Financiado por la Unión Europea NextGenerationEU
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
Gobierno de Navarra Nafarroako Gobernua
AGENDA 2030

PLIEGO DE CLÁUSULAS TÉCNICAS

QUE HAN DE REGIR LA CONTRATACIÓN DE UN "SERVICIO DE EASM Y PROTECCIÓN DE IDENTIDAD DIGITAL PARA EMPRESAS EN NAVARRA"

MAYO DE 2025

Navarra de Servicios y Tecnologías, S.A.
| C/ Orcoyen, s/n. 31011 Pamplona - Navarra |
| info@nasertic.es | www.nasertic.es |
| Tel: 848 420 500 | Fax: 848 426 751 |

Índice

1 CONTEXTO

1.1 Introducción

Las amenazas a la seguridad de la información han existido siempre, pero ha sido en los últimos años cuando los riesgos asociados a las mismas han sufrido un crecimiento exponencial. La adopción de tecnologías como elementos fundamentales en los procesos de negocio influye de forma relevante en el impacto de los ciberataques. Igualmente, junto con el desarrollo de las nuevas tecnologías ha aumentado la complejidad de los sistemas empleados por los atacantes para poner en jaque la información y ha aumentado la probabilidad de que se produzcan estos ataques. Esto provoca que el riesgo al que se ven expuestas las organizaciones sea especialmente alto, dinámico y difícil de gestionar, tal y como nos demuestra conocer a diario nuevas empresas y entidades que han visto su funcionamiento paralizado por ciberataques.

Es necesario tanto innovar en ciberseguridad como acercar la ciberseguridad a un ámbito cada vez más sensible y expuesto: el tejido empresarial. Por un lado, por la rápida evolución de las tecnologías y la necesidad por parte de las organizaciones de adoptarlas para ser cada vez más competitivas y eficientes. Además, es imprescindible mantener el ritmo de innovación en ciberseguridad para poder adoptar nuevas tecnologías sin superar un nivel de riesgo aceptable. Para ello, se deben generar espacios de colaboración regional público-privada, involucrando administración, empresas y academia, para impulsar la innovación, la adopción de soluciones de ciberseguridad y la generación de talento.

1.2 Iniciativas en el ámbito de la ciberseguridad en Navarra

El Gobierno de Navarra no ha sido ajeno a esta realidad, apostando en este ámbito por dos iniciativas de referencia en Navarra:

- **Polo de Innovación Digital de Navarra (Polo IRIS)**: nace con la misión de '*contribuir a la aceleración de la transformación digital de innovación en Navarra, actuando como catalizador y ventanilla única de la digitalización de la región a través de la prestación eficiente de servicios, la gestión eficaz de sus recursos y la generación de espacios de colaboración con los agentes clave público-privados'*. La visión del Polo es la de '*constituirse como el espacio de referencia en materia de digitalización e innovación de Navarra, favoreciendo la colaboración y generación de alianzas entre todos los agentes económicos y sociales de la región e impulsando su transformación a través de servicios avanzados'*. Se puede caracterizar a través de los siguientes pilares fundamentales:
  1. Como respuesta a los retos de transformación digital de la región.
  2. Como ventanilla única de transformación digital e innovación en Navarra.
  3. Como impulsor de la especialización tecnológica en Navarra.
  4. Como catalizador de servicios digitales al tejido empresarial navarro.
  5. Como promotor de una sociedad digital en Navarra.

  Es en el punto tercero, donde el Polo focaliza esfuerzos en el **impulso de áreas de especialización tecnológica** que permitan impulsar la competitividad global de la

Comunidad Foral de navarra y que, de forma específica, contribuyan al desarrollo de los sectores estratégicos fijados en la Estrategia de Especialización Inteligente de Navarra S4.

Una de estas áreas de especialización es la **Ciberseguridad**. Abarca todas aquellas actividades o procesos mediante los que los sistemas de información y comunicación y el contenido de los mismos son protegidos de o defendidos contra daños y contra su uso, modificación o explotación no autorizados.

- **Navarra Cybersecurity Center (NavCC)**: Su principal objetivo es el **impulso al desarrollo de iniciativas en torno a la ciberseguridad** que deriven en un aumento de la ciber resiliencia en todos los ámbitos de la Comunidad Foral de Navarra, incluyendo el tejido empresarial y con especial foco en pymes y autónomos y establecerse como ventanilla única en materia de seguridad digital.

  Las iniciativas se dirigen a la dinamización del sector de la ciberseguridad tanto desde el punto de la oferta de los servicios ofrecidos en la Comunidad Foral, como desde el punto de vista de la demanda y utilización de dichos servicios. Por tanto, tiene como objetivo estratégico contribuir a la transformación socioeconómica sostenible de Navarra en un entorno digital e hiperconectado, seguro y ciberresiliente.

Ambas iniciativas están íntimamente relacionadas, siendo el NavCC el principal instrumento para el desarrollo del área de especialización de ciberseguridad del Polo de Innovación Digital de Navarra IRIS.

1.3 Objetivos estratégicos en Ciberseguridad para el tejido empresarial navarro

En este apartado se definen las bases estratégicas del área de especialización de Ciberseguridad del Polo de Innovación Digital de Navarra para potenciar este ámbito.

La transversalidad y globalidad del ciberespacio supone que la ciberseguridad sea un tema clave en todos los sectores de actividad. Precisamente por ello la cooperación y compartición de avances y conocimiento permiten mayores logros en la protección frente a las ciber amenazas. La ciberseguridad tiene un carácter transversal que afecta a todo el tejido empresarial, pero también a Administraciones Públicas y a la sociedad en su conjunto. Por tanto, el área de especialización de Ciberseguridad del Polo de Innovación Digital de Navarra, entendiendo la ciberseguridad como una oportunidad económica, profesional y empresarial, se centra en potenciar iniciativas tractoras con potencial para escalado en distintos sectores industriales y productivos, incluyendo también acciones relacionadas con la sensibilización respecto a los riesgos inherentes al mundo conectado.

Con todo lo anterior, podemos definir los siguientes **objetivos estratégicos en materia de ciberseguridad, canalizados a través del Navarra Cybersecurity Center (área de especialización del Polo IRIS)**:

1. Contribuir, desde el impulso público, a que el proceso de digitalización y la hiperconectividad en un entorno ciberseguro produzcan una transformación socioeconómica sostenible en términos de **productividad y empleo**.

2. Impulsar proyectos regionales de ciberseguridad, asegurando su eficiencia y maximizando su impacto a través de la **coordinación, la colaboración y la complementariedad** de la colaboración público-privada.

3. Impulsar el **equilibrio territorial** en materia de ciberseguridad, de modo que ningún ámbito se quede rezagado en un objetivo global como el impulso a la cultura de la ciberseguridad para empresas y ciudadanía.

4. Fomentar el crecimiento estratégico de un **sector clave como el TIC**, pero también otros **sectores económicos estratégicos** en las economías regionales a través de la transformación y especialización digital.

5. Establecer las bases para un **entorno de colaboración estable y sostenible** a medio y largo plazo que velen por el avance coordinado en aspectos de ciberseguridad.

Para el desarrollo de los objetivos estratégicos anteriores, se han definido las siguientes **líneas de actuación**:

1. Creación de un centro de ciberseguridad regional.
2. Fomento del ecosistema empresarial en el sector de la ciberseguridad.
3. Creación de centros demostradores.
4. Gestión del talento.
5. Acciones de sensibilización.

2 OBJETO OBJETIVOS Y ALCANCE DE LA CONTRATACIÓN

2.1 Objeto

El objeto del presente pliego es definir las cláusulas técnicas particulares que han de regir la contratación de un **"Servicio de EASM & Brand Protection y Protección de Identidad Digital para empresas en Navarra"**, detallando objetivos, alcance, así como la descripción de los requisitos técnicos mínimos obligatorios y condiciones técnicas generales que deberán considerarse para la prestación del servicio.

2.2 Objetivos

El principal objetivo de la contratación de un **"Servicio de EASM & Brand Protection y Protección de Identidad Digital para empresas en Navarra"** es poner a disposición del tejido empresarial navarro, un servicio de evaluación de la superficie externa de ataque, protección de marca y protección de identidad digital que permita medir, de una manera objetiva y estandarizada, el nivel de exposición en Ciberseguridad de las empresas y ciertos directivos de estas, proporcionando al mismo tiempo un itinerario de mejora personalizado con una propuesta de acciones que permitan impulsar las capacidades de ciberresiliencia, elevando de esta manera el nivel de madurez en Ciberseguridad de las empresas navarras.

El servicio se apoyará en herramientas que permitan llevar a cabo el análisis de superficie de ataque y protección de marca, así como la protección de identidad digital, y ofrecerá a las empresas un acompañamiento cercano durante todo el proceso que incluirá reuniones periódicas, la notificación de incidentes, elaboración de informes y planes de mejora personalizados y el seguimiento de los mismos.

Adicionalmente, el servicio permitirá al Navarra Cybersecurity Center obtener una visión global y comparativa sectorial del grado de exposición externa en el tejido empresarial Navarro, identificando los puntos fuertes y débiles y aquellas acciones de mejora que tengan un mayor ratio coste/beneficio. Así mismo, el servicio permitirá cuantificar y medir el nivel de mejora obtenido tras acometer las acciones recomendadas.

2.3 Alcance

El alcance de la presente contratación comprende los siguientes aspectos, cuyos requisitos técnicos se detallan en el punto 3 DESCRIPCIÓN DEL SERVICIO:

- **Herramienta de EASM & Brand Protection** en modalidad **SaaS**:
  - Modelo de suscripción con **licenciamiento** para cubrir **50 empresas**, de acuerdo al siguiente esquema:
    - **20 licencias concurrentes totales** con un periodo de validez hasta el **31 de mayo de 2026**, de las cuales:
      - **15 licencias serán rotatorias**, para poder cubrir un total de **45 empresas** divididas en 3 campañas trimestrales.

- **5 licencias serán permanentes**, para permanecer asignadas durante toda la duración del contrato a 5 empresas.

NOTA 1: Las empresas objetivo del servicio serán **PYMES de tamaño medio**, representativas de su sector y con impacto dentro del tejido empresarial navarro. Las empresas se identificarán por parte del Navarra Cybersecurity Center a lo largo de la ejecución del servicio.

NOTA 2: Al tratarse de una modalidad SaaS, el licenciamiento **incluirá** todas las actividades de **soporte**, **mantenimiento y actualización de la plataforma**.

- **Herramienta de Protección de Identidad Digital** en modalidad **SaaS**:
  - Modelo de suscripción con **licenciamiento** para monitorizar **50 perfiles VIP** de distintas empresas, de acuerdo al siguiente esquema:
    - **20 licencias concurrentes totales** con un periodo de validez hasta el **31 de mayo de 2026**, de las cuales:
      - **15 licencias serán rotatorias**, para poder cubrir un total de **45 perfiles VIP** divididos en 3 campañas trimestrales.
      - **5 licencias serán permanentes**, para permanecer asignadas durante toda la duración del contrato a 5 perfiles VIP.

NOTA 1: Los perfiles VIP objetivo del servicio serán independientes de las empresas participantes en el servicio de EASM & Brand Protection. Estos perfiles se identificarán por parte del Navarra Cybersecurity Center a lo largo de la ejecución del servicio.

NOTA 2: Al tratarse de una modalidad SaaS, el licenciamiento **incluirá** todas las actividades de **soporte, mantenimiento y actualización de la plataforma**.

- Servicios profesionales de **acompañamiento** para las **empresas** que participarán en las campañas:
  - **Reunión inicial** para la recolección de necesidades y definición de objetivos
  - **Provisión y gestión de las plataformas** de EASM & Brand Protection y Protección de Identidad Digital
  - **Seguimiento** continuo, incluyendo workshops periódicos, presenciales y remotos, para la presentación de resultados y validación de las medidas adoptadas
  - **Informes personalizados** y plan de mejora para cada empresa

- Servicios profesionales de **reporting ejecutivo** para el **NavCC** que permitan obtener una **visión global** y **comparativa sectorial anonimizada** de los resultados obtenidos en las diferentes campañas, enfatizando los puntos fuertes y las áreas de mejora a impulsar:
    - **Informe ejecutivo** a cierre de cada una de las campañas
    - **Informe final global** a la finalización del servicio

La propuesta presentada deberá cumplir con los siguientes hitos para la ejecución de las diferentes fases del proyecto:

- **FASE 0: Puesta en Marcha de las plataformas SaaS**
  Incluye la puesta en marcha de las plataformas de EASM & Brand Protection y Protección de Identidad Digital en modalidad SaaS, de cara a poder lanzar la primera campaña.
  Esta fase deberá quedar entregada y aprobada dentro del **mes** siguiente a la fecha de envío del pedido.

- **FASE 1: Primera Campaña**
  En esta fase se ejecutará la primera campaña del servicio para las empresas identificadas por parte del Navarra Cybersecurity Center. Se generarán los informes ejecutivos agregados.
  Esta fase deberá quedar entregada y aprobada dentro de los **cuatro meses** siguientes a la fecha de envío del pedido.

- **FASE 2: Segunda Campaña**
  En esta fase se ejecutará la segunda campaña del servicio para las empresas identificadas por parte del Navarra Cybersecurity Center. Se generarán los informes ejecutivos agregados.
  Esta fase deberá quedar entregada y aprobada dentro de los **siete meses** siguientes a la fecha de envío del pedido.

- **FASE 3: Tercera Campaña**
  En esta fase se ejecutará la tercera y última campaña del servicio para las empresas identificadas por parte del Navarra Cybersecurity Center. Se generarán los informes ejecutivos agregados de esta tercera campaña así como los globales del proyecto completo.
  Esta fase deberá quedar entregada y aprobada antes del **31 de mayo de 2026**.

3 DESCRIPCIÓN DEL SERVICIO

En este apartado se describen las características técnicas que conforman el objeto del contrato y que el adjudicatario deberá prestar, no siendo el listado que aparece a continuación una relación exhaustiva de las características del servicio contratado, sino las actividades generales demandadas por NASERTIC, cubriendo los aspectos de tareas a realizar y los resultados esperados.

Los referidos requisitos deben entenderse como mínimos (a excepción de que se indique lo contrario). El licitador puede ofertar prestaciones superiores a las solicitadas, que se tendrán en cuenta durante la valoración técnica de la oferta, en los términos descritos en los criterios de adjudicación detallados en el pliego de cláusulas administrativas.

El adjudicatario deberá aportar y describir en su oferta las funcionalidades de las herramientas de EASM & Brand Protection y Protección de Identidad Digital, así como los servicios de acompañamiento y reporting indicando los conocimientos, metodologías, herramientas y equipo de trabajo.

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

Para la prestación del servicio, el **adjudicatario** deberá ejecutar las siguientes actividades y cumplir con los siguientes requerimientos:

3.1 Herramienta de EASM & Brand Protection

El servicio incluirá la **provisión de una herramienta de EASM & Brand Protection**, basada en una plataforma SaaS, que permita a las empresas navarras analizar su **nivel de exposición en Ciberseguridad** desde una perspectiva externa y la generación de **planes de mejora personalizados** en base al estado de esta.

Debe proporcionar una visión de superficie de exposición de los activos y la marca de la empresa desde el punto de vista de un atacante, lo que permitirá a las organizaciones identificar activos desconocidos, riesgos y exposición. Desde el conocimiento de estos aspectos, permitirá la mitigación y el control de estos problemas. La herramienta deberá proporcionar información sobre los activos digitales, posibles problemas de seguridad y exposición de marca. A través de esta información se debe poder identificar activos expuestos, tanto conocidos como desconocidos, conocer las vulnerabilidades asociadas y priorizar la remediación de problemas críticos.

El **objetivo** de la herramienta de EASM & Brand Protection es proporcionar un análisis sobre el estado actual de exposición en Ciberseguridad de las PYMES navarras seleccionadas por el Navarra Cybersecurity Center así como un plan de mejora, en base a un análisis externo y no intrusivo del nivel de exposición basado en las principales categorías de exposición de superficie y marca (Red, Gestión de parches, Fuga de datos,

Análisis web, Reputación IP, Salud de DNS, Seguridad Email, Credenciales filtradas, Inteligencia de RRSS, etc.)

Para ello, la herramienta de EASM & Brand Protection debe permitir optar por un **modelo de análisis continuo de la superficie externa de ataque y protección de marca en ciberseguridad**, permitiendo **elaborar un plan de mejora y/o remediación**, basado en las principales debilidades detectadas.

La **herramienta de EASM & Brand Protection** deberá cumplir con los siguientes **requisitos mínimos**:

- Funcionamiento **no intrusivo y automatizado.** La herramienta debe actuar desde una perspectiva externa, siendo innecesario tener que solicitar cualquier actuación dentro de la infraestructura de las empresas monitorizadas.
- **Análisis continuo:** Debe escanear continuamente todos los activos descubiertos para detectar actualizaciones, como nuevos puertos o servicios. Los resultados se actualizarán al realizar un refresco.
- La medición del **nivel de exposición** externa analizando dominios e IPs expuestos a internet por las empresas.
- El análisis de superficie de ataque incluirá distintos ámbitos digitales de **Internet, Deep Web y Dark Web** como mínimo. Estos deben incluir: Repositorios GIT, sitios Paste, Foros, RRSS, etc.
- La herramienta deberá ser capaz de proporcionar una serie de **recomendaciones de mejora personalizadas**, a partir de los resultados del análisis, proponiendo una serie de medidas concretas que permitan reducir el nivel de exposición de la superficie de ataque.
- La herramienta deberá ser capaz de generar **informes** sobre el estado y evolución de la exposición de cada empresa, indicando como ha mejorado/empeorado ésta en el tiempo.
- La herramienta deberá contar con un **manual o guía de ayuda** que facilite el uso, comprensión y explotación de la misma.
- Debe ser una plataforma **SaaS**, públicamente accesible y convenientemente **securizada**. Se deberán proporcionar informes de las últimas certificaciones/auditorías de ciberseguridad de la misma.
- Debe permitir la definición de **diferentes roles de acceso** en función de la tipología de los grupos de usuarios (empresas finales y NavCC).
- La herramienta debe cumplir con las siguientes **funciones**:
    - **Descubrimiento de activos**, teniendo la posibilidad de añadir nuevos activos o eliminarlos de manera manual.
    - **Análisis de fallos de seguridad**. Una vez identificados los activos, debe realizar un análisis para detectar vulnerabilidades y fallos de seguridad conocidos en los activos expuestos:
        - **Resumen** de todos los fallos de seguridad expuestos.
        - **Categorización** de los fallos detectados (Red, Gestión de parches, Análisis web, Reputación IP, Salud de DNS, Seguridad Email…).

- Información sobre los **servicios y puertos expuestos**, indicando cuales de esos servicios son ampliamente explotados de manera habitual.

- Monitorización continua de **robo de credenciales** y alerta sobre posibles **fugas de credenciales** relacionadas con direcciones de correo o usuarios corporativos. Como parte de la recopilación consolidada, las credenciales filtradas se obtendrán de múltiples **fuentes** como:
  - Bases de datos filtradas o comprometidas públicamente
  - Bases de datos compartidas de forma privada
  - Sitios de pasting
  - Infecciones de malware
- **Protección de marca**: Debe detectar amenazas como ataques de phishing basados en la web, typo-squatting, defacement de sitios, aplicaciones fraudulentas, filtraciones de datos e imitaciones de marca en redes sociales. Este módulo se utilizará para detectar actividades de forma temprana y tomar medidas, como la eliminación de sitios web o aplicaciones, para proteger el valor, la confianza, la integridad y la reputación de la marca. En este módulo se debe incluir la identificación de las siguientes amenazas:
  - **Dominios fraudulentos**, aportando una lista de dominios que se están creando con la intención de suplantar los dominios de la organización. La herramienta deberá utilizar las siguientes técnicas para descubrir estos dominios:
    - **Typo-squatting**: Esta técnica consiste en generar varias combinaciones de palabras clave que son similares a los nombres de dominio de la organización. Estas combinaciones se comparan con dominios recién observados, y cualquier dominio coincidente se mantiene bajo monitoreo.
    - **Integración de Fuentes de Phishing**: Este método compara las URL de phishing reportadas y conocidas con la marca de la organización.
    - **Suplantación de Marca**: Es una técnica que identifica si el dominio o la URL detectada aloja contenido que suplanta maliciosamente la marca de la organización, aunque no necesariamente esté alojando una página de phishing explícita.
    - **Detección de Logotipos**: Esta técnica complementa la de Suplantación de Marca al identificar si el dominio o URL capturado aloja una página web que muestra el logotipo de la organización.
    - **Detección de Registros MX**: Los registros MX se utilizan para especificar qué servidor de correo es responsable de gestionar el correo electrónico de un dominio en particular. Esta técnica permite identificar dominios que, aunque no estén alojando contenido web malicioso, podrían estar configurados para enviar correos electrónicos de phishing.

- **Amenazas en Redes Sociales:** Muestra una lista de perfiles que suplantan a los perfiles de redes sociales de la organización. Esta función debe ser compatible con las plataformas de redes sociales X (anteriormente conocida como Twitter), LinkedIn, Facebook e Instagram.
- **Exposición de Repositorios de Código:** Muestra una lista de atributos que han sido expuestos en repositorios de código.
- **Exposición de Buckets Abiertos:** Muestra una lista de archivos expuestos en buckets abiertos.

- **Integraciones con terceros**: La herramienta deberá tener desarrolladas integraciones con al menos plataformas Cloud como: AWS, Azure y Google Cloud Platform.

La **herramienta de EASM & Brand Protection** se entiende como **herramienta comercial ya desarrollada** en modalidad **SaaS**, viva y en constante evolución, por lo que será labor exclusiva del adjudicatario el mantenimiento de la misma y las actualizaciones a las nuevas versiones que se liberen como parte de la evolución estratégica de la herramienta durante el plazo de vigencia del contrato, sin que ello suponga ningún coste adicional al ya establecido.

3.2 Herramienta de Protección de Identidad Digital

El servicio incluirá la **provisión de una herramienta de Protección de Identidad Digital**, basada en una plataforma SaaS, que permita a determinados perfiles VIP de empresas navarras analizar el **nivel de exposición de su identidad digital en Ciberseguridad** desde una perspectiva externa y la generación de **planes de mejora personalizados** en base al estado de esta.

El **objetivo** de la herramienta de Protección de Identidad Digital es proporcionar un análisis en tiempo real de exposición de la identidad, activos digitales y actividades en curso relacionadas sobre ciertos perfiles VIP (directivos) de empresas navarras y un plan de mejora, en base a un análisis externo y no intrusivo del nivel de exposición basado en las principales categorías de exposición de identidad digital (información personal identificativa, documentos de identidad, activos financieros, perfiles de RRSS, etc.)

Debe ayudar a prevenir riesgos asociados con la suplantación de identidad, fraudes financieros y otras amenazas que puedan comprometer la integridad personal y patrimonial de los usuarios monitorizados.

Para ello, la herramienta de Protección de Identidad Digital debe permitir optar por un **modelo de análisis continuo de la exposición de identidad digital**, permitiendo **elaborar un plan de mejora y/o remediación**, basado en las principales debilidades detectadas.

La **herramienta de Protección de Identidad Digital** deberá cumplir con los siguientes **requisitos mínimos**:

- Funcionamiento **no intrusivo y automatizado**. La plataforma deberá tener un funcionamiento 100% automatizado sin necesidad de intervención humana.
- La medición del **nivel de exposición** de **Identidad Digital** se realizará analizando distintos ámbitos digitales de **Internet, Deep Web y Dark Web** como mínimo. Estos deben incluir: Repositorios GIT, sitios Paste, Foros, RRSS, etc.
- La información analizada deberá ser únicamente relativa a aquellos perfiles sobre los que se haya obtenido la correspondiente autorización de protección, garantizando así que se **cumplen** estrictamente los **límites normativos** aplicables en cada caso.
- La herramienta deberá ser capaz de proporcionar una serie de **recomendaciones de mejora personalizadas**, a partir de los objetivos fijados y los resultados del análisis, proponiendo una serie de medidas concretas que permitan alcanzar esos objetivos.
- La herramienta deberá ser capaz de generar **informes** sobre el estado y evolución de la exposición de identidad de cada perfil analizado, indicando como ha mejorado/empeorado ésta en el tiempo.
- La herramienta deberá contar con un **manual o guía de ayuda** que facilite el uso, comprensión y explotación de la misma.
- El acceso a la herramienta se hará a través de una **plataforma SaaS centralizada**, públicamente accesible y convenientemente **securizada**. Se deberán proporcionar informes de las últimas certificaciones/auditorías de ciberseguridad de la misma.
- Debe permitir la definición de **diferentes roles de acceso** en función de la tipología de los grupos de usuarios (empresas finales y NavCC).
- La herramienta debe cumplir con las siguientes **funciones**:
    - Debe **monitorizar y salvaguardar** diversas categorías de **información personal sensible** incluyendo:
        - **Información personal identificativa:** Como nombres completos, apodos y datos de contacto (correos electrónicos y números de teléfono).
        - **Documentos de identidad**: Incluyendo DNI, tarjeta sanitaria, pasaporte y carnet de conducir.
        - **Activos financieros**: Cuentas bancarias, tarjetas de crédito, criptowallets y operaciones financieras en curso.
        - **Perfiles en redes sociales**: Cuentas en plataformas como LinkedIn, Facebook, X (anteriormente Twitter), Instagram y Telegram.

La **herramienta de Protección de Identidad Digital** se entiende como **herramienta comercial ya desarrollada** en modalidad **SaaS**, viva y en constante evolución, por lo

que será labor exclusiva del adjudicatario el mantenimiento de la misma y las actualizaciones a las nuevas versiones que se liberen como parte de la evolución estratégica de la herramienta durante el plazo de vigencia del contrato, sin que ello suponga ningún coste adicional al ya establecido.

3.3 Servicio de acompañamiento y reporting

El servicio incluirá acciones de **acompañamiento y reporting** cuyo objetivo es acompañar a las empresas en la ejecución de las campañas, y al Navarra Cybersecurity Center en el reporting ejecutivo de los resultados obtenidos y las conclusiones derivadas de ellos.

El servicio de **acompañamiento a las empresas** deberá cumplir con los siguientes **requisitos mínimos**:

- Recopilación de necesidades y objetivos de cada empresa, para establecer las bases y expectativas del servicio.
- Provisión y gestión de las plataformas de EASM & Brand Protection y Protección de Identidad Digital para cumplir con las necesidades definidas.
- Monitorización continua de la superficie de exposición, protección de marca y perfiles VIP.
- Seguimiento continuo con las empresas para tratar las detecciones, incluyendo workshops periódicos, presenciales y remotos, presentación de resultados y validación de las medidas adoptadas
- Informe final personalizado de conclusiones (técnico y ejecutivo), incluyendo scoring de riesgo, resumen de hallazgos más importantes y propuesta de plan de mejora personalizado para la empresa.

El servicio de **reporting ejecutivo** para el **NavCC** deberá cumplir con los siguientes **requisitos mínimos**:

- Creación de un **informe ejecutivo** para el NavCC con datos globales y comparativa sectorial que permita reflejar los diferentes grados de exposición en ciberseguridad por sector.
- Los datos deben estar anonimizados, de manera que se puedan publicar los resultados sin desvelar información sensible de las empresas.
- Resumen ejecutivo de los resultados obtenidos en las diferentes campañas, enfatizando los puntos fuertes y las áreas de mejora a impulsar.

- Los informes se actualizarán al cierre de cada una de las campañas y al finalizar el servicio.

4 METODOLOGÍA Y PLAN DE TRABAJO

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 (3 DESCRIPCIÓN DEL SERVICIO). En la metodología la empresa licitadora deberá detallar la forma en la que abordará cada uno de los servicios definidos para el proyecto. El nivel de detalle aportado será el necesario para expresar que el método propuesto permitirá alcanzar los objetivos fijados.

La empresa licitadora deberá presentar un plan de trabajo que incluya, al menos, las tareas, hitos y entregables asociados a los trabajos. Dichas propuestas deberán estar basadas en su experiencia y se incluirá una descripción que detalle cada tarea definiéndola con un grado de profundidad que permita comprender su alcance.

5 EQUIPO DE TRABAJO

El equipo estará formado por el número de profesionales, perfiles y dedicaciones que la empresa adjudicataria considere necesario para satisfacer, con garantías, todos y cada uno de los servicios antes descritos. En particular, se considera que el equipo de trabajo debería estar, al menos, compuesto por los siguientes perfiles:

- **Gestor del Servicio**: punto único de contacto para el control de la operativa del servicio con el Navarra Cybersecurity Center.
- **Equipo de Servicio**: encargado de proporcionar los servicios de acompañamiento a las empresas y reporting para el Navarra Cybersecurity Center.

Los profesionales que sean responsables de la ejecución del trabajo deberán disponer de la cualificación y experiencia necesarias para que se lleven a cabo de forma satisfactoria los trabajos indicados y se alcancen los objetivos deseados.

El personal asignado al contrato dependerá exclusivamente de la empresa adjudicataria. En ningún supuesto podrá considerarse con relación laboral, contractual, funcionarial o de naturaleza alguna respecto del Gobierno de Navarra, NASERTIC, y/o sociedades

participadas por los mismos, tanto durante la vigencia del contrato como al término de este.

6 DIRECCIÓN Y CONTROL DE LOS TRABAJOS

Corresponde a la Dirección Técnica del proyecto en NASERTIC, 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, NASERTIC indicará al comienzo del proyecto, la persona que ostentará la Dirección de Proyecto en NASERTIC y la composición de miembros del Equipo Director. Las funciones de este equipo en relación con el presente pliego serán:

- Velar por el adecuado cumplimiento de los servicios contratados.
- Independientemente de las reuniones ya establecidas en el Plan de Proyecto, la Dirección 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 adjudicatario será responsable de la redacción y distribución de los informes de seguimiento y las correspondientes actas de reunión.
- Con el fin de garantizar que se satisfacen las necesidades y prioridades establecidas por el Equipo Director de Proyecto, se marcarán desde el lanzamiento las directrices de los trabajos a realizar, siendo estas directrices de obligado cumplimiento por parte del adjudicatario.
- 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 de desviación (en plazo y/o alcance) a lo largo del proyecto.

En las reuniones periódicas se evaluarán todas aquellas incidencias habidas que se hubieran originado en el cumplimiento de los objetivos planificados. Cuando a juicio de la Dirección del Proyecto, tales incidencias fueran imputables al adjudicatario, 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 Pliego de Cláusulas Administrativas Particulares.

7 OBLIGACIONES DE INFORMACIÓN Y DOCUMENTACIÓN

Durante la ejecución de los trabajos objeto del contrato, el adjudicatario se compromete, en todo momento, a facilitar a las personas designadas por la Dirección de Proyecto, la información y documentación que éstas 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 utilizados para resolverlos.

Así mismo, el adjudicatario estará obligado a asistir y colaborar, a través del personal que designe a este propósito, en las reuniones de seguimiento del proyecto definidas por la Dirección de Proyecto, quién se compromete a citar con la debida antelación al personal de la adjudicataria.

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

En este sentido, el adjudicatario deberá informar a la Dirección de Proyecto 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 la Dirección de Proyecto, de cumplimiento de los servicios.

El adjudicatario proporcionará, sin coste adicional para la Sociedad, una copia en soporte digital con toda la documentación generada durante la prestación de los servicios objeto del contrato.