

Norma de Monitorización de Seguridad de la Información

Junio 2026

Historial de Versiones				
Versión	**Fecha**	**Autor**	**Detalle**	**Aprobador**
1.0	Julio 2025	IS	Creación del Documento	Chief Information Security Officer (CISO)
1.1	Enero 2026	IS	Revisión del Documento Tiempo de retención de logs modificado	Chief Information Security Officer (CISO)
2.0	Junio 2026	IS	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. Gestión de Eventos de Seguridad de la Información 5

2.1 Principios 5

2.2 Activación y anulación de registros de logs 5

2.3 Análisis de eventos de seguridad 6

2.4 Retención y accesos no autorizados 6

3. Responsabilidades 7

4. Referencia normativa 8

4.1 Controles de la normativa ISO27001:2022 y ENS 8

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 del documento, así como su relación y dependencia con el resto de los documentos normativos.

Este documento será revisado, por lo menos, anualmente, salvo que existan circunstancias que recomienden o exijan una revisión antes de dicha fecha.

1.1 Objeto

El objetivo del presente documento es detallar los principales aspectos de definición, activación, conservación, salvaguarda, revisión, registro y acceso a los registros de actividades (en adelante logs) producidos por los sistemas del Grupo FCC, con el fin de monitorizar el uso de los sistemas de información y la información almacenada en ellos.

1.2 Alcance

Esta Norma es de aplicación sobre cualquier log obtenido a partir de la monitorización de los sistemas del grupo FCC, independientemente de la herramienta empleada y el activo o recurso al que afecte.

La presente Norma también aplica a todo el personal interno o colaborador externo y sistema de información involucrado en la monitorización y gestión de logs descrito anteriormente.

2. Gestión de Eventos de Seguridad de la Información

2.1 Principios

Todos los sistemas y aplicaciones del grupo FCC deberán tener activada la auditoria de seguridad y generar registros de los eventos. Estos eventos serán guardados en los sistemas para su análisis a posteriori cuando se precisa una investigación, según la configuración de retención. Los logs de los sistemas que tratan datos sensibles serán enviados en (pseudo) tiempo real a la plataforma corporativa de gestión de logs, SIEM, por sus siglas en Ingles (Security Information and Event Management).

2.2 Activación y anulación de registros de logs

Todos los sistemas de información serán sincronizados con la misma fuente de hora para poder construir una línea de tiempo de los sucesos y para la correlación de los eventos. Los eventos que deberán ser registrados en los sistemas de información contendrán al menos la siguiente información:

- Nombre del sistema donde se generó
- Marca de tiempo cuando surgió el evento, incluyendo fecha y hora
- Identificador del evento, según la tecnología utilizada
- Identificación del usuario que ha causado el evento
- Identidad o nombre de los datos, componentes del sistema o recursos afectados.
- Resultado de la acción realizada.

Los eventos que deberán ser identificados y registrados en todos los sistemas de información deberán ser:

- Accesos o intentos de acceso a los sistemas y la información contenida en ellos.
- Todas las acciones realizadas por cuentas de usuario con privilegios elevados.
- Uso y cambios de los mecanismos de identificación y autenticación, incluidos entre otros el login, la creación y borrado de cuentas de usuario, el escalado de privilegios.
- Modificaciones en la auditoria de seguridad: inicialización, detención o borrado de logs.
- Creación y eliminación de objetos de nivel de sistema como tablas de bases de daros o procedimientos almacenados.

Todo nuevo aprovisionamiento de sistemas on-premise o en entornos nube deberá cumplir desde el inicio con los requisitos de auditoría y monitorización mencionados en esta norma. El departamento de SI coordinará con los departamentos de Tecnología de la Información y Telecomunicaciones la correcta ingesta de los logs en la plataforma de monitorización de seguridad.

En caso de baja de sistemas de información, los departamentos de Tecnología de la Información y Telecomunicaciones notificarán al departamento de SI la baja del activo para que se proceda a reconfigurar la plataforma de monitorización de seguridad acorde a la eliminación de los activos.

En la plataforma SIEM se definirán casos de uso para la generación de alertas en tiempo real, o para la generación de informes. La lógica programada en estos casos de uso servirá para detectar actividad sospechosa o maliciosa, que pueden ser signo de algún tipo de ataque o acceso no deseado a los sistemas y/o la información contenida en ellos.

2.3 Análisis de eventos de seguridad

Los eventos de seguridad recopilados mediante los mecanismos de monitorización establecidos por FCC serán analizados con el objetivo de identificar actividades anómalas, comportamientos sospechosos, incumplimientos de los requisitos de seguridad o potenciales incidentes de seguridad de la información.

El análisis podrá realizarse mediante las capacidades de correlación, detección y generación de alertas de las herramientas de monitorización implantadas, así como mediante revisiones específicas cuando resulte necesario.

Los eventos y alertas que se consideren relevantes serán evaluados para determinar su naturaleza, alcance e impacto potencial, así como la necesidad de aplicar medidas adicionales de contención, investigación o escalado.

Cuando del análisis realizado se concluya que un evento constituye un incidente de seguridad de la información, éste será gestionado de acuerdo con lo establecido en la norma IS_ST_08 Gestión de Incidentes de Seguridad de la Información.

2.4 Retención y accesos no autorizados

Para poder realizar un análisis forense digital, la retención de los logs configurada en los sistemas será de al menos 12 meses y podrá ser configurada en los propios sistemas de información, o en el SIEM en el caso de haber sido recogidos mediante dicha plataforma.

Se protegerán los logs para evitar cualquier tipo de modificación o acceso no autorizado. La protección de estos archivos se deberá gestionar mediante un proceso de supervisión que lleve a cabo la monitorización de integridad de ficheros. Este proceso se encargará de verificar que los programas y archivos del sistema operativo no se vean comprometidos.

3. Responsabilidades

El departamento de SI deberá:

- Verificar que no surgen conflictos entre las normas que se hayan establecido para el registro de logs. Cuando sea notificado de las alertas o actividades sospechosas que surjan en los sistemas de información o el entorno de red, el responsable deberá tomar las medidas oportunas con las que se deberá actuar para evitar cualquier incidente.
- Comprobar que la generación y recogida de los logs se realizan sin incidencia y reestablecer a la mayor brevedad posible en caso de sufrir alguna incidencia.

El departamento de IT deberá:

- Activar la auditoria en todos los sistemas de información en los que sea necesario generar un registro de actividad, según las directrices del departamento de SI.
- Informar al departamento de SI la baja de un sistema de información

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.

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
5.25	Evaluación y decisión sobre eventos de seguridad de la información	[op.exp.7] Gestión de Incidentes
5.33	Protección de los registros	[op.exp.8] Registro de la actividad; [op.mon.3] Vigilancia
6.8	Reporte de eventos de seguridad de la información	[op.exp.7] Gestión de Incidentes
8.15	Registro de eventos	[op.exp.8] Registro de la actividad