Norma de Roles y Responsabilidades 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)
2.0	Julio 2021	IS	Revisión del Documento Unificación del formato con el resto de la Normativa. Actualización: • Referencias • Responsabilidades de LISO y CISO • Nuevos Comités	Chief Information Security Officer (CISO)
3.0	Diciembre 2022	IS	Actualización: • Nuevo organigrama • Nuevos roles • Nuevos Comités	Chief Information Security Officer (CISO)
4.03.1	Mayo 2024	IS	Revisión del documento de adaptación a la normativa ISO27001:2022	Chief Information Security Officer (CISO)
5.0	Julio 2025	IS	Revisión del documento de 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

El objeto de la presente Norma es definir los roles y las responsabilidades que desempeña el personal del Grupo FCC en materia de seguridad de la información en el desarrollo de sus funciones.

1.2 Alcance

La presente Norma se aplica a todos los recursos y personal del Grupo FCC que accedan a la información del Grupo con independencia de las funciones realizadas.

El Marco Normativo de Seguridad de la Información desarrolla las responsabilidades del personal del Grupo FCC que aparecen en esta Norma.

2. Desarrollo

2.1 Roles y Responsabilidades

Todos los roles y responsabilidades estarán diferenciados y, en la medida de lo posible, serán asignados de manera individualizada en la descripción del puesto de trabajo. Además de esta asignación individualizada, todas las personas que pertenezcan al Grupo FCC, sea cual sea su nivel, estarán obligadas a cumplir las normas, procedimientos y controles establecidos en materia de seguridad de la información.

A continuación, se describen los roles con sus responsabilidades en seguridad de la información. En el *Anexo I Organigrama* se muestra la estructura para la Seguridad de la Información.

Departamento de Seguridad de la Información

Las responsabilidades del departamento de SI, liderado por el CISO son:

- Definir la estrategia global, establecer el modelo de gobierno y definir e implementar los procesos de gestión de riesgos de seguridad de la información.

- Definir y actualizar el Marco Normativo de seguridad de la información y la arquitectura de seguridad global.
- Definir y supervisar los programas de formación y concienciación en seguridad de la información.
- Asegurar la adecuada gestión de amenazas, vulnerabilidades, incidentes, cumplimiento de la normativa y la eficiencia de los controles de seguridad de los sistemas de información involucrados en los servicios prestados a todo el Grupo.
- Gestionar, operar y establecer las medidas de seguridad necesarias para proteger los sistemas de información involucrados en los servicios prestados a todo el Grupo.
- Monitorizar, controlar, auditar y reportar el estado global de la seguridad en el Grupo y escalar los riesgos detectados.

Business Information Security Team

Las responsabilidades del Business Information Security Team, liderado por el LISO son:

- Representar la función de seguridad en su unidad de negocio y trasladar sus necesidades al departamento de SI.
- Implementar la arquitectura de seguridad de la información en su unidad de negocio.
- Alinear la estrategia del negocio con la estrategia de seguridad de la información y los requisitos mínimos.
- Asegurar la adecuada gestión de amenazas, vulnerabilidades, incidentes, cumplimiento de la normativa y la eficiencia de los controles de seguridad de los sistemas de información de su unidad de negocio.
- Garantizar la adecuada formación y concienciación en seguridad de la información en su unidad de negocio.
- Gestionar, operar y establecer las medidas de seguridad necesarias para proteger los sistemas de información involucrados en servicios que afectan a su unidad de negocio que no forman parte de los servicios horizontales.
- Monitorizar y reportar el estado global de la seguridad de su negocio y escalar los riesgos detectados.

Usuarios de los sistemas de información.

Los usuarios de los sistemas de información tendrán como responsabilidades:

- Cumplir con las medidas establecidas en el cuerpo normativo relativo a la seguridad de la información y comprender las consecuencias de su incumplimiento.
- Tratar la información del Grupo FCC sólo para el desarrollo de sus funciones.
- Comunicar aquellos incidentes de seguridad o malos usos de los activos de información de los que se tenga conocimiento.
- Estar completamente informado del rol, funciones y responsabilidades y expectativas de seguridad en que derivan su cargo dentro del grupo.

Las responsabilidades del departamento de Auditoría Interna:

- Revisar el estado de implantación y madurez del Cuerpo Normativo.
- Evaluar los procedimientos de análisis de riesgos y gestión de proveedores, así como el modelo de gestión de la seguridad de la información.
- Auditar el plan de continuidad de negocio y los procesos de respuesta y recuperación ante incidentes.
- Informar al CISO y al departamento de SI los aspectos identificados durante las auditorías.

2.2 Coordinación de seguridad de la información

El Grupo FCC se ha dotado de una estructura de comités de seguridad para la definición, elaboración, desarrollo y control de las actividades relacionadas con la seguridad de la información.

La seguridad de la información es una necesidad para el correcto desarrollo del negocio a la que todas las áreas del Grupo FCC deben de contribuir. Los comités de seguridad tienen, como su principal función, la coordinación de las medidas que se adopten respecto de la gestión de la seguridad de la información. A petición del departamento de SI se podrán constituir aquellos comités, foros o grupos de trabajo que se consideren necesarios.

Comité de Ciberseguridad

El Comité de Ciberseguridad es el órgano encargado de comunicar la estrategia de seguridad a toda la organización. Se convocará trimestralmente, liderado por el CISO, siendo el primer comité del año prioritario y estratégico.

Objeto:

- Primer comité del año: Difundir la estrategia global de seguridad y realizar el seguimiento anual del plan director.
- Resto de comités: Realizar el seguimiento trimestral de los planes de acción derivados del plan director y escalar los incidentes relevantes de seguridad.

A este Comité deberán asistir:

- Director de Sistemas y Tecnologías de la Información – CIO, Corporativo
- Director del departamento de SI – CISO.

- Local Information Security Office – LISO, de cada unidad de negocio.
- Directores de Sistemas y Tecnologías de la Información (CIOs) de cada unidad de negocio.

Los comités de seguridad cumplirán la función de mantener actualizada a la organización en materia de seguridad, coordinar la estrategia y otras funciones entre las que se encuentran:

- Conocer los principales retos a los que se enfrentan las unidades de negocio.
- Fomentar la colaboración transversal entre unidades
- Asegurar que la organización conoce los riesgos, incidentes e incidencias de seguridad que ocurren a nivel global
- Asesorar e intercambiar conocimiento sobre nuevas tecnologías, servicios, retos, etc.

Comité de Control de Seguridad

El Comité de control de seguridad es el órgano encargado de coordinar y revisar el estado de seguridad en las diferentes unidades de negocio. Este comité podrá tener calidad de foro o grupo de trabajo si es necesario. Se convocará mensualmente con cada una de las unidades de negocio y será liderado por un representante del departamento de SI.

Objeto: Realizar el seguimiento de las iniciativas de los planes de acción. Escalar cualquier incidente, incidencia o cambio relevante.

A este Comité deberán asistir:

- Un representante del Global Information Security Team.
- LISO o CISO de la unidad de negocio.

El Comité de Coordinación TI:

El Comité de Coordinación de TI es el órgano encargado de informar y realizar seguimiento de los riesgos tecnológicos más relevantes, y decidir las estratégicas de mitigación de estos. Así como, coordinar y realizar el seguimiento de las acciones que se deriven de los acuerdos adoptados en el Comité.

Objeto:

- Informar a la Dirección General Corporativa de los riesgos de tecnologías de la información.
- Coordinación y seguimiento del Plan director de Proyectos.
- Supervisar los incidentes relevantes, así como de la definición y activación de Planes de Respuesta.

A este Comité deberán asistir:

- Director de Sistemas y Tecnologías de la Información Corporativo.
- Director del departamento de SI – CISO.
- Director de Aplicación.
- Director de Infraestructura.

Privacy Board

El Comité Seguridad de la Información y Protección de datos personales es el órgano encargado de definir y evaluar el cumplimiento de requisitos regulatorios respecto a la protección de datos personales.

Objeto:

- Informar sobre cuestiones referentes a Protección de Datos.
- Informar sobre nuevas regulaciones.
- Definir y aprobar los niveles de riesgo respecto a la Protección de Datos.
- Apoyar en la gestión de incidentes críticos/Comunicaciones urgentes a autoridades reguladoras.

A este Comité deberán asistir:

- Director del departamento de SI – CISO.
- Director de Asesoría Jurídica.
- Director de Recursos Humanos.
- Director del Departamento de Auditoría Interna, Gestión de Riesgos y Cumplimiento de FCC.
- Director de la División de Sistemas y Tecnologías de la Información.
- Coordinador de Protección de Datos del Grupo FCC.
- Cualquier otro miembro de Seguridad de la Información o Protección de datos que se crea relevante para tratar algún aspecto en cuestión.

3. Cambios en los Roles y Responsabilidades

Corresponde a la Comisión de Auditoria la aprobación de los cambios en los roles y responsabilidades. Este Comité elevará su decisión a la Dirección General del Grupo FCC para su firma y comunicación dentro del Grupo.

4. Referencia normativa

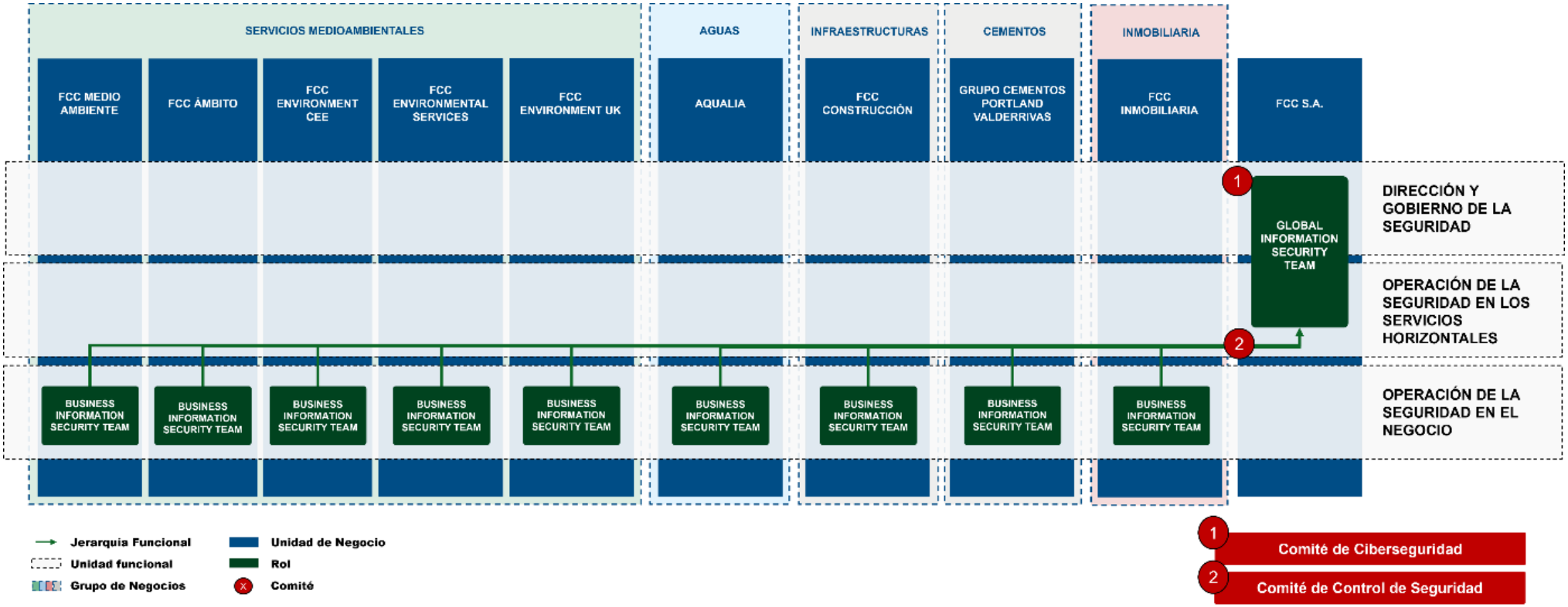
El presente documento ha sido revisado por el departamento de SI y su redacción toma como referencia el estándar internacional ISO27001:2022.

4.1 Controles de la normativa ISO27001:2022 y ENS

ID Control ISO	Control ISO/IEC 27001:2022	Correspondencia ENS

5.2	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
5.4	Responsabilidades de la dirección	[org.1] Política de Seguridad; Art. 13 Organización e implantación del proceso de seguridad
5.5	Contacto con las autoridades	Art. 25 Incidentes de seguridad; [op.exp.7] Gestión de incidentes
5.6	Contacto con grupos de interés especial	Art. 13 Organización e implantación del proceso de seguridad; [org.1] Política de Seguridad
5.7	Inteligencia de amenazas	[op.mon.3] Vigilancia

Anexo I Organigrama



Anexo II Matriz RASCI

	CIO	CISO	CTO	CFO	DPO	Responsable Aplicaciones	Responsable Seguridad Física	Director IT	Responsable SI (UN)	Responsable OT (UN)	Responsable IT (BU)	DPO (BU)	RRHH	Comisión de auditoría	Proveedor externo	Equipo Infraestructura	Equipo Gobierno & SMO	Auditoría Interna	Asesoría Jurídica	Director Secretaría General	Equipo Seguridad Física	Legal	Compras
Estrategia y Gestión de recursos de seguridad	C	R		I											S								
Gobierno y reporte de la seguridad	C/I	R/A													S								
BISO y gestión de la entidad		C/I						A	R						S								
Ejecución del programa de seguridad	C/I	R/A													S								
Gestión de riesgos de seguridad	I	R/A													S								
Política de seguridad	I	R			C								C	A	S				C				
Gestión y recuperación de la continuidad de negocio	I	C	A												S	R							
Gestión de la seguridad de terceras partes	I	R/A											S										
Cultura y comportamiento de seguridad	I	R/A			C								S										
Seguridad física y personal		C/I					R													A	S		
Cumplimiento regulatorio	I	R/A			S				R												C		
RFP & gestión de las Due-Diligence	A/I	R			C																		S
Control de calidad y prueba de controles de seguridad	I	R/A																C					
Gestión de solución DLP	I	R/A	C																				
Gobierno de la protección del dato	I	A			R										S							C	
Gestión de la protección de datos en todo el ciclo de vida		A/C/I			R				R			R			S								
Arquitectura, estándares y guías de seguridad	I	A/C	A													R							
Infraestructura y desarrollo de productos de seguridad	I	A/C	A													R							
Configuración segura de dispositivos	I	A/C	A													R							
Soluciones criptográficas	I	A/C	A													R							
Consultoría y asesoría de seguridad	I	R/A													S								
Estándares de seguridad en entornos operacionales OT		R								R	A					C							
Gestión de incidentes	I	R/A													S								
Análisis forense	I	R/A													S								
Gestión de la plataforma de operaciones de seguridad	I	R/A													S								
Monitorización de los incidentes y eventos de seguridad	I	R/A													S								
Gestión de vulnerabilidades	I	R/A													S								
Operaciones de DLP	I	R/A													S								
Protección de marca	I	R/A													S								
Cyber Threat Intelligence	I	R/A													S								
Pruebas y simulaciones de ciberseguridad	I	R/A													S								
Ciberanálisis	I	R/A													S								
Gestión de accesos		C	A/I								R		R				R						
Gestión del ciclo de vida del usuario		C	A/I								R						R						
Gestión de accesos privilegiados		A/C	A/I								R						R						
Gestión de las relaciones con el negocio	A/I	R																					
Herramientas y Tecnología	I		A/I								R				S		R						
Seguridad perimetral	I	A/C	A												S	R							
Seguridad de la red interna	I	A/C	A												S	R							
Configuración segura y bastionado	I	A/C	A												S	R							
Protección antimalware	I	R/A/C	A												S	R							
Seguridad de la red interna	I	R/A/C	A												S	R							
Seguridad del entorno OT		C	C							R/A/S/I													
S-SDLC	I		A			R/A									S	R							
Protección de las aplicaciones postdesarrollo	C	R/A/C													S								