Norma de Gestión de Copias de Respaldo 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)
	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 ISO27001:2022	Chief Information Security Officer (CISO)
2.0	Julio 2025	IS	Revisión del documento y adaptación a 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

El objeto de la presente Norma es establecer los requisitos de conservación y protección necesarios para asegurar la integridad, confidencialidad, disponibilidad, autenticidad y trazabilidad de la información, el software y los sistemas del Grupo FCC durante todo el ciclo de vida de las copias de respaldo.

1.2 Alcance

Esta Norma es de aplicación sobre los dispositivos de almacenamiento utilizados por los sistemas de información gestionados por el Grupo FCC. En concreto:

- Discos fijos u otros dispositivos de almacenamiento no volátiles, cuya forma de operar sea aislada o con conexión a la red.
- Otros soportes electrónicos extraíbles.

Se entiende por gestión de copias de respaldo las actividades de:

- Realización de copias de seguridad.
- Pruebas de recuperación e integridad de la información.
- Mantenimiento y almacenamiento de los dispositivos.
- Borrado de la información de las copias de respaldo.

La correcta realización de estas acciones asegurará el proceso de resguardo y recuperación efectiva de la información.

Durante toda la exposición de esta Norma, se usarán indistintamente los términos de copia de seguridad y copia de respaldo.

2. Desarrollo

2.1 Principios

Las copias de respaldo que se realizarán de los sistemas de la información del Grupo FCC se regirán por los siguientes principios:

- serán documentadas y planificadas en base a:
  - la criticidad de los procesos de información;
  - los tiempos objetivo de recuperación y restauración;
  - el tiempo de resguardo de los registros considerado en las disposiciones legales vigentes;
- serán planificadas contemplando:
  - las medidas específicas para asegurar que la información pueda ser recuperada en caso de incidente o contingencia;
  - el cumplimiento de los requisitos definidos en esta Norma, así como en las relacionadas;
- estarán sometidas, durante todo su ciclo de vida, a medidas de protección organizativas y técnicas proporcionales:
  - al nivel del riesgo de la información que contienen;
  - al nivel de clasificación de la misma. En este sentido, los medios de almacenamiento de las copias de respaldo deberán etiquetarse y protegerse con el máximo nivel de clasificación de la información que almacenen;
- estarán almacenadas en dispositivos que:
  - aseguren la disponibilidad de la información durante el tiempo en que esta vaya a ser conservada;
  - cumplan, en el caso de que se tengan que migrar datos de un soporte de almacenamiento a otro, con los procedimientos operativos de seguridad definidos para este tipo de acciones, garantizando el soporte destino, al menos, la misma seguridad que el soporte donde se encuentre inicialmente la información;
- estarán protegidas, cifradas, etiquetadas y transportadas cumpliendo con los requisitos establecidos en la Política de Gestión de la Información y conforme con la legislación vigente.

Si el Grupo FCC utilizase un servicio externo al Grupo para la gestión de las copias, éste deberá también contratarse en conformidad con lo establecido en la Norma de Seguridad de Empresas Externas.

Figura 1: *Principios de Gestión de Copias de respaldo*

2.2 Copias de Respaldo

Las copias de respaldo de los sistemas de información se deberán realizar asegurando la recuperación total del sistema ante cualquier eventualidad, salvaguardando en cada una de las fases del ciclo de vida, la confidencialidad e integridad de la información tratada.

Las copias de respaldo serán efectuadas por personal autorizado y formado para el correcto desempeño de tales acciones.

La periodicidad en la realización de las copias de seguridad podrá estar definida en los acuerdos de nivel de servicio, los procedimientos o las guías de uso de los sistemas de información gestionados por el Grupo FCC, en cualquier caso, esta periodicidad deberá ser siempre igual o inferior a una semana.

Los procedimientos de realización de copias de seguridad se automatizarán, en aquellos sistemas donde técnicamente sea posible, de forma que se faciliten las tareas operacionales y la prevención de errores.

En el proceso de generación de dichas copias, así como cualquier acción sobre ellas, se deberán generar registros de auditoria precisos y completos, sobre quién ha realizado la operación y en qué momento se ha hecho, el motivo y el contenido de la copia. Las copias deberán estar referenciadas por un código o número de secuencia.

2.3 Pruebas de Copias de Respaldo.

Las copias de seguridad y los procedimientos de recuperación se probarán al menos una vez al año, asegurando:

- Que son capaces de recuperar correctamente la información en caso de necesidad o emergencia.
- Que dicha restauración se ajusta al tiempo de restauración objetivo.
- Que las pruebas de recuperación se realizan en un entorno de testeo sin que haya posibilidad de sobrescribir el sistema de almacenamiento original y evitar pérdidas de datos irreparables.
- Que se puede detectar posibles fallos durante el proceso de realización de las copias.

2.4 Recuperación de la Información

La recuperación de la información a partir de las copias de seguridad deberá:

- Ser autorizada por el responsable de la información o la persona/as en las que delegue tal acción.
- Realizarse, en base a un procedimiento formal, por personal cualificado y autorizado para la ejecución de tales tareas.
- Documentarse en un registro donde se detalle la información de identificación de la operación, del soporte y de la información recuperada, así como los resultados y los hechos relevantes que se hayan podido producir.

2.5 Conservación de las Copias de Respaldo

Los soportes de información que contienen las copias de seguridad se deberán almacenar en un medio adecuado y a una distancia capaz de protegerse de cualquier daño procedente de una contingencia ocurrida en el emplazamiento donde se encuentran los sistemas de información principal.

Se deberá mantener un registro de entrada y salida de las copias de seguridad formalmente documentado.

Las copias de seguridad que guarden Información No Restringida (Uso Público) deberán permanecer almacenadas, al menos, un mínimo de un año manteniendo unos controles de seguridad que impidan el robo y el deterioro de los soportes.

Las copias de seguridad que guarden Información Restringida (Uso Interno, Confidencial y Secreta), deberán permanecer almacenadas, al menos, un mínimo de dos años, estando accesibles únicamente por personal correctamente autorizado. Los soportes que contengan este tipo de información deberán estar salvaguardados de cualquier amenaza física y ambiental en armarios ignífugos con llave u otra ubicación donde se utilicen controles de acceso físico o lógico que aseguren la confidencialidad y la integridad de la misma.

Los periodos de conservación cumplirán con los que exija la legislación vigente o con las necesidades determinadas por el responsable de la información.

2.6 Copias de respaldo en nube

- Las copias de seguridad en la nube deberán:
  - Configurarse siguiendo las recomendaciones de proveedor de servicios cloud adquiridos por el grupo FCC.
  - Poder ser monitorizadas y auditables para identificar cualquier tipo de actividad sospechosa.

Se recomienda redundancia en las copias de respaldo, si existen varias copias de respaldo en la nube, es recomendable tener alguna copia local en caso de que se produzcan errores o problemas en la nube.

2.7 Borrado de la Información

El borrado de las copias de seguridad deberá:

- realizarse mediante mecanismos corporativos adecuados a la clasificación de la información y el riesgo aparejado a su revelación;
- dar como resultado una acción irreversible sobre la recuperación de la información.

En el caso de que el soporte no permita el borrado de su información, se deberá asegurar la destrucción física del mismo.

3. Responsabilidades

El departamento de SI deberá:

- Verificar la adecuada implantación de la presente Norma.
- Verificar, en su caso, el método de cifrado a utilizar de conformidad con la Norma de Cifrado de Información de FCC.

La División de Sistemas y Tecnología de la Información, en adelante DSTI deberá:

- Gestionar los requisitos de seguridad establecidos en todo el ciclo de vida de las copias de respaldo.
- Proporcionar los medios adecuados para la realización de las copias de seguridad de los sistemas gestionados por la DSTI.
- Asegurar que toda la información del Grupo FCC contenida en copias de respaldo de los sistemas gestionados por la DSTI pueda ser recuperada ante cualquier eventualidad.
- Implantar los medios técnicos necesarios para proteger la seguridad de la información almacenada en los soportes de respaldo.
- Configurar los registros de auditoría de las acciones realizadas durante todo el ciclo de vida de las copias de respaldo.

Los Responsables de la Información deberán:

- Clasificar la información almacenada en los soportes de recuperación.
- Autorizar la recuperación de la información contenida en las copias de respaldo.
- Verificar la correcta implantación de los controles establecidos en la presente Norma, sobre las copias de respaldo que contengan información de la que es responsable.

Los usuarios de los sistemas de información deberán realizar copias de respaldo de la información almacenada en los recursos corporativos puestos a su disposición.

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

5.1	Políticas para la seguridad de la información	[org.1] Política de Seguridad; [org.2] Normativa de Seguridad
5.15	Control de acceso	[op.acc.2] Requisitos de acceso
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
8.8	Gestión de vulnerabilidades técnicas	[op.mon.3] Vigilancia; [op.exp.4] Mantenimiento y actualizaciones de seguridad
8.12	Prevención de fugas de datos	[mp.com.1] Perímetro seguro; [mp.com.2] Protección de la confidencialidad; [mp.si.2] Criptografía; [mp.eq.3] Protección de dispositivos portátiles
8.13	Copias de seguridad de la información	[mp.info.6] Copias de seguridad
8.17	Sincronización de relojes	[op.exp.8] Registro de la actividad

Anexo I Procedimiento de almacenamiento y transporte de Copias de Respaldo

El Grupo FCC cuenta con un procedimiento donde se reflejan los requisitos de transporte y almacenamiento de las Copias de Respaldo.

Anexo II Periodicidad y retención mínima de Copias de Respaldo

Clasificación de la información	Periodicidad mínima de las Copias de Respaldo	Retención mínima de las Copias de Respaldo
Informació de Uso Público	Semanal	1 año
Información de Uso Interno	Semanal	1 año
Información Confidencial	Semanal	1 año
Información Secreta	Semanal	1 año