GOBIERNO DE ESPAÑA
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL

Servicio de análisis y diagnóstico del talento en ciberseguridad en España

PCT. EXP. 030/20

017 TU AYUDA EN CIBERSEGURIDAD

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

INDICE

1. ALCANCE Y OBJETO DEL CONTRATO

1.1. ANTECEDENTES

S.M.E. Instituto Nacional de Ciberseguridad de España M.P., S.A. (en adelante INCIBE), es una Sociedad Mercantil Estatal dependiente del Ministerio de Asuntos Económicos y Transformación Digital a través de la Secretaría de Estado de Digitalización e Inteligencia Artificial, es la entidad de referencia para el desarrollo de la ciberseguridad y de la confianza digital de los ciudadanos, la red académica y de investigación española (RedIRIS) y las empresas, especialmente para sectores estratégicos.

La misión de INCIBE es reforzar la ciberseguridad, la confianza y la protección de la información y privacidad en los servicios de la Sociedad de la Información, aportando valor a ciudadanos, empresas, Administración, red académica y de investigación española, sector de las tecnologías de la información y las comunicaciones y sectores estratégicos en general.

La visión de INCIBE es conseguir sus objetivos mediante:

- El compromiso de profesionales altamente cualificados, comprometidos con sus proyectos y capaces de generar valor e innovación de forma continua.
- La dinamización del sector TIC, desde una perspectiva de igualdad de oportunidades, generando nuevos negocios y oportunidades para clientes, proveedores y profesionales.
- El soporte a los ciudadanos, empresas, administraciones, RedIRIS junto con sus instituciones afiliadas y sectores estratégicos, todos ellos claves para un desarrollo de las nuevas tecnologías con un alto impacto social.
- La generación de inteligencia en ciberseguridad como medio necesario para el desarrollo de tecnologías y conocimiento a aplicar en nuevas herramientas y estrategias.

Actualmente existe una gran demanda de profesionales en ciberseguridad y aunque en la última década este número se ha cuadriplicado, no alcanza a cubrir la demanda existente. Por ello, muchos países europeos están estableciendo las competiciones de ciberseguridad a nivel nacional para la búsqueda de jóvenes talentos en la materia, animándoles a seguir una carrera técnica profesional en ciberseguridad.

La proliferación de nuevas amenazas, con un grado de sofisticación creciente, conduce a la necesidad de incorporar profesionales expertos en ciberseguridad en distintos tipos de organizaciones. En este marco, INCIBE ha impulsado una serie de actuaciones que pretenden contribuir a contrarrestar la brecha entre oferta y demanda de profesionales en ciberseguridad en España.

De forma paralela, en los últimos años, se ha generado un ecosistema de estimulación, identificación y atracción de talento en ciberseguridad en torno a INCIBE, en colaboración con los centros de formación, las universidades y la iniciativa privada y buscando siempre la acción complementaria de las iniciativas que otros agentes están desarrollando para la capacitación de profesionales.

1.2. OBJETO

El objeto del presente contrato es la elaboración de un informe de diagnóstico de fuerza laboral en materia de ciberseguridad en España y la definición de escenarios de intervención que, a través de metodologías participativas con los principales actores del ecosistema, permita lograr:

- Cuantificar y segmentar la fuerza laboral actual de profesionales de la ciberseguridad en España y la demanda existente; así como sus características, conocimientos y habilidades en materia de ciberseguridad necesarias en cada uno de los segmentos (perfiles) identificados.
- Caracterizar la fuerza laboral requerida proporcionando detalles sobre estimaciones de brechas;
- Estimar la brecha actual de la fuerza laboral de ciberseguridad en España;
- Identificar las mejores prácticas en gestión del talento en las ocho economías globales con mayor madurez en el campo de la ciberseguridad (por ej. EEUU, Israel, Rusia, Canadá, Reino Unido, Malasia, China y Francia).
- Definir los escenarios de intervención para cada tipología de profesionales de la ciberseguridad identificados, revisando los pasos clave en la carrera profesional de ciberseguridad en función de la demanda identificada;
- Identificar y consensuar, con los principales actores involucrados, recomendaciones a corto, medio y largo plazo para la creación y consolidación de equipos y profesionales de ciberseguridad cualificados ahora y en el futuro.

Además, en base a los resultados del informe de diagnóstico se elaborará un plan de acción que nos permita llevar a cabo una serie de acciones justificadas.

2. REQUISITOS TÉCNICOS

2.1. CONSIDERACIONES PREVIAS

En este apartado se describen los servicios, características y requisitos que conforman el objeto del contrato y que el licitador deberá prestar, no siendo el listado que aparece a continuación una relación exhaustiva de los servicios contratados, sino las líneas generales demandadas por INCIBE, cubriendo a grandes rasgos los aspectos de tareas a realizar y resultados esperados.

Estos requisitos deben entenderse como mínimos, pudiendo los licitadores ampliarlos y mejorarlos en sus ofertas. Las propuestas que ofrezcan características inferiores y que no cubran estos mínimos, no serán tomadas en consideración en el presente procedimiento de adjudicación. El licitador puede ofertar prestaciones superiores a las solicitadas, que se considerarán positivamente en la valoración técnica de la oferta.

El contratista deberá aportar los conocimientos y metodologías así como apoyarse en las herramientas necesarias para asegurar un resultado óptimo.

El contratista se obliga a guardar secreto y a hacerlo guardar al personal que emplee para la ejecución del contrato, respecto a toda la información de la Sociedad que con motivo del desarrollo de los trabajos llegue a su conocimiento, no pudiendo utilizarla para sí o para otra persona o entidad.

2.2. DESCRIPCIÓN DE LOS TRABAJOS

El listado de los trabajos y servicios a prestar se detallan a continuación.

Adicionalmente a la realización de los mismos, el adjudicatario dará soporte a INCIBE en las tareas de logística así como en la gestión/seguimiento/actas de reuniones, etc. Se deberá especificar la metodología de trabajo que se llevará a cabo para la realización de cada uno de los trabajos indicados.

2.2.1. Elaboración del estudio de caracterización

La proliferación de programas sobre ciberseguridad se ha multiplicado en los últimos años, cuestión que responde a la dependencia de, cada vez más, sectores laborales y actividades de la vida cotidiana del sector TIC, y a la escasez de profesionales cualificados en ciberseguridad. Esta falta de profesionales se evidencia a nivel mundial, europeo y también español, y nos hace más vulnerables ante ataques.

La desconexión entre oferta y demanda de profesionales de ciberseguridad en nuestro país se manifiesta, además, en la falta de competencias demandadas por los reclutadores. A la problemática de falta de profesionales se une el hecho de que la formación y conocimientos de que disponen los escasos profesionales no está alineada con las necesidades de los reclutadores de talento: Gobierno, sector público y privado, así como el ámbito académico.

Se hace necesario que haya una efectiva conexión entre oferta y demanda de talento en ciberseguridad en España, que garantice soluciones a corto, medio y largo plazo al reto de conseguir más profesionales en ciberseguridad y mejor preparados.

En este contexto, los objetivos de este estudio son, entre otros:

- Analizar la situación actual del talento en materia de ciberseguridad en España (incluye mejores prácticas a nivel internacional) con foco en la oferta y la demanda existente y segmentado por tipología de profesional de ciberseguridad.
- Desarrollar las competencias necesarias para el ejercicio de la profesión de ciberseguridad en sus diversas facetas y para cada una de las tipologías identificadas anteriormente.
- Definir los escenarios de intervención adaptados a los distintos perfiles identificados durante el análisis y recomendaciones a corto, medio y largo plazo e indicadores para su seguimiento.
- Realizar un diagnóstico con los principales hallazgos y recomendaciones en el ámbito de la atracción y retención del talento, las competencias requeridas para los puestos de trabajo demandados, las herramientas y la administración y gestión de dicho talento;

Para ello, se necesita, en primer lugar, un diagnóstico riguroso sobre el estado actual del talento en ciberseguridad en España.

Se espera que el Estudio sobre el talento en ciberseguridad en España[1] trate, al menos, los siguientes aspectos[2]:

1. Resumen ejecutivo
2. Objetivos
3. Metodología empleada
4. Aproximación y contexto, análisis del sector en cifras. Datos de la industria española de ciberseguridad: Número de empresas, volumen de negocio, tendencia, etc. Será importante determinar no solo el estado anterior y actual del sector, sino también su desarrollo futuro. En este contexto se contemplarán, no sólo las empresas cuyo core es la ciberseguridad, sino todas aquellas que necesitan de profesionales cualificados en esta materia (tanto de perfiles técnicos como de otros perfiles que tengan relación con la ciberseguridad).
5. Análisis de la Oferta de Talento en ciberseguridad

- Introducción
- Análisis cualitativo: formación en ciberseguridad en España
    - La ciberseguridad en los distintos niveles educativos: asignaturas, estudios y competencias adquiridas
        - Educación Primaria
        - Educación Secundaria
        - Bachillerato
        - Formación Profesional
        - Universidad
        - Estudios de postgrado
    - Formación no oficial en ciberseguridad. Competencias adquiridas.

[1] El estudio a publicar llevará por título: ¿Cómo es el talento en ciberseguridad en España? Catálogo de perfiles profesionales demandados por el sector

[2] La propuesta temática no se trata de un índice cerrado, sino de una propuesta de mínimos.

  - Certificaciones profesionales
  - Cursos, MOOC
  - Otros

- El aprendizaje autodidacta en el sector de la ciberseguridad. Competencias adquiridas
  - Comunidades hackers
  - Eventos y conferencias de ciberseguridad
  - Competiciones
  - Otros
- Caracterización de la fuerza de trabajo mediante la identificación de distintos tipos de perfiles de trabajadores en el sector. Modelo basado en personas, capacidades y conocimiento. Este modelo establecerá distintas categorías, cada una de ellas puede contener distintas áreas de conocimiento y dentro de estas se describirán los distintos roles con sus funciones.

  Proporcionando un lenguaje común que nos permita hablar sobre los roles y trabajos de ciberseguridad. Ejemplo: Metodología NICE.[3]

- Análisis de la escasez de profesionales en ciberseguridad. Cuantificación de la brecha entre la oferta y la demanda de profesionales del sector. Número de puestos no cubiertos y tendencia de futuro (en este análisis se contemplarán, no sólo las vacantes de perfiles técnicos, sino también de otros perfiles que tengan relación con la ciberseguridad – legales, educativos, médicos, etc.-)).
- Problemática actual desde diferentes perspectivas: Cliente, Proveedor, profesional e Industria.
- Reciclaje profesional hacia la ciberseguridad. Colectivos con potencial. Experiencias en otros países y sectores.
- Incorporación de la mujer en el sector de la ciberseguridad. Porcentaje de mujeres en activo dentro del sector. Análisis de las causas de la escasa vocación de la mujer en carreras técnicas y en perfiles relacionados con la ciberseguridad (técnicos o no). Análisis de la brecha de género dentro del sector.
- Incorporación de otros colectivos sensibles en el sector de la ciberseguridad (personas con discapacidad, en riesgos de exclusión, etc.). Porcentajes en activo dentro del sector. Análisis de las causas de la escasa vocación de estos colectivos en carreras técnicas y en perfiles relacionados con la ciberseguridad (técnicos o no).
- Análisis de los factores que influyen en la fuga de talento: Perspectiva empleado vs empresa.
  - Condiciones laborales del sector en España: Jóvenes recién titulados vs talento senior.
  - Salarios en el sector de ciberseguridad en España.

[3] NICE Cybersecurity Framework: https://www.nist.gov/itl/applied-cybersecurity/nice/nice-cybersecurity-workforce-framework-resource-center

- Carreras profesionales e incentivos.

- Análisis cuantitativo: volumen de egresados, situación actual, estimaciones y proyección a futuro.

6. Análisis de la Demanda de Talento en ciberseguridad

- Introducción
- Análisis cualitativo (en este análisis se deben contemplar tanto los perfiles más técnicos en CS como aquellos que no son técnicos pero deben tener conocimientos en esta materia – legales, médicos, educadores, psicólogos, etc.-).
    - Quién busca profesionales en ciberseguridad en España.
    - Catálogo de Perfiles de ciberseguridad a nivel nacional: descripción de los perfiles profesionales de ciberseguridad demandados por los reclutadores en España:
        - Ocupaciones, conocimientos, habilidades, competencias y cualificaciones.
    - Como están abordando las empresas la escasez de talento. Tendencias y nuevas oportunidades de negocio.
    - Retención del talento: el reto de las empresas, desarrollo de programas de incentivos y planes de carrera.
    - Principales skills demandas por las empresas: Técnicas, analíticas y soft skills. Identificación de aquellas con mayor escasez o más difíciles de cubrir.
        - Comparativa entre lo que ofrece el mercado de talento (oferta) y lo que buscan las empresas (demanda).
- Análisis cuantitativo
    - Volumen de profesionales en ciberseguridad que trabajan en España. Situación actual y proyección a futuro.
    - Volumen de profesionales en ciberseguridad demandados en España. Situación actual y proyección a futuro.
    - Análisis sectorial.
    - Análisis geográfico.

7. Casos de éxito: Iniciativas de Promoción del Talento en ciberseguridad a nivel internacional

8. Conclusiones

9. Indicadores

10. Recomendaciones

- Recomendaciones al Sector Público.
- Recomendaciones a los Reclutadores de Talento y/o empresas.
- Recomendaciones a las Instituciones formativas.
- Recomendaciones a personas con potencial para dedicarse profesionalmente a la ciberseguridad.

11. Anexos

- Identificación y análisis de las mejores prácticas en gestión del talento en las ocho economías globales con mayor madurez en el campo de la ciberseguridad (por ej. EEUU, Israel, Rusia, Canadá, Reino Unido, Malasia, China y Francia).

El contratista deberá aportar los siguientes entregables:

- Entregable 1: Informe de cierre de trabajo de campo.
- Entregable 2: Archivos en bruto (grabaciones / transcripciones de entrevistas, archivo Excel con los datos de las encuestas).
- Entregable 3: Estudio en formato editable (.doc) conforme a los requisitos formales y estéticos aportados por INCIBE
- Entregable 4: Archivo Excel con los gráficos, tablas e indicadores conforme a los requisitos formales y estéticos aportados por INCIBE
- Entregable 5: Estudio maquetado para publicación web conforme a los requisitos formales y estéticos definidos por INCIBE. Incluirá elementos gráficos y audiovisuales tales como imágenes, infografías y vídeos.
- Entregable 6: Resumen ejecutivo con los principales resultados que resulte atractivo para su divulgación.

2.2.2. Elaboración del Plan de acción

En base a las conclusiones extraídas de los análisis anteriores, el contratista propondrá una hoja de ruta con las acciones derivadas de la fase de diagnóstico anterior en la que se lleva a cabo una caracterización del mercado de talento.

Todas las actuaciones deberán estar orientadas a facilitar la consecución de los siguientes objetivos:

- Definir los escenarios de intervención adaptados a los distintos perfiles identificados durante el análisis.
- Facilitar la conexión en materia de identificación y captación de talento en ciberseguridad entre el sector educativo y los reclutadores.
- Elevar el número de expertos en ciberseguridad (tanto a nivel técnico como a otros niveles).
- Enfocar la oferta formativa en ciberseguridad de acuerdo a las necesidades de los reclutadores.
- Estimular programas de capacitación en ciberseguridad.
- Definir acciones y contenidos de formación/capacitación para cada uno de los itinerarios y perfiles de formación identificados en el estudio de caracterización. Ejemplo: Metodología NICE
    - Estos itinerarios podrán contar con contenidos de INCIBE y de terceros y se dividirán por niveles de conocimiento.
- Estimular programas de captación y promoción de talento en diferentes sectores de población (tanto aquellos que están en momento de elegir su primera opción laboral como aquellos que ya están en el mercado laboral pero desean reorientar sus

carreras, como aquellos que todavía no se han planteado esta opción – por edad o por otros factores -, etc.).
- Priorizar las líneas de acción y sus actividades.
- Aumentar la notoriedad de marca INCIBE y el alcance de sus acciones relativas a los públicos objetivos identificados en la fase de diagnóstico.
- Medir y evaluar la implementación de acciones y sus resultados.

La etapa de diagnóstico anterior permitirá al contratista identificar los puntos críticos y categorizarlos de la siguiente manera: Oportunidades, Amenazas, Fortalezas o Debilidades. Utilizando por tanto el análisis DAFO (Debilidades, Amenazas, Fortalezas y Oportunidades), mediante una matriz.

En este plan se ordenarán los objetivos por niveles de preferencia y/o prioridad con el objetivo de identificar la importancia de cada acción en un horizonte temporal de cara a cumplir los objetivos.

Se llevará a cabo una identificación de líneas estratégicas prioritarias o básicas sobre las que centrar esfuerzos.

Este plan de acción contendrá, al menos, los siguientes apartados:

- Introducción
- Misión y Visión
- Análisis de la situación Actual (Análisis PEST)
- Análisis DAFO, basado en la fase de diagnóstico.
- Prioridades estratégicas.
- Plan de acción y cronograma.
- Seguimiento de indicadores y evaluación.

Las **acciones** deberán ser **escalables**, de **alto impacto** y que **permitan llegar a un gran número de personas de manera eficiente**, empleando para ello los canales necesarios y adaptados a los diferentes públicos objetivo identificados.

El contratista deberá aportar los siguientes entregables:

- Entregable 7: Plan de acción detallado, conforme a los requisitos formales y estéticos aportados por INCIBE
- Entregable 8: Resumen ejecutivo con el resumen de acciones presentado de manera ejecutiva, gráfica y visual.

3. METODOLOGÍA

La empresa licitadora deberá proponer, de manera clara, la metodología a seguir durante el desarrollo del proyecto, cumpliendo los objetivos y características fijados en el presente pliego.

En la metodología la empresa licitadora deberá detallar la forma en la que abordará los trabajos a realizar según lo descrito en el apartado [2.2 DESCRIPCIÓN DE LOS TRABAJOS]. El nivel de detalle aportado será el necesario para expresar que el método propuesto permitirá alcanzar los objetivos fijados.

La metodología empleada es la parte más importante del servicio, debe ser **sólida, contrastada y detallada**, de manera que pueda permitir a INCIBE realizar distintas oleadas en distintos periodos de tiempo con el objetivo de poder actualizar los datos del estudio y ver la evolución en el futuro.

Para ello, es de vital importancia en las distintas técnicas de investigación tener en cuenta a todos los agentes de la **cadena de valor en ciberseguridad**, de manera que sea posible tener un diagnóstico preciso de lo que está pasando en el sector obteniendo el conocimiento de los principales actores del ecosistema.

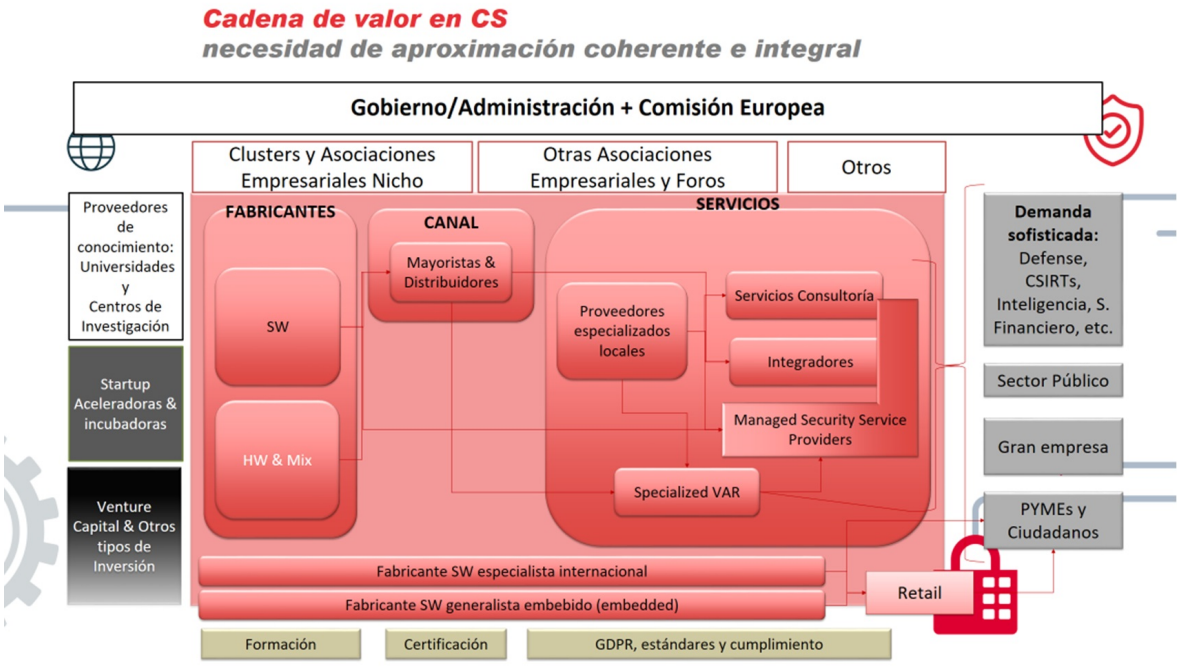

Figura 1: Cadena de valor del sector ciberseguridad

El contratista deberá tener en cuenta a todos estos agentes en la metodología del estudio, así como, los Organismos públicos nacionales e internacionales, Asociaciones sectoriales de referencia y Organismos de estudios sectoriales y tendencias que se detallan en el aparatado siguiente.

En la selección de la metodología, la empresa proveedora incluirá, al menos, las siguientes técnicas de investigación y análisis de mercado.

Esta metodología será elaborada por el adjudicatario de manera detallada y minuciosa y entregada a INCIBE para su validación y solicitud de posibles ajustes.

3.1. Técnicas cuantitativas

Con el fin de asegurar la calidad de los trabajaos realizados, el contratista deberá emplear una metodología sólida que contenga las siguientes técnicas de análisis cuantitativas:

- **Análisis documental o desk research.** La empresa contratista deberá realizar un análisis profundo de la documentación que le pueda proporcionar INCIBE como input, así como una recopilación y estudio de fuentes secundarias nacionales e internacionales que identifique el proveedor y que puedan contribuir a enriquecer el diagnóstico. Fuentes relevantes a tener en cuenta (a continuación se presenta una primera aproximación que el adjudicatario deberá revisar y completar de manera justificada):
  - **Organismos públicos nacionales e internacionales**: aquellos que tienen competencias en el ámbito de la ciberseguridad, bien por el desarrollo de actuaciones relacionadas con CERTs o bien por la promoción de entornos de confianza digital para ciudadanos y empresas:
    - United Nations specialized agency for ICTs (ITU).
    - Organization for Security and Co-operation in Europe (OSCE).
    - World Summit on the Information Society (WSIS).
    - International Telecommunication Union (ITU).
    - European Cybercrime Centre.
    - EUROPOL.
    - European Union Agency for Cybersecurity (ENISA).
    - Homeland Secturity USA
    - Office of Cyber Security and Information Assurance UK
    - Instituto Nacional de Ciberseguridad (INCIBE)
    - Red.es
    - Empresa Nacional de Innovación (ENISA)
    - Agencia Española de Protección de Datos (AEPD)
    - CERT EU
    - US-CERT
    - CERTGOVIL (ISRAEL)
    - Centro Nacional de Protección de las Infraestructuras Críticas (CNPIC).
    - Centre de Seguretat de la Informació de Catalunya (CESICAT)
    - AndalucíaCERT
    - CSIRT-CV Centro de Seguridad TIC de la Comunitat Valenciana
    - Red Iris
    - esCERT-UPC
    - European Cyber Security Organisation: ECSO
    - SEPE: Servicio Público de Empleo Estatal.
  - **Asociaciones sectoriales de referencia**: Se contará con un conjunto de organismos y asociaciones de referencia, tanto en relación directa con el

sector de la CS como en otros ámbitos como la Sociedad del Conocimiento, TIC, Seguridad de la información, etc.

- Information security fórum (ISF).
- Information systems audit and control association (ISACA)
- (ISC)²: IT certification and security experts
- Cloud Security Alliance, Internet Governance Forum (IGF)
- Autelsi: Asociación Española de Usuarios de Telecomunicaciones y de la Sociedad de la Información.
- ISMS Forum Spain
- AMETIC
- CONETIC
- Agrupación empresarial innovadora en ciberseguridad y tecnologías avanzadas (AEI Ciberseguridad).
- Red de Excelencia Nacional de Investigación en Ciberseguridad (RENIC).

- **Organismos de estudios sectoriales y tendencias**: En esta categoría, se engloban todos aquellos organismos y entidades privados, de prestigio reconocido, dedicadas al estudio, a las predicciones de futuro y al adelanto de tendencias globales, en el ámbito general como en el ámbito tecnológico.
  - OCDE
  - World Economic Forum
  - Forrester
  - Gartner
  - Kennedy
  - Mckinsey quarterly
  - MIT
  - ONTSI
  - etc.

- **Realización de encuestas:** El contratista deberá realizar, al menos, 400 encuestas a diferentes agentes del mercado de talento de ciberseguridad en España. Teniendo en cuenta la cadena de valor descrita en el apartado anterior. Es muy importante contar de manera representativa con la visión de todos los actores del ecosistema (a continuación se presenta una primera aproximación que el adjudicatario deberá revisar y completar de manera justificada y aportando detalle en los encuestados finales).
  - **Oferta**: Demandantes de empleo, estudiantes y trabajadores en activo (tanto del sector como de otros posibles sectores).
  - **Demanda**: empresas privadas y públicas (Perfiles de alto nivel jerárquico, responsables de RRHH, cargos medios etc.), empresas de recruiting, startups, etc. Tanto del sector de la ciberseguridad como de otros sectores que necesiten perfiles con conocimientos o bien en ciberseguridad o bien mixtos (medicia-ciberseguridad, legal-ciberseguridad, etc.).
  - **Otros**: Universidades y centros de formación, asociaciones empresariales, Gobierno/administración, Comisión Europea, etc.

El diseño muestral y los cuestionarios serán aprobados por INCIBE.

3.2. Técnicas cualitativas

Con el fin de asegurar la calidad de los trabajaos realizados, el contratista deberá emplear una metodología sólida que contenga, al menos, las siguientes técnicas de análisis cualitativas (para cada uno de los puntos, el adjudicatario deberá realizar un desglose detallado de las fuentes que se incluirán en cada uno de ellos y que deberá ser revisada y aprobada por INCIBE).

- **Entrevistas en profundidad a un mínimo de 20 actores relevantes en el sector.** El contratista deberá contar con la visión de actores relevantes en el mercado del talento en ciberseguridad a través de la realización de entrevistas en profundidad a **distintos actores de la cadena de valor de ciberseguridad**, personas procedentes de, al menos, el sector público, privado y académico, además de a jóvenes talentos con potencial para acceder profesionalmente al sector de la ciberseguridad.

  La relación de actores a entrevistar y, en su caso, el guion para las entrevistas semi-estructuradas serán aprobados por INCIBE que verificará los aspectos indicados anteriormente así como la heterogeneidad de perfiles, descartados los actores inoportunos a efectos del proyecto o no debidamente justificados, y haciendo especial foco en la representatividad de la cadena de valor en los encuestados.

- **Focus group o grupos de trabajo con actores relevantes del sector,** orientados a generar una discusión libre y guiada sobre las necesidades planteadas y el estado actual del mercado de talento de ciberseguridad en España. Se celebrarán, **al menos, dos sesione**s con el objetivo de profundizar y enriquecer el estudio y las conclusiones obtenidas. Se garantizará un número total de actores adecuado y la heterogeneidad de perfiles. La propuesta debidamente justificada será aprobada por INCIBE.

- **Grupos de discusión sobre temas específicos**: Como complemento a la técnica anterior y con el objetivo de amplificar distintos temas específicos en los que ya conocemos o sobre los que ya hemos extraído conclusiones basadas en los datos del análisis cuantitativo y que pueda resultar interesante para ahondar más en las conclusiones del estudio. Ejemplo: Presencia de la mujer en el sector, retención del talento en España, etc. Se garantizará un número total de actores adecuado y la heterogeneidad de perfiles. La propuesta debidamente justificada será aprobada por INCIBE.

- **Panel de expertos**: Enfocados en ciberseguridad, innovación y emprendimiento, riesgos TI, tendencias de mercado, internacionalización, talento, formación en ciberseguridad, etc. Este equipo, que contará con un **mínimo de 6 expertos**, tendrá un rol de apoyo y soporte al equipo de proyecto permanente, formado por un panel de expertos con amplios conocimientos en todos los ámbitos, cubriendo todas las necesidades que se puedan plantear a lo largo del mismo.

- **Revisión del entregable final por, al menos, tres expertos.** Los expertos pueden ser profesionales externos a la empresa contratista y su dedicación puede no ser exclusiva al proyecto. La relación de los tres expertos será aprobada por INCIBE.

El contratista en ejecución del contrato presentará su propuesta justificada de expertos con detalle de nombre y apellidos, puesto y empresa o institución para la que prestan sus servicios. Se verificará que los expertos son relevantes para los objetivos del proyecto y/o que su participación está suficientemente justificada.

4. EQUIPO DE TRABAJO

4.1. COMPOSICIÓN

El equipo estará formado por el número de profesionales que la empresa contratista considere necesario para satisfacer con garantías todos y cada uno de los trabajos antes descritos.

Los profesionales que formen el equipo de trabajo deberán contar con experiencia contrastada en el desarrollo de los trabajos requeridos y con un carácter multidisciplinar, de modo que éstos dispongan de amplios conocimientos y habilidades en relación con distintos ámbitos o áreas requeridos por las distintas fases de la propuesta.

El equipo de trabajo contará con un apoyo continuado de expertos en todos los ámbitos objeto de los trabajos, de forma que el equipo de trabajo pueda acudir siempre a un panel de expertos con el que contrastar o diseñar los trabajos a realizar.

El objetivo es que se pueda garantizar la consecución de todos los objetivos del proyecto, como un apoyo experto puntual y continuado durante la ejecución de los trabajos, con objeto de responder a distintas demandas y necesidades estratégicas u operativas que puedan surgir durante el proyecto.

Se requerirá en el equipo de trabajo:

- Conocimiento experto en estudios de mercado, con un mínimo de 24 meses de experiencia en este ámbito.
- Conocimiento experto en el entorno TIC y/o ciberseguridad, al menos en 1 de los miembros del equipo.

4.2. REQUISITOS DEL JEFE DE PROYECTO

Como parte del equipo propuesto por el contratista, deberá existir un perfil que ejerza tareas de coordinación, interlocución y jefatura del proyecto.

El jefe del proyecto será la persona encargada de gestionar el contrato y de ser el principal punto de contacto con INCIBE (a través de su Dirección técnica). Para ello realizará las funciones que se definen a continuación:

- Dirigir a los medios personales que presten los servicios, impartiendo al efecto las órdenes e instrucciones necesarias para la ejecución de la misma en tiempo y forma, cumpliendo todos y cada uno de los compromisos adquiridos, velando por el adecuado cumplimiento de los trabajos en relación con el equipo de trabajo del contratista.
- Realizar las funciones de contacto directo e interlocutor con la Dirección técnica de INCIBE.
- Notificar a la Dirección técnica de INCIBE las incidencias del proyecto que sean transcendentes para el mismo y el grado de evolución de los servicios.
- Elaborar los informes de seguimiento, reportes, estadísticas, presentaciones o cualquier otra documentación que pueda resultar de interés para INCIBE.

- Redacción y distribución de las actas de reunión en las que participe el contratista.
- Notificar a la Dirección técnica de INCIBE el cumplimiento de los hitos de facturación a medida que se vayan cumpliendo y elaborar los informes de facturación correspondientes para su validación y aprobación por parte de la Dirección técnica de INCIBE previo a la emisión de las facturas correspondientes.

En el caso del Jefe de Proyecto se requiere:

- Un mínimo de 24 meses de experiencia como jefe de proyectos.
- Conocimiento demostrable en la coordinación y elaboración de estudios en el entorno de ciberseguridad y/o sector TIC.

5. PLANIFICACIÓN

Los trabajos se realizarán a lo largo de 6 meses.

La planificación definitiva del proyecto se determinará a partir de la reunión de lanzamiento.

5.1. REUNIÓN DE LANZAMIENTO

Este hito tendrá lugar tan pronto como sea posible dentro de los 7 días siguientes a la formalización del contrato. En esta reunión se establecerán todos los acuerdos para conseguir el desarrollo exitoso del proyecto. Asimismo, se establecerán los canales de comunicación entre los equipos de trabajo del contratista e INCIBE, y el contratista presentará la especificación detallada de su metodología de proyecto.

La **metodología del proyecto será validada y aprobada por INCIBE**, reservándose el derecho de solicitar cambios que se adapten a los objetivos planteados, siempre velando por el cumplimiento de estos y la generación de un estudio con una metodología sólida que tenga en cuenta a todos los agentes de la cadena de valor del sector ciberseguridad y que permita realizar distintas oleadas en el futuro basadas en las mismas técnicas.

INCIBE proporcionará, en dicha reunión, toda la información que deba ser necesaria conocer por el contratista para la organización y coordinación de las actividades.

El contratista entregará una especificación detallada del proyecto en el que se contemplarán los principales aspectos a desarrollar:

- Presentación del equipo del proyecto.
- Presentación de los trabajos a realizar.
- Presentación de la metodología a usar por el contratista en cuanto a organización de recursos y seguimiento de los trabajos.
- Planificación definitiva del proyecto, definición de hitos y cronograma planificado para los mismos. Esta planificación podrá ser revisada durante la ejecución del contrato, junto con el Director/a de Proyecto de INCIBE, para adaptarla a las necesidades del servicio con la finalidad de que el servicio sea prestado de manera adecuada, eficaz y eficiente.
- Cualquier otra tarea que redunde en el óptimo desarrollo del proyecto.

5.2. REUNIONES DE SEGUIMIENTO

A raíz de la reunión de lanzamiento y con periodicidad mensual el contratista, a través de su Jefe de Proyecto, se reunirá con la dirección técnica del proyecto de INCIBE con la finalidad de realizar un seguimiento periódico de las tareas asociadas al contrato. Para dichas reuniones el contratista elaborará todos los meses un informe técnico de seguimiento con los siguientes aspectos:

- Grado de cumplimiento de los objetivos e hitos establecidos para cada una de las actividades a realizar.
- Lista de riesgos detectados que puedan comprometer el cumplimiento de los objetivos e hitos marcados, así como una propuesta de acciones para su mitigación o eliminación.
- Trabajos realizados y resultados obtenidos.

- Trabajos planificados para el siguiente periodo y objetivos que se pretenden cumplir para cada uno de los servicios.
- Identificación de mejoras que se puedan aplicar para el cumplimiento de los objetivos del servicio.

En general, las reuniones de seguimiento se llevarán a cabo de forma telemática aunque, excepcionalmente, será posible tener reuniones presenciales, que se celebrarán en las oficinas de INCIBE de León. En caso de que una de las partes requiera una reunión presencial, lo notificará con suficiente antelación a la otra parte y se fijará una fecha de reunión que satisfaga a ambos.

Debido a la naturaleza del proyecto, además de las reuniones de seguimiento, deberá existir comunicación continua durante la ejecución del contrato para intercambiar información en tiempo real y realizar seguimiento, para ser capaces de detectar posibles riesgos con la mayor antelación posible.

5.3. CIERRE DEL PROYECTO Y MEMORIA FINAL

En este hito, al alcanzar la finalización del proyecto, el contratista deberá presentar una Memoria Final, como informe justificativo del alcance efectivo de los trabajos realizados, con detalle de entregables, recursos consumidos, objetivos e hitos conseguidos.

Asimismo se deberá asegurar que todos los entregables generados a lo largo del proyecto se encuentren correctamente ubicados, documentados y en sus versiones finales/actuales.

La reunión de cierre no se llevará a cabo hasta que INCIBE no haya recibido y validado previamente toda la documentación asociada al proyecto.

6. DIRECCIÓN Y SEGUIMIENTO DE LOS TRABAJOS

Corresponde a la Dirección Técnica del proyecto, la completa supervisión y dirección de los trabajos, proponer las modificaciones convenientes o, en su caso, proponer la suspensión de los mismos si existiese causa suficientemente motivada.

Para la supervisión de la marcha de los trabajos, INCIBE indicará al comienzo del proyecto la persona designada como Director/a Técnico/a del proyecto. Sus funciones en relación con el presente Pliego serán:

1. Velar por el adecuado cumplimiento de los servicios contratados.
2. Ser el interlocutor con la empresa contratista para todas las tareas de coordinación del proyecto.
3. Emitir las certificaciones parciales de recepción de los trabajos.
4. Fijar reuniones periódicas entre la Sociedad y el contratista con el fin de determinar, analizar y valorar las incidencias que, en su caso, se produzcan durante la ejecución del contrato.

Independientemente de las reuniones establecidas en este pliego, el Director Técnico de proyecto podrá convocar cuantas reuniones de seguimiento del proyecto considere oportunas para asegurar el cumplimiento del calendario del proyecto así como la correcta consecución de los objetivos propuestos. El contratista será responsable de la redacción y distribución de las correspondientes actas de reunión.

Con el fin de garantizar que se satisfacen las necesidades y prioridades establecidas por el Director Técnico del proyecto, este marcará las directrices de los trabajos a realizar, siendo estas directrices de obligado cumplimiento por parte del contratista.

Durante el desarrollo del proyecto se podrán solicitar, como parte de las tareas de seguimiento y control, entregas intermedias que permitan tanto la verificación del trabajo realizado, como evitar y reducir riesgos a lo largo del proyecto.

Las rectificaciones derivadas de decisiones sobrevenidas que no tengan como origen errores u omisiones del contratista se computarán y abonarán como horas de trabajo dentro del proyecto.

7. FORMA DE EJECUCIÓN

7.1. LUGAR DE REALIZACIÓN DE LOS TRABAJOS

El centro habitual de trabajo serán las oficinas e instalaciones de la empresa contratista, sin perjuicio de las reuniones presenciales que fueran necesarias para la correcta ejecución de los trabajos.

7.2. CONTROL DE CALIDAD

Sin perjuicio de las obligaciones asumidas en su oferta, el contratista, a través del supervisor designado a tal efecto, deberá seguir los procedimientos de aseguramiento de la calidad existentes en la ejecución del contrato.

El contratista reconoce el derecho de la Sociedad para examinar por medio de auditores, externos o propios, el fiel cumplimiento de los trabajos por él realizados.

INCIBE tendrá derecho a llevar a cabo auditorías de las actividades de los contratistas para asegurarse de que la ejecución de los trabajos se lleva de acuerdo con lo establecido en el presente Pliego. Todo el material e información requerida para dichas inspecciones y auditorías por los representantes de la Sociedad estará disponible sin restricciones. La Sociedad notificará al contratista con dos semanas de antelación la auditoría y con un día de antelación la inspección a realizar, y el contratista tendrá la obligación de:

- Facilitar el acceso al material solicitado por el grupo auditor.
- Designar personas responsables que acompañen a los auditores.
- Facilitar un entorno de trabajo adecuado en el mismo lugar en que tiene lugar la auditoría.
- Cooperar con el auditor.
- Participar en las reuniones que convoque el auditor.
- Analizar los datos encontrados para que el informe sea real.
- Emprender rápidamente acciones correctoras y/o preventivas.
- Emitir una respuesta oficial para cada uno de los defectos que haya detectado el grupo de auditores.

La valoración final de la calidad de los servicios prestados corresponde a la Sociedad y su equipo asesor, siendo potestad suya solicitar la subsanación de los posibles errores detectados.

7.2.1. Flujo de revisión de los entregables

Se define el proceso de control de calidad para la documentación que se genere como un flujo de revisión que permita a INCIBE evaluar la calidad de los contenidos.

Se establece el proceso de revisión ordinario compuesto por dos iteraciones, es decir, se enviará la versión inicial a INCIBE para la primera revisión, el equipo de proyecto por parte de INCIBE realizará la evaluación de los contenidos y solicitará posibles cambios, sugerencias o mejoras al contratista, este realizará los ajustes y modificaciones necesarias según las indicaciones de INCIBE y elaborará la segunda versión del documento, que será

revisada por INCIBE para confirmar la adecuación de las modificaciones y dar por cerrado el entregable.

A continuación se muestra el diagrama del flujo óptimo de revisión de entregables.

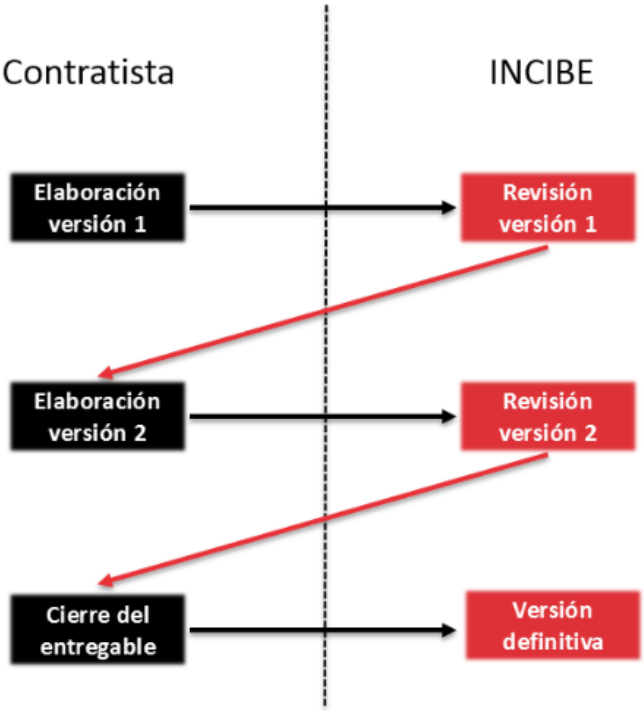

Figura 1. Flujo de revisión de entregables

7.3. OBLIGACIONES DE INFORMACIÓN Y DOCUMENTACIÓN

Durante la ejecución de los trabajos objeto del contrato, el contratista se compromete, en todo momento, a facilitar a las personas designadas por el Director/a de Proyecto de INCIBE, la información y documentación que estas soliciten para disponer de un pleno conocimiento de las circunstancias en que se desarrollan los trabajos, así como de los eventuales problemas que puedan plantearse y de las tecnologías, métodos y herramientas necesarias para resolverlos.

Asimismo el contratista estará obligado a asistir y colaborar, a través del personal que designe a este propósito, en las reuniones de seguimiento del proyecto definidas por el Director/a de Proyecto de INCIBE, quien se compromete a citar con la debida antelación al personal del contratista.

Como parte de las tareas objeto del contrato, el contratista se compromete a generar la documentación de los trabajos realizados, de acuerdo con los criterios que establezca en cada caso el Director/a de Proyecto de INCIBE. Toda la documentación generada por el contratista durante la ejecución del contrato será propiedad exclusiva de INCIBE sin que el contratista pueda conservarla, ni obtener copia de la misma o facilitarla a terceros sin la expresa autorización por escrito de INCIBE, que la concederá, en su caso y con expresión del fin, previa petición formal del contratista.

En este sentido, el contratista deberá informar al Director/a de Proyecto de INCIBE sobre distintos aspectos relacionados con el funcionamiento y la calidad de los servicios prestados. Entre ellos será necesario presentar un informe, en el formato y con la periodicidad que defina el Director/a de Proyecto de INCIBE, de cumplimiento de los servicios y que contendrá entre otros los siguientes puntos, si proceden:

- Trabajos realizados y resultados obtenidos en el período vigente.
- Trabajos planificados para el siguiente periodo.
- Identificación de mejoras que se puedan aplicar para el cumplimiento de los objetivos de los proyectos en los que esté involucrado.

El contratista proporcionará, sin coste adicional para la Sociedad, una copia en soporte digital (CD-ROM, DVD, llave USB, disco duro) con toda la documentación generada durante la presentación de los servicios objeto del contrato, así como los ficheros maestros de posibles imágenes, diagramas, planos u otros elementos generados.

7.4. HITOS DE FACTURACIÓN

Se definen los siguientes hitos de facturación:

Hito	Entregable	% de facturación (sobre precio total de contratación)	Importe máximo de facturación (sobre 120.000€)
1	Entregable 1: Informe final de trabajo campo	10%	**12.000€**
2	Entregable 2: Archivos en bruto (grabaciones / transcripciones de entrevistas, archivo Excel con los datos de las encuestas)	5%	**6.000€**
3	Entregables 3 y 4: ■ Estudio en formato editable conforme a los requisitos formales y estéticos aportado por INCIBE ■ Archivo Excel con los gráficos, tablas e indicadores	45%	**54.000€**
4	Entregable 5: Estudio maquetado para publicación web que incluya elementos gráficos y audiovisuales tales como imágenes, infografías y vídeos Entregable 6: Resumen ejecutivo con los principales resultados que resulte atractivo para su divulgación.	15%	**18.000€**
5	Entregables 7 y 8: ■ Plan de acción detallado, conforme a los requisitos formales y estéticos aportados por INCIBE	30%	**30.000€**

Hito	Entregable	% de facturación (sobre precio total de contratación)	Importe máximo de facturación (sobre 120.000€)
	■ Resumen ejecutivo con el resumen de acciones presentado de manera ejecutiva, gráfica y visual.		
Total		**100%**	**120.000€**

Tabla 1: Hitos de facturación

La facturación de los trabajos realizados se efectuará sobre la base de una adecuada prestación del servicio por parte del contratista según la distribución de los hitos citados anteriormente, cuyo detalle se deberá reflejar en el reporte final que se entregará a INCIBE.

En las reuniones periódicas hasta la finalización del contrato, se evaluarán todas aquellas incidencias habidas que se hubieran originado en el cumplimiento de los objetivos planificados. Cuando a juicio del Director Técnico, tales incidencias fueran imputables al contratista, por falta de responsabilidad, incompetencia, desidia u otras causas de índole similar, podría la facturación resultante quedar minorada por el importe que corresponda de acuerdo a las penalizaciones establecidas en el presente Pliego.

8. PRESENTACIÓN DE LAS OFERTAS TÉCNICAS

Con independencia de que el licitador pueda adjuntar a su oferta cuanta información complementaria considere de interés, ésta deberá constar de los apartados descritos en el punto 15.2.2. del Pliego de Características Generales y deberá respetar el mismo orden (así como contemplar todos los requisitos descritos en el presente pliego).

9. CRITERIOS DE VALORACIÓN

Los criterios de valoración son los recogidos en el anexo VI del Pliego de Características Generales.

León, 19 de mayo de 2020
DIRECTORA GENERAL
INSTITUTO NACIONAL DE CIBERSEGURIDAD DE ESPAÑA, S.A.

Resuelve aprobar el presente pliego