Norma de Laboratorios de Sistemas 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)
1.1	Julio 2020	IS	Actualización 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 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)

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 directrices que permitan asegurar la integridad, confidencialidad, autenticidad y trazabilidad de la Información del Grupo FCC cuando se realicen actividades de configuración, pruebas, mantenimiento, reparación o destrucción de activos o sistemas de información.

1.2 Alcance

Esta Norma es de aplicación sobre cualquier activo o sistema de información del Grupo FCC sobre el que se realicen tareas de configuración, prueba, mantenimiento, reparación, o destrucción, independientemente de la información que trate y del laboratorio donde se realicen estas actividades.

2. Desarrollo

2.1 Principios

La seguridad de la información en los laboratorios de sistemas del Grupo FCC se fundamenta en los siguientes principios:

- Los laboratorios darán servicio exclusivamente a los sistemas y activos de información del Grupo FCC, salvo que el departamento de SI autorice el soporte a activos de otros propietarios.

- Cualquier tarea realizada sobre un activo o sistema en un laboratorio requerirá de un proceso de autorización y acceso, con carácter previo a su ejecución por parte del responsable de la información del activo, Cuando alguna o varias de las tareas a las que se refiere la presente Norma fueran ejecutadas por colaboradores externos al Grupo FCC, se deberán cumplir las medidas de seguridad establecidas en la Norma de Empresas Externas.
- Las medidas de seguridad a adoptar en las operaciones de configuración, prueba, mantenimiento, reparación o destrucción de activos informáticos deberán ser proporcional al nivel de clasificación de la información que alberguen.

2.2 Laboratorios de Sistemas

Los laboratorios de sistemas deberán implantar un entorno de trabajo controlado y acorde con los niveles de protección establecidos para los recursos informáticos con los que operen. Independientemente de su ubicación, los laboratorios de sistemas deberán de:

- Adoptar los principios recogidos en la Norma de Seguridad Física y en las Normas de Control de Accesos y la Norma de Control de la Configuración y del Cambio con la finalidad de evitar la alteración, pérdida, tratamiento y/o acceso no autorizado a la información del Grupo FCC tratada por los activos informáticos sobre los que se realice la operativa diaria.
- Todos los activos que se encuentren en los laboratorios deberán estar correctamente identificados y registrados. Adicionalmente, se deberán registrar las entradas y salidas de los activos informáticos que se manipulen en el laboratorio de sistemas, así como de aquellos que se desechen como consecuencia de la operativa del mismo.
- El registro de entrada/salida deberá contener al menos los siguientes campos sobre el activo o conjunto de activos:
    - Tipo de activo.
    - Fecha y hora.
    - Emisor.
    - Destinatario.
    - Departamento/área/empresa propietaria de la información.
    - Número de activos.
    - Forma de envío.
    - Persona responsable de la recepción/entrega debidamente autorizada.

- En el caso de ocurrir un incidente de seguridad de cualquier tipología durante la estancia de un activo informático en el laboratorio se seguirán las medidas asociadas de acuerdo con lo establecido en la Norma de Gestión de Incidentes. Se registrará el incidente de seguridad de forma completa siguiendo las directrices de la Norma de Gestión de Incidentes y se pondrá en conocimiento del responsable de la información correspondientes.
- Cuando las operaciones de configuración, pruebas, mantenimiento, reparación, o destrucción de activos informáticos sean realizadas por personal interno o colaboradores del Grupo FCC fuera de sus instalaciones, se deberán adoptar las medidas que garanticen la protección de la información, de acuerdo con la Norma de Empresas Externas y la Política de Uso de Medios Tecnológicos, Guía de Seguridad en el Trabajo a Distancia.
- Adoptar las medidas necesarias para impedir cualquier recuperación indebida de los datos e información contenida en los activos informáticos que abandonen estas instalaciones como consecuencia de operaciones de mantenimiento o destrucción.

3. Responsabilidades

El departamento de SI deberá:

- Aprobar y supervisar los controles lógicos y físicos establecidos para la gestión del laboratorio de sistemas informáticos de FCC.
- Analizar aquellos incumplimientos de la presente Norma que pudieran constituir un incidente de seguridad.
- Estar informado y analizar las más recientes tendencias en vulnerabilidades reales a nivel global y guiar a la organización través de la mejora continua y ser partícipe activo de la transmisión del conocimiento y mejores prácticas.

La División de Sistemas y Tecnologías de Información tendrá que:

- Implantar los procedimientos operativos que permitan garantizar los niveles de seguridad de la información en los laboratorios y en las actividades que se realicen en ellos.
- Registrar los movimientos de entrada, salida y destrucción de los recursos informáticos que se manipulen en el laboratorio de sistemas.
- Informar al departamento de SI de cualquier indicio, intento o realización de una acción contraria a la presente Norma, o de cualquier comportamiento anómalo en el control de acceso de las aplicaciones y sistemas.

El Responsable de la Información tiene como obligación:

- Autorizar la configuración, pruebas, mantenimiento, reparación, o destrucción de los recursos informáticos que traten Información de FCC de la que sea responsable.

El personal interno de FCC y colaboradores tendrán que:

- Considerar la metodología “Zero Trust” como principio de actuación en los laboratorios de sistemas, cuyo objetivo es que cualquier acceso, modificación y creación de acticos en estos, deben ser verificados y formalmente procesados.

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
5.8	Seguridad de la información en la gestión de proyectos	[op.pl.3] Adquisición de nuevos componentes
8.25	Seguridad en el ciclo de vida del desarrollo	[mp.sw.1] Desarrollo de aplicaciones
8.26	Requisitos de seguridad en las aplicaciones	[mp.sw.1] Desarrollo de aplicaciones; [mp.s.2] Protección de servicios y aplicaciones Web
8.27	Arquitectura de sistemas seguros y principios de ingeniería	[op.pl.2] Arquitectura de Seguridad; [mp.sw.1] Desarrollo de aplicaciones
8.28	Codificación segura	[mp.sw.1] Desarrollo de aplicaciones
8.29	Pruebas de seguridad en desarrollo y aceptación	[mp.sw.2] Aceptación y puesta en servicio
8.30	Desarrollo subcontratado	[op.ext.1] Contratación y acuerdos de nivel de servicio; [mp.sw.1] Desarrollo de aplicaciones; [mp.sw.2] Aceptación y puesta en servicio; [op.ext.3] Protección de la cadena de suministro

8.31	Separación de los entornos de desarrollo, prueba y producción	[mp.sw.2] Aceptación y puesta en servicio