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 CONCIENCIACIÓN EN CIBERSEGURIDAD PARA LA SOCIEDAD NAVARRA"

AGOSTO 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 Concienciación en Ciberseguridad para la Sociedad 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 Concienciación en Ciberseguridad para la Sociedad Navarra",** en el marco de actuaciones del Navarra Cybersecurity Center (NavCC) es poner a disposición de la ciudadanía, del entorno educativo y del tejido empresarial y social navarro un conjunto de recursos, herramientas y actividades que permitan elevar el conocimiento, concienciación y sensibilidad general en materia de ciberseguridad. Este conjunto de acciones, tanto presenciales como digitales, contribuirán a fortalecer la ciberresiliencia individual y colectiva e impulsarán el nivel de madurez en ciberseguridad de la sociedad navarra de forma transversal.

Como soporte central del ecosistema de sensibilización, el adjudicatario desarrollará e implantará un portal web específico para el NavCC, que aglutine los contenidos formativos y divulgativos, los recursos interactivos, los indicadores de impacto y el acceso a los distintos servicios y materiales. Este portal deberá ser accesible, seguro, adaptable a distintos dispositivos y conforme a los estándares de calidad, accesibilidad y usabilidad definidos en la normativa vigente.

Además, el adjudicatario deberá diseñar, proponer y elaborar los materiales a compartir en los distintos perfiles del NavCC en redes sociales institucionales, como noticias, píldoras, videos cortos, etc. Esto permitirá maximizar la difusión de los mensajes clave, promover la participación ciudadana y reforzar la identidad pública del programa de concienciación, así como dar a conocer la propia web del centro. Cabe destacar que la estrategia de comunicación digital, así como la publicación de los contenidos generados por el licitador en redes sociales, será llevada a cabo internamente desde el NavCC, quedando así fuera del alcance de esta licitación.

Asimismo, el prestatario del servicio diseñará y ejecutará campañas de concienciación multicanal, desarrollará contenidos adaptados a distintos perfiles (ciudadanía, jóvenes, mayores, pymes, colectivos con riesgo elevado, etc.), y proporcionará informes ejecutivos de impacto, con objeto de presentar los resultados de las actividades desarrolladas y la evolución del nivel de sensibilización mediante indicadores objetivos y medibles.

De esta manera, el prestatario deberá definir e implementar un plan de acción personalizado y priorizado, que contemple la generación de contenidos en diversos formatos (noticias, píldoras, vídeos, infografías, podcasts, contenidos virales, actividades presenciales, etc.), así como la evaluación continua de su efectividad, permitiendo ajustar las acciones conforme a los perfiles, canales y temáticas más relevantes.

En este marco, una de las acciones destacadas será la planificación, preparación y ejecución de las jornadas presenciales dirigidas a la ciudadanía y centros educativos que se desarrollarán durante la Semana Navarra de la Ciberseguridad, que se celebrará en la tercera semana de octubre. La preparación y producción de los contenidos asociados deberá iniciarse desde el comienzo del contrato, garantizando su adecuada planificación y alineación con los objetivos del NavCC.

Adicionalmente, el servicio permitirá al NavCC obtener una visión global y segmentada del estado de sensibilización de la sociedad navarra en materia de ciberseguridad, facilitando la medición del impacto de las actuaciones realizadas y la identificación de necesidades específicas por sectores, territorios o franjas de edad, contribuyendo así a la mejora continua de la ciberresiliencia del conjunto de la sociedad navarra.

Cabe destacar que las acciones, metodologías y materiales generados en el marco del presente contrato se podrán utilizar también en otros ámbitos o contextos, como puede ser el de la Administración Pública, las Entidades Locales o las Sociedades Públicas, siempre dentro de los términos de licenciamiento acordados.

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 del presente documento:

- Desarrollo y ejecución de jornadas presenciales en el marco de la Semana Navarra de la Ciberseguridad:
  - Semana temática que tendrá lugar durante la tercera semana del mes de octubre (20-26 de octubre).
  - Incluirá jornadas presenciales en centros educativos, eventos abiertos a la ciudadanía y distribución de materiales promocionales.
  - La preparación y producción de contenidos para esta semana comenzará desde el inicio del proyecto.

- Desarrollo y dinamización del portal web del Navarra Cybersecurity Center (NavCC):
  - Creación y despliegue de un portal web dinámico, accesible y adaptado a la imagen institucional del centro, que actúe como repositorio central de los servicios del NavCC, así como de sus contenidos, recursos, campañas e indicadores de impacto entre otros.
  - El portal incluirá todos los servicios actuales del NavCC (Libro Blanco, herramienta de autodiagnóstico, EASM, etc.), así como su personalización gráfica (look & feel) y métricas de uso.

- Diseño, propuesta, elaboración y producción de materiales originales de capacitación y concienciación para su difusión en los perfiles de redes sociales del NavCC y en otros canales de comunicación del centro. Estos materiales podrán incluir noticias, píldoras informativas, vídeos, infografías, podcasts, contenidos virales y referencias a actividades presenciales, en los formatos especificados en el

punto 3 DESCRIPCIÓN DEL SERVICIO del presente pliego. La publicación en las redes sociales del NavCC será gestionada internamente por el propio centro.

- Ejecución de campañas de sensibilización y concienciación:
  - Diseño, desarrollo y ejecución de campañas presenciales (al menos 60 jornadas en centros educativos, colectivos específicos y ciudadanía).
  - Ejecución de campañas online (al menos 40 sesiones) dirigidas a diferentes colectivos.

- Elaboración de informes e indicadores de impacto:
  - Diseño de métricas de evaluación (KPIs) y seguimiento de resultados.
  - Elaboración de informes ejecutivos sobre el alcance y efectividad de las campañas y materiales, con periodicidad acordada.

- Coordinación, gestión y seguimiento del proyecto:
  - Asignación de un perfil de coordinador y dinamizador con presencia física en la sede del NavCC, sita en el Polo de Innovación Digital IRIS Navarra y con dedicación exclusiva al proyecto.

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

- **FASE 0: Planificación de las jornadas integradas en la Semana Navarra de la Ciberseguridad y puesta en marcha de redes sociales institucionales**
  Esta fase incluye la planificación, preparación y ejecución de las jornadas presenciales dirigidas a ciudadanía y centros educativos, que se desarrollarán durante la Semana Navarra de la Ciberseguridad. A su vez, contempla la activación inicial de los canales institucionales en redes sociales, con programación de publicaciones y difusión de contenidos alineados con los objetivos del proyecto.
  El perfil dinamizador asignado liderará la ejecución integral de esta fase y deberá contar con un plan global de trabajo que asegure la continuidad y evolución del resto de fases del proyecto. Este plan incluirá hitos, cronograma, recursos implicados y mecanismos de coordinación con el resto de los actores participantes.

  Esta fase deberá estar finalizada y validada por las personas gestores del proyecto por parte de NASERTIC en el plazo máximo de un (1) mes desde la fecha de envío del pedido.

- **FASE 1: Primera campaña de sensibilización y dinamización y puesta en producción del portal web del NavCC**
  Durante esta fase se desarrollará la primera campaña de sensibilización, que comprenderá acciones presenciales y online dirigidas a distintos públicos objetivos, así como la generación y difusión de contenidos multicanal en diversos formatos como vídeos, infografías, podcasts, entre otros. Igualmente, se llevarán a cabo actividades formativas y acciones de comunicación digital, garantizando la coordinación y el soporte técnico continuado durante toda la fase.

Adicionalmente, esta fase incluirá el desarrollo y la puesta en producción del portal web del NavCC, integrando su validación funcional y la carga de contenidos iniciales. Asimismo, se desarrollarán y dinamizarán contenidos específicos para las redes sociales del NavCC.

El perfil dinamizador será el responsable de liderar la ejecución de esta fase, asegurando la entrega en tiempo y forma de los contenidos y la correcta coordinación con todos los actores implicados, con el objetivo de garantizar el despliegue eficaz de la campaña de sensibilización y la adecuada puesta en marcha del portal web.

Esta fase deberá estar finalizada y validada por las personas gestores del proyecto por parte de NASERTIC para el **31 de diciembre de 2025.**

- **FASE 2: Segunda campaña de sensibilización y dinamización**
  Esta segunda fase se enfocará en proporcionar continuidad a las acciones iniciadas en la campaña anterior. Se mantendrá la generación regular de contenidos de concienciación por parte del licitador, con nuevos materiales audiovisuales y recursos interactivos para las distintas plataformas. Asimismo, se seguirán desarrollando acciones presenciales en centros educativos, con colectivos específicos, y ciudadanía ajustando su enfoque en función de los aprendizajes y métricas recogidas en la primera campaña. Se reforzarán también las campañas digitales en redes sociales. El portal web seguirá siendo el eje central de contenido, actualizándose con nuevos materiales y recursos. Asimismo, se mantendrá la supervisión de su correcto funcionamiento conforme a los requisitos establecidos en la presente licitación. El perfil dinamizador continuará ejerciendo su papel transversal de coordinación, asegurando la coherencia entre las acciones, la entrega regular de contenidos y materiales y la monitorización de indicadores clave (KPIs) definidos para medir el impacto del proyecto.

  Esta fase deberá estar finalizada y validada por las personas gestores del proyecto por parte de NASERTIC para el **31 de marzo de 2026.**

- **FASE 3: Tercera campaña de sensibilización y dinamización**
  Esta fase del proyecto estará orientada a finalizar el ciclo de sensibilización propuesto mediante el desarrollo de una tercera campaña de concienciación, que permita ampliar el alcance y reforzar la ciberresiliencia de la sociedad navarra. Esta campaña incluirá nuevas acciones presenciales y online, así como la producción de contenidos multicanal que refuercen el hilo conductor del proyecto. Durante esta fase, el portal web del NavCC continuará operando como plataforma principal de referencia, manteniéndose actualizada con los contenidos oportunos. El perfil dinamizador será responsable de coordinar el cierre operativo del proyecto, supervisando la ejecución de la campaña final, la recopilación de evidencias, y la elaboración de una evaluación interna global, basada en los indicadores de impacto definidos desde el inicio del proyecto.

  Tras la realización de esta campaña de concienciación, el adjudicatario presentará un (1) informe de impacto consolidado. En esta última fase de ejecución, el

adjudicatario presentará lecciones aprendidas, así como las propuestas de continuidad. Esta fase incluirá además la entrega de los materiales desarrollados, repositorios organizados y estadísticas de uso.

Esta última fase deberá estar finalizada y validada por las personas gestores del proyecto por parte de NASERTIC para el **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.

Durante la ejecución del contrato, el adjudicatario se obliga a guardar secreto profesional sobre toda la información a la que acceda en el marco de la prestación del servicio, así como a asegurar que todo el personal implicado en el proyecto mantendrá la misma confidencialidad. Dicha información no podrá ser utilizada, copiada ni cedida total ni parcialmente para fines distintos a los establecidos en el presente contrato.

Para la prestación del servicio, el **adjudicatario** deberá presentar en su oferta una descripción detallada de las siguientes líneas de trabajo, incluyendo para cada una de ellas las funcionalidades, metodologías, herramientas y recursos humanos previstos:

3.1 Semana Navarra de la Ciberseguridad

El servicio incluirá la **preparación y ejecución de actividades integradas en la Semana Navarra de la Ciberseguridad**, acción destacada del proyecto que se desarrollará durante la tercera semana del mes de octubre (20-26 de octubre). Este evento tiene carácter emblemático dentro de la estrategia del NavCC, y tiene como objetivo visibilizar la importancia de la ciberseguridad en todos los ámbitos de la sociedad navarra mediante actividades, contenidos y acciones de sensibilización y comunicación.

Dentro del alcance de la presente licitación, el adjudicatario deberá:

- Presentar una **propuesta de planificación de actividades integradas en la semana temática**, que deberá incluir:
  - Un **cronograma** detallado de **actividades presenciales** propuestas.
  - La propuesta de ubicaciones y espacios.
  - Una estimación de los recursos necesarios para su ejecución.
  - 6 jornadas presenciales en 3 ubicaciones diferentes (Pamplona, Tudela y Estella).
- Organizar **jornadas presenciales** en **centros educativos** y en **espacios públicos**, dirigidas fundamentalmente a ciudadanía general y centros educativos. Estas actividades podrán adoptar formatos susceptibles de ser propuestos por parte del licitador.

Quedan excluidas del alcance de esta licitación otras acciones complementarias relacionadas con la Semana Navarra de la Ciberseguridad, tales como:

- La **logística** y **producción audiovisual** global del **evento**, así como la gestión y reserva de los espacios físicos.
- La **gestión de prensa** y **cobertura mediática** general.

Estas acciones serán gestionadas directamente por el NavCC. No obstante, el **perfil coordinador** del adjudicatario será responsable de **asegurar la coordinación efectiva con el NavCC,** de forma que las actuaciones previstas en la presente licitación estén **alineadas, no duplicadas y correctamente integradas** dentro de la programación global de la Semana. Adicionalmente, el adjudicatario deberá:

- Prestar especial atención a la **campaña de comunicación previa de las actividades bajo su responsabilidad**, asegurando la generación de contenido con **al menos un mes de antelación**, con el fin de generar interés, fomentar inscripciones y facilitar la participación ciudadana.

- Garantizar la coordinación de la **documentación audiovisual de las actividades organizadas dentro del contrato**, para su posterior difusión digital o institucional, colaborando directamente con el NavCC para asegurar una cobertura mediática adecuada del evento.

- Mostrar capacidad para **movilizar actores locales**, así como asociaciones, centros educativos, colectivos sociales y empresas del ámbito tecnológico, con el objetivo de construir una programación variada, creativa y coherente con las **líneas estratégicas del NavCC**.

3.2 Desarrollo e implantación del portal web del NavCC

El servicio incluirá el diseño, desarrollo, implantación y mantenimiento de un portal web del NavCC, que actuará como eje central de comunicación, divulgación y difusión de servicios, recursos y actividades de sensibilización en materia de ciberseguridad dirigidas a la ciudadanía, el entorno educativo y el tejido empresarial navarro.

El objetivo principal del portal es servir como plataforma digital de referencia en ciberseguridad para la sociedad navarra, garantizando la integración con todos los servicios disponibles para el ecosistema empresarial, el acceso centralizado a materiales formativos, campañas, eventos, datos de impacto y noticias.

Para ello, el portal deberá cumplir con los siguientes **requisitos mínimos**:

- **Diseño adaptado y personalizado**. El portal deberá permitir adaptar su imagen a la identidad corporativa del NavCC (logotipos, colores corporativos, tipografía, etc.). La interfaz debe ser clara con especial atención a la experiencia de usuario. Para este fin, se facilitará al adjudicatario el manual de identidad del centro.
- **Despliegue y hosting de la plataforma**. El despliegue se realizará en un hosting proporcionado por el adjudicatario, el cual deberá cumplir con los requisitos mínimos indicados en el Acuerdo de Nivel de Servicio (SLA) – Requisitos Seguridad Portal Web.

- **Desarrollo con criterios de accesibilidad y usabilidad**. Será imprescindible que cumpla con los criterios de accesibilidad y usabilidad web vigentes, alcanzando al menos el nivel AA del estándar WCAG. Asimismo, deberá garantizarse su correcta visualización en todo tipo de dispositivos (ordenadores, tabletas, móviles) y navegadores actuales, sin requerir complementos adicionales.

  Del mismo modo, el portal deberá desarrollarse siguiendo buenas prácticas de optimización para motores de búsqueda (SEO), con el fin de asegurar una adecuada indexación en buscadores y mejorar su visibilidad.

- **Gestión de contenidos (CMS)**. El portal deberá incorporar un sistema de gestión de contenidos (CMS) estable, con soporte activo, y permitir la gestión diferenciada de roles de usuario (editores, administradores, etc.).

- **Asistente virtual**. El portal web deberá contar con un asistente virtual inteligente capaz de proporcionar orientación avanzada y contextualizada a los usuarios. Este asistente deberá ser capaz de resolver dudas frecuentes, ofrecer recomendaciones personalizadas y redirigir al usuario hacia secciones específicas del portal, entre los que se encuentran los servicios del NavCC o materiales concretos, con el objetivo de promover una experiencia de uso fluida. En particular, el asistente deberá ser capaz de interpretar las necesidades específicas expresadas por el usuario y dirigirlo de forma precisa al contenido relevante dentro de dichos servicios o recursos del NavCC. El asistente deberá estar disponible en, al menos, los siguientes idiomas: euskera, castellano e inglés.

- **Secciones mínimas del portal.** Como mínimo, el portal deberá contemplar las siguientes secciones:
  - Incorporación de un asistente virtual.
  - El portal debe ser multiidioma (mínimo euskera, inglés y castellano).
  - Página de inicio con novedades destacadas
  - Calendario de eventos y actividades
  - Repositorio con todos los recursos de concienciación (noticias, píldoras, vídeos, infografías, podcasts, contenidos virales, actividades presenciales, etc.)
  - Sección con todos los servicios del NavCC (Libro Blanco, herramienta de autodiagnóstico, EASM, etc.)
  - Apartado de contacto y preguntas frecuentes (FAQ)
  - Sección destinada a la difusión de eventos y actividades impulsadas por el NavCC, incluyendo, entre otros, la Semana Navarra de la Ciberseguridad.
  - Espacio con enlaces directos a los perfiles de redes sociales institucionales del NavCC.

- **Seguridad y privacidad del portal web.** Lo relativo a este apartado deberá cumplir con los requisitos mínimos indicados en el Acuerdo de Nivel de Servicio (SLA) – Requisitos Seguridad Portal Web.

Según lo establecido en el Pliego de Cláusulas Administrativas (PCA), y atendiendo a los criterios sometidos a juicios de valor, se valorará la inclusión de funcionalidades adicionales, la originalidad y creatividad global de la propuesta.

El portal web deberá estar operativo al finalizar la FASE 1 del proyecto, y deberá mantenerse actualizado durante toda la duración del contrato.

- La plataforma deberá ser escalable, de modo que pueda incorporar nuevas secciones o funcionalidades a futuro.
- El adjudicatario será responsable del mantenimiento y actualizaciones técnicas necesarias, sin coste adicional durante la vigencia del contrato.

3.3 Redes sociales institucionales del NavCC

El servicio incluirá el diseño, propuesta y elaboración de materiales para compartir en los distintos perfiles de redes sociales del NavCC, con el objetivo de establecer canales efectivos de comunicación digital que favorezcan la divulgación de contenidos, la interacción con la ciudadanía e incrementen el impacto de las campañas de concienciación.

La publicación de estos materiales y contenidos en las RRSS del centro será llevada a cabo internamente desde el NavCC, quedando así este aspecto fuera de la presente licitación.

- El adjudicatario deberá desarrollar un **plan estratégico** de **creación de materiales** para redes sociales, que contemple la definición del tipo de contenidos, frecuencia de publicación y formatos utilizados.

- Se deberán crear contenidos de forma periódica, **adaptados al canal, al perfil del público objetivo y a la actualidad**, incluyendo noticias breves, recomendaciones, vídeos, retos, materiales educativos, encuestas y mensajes clave de campañas en curso. También podrán utilizarse hashtags temáticos y elementos visuales que refuercen la identidad del proyecto.

- En caso de eventos alrededor de la Semana Navarra de la Ciberseguridad, campañas presenciales u online, se deberá crear contenido orientado a reforzar las acciones en redes, tanto antes como durante y después de cada hito, asegurando la **máxima visibilidad** y **cobertura digital**.

- Se prestará especial atención a la **calidad gráfica** y **comunicativa de los contenidos**, que deberán ser coherentes con la identidad corporativa del NavCC y estar correctamente adaptados al entorno de cada red social.

3.4 Producción de materiales de capacitación y concienciación

El servicio incluirá la generación de materiales didácticos y de concienciación dirigidos a distintos perfiles de la sociedad navarra, con el fin de apoyar las campañas y jornadas previstas, reforzar el aprendizaje y ofrecer recursos reutilizables que permitan consolidar conocimientos en materia de ciberseguridad.

El adjudicatario deberá diseñar y elaborar un conjunto de contenidos multimedia en formatos variados, accesibles, adaptados a distintos niveles de conocimiento y tipos de usuario, desde público general hasta colectivos específicos como estudiantes de secundaria, personas mayores o profesionales de diferentes sectores.

Todo el material generado en el contexto de la presente licitación será propiedad del NavCC.

Los materiales de capacitación y concienciación deberán cumplir con los siguientes requisitos mínimos:

- Se deberán elaborar, como mínimo:
  - Diez (10) vídeos de concienciación con estructura narrativa acompañados de un hilo conductor (formato miniserie), con elementos gráficos y duración adecuada.
  - Doce (12) infografías o guías visuales en formato compartible de buenas prácticas en materia de ciberseguridad.
  - Doce (12) retos virales gamificados diseñados para maximizar su difusión en redes sociales.
  - Doce (12) podcasts de ciberseguridad.
  - Boletín mensual del estado de ciberseguridad en Navarra con suscripción de las últimas noticias.
  - Noticias y alertas de seguridad semanales.

- Deberá presentarse una estrategia global con los objetivos de concienciación que se quieren conseguir y cómo se alcanzan con los distintos materiales propuestos.

- Todos los materiales deberán entregarse en formatos digitales adecuados para su integración en el portal web, difusión en redes sociales o impresión bajo demanda, incluyendo versiones editables, si así lo requiere el NavCC. Los vídeos deberán estar subtitulados en multiidioma (euskera y castellano) y los audios deberán acompañarse de una breve transcripción o resumen.

- Deberá contarse con la capacidad de generar contenidos dirigidos a personas usuarias tanto en euskera (al menos en un 20% del total) como en castellano, esto deberá acordarse previamente con el NavCC en función de la tipología del contenido y la plataforma de difusión del mismo.

- Los contenidos deberán tener una periodicidad de publicación coherente con la estrategia del NavCC, favoreciendo la continuidad y evitando periodos prolongados sin actualizaciones. Será responsabilidad del perfil dinamizador planificar y coordinar dicha periodicidad, asegurando su alineación con la estrategia de comunicación global definida internamente por el NavCC.

- El adjudicatario será responsable de la propuesta de las líneas temáticas, el guion, diseño y producción de los materiales, así como de su validación previa con el equipo del NavCC antes de su publicación.

3.5 Ejecución de campañas de sensibilización y concienciación

El servicio incluirá el diseño, planificación, ejecución y seguimiento de un conjunto de **campañas de sensibilización y concienciación en ciberseguridad**, dirigidas a la ciudadanía navarra, al ámbito educativo, al tejido empresarial y a colectivos específicos, con el objetivo de fomentar comportamientos digitales seguros y aumentar la concienciación en materia de ciberseguridad en la sociedad navarra.

Deberán cumplir con los siguientes requisitos mínimos:

- El adjudicatario deberá diseñar un **plan general de campañas**, que contemple la segmentación del público destinatario, los objetivos de comunicación, los mensajes clave, los canales utilizados (presenciales y digitales), el cronograma de ejecución y los formatos de los contenidos.

- Las campañas deberán desarrollarse en **modalidad presencial y online**. Se establece como mínimo la realización de 60 jornadas presenciales y 40 sesiones digitales a lo largo del periodo de ejecución del contrato.

- Las **jornadas presenciales** se organizarán en distintos entornos, priorizando centros educativos (secundaria y formación profesional), espacios públicos de interés (ciudadanía) y sectores profesionales que requieran especial atención. A efectos de la presente licitación, se entiende por jornada el desarrollo de múltiples actividades a lo largo de un día, en una misma ubicación física para un colectivo concreto. Estas acciones podrán adoptar el formato de charlas, talleres prácticos o dinámicas participativas adaptadas al público objetivo.

- A efectos de la presente licitación, se entiende por **sesión online** aquella actividad formativa o divulgativa que se desarrolla íntegramente en un entorno digital, mediante plataformas de videoconferencia o herramientas equivalentes, dirigida a un público previamente definido. Estas sesiones podrán complementarse con publicaciones digitales y acciones complementarias en redes sociales relacionadas con su contenido. Podrán adoptar el formato de charlas, talleres virtuales, presentaciones interactivas o dinámicas participativas, y tendrán una duración suficiente para garantizar la consecución de los objetivos planteados.

- Se garantizará que las campañas estén adaptadas al nivel de madurez en materia de ciberseguridad de los distintos perfiles destinatarios.

- El adjudicatario será responsable de la convocatoria de participantes de la campaña, la coordinación, la elaboración de materiales de cada campaña y su respectiva evaluación del impacto.

- La ejecución de las campañas deberá estar debidamente coordinada con el equipo del NavCC, y su planificación deberá permitir una **cobertura regular y equilibrada en el tiempo y en el territorio**, evitando concentraciones de actividades en periodos reducidos o zonas concretas.

- De acuerdo con lo establecido en el Pliego de Cláusulas Administrativas (PCA), se valorará, conforme a los criterios sometidos a juicios de valor, la utilización de

técnicas creativas e innovadoras como puntos clave para aumentar la visibilidad y el impacto.

Cada campaña deberá ser evaluada en términos de participación y alcance, mediante mecanismos de recogida de datos (asistencia, impresiones, visualizaciones, encuestas de satisfacción, etc.) que alimentarán los informes globales de seguimiento del proyecto.

3.6 Coordinación, seguimiento y evaluación de ejecución del servicio

El adjudicatario deberá garantizar una gestión coordinada del proyecto mediante el cumplimiento de los siguientes requisitos:

- **Responsabilidad general del servicio.** El adjudicatario será responsable de garantizar una gestión eficiente, proactiva y coordinada del conjunto de actividades previstas en el marco del contrato. Deberá garantizar el cumplimiento de los plazos establecidos y la calidad técnica de los entregables en todas las fases del proyecto.

- **Asignación de un perfil de coordinación técnica y operativa.** Se deberá asignar un perfil con dedicación exclusiva como coordinador/dinamizador del proyecto, que prestará su servicio de forma presencial en las instalaciones del NavCC, actuando como punto de contacto permanente. Actuará como interlocutor principal para la implementación de las acciones derivadas de la presente licitación.

- **Funciones del perfil dinamizador.** El perfil dinamizador asumirá las siguientes responsabilidades:

    - Coordinación técnica y operativa del proyecto.
    - Planificación de actividades y seguimiento del cronograma.
    - Supervisión de la correcta ejecución del servicio.
    - Propuesta de medidas correctoras cuando sea necesario.
    - Entrega en tiempo y forma de los materiales para su difusión en los distintos canales (web, redes sociales, medios, etc.).
    - Coordinación con todas las partes implicadas, tanto internas como externas, incluyendo:
        - Personal técnico del NavCC
        - Entidades colaboradoras
        - Agentes institucionales
        - Otros proveedores participantes en acciones complementarias promovidas por el NavCC.

- **Sistema de evaluación y seguimiento del servicio.**
    - El adjudicatario deberá proponer, establecer y mantener un sistema de indicadores (KPIs) para la evaluación continua del servicio.
    - Estos indicadores deberán ser validados por el NavCC e incluirán:
        - **Métricas cuantitativas:** alcance, visualizaciones, participación, etc. Se deberán incluir, además, métricas de interacción con el portal web.

- **Métricas cualitativas:** utilidad percibida, nivel de satisfacción, etc. Asimismo, se deberán incluir la evaluación de la experiencia del usuario del portal web mediante encuestas breves, comentarios recogidos y/o el índice de recomendación.

- **Informes de seguimiento y documentación de resultados.** A lo largo del proyecto, se requerirá la entrega periódica de informes de seguimiento, de carácter técnico y ejecutivo, que recojan el grado de ejecución de cada una de las actividades desarrolladas junto con indicadores asociados a los mismos. Al finalizar el contrato, se deberá entregar una memoria final del proyecto, que recoja de forma estructurada todos los resultados obtenidos, lecciones aprendidas, materiales producidos, estadísticas globales y propuestas de mejora, junto con el material de todos los recursos generados durante la ejecución del 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 debe estar, al menos, compuesto por los siguientes perfiles:

- **Coordinador/Dinamizador del Servicio**: punto único de contacto para el control de la operativa del servicio que desempeñará su papel de forma presencial en las instalaciones del NavCC.
- **Equipo de Consultoría**: encargado de proporcionar apoyo en la parte más técnica relativa a los servicios de sensibilización, concienciación y elaboración de materiales de concienciación para la ejecución de las diferentes campañas y jornadas establecidas durante la ejecución del servicio.
- **Equipo de Soporte**: responsable de la gestión y resolución de incidencias y vulnerabilidades reportadas, así como de garantizar el cumplimiento de los niveles de servicio (SLA) establecidos en el presente pliego.

- **Equipo de Desarrollo del Portal Web**: responsable del diseño, desarrollo, pruebas y mantenimiento evolutivo del portal web objeto de la licitación, asegurando que cumpla con los requisitos funcionales y técnicos establecidos en el marco de la presente licitación.

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.

8 ACUERDO DE NIVEL DE SERVICIO (SLA) – REQUISITOS SEGURIDAD PORTAL WEB

8.1 OBJETO Y ALCANCE

El presente Acuerdo de nivel de Servicio (SLA) tiene por objeto establecer las condiciones mínimas para el desarrollo, alojamiento, operación, mantenimiento, soporte y protección de un portal web corporativo. Incluye los requisitos técnicos y de ciberseguridad, así como los niveles de servicio exigidos al proveedor responsable.

El proveedor se compromete a prestar los servicios conforme a los estándares de calidad, seguridad, disponibilidad y cumplimiento normativo descritos en este documento.

8.2 REQUISITOS DEL PROVEEDOR

8.2.1 Cumplimiento normativo y certificaciones

El proveedor deberá acreditar que el **servicio de hosting ofrecido** cumple con el **Esquema Nacional de Seguridad (ENS)** en su categoría **Media o Alta**, mediante certificación oficial en vigor. Deberá aportar la evidencia correspondiente (certificación y/o declaración de conformidad emitida por entidad acreditada), válida durante toda la vigencia del contrato.

8.2.2 Metodología de desarrollo seguro (S-SDLC)

Durante todo el ciclo de vida del software, el proveedor aplicará metodologías que garanticen la incorporación de controles de seguridad desde la fase de análisis y diseño, que incluyan al menos:

- Definición de requisitos de ciberseguridad desde el diseño, funcional y técnico.
- Control de autenticación y autorización.
- Validación y sanitización de entradas y salidas para prevenir inyecciones y otros fallos de seguridad.
- Cifrado de datos sensibles, tanto en tránsito como en reposo, de acuerdo con estándares actuales.
- Gestión segura de sesiones de usuario.
- Protección frente a las principales amenazas recogidas en la guía OWASP Top 10 y otras referencias reconocidas.
- Registro seguro y centralizado de eventos.
- Aplicación de análisis de seguridad de código fuente (SAST), análisis de componentes y dependencias (SCA), y análisis dinámico de seguridad en aplicaciones en ejecución (DAST), en los momentos adecuados del ciclo de vida.
- Realización de pruebas de intrusión (pentesting) para identificar y valorar riesgos de seguridad explotables, y garantizar su resolución efectiva.

La planificación y frecuencia de estas actividades deberá adaptarse a los hitos del proyecto y permitir la identificación y corrección oportuna de vulnerabilidades antes de la puesta en producción y durante el mantenimiento del sistema.

8.3 INFRAESTRUCTURA, SEGURIDAD TÉCNICA Y ENTORNOS

El proveedor garantizará que el portal se despliegue y opere sobre una infraestructura segura, escalable y alineada con buenas prácticas de ciberseguridad, cumpliendo como mínimo con los siguientes aspectos:

8.3.1 Entornos y arquitectura

- Separación lógica y física de los entornos de preproducción y producción.
- Infraestructura alojada en centros de datos con certificación Tier II o superior, o en proveedores cloud con acreditaciones de seguridad equivalentes.
- Hosting dentro del Espacio Económico Europeo, preferentemente en territorio nacional.
- Arquitectura que garantice alta disponibilidad.

8.3.2 Configuración y mantenimiento

- Uso obligatorio de **comunicaciones cifradas (TLS 1.3 recomendado)**
- Mantenimiento del framework y librerías actualizado automáticamente o al menos, bajo revisión mensual.
- Aplicación periódica de **parches de seguridad,** en el caso de **ser críticos, en un plazo máximo de 24 horas**.

8.3.3 Monitorización y control continuo

- Monitorización en tiempo real de la infraestructura, logs de aplicación y eventos de seguridad.
- Implementación de SIEM o herramienta equivalente con alertas configuradas.
- Realización de dos auditorías técnicas durante la ejecución del contrato.
- Copias de seguridad diarias automáticas con retención mínima de 30 días y restauraciones probadas trimestralmente.

8.3.4 Protección perimetral y reputacional

- **Firewall de Aplicación Web (WAF)** configurado con reglas continuamente actualizadas conforme a las mejores prácticas de la industria.
- Protección activa frente a **ataques DDoS** mediante proveedor especializado.
- Monitorización contra defacement y alteraciones no autorizadas en el contenido del portal.

8.4 GESTIÓN DE VULNERABILIDADES

El proveedor se compromete a detectar, notificar y corregir fallos de seguridad de acuerdo con la siguiente tabla de tiempos máximos de remediación:

Criticidad	Tiempo remediación
Crítica	≤ 24 horas
Alta	≤ 1 día hábil
Media	≤ 7 días hábiles
Baja	≤ 15 días hábiles

Asimismo, deberán presentarse informes detallados que incluyan las vulnerabilidades detectadas durante la realización de las correspondientes auditorías de seguridad, así como su evolución y el estado de corrección. Será obligatorio realizar, como mínimo:

- Una (1) ejecución de herramientas de análisis estático de código (SAST) y de análisis de componentes (SCA) inmediatamente anterior a la puesta en producción del portal web.
- Dos (2) pruebas de intrusión (pentesting): una inmediatamente anterior a la puesta en producción del portal web y otra que deberá realizarse al menos dos meses antes de la finalización del contrato.

8.5 SOPORTE TÉCNICO Y ATENCIÓN A INCIDENCIAS

8.5.1 Cobertura del soporte

- Horario estándar: de lunes a viernes de 08:00 a 18:00 (en horario local)
- Atención 24x7 para incidencias de alta criticidad.
- Canales habilitados para la atención: el proveedor deberá proporcionar y gestionar un sistema de **Service Desk** para la atención de incidencias, peticiones y consultas relacionadas con el servicio. Adicionalmente, se habilitará la atención mediante **correo electrónico**.

8.5.2 Tiempos de respuesta

Nivel de incidencia	Tiempo respuesta máximo
Crítica	≤ 1 hora
Alta	≤ 4 horas

Media/Baja	≤ 1 día hábil

8.6 INDICADORES DE NIVEL DE SERVICIO

Se establecen los siguientes indicadores clave que deberán cumplirse mensualmente:

- Disponibilidad del portal: ≥ 99.5%
- Tiempo medio de respuesta ante incidentes de alta criticidad: ≤ 4 horas
- Tiempo medio de recuperación (MTTR): ≤ 10 horas
- Ejecución y aplicación de parches de seguridad en plazo: ≥ 90%
- Ejecución de backups: ≥ 99%

8.7 PENALIZACIONES POR INCUMPLIMIENTO

El incumplimiento de los niveles de servicio descritos implicará la aplicación de penalizaciones económicas proporcionales al impacto y duración de la afectación. Las reincidencias podrán conllevar revisión del acuerdo o cancelación anticipada del contrato.

8.8 DOCUMENTACIÓN Y EVIDENCIAS REQUERIDAS

El proveedor deberá entregar, al inicio del contrato, la siguiente documentación actualizada:

- Certificación oficial en vigor que acredite el cumplimiento del Esquema Nacional de Seguridad (ENS) en categoría Madia o Alta, correspondiente al servicio de hosting contratado.

El proveedor deberá entregar, al menos una vez al trimestre o de forma puntual a solicitud del cliente, la siguiente documentación actualizada:

- Evidencias de ejecución de pruebas de seguridad (SAST, SCA o equivalentes).
- Informes de auditorías técnicas y/o pruebas de penetración realizadas tras la ejecución de estas.
- Registro de actualizaciones y parches de seguridad aplicados.
- Reportes de vulnerabilidades y documentación asociada a la gestión y resolución de incidencias.