OBJETO

- Regular naturaleza, misión, dependencia y funciones OCC

- **Deber de comunicación** de determinados delitos (DGP y DGGC)

→ **Sin perjuicio deber grabación** investigaciones ciberdelitos

NATURALEZA Y MISIÓN

- Sin perjuicio del ámbito de actuación de las Fuerzas y Cuerpos de Seguridad del Estado, la OCC es el **órgano de coordinación de la SES en materia de ciberseguridad, desinformación y lucha contra la cibercriminalidad**.

La Instrucción fija **cinco misiones principales** (que no hemos de confundir con sus funciones):

→ Asesoramiento al Secretario de Estado de Seguridad en materia de ciberseguridad, desinformación y cibercriminalidad

→ Ejerce las funciones atribuidas al SES en materia de ciberseguridad de entidades críticas

→ Coordina la investigación tecnológica de las unidades de las FCSE y les presta apoyo

→ Ejerce de **canal específico de coordinación** de órganos dependientes del SES con autoridades nacionales e interancionales y los equipos de respuesta CSIRT

→ Participa en el **Sistema de Seguridad Nacional** representando al SES en cuestiones relacionadas con ciberseguridad y desinformación que le encomiende el Director General de Coordinación y Estudios (DGCE)

DEPENDENCIA

La OCC está integrada, **orgánica y funcionalmente,** en la **Dirección General de Coordinación y Estudios** (DGCE) de la SES, dependiendo directamente de su titular.

PROCEDIMIENTOS DE COORDINACIÓN Y COMUNICACIÓN DE CIBERINCIDENTES POR LAS FCSE

→ La OCC los **desarrolla**

→ La DGCE los **valida**

→ La SES los **autoriza**

→ Las FCSE los **cumplen**

Excepción:

→ Los procedimientos estrictamente técnicos → la OCC los comunica directamente a las FCSE.

PUBLICACIÓN Y EFECTOS

En el **plazo de los doce meses** siguientes a la publicación de la presente instrucción se revisará la eficacia de las disposiciones establecidas en la misma.

FUNCIONES

Las funciones se anidan dentro de cada una de las cinco misiones. Es decir, **para cada misión la Instrucción fija un número de funciones determinado** por lo que para una mejor comprensión hemos de repetir el listado anterior.

1. Asesoramiento Estratégico y generación de Inteligencia

→ Constituirse como **punto de referencia de inteligencia estratégica** en materia de cibercriminalidad, ciberseguridad y desinformación **a través del Observatorio de Cibercriminalidad** con la participación activa de otros organismos dependientes de la Secretaría de Estado de Seguridad, particularmente el **CITCO**, así como, en su caso, de las **Policías Autonómicas**

- Monitorización **permanente** del ciberespacio y elaborar inteligencia periódica de amenazas dando traslado al DGCE; al CITCO de los relativos a cibercriminalidad, ciberterrorismo o hacktivismo; y, en su caso, a las FCSE

- Monotirazción **específica** de ciberamenazas y emisión de informes de ciberinteligencia de eventos de especial relevancia para la seguridad pública

→ Informes **puntuales** de alerta sobre amenazas graves o inminentes

→ Informes **estadísticos** de cibercriminalidad y ciberseguridad

→ Análisis de situación y guías de buenas prácticas

→ Mantener actualizado el **Plan Estratégico de Cibercriminalidad** del Ministerio del Interior como **instrumento principal** para la planificación de su actividad de potenciación de la ciberseguridad, concienciación y prevención en la lucha contra cibercriminalidad y desinformación

2. Responsabilidad en materia de ciberseguridad atribuida al SES

Desempeñar todas las funciones asignadas a la SES relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión Europea:

→ **Evaluación técnico-legal:** Incidentes notificados por sujetos obligados.

→ **Comunicación y asignación:** **Ministerio Fiscal + Policía Judicial** + asignación según procedimiento predeterminado

- Incluye **petición urgente al CITCO** → su respuesta será tenida en cuenta para la asignación.

→ Seguimiento directo: Incidentes de especial relevancia, alarma social, complejidad o gravedad.

→ Plataforma Nacional: Operación exclusiva de la Plataforma Nacional de Notificación y Seguimiento de Ciberincidentes

→ Convocatoria **Mesa Cíber**

→ Acceso al **Catálogo Nacional de Entidades Críticas y Estratégicas**

3. Coordinación y Apoyo Técnico

→ Elaborar y coordinar **dispositivos extraordinarios:** Eventos relevantes (incluidos procesos electorales) + integración información amenazas + coordinación con CSIRT nacionales de referencia.

→ **Apoyo técnico FCSE**:

- Análisis de malware + patrones y tendencias

- Incidentes de **especial peligrosidad/impacto** (OCC estime necesario o iniciativa propia o de FCSE)

→ **IOC / TTP** : Creación, tratamiento y compartición de Indicadores de Compromiso (IOC) y Tácticas, Técnicas y Procedimientos (TTP)

→ **Abuso sexual infantil** → Coordinación redes nacionales e internacionales → especial referencia a NC-MEC (National Center for Missing & Exploited Children).

4. Canal específico de comunicación CSIRT y autoridades competentes

→ **Canal específico SES de comunicación** con CSIRT nacionales de referencia con:

- otros CSIRT nacionales o internacionales, públicos o privados

- autoridades competentes nacionales e internacionales.

→ **Punto de contacto nacional de Coordinación operativa** (ataques contra sistemas de información).

→ **Impulsar cooperación internacional:** Participación en foros, grupos de trabajo y conferencias.

→ **Ciberejercicios y ciberresiliencia** → Diseño, organización y coordinación.

→ **Acuerdos y Convenios** : Impulso, revisión y actualización de acuerdos en ciberseguridad, ciberinteligencia, cibercriminalidad y desinformación.

5. Participación en el Sistema de Seguridad Nacional

→ **Estrategias realizadas en el seno del Sistema de Seguridad Nacional (ciberseguridad):** Colaborar en la elaboración y ejecución en materia de ciberseguridad, cibercriminalidad, desinformación y ciberresiliencia de **infraestructuras críticas**.

→ **Participación en propio nombre, representación SES o DGCE** en comisiones, comités, foros y grupos de trabajo.

→ **Proyectos normativos:** Colaboración en normativa nacional e internacional relacionada con ciberseguridad, cibercriminalidad y desinformación