Norma de Seguridad de Redes

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)
1.3	Noviembre 2011	IS	Inclusión apartada “seguridad en redes inalámbricas” y “anexo I”	Chief Information Security Officer (CISO)
1.4	Marzo 2013	IS	Actualización general del documento: Introducción, alcance, diseño de la arquitectura de red, Interconexión.	Chief Information Security Officer (CISO)
	Octubre 2019	IS	Revisión del Documento	Chief Information Security Officer (CISO)
1.5	Julio 2020	IS	Actualización del documento	Chief Information Security Officer (CISO)
2.0	Julio 2021	IS	Unificación del formato. Actualización de Referencias Añadir el Anexo de Seguridad de Redes inalámbricas en un punto de la norma	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)

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 los requisitos de seguridad en las redes de comunicaciones del Grupo FCC e interconexión con redes externas, con la finalidad de asegurar la disponibilidad, integridad, confidencialidad, autenticidad, trazabilidad y auditabilidad de la información que se transmite por ellas y de los recursos de información conectados a las mismas.

1.2 Alcance

La Norma se aplica a todas las redes de comunicación del Grupo FCC y de las interconexiones con otras redes tanto públicas como privadas. Las redes de comunicación abarcan tanto las redes cableadas como todas las redes inalámbricas del Grupo FCC.

2. Desarrollo

2.1 Diseño y Desarrollo de la Arquitectura de Red

El diseño y desarrollo de la arquitectura de las redes del Grupo FCC son elementos básicos para la seguridad de las comunicaciones internas y externas de la información. Un correcto diseño, ayudará a la consecución de los objetivos de seguridad y favorecerá un crecimiento futuro de la red.

Los **principios** que deberán ser tenidos en cuenta en el diseño y desarrollo de las redes de comunicación para poder asegurar los niveles de seguridad asignados, son los siguientes:

- El acceso a las redes deberá basarse en criterios de identificación, autenticación y autorización de acceso previa a la conexión, cumpliendo con los principios de "necesidad de conocer" y "mínimo privilegio" establecidos en la Norma de Control de Accesos.
- El diseño deberá considerar la disponibilidad, integridad, confidencialidad, autenticidad, trazabilidad y auditabilidad de la información que circule por ellas.
- Se deberán bloquear todas las conexiones a menos que hayan sido específicamente autorizadas (Principio de control del tráfico).
- Las redes deberán estar operativas y disponibles con carácter ininterrumpido.
- Se deberán utilizar tecnologías dominantes en el mercado, suficientemente probadas en la industria y basadas en estándares.
- La segmentación de la red se deberá realizar en dominios según criterios de sensibilidad (clasificación de la información), tipo de negocio, funcionalidad (Ej.: servidores de aplicación, bases de datos...) y otros que se consideren necesarios.
- Se deberán proteger todas las áreas de servicio o dominios, tanto internamente como a nivel perimetral, mediante tecnologías cortafuegos, que deberán tener establecidas las correspondientes políticas de seguridad y estar toda la actividad monitorizada.
- Se deberá asegurar una alta disponibilidad de todos los componentes de la arquitectura de red perimetral.
- Los servicios accesibles desde redes externas y/o Internet, se deberán realizar a través del despliegue de una zona de intercambio, comúnmente denominada Zona Desmilitarizada (DMZ).
- La seguridad de las redes de comunicaciones del Grupo FCC deberá ser multinivel, abarcando los diferentes tipos de dispositivos que componen las redes, con la finalidad de reducir el impacto de las posibles amenazas que estas pudiesen sufrir.
- Se deberán activar los registros de auditoria en los dispositivos de red en aras de poder analizar e investigar el tráfico de red generado.
- De manera general se deberá mantener actualizada la documentación relativa a los diagramas de redes y los archivos de configuración de los dispositivos.

2.2 Instalación y Configuración de Redes

La configuración de las redes durante las etapas de instalación y mantenimiento es esencial a la hora de conseguir los niveles de seguridad que el Grupo FCC se haya propuesto en cada una de sus redes de comunicación.

La instalación de las redes de comunicación del Grupo FCC tendrá en cuenta los siguientes principios:

- Todos los dispositivos de red estarán ubicados en una zona segura con acceso limitado y controlado de acuerdo con la Norma de Seguridad Física del Grupo FCC.
- Los puntos de conexión entre las redes de comunicaciones del Grupo FCC y, las de los operadores de telecomunicaciones y proveedores de acceso, deberán encontrarse ubicados en entornos seguros con accesos controlados.

La configuración de las redes de comunicaciones tendrá en cuenta los siguientes **principios**:

- Las redes de comunicaciones deberán cumplir con los requisitos de seguridad que se determinen en función de los riesgos definidos y del nivel de clasificación de la información que traten o accedan.
- Todos los dispositivos de red deberán estar protegidos con contraseñas, en conformidad con la Norma de Seguridad en Contraseñas. Las cuentas para los dispositivos de red deberán crearse con el nivel mínimo de privilegios que permita la realización de sus funciones.
- Todas las redes del Grupo FCC deberán seguir el Plan de Direccionamiento del Grupo FCC.
- Las interfaces locales de los enrutadores que conectan con las redes externas deberán configurarse de forma que solo se acepten paquetes de entrada que tengan como destino las direcciones de red que se encuentren dentro del espacio de direcciones de la red interna o redes confiables.
- Las direcciones de red del proveedor de acceso no deberán distribuirse ni anunciarse dentro de la red de comunicaciones del Grupo FCC.
- Los servidores DHCP se deberán configurar de forma que registren los nombres de equipos o dirección MAC de los clientes, así como, que estos registros estén disponibles durante un periodo mínimo de 7 días en el propio servidor y durante el tiempo que establece la directiva de monitorización de seguridad en un sistema de gestión de eventos.
- Se deberán inhabilitar todas las funciones, puertos y servicios excepto aquellos estrictamente necesarios para el funcionamiento operativo de la red.

- Todos los cortafuegos deberán tener configurado el parámetro “denegar por defecto”.
- Todo el tráfico entrante/saliente a/de la red del Grupo FCC deberá pasar a través de cortafuegos y estar monitorizado a través de sistemas de detección y prevención de Intrusiones (IDS/IPS).
- Todo el tráfico saliente, independientemente de su destino, deberá ser filtrado de modo que se verifique que la dirección de origen del paquete pertenece a la red interna local.
- Todo el tráfico saliente hacia redes externas deberá ser analizado mediante mecanismos de prevención de fuga de información, con el fin de detectar envíos de información restringida hacia el exterior de manera no autorizada.
- El tráfico deberá estar cifrado siempre que se transmita información restringida tanto en la red interna como en redes públicas.
- Se deberá monitorizar el tráfico de red, tanto interno como con externo, por medio de:
  - Registros de auditoría de accesos y actividad.
  - Análisis e inspección en tiempo real.
- Los equipos de los usuarios finales conectados a la red interna deberán mantener una dirección IP privada durante toda la sesión, con el objetivo de mantener la trazabilidad de la dirección IP con el usuario.

Donde sea técnicamente posible, las redes de comunicaciones deberán:

- Utilizar un servidor de autenticación que otorgue las credenciales necesarias para el acceso administrativo a todos los dispositivos de red.
- Configurarse de forma que todos los dispositivos de red finalicen la sesión a través del puerto de consola en caso de inactividad prolongada.

2.3 Gestión de Redes

La seguridad asociada a la gestión de las redes de comunicación tendrá que contemplar los siguientes principios:

- Todas las redes de comunicaciones deberán operar y administrarse utilizando procedimientos documentados de forma que permitan un uso eficiente de las mismas y una protección efectiva de la información que circula por ellas.
- La gestión de la configuración, actualización y cambio deberá realizarse siguiendo los procedimientos establecidos, de conformidad con la Norma de Gestión de la Configuración y del Cambio.

- Las redes del Grupo FCC deberán gestionarse por administradores de sistemas debidamente cualificados, que serán responsables de supervisar las tareas diarias de operación y seguridad de los sistemas. Además, las actividades de los administradores de sistemas deberán poder ser auditadas.
- Existirá una red de gestión o administración, separada de la red datos, en la que estarán conectados todos los elementos de comunicaciones principales, y a la que sólo podrán conectarse los administradores de redes y sistemas.
- La conexión y utilización de los componentes de las redes de comunicaciones del Grupo FCC, software y hardware que no hayan sido aprobados expresamente por la División de Sistemas y Tecnologías de la Información del Grupo FCC, en adelante DSTI, está terminantemente prohibida.
- Los cortafuegos deberán estar en ejecución en todo momento y serán administrados de forma centralizada.
- Todos los sistemas deberán estar sincronizados con la misma hora.
- La conexión entre un proveedor de acceso y el Grupo FCC tendrá que cumplir con la Norma de Seguridad de Empresas Externas del Grupo.

2.4 Interconexión de Redes

Las conexiones con redes externas a FCC, así como a sedes del Grupo FCC que no se encuentren integradas dentro de la red corporativa y no compartan los mismos niveles de seguridad, deberán establecerse mecanismos que aseguren la disponibilidad, integridad, confidencialidad, autenticidad, trazabilidad y auditabilidad de la información que circule por cada nodo de las mismas. Con esta finalidad:

- La contratación de servicios de conexión con Internet deberá garantizar el cumplimiento con lo establecido en la Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSICE).
- La conexión entre redes externas y el Grupo FCC deberá realizarse en conformidad con la Norma Seguridad en las Empresas Externas.
- El acceso remoto a los recursos de la red se permitirá exclusivamente a los usuarios autorizados a tal efecto, autenticados al sistema, restringiendo sus privilegios y cifrando los datos si el nivel de clasificación de la información exige esta medida.
- La conexión a cualquier red externa al Grupo FCC y sedes del Grupo FCC no integradas dentro de la red corporativa deberá incluir las siguientes medidas y sistemas de seguridad:

- Pasarela segura de conexión mediante VPN, con mecanismos robustos de autenticación y cifrado, siempre que la conexión sea por una red pública.
- Sistema de Detección de Intrusiones de red externa.
- Enrutador con lista de control de accesos (ACLs).
- Cortafuegos.
- Zona desmilitarizada (DMZ) si fuese necesario el acceso a servicios públicos.
- En conexiones redes externas no podrán compartirse los servidores de Servicio de Nombres (Domain Name Service DNS).
- La interconexión entre la red corporativa y otras sedes del grupo deberá realizarse de tal forma que la red corporativa sea el punto central de protección y gestión, evitando despliegues de cortafuegos en cada sede, excepto en casos que la sede tenga conexión con otras redes no corporativas (Internet, Terceros, etc.).

- De forma general, no estará permitida la contratación de servicios de conexión a redes públicas distintos a los ofrecidos por la DSTI. En aquellos casos que, por causas de negocio justificadas, sea necesaria la contratación de servicios no corporativos, se permitirán dichas conexiones siempre y cuando se implanten las medidas compensatorias que dicte el departamento de SI.

2.5 Seguridad en Redes Inalámbricas

A continuación, se describen los requisitos de seguridad que se deberá implantar en los principios específicos que tendrán que considerarse para las redes inalámbricas y que serán de forma adicionales a los ya descritos en los apartados anteriores.

La **instalación y configuración de redes inalámbricas** del Grupo FCC deberán cumplir con los siguientes principios:

- Los puntos de acceso físicos deberán estar protegidos para prevenir intentos de manipulación. Además, estos equipos deberán estar alejados de fuentes externas que puedan provocar interferencias electromagnéticas.
- La potencia de la señal debe ser la mínima suficiente para cubrir el área física del emplazamiento que quiera dar servicio, con el fin de evitar que la señal llegue con demasiada potencia fuera de las instalaciones. En la medida de lo posible estarán en el centro de la sala y separadas de los muros exteriores y ventanas.
- La información deberá ser cifrada previa a su transmisión, para proteger su confidencialidad, integridad, autenticidad y trazabilidad. El cifrado debe cumplir con los

principios definidos en la Norma de Criptografía (se describe en detalle en el Procedimiento de Cifrado).

- Implementación de sistemas de detección/prevención de intrusos (IDS/IPS) para redes inalámbricas.
- Cambiar el SSID por defecto, por un nombre que no permita identificar la organización.
- En caso de redes inalámbricas de acceso público o para invitados, deberá existir un cortafuegos para separar la red interna cableaba de la red inalámbrica.

El **control de acceso a las redes inalámbricas** de FCC deberá cumplir, además de los principios de la Norma de Control de Acceso, los siguientes principios específicos:

- El protocolo de autenticación para redes inalámbricas deberá estar reconocido por la Industria como seguro (ver Procedimiento de Cifrado).
- La autenticación deberá delegarse a un tercero, nunca en el propio punto de acceso de la red inalámbrica. La autenticación será mutua tanto de cliente como punto de acceso.
- En el caso de redes donde los usuarios almacenan y transmiten información confidencial, el acceso deberá realizarse con certificados u otro mecanismo de autenticación robusto.
- Desconexión automática de clientes con más de 60 minutos inactivos.
- Los dispositivos clientes, antes de la conexión a la red inalámbrica, deberán cumplir con una serie de requisitos (dispositivo autorizado, antivirus actualizado, parches instalados, cortafuegos activado, entre otros).
- El acceso a los puntos de acceso por parte de los administradores deberá realizarse con mecanismos de autenticación robustos. Además, las tareas de administración deberán realizarse “fuera de banda”, mediante una red cableada (cifrado) o en modo local.

Las situaciones de uso **no permitidas** para redes inalámbricas son las siguientes:

- Redes ad-hoc (conexiones directas entre dos o más equipos, sin punto de acceso), en las que al menos uno de los equipos tenga acceso a la red interna o disponga de información confidencial, a no ser que estén justificadas por motivos de negocio y debidamente controladas.
- Puntos de acceso no aprobados por el departamento de SI.

2.5.1 Protocolos de Seguridad para Redes Inalámbricas

Las recomendaciones con relación a los protocolos de autenticación y cifrado para redes inalámbricas realizadas por la Industria (Wifi Alliance) se recogen en el Procedimiento de Cifrado.

2.5.2 Red Inalámbrica para personal interno

2.5.2.1 ALCANCE

La red inalámbrica para personal interno es aquella red dispuesta únicamente para la conexión de ordenadores portátiles corporativos. Estos ordenadores estarán maquetados por la DSTI con la configuración por defecto del Grupo FCC, que incluye los certificados correspondientes de las credenciales del usuario.

2.5.2.2 DIRECTRICES

- Se deberá acceder a esta red únicamente mediante certificado instalado en el equipo y este, deberá estar asociado a las credenciales del empleado interno.
- No deberá ser accesible por colaboradores externos y únicamente será accesible mediante ordenadores portátiles.

2.5.3 Red Inalámbrica de Invitados

2.5.3.1 ALCANCE

Red inalámbrica de invitados es aquella red dispuesta para personas externas al Grupo FCC (proveedores, clientes, etc.), que se encuentran en las instalaciones del Grupo FCC y que requieren conexión a Internet. Esta red no tiene acceso a la red interna.

2.5.3.2 DIRECTRICES

A continuación, se detallan las directrices a seguir para el escenario de redes inalámbricas de invitados:

- Para permitir el acceso de un externo a la red de invitados, un empleado del Grupo FCC deberá crear un acceso registrándolo en el Sponsor Wifi Portal. Se podrá solicitar la conexión tanto para un individuo como para un colectivo, especificando el número de conexiones máxima. En este último caso no será necesario identificar a esos individuos.
- La responsabilidad de uso de la red por el usuario invitado recaerá siempre sobre el empleado que ha creado el acceso.

- La duración máxima de la autenticación del usuario será una jornada laboral. Pasado ese tiempo se revoca automáticamente el acceso. Automáticamente se revocará el acceso a las 24.00 del día en que se realizó la petición.
- Se podrá crear el acceso hasta un máximo de 7 días. Este plazo será ampliable si existe una necesidad de negocio justificada.
- El invitado sólo podrá acceder a esta red, máximo, con 3 dispositivos.
- En todo caso la red inalámbrica para invitados estará separada de la red interna corporativa. Además, los usuarios que accedan a esta red no tendrán visibilidad del resto que estén conectados a la misma.

2.5.4 Red Inalámbrica para acceso de Dispositivos Móviles Corporativos

2.5.4.1 ALCANCE

Red inalámbrica para acceso de dispositivos móviles corporativos es aquella red dispuesta para personal del Grupo FCC que necesite acceso a Internet para el uso en sus dispositivos móviles. Esta red se encuentra separada de la red corporativa y no tiene acceso a la red interna.

2.5.4.2 DIRECTRICES

A continuación, se detallan las directrices para el acceso a redes inalámbricas sin certificado a través de dispositivos móviles corporativos:

- El acceso se permite a todo personal interno del Grupo FCC.
- Para acceder a esta red se deberá solicitar el acceso mediante un formulario o si se tiene instalado un MDM corporativo en su dispositivo.
- Las peticiones de acceso deberán ser tramitadas a través del **Global Service Desk**, que tendrá que realizar las gestiones oportunas para permitirle acceso.
- La duración máxima del acceso a esta red inalámbrica será de 1 año.
- El usuario sólo podrá acceder desde el equipo identificado durante el proceso de registro.
- Durante el primer acceso se le mostrarán al usuario los términos de acceso que tendrán que ser aceptados para poder acceder.
- En todo caso la red inalámbrica para acceso de dispositivos móviles estará separada de la red interna corporativa.

3. Responsabilidades

El departamento de SI deberá:

- Definir las necesidades de la seguridad de las redes de comunicaciones del Grupo FCC.
- Proponer y coordinar la realización de auditorías de red, pruebas de intrusión y escaneo de vulnerabilidades que se consideren oportunas para mantener el nivel de seguridad de las redes de comunicación.
- Informar de las pruebas de vulnerabilidad efectuadas, así como de las acciones realizadas, conclusiones y recomendaciones tras la investigación de cualquier incidente o potencial incidente de seguridad.
- Verificar la implantación y eficacia de los controles y monitorización de seguridad de las redes.
- Monitorizar en tiempo real el tráfico de red para detectar los usos no autorizados, los intentos de intrusiones y el compromiso de cualquiera de los dispositivos de la red.
- Definir las directrices del filtrado web para reducir la exposición a contenido malicioso.

La DSTI deberá:

- Definir y mantener actualizada:
    - La arquitectura de conexión e interconexión de redes y el Plan de Direccionamiento de Red.
    - La topología de la red del Grupo FCC, especialmente la referida a todos los enlaces externos e internos, subredes y equipamiento de red.
- Elaborar los procedimientos para la securización de los elementos de la red.
- Mantener un inventario de elementos de red, entre los cuales estarían los puntos de acceso a redes inalámbricas autorizados.
- Revisar todos los requisitos de las conexiones, al menos semestralmente, para asegurar que siguen vigentes y evaluar la situación de las redes no documentadas descubiertas en las inspecciones.
- Establecer los mecanismos técnicos necesarios para mantener sincronizada la hora de todos los componentes de la red.
- Informar al departamento de SI de cualquier incidente o potencial incidente de seguridad, que afecte a las redes de comunicación de FCC.
- Definir las necesidades de las respectivas áreas de negocio en materia de seguridad de las redes de comunicación de FCC.

Los Usuarios deberán:

- Notificar de forma inmediata a la DSTI acerca de cualquier fallo detectado en los sistemas y/o recursos de la red.
- Utilizar los recursos de la red para fines exclusivamente relacionados con el desempeño de sus funciones dentro de FCC, y en general según lo especificado en el Política de Uso de Medios Tecnológicos, relativo al uso de sistemas a través de la red.

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 accesos	[op.acc.2] Requisitos de acceso
5.37	Procedimientos operativos documentados	[org.3] Procedimientos de Seguridad
8.7	Protección contra malware	[op.exp.6] Protección frente a código dañino
8.10	Eliminación de información	[mp.si.5] Borrado y destrucción
8.20	Seguridad de redes	[mp.com.1] Perímetro seguro
8.21	Seguridad de los servicios de red	[mp.com.2] Protección de la confidencialidad; [mp.com.3] Protección de la integridad y autenticidad
8.22	Segregación de redes	[mp.com.4] Separación de flujos de información en la red
8.23	Filtrado web	[mp.s.3] Protección de la navegación Web
8.24	Uso de criptografía	[op.exp.10] Protección de claves criptográficas; [mp.si.2] Criptografía; [mp.info.3] Firma electrónica
8.27	Arquitectura del sistema seguro y	[op.pl.2] Arquitectura de Seguridad; [mp.sw.1] Desarrollo de aplicaciones

	principios de ingeniería	
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