos				
2.1.1	Lectura: sin restricciones	X			
2.12	Lectura: usuarios internos y terceras partes		X		
2.1.3	Lectura: usuarios internos y terceras partes autorizadas			X	X
2.1.4	Escritura: usuarios autorizados	X	X	X	X
2.1.5	Acceso: todo el público	X			
2.1.6	Acceso: ID de usuario + contraseña		X	X	
2.1.7	Acceso: ID de usuario + contraseña + posibilidad de requerir un MFA				X
2.1.8	Auditoría de control de acceso			X	X
2.2	Almacenamiento				
2.2.1	Cifrado			X	X
2.2.2	Copias de seguridad	X	X	X	X
3	**DISTRIBUCIÓN**				
3.1	Transmisión por redes internas				
3.1.1	Intranet (todo el personal)	X	X		
3.1.2	Intranet (con restricciones de acceso)			X	
3.1.3	Correo corporativo sin protección	X	X		
3.1.4	Correo corporativo con protección de contraseña			X	
3.1.5	Autorización explicita del propietario para su transmisión				X
3.1.6	Cifrado de documento obligatorio			X	X
3.1.7	Cifrado del documento si es necesario		X		
3.1.8	Aviso de confidencialidad en la firma del correo			X	X

Anexo II Guía de buenas prácticas para el uso de soportes de información

Siempre que sea práctico y necesario se deberá solicitar autorización para la retirada o eliminación de los soportes del Grupo y se deberá mantener un registro de entrada y salida.

Los soportes del Grupo deberán estar siempre almacenados en un entorno seguro, siguiendo los requisitos especificados por el fabricante. Dicho almacenamiento tendrá que ser acorde a la clasificación de la información que contenga.

Se deberán usar técnicas criptográficas siempre que la integridad, la confidencialidad, ó la autenticidad de la información contenida en el soporte de almacenamiento sea considerada como importante.

El Grupo mantendrá los puertos destinados a medios de almacenamiento extraíbles bloqueados siempre y cuando no exista una razón organizativa para su uso. En caso de que exista dicha razón, la transferencia de la información a dichos medios de almacenamiento deberá ser controlada.

Para evitar el acceso no autorizado se evitará el uso del servicio postal o mensajería para el envio de medios de almacenamiento.

-