Norma de Criptografía 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)
1.0	Octubre 2016	IS	Modificación Norma ISO/IEC 27002:2013	Chief Information Security Officer (CISO)
1.0	Agosto 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 Actualización: - Identificación del dato - Gestión de claves y certificados	Chief Information Security Officer (CISO)
3.0	Mayo 2024	IS	Revisión del Documento y adaptación a normativa ISO 27001:2022	Chief Information Security Officer (CISO)
4.0	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 establece las medidas necesarias para asegurar la confidencialidad, integridad, autenticidad, trazabilidad y no repudio de la información para proporcionar un mayor nivel de seguridad frente al acceso, divulgación o uso no autorizado cuando se transmite o almacena información, las medidas incluyen:

- Una estrategia de cifrado de la información para todo el Grupo FCC.
- Una gestión estandarizada y adecuada de las claves de los sistemas de información.
- Un inventario de métodos criptográficos permitidos, así como sus características y casos de uso.

Y con ello, definiendo la asignación, implantación mantenimiento, supervisión y aplicación de las medidas de cifrado adecuadas en los sistemas de información del Grupo.

1.2 Alcance

Esta norma es de aplicación en toda información digital del Grupo FCC en reposo o en tránsito, cuyo nivel de confidencialidad aconseje la necesidad de protegerla mediante mecanismos criptográficos y cualquier desviación debe ser registrada

Toda implementación que requiere el uso de criptografía basada en tecnologías de la información debe cumplir y adherirse a esta Norma. Esto incluye:

- Sistemas de información, aplicaciones y servicios, infraestructuras y plataformas en las instalaciones.
- Puestos de usuario y dispositivos móviles corporativos.
- Dispositivos de almacenamiento corporativos portable o extraíbles.
- Sistemas de información, aplicaciones, servicios y/o medios de almacenamiento (SaaS, IaaS, PaaS) en la infraestructura local o en la nube.

2. Desarrollo

2.1 Principios

Los principios fundamentales en los que se basa la presente Norma del Grupo FCC son los siguientes:

- El cifrado de la información se regirá por el riesgo o impacto potencial de un incidente y no por la probabilidad de que se materialice tal incidente.
- Las medidas de cifrado que se aplicarán a la información serán proporcionales al nivel de riesgo de la información que contienen y al nivel de confidencialidad de la misma, consecuentemente estableciendo el tipo y nivel de calidad del algoritmo criptográfico requerido
- Los productos y algoritmos elegidos para cifrar la información deberán:
  - Estar certificados a nivel industrial.
  - Ser utilizados y gestionados únicamente por el personal autorizado.
  - Ser evaluados, aprobados e inventariados por el departamento de SI con cierta periodicidad.
- La estrategia de implantación deberá tener en consideración el efecto de la utilización de los mecanismos de cifrado sobre el rendimiento de la tecnología y/o sistemas informáticos utilizados, evitando que su implantación degrade la disponibilidad de estos sistemas.
- Se deberá evaluar el impacto y rendimiento derivado de la utilización de información encriptada sobre controles cuyo fin último es la inspección de contenido de tipo malware o filtrado de contenido.
- La aplicación de medidas de cifrado deberá ser integral y tener en cuenta:
  - Toda la información que requieren protección
  - Todas las ubicaciones donde se almacenen información
  - Todos los flujos de información durante la transición de un sistema a otro
  - Toda la gestión del ciclo de vida de las claves
- Todas las soluciones criptográficas deben de estar protegidas contra modificación y pérdida. Además, las claves secretas y privadas requieren protección contra el uso no autorizado, así como, contra la divulgación de las mismas.
- Se debe realizar una gestión apropiada de las claves criptográficas a través de procedimientos seguros para generar, almacenar, archivar, distribuir, recuperar, retirar y eliminar las claves criptográficas

Todas las soluciones utilizadas para la criptografía deben estar aprobadas por el departamento de SI.

2.2 Identificación de la Información

Toda información, objeto de la presente Norma, se considera como información sensible, y por tanto se debe cifrar antes de su distribución y/o almacenamiento. Las soluciones de cifrado utilizadas se eligen en base al tratamiento y nivel de clasificación de la información. De forma general, según el manejo de la información, se dividen en dos grandes grupos:

2.2.1 Información en reposo

La información en reposo es aquella información almacenada en sistemas de información tanto físicos como lógicos.

Dentro de esta categoría se incluyen, por ejemplo, información alojada en bases de datos, archivos, registros y copias de seguridad, almacenada en dispositivos como servidores, servicios en la nube, ordenadores portátiles/de sobremesa, dispositivos de almacenamiento externo, etc.

2.2.2 Información en tránsito

La información en tránsito es la información que se transmite a través de las redes o canales de comunicación, ya sean redes públicas (p. ej. Internet) o redes privadas (p. ej. LAN corporativa). Así como, la información en movimiento entre diferentes sistemas de información, dispositivos o aplicaciones.

2.3 Estrategia de Cifrado

El propósito de este apartado es establecer los controles para la correcta gestión de los procesos criptográficos y una correcta gestión de claves, con el fin de proteger la confidencialidad, disponibilidad, integridad, autenticidad, trazabilidady no repudio de la información, así como, la autenticación en todos los sistemas, servicios y/o aplicaciones del Grupo FCC.

La estrategia de cifrado de la información se fundamentará en las siguientes medidas técnicas y organizativas:

- El cifrado se podrá realizar a través de técnicas hardware y/o software.
- El almacenamiento y la transmisión de la información debe estar cifrada en función del riesgo y el nivel de clasificación de la información.
- La información y sus soportes a cifrar, mediante los métodos criptográficos aprobados, serán los siguientes:
    - Las credenciales almacenadas o transmitidas por cualquier sistema de información.
    - La información de carácter personal especialmente sensible (como datos sobre la ideología, la raza, la religión, la salud, etc.) o aquella información de carácter personal que deban ser cifrado como resultado de la evaluación de riesgos del tratamiento.
    - En el caso de la Información clasificada como Secreta o Confidencial deberán de cifrarse:
        - Las copias de respaldo.
        - Los correos electrónicos.
        - Las transmisiones enviadas a través de la red interna corporativa, así como, fuera de los sistemas de información del Grupo FCC
        - La comunicación y los accesos desde sistemas o equipos remotos.
        - La información almacenada en cualquier servidor, estación de trabajo o dispositivo cuando no se pueda garantizar su protección mediante controles físicos o lógicos y la información corra el riesgo de ser comprometida o robada.

2.3.1 Gestión de claves y certificados

En todos los sistemas donde exista información cifrada deberán existir procedimientos de gestión del material criptográfico, y estos deberán asegurar el acceso a las claves cuando sea necesario, la segregación de funciones y la rotación de tareas. Las claves y certificados se deberán usar únicamente para el propósito por el que fueron emitidos originalmente (por ejemplo, cifrado de documentos, firma digital o autenticación). Esta gestión se basa en los siguientes principios:

- La gestión de claves, siempre que sea posible, se realizará con tecnologías basadas en servicios de directorio, como puede ser el Directorio Activo. Almacenándose de forma segura en un emplazamiento distinto al lugar donde se aloje la información cifrada.
- La emisión de certificados y claves se realizará exclusivamente a través las autoridades de certificación autorizadas y aprobadas.
- Se deberá considerar los posibles impedimentos legales sobre el uso de técnicas criptográficas antes de realizar cualquier transmisión de información cifrada, para ello se deberá contactar con el departamento de SI.
- Los algoritmos de cifrado y las longitudes de las claves utilizadas se revisarán cada año para garantizar que están actualizados con las últimas normas y requisitos reglamentarios.
- Se evaluará la longitud de las claves de cifrado en relación con el algoritmo asociado y el nivel de clasificación de la información que debe de ser protegida.
- Las funciones de cifrado, descifrado y de gestión de claves deberán ser transparentes al usuario.
- Los Responsables de la Información notificarán sus necesidades en materia de cifrado a el departamento de SI.

3. Responsabilidades

El departamento de SI deberá:

- Definir las necesidades del control y gestión de las técnicas criptográficas.
- Supervisar la adecuada implantación de la presente norma.
- Monitorizar y evaluar cualquier incidente de seguridad relacionado con el cifrado de la información.
- Definir y actualizar un inventario de métodos criptográficos.
- Generar inteligencia sobre amenazas en criptografía y vulnerabilidades.

La División de Sistemas y Tecnología de la Información deberá:

- Gestionar:
  - Las soluciones criptográficas implantadas en el Grupo FCC.
  - Las guías para la implantación y gestión de las herramientas de cifrado, así como los procedimientos para la custodia y recuperación de las claves de cifrado.
- Notificar al departamento de SI los incidentes de seguridad reportados en materia de cifrado.

Los Responsables de la Información notificarán sus necesidades en materia de cifrado al departamento de SI.

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 para la seguridad de la información	[org.1] Política de Seguridad; [org.2] Normativa de Seguridad
5.2	Roles y responsabilidades de seguridad de la información	[org.4] Proceso de Autorización
5.3	Segregación de funciones	[op.acc.3] Segregación de funciones y tareas
5.5	Contacto con las autoridades	[op.exp.7] Gestión de Incidentes
5.6	Contacto con grupos de interés especial	[org.1] Política de Seguridad
5.7	Inteligencia de Amenazas	[op.mon.3] Vigilancia
5.8	Seguridad de la información en la gestión de proyectos	[op.pl.3] Adquisición de nuevos componentes

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
5.12	Clasificación de la información	[mp.info.2] Calificación de la información
5.13	Etiquetado de la información	[mp.si.1] Marcado de soportes
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
5.15	Control de accesos	[op.acc.2] Requisitos de acceso
5.36	Cumplimiento de las políticas, reglas y normas de seguridad de la información	[org.4] Proceso de Autorización; [op.exp.3] Gestión de la Configuración; [op.exp.4] Mantenimiento y Actualizaciones de Seguridad
6.7	Trabajo en remoto	[org.2] Normativa de Seguridad; [mp.per.2] Deberes y Obligaciones
8.1	Dispositivos de punto final de usuario	[mp.eq.3] Protección de dispositivos portátiles; [mp.eq.4] Otros dispositivos conectados a la red
8.11	Enmascaramiento de datos	[mp.info.1] Datos personales
8.12	Prevención de fuga 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	Copia de seguridad de la información	[mp.info.6] Copias de seguridad
8.24	Uso de criptografía	[op.exp.10] Protección de claves criptográficas; [mp.si.2] Criptografía; [mp.info.3] Firma electrónica
8.34	Protección de los sistemas de información durante las pruebas de auditoría	[op.exp.2] Configuración de Seguridad; [op.exp.3] Gestión de la Configuración; [op.exp.4] Mantenimiento y Actualizaciones de Seguridad; [mp.s.2] Protección de Servicios Web