Norma de Control de Accesos

del Grupo FCC

Octubre 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)
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)
2.3	Octubre 2025	IS	Modificación cuentas genéricas	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 definir los mecanismos que permitan gestionar el acceso a la información tratada en los sistemas de información del Grupo FCC, mediante mecanismos que aseguren que la misma, únicamente esté disponible a usuarios debidamente autorizados.

1.2 Alcance

Esta Norma es de aplicación a aquellos usuarios, tanto internos como colaboradores del Grupo FCC, que accedan a la información contenida en los sistemas de información de FCC, así como a los recursos asociados a los mismos, como consecuencia de su gestión y/o utilización, con independencia de:

- La modalidad del acceso (lógico o físico).
- La ubicación desde la cual se realiza el mismo (local o remoto).

2. Desarrollo

2.1 Principios

- El control de acceso encuentra su justificación en el principio de “necesidad de conocer” (need-to-know) por el cual se debe asegurar que los usuarios únicamente accedan a aquella información o recursos a los que hubieran sido autorizados y que resulten imprescindibles para el desarrollo de sus funciones.
- De forma predeterminada los perfiles de acceso definidos no podrán acceder a ningún recurso del Grupo FCC hasta que se le concedan los permisos correspondientes. Los perfiles constituyen grupos de derecho de acceso específicos que reflejan los permisos que uno o varios puestos de trabajo deben de tener sobre un recurso de información o un sistema.
- Como norma general, debe de existir consistencia lógica entre los permisos de acceso y el nivel de clasificación de la información a la que se trata de acceder.
- Los mecanismos de control de acceso deberán gestionar el acceso a información o recursos del Grupo FCC, con independencia del formato en que se presente o lugar en el que se encuentre.
- El control de acceso deberá cumplir los requisitos mínimos de seguridad que se determinen en función del nivel de clasificación de la información que traten, de acuerdo a lo dispuesto en la Política de Gestión de la Información.
- Cuando un sistema de información trata indistintamente información clasificada en varios de los niveles definidos en el Modelo de Clasificación de la Información establecido en el Grupo FCC, se implantarán las medidas de seguridad que correspondan a la información clasificada en el nivel más elevado.
- El acceso físico en las instalaciones del Grupo FCC donde se encuentren ubicados los sistemas de información deberá gestionarse en conformidad con lo dispuesto en la Norma de Seguridad Física de las instalaciones.
- En el caso de que sean empresas externas las que traten información del Grupo FCC, tanto el acceso físico en las instalaciones donde se encuentren ubicados los sistemas de información, como el acceso físico o lógico a dichos sistemas, deberán ser gestionados en conformidad con lo dispuesto en la Norma de Empresas Externas.
- Los controles de acceso a la información deberán respetar la normativa vigente, que resultara de aplicación.

- El control de acceso del grupo FCC deberá basarse en el principio de mínimo privilegio el cual establece que cada usuario, proceso o sistema debe tener sólo los privilegios necesarios para realizar su función específica y nada más minimizando así los riesgos asociados con el acceso innecesario a datos y recursos.

2.2 Gestión de Accesos

- Todos los sistemas de información e instalaciones del Grupo FCC que traten su información deberán tener implantados mecanismos de control de acceso en los que se pueda llevar un registro de la actividad.
- El acceso se fundamentará en perfiles de acceso que permitan la identificación inequívoca y personalizada de los usuarios o entidad (p.ej: Items lógicos como robots, máquinas, dispositivos o servicios...).
- Se definirán listas de control de accesos sobre recursos o funciones de los sistemas. Estas listas incluirán los distintos perfiles de acceso que se hayan definido.
- Los derechos de acceso se basarán en los permisos de lectura, escritura y ejecución.
- Los responsables de la información especificarán quién tiene derecho a la utilización de los perfiles que tratan información de la que son responsables.
- La asignación múltiple de identidades a un sólo usuario o entidad deberá ser formalmente justificada y alineada con las necesidades del negocio o por necesidades operacionales.
- FCC ha identificado tres tipos de cuentas de acceso:
    - Cuenta de Usuario: Cuenta de acceso a un sistema otorgada por razones de negocio a una persona individual.
    - Cuenta de Servicio: Cuenta de usuario utilizada por una aplicación o sistema para poder acceder de manera automatizada a otro sistema.
    - Cuenta Genérica: Cuenta con contraseña compartida por un colectivo de personas para el acceso a un sistema. Únicamente se autorizará el uso de cuentas genéricas que se empleen para el acceso a estaciones de trabajo y se requerirá, en todo caso, una segunda autenticación nominativa para el acceso a cualquier aplicativo o entorno productivo.
- Los responsables nominales de estas cuentas serán
    - La persona a la que se le asignado la Cuenta de Usuario.

  - La persona asignada como responsable del servicio en el caso de una Cuenta de Servicio.
  - La persona responsable de la información o responsable de la aplicación accedida en el caso de Cuentas Genéricas.

- Quedan prohibidas, salvo excepciones debidamente justificadas y aprobadas por el departamento de SI:
  - Las Cuentas de Servicio con privilegios de administrador de sistemas.
  - Las Cuentas Genéricas.
- Cuando, debido a necesidades de negocio, se requiera la creación y el uso de alguno de los tipos de cuenta anteriores, los responsables de estas cuentas deberán realizar un estudio de los riesgos asociados.
- La actividad realizada con las cuentas privilegiadas de servicio o las Cuentas Genéricas, deberán ser monitorizadas quedando registrados sus accesos en la auditoría del sistema.
- Con carácter general, el responsable de la aplicación revisará los derechos de acceso concedidos a los usuarios al menos una vez al año. Se podrá establecer un periodo distinto si existe una necesidad de negocio clara, en este caso, quedarán reflejados en los procedimientos que desarrollen la presente Norma.
- Cada responsable de la información llevará a cabo una revisión de los derechos existentes, teniendo en cuenta:
  - Su necesidad de continuidad.
  - Lo apropiado de estos derechos.
- El responsable de la Cuenta Genérica revisará trimestralmente los derechos de acceso asociados a dicha cuenta.
- Los administradores de las altas, bajas y modificaciones de los perfiles de acceso a los sistemas y recursos deberán mantener copias de la solicitud de estos cambios y de las revisiones al menos durante un año tras haberse producido.
- El mecanismo de adjudicación de permisos de acceso deberá permitir trazar los cambios en los privilegios y sus autorizaciones. Se considera privilegio el derecho a funciones que puedan sortear los controles de seguridad.

- Los procedimientos que desarrollen los requisitos y circunstancias aplicables deberán considerar cada una de las fases del ciclo de vida de un acceso de usuario, desde su solicitud, hasta su anulación o revocación.
- El cambio en responsabilidades o funciones implicará la alteración de los derechos autorizados o la supresión de las autorizaciones de acceso concedidas.
- Las aplicaciones y sistemas deberán contemplar la existencia de una relación o registro actualizado de los usuarios, y de sus perfiles de acceso.
- Los sistemas de información que posean como medio de autenticación el uso de contraseñas deberá de regirse por lo dispuesto en la Norma de Seguridad en Contraseñas.
- Los procedimientos que documenten el uso y administración de los sistemas de información deberán contemplar las medidas de control de acceso y los perfiles en función del tipo de acceso (administrativo, usuario, proceso, etc.).
- Los sistemas de información que traten Información Restringida deberán estar constantemente monitorizados para detectar cualquier intento de acceso no autorizado o el uso de derechos de acceso distintos de los autorizados.
- Esta monitorización deberá registrar todos los intentos exitosos y fallidos de acceso, como mínimo, la fecha y la hora, el usuario que lo realiza, el recurso accedido, el recurso mediante el cual se está realizando el intento de acceso y el resultado de la acción.

3. Responsabilidades

El departamento de SI deberá:

- Definir las necesidades de control de acceso a los sistemas de información.
- Aprobar y supervisar los controles establecidos para la gestión del control de accesos a los sistemas de información.
- Revisar los registros de auditoría de los accesos con la finalidad de verificar que estos estén actualizados y se correspondan con la verdadera necesidad de los usuarios.
- Controlar el seguimiento y la adecuada implantación de lo dictado en esta norma.

La División de Sistemas y Tecnología de la Información tiene como responsabilidad:

- Gestionar:

  - Las medidas establecidas para los perfiles de acceso y las cuentas de acceso asignadas a cada perfil.
  - Los procedimientos para la implantación y gestión de los mecanismos de control de acceso

- Monitorizar el funcionamiento de los sistemas de información del Grupo FCC bajo su control.
- Notificar al departamento de SI de los incidentes de seguridad reportados.

Los Responsables de la Información deberán:

- Definir los derechos de los perfiles de acceso.
- Aprobar formalmente los accesos a los sistemas de información bajo su responsabilidad.
- Velar por el cumplimiento de la presente Norma e informar de cualquier discrepancia observada al departamento de SI.
- Comunicar al departamento de SI de la ausencia prolongada en la actividad de los usuarios, tanto si estas han sido planificadas como si no fueron conocidas con antelación

Los Usuarios tienen como responsabilidad:

- Proteger adecuadamente sus credenciales de acceso a los sistemas de Información del Grupo FCC.
- Comprender las consecuencias que puede ocasionar el incumplimiento de la presente Norma.
- Notificar de forma inmediata al departamento de SI de cualquier sospecha de violación de la presente Norma.
- Notificar cualquier incidente en el que datos personales puedan verse o se hayan visto comprometidos al DPO/Coordinador de Protección de Datos del área correspondiente.
- Informar inmediatamente al departamento de SI de la pérdida, robo o inutilización de cualquier dispositivo.

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
5.16	Gestión de identidades	[op.acc.1] Identificación
5.17	Información de autenticación	[op.acc.1] Identificación; [op.acc.2] Requisitos de Acceso
5.18	Derechos de acceso	[op.acc.4] Proceso de gestión de derechos de acceso
7.1	Perímetros de seguridad física	[mp.if.1] Áreas separadas con control de acceso
7.2	Entrada física	[mp.if.2] Identificación de las personas; [mp.if.7] Registro de entrada y salida de equipamiento
7.3	Aseguramiento de oficinas, salas e instalaciones	[mp.if.1] Áreas separadas con control de acceso; [mp.if.3] Acondicionamiento de los locales
7.4	Supervisión de la seguridad física	[mp.if.1] Áreas separadas con control de acceso; [mp.info.1] Datos personales
7.5	Protección contra amenazas físicas y ambientales	[mp.if.3] Acondicionamiento de los locales; [mp.if.5] Protección frente a incendios; [mp.if.6] Protección frente a inundaciones
7.6	Trabajar en áreas seguras	[mp.if.1] Acondicionamiento de los locales; [org.2] Normativa de seguridad
7.7	Escritorio despejado y pantalla despejada	[mp.eq.1] Puesto de trabajo despejado; [mp.eq.2] Bloqueo del puesto de trabajo
7.8	Ubicación y protección del equipo	[mp.if.1] Áreas separadas con control de acceso; [mp.eq.3] Protección de dispositivos portátiles
7.9	Seguridad de los activos fuera de las instalaciones	[mp.eq.3] Protección de dispositivos portátiles
7.10	Sistemas 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

7.11	Servicios públicos de suministro	[mp.if.4] Energía eléctrica
7.12	Seguridad del cableado	[mp.if.3] Acondicionamiento de los locales
7.13	Mantenimiento de equipos	[op.exp.4] Mantenimiento y actualizaciones
7.14	Eliminación segura o reutilización de equipos	[mp.si.5] Borrado y destrucción
8.2	Derechos de acceso privilegiado	[op.acc.1] Identificación
8.15	Registro	[op.exp.8] Registro de la actividad