PLIEGO DE PRESCRIPCIONES TÉCNICAS PARA LA CONTRATACIÓN DE LOS SERVICIOS TÉCNICOS DE SOPORTE Y ANÁLISIS PARA SEGURIDAD INTEGRAL EN EL CENTRO NACIONAL DE PROTECCIÓN DE INFRAESTRUCTURAS CRÍTICAS Y EN LA OFICINA DE COORDINACIÓN DE CIBERSEGURIDAD

1. INTRODUCCIÓN

El presente pliego de prescripciones técnicas tiene por objeto justificar la contratación de la prestación de servicios técnicos de soporte y análisis para la seguridad integral en el Gabinete de Coordinación y Estudios, de la Secretaría de Estado de Seguridad (Ministerio del Interior), y en concreto dentro de este primer órgano, al Centro Nacional de Protección de Infraestructuras Críticas (CNPIC) y a la Oficina de Coordinación de Ciberseguridad (OCC).

El Real Decreto 734/2020, de 4 de agosto, por el que se desarrolla la estructura orgánica básica del Ministerio del Interior, asigna al Gabinete de Coordinación y Estudios impulsar, coordinar y supervisar, a través del Centro Nacional de Protección de Infraestructuras Críticas (CNPIC), todas las actividades que tiene encomendadas la Secretaría de Estado en relación con la protección de las infraestructuras críticas en el territorio nacional, en colaboración con otros Departamentos ministeriales.

Por otra parte, en el ámbito de la ciberseguridad, la legislación vigente encomienda a la Oficina de Coordinación de Ciberseguridad (OCC), del Gabinete de Coordinación y Estudios, de la Secretaría de Estado de Seguridad (Ministerio del Interior), un papel relevante en la gestión de los ciberataques a los sistemas de información de los Operadores Críticos, de Servicios Esenciales y otros estratégicos y sus proveedores, así como en la coordinación técnica de las actividades operativas y de investigación que, en ese ámbito, requieren la implicación de las unidades tecnológicas de las Fuerzas y Cuerpos de Seguridad del Estado.

En este sentido, la OCC asume las competencias de coordinación técnica del Ministerio del Interior con el INCIBE-CERT en la gestión y resolución de incidentes en materia de ciberseguridad, sin perjuicio de otras acciones llevadas a cabo en conjunción con el CCN-CERT del Centro Nacional de Inteligencia y otros CSIRT nacionales.

Además, el Real Decreto 734/2020, establecen que la OCC actúa como punto de contacto nacional de coordinación operativa para el intercambio de información con la Comisión Europea y los Estados miembros, en el marco de lo establecido por la Directiva 2013/40/UE de 12 de agosto de 2013, relativa a los ataques contra los sistemas de información.

Finalmente, el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información, que transpone la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión Europea, asigna también a la Secretaría de Estado de Seguridad (Ministerio del Interior), importantes responsabilidades en la gestión y comunicación de incidentes de servicios esenciales.

El crecimiento en el número de incidentes de ciberseguridad con impacto en los Operadores Críticos y en los de Servicios Esenciales así como en otros considerados estratégicos nacionales; el aumento de las tipologías de ciberataque, su evolución y complejidad; así como el aumento en el

número de requerimientos recibidos en la OCC por parte de los Operadores y otras entidades gubernamentales para la resolución y esclarecimiento de los incidentes de seguridad de los sistemas de información de una forma conjunta y coordinada, requieren el desarrollo de una serie de capacidades, que si bien en algunos casos se han venido prestando de forma exclusiva desde la OCC, requieren de una potenciación y continuidad estable en el tiempo, que permita operar las 24 horas del día, los 7 días de la semana, 365 días al año con una calidad en el servicio acorde con la importancia en la protección de infraestructuras críticas. La gestión de estos incidentes exige especialización, disponibilidad y respuesta inmediata en tanto en cuanto podrían llegar a afectar a los servicios esenciales prestados por Operadores Críticos nacionales, Operadores de Servicios Esenciales y Operadores estratégicos y sus proveedores.

Sobre la base de lo dispuesto en la Directiva UE 40/2013 relativa a los ataques contra los sistemas de información, por la que se requiere de España la designación de un punto de contacto nacional para el intercambio de información de carácter policial; adquiriendo esta responsabilidad la Secretaría de Estado de Seguridad, al objeto de canalizar las peticiones de ayuda policial por parte de otros estados miembros de la UE. Dicha designación fue trasladada a la Comisión Europea por el Embajador, responsable permanente de España ante la UE con fecha 3 de mayo de 2016.

2. OBJETO DE LA CONTRATACIÓN

Constituye el objeto de la contratación la prestación de servicios técnicos de soporte y análisis para la seguridad integral en los órganos dependientes del Gabinete de Coordinación y Estudios, el CNPIC y la OCC, focalizadas en el análisis en profundidad de las tareas de protección y seguridad para la gestión, seguimiento y resolución de incidentes de seguridad que afecten a Infraestructuras Críticas (IC, de la Ley 8/2011), Operadores de Servicios Esenciales (del RDL 12/2018), operadores estratégicos y sus proveedores, la atención del centro de recepción de incidencias de ciberseguridad gestionada, con soporte 24x7x365, así como apoyo técnico en las labores de persecución de la cibrecriminalidad y el ciberterrorismo, y la prestación de un servicio de suministro de información obtenida a través de distintas fuentes, que permita a los analistas de la OCC y el CNPIC evaluarla oportunamente con objeto de desarrollar los cometidos que tiene encomendados, entre los que se encuentran la monitorización y la vigilancia digital en busca de ciberamenazas de distinta naturaleza relacionadas con el terrorismo y ciberterrorismo, hacktivismo, movimientos radicales, ciberdelincuencia y ciberataques o acciones cibernéticas llevadas a cabo por otros Estados y que puedan tener impacto sobre intereses españoles materializados en los operadores referidos, para proveer informes estratégicos y operativos a las altas instancias del Ministerio del Interior, Secretaría de Estado de Seguridad, Dirección General de la Policía y Dirección General de la Guardia Civil.

3. DESCRIPCIÓN DEL CONTENIDO DE LOS SERVICIOS

El adjudicatario deberá aportar el conocimiento y las metodologías necesarias, apoyándose en los recursos técnicos que considere necesarios (que serán facilitados por el adjudicatario), para asegurar un resultado óptimo en la prestación del servicio. Se entiende por recurso técnico, cualquier tipo de software, hardware o licencia necesaria para la prestación del servicio en condiciones óptimas.

El adjudicatario se obliga a guardar secreto, y hacerlo guardar al personal que emplee para la elaboración de la oferta y/o ejecución del contrato, respecto a toda la información relacionada con el

CNPIC y la OCC, así como del Ministerio del Interior en su conjunto, que con motivo del desarrollo de dichos trabajos y prestación de servicios descritos en el presente documento llegue a su conocimiento, no pudiendo utilizarla para sí, ni para otras personas o mercantiles.

El alcance del contrato abarca los siguientes servicios:

3.1. SERVICIOS DE SOPORTE DE ATENCIÓN DE INCIDENCIAS DE SEGURIDAD (24X7X365).

Este servicio comportará la realización de las siguientes tareas:

- Gestión integral de incidentes de ciberseguridad y seguridad física de Operadores Críticos y Operadores de Servicios Esenciales.
- Operación y gestión del sistema de comunicación AlertPIC.
- Atención del punto de contacto nacional para el intercambio de información en las peticiones de ayuda policial por parte de otros estados miembros conforme lo establecido en la Directiva 2013/40 y legislación adoptada por la Secretaría de Estado de Seguridad.

Este servicio será atendido al menos por un operador en las propias instalaciones del CNPIC y la OCC, actualmente ubicadas en el Centro Tecnológico de la Seguridad del Estado en El Pardo (Madrid) durante las 24 horas del día, siete días a la semana los 365 días del año, sin perjuicio de ser reforzado por más personal si las necesidades del servicio lo demandan.

3.2. APOYO TÉCNICO PARA ANÁLISIS EN PROFUNDIDAD DE LAS TAREAS DE PROTECCIÓN Y SEGURIDAD PARA LA GESTIÓN, SEGUIMIENTO Y RESOLUCIÓN DE INCIDENTES

El análisis en profundidad de las tareas de protección y seguridad de la información de Infraestructuras Críticas, Operadores de Servicios Esenciales, operadores estratégicos y sus proveedores, para la gestión, seguimiento y resolución de incidencias comporta la realización de las siguientes tareas:

- Realización de tareas de consultoría en materia de ciberseguridad
- Realización de tareas de detección de incidentes de ciberseguridad
- Realización de tareas de reacción ante incidentes de ciberseguridad
- Realización de tareas de análisis de patrones y tendencias de los incidentes de ciberseguridad
- Elaboración de informes estadísticos en materia de ciberseguridad.
- Gestión de activos tecnológicos
- Realización de labores de cibervigilancia (vigilancia digital y tecnológica) en redes sociales u otros entornos y redes digitales o virtuales, empleando herramientas que faciliten las labores de ciberinteligencia y monitorización del ciberespacio.
- Supervisión y coordinación con la actividad del servicio de provisión de información.

Dichas tareas deberán ser realizadas al menos por dos analistas de ciberseguridad con disponibilidad plena para este contrato de lunes a viernes de cada semana del año en horario de la jornada de trabajo ordinario del CNPIC y la OCC.

3.3. SERVICIO DE PROVISIÓN DE INFORMACIÓN

El adjudicatario deberá suministrar al CNPIC y la OCC información sobre las materias y mediante los entregables que se describen en este pliego. Esta información guardará la estructura que se indica para los distintos entregables y vendrá acompañada de un análisis de la misma en las condiciones que se mencionan en este pliego.

Dichas tareas deberán ser realizadas en modalidad no presencial y puestas a disposición del CNPIC y la OCC, preferentemente desde la infraestructura de la empresa adjudicataria.

3.3.1. SERVICIO DE PROVISIÓN DE INFORMACIÓN SOBRE YIHADISMO.

Este servicio comportará la realización de las siguientes tareas:

- Seguimiento de aquellos grupos yihadistas que tengan actividad en Europa, prestando especial dedicación a aquellos que actúen en España. Este seguimiento incluirá grupos que lleven a cabo acciones físicas y/o cibernéticas, describiendo de forma detallada la actividad de cada uno de ellos.

- Seguimiento de aquellos grupos yihadistas que aun no teniendo actividad directa en Europa, hagan alguna referencia para llevar a cabo acciones en el continente. Prestando especial atención a aquellos que hagan referencia a España. Este seguimiento incluirá grupos que lleven a cabo acciones físicas y/o cibernéticas, describiendo de forma detallada la actividad de cada uno de ellos.

El referido seguimiento evaluará al menos las siguientes actividades llevadas a cabo por estos grupos:

- Publicación de manuales, describiendo y analizando su contenido.

- Distribución de propaganda y amenazas, describiendo y analizando su contenido.

- Distribución de aplicaciones informáticas tanto para ordenadores como para dispositivos móviles.

- Distribución de otros materiales que compartan utilizando tecnologías de la información y comunicación.

- Campañas y formas de reclutamiento, radicalización y financiación, entre esta información se incluirá siempre que sea posible cuentas de criptomonedas.

- Acciones físicas o cibernéticas, con especial énfasis en aquellas dirigidas contra infraestructuras concretas ubicadas en territorio nacional.

- Cualquier otra información que pudiera ser relevante para los intereses o la seguridad nacional.

Se tratará de atribuir, siempre que sea posible, una determinada actividad a un determinado grupo de los identificados anteriormente, indicando en estos casos la adscripción, pertenencia, influencia o inspiración de los mismos con las distintas corrientes de terrorismo yihadista existentes. En caso de que no sea posible llevar a cabo esta atribución, se motivará este aspecto.

No obstante lo anterior, el sistema de retroalimentación que se establece en el apartado 5.2.10 permitirá la inclusión por parte del del Gabinete de Coordinación y Estudios de grupos, entidades y acciones concretas relacionadas con esta materia sobre las cuales el adjudicatario debe proveer de información.

3.3.2. SERVICIO DE PROVISIÓN DE INFORMACIÓN SOBRE HACKTIVISMO.

Esta actividad consistirá en el seguimiento de los grupos y entidades relacionadas con el hacktivismo así como de sus acciones, entendiéndose como tales toda actividad cibernética con fines reivindicativos de derechos, promulgación de ideas de cualquier índole, protestas o quejas de la sociedad en general, a través de acciones contra la seguridad de los sistemas informáticos.

Además de lo anterior se incluirán en este apartado toda actividad encaminada a producir desestabilización en la sociedad. Esta desestabilización se entiende en sentido amplio, incluida la manipulación de la información, ya sea para promover la alteración de la voluntad del votante en caso de procesos electorales o para poner en riesgo el normal desenvolvimiento de la actividad del país.

Para ello se deberá analizar su actividad de forma general, prestando especial atención a aquellas circunstancias que podrían tener un impacto negativo en las infraestructuras o servicios esenciales, y sus posibles interdependencias a nivel nacional o internacional.

Esta actividad se llevará a cabo sin límites territoriales, de cara a poder evaluar el impacto de incidentes similares a los descritos en este apartado en organismos, entidades o infraestructuras de otros países.

No obstante lo anterior, el sistema de retroalimentación que se establece en el apartado 5.2.10 permitirá la inclusión por parte del Gabinete de Coordinación y Estudios de grupos, entidades y acciones concretas relacionadas con esta materia sobre las cuales el adjudicatario debe proveer de información.

3.3.3. SERVICIO DE PROVISIÓN DE INFORMACIÓN SOBRE CIBERCRIMINALIDAD.

Esta actividad estará referida al desarrollo de un seguimiento de los grupos y entidades relacionadas con la cibercriminalidad, entendiéndose como tal cualquier actividad delictiva llevada a cabo mediante equipos informáticos o a través de Internet.

Estas actividades de cibercriminalidad se entenderán de interés para su seguimiento cuando:

- Afecten a servicios esenciales nacionales.
- Afecten a servicios esenciales de otros países siempre que estén englobados dentro de una campaña de ataques o aun siendo una acción aislada tenga repercusión mediática.

No obstante lo anterior, el sistema de retroalimentación que se establece en el apartado 5.2.10 permitirá la inclusión por parte del del Gabinete de Coordinación y Estudios de grupos, entidades y acciones concretas relacionadas con esta materia sobre las cuales el adjudicatario debe proveer de información.

3.3.4. SERVICIO DE PROVISIÓN DE INFORMACIÓN SOBRE ACCIONES ATRIBUIBLES A OTROS ESTADOS.

Esta actividad estará referida al desarrollo de un seguimiento de amenazas cibernéticas detrás de las cuales se encuentren o pudieran encontrarse otros Estados o entidades relacionadas con los mismos y que tengan como objetivo perturbar el funcionamiento de servicios esenciales nacionales.

Además de lo anterior se incluirán en este apartado toda actividad encaminada a producir desestabilización en la sociedad. Esta desestabilización se entiende en sentido amplio, incluida la manipulación de la información, ya sea para promover la alteración de la voluntad del votante en caso de procesos electorales o para poner en riesgo el normal desenvolvimiento de la actividad de nuestro país.

No obstante lo anterior, el sistema de retroalimentación que se establece en el apartado 5.2.10 permitirá la inclusión por parte del Gabinete de Coordinación y Estudios de grupos, entidades y acciones concretas relacionadas con esta materia sobre las cuales el adjudicatario debe proveer de información.

3.3.5. SERVICIO DE PROVISIÓN DE INFORMACIÓN SOBRE ACCIONES ATRIBUIBLES A MOVIMIENTOS RADICALES.

Seguimiento de aquellos grupos radicales que tengan actividad en Europa, prestando especial dedicación a aquellos que actúen en España. Este seguimiento incluirá grupos que lleven a cabo acciones físicas y/o cibernéticas, describiendo de forma detallada la actividad de cada uno de ellos. El referido seguimiento evaluará al menos las siguientes actividades llevadas a cabo por estos grupos:

- Publicación de manuales.
- Distribución de propaganda, amenazas, aplicaciones informáticas tanto para ordenadores como para dispositivos móviles y otros materiales que compartan utilizando tecnologías de la información y comunicación.
- Campañas y formas de reclutamiento, radicalización y financiación, entre esta información se incluirá siempre que sea posible cuentas de criptomonedas.

- Acciones físicas o cibernéticas, con especial énfasis en aquellas dirigidas contra infraestructuras concretas ubicadas en territorio nacional.

- Cualquier otra información que pudiera ser relevante para los intereses o la seguridad nacional.

Se tratará de atribuir, siempre que sea posible, una determinada actividad a un determinado grupo de los identificados anteriormente, indicando en estos casos la adscripción, pertenencia, influencia o inspiración de los mismos con las distintas corrientes de radicalismo existentes. En caso de que no sea posible llevar a cabo esta atribución, se motivará este aspecto.

No obstante lo anterior, el sistema de retroalimentación que se establece en el apartado 5.2.10 permitirá la inclusión por parte del Gabinete de Coordinación y Estudios de grupos, entidades y acciones concretas relacionadas con esta materia sobre las cuales el adjudicatario debe proveer de información.

3.3.6. SERVICIO DE PROVISIÓN DE INFORMACIÓN SOBRE EVENTOS DE ESPECIAL INTERÉS.

Se desarrollará una actividad de seguimiento similar a los casos anteriores, y como refuerzo de éstos, referida en este caso a eventos o temáticas concretas que, por su relevancia, se consideren de especial interés para el del Gabinete de Coordinación y Estudios. En este sentido serán hasta doce (12) eventos de especial interés, a cubrir cada doce (12) meses, cuya temática será la que requiera el del Gabinete de Coordinación y Estudios, con la posibilidad de poder desarrollarse tres de ellos de forma simultánea.

4. METODOLOGÍA DE TRABAJO. DESARROLLO DEL SERVICIO

4.1. SERVICIOS DE SOPORTE DE ATENCIÓN DE INCIDENCIAS DE CIBERSEGURIDAD (24X7X365)

4.1.1. GESTIÓN DE INCIDENTES

En líneas generales, los incidentes gestionados por la Secretaría de Estado de Seguridad, a través del Gabinete de Coordinación y Estudios, como autoridad competente en base al Real Decreto-ley 12/2018 de seguridad de las redes y sistemas de información, corresponderán con aquellos comunicados tras superar los umbrales establecidos en la Guía Nacional de Notificación y Gestión de Ciberincidentes[1] y resto de normativa vigente en materia de ciberseguridad, en especial toda aquella derivada del Real Decreto-ley 12/2018. Además, se gestionarán todos aquellos incidentes comunicados voluntariamente, así como aquellos que sean detectados de forma proactiva en el ejercicio de las funciones propias de la OCC de la Secretaría de Estado de Seguridad.

[1] https://www.incibe-cert.es/sites/default/files/contenidos/guias/doc/guia_nacional_notificacion_gestion_ciberincidentes.pdf

Para llevar a cabo la gestión de incidentes se ejecutarán los procedimientos específicos de la OCC en la materia, y se pondrán en práctica los mecanismos de tratamiento de incidentes previamente definidos, y consistentes en la puesta en práctica de las siguientes fases:

- FASE 1. GESTIÓN INICIAL. Labores preliminares.
- FASE 2. TRIAJE. Categorización de una incidencia en incidente o evento.
- FASE 3. COMUNICACIÓN INTERNA. Puesta en conocimiento de cadena de mando.
- FASE 4. ANÁLISIS TÉCNICO-LEGAL. Análisis de la información por responsables de la OCC.
- FASE 5. COMUNICACIÓN EXTERNA. Puesta en conocimiento de organismos externos.
- FASE 6. GESTIONES ADICIONALES. Almacenamiento, revisión y actualización.
- FASE 7. VALORACIÓN. Conclusiones del incidente e informes de valoración.

Ilustración 1. Flujo de gestión de incidencias OCC

A continuación, se muestra aquella tipología de incidentes de obligada notificación por parte de operadores de servicios esenciales cuya autoridad competente sea la Secretaría de Estado de Seguridad en base a la peligrosidad de los mismos (NIVEL DE PELIGROSIDAD ALTO, MUY ALTO o CRÍTICO), así como aquellos incidentes de comunicación potestativa por parte de los sujetos obligados (NIVEL DE PELIGROSIDAD MEDIO o BAJO):

NIVEL DE PELIGROSIDAD ASOCIADO A UN CIBERINCIDENTE
NIVEL CRÍTICO
APT
NIVEL MUY ALTO
Distribución de malware
Configuración de malware
Robo
Sabotaje
Interrupciones
NIVEL ALTO
Pornografía infantil, contenido sexual o violento inadecuado
Sistema infectado
Servidor C&C (Mando y Control)
Compromiso de aplicaciones
Compromiso de cuentas con privilegios
Ataque desconocido
DoS (Denegación de servicio)
DDoS (Denegación distribuida de servicio)
Acceso no autorizado a información
Modificación no autorizada de información
Pérdida de datos
Phishing

Ilustración 2. Incidentes nivel 2. Comunicación obligatoria a OCC

NIVEL DE PELIGROSIDAD ASOCIADO A UN CIBERINCIDENTE
NIVEL MEDIO
Discurso de odio
Ingeniería social
Explotación de vulnerabilidades conocidas
Intento de acceso con vulneración de credenciales
Compromiso de cuentas sin privilegios
Desconfiguración
Uso no autorizado de recursos
Derechos de autor
Suplantación
Criptografía débil
Amplificador DDoS
Servicios con acceso potencial no deseado
Revelación de información
Sistema vulnerable
NIVEL BAJO
Spam
Escaneo de redes (scanning)
Análisis de paquetes (sniffing)
Otros

Ilustración 3. Incidentes nivel 1. Comunicación potestativa a OCC

Adicionalmente, deberá tenerse presente la posibilidad de comunicación en base a la obligatoriedad de la notificación de incidentes que superen los umbrales específicos asociados al nivel de impacto (NIVEL DE IMPACTO ALTO, MUY ALTO o CRÍTICO) de cada incidente.

Las incidencias de ciberseguridad, que podrán ser reportadas a través de diferentes vías de entrada (correo electrónico, teléfono, AlertPIC, monitorización proactiva, etc.), serán evaluadas de forma preliminar siguiendo los criterios definidos por la Secretaría de Estado de Seguridad, para su clasificación en base a su peligrosidad, impacto u otras características propias del incidente o del contexto en el que tengan lugar. En función de dicho análisis, recogido en los procedimientos de la OCC, los incidentes pueden ser clasificados como:

- Incidentes de ciberseguridad de NIVEL 1 de operación: una vez clasificados, tendrán que ser gestionados conforme lo indicado en los procedimientos de trabajo establecidos para estos casos específicamente definidos por la OCC.

- Incidentes de ciberseguridad de NIVEL 2 de operación: aquellos que sean clasificados así por alguno de los siguientes motivos:
    - Nivel de peligrosidad o impacto Alto, Muy Alto o Crítico
    - Incidentes detectados o comunicados pertenecientes al sector nuclear
    - Requerimiento de capacidades avanzadas o específicas de miembros del CNPIC o de la OCC en particular, no disponibles en el NIVEL 1 de operación.

Para el seguimiento de incidentes se empleará una herramienta de ticketing propia de la OCC, desarrollada en tecnología RTIR, cuyo mantenimiento y correcto funcionamiento será responsabilidad de la empresa adjudicataria. En su defecto se empleará una Base de Datos (BD) de diseño propio, en la cual mediante un sistema de *tickets* se realiza el asiento de las gestiones tendentes a la resolución de los incidentes. Adicionalmente, en el caso de no disponer de herramienta de ticketing, junto con la BD se empleará un gestor documental en el que se almacenará toda la información asociada con la gestión de incidentes.

Para la comunicación de incidentes de ciberseguridad a los CSIRT de referencia (INCIBE-CERT y CCN-CERT), acaecidos en el seno de las Infraestructuras Críticas y los Operadores de Servicios Esenciales se emplean herramientas de ticketing comerciales adaptadas, como RTIR[2] o LUCIA (basado también en RTIR), además de correo electrónico cifrado mediante PGP.

La comunicación de incidencias de Ciberseguridad en la OCC puede tener entrada a través de los siguientes canales:

- Origen interno.
- CSIRT de referencia. Es la que se establece en el RD-L 12/2018. El OSE/OC notifica a la OCC a través de su CSIRT de referencia.
- OSE/OC. Aunque no es el canal del RD-l 12/2018, al no existir una mención para la notificación por la Ley 8/2011, las incidencias puede entrar directamente desde el OC. En cuyo caso se notificaría al CSIRT de referencia.
- CNPIC.
- FCSE. Unidades centrales o periféricas de las FCSE. En cuyo caso se notificaría al CSIRT de referencia.
- CEPIC. Notificaciones que previamente el CEPIC ha conocido a través de FCSE, CITCO, CNI u otros informadores. En cuyo caso se notificaría a su CSIRT de referencia.
- Otros colaboradores, que también se notificaría a su CSIRT de referencia:
    - Departamento de Seguridad Nacional (DSN)
    - CITCO.
    - Centro Nacional de Inteligencia (CNI)
    - CSIRT autonómicos.
    - INTERPOL, EUROPOL, ENISA, Comisión Europea (DG HOME, DG CNECT, etc.).
    - Otras Instituciones europeas o internacionales (OTAN, OSCE, ONU, OEA, etc.)

[2] https://bestpractical.com/rtir

- Entidades públicas extranjeras (servicios de inteligencia, unidades ministeriales de interior, de asuntos exteriores, policías, etc.)
- Unidades militares nacionales o extranjeras.
- Colaboradores privados y particulares (servicios de auditorías, servicios de ciberseguridad, centros operativos de ciberseguridad -SOC, CERT-, etc.)

La metodología de trabajo se basará en la operativa habitual de un Centro de Respuesta a Incidentes de Ciberseguridad, y atenderá a las instrucciones técnicas y guías disponibles es vigor aprobadas por la OCC.

Se determinará, durante el primer mes de vigencia del contrato, el procedimiento para la gestión de incidentes de seguridad del ámbito físico en el que se vea afectado algún operador crítico y operador de servicios esenciales.

4.1.1.1. OPERACIÓN DE ALERTPIC

AlertPIC es un sistema colaborativo de mensajería instantánea, disponible en plataformas móviles y web, que permite la comunicación de incidencias e incidentes entre el CNPIC, la OCC, los Operadores de Infraestructuras Críticas, de Servicios Esenciales, operadores estratégicos y sus proveedores, así como los centros de respuesta a la resolución de incidentes de seguridad de la información (INCIBE-CERT y CCN-CERT).

La plataforma permite una gestión centralizada del servicio a través de un portal web, sobre el cual el adjudicatario del contrato prestará un servicio en formato 24x7x365 que comprende las siguientes tareas:

- Gestión de usuarios adscritos al sistema (altas, bajas, modificaciones).
- Distribución de software para los equipos clientes.
- Gestión de salas de comunicación (creación, adscripción de usuarios, moderación y control de la sala).
- Recepción de las llamadas de voz utilizadas por el sistema.
- Emisión de Avisos corporativos.
- Gestión de las comunicaciones entre el CNPIC y la OCC y el resto de usuarios (alertas, incidencias, y comunicaciones).

El adjudicatario deberá utilizar esta herramienta en su operativa diaria, en el marco de la comunicación con terceros para el intercambio de información de interés relacionada con la resolución de incidentes, informes de amenaza u otros que se determinen oportunamente.

4.1.1.2. ATENCIÓN DEL PUNTO DE CONTACTO NACIONAL DIRECTIVA 2013/40

Dentro del servicio de soporte de atención de incidencias de ciberseguridad se incluye la atención de las peticiones de ayuda policial por parte de otros Estados Miembros, en relación con el intercambio de información sobre ciberdelitos con otros países u órganos internacionales. En respuesta a lo dispuesto en la Directiva UE 40/2013, relativa a los ataques contra los sistemas de

información, y en la que se requiere de España la designación de un punto de contacto nacional para el intercambio de información de carácter policial, desempeñando dicha función la Secretaría de Estado de Seguridad al objeto de canalizar las peticiones de ayuda policial por parte de otros estados miembros. Estas acciones vienen recogidas en los procedimientos internos de funcionamiento adoptados por la Secretaría de Estado de Seguridad, y consisten, en líneas generales, en la puesta en práctica de las siguientes fases:

- FASE 1. RECEPCIÓN DE INFORMACIÓN
- FASE 2. REENVÍO DE PETICIÓN. Canalización de información.
- FASE 3. REENVÍO DE CONTESTACIÓN. Remisión de información solicitada
- FASE 4. CIERRE DE PROCESO.

Estos tres trámites descritos pueden también presentarse en sentido inverso al descrito, al iniciarse la solicitud de ayuda desde las FCSE, la cual sería canalizada hacia el órgano policial extranjero correspondiente.

Los tiempos de atención se ajustarán a los marcados en los procedimientos internos de trabajo de la OCC, y en caso de incumplimiento de los mismos se atenderá a lo recogido en el apartado referente a Acuerdos de Nivel de Servicio del presente Pliego.

4.1.1.3. VOLUMEN DE TRABAJO ESTIMADO

A efecto meramente indicativo se estima que el número de incidencias a gestionar en el Centro de Atención de Incidencias de Ciberseguridad es el siguiente:

- Incidentes de Ciberseguridad: 3000/mes.
- Operaciones del sistema AlertPIC: 5000/mes.
- Solicitudes de ayuda policial relacionadas con el punto de contacto nacional: 100/mes.

En todo caso, el adjudicatario deberá dar cobertura a la totalidad de las incidencias que se presenten.

4.2. APOYO TÉCNICO PARA ANÁLISIS EN PROFUNDIDAD DE LAS TAREAS DE PROTECCIÓN Y SEGURIDAD PARA LA GESTIÓN, SEGUIMIENTO Y RESOLUCIÓN DE INCIDENTES

Comprende las siguientes actividades:

4.2.1. REALIZACIÓN DE TAREAS DE CONSULTORÍA EN MATERIA DE CIBERSEGURIDAD

El adjudicatario deberá disponer, a través de los recursos humanos que aporte al contrato, de la capacidad de ejecutar las siguientes funciones en materia de consultoría:

- Elaboración de informes bajo petición en materia de ciberseguridad
- Apoyo al desarrollo de normativa, guías y políticas en materia de ciberseguridad
- Asesoramiento multidisciplinar en materia de ciberseguridad

- Asesoramiento y apoyo específico en materia de auditorías pentesting
- Desarrollo de scripts y capacidad de implementación de herramientas en materia de ciberseguridad

En este sentido, se emplearán herramientas de software libre y open source junto con herramientas comerciales, siendo necesario que el adjudicatario aporte como mínimo dos (2) usuarios de las siguientes herramientas comerciales a lo largo de la duración del contrato para personal funcionario de la OCC:

- TABLEAU version creator o similar.

4.2.2. REALIZACIÓN DE TAREAS DE DETECCIÓN DE INCIDENTES DE CIBERSEGURIDAD

En el marco de las tareas inherentes de la OCC, se llevarán a cabo funciones asociadas a la detección de ciberincidentes o vulnerabilidades que puedan tener un elevado riesgo asociado para la prestación de servicios esenciales. El adjudicatario deberá colaborar en las tareas acometidas al efecto por el personal de la OCC en este sentido, particularmente en lo que respecta a la evaluación remota de activos a través de Internet, con objeto de identificar potenciales anomalías o vulnerabilidades susceptibles de ser explotadas por ciberatacantes. Para ello, las acciones se focalizarán en la detección de:

- Sistemas de información u operación potencialmente comprometidos
- Sistemas de información u operación potencialmente vulnerables
- Fugas de datos
- Exposición de Operador de Servicios Esenciales. Reputación de IPs, dominios y otros activos.

Para ese fin, se implementarán mecanismos adecuados para la recopilación, análisis y explotación de la información de interés asociada a los activos tecnológicos de los Operadores de Servicios Esenciales, sus proveedores de servicios u otros organismos, entidades o individuos que así lo requieran. El servicio se llevará a cabo, al menos, mediante la puesta en práctica de técnicas basadas en la explotación de motores de búsqueda generales y específicos o el uso de cualesquiera otras herramientas o técnicas que se consideren oportunas para la supervisión del cumplimiento de las obligaciones de seguridad de los sujetos obligados conforme la normativa vigente en este ámbito. Así mismo se ejecutará el procesamiento de la información proveniente de fuentes abiertas (como pueden ser las blogs, páginas web, etc), así como de fuentes cerradas (información privada de entidades de seguridad, indicadores de compromiso, foros de seguridad, etc.). Estos mecanismos, salvo autorización específica del afectado, consistirán en la ejecución de técnicas pasivas que no afectarán, en ningún caso, a la operativa del activo tecnológico analizado. En este sentido, se emplearán herramientas de software libre y open source junto con herramientas comerciales, siendo necesario que el adjudicatario aporte como mínimo dos (2) usuarios de cada una de las siguientes herramientas comerciales a lo largo de la duración del contrato para personal funcionario de la OCC:

- SHODAN o similar.
- DOMAIN TOOLS o similar.
- NESSUS o similar.

De todos los trabajos ejecutados se realizarán los informes pertinentes, en los que se detallarán las actuaciones realizadas, y las posibles soluciones para la mitigación de la amenaza. La elaboración de estos informes será responsabilidad de la empresa adjudicataria, y contendrá los siguientes puntos, de forma orientativa:

- Resumen ejecutivo
- Antecedentes
- Investigación
  - Descripción del Ciberincidente / Vulnerabilidad
  - Detección
  - Mitigación
  - Eliminación
- Indicadores de Compromiso asociados
- Recomendaciones
- Conclusiones

4.2.3. REALIZACIÓN DE TAREAS DE REACCIÓN ANTE INCIDENTES DE CIBERSEGURIDAD

De forma específica, dentro del NIVEL 2 de operación de incidentes de ciberseguridad, la OCC mantiene tareas de mitigación, investigación y resolución de incidentes de gran impacto e importancia; por afectar éstos a un importante número de Infraestructuras Críticas, Operadores de Servicios Esenciales y otros operadores estratégicos o sus proveedores, o por considerarse amenazas avanzadas focalizadas de forma específica en objetivos particulares. Ejemplo de ello son las recientes amenazas de ciberseguridad detectadas a lo largo del año 2019 y 2020: *Ragnar-locker, Snake-Ekans, Phobos, Ryuk, etc.*

La investigación de estos ciberincidentes requiere que el adjudicatario lleve a cabo las tareas específicas de investigación cibernética como son: análisis estático y dinámico de malware, el reversing de muestras potencialmente maliciosas, la definición de indicadores de compromiso (IOC) sobre amenazas, la detección de patrones de comportamiento en incidentes, así como el procesamiento y análisis de documentos técnicos sobre las tareas anteriormente relacionadas a lo largo del desarrollo de la gestión del incidente.

Adicionalmente, en el caso particular de incidentes Críticos, u otros de relevancia así establecidos, la adjudicataria aportará un informe de carácter técnico en el que se consignará la información que estime oportuno, y que se remitirá cuando así se indique conforme los procedimientos de la OCC. El informe técnico requerido contendrá los siguientes puntos, de forma orientativa:

- Resumen ejecutivo
- Descripción del incidente
- Análisis de muestras de malware
- Análisis de Tácticas Técnicas y Procedimientos (TTPs) empleados
- Indicadores de Compromiso asociados al incidente
- Recomendaciones
- Conclusiones

4.2.4. REALIZACIÓN DE TAREAS DE REACCIÓN ANTE INCIDENTES DE SEGURIDAD DE NATURALEZA FÍSICA

La gestión de los incidentes de seguridad de naturaleza física acaecidos en operadores críticos y de servicios esenciales se realizará atendiendo al procedimiento que se facilitará a la empresa adjudicataria durante el primer mes de vigencia del contrato.

4.2.5. REALIZACIÓN DE TAREAS DE ANÁLISIS DE PATRONES Y TENDENCIAS DE LOS INCIDENTES DE CIBERSEGURIDAD

A lo largo de cada año de duración del contrato, el adjudicatario deberá llevar a cabo un tratamiento de la información suministrada al CNPIC y la OCC en el marco de sus funciones propias. En base a ello, se realizarán informes de seguimiento en los que se detallará y analizará la presencia de campañas, o la concurrencia de varios incidentes de ciberseguridad de una determinada tipología, sector estratégico, nivel de peligrosidad o impacto o cualquier otra circunstancia que indique. Para la elaboración de estos documentos, el adjudicatario deberá seguir lo establecido en los procedimientos internos de trabajo de la OCC. El informe técnico requerido contendrá los siguientes puntos, de forma orientativa:

- Resumen ejecutivo
- Descripción de las campañas o incidentes detectados
- Análisis de Tácticas Técnicas y Procedimientos (TTPs) empleados (siempre que sea posible se implementará el framework MITRE ATT&CK para el análisis de los ciberincidentes)
- Análisis de patrones de comportamiento y ataques detectados, posibles grupos APT o cibercriminales asociados, así como software y herramientas empleadas.
- Recomendaciones
- Conclusiones

4.2.6. ELABORACIÓN DE INFORMES ESTADÍSTICOS EN MATERIA DE CIBERSEGURIDAD

El adjudicatario deberá llevar a cabo una gestión de la información de carácter estadístico derivada del ejercicio de las funciones del CNPIC y la OCC. Para ello deberá aportar con carácter mensual un informe estadístico siguiendo lo establecido en los procedimientos de trabajo internos de la OCC. Así mismo deberá aportarse un informe anual en el que se recojan los datos relativos a cada año natural.
Además, el adjudicatario deberá disponer de capacidad suficiente para la remisión de los datos estadísticos actualizados en cualquier momento del contrato en que les sean solicitados, independiente del aporte que realicen con carácter mensual y anual.

4.2.7. GESTIÓN DE ACTIVOS TECNOLÓGICOS

En el marco de las labores de la Secretaría de Estado de Seguridad, como autoridad competente conforme el Real Decreto-ley 12/2018 de seguridad de las redes y sistemas de información, el Gabinete de Coordinación y Estudios, a través de la OCC, tiene la necesidad de llevar a cabo la gestión de activos a su disposición. Para ello, el adjudicatario deberá llevar a cabo la gestión

operativa de los activos tecnológicos conforme lo indicado en los procedimientos de trabajo internos de la OCC.

El Gabinete de Coordinación y Estudios es el propietario de toda la documentación elaborada por el adjudicatario. Éste se encargará de disponer de todas las autorizaciones y permisos necesarios para poder dar cumplimiento a esta previsión, siendo responsabilidad del adjudicatario cualquier pago o reclamación relativa a esta falta de autorizaciones.
El personal del Gabinete de Coordinación y Estudios será responsable de la validación y aprobación de los documentos elaborados por el personal del adjudicatario. En caso de que la calidad de los documentos sea muy baja o de manera recurrente y / o prolongada en el tiempo de prestación de los servicios no alcance los niveles requeridos se aplicarán las penalizaciones establecidas en la presente licitación.

4.2.8. PROVISIÓN DE INFORMACIÓN

La metodología de trabajo para lo especificado en el apartado 3.3 se desarrollará según lo establecido en este pliego, con la coordinación de los analistas contratados por la empresa adjudicataria que prestan servicio en las infraestructuras del CNPIC y la OCC, y el personal en plantilla perteneciente al CNPIC y la OCC. Este servicio se materializará en forma de entregables que se describen en el siguiente apartado.

La información obtenida de las actividades del apartado 3.3 resultará de una monitorización como mínimo de las siguientes fuentes:

- Fuentes abiertas.
- Fuentes cerradas (aquellas accesibles a través de un registro y autentificación previa del usuario)
- Aplicaciones y servicios de mensajería instantánea.
- Redes sociales.
- Foros.
- Deep y Dark Web (Tor, Freenet, I2P, etc.).

Se requerirá que la información provista al CNPIC y la OCC proceda de las fuentes mencionadas, especialmente de aplicaciones y servicios de mensajería instantánea como Telegram, WhatsApp, etc. No obstante lo anterior, el sistema de retroalimentación que se establece en el apartado 5.2.10 permitirá la inclusión por parte del Gabinete de Coordinación y Estudios de las fuentes que estime oportunas.

5. ENTREGABLES

Dentro de los tres primeros meses de vigencia del contrato, el adjudicatario deberá remitir a la OCC un informe que desarrolle la elaboración de un mecanismo para la revisión, adaptación y actualización de los procedimientos de trabajo en uso en la OCC por parte del adjudicatario. Estos procedimientos se facilitarán al adjudicatario una vez comience a desarrollar su trabajo.

Todas los entregables serán elaborados mediante herramientas ofimáticas del paquete de Microsoft Office, y a petición del CNPIC y la OCC, se podrá solicitar la edición y maquetación de informes con herramientas específicas, compatibles con Adobe InDesign.

5.1. SERVICIOS DE SOPORTE DE ATENCIÓN DE INCIDENCIAS DE SEGURIDAD (24X7X365) Y APOYO TÉCNICO PARA ANÁLISIS EN PROFUNDIDAD DE LAS TAREAS DE PROTECCIÓN Y SEGURIDAD PARA LA GESTIÓN, SEGUIMIENTO Y RESOLUCIÓN DE INCIDENTES

5.1.1. INFORME TÉCNICO DE SEGUIMIENTO

El adjudicatario deberá remitir asimismo a la OCC o al CNPIC, un informe técnico de seguimiento, con una periodicidad quincenal. Estos reportes constarán, al menos, de los siguientes puntos:

- Incidencias en el cumplimiento del ANS establecido con el adjudicatario conforme lo indicado en este documento
- Relación de incidentes gestionados y su estado (ABIERTO, CERRADO o ABANDONADO) especificando su nivel de gestión (NIVEL 1 y 2 de operación, así como aquellas categorizaciones que se indiquen)
- Relación de incidentes gestionados en base a su nivel de peligrosidad, nivel de impacto, tipología, sector estratégico y cualesquiera otras clasificaciones se le indique previamente
- Informe-resumen de las actuaciones llevadas a cabo en la plataforma AlertPIC
- Informe-resumen de las solicitudes de ayuda policial tramitadas como punto de contacto nacional.
- Informe-resumen de las actuaciones llevadas a cabo en materia de
    - Consultoría en materia de ciberseguridad
    - Detección de incidentes de ciberseguridad
    - Reacción ante incidentes de ciberseguridad
    - Análisis de patrones y tendencias de los incidentes de ciberseguridad
    - Elaboración de informes estadísticos en materia de ciberseguridad.
    - Gestión de activos tecnológicos
- Incidencias técnicas, de organización o estructurales en el desarrollo de los trabajos asignados.
- Identificación de mejoras que se puedan aplicar para el cumplimiento de los objetivos del servicio si se aprecian.

Se significa que al margen de estos reportes periódicos de control, el adjudicatario deberá registrar debidamente todas las actuaciones relacionadas con la gestión y seguimiento de los ciberincidentes gestionados, especificando en todo caso:

- ASUNTO
- ORIGEN
- FECHA
- TICKET OCC
- HORA

- TICKETS EXTERNOS
- FECHA INCIDENCIA
- CLASIFICACIÓN
- TIPO
- ESTADO
- VERACIDAD DE LA INFORMACIÓN
- NIVEL DE PELIGROSIDAD
- NIVEL DE IMPACTO
- ANALISTA ASIGNADO SI PROCEDE:
- OBSERVACIONES
- ACCIONES REALIZADAS

El adjudicatario deberá proporcionar, en el momento en que se le requiera, información relativa a la consulta de ciberincidentes por:

- DÍA.
- SEMANA.
- MES.
- AÑO.
- SECTOR/SUBSECTOR ESTRATÉGICO.
- OPERADOR /AFECTADO.
- ASIGNACIÓN A FFCCSE.

Asimismo se deberá poder combinar este tipo de búsquedas entre sí, a fin de elaborar búsquedas complejas.

5.1.2. INFOME ANUAL DE SEGUIMIENTO

Al alcanzar la fecha final del proyecto, el adjudicatario deberá presentar una Memoria Final, en la que se detallarán de forma global y precisa, y referidos al año de contrato, todos aquellos puntos desarrollados en los informes técnicos de seguimiento.

Asimismo, el adjudicatario deberá facilitar al CNPIC y la OCC y/o Ministerio del Interior, según se determine, una exportación de los incidentes tramitados y sus correspondientes gestiones, así como los datos obtenidos en el resto de los servicios contratados, en un formato estándar importable por otras aplicaciones de gestión de incidentes o de bases de datos (Ej.: XML, CSV…).

5.2. SERVICIO DE PROVISIÓN DE INFORMACIÓN

5.2.1. ESTRUCTURA Y CONTENIDO DE LOS ENTREGABLES QUE SE REMITAN AL CNPIC Y LA OCC.

Todos los entregables que se detallan a continuación, se ajustarán al contenido, estructura y formato que sea detallado en cada caso por el CNPIC y la OCC.

Todas las informaciones que sean remitidas al CNPIC y la OCC y que se encuentren en idioma distinto al español que se incluyan en los entregables deberán estar acompañadas de su correspondiente traducción.

5.2.2. INFORMES EXTRAORDINARIOS.

Los informes extraordinarios tendrán un carácter estratégico. La finalidad de estos informes es dar conocimiento de lo que ha sucedido en el periodo de tiempo analizado y sobre cómo ha evolucionado. El análisis básico debería permitir conocer datos como tipología, objetivos, autores, impacto potencial, impacto real, países afectados, etc.

El análisis con enfoque estratégico debería incluir, además de lo contenido en el análisis básico, cuestiones tales como distribución temporal de la amenaza durante el tiempo analizado, coincidencia de la misma con determinados eventos, si se trata de amanazas dirigidas o de oportunidad, si la amenaza es cada vez más sofisticada o por el contrario es similare, si el impacto de la misma es cada vez mayor o menor etc. Se trata pues de aportar datos que permitan conocer no solo el nivel de la amenaza, sino su evolución (si aumenta o disminuye), analizando evoluciones en el impacto, en la sofisticación, frecuencia y otros parámetros.

Los informes extraordinarios tendrán un carácter semestral y anual, y contendrán:

- Resumen ejecutivo
- Hallazgos clave:
    - Ciberterrorismo
    - Hacktivismo
    - Cibercriminalidad
    - Acciones cibernéticas atribuibles a otros estados.
    - Radicalismos.
- **Sobre ciberterrorismo:**
    - Propaganda. Análisis cuantificando y distinguiendo a qué país está dirigida. Elaboración de gráficas.

- Amenazas. Análisis cuantificando y distinguiendo a qué país está dirigida. Elaboración de gráficas.
- Publicaciones (revistas), análisis por número de ellas y tipo. Elaboración de gráficas.
- Presencia online, número de Webs, foros y blogs detectados. Distinguir si es posible por corriente yihadista. Elaboración de gráficas.
- Ciberataques. Tipologías, impacto y objetivos atacados. Elaboración de gráficas por tipo de ataque y objetivos atacados.
- Indicación de los grupos más activos, analizando sus capacidades, el impacto generado con sus acciones y su potencial impacto.
- Uso de internet por parte de grupos terroristas, uso común y nuevas tendencias.
- Acciones contra con servicios esenciales
- Número de referencias a España. Elaboración de gráficas por meses.

➢ **Sobre hacktivismo:**

- Ciberataques, elaboración de gráficas por tipología de ataques, por grupos y por países afectados.
- Indicación de los grupos más activos, analizando sus capacidades, el impacto generado con sus acciones y su potencial impacto.
- Presencia online, número de Webs, foros y blogs detectados. Elaboración de gráficas.
- Uso de internet por parte de los grupos hacktivistas, uso común y nuevas tendencias
- Acciones contra con servicios esenciales

➢ **Sobre Cibercriminalidad:**

- Ciberataques, elaboración de gráficas por tipología de ataques y por países afectados.
- Indicación de los grupos más activos, analizando sus capacidades, el impacto generado con sus acciones y su potencial impacto.
- Ciberdelitos cometidos contra servicios esenciales.
- Análisis general del impacto.

➢ **Sobre actos atribuibles a otros estados:**

- Estados a los que se les atribuyen los actos, elaboración de gráficas.

- Efectos de los actos analizados, incluyendo aquellos efectos que hayan podido tener sobre los servicios esenciales.

➢ **Radicalismos.**

- Elaboración de gráficas por acciones realizadas, bien físicas o cibernéticas.
- Elaboración de gráficas por tipologías de ciberataques.
- Efectos de los actos analizados, incluyendo aquellos efectos que hayan podido tener sobre los servicios esenciales.

5.2.3. INFORMES PERIÓDICOS (MENSUALES/QUINCENALES).

- Un (1) resumen ejecutivo, de la información obtenida en el que se detallen tendencias, novedades y resumen de las noticias o hechos más relevantes.
- Para cada tipo de información encontrada, un titular, un resumen y un análisis de dicha información. Se añadirán las imágenes necesarias para aclarar, representar o contextualizar la información aportada.
- Análisis de las entidades (grupos, usuarios de redes sociales, servicios de mensajería instantánea, personas físicas, etc.) relacionadas con la materia objeto del informe (bien por obtención propia o facilitadas para su seguimiento por el CNPIC y la OCC). Dependiendo de la entidad analizada, el citado análisis determinará, sin ser una lista cerrada, adscripción ideológica, motivación, componentes del grupo, grupo al que pertenece una entidad, datos biográficos, identidades digitales (cuentas en redes sociales, mensajería instantánea, blogs, páginas web, cuentas de correo electrónico, etc.), acciones previas, capacidades técnicas y aquellos otros datos que el CNPIC y la OCC estime oportunos y le sean solicitados oportunamente a la empresa adjudicataria.
- Análisis forense de los archivos y aplicaciones que estén relacionados con las noticias o hechos recogidos en cada informe. Este análisis consistirá por una parte en un análisis de malware de los archivos y aplicaciones mencionados y en caso de encontrarse algún tipo de malware, un análisis estático y dinámico del mismo. Y por otra, en la extracción de los metadatos que pudieran contener los mismos y que pudieran ser de interés para determinar su origen, fuente de producción, medios utilizados para su producción, fechas, etc.
- Un análisis de impacto y posibles consecuencias de la información evaluada, que deberá estar contextualizada estableciendo enlaces con casos precedentes o con cualquier otra información previa que pueda estar relacionada.

5.2.4. ALERTAS INSTANTÁNEAS.

- Título.
- Resumen de la información encontrada y análisis de la misma.

- Justificación de la alerta y un análisis del impacto y de las posibles consecuencias de esta información, que deberá estar contextualizada estableciendo enlaces con casos precedentes o con cualquier otra información previa que pueda estar relacionada.

5.2.5. NOTAS DIARIAS.

- Un (1) resumen ejecutivo.
- Para cada tipo de información encontrada, un titular, un resumen, un análisis y aquellas imágenes necesarias para aclarar, representar o contextualizar la información aportada.
- Un análisis de impacto y posibles consecuencias de la información evaluada, que deberá estar contextualizada estableciendo enlaces con casos precedentes o con cualquier otra información previa que pueda estar relacionada.

5.2.6. ELEMENTOS COMUNES A LOS INFORMES EXTRAORDINARIOS, INFORMES PERIÓDICOS, ALERTAS Y NOTAS DIARIAS.

- Se incluirán detalladamente las fuentes donde se ha obtenido la información.
- Se adjuntarán las imágenes que se obtengan durante el seguimiento y análisis de la información recopilada, para ilustrar la información.
- Se aportarán los enlaces necesarios, en su caso, para la descarga del material audiovisual o documentos relacionados con la información.
- Se aportarán los enlaces originales directos a la información suministrada.
- Se presentarán en formato Microsoft Word y pdf sin proteger contra copia, escritura o impresión, y sin marcas de agua que identifiquen a la empresa adjudicataria. El formato de maquetación será determinado en cada caso por el CNPIC y la OCC.
- Cuando se trate de datos masivos (como pudieran ser conexiones de internet, descarga de contenido de redes sociales, etc.) estos se aportarán en un archivo con formato XML o como se indique por parte del CNPIC y la OCC, así como en otros dos archivos debidamente maquetados y listos para su visualización por parte del usuario final (Microsoft Word y Pdf). El formato de maquetación será determinado en cada caso por el CNPIC y la OCC.

5.2.7. PERIODICIDAD DE LOS ENTREGABLES QUE CONTIENEN LA INFORMACIÓN.

A demanda del CNPIC y la OCC, y para informes de pauta mensual, se podrá solicitar la elaboración de un solo informe agregado en lugar de informes temáticos.

5.2.7.1. PARA EL SERVICIO DE PROVISIÓN DE LA INFORMACIÓN SOBRE YIHADISMO.

- Un (1) informe quincenal remitido los días 01 y 15 de cada mes antes de las 10:00 horas (que contengan la información encontrada durante esas quincenas)
- Tantas alertas instantáneas como se precisen si la información es especialmente relevante, teniendo este carácter cuando se trate de acciones que pudieran tener lugar en un corto espacio de tiempo o su no remisión al tiempo de tener conocimiento impidiera o pudiera impedir su uso operativo por parte de las Fuerzas y Cuerpos de Seguridad.

5.2.7.2. PARA EL SERVICIO DE PROVISIÓN DE LA INFORMACIÓN SOBRE HACKTIVISMO.

- Un (1) informe mensual remitido el día 1 de cada mes antes de las 10:00 horas.
- Tantas alertas instantáneas como se precisen si la información es especialmente relevante, teniendo este carácter cuando se trate de acciones que pudieran tener lugar en un corto espacio de tiempo o su no remisión al tiempo de tener conocimiento impidiera o pudiera impedir su uso operativo por parte de las Fuerzas y Cuerpos de Seguridad.

5.2.7.3. PARA EL SERVICIO DE PROVISIÓN DE LA INFORMACIÓN SOBRE CIBERCRIMINALIDAD.

- Un (1) informe mensual remitido el día 1 de cada mes antes de las 10:00 horas.
- Tantas alertas instantáneas como se precisen si la información es especialmente relevante, teniendo este carácter cuando se trate de acciones que pudieran tener lugar en un corto espacio de tiempo o su no remisión al tiempo de tener conocimiento impidiera o pudiera impedir su uso operativo por parte de las Fuerzas y Cuerpos de Seguridad.

5.2.7.4. PARA EL SERVICIO DE PROVISIÓN DE LA INFORMACIÓN SOBRE ACCIONES ATRIBUIBLES A OTROS ESTADOS.

- Un (1) informe mensual remitido el día 15 de cada mes antes de las 10:00 horas.
- Tantas alertas instantáneas como se precisen si la información es especialmente relevante, teniendo este carácter cuando se trate de acciones que pudieran tener lugar en un corto espacio de tiempo o su no remisión al tiempo de tener conocimiento impidiera o pudiera impedir su uso operativo por parte de las Fuerzas y Cuerpos de Seguridad.

5.2.7.5. PARA EL SERVICIO DE PROVISIÓN DE LA INFORMACIÓN SOBRE ACCIONES ATRIBUIBLES A MOVIMIENTOS RADICALES.

- Un (1) informe mensual remitido el día 15 de cada mes antes de las 10:00 horas.

- Tantas alertas instantáneas como se precisen si la información es especialmente relevante, teniendo este carácter cuando se trate de acciones que pudieran tener lugar en un corto espacio de tiempo o su no remisión al tiempo de tener conocimiento impidiera o pudiera impedir su uso operativo por parte de las Fuerzas y Cuerpos de Seguridad.

5.2.7.6. PARA EL SERVICIO DE PROVISIÓN DE LA INFORMACIÓN SOBRE EVENTOS DE ESPECIAL INTERÉS.

- Al menos una (1) nota diaria (remitida antes de las 12:00 horas (o la que el CNPIC y la OCC establezcan) que recoja la información encontrada y analizada desde las 12:00 horas del día anterior hasta las 12:00 horas del día de su remisión al CNPIC y la OCC)

- Un (1) informe semanal (remitido el día y hora que se establezca), que resuma la actividad de toda la semana y contenga un análisis con visión prospectiva y estudio estadístico.

- Un informe final (remitido el último día del evento de especial interés o cuando el CNPIC y la OCC establezcan) que resuma los hechos más relevantes y muestre la evolución de los acontecimientos que se hayan reflejado en entregables anteriores, así como valoraciones estadísticas.

- Tantas alertas instantáneas como se precisen si la información es especialmente relevante, teniendo este carácter cuando se trate de acciones que pudieran tener lugar en un corto espacio de tiempo o su no remisión al tiempo de tener conocimiento impidiera o pudiera impedir su uso operativo por parte de las Fuerzas y Cuerpos de Seguridad.

- La ventana temporal de la cobertura de información sobre estos eventos será de 30 días consecutivos.

- El CNPIC y la OCC podrán requerir hasta doce (12) servicios anuales de provisión de información sobre eventos de especial interés por cada periodo de un año a contar desde el inicio de la prestación del servicio.

- Para eventos de mayor duración a los 30 días, a efectos de contabilización de servicios, se consumirán tantos servicios como periodos de 30 días se alargue el evento.

5.2.7.7. PARA LOS INFORMES EXTRAORDINARIOS.

Se presentarán:

- Un informe extraordinario cada seis meses (contando desde el inicio del contrato) que refleje la información de ese periodo concreto de tiempo.

- Un informe al año (contando desde el inicio del contrato) que refleje la información de ese periodo concreto de tiempo.

5.2.8. REMISIÓN DE LA INFORMACIÓN AL CNPIC Y LA OCC.

La forma de remitir esta información al CNPIC y la OCC será a través de sistemas informáticos y procedimientos que garanticen la confidencialidad y la integridad de la misma.

El envío de informes, informes extraordinarios, alertas y notas diarias se realizará por correo electrónico a una dirección de correo a determinar por el CNPIC y la OCC.

El material adjunto a los reportes anteriores que por su tamaño no permita el envío a través de correo electrónico, se pondrá a disposición del CNPIC y la OCC a través de un servicio de repositorio que facilite su descarga y que mantenga las debidas medidas de seguridad, confidencialidad y disponibilidad de este material.

5.2.9. EXPOSICIÓN DE LA INFORMACIÓN.

Respecto al análisis de la información aportada al CNPIC y la OCC, ésta deberá estar correctamente interrelacionada y organizada, es decir, el análisis de la información ha de hacerse en su contexto y relacionándolo si es el caso, con aquella otra información que ya se haya reportado.

Respecto a las entidades digitales reportadas al CNPIC y la OCC, siempre que sea posible se identificará personalmente a las mismas en las materias objeto de los informes, alertas y notas diarias informando por ejemplo y sin ser una lista cerrada de nombre y apellidos y otros datos de filiación, perfiles en redes sociales, direcciones de correo electrónico, ubicación donde se encuentra, adscripción, pertenencia o afinidad a grupos y organizaciones, etc.

Respecto al contenido reportado a CNPIC y la OCC, si en el mismo se reporta información técnica, tal como pudiera ser por ejemplo un ciberataque, se aportarán además del correspondiente análisis, todos los datos técnicos posibles así como evidencias de los mismos.

5.2.10. RETROALIMENTACIÓN DE LA EMPRESA ADJUDICATARIA.

Se establecerá un sistema de retroalimentación por parte de la empresa adjudicataria, en el cual el CNPIC y la OCC puedan:

- Enviar datos sobre los cuales sea necesario encontrar información detallada, incluyéndose por tanto dentro de los elementos que la adjudicataria ha de investigar.
- Reconducir las investigaciones que lleve a cabo la empresa adjudicataria si la información obtenida por la misma y remitida al CNPIC y la OCC no satisface las necesidades de éste.
- Aclarar determinados aspectos de la información que le haya sido remitida por parte de la empresa adjudicataria.

El sistema de retroalimentación establecido habrá de permitir esta retroalimentación durante la vigencia del contrato y permitirá su ejecución mediante correo electrónico y teléfono. No obstante lo anterior, tanto la empresa adjudicataria como el CNPIC y la OCC podrán acordar reuniones de coordinación entre las dos partes.

5.2.11. COLABORACIÓN ENTRE EMPRESA ADJUDICATARIA Y EL CNPIC Y LA OCC.

Además del sistema de retroalimentación previsto en el apartado anterior, para el suministro de información especificados en el apartado 3.3 se realizará previamente una reunión con el CNPIC y la OCC a los efectos de planificar los procesos de trabajo dentro del ciclo de inteligencia para satisfacer las necesidades de información relativas a los citados apartados.

Así mismo, el CNPIC y la OCC se reservan el derecho de poder verificar en cualquier momento que se está dando cumplimiento a los procesos de trabajo planificados en el párrafo anterior. Para llevar a cabo esta verificación, el CNPIC y la OCC podrán plantear a la empresa adjudicataria en cualquier momento el llevar a cabo en su caso, las reuniones oportunas en las instalaciones de la adjudicataria para supervisar in situ los diferentes procesos de trabajo (como por ejemplo y sin ser una lista cerrada, las fuentes de obtención, entidades y grupos objeto de seguimiento, herramientas utilizadas para la obtención, tratamiento y análisis de los datos, etc.).

6. ACUERDOS DE NIVEL DE SERVICIO (ANS)

El adjudicatario queda obligado al cumplimiento de la ejecución total de las prestaciones recogidas en las ofertas que de cumplimiento a los presente pliego y en las prescripciones del contrato.

Asimismo, la prestación de servicios del adjudicatario deberá cumplir unos estándares de calidad mínimos que permitan hacer un aprovechamiento adecuado y den respuesta a las necesidades del CNPIC y la OCC. En caso de que los servicios no alcancen estos mínimos de calidad requeridos se considerará la existencia de un incumplimiento de acuerdo con el modelo recogido en este apartado.

A continuación se describe el modelo de penalizaciones que se aplicarán por el incumplimiento de los indicadores y Acuerdos de Nivel de Servicio ("ANS") definidos, de acuerdo con los criterios, cuantificación y método de cálculo establecidos más adelante, entendiendo que un mismo hecho puede dar lugar a la aplicación de diferentes incumplimientos y las correspondientes penalizaciones de igual o diferente tipo.

El importe total de las penalizaciones no podrá ser superior al 10% del presupuesto anual del contrato. De acuerdo con lo establecido en el artículo 212 de la LCSP el CNPIC y la OCC se reservarán el derecho a resolver el contrato cuando el cumplimiento de las diferentes prestaciones sea notablemente defectuoso o alcance los umbrales de las penalizaciones recogidos en la legislación vigente.

En ningún caso las penalizaciones tendrán finalidad recaudatoria, por lo que su aplicación no sustituirá ni minorará la indemnización que por daños y perjuicios pudiera resultar de los correspondientes incumplimientos.

TIPO	NOMBRE	DESCRIPCIÓN	FORMULA DE CÁLCULO	PERIODICIDAD (T)	UMBRAL INICIAL (Ui)	UMBRAL FINAL (Uf)	PENALIZACIÓN MÁXIMA (Pmax)
Personal	Exceso de rotación	Abandono voluntario o forzoso del servicio por parte de un recurso humano incluido al inicio del periodo de medición del indicador	Número de personas desvinculadas del equipo	Trimestral	1	3	20% del coste mensual del servicio o equivalente en pago semestral o anual
Personal	Tiempo de reposición	Tiempo de sustitución de un recurso por otro en caso de rotación del personal	Días de desviación respecto del término de reposición de recursos definido	Por recurso	5 días	15 días	10% del coste mensual del servicio o equivalente en pago semestral o anual
Operativa AlertPIC	ALP-Gestión usuarios	Gestión de usuarios adscritos (altas, bajas, modificaciones)	Horas de desviación en la gestión respecto de las definidas en procedimientos internos	Por cada requerimiento de gestión	12 horas	24 horas	10% del coste mensual del servicio o equivalente en pago semestral o anual
Operativa AlertPIC	ALP-Distribución software	Distribución de software para equipos clientes	Días de desviación en la distribución respecto de las definidas en procedimientos internos	Por cada requerimiento de distribución	1 día	7 días	10% del coste mensual del servicio o equivalente en pago semestral o anual
Operativa AlertPIC	ALP-Emisión de avisos	Emisión de avisos corporativos	Horas de desviación en la remisión de información respecto de las definidas en procedimientos internos	Por cada solicitud de emisión	1 hora	6 horas	10% del coste mensual del servicio o equivalente en pago semestral o anual
Operativa AlertPIC	ALP-Gestión comunicaciones	Gestión de comunicaciones entre CNPIC y la OCC y los usuarios. Atención a peticiones, llamadas, etc.	Horas de desviación en la comunicación respecto de las definidas en procedimientos internos	Por cada comunicación	1 hora	6 horas	10% del coste mensual del servicio o equivalente en pago semestral o anual

TIPO	NOMBRE	DESCRIPCIÓN	FORMULA DE CÁLCULO	PERIODICIDAD (T)	UMBRAL INICIAL (Ui)	UMBRAL FINAL (Uf)	PENALIZACIÓN MÁXIMA (Pmax)
Operativa incidentes 40/2013	2013-40_Comunicación Telefónica	Puesta en conocimiento de requerimiento	Horas de desviación en la comunicación telefónica respecto de las definidas en procedimientos internos	Por cada requerimiento Directiva 2013/40	0,5 horas	2 horas	20% del coste mensual del servicio o equivalente en pago semestral o anual
Operativa incidentes 40/2013	2013-40_Remisión de información	Remisión de requerimiento a FCSE	Horas de desviación en la remisión de información a FCSE respecto de las definidas en procedimientos internos	Por cada requerimiento Directiva 2013/40	0,5 horas	2 horas	10% del coste mensual del servicio o equivalente en pago semestral o anual
Operativa incidentes 40/2013	2013-40_Seguimiento de gestión	Remisión de información a requirente si procede	Horas de desviación en la comunicación telefónica respecto de las definidas en procedimientos internos	Por cada requerimiento Directiva 2013/40	0,5 horas	2 horas	10% del coste mensual del servicio o equivalente en pago semestral o anual
Operativa incidentes 12/2018	12-2018_Comunicación interna incidente	Remisión de la ficha de apertura de incidente	Horas de desviación en la entrega respecto de las definidas en procedimientos internos	Por incidente NIVEL 2	1 hora	6 horas	20% del coste mensual del servicio o equivalente en pago semestral o anual
Operativa incidentes 12/2018	12-2018_Actualización incidente	Remisión de la ficha de actualización de incidente	Horas de desviación en la entrega respecto de las definidas en procedimientos internos	Por incidente NIVEL 2	1 hora	6 horas	10% del coste mensual del servicio o equivalente en pago semestral o anual

TIPO	NOMBRE	DESCRIPCIÓN	FORMULA DE CÁLCULO	PERIODICIDAD (T)	UMBRAL INICIAL (Ui)	UMBRAL FINAL (Uf)	PENALIZACIÓN MÁXIMA (Pmax)
Operativa incidentes 12/2018	12-2018_Cierre incidente	Remisión de la ficha de cierre de incidente	Horas de desviación en la entrega respecto de las definidas en procedimientos internos	Por incidente NIVEL 2	1 hora	6 horas	10% del coste mensual del servicio o equivalente en pago semestral o anual
Operativa incidentes 12/2018	12-2018_Comunicación externa incidente	Remisión de la ficha al destino indicado	Horas de desviación en la remisión respecto de las definidas en procedimientos internos	Por incidente NIVEL 2	1 hora	6 horas	10% del coste mensual del servicio o equivalente en pago semestral o anual
Operativa incidentes 12/2018	12-2018_Gestión incidente	Remisión de la ficha apertura/actualización/cierre de incidente	Días de desviación en la entrega respecto de las definidas en procedimientos internos	Por incidente NIVEL 1	1 días	7 días	10% del coste mensual del servicio o equivalente en pago semestral o anual
Provisión de información	Plazos de los entregables	Grado de satisfación del CNPIC y la OCC con respecto a los plazos en los que se remiten los entregables.	Un punto por cada retraso mayor de un día.	Anual	1	3	10% del coste mensual del servicio o equivalente en pago semestral o anual
Provisión de información	Contenido, estructura y formato de los entregables	Grado de satisfacción del CNPIC y la OCC respecto a la estructura, formato y contenidos de los entregables	Un punto por cada informe con contenidos insuficientes. Medio punto por cada informe con estructura o formatos incorrectos.	Anual	2	4	10% del coste mensual del servicio o equivalente en pago semestral o anual

TIPO	NOMBRE	DESCRIPCIÓN	FORMULA DE CÁLCULO	PERIODICIDAD (T)	UMBRAL INICIAL (Ui)	UMBRAL FINAL (Uf)	PENALIZACIÓN MÁXIMA (Pmax)
Provisión de información	Repositorio para descarga de material que por su tamaño no permita envío por correo	Grado de satisfacción del CNPIC y la OCC respecto al servicio de repositorio que facilite la descarga del material que por su tamaño no permita el envío a través de correo electrónico	Un punto por cada ocasión en la que se encuentre indisponible un máximo de 24h	Anual	1	3	10% del coste mensual del servicio o equivalente en pago semestral o anual
Calidad	Calidad del sistema de gestión de incidentes	Grado de satisfacción del CNPIC y la OCC respecto del servicio prestado	Puntuación de 1 a 10 en encuestas realizadas a CNPIC y la OCC	Mensual	8	5,5	20% del coste mensual del servicio o equivalente en pago semestral o anual
Calidad	Idoneidad de los informes técnicos aportados	Grado de satisfacción del CNPIC y la respecto de la calidad de los informes técnicos	Puntuación de 1 a 10 en encuestas realizadas a CNPIC y la OCC	Mensual	8	5,5	10% del coste mensual del servicio o equivalente en pago semestral o anual
Calidad	Satisfacción respecto de los informes técnicos aportados	Grado de satisfacción del CNPIC y la OCC respecto de la idoneidad de los informes técnicos	Puntuación de 1 a 10 en encuestas realizadas a CNPIC y la OCC	Mensual	8	5,5	20% del coste mensual del servicio o equivalente en pago semestral o anual

6.1. MODELO DE PENALIZACIONES POR LOS SERVICIOS

El licitador deberá ajustarse al modelo penalizaciones que a continuación se describe y que incluye los siguientes puntos:

- Cálculo de las penalizaciones
- Aplicación de las penalizaciones
- Irregularidades en las medidas

6.1.1. CÁLCULO DE LAS PENALIZACIONES

Las penalizaciones se aplicarán por incumplimiento de los Niveles de Servicio indicados en la tabla de Acuerdos de Nivel de Servicio.

El cálculo del importe de la penalización se realizará sobre el importe de facturación del servicio por el periodo de cálculo o equivalente.

Previa exposición de las fórmulas, se exponen a continuación las definiciones de los conceptos principales:

- Umbral inicial (Ui): valor a partir del cual se empezará a penalizar el servicio. Siempre tendrá un valor positivo.
- Umbral final (Uf): valor a partir del cual la penalización es máxima (Pmax). Siempre tendrá un valor positivo.
- Pmax: penalización máxima aplicable por cada ANS cuando se llega o se supera el umbral final.
- Tipo de penalización: las penalizaciones pueden ser por proyecto o por servicio. En cada ANS se especificará el tipo.
- Valor: es el valor del indicador del servicio que se comparará con los umbrales establecidos en el pliego.
- Penalización (Valor): es el valor de la penalización en función del valor del indicador.
- Importe Facturable (IF): suma del importe a facturar mensualmente como consecuencia de las penalizaciones por incumplimiento de ANS.

A continuación se indican las fórmulas que serán de aplicación para cada ANS especificado en el pliego:

Si Ui > Uf	Si valor ≥ Ui	: P(valor) = 0
	Si Ui > valor > Uf	: P(valor) = Pmax [(Ui - valor)/(Ui – Uf)]
	Si valor ≤ Uf	: P(valor) = Pmax
Si Ui = Uf	Situación no existente en indicadores	
Si Ui < Uf	Si valor ≤ Ui	: P(valor) = 0
	Si Ui < valor < Uf	: P(valor) = Pmax [(valor- Ui)/(Uf – Ui)]
	Si valor ≥ = Uf	: P(valor) = Pmax

Tabla 1. Fórmulas de aplicación para los ANS

Mensualmente se calculará el importe mensual de los ANS que son aplicables y se consolidará en el indicador IF (Importe Facturable).

- IF = Σ (Penalizaciones aplicables de todos los ANS)
- IF será el importe global de la factura mensual.

La suma de los IFS acumulados de todos los meses de la duración del contrato en ningún caso puede superar el 10% del importe total de contrato. En caso de hacerlo será necesario revisar con detalle los motivos de los incumplimientos que han generado esta situación, sin perjuicio de la disposición de las facultades del CNPIC y la OCC de resolución contractual reconocidas en la normativa de contratación vigente.

6.1.2. APLICACIÓN DE LAS PENALIZACIONES.

El Gabinete de Coordinación y Estudios tiene la potestad de decidir aplicar las penalizaciones económicas o bien las compensaciones en servicios equivalentes.

El Gabinete de Coordinación y Estudios tiene la potestad de decidir no aplicar las penalizaciones asociadas por el incumplimiento de los niveles de servicio acordados en determinadas casuísticas. Como regla general quedan excluidas las penalizaciones cuando:

- Existan situaciones extraordinarias que den lugar a alteraciones que desvirtúen la medida.
- Cuando se produzca una situación excepcional de un incremento drástico de la actividad, no atribuible al adjudicatario que impida la consecución de los ANS acordados.
- Cuando la desviación sea provocada por componentes que no están bajo la responsabilidad del adjudicatario.
- Cuando el servicio quede parado por causas ajenas al mismo servicio, ya sean paradas programadas o no.

Al inicio del contrato, el adjudicatario podrá solicitar al Gabinete de Coordinación y Estudios la revisión temporal y transitoria de las penalizaciones sobre los ANS que crea necesarias en atención a elementos de carácter extraordinario. El Gabinete de Coordinación y Estudios estudiará su viabilidad y/o aplicación y las aprobará por escrito, en su caso.

6.1.3. INCIDENCIAS EN LAS MEDIDAS DE INDICADORES

En caso de incidencias en la medida del valor de un Indicador asociado a un ANS debidas a errores materiales, o cuando exista falta de colaboración por parte del adjudicatario en la determinación del valor correcto, se considerará que el indicador no ha llegado al Nivel Mínimo de Servicio, aplicándose la penalización correspondiente.

Se considerará que hay incidencia en la medida de un Indicador cuando el valor de éste, facilitado por el adjudicatario difiera en más de un 15% respecto del valor real auditado que resulte del proceso de auditoría que se lleve a cabo desde el servicio.

Se considerará falta de colaboración cuando confluyan todos los siguientes factores:

- Que el auditor que se designe en el mencionado proceso de auditoría aporte evidencia de una solicitud de información en un plazo concreto dirigida al adjudicatario.

- Que la solicitud de información pedida y el plazo sean razonables a juicio del Gabinete de Coordinación y Estudios.
- Que el adjudicatario no pueda aportar ninguna evidencia que pruebe que se haya facilitado la información solicitada dentro del plazo especificado o en su defecto no haya dado una explicación razonable del motivo del retraso.

6.1.4. FACTURACIÓN DE LAS PENALIZACIONES

El importe correspondiente a las penalizaciones aplicadas al adjudicatario es resultado de sumar los importes de penalización correspondientes al incumplimiento de los niveles de servicios acordados en el contrato. Las penalizaciones en forma de dedicación se devolverán con horas de servicio. Si esto no fuera posible se convertirán en importe y se compensarán de acuerdo con lo establecido en el presente apartado.

El adjudicatario abonará, mediante el procedimiento de compensación, las penalizaciones automáticamente a la factura que por sus servicios deba abonar. En caso de no poder compensarse los importes por causas imputables al adjudicatario, éste deberá satisfacer el importe mediante el pago correspondiente.

La no incorporación de esta reducción del importe por cualquier causa (tramitación, incidencia en plazos de facturación, etc.) no eximirá al adjudicatario de su obligación de pago en los términos que se determine.

7. MEDIOS HUMANOS A DISPOSICIÓN DEL CONTRATO

7.1. MEDIOS HUMANOS A DISPOSICIÓN DEL CONTRATO

El adjudicatario deberá poner a disposición del contrato los recursos personales necesarios para su correcta ejecución. En todo caso, deberá designar:

COORDINADOR GENERAL: Esta figura tendrá las funciones de interlocución con el CNPIC y la OCC, y será el responsable de coordinar todos los trabajos a desarrollar por la adjudicataria.

Requisitos mínimos. Para el ejercicio de las funciones de Coordinador General, será imprescindible reunir los siguientes requisitos:

- EXPERIENCIA PROFESIONAL: Experiencia acreditada en trabajos de consultoría en materia de ciberseguridad de al menos CINCO AÑOS (5).
- FORMACIÓN: Titulación universitaria equivalente a Nivel 3: Master Universitario.
- HABILIDADES: Conocimientos demostrables, mediante formación o experiencia previa en la materia, en herramientas de generación y presentación de información para hacer más eficiente la comunicación, así como en la redacción de informes ejecutivos y asesoría a alta dirección.

Requisitos a valorar

- A) Encontrarse en posesión de Master Universitario en materia de ciberseguridad
- B) Disponer de certificaciones en la materia. CEH/OSCP/CISA/CISM/CISSP

ANALISTA: El adjudicatario deberá garantizar que el servicio de análisis en profundidad de las tareas de protección y seguridad de la información de Infraestructuras Críticas y Operadores de Servicios Esenciales y operadores estratégicos o sus proveedores cuente con el número necesario de analistas de ciberseguridad, asegurando siempre la presencia de DOS analistas como mínimo (cada uno con un perfil de los que se describen en este apartado), de lunes a viernes, en las instalaciones del CNPIC y la OCC y de un analista localizable por vía telefónica o por correo electrónico los sábados, domingos y festivos, durante toda la vigencia del contrato. Los analistas deberán cumplir con el siguiente perfil profesional:

ANALISTA 1. PERFIL INCIDENTES

Requisitos mínimos. Para el ejercicio de las funciones de Analista, será imprescindible reunir los siguientes requisitos:

- EXPERIENCIA PROFESIONAL: Experiencia acreditada en materia de análisis estático y dinámico de malware, hacking ético, manejo de lenguaje de programación Python y Perl, así como auditoría a sistemas de información y comunicación Microsoft Windows, GNU/Linux y plataformas web, de al menos DOS AÑOS (2).
- FORMACIÓN: Titulación universitaria mínima equivalente a Nivel 2: Grado. Disponer de titulación equivalente a Ingeniero Superior o Técnico en Informática, Telecomunicaciones o semejante.

- HABILIDADES: Conocimientos demostrables, mediante formación o experiencia previa en la materia, en la redacción de informes técnicos con calidad en materia de ciberseguridad.

Requisitos a valorar

- A) Encontrarse en posesión de Master Universitario en materia de ciberseguridad
- B) Disponer de certificaciones en la materia. CEH/OSCP/CISA/CISM/CISSP

ANALISTA 2. PERFIL INTELIGENCIA

Requisitos mínimos. Para el ejercicio de las funciones de Analista, será imprescindible reunir los siguientes requisitos:

- EXPERIENCIA PROFESIONAL: Experiencia acreditada en materia de búsquedas en fuentes de información y análisis de inteligencia y de información OSINT (Open Source Intelligent) y SOCMINT (Social Media Intelligence), o conocimientos en movimientos extremistas, radicales y geointeligencia de al menos DOS AÑOS (2).
- FORMACIÓN: Titulación universtaria mínima equivalente a Nivel 2: Grado. Disponer de titulación equivalente a Ingeniero Superior o Técnico en Informática, Telecomunicaciones o semejante, o de ciencias de la información, comunicación audiovisual o similar.
- HABILIDADES: Conocimientos demostrables, mediante formación o experiencia previa en la materia, en la redacción de informes técnicos con calidad en materia de ciberinteligencia.

Requisitos a valorar

- A) Encontrarse en posesión de Master Universitario en materia de ciberseguridad
- B) Disponer de certificaciones en la materia. CEH/OSCP/CISA/CISM/CISSP

OPERADOR: La empresa adjudicataria deberá garantizar que el servicio de soporte a la gestión de incidencias de ciberseguridad (definido en los apartados 3.1 y 4.1 del presente Pliego) cuente con el número necesario de operadores para la atención adecuada del mismo, siempre en número no inferior a CINCO (5), asegurando siempre la presencia de al menos un operador durante 24 horas al día, siete días a la semana, durante toda la vigencia del contrato. Los operadores deberán cumplir con el siguiente perfil profesional:

- EXPERIENCIA PROFESIONAL: Experiencia acreditada de UN AÑO (1) en materia de gestión de incidentes de ciberseguridad, o en materia de tareas de análisis de inteligencia.
- FORMACIÓN: Estudios mínimos reglados de Bachiller o equivalentes reconocidos por el Ministerio de Educación y Formación Profesional del Gobierno de España.

El mismo día de la formalización del contrato, la empresa adjudicataria deberá facilitar al CNPIC y la OCC la relación nominal del personal adscrito al contrato, con indicación de nombre, apellidos, número de DNI, teléfono móvil y dirección de correo electrónico de cada uno de ellos, así como la documentación acreditativa sobre el cumplimiento de los requisitos correspondientes al perfil profesional exigido.

Teniendo en cuenta las características concurrentes en el presente contrato, el lugar de prestación de los servicios, así como el carácter confidencial de la información a manejar, la Secretaría de Estado de Seguridad, a través del CNPIC y la OCC se reserva la facultad de rechazar a alguno de los profesionales propuestos, debiendo, en tal caso, ser sustituido por otro profesional que cumpla los mismos requisitos exigidos para el profesional sustituido en los anteriores párrafos de este apartado. Esta facultad se mantendrá a lo largo del periodo de vigencia del contrato.

7.2. CONDICIONANTES DEL EQUIPO DE TRABAJO A DISPOSICIÓN DEL CONTRATO

No podrán formar parte del equipo de trabajo personas con contrato comprometido con otra entidad, pública o privada, para el mismo periodo de ejecución de esta contratación. La comprobación fehaciente de esta anomalía podrá significar la resolución del contrato.

El adjudicatario asumirá los costes derivados de la formación y actualización formativa del personal que se adscriba a este proyecto.

El adjudicatario deberá indicar al personal adscrito al proyecto las tareas que se deban ejecutar en el marco de la prestación de estos servicios, así como la metodología de trabajo a llevar a cabo en el caso de que los incidentes atendidos deban ser escalados a un nivel superior de resolución.

El adjudicatario velará especialmente porque los trabajadores adscritos a la ejecución del contrato desarrollen su actividad sin extralimitarse en las funciones desempeñadas respecto de la actividad delimitada en los Pliegos que rigen este contrato.

7.3. MODIFICACIONES EN LA COMPOSICIÓN DEL EQUIPO DE TRABAJO

El adjudicatario procurará que exista estabilidad en el equipo de trabajo, y que las variaciones en su composición sean puntuales y obedezcan a razones justificadas, en orden a no alterar el buen funcionamiento del servicio.

En caso de que el adjudicatario, en el marco de la prestación de los servicios descritos, tuviera que proceder a la sustitución de personal adscrito al proyecto, deberá comunicar tal circunstancia al Director Técnico con un preaviso de quince días, entregando justificación escrita, detallada y suficiente, que motive dicho cambio. En todo caso, el personal que se incorpore deberá reunirlas mismas condiciones que fueron requeridas en la constitución del equipo inicial.

Los posibles inconvenientes de adaptación al entorno de trabajo y al proyecto debidos a sustituciones de personal no influirán en el calendario de los trabajos, siendo la empresa adjudicataria la responsable de ofrecer un servicio de desarrollo uniforme.

8. MEDIOS MATERIALES A DISPOSICIÓN DEL CONTRATO.

La empresa adjudicataria deberá disponer de los siguientes medios, que los mantendrá a disposición del contrato, durante toda la vigencia del mismo:

- Una Oficina operativa abierta en Madrid, dotada con líneas fijas de teléfono y fax y dirección de correo electrónico.
- Líneas de teléfono móvil y dirección de correo electrónico individual para el Coordinador General y los operadores y analistas mencionados en el apartado 6.1 del presente PPT.
- Equipos portátiles, licencias de software y medios necesarios para la ejecución de las tareas recogidas en el apartado relativo a apoyo técnico para análisis en profundidad de las tareas de protección y seguridad para la gestión, seguimiento y resolución de incidentes.

Con anterioridad a la formalización del contrato deberá facilitar al Gabinete de Coordinación y Estudios los datos referidos a la dirección postal de las oficinas en Madrid, así como números de los teléfonos fijo y móvil y del fax, las direcciones de correo electrónico, así como los medios descritos en el párrafo anterior.

El Gabinete de Coordinación y Estudios proveerá la conexión a los sistemas que sean necesarios para el cumplimiento de las tareas descritas en este documento.

En caso de que el adjudicatario provea recursos técnicos propios para el buen desarrollo del proyecto, asegurará su integración o interconexión con los sistemas propios empleados por el CNPIC o por la OCC, según corresponda.

El adjudicatario suministrará el listado de aquellos elementos técnicos que serán empleados como parte de la prestación del servicio de manera eficiente. La adaptación de dichos elementos a las vicisitudes particulares de este servicio correrá a cargo del mismo, quien estará obligado a respetar, en todo caso, las necesidades descritas en este documento.

9. LUGAR DE PRESTACIÓN DE LOS SERVICIOS

Los servicios asociados al soporte de gestión de incidencias de ciberseguridad, descrito en los apartados 3.1 y 4.1 del presente Pliego, se desarrollarán presencialmente en las instalaciones del CNPIC y la OCC, actualmente ubicadas en El Pardo, Madrid.

Los servicios asociados al servicio de análisis en profundidad de las tareas de protección y seguridad de la información de Infraestructuras Críticas, Operadores de Servicios Esenciales y otros operadores estratégicos, o sus proveedores, para la gestión, seguimiento y resolución de incidencias, se desarrollarán indistintamente en las oficinas de la empresa adjudicataria y en las instalaciones del CNPIC y la OCC actualmente ubicadas en El Pardo, Madrid. No obstante, se asegurará la presencia de al menos dos “analistas de ciberseguridad” en estas últimas instalaciones, en días laborables de lunes a viernes, durante los horarios habituales de trabajo del CNPIC y la OCC.

Con relación a estos últimos servicios, en los sábados, domingos y festivos se asegurará la posibilidad de acudir a los servicios de un analista de ciberseguridad para la realización de tareas incluidas en los mismos, cuando no sea posible, por razones de urgencia, esperar a la intervención de dicho profesional en el primer día hábil siguiente.

10. INCORPORACIÓN DEL EQUIPO Y COMIENZO DEL SERVICIO

El contrato comenzará a ejecutarse por el contratista el mismo día del inicio de su vigencia.

No obstante, dentro de los siete primeros días de vigencia, como máximo, el contratista deberá llevar a cabo la planificación general de los servicios, la organización de los equipos de trabajo y la disposición de los medios necesarios para ello. Transcurrido este plazo, los equipos de trabajo y los medios deberán estar plenamente operativos para la efectiva prestación de los servicios descritos en los apartados 3 y 4 del presente PPT, sin dilación de ningún tipo.

11. REQUISITOS DE SEGURIDAD

La seguridad es un factor primordial en el presente servicio. Todos los ámbitos del presente servicio se realizarán de forma que cumplan los requisitos de seguridad establecidos al efecto.

11.1. SEGURIDAD Y CONFIDENCIALIDAD DE LA INFORMACIÓN

La empresa adjudicataria y el personal encargado de la realización de las tareas guardarán secreto profesional sobre todas las informaciones, documentos y asuntos a los que tengan acceso o conocimiento durante la vigencia del contrato, estando obligados a no hacerlos públicos o enajenar cuantos datos conozcan como consecuencia o con ocasión de su ejecución, incluso después de finalizar el plazo contractual.

El adjudicatario tomará las medidas adecuadas para garantizar la confidencialidad del servicio en los términos que se señalan en el apartado correspondiente del Cuadro de Características del PCAP.

11.2. PROPIEDAD INTELECTUAL

Los derechos de explotación de todo el material, documentos, desarrollos, código fuente, así como de cualquier resultado de la I+D+i, y cualesquiera otros resultados elaborados por el contratista, y/ o sus empleados, realizados al amparo del presente contrato para la prestación del servicio serán propiedad del Gabinete de Coordinación y Estudios (Ministerio del Interior), con exclusividad y en todo el mundo, a no ser que exista escrito en contrario debidamente firmado por el Gabinete de Coordinación y Estudios. Todo ello será extensible en cualquier modalidad y bajo cualquier formato y sin perjuicio de los derechos de terceros sobre componentes integrados dentro de los resultados. El contratista reconoce los derechos de Propiedad Intelectual del Gabinete de Coordinación y Estudios sobre todas las tareas desarrollas en la prestación del presente servicio, cediendo todos los derechos de explotación y propiedad de los mismos.

El contratista cede de manera exclusiva al Gabinete de Coordinación y Estudios todos los derechos necesarios (en particular, los derechos de reproducción, comunicación pública, distribución y transformación), sobre los resultados derivados de su labor en el marco de la prestación de este servicio. A los efectos de este contrato, si el resultado consiste en software, el concepto de resultado comprende también su documentación preparatoria, la documentación técnica y los manuales de uso del desarrollo. Por tanto, junto con el software propiamente dicho deberán entregarse todos aquellos elementos que son esenciales para su correcto funcionamiento, o para posibles desarrollos posteriores; y todos los entregables recogidos en el Pliego, y por tanto la documentación generada para la creación del software como son los datos, listados, software, diagramas y esquemas elaborados en la fase de análisis.

El CNPIC y la OCC podrán realizar copias del software o base de datos, e instalarlos en cuántos equipos informáticos y/o electrónicos estime oportuno, y utilizarlos en su actividad; así como modificar o adaptar en cualquier momento el código fuente, el programa, el sistema y en general todos los medios puestos a disposición del proyecto necesarios para su funcionamiento y los resultados obtenidos con el fin de adaptarlo a sus características o necesidades específicas y/o ponerlos a disposición de terceros.

El contratista garantiza que es el titular de los correspondientes derechos de propiedad intelectual e industrial cedidos en relación con los resultados, o tiene derechos para cederlos y que la consecuente cesión de derechos no infringirá ningún derecho de terceros, las correspondientes licencias de uso originarias que regulen cualquier componente de los resultados, la normativa vigente, o el presente acuerdo.

En el supuesto de que el contratista haya aportado como resultado elementos sobre las que existan derechos de terceros, lo establecido en los párrafos anteriores quedará condicionado a las limitaciones establecidas en la correspondiente licencia de terceros, en particular las licencias de software de fuentes abiertas que puedan aplicarse a dicha contribución. En consecuencia, el contratista, se compromete a informar y documentar detalladamente al Gabinete de Coordinación y Estudios, y prestar ayuda a éste, en cuanto a información y documentación, sobre cualesquiera reservas y derechos legales de terceros que pudieran existir sobre las contribuciones que el mismo haya aportado a los resultados.

Si los trabajos para su compatibilidad con la solución propuesta tuvieran que respetar licenciamientos de fuentes abiertas se elegirá entre los diferentes licenciamientos posibles que no vulneren los derechos de terceros la opción más compatible y beneficiosa para los intereses del CNPIC y la OCC. En este caso serán el CNPIC y la OCC, en base a las propuestas de licenciamiento legalmente posibles formuladas, quienes seleccionen la que desee utilizar.

- En todo, en lo relativo del uso de software para la prestación de los servicios:

En ningún caso el contratista mantendrá, instalará o configurará software sin las licencias y permisos debidos. El contratista garantiza al Gabinete de Coordinación y Estudios que todo el software que sea empleado para implementar sus funciones es original, y no vulnera ninguna ley, derecho o interés de tercero alguno, en especial los referidos a propiedad industrial e intelectual, y que cuenta con las correspondientes licencias de uso. Además se cederá al Gabinete de Coordinación y Estudios derechos sobre dichas licencias si la incorporación del software fuese necesaria para la operatividad o funcionamiento de los resultados objeto del contrato.

- En todo caso, en lo relativo a la responsabilidad:

El contratista vendrá obligado a exonerar al Gabinete de Coordinación y Estudios de cualquier tipo de responsabilidad frente a terceros, por reclamaciones de cualquier índole que tengan origen en el incumplimiento de las obligaciones de propiedad intelectual o por licenciamientos inadecuados a las necesidades del Gabinete de Coordinación y Estudios que impidan el cumplimiento del objeto del presente contrato y responderá frente a este de dichas acciones.

- En todo caso, en lo relativo a los logos y marcas:

El contratista no podrá hacer uso del nombre, logotipo o cualquier signo distintivo o material que le haya facilitado el Gabinete de Coordinación y Estudios, en concreto el CNPIC y la OCC para el cumplimiento de las obligaciones derivadas del presente contrato fuera de las circunstancias y fines de éste, ni una vez terminada la vigencia del mismo.

12. PLANIFICACIÓN, DIRECCIÓN Y SEGUIMIENTO DE LOS TRABAJOS

Corresponde al Gabinete de Coordinación y Estudios, que las ejercerá a través del CNPIC y la OCC, las funciones de dirección, coordinación general, seguimiento y supervisión de las prestaciones del contrato.

El Gabinete de Coordinación y Estudios designarán un Director Técnico cuyas funciones en relación con el objeto del presente pliego serán las siguientes:

- Mantener la interlocución con la empresa adjudicataria a través del Coordinador General designado por la misma
- Velar por el cumplimiento de los servicios prestados
- Emitir las certificaciones parciales de la realización de los mismos
- Convocar las reuniones que estime necesarias entre el adjudicatario (a través del Coordinador General) y el CNPIC y la OCC, al objeto de realizar un seguimiento adecuado del proyecto, analizando y valorando las incidencias o problemáticas acaecidas en el seno de la prestación del servicio. El adjudicatario, a través del Coordinador General designado por el mismo, tendrá la obligación de asistir a dichas reuniones y colaborar en lo que resulte preciso. La convocatoria a dichas reuniones deberá realizarse por el Director Técnico del CNPIC y la OCC con la suficiente antelación que garantice la adecuada presencia del personal designado por el adjudicatario. Asimismo, el Coordinador General designado por el adjudicatario podrá proponer las reuniones que considere oportunas, que se llevarán a cabo previa valoración de idoneidad por parte del Director Técnico del CNPIC y la OCC. En todo caso, el adjudicatario será el responsable de la elaboración y distribución de las actas que se deriven de la celebración de las reuniones mantenidas entre el CNPIC y la OCC y el adjudicatario.
- Incorporar al servicio, durante su realización, las personas que estime necesarias para verificar y evaluar todas las actuaciones a su cargo.

El Coordinador General designado por la adjudicataria tendrá entre sus obligaciones las siguientes:

- Actuar como interlocutor único de la empresa adjudicataria frente al CNPIC y la OCC y/o Ministerio del Interior canalizando las comunicaciones pertinentes, entre la empresa

contratista y el personal prestatario de los servicios descritos de forma directa; así como en todo lo relativo a las cuestiones derivadas de la ejecución del contrato.

- Distribuir el trabajo entre el personal encargado de la ejecución del contrato, e impartir a dichos trabajadores las órdenes e instrucciones de trabajo que sean necesarias en relación con la prestación del servicio contratada.
- Supervisar el correcto desempeño, por parte del personal integrante del equipo de trabajo, de las funciones que tengan encomendadas, así como de controlar la asistencia de dicho personal al puesto de trabajo, sin perjuicio de los controles de acceso que se deriven del uso de las instalaciones del CNPIC y la OCC y/o Ministerio del Interior.
- Organizar el régimen de vacaciones del personal adscrito a la ejecución del contrato, debiendo a tal efecto coordinarse adecuadamente la empresa adjudicataria con el CNPIC y la OCC, con el fin de no alterar el buen funcionamiento del servicio.
- Informar al CNPIC y la OCC acerca de las variaciones, ocasionales o permanentes, en la composición del equipo de trabajo adscrito a la ejecución del contrato.
- Notificar a CNPIC y la OCC las incidencias del proyecto que sean transcendentes para el mismo y el grado de evolución de los servicios.
- Recibir las peticiones periódicas del CNPIC y la OCC acerca de la evolución de los servicios, informes, análisis y resultados.
- Generar la documentación de los trabajos realizados conforme a los criterios que, en cada caso, establezca el Director Técnico del CNPIC y la OCC. Toda la documentación generada por el adjudicatario durante la ejecución del contrato será propiedad exclusiva del CNPIC y la OCC (Ministerio del Interior) sin que el adjudicatario pueda conservarla, ni obtener copia de la misma, o facilitarla a terceros sin la expresa autorización por escrito del CNPIC y la OCC, quien podrá concederla cuando lo considere oportuno y con expresión del fin, previa petición formal del adjudicatario por escrito. En caso de que lo considere necesario el Director Técnico del CNPIC y la OCC, el adjudicatario proporcionará al CNPIC y la OCC en soporte digital (CD-ROM, DVD, memoria de almacenamiento USB, Gestor Documental, etc.) la documentación generada durante la prestación de los servicios objeto del contrato, así como las informaciones que le sean requeridas.
- Facilitar al Director Técnico designado por el CNPIC y la OCC la información y documentación que éste solicite en cualquier momento para disponer de un pleno conocimiento de las circunstancias en que se desarrollan los trabajos objeto de este PPT, así como de los eventuales problemas que puedan plantearse y de las tecnologías, métodos y herramientas utilizados para resolverlos.
- Otras que puedan estimarse apropiadas para el buen funcionamiento de los servicios prestados, dentro del objeto del presente contrato.

El seguimiento y control del servicio se efectuará sobre las siguientes bases:

- Seguimiento continuo y concomitante de la evolución del servicio entre el Coordinador General y el Director Técnico.
- El Director Técnico podrá determinar los procedimientos y herramientas a utilizar para poder llevar a cabo la planificación, seguimiento y control de los servicios.
- Reuniones de seguimiento y revisiones técnicas, con periodicidad quincenal, del Coordinador General y del Director Técnico (o persona en quien éste delegue), al objeto de revisar el

grado de cumplimiento de los objetivos, los productos obtenidos conforme a la metodología empleada, las reasignaciones y variaciones de efectivos de personal dedicado al proyecto, las especificaciones funcionales de cada uno de los objetivos y la validación de las programaciones de actividades realizadas.

- El calendario de realizaciones será planificado y ajustado por períodos quincenales, con la participación y obligada aceptación del mismo por parte del adjudicatario.

Tras las revisiones técnicas, de las que se levantará acta, el Director Técnico podrá rechazar en todo o en parte los trabajos realizados, en la medida que no respondan a lo especificado en la metodología, no se ajusten a lo dispuesto en las reuniones de planificación o no superen los controles de calidad acordados.

13. TRANSFERENCIA TECNOLÓGICA

Durante la ejecución de los servicios objeto del contrato el adjudicatario se compromete, en todo momento, a facilitar a las personas designadas por el CNPIC y la OCC a tales efectos, la información y documentación que éstas soliciten para disponer de un pleno conocimiento de las circunstancias en que se prestan los servicios, así como de los eventuales problemas que puedan plantearse y de las tecnologías, métodos, y herramientas utilizadas para resolverlos.

14. DOCUMENTACIÓN DE LOS TRABAJOS

Como parte del objeto del contrato, el adjudicatario se compromete a generar, toda la documentación que sea aplicable, de la especificada en la metodología reseñada en el apartado 5 “ENTREGABLES”.

La documentación quedará en propiedad exclusiva del Gabinete de Coordinación y Estudios, y en concreto del CNPIC y la OCC, sin que el contratista pueda conservarla, ni obtener copia de la misma o facilitarla a terceros sin la expresa autorización del Centro, que la daría en su caso previa petición formal del contratista con expresión del fin.

15. TERMINOLOGÍA

Siguiendo la línea terminológica referenciada por la Estrategia de Ciberseguridad Nacional, a lo largo del presente documento, y de la prestación del servicio, se utilizará el término ciberincidente como sinónimo de incidente de seguridad en el ámbito de las Tecnologías de la Información y Comunicación (TIC).

- **INCIDENTE:** Todo hecho que tenga efectos adversos en la seguridad de las redes y sistemas de información, y que afecte o pueda afectar a algún operador crítico o estratégico, y que tendrá que ser gestionado por el adjudicatario.

- **SERVICIO DE CIBERSEGURIDAD:** Servicio prestado por el adjudicatario al Gabinete de Coordinación y Estudios (Ministerio del Interior), y de forma particular al CNPIC y a la OCC, en el marco de la contratación del presente Pliego de Prescripciones Técnicas (PPT).

- **NIVELES DE GESTIÓN:** En base a la taxonomía de los ciberincidentes comunicados, niveles de criticidad y complejidad, estos serán gestionados por un primer NIVEL 1 en exclusiva por el adjudicatario, o escalado a un NIVEL 2, donde la parte de gestión técnica recae en el CNPIC y la OCC, y la parte de gestión y seguimiento en el servicio que prestará el adjudicatario.
- **ESCALADO:** Proceso por el cual, el prestatario del servicio, eleva el nivel de gestión de un ciberincidente, del NIVEL 1 al NIVEL 2.

Madrid, 22 de octubre de 2020

El Director del Gabinete de Coordinación y Estudios

Fdo.: José Antonio Rodríguez González