

Norma de Gestión de Vulnerabilidades de Grupo FCC

Julio 2026

Historial de Versiones				
Versión	**Fecha**	**Autor**	**Detalle**	**Aprobador**
1.0	Julio 2021	SI	Creación del Documento	Chief Information Security Officer (CISO)
1.1	Junio 2024	SI	Revisión documento	Chief Information Security Officer (CISO)
1.2	Julio 2025	SI	Revisión del documento y adaptación a normativa ISO27001:2022 y ENS	Chief Information Security Officer (CISO)
2.0	Julio 2026	SI	Revisión del documento y cambio de formato	Chief Information Security Officer (CISO)

ÍNDICE

1. Introducción....4

1.1 Objeto....4

1.2 Alcance....4

2. Contenido....5

2.1 Principios....5

2.2 Identificación de activos y alcance....6

2.3 Escaneo de activos....7

2.4 Categorización....8

2.5 Reporte....9

2.6 Remediación....10

2.6.1 Parcheado....10

2.6.2 Excepciones....11

2.7 Reevaluación....11

3. Responsabilidades....12

4. Referencia normativa....14

4.1 Controles de la normativa ISO27001:2022 y ENS....14

1. Introducción

El Grupo FCC cuenta con una amplia infraestructura tecnológica, así como con un elevado número de Sistemas de Información. Éstos están interconectados entre sí, en ocasiones, incluso, con otros Sistemas de Información de terceros, pudiendo ser accesibles tanto desde redes públicas como desde redes privadas. En ocasiones, los activos de información pueden tener debilidades que pueden ser explotadas por agentes maliciosos con el fin de actuar contra la seguridad de los datos y la información de la Organización. La cultura de ciberseguridad del Grupo FCC se sustenta en el principio de prudencia y asume la inexistencia del riesgo cero cuando se trata de amenazas que atenten la seguridad de la información. Por este motivo, para Grupo FCC se hace imprescindible contar con una política y un proceso establecido de gestión de las debilidades o vulnerabilidades de los activos de información de la organización.

La elaboración de esta norma de gestión de vulnerabilidades responde a la necesidad de regular internamente los objetivos, las actividades y las responsabilidades del personal y los sistemas involucrados en la seguridad de la información del Grupo en cuanto a la detección, tratamiento y resolución de las vulnerabilidades técnicas presentes en las Redes, la Infraestructura y los Sistemas de Información de Grupo FCC.

Esta Norma se enmarca en el cuerpo normativo de Seguridad de la Información de Grupo FCC para dar cobertura a los equipos involucrados en la identificación, el seguimiento y la corrección de vulnerabilidades técnicas.

1.1 Objeto

La presente Norma tiene por objeto establecer los criterios que deben cumplirse en materia de ciberseguridad en los procesos de gestión de vulnerabilidades en aras de garantizar la confidencialidad, integridad, autenticidad, trazabilidad y disponibilidad de los activos de información (propios o de terceros), así como el cumplimiento de los requerimientos regulatorios vigentes que sean de aplicación.

1.2 Alcance

Esta Norma aplica a todas las empresas del grupo con participación mayoritaria, así como a aquellas empresas o entidades sobre las que el grupo tenga la responsabilidad de su operación y/o gestión.

Se aplica a todo activo de información, de red o de infraestructura que tenga alguna implicación o vinculación con Grupo FCC, ya sea propio o de un tercero que presta un servicio al Grupo.

2. Contenido

2.1 Principios

La gestión de vulnerabilidades en Grupo FCC se sustenta en los siguientes principios:

- La gestión de vulnerabilidades es un proceso continuo.
- Se entiende por vulnerabilidad técnica la debilidad de un activo o ausencia de control que puede ser usada por un atacante para dañar o tomar control sobre el mismo.
- Se establecen medidas técnicas y organizativas para identificar las vulnerabilidades en los activos de información, de red y de infraestructura que afectan a los Negocios de Grupo FCC.
- Las vulnerabilidades se clasifican y se prioriza su resolución de acuerdo con su criticidad o nivel de riesgo.
- Toda vulnerabilidad debe quedar registrada y se documentará todo el proceso hasta su resolución, ya sea mediante la aplicación de acciones correctoras que mitiguen el riesgo o mediante la aceptación formal del riesgo cuando esta sea la opción aprobada.
- Las vulnerabilidades identificadas serán gestionadas de acuerdo con su nivel de criticidad y riesgo para Grupo FCC, definiéndose en cada caso las acciones correctoras o mitigadoras, así como los plazos de resolución correspondientes. Excepcionalmente, cuando tras su análisis y evaluación se considere oportuno, el riesgo asociado podrá ser formalmente aceptado por la DSIGRT de acuerdo con el procedimiento establecido (2.6.2 Excepciones).
- Se comunica a las partes interesadas la identificación de una vulnerabilidad técnica y se informa periódicamente del estado de su resolución.
- Cuando la legislación vigente así lo requiera, se deberá notificar la existencia de vulnerabilidades críticas, así como aportar la información que se requiera para cumplir con la regulación que aplique en cada caso.
- Se realizarán análisis periódicos de los Sistemas, Redes e Infraestructuras tecnológicas para la detección de vulnerabilidades, de acuerdo con el ciclo de parcheo establecido por los fabricantes y con una frecuencia determinada por la criticidad de cada activo.
- Se analizan los Sistemas de Información para detectar vulnerabilidades técnicas de forma previa a su puesta en producción.
- Se analizan los Sistemas de Información para detectar vulnerabilidades técnicas de forma previa a la puesta en producción de cambios significativos.
- Aun cuando la infraestructura sea ajena a entidades de Grupo FCC, pero ésta contenga información propiedad o responsabilidad del Grupo o pueda afectar a las Redes y/o Sistemas de Información del Grupo, se debe asegurar la realización periódica de análisis de vulnerabilidades.
- Los análisis son realizados con herramientas automatizadas actualizadas o de forma manual.
- Los análisis son formal y debidamente documentados.

- Los análisis son correspondientemente comunicados a las partes implicadas y/o interesadas, incluyendo las autoridades públicas o privadas que exija la ley que aplique en cada caso.
- Antes de la implantación de una acción correctora, se realizan pruebas para asegurar que dicha acción no afecta negativamente a ningún Sistema y no compromete los controles de seguridad implantados.
- Todos los sistemas contaran con la última versión estable con la intención de minimizar la exposición de los sistemas a las vulnerabilidades altas y críticas reportadas por los fabricantes.

2.2 Identificación de activos y alcance

La identificación de activos del GRUPO FCC y definición del alcance de los análisis de vulnerabilidades tendrá que contemplar los siguientes principios:

- La gestión de vulnerabilidades tendrá bajo alcance todo servidor, desktop e infraestructura perteneciente o gestionada por el GRUPO FCC, incluidos los activos gestionados por terceras partes.
- Todo servidor y equipo bajo el alcance de la presente norma deberá estar incluido en una CMDB la cual debe ser revisada con una periodicidad no mayor a un mes.
- Todo servidor y equipo previo a su puesta en producción o entrega a usuario final deberá ser añadido a la CMDB mencionada en el punto anterior y ser preparado para la realización de escaneos de vulnerabilidades.
- Toda aplicación que cumpla alguna de los siguientes parámetros deberá ser sometida a un análisis de vulnerabilidades:
    - Aplicaciones que traten datos personales.
    - Aplicaciones que traten información confidencial o secreta.
    - Aplicaciones categorizadas como críticas por las líneas de negocio.
    - Aplicaciones expuestas a internet.
    - Aplicaciones con un alto riesgo reputacional en caso de incidente.

2.3 Escaneo de activos

Los escaneos de vulnerabilidades del GRUPO FCC tendrán que contemplar los siguientes principios:

- Los escaneos de vulnerabilidades sobre servidores y equipos de usuarios finales se llevarán a cabo automáticamente con una periodicidad acorde a la normativa vigente pero nunca superior al mes.
- Se deberá realizar un análisis de vulnerabilidades sobre toda aplicación que cumpla alguna de las siguientes condiciones:
    - Se ha realizado un cambio en el código de la aplicación.
    - Se ha realizado un cambio en la configuración de la aplicación o de la infraestructura donde se aloja.
    - Se ha incluido o excluido un módulo, plugin o API.
    - Se ha realizado una migración de la aplicación.
    - Se ha modificado el hardware donde se aloja la aplicación.
    - Se sospecha de la existencia de una vulnerabilidad.
    - La normativa vigente lo solicite.
- Los escaneos sobre aplicaciones se realizarán bajo petición y se deberá proporcionar por lo menos la siguiente información:
    - Nombre de la aplicación.
    - Responsable de la aplicación.
    - Línea de negocio a la que pertenece la aplicación.
    - Tipo de análisis a realizar: análisis dinámico (DAST) o estático (SAST)
    - Para los análisis de tipo DAST se deberá proporcionar los enlaces e instrucciones de acceso necesarios para llevar a cabo el análisis.
    - Para los análisis de tipo SAST se deberá proporcionar el código fuente de la aplicación y las instrucciones para su compilación.
    - Credenciales en caso de que sean necesarias.
    - Información que se considere de necesidad para la realización del análisis de vulnerabilidades.
- Los escaneos sobre infraestructura pertenecientes al GRUPO FCC se realizarán bajo demanda.
- Se le asignará una fecha de inicio a todos los escaneos solicitados bajo demanda.

2.4 Categorización

La categorización de las vulnerabilidades encontradas durante los escaneos del GRUPO FCC deberá contemplar los siguientes principios:

- La categorización de las vulnerabilidades se realizará considerando factores como:
  - La severidad asociada al CVE o CVSS.
  - La probabilidad de explotación.
  - La exposición del activo afectado.
  - La criticidad del activo.
  - El impacto potencial sobre el negocio.

- En función de la evaluación realizada sobre los criterios anteriores, las vulnerabilidades se clasificarán de mayor a menor criticidad en las siguientes categorías:
  - Crítica.
  - Alta.
  - Media.
  - Baja.
  - Informativa.

2.5 Reporte

El reporte de las vulnerabilidades encontradas durante los escaneos de vulnerabilidades del GRUPO FCC tendrán que contemplar los siguientes principios:

- Las vulnerabilidades críticas, las vulnerabilidades de tipo 0-day o aquellas para las que exista evidencia de explotación activa deberán ser comunicadas mediante alerta temprana a los responsables del activo afectado y a la DSIGRT para su evaluación y gestión prioritaria.
- Las vulnerabilidades encontradas durante análisis periódicos y automatizados se reportarán mediante un informe acordado con la DSIGRT y deberá tener al menos la siguiente información:
    - Activo afectado. Se indicará el hostname del activo afectado.
    - Nombre de la vulnerabilidad y detalle.
    - CVSS y criticidad de la vulnerabilidad.
    - Fecha de la última detección.
    - Impacto de la vulnerabilidad
    - Solución de la vulnerabilidad con recomendaciones del fabricante en caso necesario.
- Tras la realización de un análisis de vulnerabilidades solicitado bajo demanda se entregará un informe técnico con el detalle de las vulnerabilidades identificadas. Adicionalmente, cuando los resultados deban ser presentados a la Dirección, personal de Negocio o cuando el activo analizado se encuentre auditado bajo alguna certificación de seguridad, se elaborará un informe ejecutivo.
    - Informe técnico que contiene una descripción detallada de las vulnerabilidades encontradas:
        - Nombre de la vulnerabilidad.
        - CVSS y criticidad.
        - Posible impacto en caso de explotación de la vulnerabilidad.
        - Recomendaciones para la resolución de la vulnerabilidad.
        - Comentarios respecto a la vulnerabilidad.
        - Estado actual de la vulnerabilidad.
    - Informe ejecutivo que contiene:
        - Alcance del análisis.
        - Descripción del análisis.
        - Valoración de riesgo de la aplicación.
        - División de vulnerabilidades por criticidad, tipo y estado.

2.6 Remediación

2.6.1 Parcheado

El parcheado de las vulnerabilidades encontradas durante los escaneos de vulnerabilidades del GRUPO FCC tendrán que contemplar los siguientes principios:

- Se deberán establecer planes de acción para corregir las vulnerabilidades identificadas.
- Los planes de acción deberán incluir las vulnerabilidades identificadas, las acciones de remediación definidas, los responsables de su ejecución y los plazos previstos para su resolución.
- La implementación de parches o actualizaciones de aplicaciones en equipos se realizará siempre por oleadas.
- La primera oleada de parcheo a equipos se realizará a un grupo reducido con la intención de probar dicho parcheo. Las siguientes oleadas se llevarán a cabo incrementalmente sobre equipos con distintas casuísticas. Una oleada se implementará si y solo si la anterior oleada ha sido implementada con éxito y no se han encontrado problemas.
- Se considerarán parches urgentes aquellos destinados a corregir vulnerabilidades explotadas activamente, vulnerabilidades de tipo 0-day o vulnerabilidades que, por su nivel de riesgo, requieran una actuación acelerada. La implementación de estos parches tendrá una duración máxima de una quincena.
- Los parches de sistema operativo para servidores Windows se aplicarán mensualmente.
- Los parches de sistema operativo para servidores Linux se aplicarán trimestralmente.
- El seguimiento del cumplimiento de los plazos de remediación será realizado de forma periódica por la Oficina Técnica de DSIGRT.
- Los tiempos de implementación de parches para las vulnerabilidades detectadas en ejercicios DAST o SAST, en función de su criticidad son:
    - Crítica: 2 semanas.
    - Alta: 1 mes.
    - Media: 3 meses.
    - Baja: 6 meses.
    - Informativa: no cuenta con un tiempo de mitigación.
- Las vulnerabilidades que superen los plazos de remediación establecidos deberán ser reportadas al responsable del activo afectado para su regularización o, en caso de ser apropiado, para la aceptación formal del riesgo.

2.6.2 Excepciones

En aquellos casos en los que no es posible cumplir con los requisitos de esta norma, se debe dejar documentado las excepciones acordadas, siguiendo los siguientes principios:

- Para las vulnerabilidades que no pueden ser mitigadas en los plazos que establece esta norma por motivos de complejidad, disponibilidad de equipos o ventana de implementación, se acuerda con la DSIGRT el nuevo plazo de implementación de las contramedidas.

- Para las vulnerabilidades que no sean mitigadas se redacta una carta de asunción de riesgos y se almacena la carta firmada por el responsable del sistema en cuestión.

2.7 Reevaluación

La reevaluación para comprobar las mitigaciones de las vulnerabilidades encontradas durante los escaneos de vulnerabilidades del GRUPO FCC tendrán que contemplar los siguientes principios:

- Tras la mitigación de una vulnerabilidad se deberá realizar un escaneo mediante un nuevo análisis del activo. Este escaneo deberá ser solicitado por el responsable del activo y el análisis deberá tener el mismo alcance.
- Una vulnerabilidad no podrá considerarse resuelta hasta que las medidas de remediación implantadas hayan sido verificadas mediante una reevaluación satisfactoria.

3. Responsabilidades

El departamento de SI deberá:

- Verificar la adecuada implantación de la presente Norma.
- Definir y supervisar el proceso de gestión de vulnerabilidades.
- Consolidar los registros de vulnerabilidades técnicas de los diferentes Negocios del Grupo, en aras de mantener una base de datos común de debilidades técnicas en el entorno tecnológico de Grupo FCC.
- Realizar un seguimiento periódico del conjunto de vulnerabilidades técnicas existentes en el entorno tecnológico de Grupo FCC
- Notificar periódicamente del estado del arte de la gestión de vulnerabilidades en Grupo FCC a las unidades implicadas e interesadas.
- Comunicar a las unidades y entidades oportunas la existencia de vulnerabilidades críticas que supongan un alto riesgo de seguridad para la organización y garantizar que se toman las medidas apropiadas para su mitigación.

La División de Sistemas y Tecnología de la Información, en adelante DSTI deberá:

- Coordinar, planificar y, en su caso, ejecutar el proceso de monitorización e identificación de vulnerabilidades técnicas en los activos de información de Grupo FCC.
- Disponer, proporcionar y mantener la infraestructura, tecnologías y/o herramientas que faciliten una adecuada gestión de vulnerabilidades en las entidades del Grupo FCC.
- Establecer y mantener contacto con autoridades, instituciones, círculos empresariales y grupos de trabajo, públicos y privados, activamente involucrados en la identificación y evaluación de nuevas vulnerabilidades técnicas en el sector, para mantener una base de conocimiento actualizada en torno a las vulnerabilidades que puedan afectar a los Sistemas, Redes e Infraestructuras tecnológicas de Grupo FCC.

Las Unidades de Negocio de Grupo FCC son responsables de:

- Ser receptores de los diversos reportes emitidos por el equipo de identificación de debilidades técnicas y por el servicio de Ciberinteligencia y analizar su información para la toma de decisiones, así como para la implantación de medidas técnicas y/o organizativas relacionadas con la corrección de dichas debilidades.
- Realizar, o solicitar un análisis de vulnerabilidades en los sistemas de información de nueva implantación previo a su puesta en producción.
- Realizar, o solicitar un análisis de vulnerabilidades técnicas de forma previa a la puesta en producción de cambios significativos en sistemas de información ya existentes.
- Corregir las vulnerabilidades que afectan a sus activos y sistemas de información cumpliendo los plazos estipulados al efecto.

- Garantizar la adecuada gestión de vulnerabilidades en los activos de información de terceros que tenga cualquier tipo de afectación o impacto, independientemente del grado y el modo, en la infraestructura, las redes y/o los sistemas de información en uso en su Unidad de Negocio.
- Informar periódicamente a la DSIGRT del estado de resolución de las vulnerabilidades técnicas identificadas, así como de las actividades planificadas para su correcta resolución.
- Notificar a la DSIGRT de la existencia o identificación de debilidades técnicas identificadas por vías alternativas al servicio de identificación de vulnerabilidades establecido por la DSIGRT.
- Informar a la DSIGRT de sus necesidades en lo que respecta a la gestión de vulnerabilidades de sus sistemas específicos.

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
5.5	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
5.9	Inventario de información y otros activos asociados	[op.exp.1] Inventario de activos; [op.pl.2] Arquitectura de Seguridad
8.8	Gestión de vulnerabilidades técnicas	[op.mon.3] Vigilancia; [op.exp.4] Mantenimiento y actualizaciones de seguridad
8.15	Registro de eventos	[op.exp.8] Registro de la actividad
8.16	Seguimiento de actividades	[op.mon.3] Vigilancia; [mp.s.4] Protección frente a DoS
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