Norma de Bases de Datos 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 2016	IS	Modificación Norma ISO/IEC 27002:2013	Chief Information Security Officer (CISO)
	Octubre 2019	IS	Revisión del documento	Chief Information Security Officer (CISO)
1.1	Julio 2021	IS	Revisión del Documento Unificación de la estructura y formato con el resto de la Normativa.	Chief Information Security Officer (CISO)
1.2	Mayo 2024	IS	Revisión del documento y adaptación a ISO 27001:2022	Chief Information Security Officer (CISO)
1.3	Julio 2025	IS	Revisión del documento y adaptación al ENS	Chief Information Security Officer (CISO)

ÍNDICE

1. Introducción 3

1.1 Objeto 4

1.2 Alcance 4

2. Desarrollo 4

2.1 Principios 5

3. Responsabilidades 7

4. Referencia normativa 8

4.1 Controles de la normativa ISO27001:2022 y ENS 8

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 la protección de los datos albergados en las Bases de Datos del Grupo FCC frente al acceso, la alteración o la destrucción no autorizada.

1.2 Alcance

La presente Norma se aplica a todo el personal y colaboradores del Grupo FCC, en adelante FCC, con acceso a la información contenida en las Bases de Datos alojadas en los Sistemas de Información del Grupo, así como a los sistemas de información que estén interconectados a esas Bases de Datos.

2. Desarrollo

2.1 Principios

- El acceso a la Información de FCC almacenada en las Bases de Datos deberá ser autorizado por el responsable de dicha Información.
- Cuando una cuenta de acceso a una Base de Datos no se vaya a utilizar durante un periodo superior a tres meses, deberá permanecer bloqueada.
- El Responsable de la Información, efectuará controles regulares de actividad en el acceso a la Base de Datos. Cuando se identifiquen cuentas de acceso en las que se superen periodos de inactividad de tres meses, se informará al responsable correspondiente para que este tome las medidas oportunas sobre la revocación de los accesos.
- El usuario que, estando autorizado para acceder a las Bases de Datos, indebidamente modifique, destruya, copie o provoque pérdida de información será sancionado de acuerdo con el régimen disciplinario vigente.

Los administradores de Bases de Datos o el personal de FCC que realice labores de mantenimiento de Bases de Datos deberán:

- Mantener, en todo momento, la integridad y la estabilidad de las Bases de Datos.
- Conocer los riesgos y vulnerabilidades asociados al uso de bases de datos provistas por proveedores
- El control de acceso a las tablas que forman parte de la Base de Datos se realizará a través de roles/perfiles y de permisos de acceso. Estos privilegios de acceso serán los estrictamente necesarios para el desarrollo de las funciones que desempeñe el personal de FCC que vaya a tratar la información contenida en las Bases de Datos, adicionalmente, los derechos de privilegio serán otorgados de forma temporal hasta que el usuario realice los cambios o finalice la tarea pertinente
- Las contraseñas suministradas, por defecto, por el fabricante, deberán ser modificadas de acuerdo con la Norma de Seguridad de las Contraseñas del Grupo FCC.

- El uso de enlaces dentro de las Bases de Datos a información contenida en otras Bases de Datos está prohibido y solamente se podrá realizar en los casos en que se justifique formalmente su necesidad.

Las modificaciones de las Bases de Datos de FCC deberán cumplir los siguientes requisitos:

- Las modificaciones de la estructura de las Bases de Datos deberán ser autorizadas por el responsable de la información y por el administrador de la Base de Datos. El motivo de la modificación y el procedimiento técnico deberá ser debidamente documentado.
- La realización de una copia de seguridad completa antes de iniciar cualquier cambio.
- Antes de su paso a entornos reales de explotación, todas las Bases de Datos de FCC deberán ser previamente probadas en sus funcionalidades de negocio y capacidades de procesamiento
- Las modificaciones de emergencia de los datos únicamente podrán realizarse bajo circunstancias críticas, en conformidad con los procedimientos de emergencia desarrollados en las Normas de Gestión de Incidentes y de Continuidad de Negocio. En este caso siempre se considerará que ha ocurrido un incidente y, como tal, debe ser registrado.
- La verificación de la consistencia e integridad de los índices se realizará con una periodicidad máxima de un mes. Cualquier pérdida de integridad deberá ser resuelta de forma inmediata.
- Es necesario que se establezca una estrategia de actualización y optimización de índices, en función del tamaño y de los requisitos de los tiempos de respuesta establecidos, y siempre de acuerdo con las directrices fijadas en la presente Norma.
- En el caso que el negocio establezca una criticidad alta con respecto a la disponibilidad de la información, se tendrá que implantar una estrategia de redundancia de la base de datos.
- Todos los accesos, inicios de sesión, a la base de datos serán registrados en algún registro de auditoría.
- Cuando, en función del nivel de clasificación asignado a la información almacenada en las Bases de Datos de FCC, fuera obligatorio el cifrado de sus contenidos, este se realizará en conformidad con lo dispuesto en la Norma de Criptografía. El cifrado deberá realizarse sin la necesidad de intervención del usuario.
- No se podrán dejar sin protección los ficheros y áreas de carga temporales utilizados para las labores de adquisición de datos. Asimismo, se debe garantizar su borrado y destrucción segura una vez que hayan dejado de ser utilizadas. El Responsable de la Información establecerá procesos periódicos de borrado de estos datos con una periodicidad semanal.
- La gestión de las Bases de Datos deberá cumplir con los principios establecidos en la Norma de Control de Configuración y del Cambio, y en la Norma de Gestión de Copias de Respaldo.
- Las herramientas utilizadas en los procesos de limpieza, depuración y carga de los datos deberán de instalarse con sus medidas de seguridad perfectamente

configuradas y aprobadas por el grupo FCC para evitar accesos no autorizados y garantizar una manipulación de datos segura.

3. Responsabilidades

El departamento de SI deberá:

- Asegurar que las medidas de gestión y controles establecidos para las Bases de Datos de FCC se han implantado y se encuentran operativas según se expresa en la presente Norma.
- Estar al corriente y producir inteligencia sobre nuevas amenazas y vulnerabilidades en bases de datos.

La División de Sistemas y Tecnología de la Información deberá:

- Gestionar la correcta implantación de las medidas de seguridad y control tecnológico de las Bases de Datos establecidas en esta Norma.
- Notificar cualquier incidente al departamento de SI, en cumplimiento con la Norma de Incidentes del Grupo FCC.

Los Responsables de la Información deberán:

- Notificar sus necesidades respecto de las medidas de seguridad en las Bases de Datos al departamento de SI.
- Notificar, de forma inmediata al departamento de SI de cualquier sospecha de acceso sin autorización a la información.
- 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.
- Autorizar el acceso a la Información de FCC almacenada en las Bases de Datos.

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
5.2	Roles y responsabilidades en 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
5.12	Clasificación de la información	[mp.info.2] Calificación de la información
5.13	Etiquetado de la información	[mp.si.1] Marcado de soportes
5.15	Control de acceso	[op.acc.2] Requisitos de acceso
5.19	Seguridad de la información en las relaciones con los proveedores	[op.ext.1] Contratación y acuerdos de nivel de servicio
5.37	Procedimientos operativos documentados	[org.3] Procedimientos de Seguridad
8.2	Derecho de acceso privilegiado	[op.acc.1] Identificación
8.6	Gestión de la capacidad	[op.pl.4] Gestión de la Capacidad; [mp.s.4] Protección frente a la denegación de servicio
8.7	Protección contra malware	[op.exp.6] Protección frente a código dañino
8.8	Gestión de las vulnerabilidades técnicas	[op.mon.3] Vigilancia; [op.exp.4] Mantenimiento y actualizaciones
8.9	Gestión de la configuración	[op.exp.2] Configuración de Seguridad; [op.exp.3] Gestión de la Configuración
8.10	Eliminación de información	[mp.si.5] Borrado y destrucción
8.13	Copias de seguridad de la información	[mp.info.6] Copias de seguridad
8.19	Instalación de software en sistemas operativos	[op.exp.2] Configuración de seguridad; [op.acc.3] Segregación de funciones y tareas; [mp.sw.2] Aceptación y puesta en servicio
8.25	Ciclo de vida de desarrollo seguro	[mp.sw.1] Desarrollo de aplicaciones
8.27	Arquitectura del sistema seguro y principio 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
8.32	Gestión de cambios	[op.exp.5] Gestión de Cambios
8.33	Información de prueba	[mp.sw.1] Desarrollo de aplicaciones; [mp.sw.2] Aceptación y puesta en servicio