FCC Group Roles and Responsibilities Standard

January 2026

Document Version Control				
Version	**Date**	**Author**	**Detail**	**Approved by**
1.0	April 2009	IS	Document creation	FCC Executive Committee
1.1	September 2014	IS	Document Review	Chief Information Security Officer (CISO)
	October 2019	IS	Document Review	Chief Information Security Officer (CISO)
2.0	January 2026	IS	Document Review ISO/IEC 27001:2022 ENS	Chief Information Security Officer (CISO)

INDEX

1. Introduction

This document is part of the FCC Group's Information Security Regulatory Framework, which establishes the Group's mandatory precepts on Information Security.

The Security Regulatory Framework is periodically reviewed and updated periodically by the Information Security Department (hereinafter, the IS Department), in accordance with the provisions of the Regulatory Framework Management and Maintenance Document. This document contains information on the version history, revisions and approvals of this Standard, as well as its relationship and dependence on other regulatory documents.

This standard will be reviewed at least once a year, unless circumstances recommend or require an earlier revision.

1.1 Purpose

The purpose of this Standard is to define the roles and responsibilities assumed by FCC Group personnel in matters of information security in the performance of their duties.

1.2 Scope

This Standard applies to all FCC Group personnel and resources that access the Group’s information, regardless of the functions they perform. The Information Security Regulatory Framework defines and expands upon the responsibilities of FCC Group personnel described in this Standard.

2. Development

2.1 Roles and Responsibilities

All roles and responsibilities shall be differentiated and, as far as possible, individually assigned within the job description. In addition to this individualized assignment, all individuals belonging to the FCC Group, regardless of their level, are required to comply with the rules, procedures, and controls established in matters of information security.

The roles and their corresponding information security responsibilities are described below. Annex I – Organizational Chart presents the structure for Information Security.

2.1.1 Information Security Department

- The responsibilities of the Information Security Department, led by the CISO, are:
- Define the global strategy, establish the governance model, and define and implement information security risk-management processes.
- Define and update the Information Security Regulatory Framework and the global security architecture.
- Define and oversee information security training and awareness programs.
- Ensure the proper management of threats, vulnerabilities, incidents, regulatory compliance, and the effectiveness of security controls for the information systems involved in the services provided to the entire Group.
- Manage, operate, and establish the necessary security measures to protect the information systems involved in the services provided to the entire Group.
- Monitor, control, audit, and report the overall security status of the Group and escalate identified risks.

2.1.2 Business Information Security Team

The responsibilities of the Business Information Security Team, led by the LISO, are:

- Represent the security function within their business unit and communicate its needs to the Information Security Department.
- Implement the information security architecture within their business unit.
- Align the business strategy with the information security strategy and minimum requirements.
- Ensure the proper management of threats, vulnerabilities, incidents, regulatory compliance, and the effectiveness of security controls for the information systems of their business unit.
- Ensure adequate information security training and awareness within their business unit.
- Manage, operate, and establish the necessary security measures to protect the information systems involved in services affecting their business unit that are not part of horizontal services.
- Monitor and report the overall security status of their business unit and escalate identified risks.

2.1.3 Users of Information Systems

Information system users shall have the following responsibilities:

- Comply with the measures established in the regulatory framework related to information security and understand the consequences of non-compliance.
- Handle FCC Group information solely for the performance of their duties.
- Report any security incidents or misuse of information assets they become aware of.
- Be fully informed of the role, functions, responsibilities, and security expectations associated with their position within the Group.

2.1.4 Internal Audit Department Responsibilities

The responsibilities of the Internal Audit department:

- Review the implementation status and maturity of the Regulatory Framework.
- Evaluate risk-analysis procedures and supplier-management processes, as well as the information security management model.
- Audit the business continuity plan and the incident response and recovery processes.
- Report to the CISO and the Information Security Department on the findings identified during audits.

2.2 Information Security Coordination

The FCC Group has established a structure of security committees for the definition, development, implementation, and oversight of activities related to information security. Information security is essential for the proper operation of the business, and all areas of the FCC Group must contribute to it. The primary function of the security committees is to coordinate the measures adopted for the management of information security. At the request of the Information Security Department, any committees, forums, or working groups deemed necessary may be created.

2.2.1 Cybersecurity Committee

The Cybersecurity Committee is the body responsible for communicating the security strategy to the entire organization. It will convene quarterly, led by the CISO, with the first committee meeting of the year being strategic and of highest priority.

Purpose

- First committee of the year: Communicate the global security strategy and conduct the annual follow-up of the master plan.
- Subsequent committees: Conduct quarterly follow-up of the action plans derived from the master plan and escalate relevant security incidents.

The following must attend this Committee:

- Chief Corporate Information Officer (CIO)
- Director of the Information Security Department – CISO
- Local Information Security Officers (LISOs) from each business unit
- Chief Information Officers (CIOs) of each business unit

The security committees serve to keep the organization updated on security matters, coordinate the strategy, and perform additional functions, including:

- Identifying the main challenges faced by the business units
- Promoting cross-unit collaboration
- Ensuring that the organization is aware of global security risks, incidents, and issues.
- Advising and sharing knowledge on new technologies, services, challenges, and related topics

2.2.2 Security Control Committee

The Security Control Committee is the body responsible for coordinating and reviewing the security status across the different business units. This committee may operate as a forum or working group if necessary. It will convene monthly with each business unit and will be led by a representative of the Information Security Department.

Purpose

Monitor the progress of action-plan initiatives. Escalate any relevant incident, issue, or change.

The following must attend this Committee:

- A representative of the Global Information Security Team.
- The LISO or CISO of the business unit.

2.2.3 IT Coordination Committee

The IT Coordination Committee is the body responsible for reporting and monitoring the most relevant technological risks and deciding on the strategies to mitigate them.

It also coordinates and monitors the actions derived from the agreements adopted within the Committee.

Purpose

- Inform the Corporate General Management about information-technology risks.
- Coordinate and monitor the Project Master Plan.
- Oversee relevant incidents, as well as the definition and activation of Response Plans.

The following must attend this Committee:

- Corporate Chief Information Officer (CIO).
- Director of the Information Security Department – CISO.
- Applications Director.
- Infrastructure Director.

2.2.4 Privacy Board

The Information Security and Personal Data Protection Committee is the body responsible for defining and assessing compliance with regulatory requirements related to personal data protection.

Purpose

- Provide information on matters related to Data Protection.
- Report on new regulations.
- Define and approve risk levels related to Data Protection.
- Support the management of critical incidents and urgent communications to regulatory authorities.

The following must attend this Committee:

- Director of the Information Security Department – CISO.
- Director of the Legal Department.
- Director of Human Resources.
- Director of the Internal Audit, Risk Management, and Compliance Department of FCC.
- Director of the Information Systems and Technology Division.
- FCC Group Data Protection Coordinator.
- Any other Information Security or Data Protection member deemed relevant to address specific matters.

3. Changes to Roles and Responsibilities

The Audit Committee is responsible for approving any changes to roles and responsibilities. This Committee shall submit its decision to the FCC Group's General Management for signature and subsequent communication within the Group.

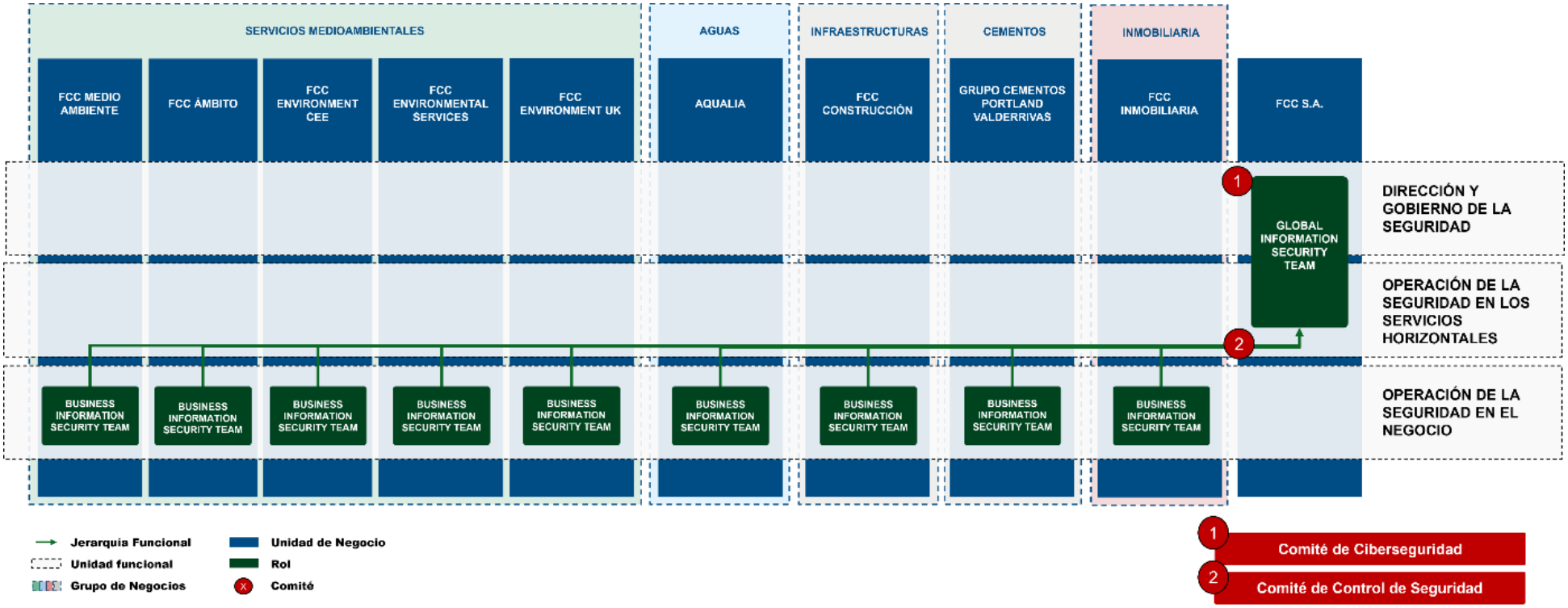
4. Normative reference

This document has been reviewed by the IS Department, and its wording is based on the international standard ISO27001:2022 and the ENS.

4.1 Regulatory controls ISO27001:2022 and ENS

ID Control ISO	ISO/IEC 27001:2022 control	ENS Correspondence
5.2	Roles and responsibilities in information security	[org.4] Authorization Process
5.3	Segregation of duties	[op.acc.3] Segregation of functions and tasks
5.4	Management responsibilities	[org.1] Security Policy; Art. 13 Organization and implementation of the security process
5.5	Contact with authorities	Art. 25 Security incidents; [op.exp.7] Incident management
5.6	Contact with special interest groups	Art. 13 Organization and implementation of the security process; [org.1] Security Policy
5.7	Threat intelligence	[op.mon.3] Monitoring

ANNEX I – Organizational chart



ANNEX II – RASCI Matrix

	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								