Norma de Gestión de Incidentes

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)
	Agosto 2019	IS	Actualización del Documento	Chief Information Security Officer (CISO)
2.1	Julio 2020	IS	Actualización del Documento	Chief Information Security Officer (CISO)
2.2	Julio 2021	IS	Unificación del formato con el resto de la normativa ISO27001:2017 Actualización de Referencias	Chief Information Security Officer (CISO)
2.3	Mayo 2024	IS	Actualización del documento en base a la normativa ISO27001:2022	Chief Information Security Officer (CISO)
2.4	Julio 2025	IS	Actualización del documento en base 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 establece los criterios necesarios para la realización de acciones destinadas a resolver cualquier incidente de seguridad de una forma rápida y efectiva, reduciendo o anulando el impacto, potencial o real, que dicho incidente pudiera tener sobre el negocio del Grupo FCC.

1.2 Alcance

Esta Norma es de aplicación sobre cualquier incidente de seguridad, materializado o en grado de tentativa, que se realice en los sistemas o instalaciones del Grupo FCC, independientemente del lugar donde se encuentre y de los recursos o la información a los que afecte.

La presente Norma también aplica a todo el personal interno o colaborador y sistema de información involucrado en el propio incidente de seguridad descrito anteriormente.

2. Seguridad en la Gestión de Incidentes

2.1 Principios

La Gestión de Incidentes no debe confundirse con la Gestión de Incidencias o Problemas, pues a diferencia de esta última, no se centra en encontrar y analizar las causas subyacentes de una incidencia concreta de hardware o de software, sino que, en lo referente al presente documento, se pretende definir exclusivamente la restauración de la actividad de los servicios de tecnologías de la información.

La presente Norma establece las actividades relacionadas con la detección, evaluación y resolución de un incidente de seguridad de la información, mientras que los procesos que rigen la recuperación de la actividad después de producirse incidentes de esta índole serán desarrollados en los documentos correspondientes que pueda elaborar FCC.

- La gestión de un incidente de seguridad de la información deberá comprender todas las fases de su ciclo de vida, desde que se tiene sospecha o conocimiento de su existencia, hasta su resolución, registro y puesta en marcha de las acciones correctivas derivadas del análisis de sus causas.
- En caso de sospecha de que un incidente se esté produciendo, se asumirá su certeza hasta que se constate que no se trata de uno de ellos.
- Cuando no se tenga una evaluación razonable del impacto que pueda tener un incidente, se asumirá el peor escenario posible hasta que se realice un análisis más pormenorizado.
- La fijación de prioridades cuando se produzcan incidentes concurrentes se basará en la seriedad o criticidad de los mismos para el negocio de FCC o para el usuario.
- Cuando el tipo de incidente no esté recogido en el acuerdo de nivel de servicio correspondiente, la prioridad de actuación se evaluará de la forma más objetiva posible basándose en el impacto o en la urgencia o demora aceptable en la operativa del proceso de negocio.
- La participación en las diferentes etapas que conforman el ciclo de resolución de la Gestión de Incidentes y de los Planes de Respuesta dependerá de la responsabilidad asignada en función a los roles y responsabilidades definidos a tal efecto.
- El personal de FCC deberá estar familiarizado con los procedimientos relativos a la Gestión de Incidentes de cada una de las áreas de seguridad en la que tenga responsabilidades, con la finalidad de que la gestión de los incidentes sea la más eficaz posible.

- El nivel de clasificación de la Información de FCC determinará el grado de desarrollo de las medidas de seguridad necesarias para prevenir, detectar y corregir incidentes que afectaran a la seguridad de esta información.
- Existe un Procedimiento de Gestión y Notificación de Brechas de Seguridad de los Datos Personales para aquellos incidentes de seguridad que afecten a datos personales de alguna de las sociedades que integra el Grupo FCC. Este Procedimiento regula la notificación, gestión y respuesta ante aquéllos incidentes que pudieran afectar a la seguridad de los datos personales, cuyo tratamiento es responsabilidad de dichas sociedades.
- Cualquier incidente que implique pérdida de la confidencialidad de la Información de FCC manejada por Empresas ajenas al Grupo, deberá de ser informada lo más rápidamente posible al departamento de SI en conformidad con la Norma Empresas Externas.

Cuando sea técnicamente posible, se deberá:

- Configurar los sistemas y aplicaciones para detectar y notificar incidentes y/o alertas de forma automática.
- Monitorizar, escanear y establecer patrones de comportamiento de los sistemas para la pronta detección de cualquier anomalía en el comportamiento de los sistemas de información.
- Disponer de un registro de las firmas de los archivos de sistema y de las aplicaciones, que permita una rápida comprobación de la integridad de estos.

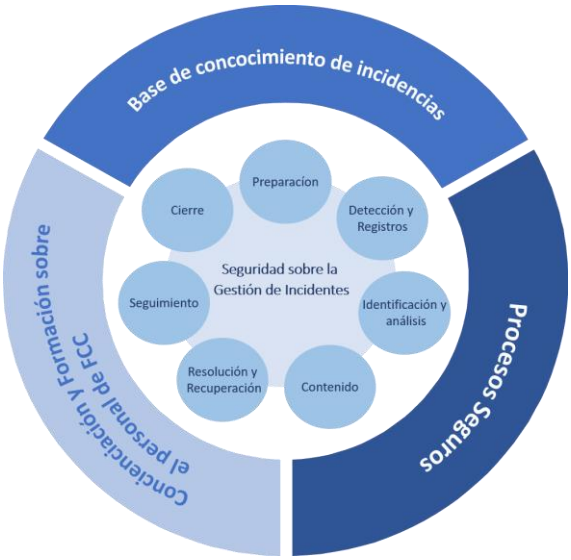

Figura 1: *Principios de Gestión de Incidentes*

2.2 Preparación previa ante incidentes

La capacidad de respuesta de FCC ante incidentes de seguridad dependerá en gran medida de su capacidad para prevenir, de la preparación de las acciones de respuesta y la agilidad para ejecutarlas en el momento que ocurra el incidente.

Además del establecimiento de los controles de seguridad sobre los sistemas, redes y aplicaciones del Grupo, es necesario que se consideren todas aquellas acciones formativas, logísticas y técnicas que faciliten una respuesta rápida, efectiva y eficiente ante los incidentes de seguridad que se puedan producir.

La experiencia, organización y conocimiento de los servicios de tecnologías de la información y de las amenazas a las que estos se enfrentan son claves para una Gestión de Incidentes que minimice los impactos en los procesos de negocio, de ahí que el departamento de seguridad de la información de FCC y los demás departamentos implicados en esta gestión deban tener definido:

- La elaboración de una tipología de posibles incidentes para cada sistema concreto y de los riesgos asumibles en cada escenario.
- La elaboración de un Plan de Respuesta ante Incidentes para cada escenario definido.
- La definición de las combinaciones de indicadores o precursores que generen las señales necesarias para concluir que se puede estar materializando un incidente.
- La asignación de funciones y tareas para cada tipo de incidente previsto.
- La formación técnica y legal, concretamente sobre las implicaciones y la vulneración de derechos a la intimidad que se puedan derivar de las tareas asociadas a la resolución de incidentes.
- La asignación de la disponibilidad de los recursos técnicos y profesionales destinados a la resolución de incidentes.

2.3 Detección y registro de incidentes.

- Cualquier incidente de seguridad de la información de cuya existencia se tuviera sospecha, duda o conocimiento deberá notificarse, con suficiente detalle y urgencia.
- El departamento de SI se encargará de convocar a los miembros del Equipo de Gestión de Incidentes que intervendrán, total o parcialmente, en las actividades de gestión del mismo.

- El Equipo de Gestión de Incidentes estará integrado, por un miembro del departamento de SI, los responsable/s de la información que se vea afectada por el incidente y el DPO, en el caso de que se vean afectados datos de carácter personal.
- La existencia de un incidente de seguridad dentro de los sistemas de información podrá ser detectada e informada por el personal interno o colaborador del Grupo FCC.
- El personal interno o colaborador del Grupo FCC que sospeche o descubra un posible incidente no realizará ninguna otra acción diferente a la comunicación del incidente de forma inmediata a los responsables técnicos, al departamento de SI o al servicio de atención al usuario (Global ServiceDesk), ante cualquier sospecha de la existencia de un incidente de seguridad
- Los responsables de la Gestión de Incidentes, como punto de contacto del Grupo FCC en materia de incidentes relativos a la seguridad de la información, deberán encontrarse disponibles y ser capaces de ofrecer respuestas adecuadas y oportunas.
- Una vez identificados como tales, todos los incidentes relativos a la seguridad de la información deberán de ser registrados y clasificados por el departamento de SI. La clasificación del incidente se establece en función de la severidad o el impacto potencial que resulte del análisis preliminar que se realice del mismo.
- El mantenimiento de este registro resulta imprescindible para analizar los posibles ataques a los sistemas y activos de información del Grupo FCC, así como para identificar a los responsables de los mismos.
- Los procedimientos que desarrollen la presente Norma deberán establecer el contenido mínimo de la información que, sobre un incidente, deba ser registrada.
- Cuando los incidentes afectaran a la seguridad de datos de carácter personal propiedad de FCC, se deberá seguir el Procedimiento de Gestión y Notificación de Brechas de Seguridad de los Datos Personales.

2.4 Identificación y análisis de incidentes

- Los incidentes registrados deberán ser identificados y evaluados para determinar su impacto sobre la actividad normal de los procesos de negocio.
- Para la evaluación de este impacto se tomará como referencia la criticidad de los activos y procesos de negocio afectados en función del tiempo previsto de inactividad y los costes asociados.

- Cuando la información notificada del incidente no fuera suficiente para llevar a cabo su evaluación y clasificación, el departamento de SI o, en su defecto, los Responsables de la Información podrán emprender las acciones que consideren oportunas para ampliar la información sobre el incidente.
- La gestión del incidente comenzará con la realización de un rápido análisis de la situación para determinar el alcance del incidente, las causas que lo produjeron y el escenario en que se está desarrollando.
- Como paso previo a la aplicación de las medidas de contención, respuesta o recuperación que deban adoptarse ante un incidente de seguridad, se deberá determinar si se puede identificar algún incidente similar ya resuelto para establecer medidas análogas.
- Los incidentes que estén sucediendo al mismo tiempo se priorizarán según su gravedad. El criterio para realizar esta evaluación de prioridades de ejecución será el ya indicado de nivel de criticidad de la información para los procesos de negocio.
- Una vez evaluada la prioridad de un incidente de seguridad, se pondrán en marcha los procedimientos de gestión relativos al incidente concreto y se documentarán convenientemente todos los pasos que se vayan realizando.
- Una vez analizado y priorizado, el incidente deberá ser notificado a las funciones o personas de FCC, de empresas externas y/o terceras partes interesadas.
- Siempre que tecnológicamente sea posible, los registros y la documentación relativa a la gestión de incidentes seguirán un formato común y uniforme, con consolidación de entradas y una política de conservación única con motivo de que puedan ser aceptadas por cualquier entidad legal nacional u otro foro disciplinario.

2.5 Contención de incidentes

- Una vez identificado el incidente, el Equipo de Gestión de Incidentes deberá tomar la decisión de si se procede a contener el incidente para evitar que aumente el impacto del mismo.
- Para esto, si procede, deberá valorar cómo asegurar la validez de la cadena de custodia de las evidencias para su posterior presentación con finalidad legal o disciplinaria y qué implicaciones tiene en términos de riesgo.
- La puesta en marcha del Plan de Respuesta ante Incidentes supondrá la implantación de una estrategia de contención para cada incidente concreto.

- Los procedimientos de Respuesta ante Incidentes deberán garantizar la segregación de tareas y el control dual, para reforzar la integridad de las evidencias obtenidas.

2.6 Resolución y recuperación de incidentes

Tras la resolución de un incidente, el responsable de la gestión deberá asegurarse:

- Que todos los sistemas afectados han sido debidamente saneados.
- Que la probabilidad de un incidente futuro de similares características se ha minimizado.
- Que se han revisado los controles de seguridad con la finalidad de evaluar la necesidad de corregirlos, ampliarlos o establecer nuevos controles.
- Que se ha registrado el incidente con su análisis, evaluación y estrategia de contención concreta.

Durante la recuperación, las actuaciones se guiarán por los procedimientos operativos que los responsables de Servicios de Tecnologías de la Información hayan aprobado.

2.7 Cierre de incidentes

- Una vez que los sistemas han vuelto a su operativa normal, el Equipo de Gestión de Incidentes procederá a notificar esta situación a todas las partes interesadas, así como a las funciones y departamentos implicados en el mismo.
- El cierre del incidente incluirá la verificación de que la información recogida sobre el mismo es suficiente para conocer adecuadamente cuál ha sido su evolución, la efectividad de las medidas adoptadas y el tiempo invertido en su resolución.
- Se deberá velar por que el origen del incidente es inequívocamente identificado y por la incorporación o actualización de los controles que mitiguen la amenaza que ha originado dicho incidente.
- En el proceso de cierre del incidente, se deberá revisar la clasificación original del incidente, actualizándola en caso de identificar que las características del incidente no se ajustan a la clasificación original.
- Tras el cierre de un incidente será conveniente realizar una evaluación de la gestión del incidente con el objetivo de valorar la completitud y madurez del proceso actual y extraer un listado de lecciones aprendidas que permitan realimentar y mejorar el modelo de gestión de incidentes vigente.

- Tras el cierre formal del incidente, se fomentará la transferencia de conocimiento obtenida durante la gestión de incidentes para capacitar a los empleados y colaboradores del grupo FCC en caso de que ocurran situaciones parecidas en el futuro.

2.8 Seguimiento de incidentes

- La información obtenida de los incidentes de seguridad de la información deberá ser documentada, de cara a poder identificar aquellos que sean recurrentes o de alto impacto. De su estudio, se podrá concluir la necesidad de mejorar o agregar controles que limiten la frecuencia y el daño de casos futuros.
- Equipo de Gestión de Incidentes deberá, dada la rápida evolución tecnológica de los sistemas de información, mantener reuniones periódicas para comentar los escenarios de nuevas amenazas.
- Este equipo se reunirá después de que se hayan producido incidentes relevantes, o que supongan nuevas técnicas de ataque, con la finalidad de proceder al análisis de los mismos y a la búsqueda de mejoras en las medidas de seguridad de la información implantadas.
- La información obtenida de las reuniones deberá permitir establecer mejoras en los procesos de gestión de incidentes, en las políticas y procedimientos de Seguridad de la Información y dotar de nuevos contenidos a los programas de formación en Seguridad de la Información tanto a nivel de usuarios como de personal técnico.

3. Responsabilidades

El departamento de SI deberá:

- Identificar cualquier incidente de seguridad durante las actividades de monitorización que realice sobre los sistemas críticos que supervisa.
- Revisar periódicamente los registros de auditoría en busca de evidencias o indicios de comportamientos sospechosos.
- Supervisar la resolución de los incidentes de seguridad de la información, así como de la puesta en marcha de las medidas correctivas o preventivas que se pudieran adoptar.
- Elevar informes de situación sobre la resolución de incidentes a la Alta Dirección del Grupo FCC.

- Mantener relaciones con todas las organizaciones y representantes legales que puedan cooperar en la resolución de los incidentes de seguridad. Elaborar y actualizar los Planes de Respuesta ante Incidentes.
- Promover que el personal técnico de FCC recibe formación y entrenamiento suficientes en materia de Gestión de Incidentes, de forma que la identificación y notificación de los mismos pueda realizarse de la forma más eficaz posible.
- Realizar las pruebas de verificación de los procedimientos de Gestión de Incidentes y de los Planes de Respuesta e identificar carencias en los mismos.

El Equipo de Gestión de Incidentes de seguridad tendrá como responsabilidad:

- Coordinar las partes interesadas durante la gestión del incidente
- Comunicar periódicamente a los interesados el estado de resolución del incidente, así como los daños e impacto producidos por el mismo.
- Gestionar eficazmente los recursos profesionales y materiales que se pongan a su cargo para la resolución del incidente.
- Tomar las decisiones que conduzcan a la resolución del incidente de acuerdo con los niveles de servicios previos a su aparición.
- Clasificar, o en caso necesario, reclasificar el incidente, de acuerdo a los criterios de clasificación de incidentes establecido.
- Coordinar la activación del Plan de Continuidad cuando sea necesario.

Los responsables de la Información tendrán que:

- Asegurar que todo el personal que accede a información bajo su responsabilidad ha recibido la formación necesaria para reconocer y reaccionar ante cualquier incidente de seguridad.
- Asegurar que se han asignado, comunicado y comprendido los roles y responsabilidades en la gestión de incidentes que afecten a los activos de información de los que son responsables.
- Cooperar con los responsables de la Gestión de Incidentes en la resolución de los mismos y proporcionar aquella información que se les pudiese demandar.

Los usuarios deberán:

- Notificar de forma inmediata a los responsables técnicos, al departamento de SI o al servicio de atención al usuario (*Global ServiceDesk*), ante cualquier sospecha de la existencia de un incidente de seguridad.

- Mantener una actitud vigilante para la identificación de cualquier incidente de seguridad.

En función de la tipología del incidente, también se podrá requerir la colaboración de otras áreas o departamentos como Legal, Recursos Humanos, Marketing, etc.

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
5.24	Planificación y preparación de la gestión de incidentes de seguridad de la información	[op.exp.7] Gestión de Incidentes
5.25	Evaluación y decisión sobre eventos de seguridad de la información	[op.exp.7] Gestión de Incidentes
5.26	Respuesta a incidentes de seguridad de la información	[op.exp.9] Registro de la Gestión de Incidentes
5.27	Aprendiendo de los incidentes de seguridad de la información	[op.exp.7] Gestión de Incidentes; [op.exp.9] Registro de la Gestión de Incidentes
5.28	Recopilación de pruebas	[op.exp.7] Gestión de Incidentes; [op.exp.9] Registro de la Gestión de Incidentes
5.29	Seguridad de la información durante la disrupción	[op.cont.1] Análisis de Impacto; [op.cont.2] Plan de Continuidad
6.8	Reporte de eventos de seguridad de la información	[op.exp.7] Gestión de Incidentes
8.34	Protección de los sistemas de información durante las pruebas de auditoría	[op.exp.2] Configuración de Seguridad; [op.exp.3] Gestión de la Configuración; [op.exp.4] Mantenimiento y Actualizaciones de Seguridad; [mp.s.2] Protección de servicios y aplicaciones Web