



PLIEGO DE CLÁUSULAS TÉCNICAS

QUE HAN DE REGIR LA CONTRATACIÓN
DE UN SERVICIO TÉCNICO INTEGRAL Y
ESPECIALIZADO DE CONCIENCIACIÓN EN
CIBERSEGURIDAD PARA NAVARRA



SEPTIEMBRE DE 2026

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.....	3
1.1	Introducción	3
1.2	Iniciativas en el ámbito de la ciberseguridad en Navarra	3
2	OBJETO OBJETIVOS Y ALCANCE DE LA CONTRATACIÓN	5
2.1	Objeto	5
2.2	Objetivos	5
2.3	Alcance	6
3	DESCRIPCIÓN DEL SERVICIO Y EQUIPO DE TRABAJO	8
3.1	Coordinación, y seguimiento del servicio	8
3.1.1	Perfil de Coordinación del Servicio.....	8
3.2	Diseño, planificación y ejecución de campañas de sensibilización y concienciación 10	
3.2.1	Estrategia de las Campañas de concienciación	10
3.2.2	Perfil de Técnico Especialista en Ciberseguridad	11
3.2.3	Perfil de Técnico en Ciberseguridad	12
3.3	Comunicación Digital, Creación de Contenidos y Gestión de Canales	13
3.3.1	Estrategia de Comunicación Digital y materiales audiovisuales	13
3.3.2	Perfil de Responsable de Comunicación Digital y Gestión de Contenidos.....	15
3.3.3	Perfil de Diseño Multimedia y Producción Audiovisual.....	16
3.4	Gestión, mantenimiento y evolución del portal web del NavCC	17
3.4.1	Portal Web del NavCC.....	17
3.4.2	Perfil de Soporte y Administración del Portal Web.	18
3.4.3	Perfil de Desarrollo y Mantenimiento Evolutivo del Portal Web.	19
4	METODOLOGÍA Y PLAN DE TRABAJO	21
5	EQUIPO DE TRABAJO	21
6	DIRECCIÓN Y CONTROL DE LOS TRABAJOS.....	22
7	OBLIGACIONES DE INFORMACIÓN Y DOCUMENTACIÓN.....	23
8	ACUERDO DE NIVEL DE SERVICIO (SLA) – REQUISITOS SEGURIDAD PORTAL WEB	24
8.1	OBJETO Y ALCANCE	24
8.2	REQUISITOS DEL PROVEEDOR.....	24
8.2.1	Metodología de desarrollo seguro (S-SDLC).....	24
8.3	GESTIÓN DE VULNERABILIDADES	24

8.4	SOPORTE TÉCNICO DE ATENCIÓN A INCIDENCIAS.....	25
8.4.1	Cobertura del soporte.....	25
8.4.2	Tiempos de atención y resolución de incidencias	25
8.5	INDICADORES DE NIVEL DE SERVICIO	26
8.6	PENALIZACIONES POR INCUMPLIMIENTO.....	26
8.7	DOCUMENTACIÓN Y EVIDENCIAS REQUERIDAS	26

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 ellas han experimentado un crecimiento exponencial. La creciente digitalización de la sociedad y la incorporación de las tecnologías de la información en todos los ámbitos de la vida cotidiana, la actividad económica y los servicios públicos han incrementado significativamente el impacto potencial de los ciberataques. Del mismo modo, la evolución tecnológica ha venido acompañada de una mayor sofisticación de las herramientas y técnicas empleadas por los actores maliciosos, aumentando tanto la probabilidad como las consecuencias de estos incidentes.

Esta situación provoca que ciudadanos, empresas, administraciones públicas y organizaciones de todo tipo estén expuestos a un nivel de riesgo elevado, dinámico y cada vez más complejo de gestionar. Cada día conocemos nuevos casos en los que ciberataques afectan a servicios esenciales, comprometen información sensible o interrumpen la actividad normal de entidades públicas y privadas, con un impacto directo sobre la sociedad en su conjunto.

En este contexto, resulta necesario fomentar una cultura de ciberseguridad que alcance a toda la sociedad. La rápida evolución de las tecnologías digitales y su adopción masiva generan nuevas oportunidades, pero también nuevos desafíos que requieren una gestión adecuada de los riesgos. Por ello, es fundamental concienciar y sensibilizar sobre los riesgos y buenas prácticas en ciberseguridad para garantizar que la transformación digital pueda desarrollarse de forma segura y confiable.

Para lograrlo, es necesario promover espacios de colaboración regional público-privada que involucren a la administración, las empresas, el ámbito académico y la sociedad civil. Esta colaboración debe servir no solo para impulsar la innovación y la adopción de soluciones de ciberseguridad, sino también para promover una cultura de ciberseguridad transversal que alcance al conjunto de la ciudadanía. La seguridad en el entorno digital no depende únicamente de la tecnología, sino también del conocimiento, la concienciación y el comportamiento de las personas. Por ello, la sensibilización y la capacitación de la población constituyen elementos clave para reducir la exposición a las amenazas digitales, fomentar un uso seguro y responsable de las tecnologías, reforzar la confianza en los servicios digitales y aumentar la resiliencia de la sociedad frente a los crecientes riesgos del ciberespacio.

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 la creación del [Navarra Cybersecurity Center \(NavCC\)](#) como centro de referencia en materia de ciberseguridad en Navarra. Su principal objetivo es el impulso para el desarrollo de iniciativas en torno a la ciberseguridad que deriven en un aumento de la ciberresiliencia

en todos los ámbitos de la Comunidad Foral de Navarra (ciudadanía, tejido empresarial, talento y administraciones públicas).

El Navarra Cybersecurity Center (NavCC) es una iniciativa liderada por el Departamento de Universidad, Innovación y Transformación Digital del Gobierno de Navarra, enmarcada en el proyecto colaborativo CIBERREG - *Impulso a la ciberseguridad desde los territorios* -, que cuenta con la participación de otras siete regiones españolas y que forma parte del [programa RETECH](#) (Redes Territoriales de Especialización Tecnológica), impulsado por la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales, coordinado por INCIBE y financiado con fondos del Plan de Recuperación, Transformación y Resiliencia (Next Generation).

Las iniciativas del Navarra Cybersecurity Center están dirigidas a la generación de una cultura de ciberseguridad en la Comunidad Foral contribuyendo de esta manera a la transformación socioeconómica sostenible de Navarra en un entorno digital, hiperconectado y ciberresiliente. En este sentido, se han definido una serie de líneas de actuación estratégicas, en las que se enmarca todo el espectro de acciones que desarrolla el centro:

- **Centro de Ciberseguridad:** sirviendo como ventanilla única y punto de referencia para acercar la ciberseguridad a la sociedad navarra, apoyándose para ello en los servicios que ofrece INCIBE (Instituto Nacional de Ciberseguridad de España)
- **Fomento del ecosistema empresarial:** identificando los actores clave en el sector de la ciberseguridad en Navarra, creando un catálogo de productos y servicios, promoviendo e incentivando una cultura de ciberseguridad entre el tejido empresarial navarro
- **Gestión del talento:** impulsando la creación de itinerarios formativos especializados en ciberseguridad, en colaboración con universidades y centros de formación profesional, con el objetivo de generar talento profesional altamente cualificado que garantice el crecimiento sostenible del sector
- **Sensibilización:** desarrollando campañas de concienciación en materia de ciberseguridad para ciudadanía y empresas que permitan elevar el conocimiento y sensibilidad sobre los riesgos, las amenazas y las medidas de prevención, contribuyendo a fortalecer la ciberresiliencia individual y colectiva.

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 Técnico Integral y Especializado de Concienciación en Ciberseguridad para 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.

La prestación de los servicios objeto del presente Pliego por parte de la empresa adjudicataria se configura como un servicio técnico integral y especializado, que permita disponer de las capacidades necesarias en cada momento para poder dar respuesta con los niveles de calidad requeridos.

El Adjudicatario deberá concretar en su respectiva oferta la propuesta de servicio y equipo técnico ofrecido que, ajustándose a lo solicitado en el Pliego, se considere idóneo para atender las necesidades en éste especificadas. No es objetivo de este el contratar un equipo de personas sino el disponer de un servicio técnico integral y especializado de concienciación en ciberseguridad ligado al cumplimiento de las metas fijadas para el proyecto, las cuales quedarán establecidas al inicio del contrato.

2.2 Objetivos

El principal objetivo de la contratación de un **"Servicio Técnico Integral y Especializado de Concienciación en Ciberseguridad para 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 digitales como presenciales, 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 mantendrá y gestionará el portal web del NavCC, que aglutina los contenidos formativos y divulgativos, los recursos interactivos, los indicadores de impacto y el acceso a los distintos servicios y materiales.

Además, el adjudicatario deberá proponer, diseñar y elaborar un plan de comunicación digital basado en una serie de contenidos a compartir en los distintos perfiles del NavCC en redes sociales institucionales, como noticias, píldoras, videos cortos, infografías, podcasts, contenidos virales 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 en redes sociales y portal web, será llevada a cabo por el propio licitador en coordinación con el NavCC.

Asimismo, el prestatario del servicio diseñará y ejecutará un plan de campañas de concienciación multicanal, basado en sesiones presenciales y on-line, y con un enfoque personalizado, priorizado y adaptado a la realidad del conjunto de la sociedad navarra y los distintos públicos objetivo (ciudadanía, menores, mayores, pymes, colectivos vulnerables, etc.). En este marco, una de las acciones destacadas será la planificación, preparación y ejecución de campañas presenciales dirigidas a la ciudadanía y centros educativos que se desarrollarán durante la duración del contrato.

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 colectivos, territorios o franjas de edad, contribuyendo así a la mejora continua de la ciberresiliencia del conjunto de la sociedad navarra.

El adjudicatario proporcionará informes ejecutivos de impacto, con objeto de presentar los resultados de las actividades desarrolladas, realizar una evaluación continua de su efectividad y permitir ajustar las acciones conforme a los perfiles, canales y temáticas más relevantes.

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 0

DESCRIPCIÓN DEL SERVICIO del presente documento:

- **Coordinación, Gestión y Seguimiento del Servicio:** Asignación de un (1) perfil de coordinador y dinamizador. El perfil coordinador será el responsable de liderar la ejecución de las distintas acciones ligadas al proyecto, asegurando la planificación, el seguimiento y la correcta coordinación con todos los actores implicados, con el objetivo de garantizar el éxito de acciones como el despliegue eficaz de las campañas de sensibilización y la adecuada dinamización del portal web y las redes sociales.
Se encargará de la elaboración de informes e indicadores de impacto: Diseño de métricas de evaluación (KPIs) y seguimiento de resultados.
Se responsabilizará de la elaboración de informes ejecutivos sobre el alcance y efectividad de las campañas y materiales, con la periodicidad acordada.
- **Diseño, planificación y ejecución de Campañas de Sensibilización y Concienciación:** Asignación de al menos dos (2) perfiles técnicos especializados en ciberseguridad con la dedicación necesaria para desarrollar las distintas campañas de sensibilización y concienciación consensuadas para los diferentes colectivos.
Se encargarán del diseño, planificación y ejecución de las campañas presenciales y on-line dirigidas a diferentes colectivos. Estas deberán ser flexibles y adaptables a las necesidades identificadas por el NavCC junto al equipo técnico aportado por el adjudicatario. Deberán abordar diferentes temáticas en función de las necesidades analizadas en cada momento, ajustando su enfoque en función de los aprendizajes y métricas recogidas a lo largo de la ejecución del contrato.
- **Comunicación Digital, Creación de Contenidos y Gestión de Canales:** Asignación de los perfiles necesarios para garantizar la definición y ejecución de un plan de comunicación digital que incluya la generación de materiales originales de comunicación y contenidos audiovisuales dirigidos a los distintos públicos de la sociedad navarra, así como la dinamización del portal web y las redes institucionales del NavCC.
- **Gestión, mantenimiento y evolución del portal web del Navarra Cybersecurity Center (NavCC):** Asignación de los perfiles necesarios para proporcionar un servicio de gestión, mantenimiento y evolución integral del portal web del NavCC, que incluya el soporte y administración del portal, así como el mantenimiento preventivo, correctivo y evolutivo de acuerdo a los acuerdos de nivel de servicio (SLAs) definidos en este pliego.

3 DESCRIPCIÓN DEL SERVICIO Y EQUIPO DE TRABAJO

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 el NavCC, 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.

El Adjudicatario deberá contar con la totalidad de los medios humanos desde el primer día de inicio del proyecto. y deberá hacerse cargo de cuantos gastos por desplazamiento y dietas sean necesarios por parte del equipo técnico para la correcta ejecución de las acciones acordadas a lo largo de la duración de todo el 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 Coordinación, y seguimiento del servicio

El adjudicatario deberá garantizar la correcta coordinación, planificación, seguimiento y control global de la ejecución del contrato. Para ello deberá poner a disposición del servicio los siguientes perfiles:

- **Perfil de Coordinación del Servicio**

3.1.1 Perfil de Coordinación del Servicio

El **perfil de** Coordinador del Servicio deberá cumplir con las siguientes responsabilidades y funciones:

- **Responsabilidad general del servicio.** El coordinador será el encargado de garantizar una gestión y ejecución 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.

- **Punto de contacto único.** El coordinador actuará como punto de contacto permanente e interlocutor principal del servicio.
- **Presencialidad.** El adjudicatario garantizará la presencia física del coordinador en la sede del NavCC, sita en el Polo de Innovación Digital IRIS Navarra. cuando resulte necesaria para reuniones, campañas, eventos, coordinación y demás actuaciones que requieran presencialidad.
- **Coordinación técnica y operativa del proyecto.** El perfil de coordinación asumirá las siguientes responsabilidades:
 - Planificación de actividades y supervisión de la correcta ejecución del servicio, incluyendo la entrega en tiempo y forma de los materiales para su difusión en los distintos canales (web, redes sociales, medios, etc.).
 - Propuesta de medidas correctoras cuando sea necesario.
 - Coordinación con todas las partes implicadas, tanto internas como externas, incluyendo personal técnico del adjudicatario, personal técnico del NavCC, entidades colaboradoras, agentes institucionales y otros proveedores participantes en acciones complementarias promovidas por el NavCC.
 - Coordinación de la planificación de las campañas con el equipo del NavCC para garantizar una cobertura regular y equilibrada en el tiempo y en el territorio, evitando concentraciones de actividades en periodos reducidos o zonas concretas.
 - Coordinación de la ejecución de las campañas con el equipo técnico del adjudicatario: diseño global de las campañas, materiales, difusión, inscripciones, ejecución y evaluación en términos de participación, alcance e impacto.
- **Métricas de seguimiento del servicio.** El coordinador 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, asistencia, impresiones, encuestas de satisfacción, etc. Se deberán incluir, además, métricas de interacción con el portal web.
 - **Métricas cualitativas:** utilidad percibida, nivel de satisfacción, etc. Asimismo, se deberá 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:
 - **Informe Anual:** Al finalizar cada anualidad del contrato, se deberá entregar una memoria final que recoja de forma estructurada todos los resultados obtenidos, materiales producidos, estadísticas globales, lecciones aprendidas y

propuestas de mejora, junto con el material de todos los recursos generados durante la ejecución del servicio.

- **Informe por Campaña:** Tras la realización de cada una de las distintas campañas de concienciación, el adjudicatario presentará un (1) informe de impacto consolidado. Se presentarán regularmente lecciones aprendidas, así como distintas propuestas de continuidad en este tipo de iniciativas. Se incluirá además la entrega de los materiales desarrollados, repositorios organizados y estadísticas de uso.

3.2 Diseño, planificación y ejecución de campañas de sensibilización y concienciación

El adjudicatario se encargará del diseño, planificación y ejecución 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.

Para ello deberá poner a disposición del servicio los siguientes perfiles:

- **Perfil de Técnico Especialista en Ciberseguridad**
- **Perfil de Técnico en Ciberseguridad**

3.2.1 Estrategia de las Campañas de concienciación

A través de los perfiles anteriormente definidos, el adjudicatario deberá garantizar el diseño, planificación y ejecución de diferentes campañas de concienciación y sensibilización, asegurando que estas sean **flexibles y adaptables** a las necesidades identificadas por el NavCC y que evolucionen durante la ejecución del contrato en función de los resultados obtenidos y de las prioridades establecidas.

Las campañas irán destinados a los distintos públicos objetivo de la sociedad navarra, incluyendo, entre otros, ciudadanía, menores y jóvenes, personas mayores, entorno educativo, tejido empresarial —con especial atención a pymes y personas trabajadoras autónomas—, colectivos vulnerables y otros grupos que determine el NavCC durante la ejecución del contrato.

Las campañas estarán compuestas por un conjunto de sesiones presenciales y/o on-line, donde:

- **Sesiones presenciales:** A efectos de la presente licitación, se entiende por sesión el desarrollo de múltiples actividades a lo largo de un mismo día, en una misma ubicación física para un colectivo concreto. Estas sesiones podrán adoptar el

formato de charlas, talleres prácticos o dinámicas participativas adaptadas al público objetivo.

Las sesiones 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

El proceso de organización de las sesiones, reserva de espacios, difusión, inscripción etc. será gestionado por el adjudicatario. Los costes de reserva de espacios o de merchandising específicos no correrán a cargo del adjudicatario.

- **Sesiones on-line:** 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.

El adjudicatario garantizará que las campañas estén **adaptadas al nivel de madurez** en materia de ciberseguridad de los distintos públicos objetivo y coordinada a través de un análisis exhaustivo de sus necesidades.

En respuesta a la presente licitación, el adjudicatario deberá presentar una propuesta de **estrategia global de campañas de concienciación**, identificando los objetivos de concienciación perseguidos y cómo se alcanzan con las distintas campañas propuestas.

Esta estrategia no será estática, sino que se tomará como punto de partida y se irá adaptando y validando según las necesidades conforme avance la ejecución del proyecto en base al mutuo acuerdo entre el NavCC y el adjudicatario. Asimismo, todo el material generado en el contexto de la presente licitación será propiedad del NavCC

3.2.2 Perfil de Técnico Especialista en Ciberseguridad

El perfil de Técnico Especialista en Ciberseguridad debe ser un perfil con amplio bagaje, conocimientos técnicos, normativos y excelentes habilidades de comunicación. Este perfil deberá cumplir con las siguientes responsabilidades y funciones:

- **Responsabilidad de la ejecución de las campañas.** El técnico especialista será el encargado de garantizar la correcta ejecución de las campañas de concienciación y sensibilización, asegurando que estas sean **flexibles, adaptables** y que evolucionen durante la ejecución del contrato en función de los resultados obtenidos y de las prioridades establecidas.
- **Presencialidad.** El adjudicatario garantizará la presencia física de los técnicos de ciberseguridad en la sede del NavCC, sita en el Polo de Innovación Digital IRIS Navarra. cuando resulte necesaria para reuniones, campañas, eventos, coordinación y demás actuaciones que requieran presencialidad.

- **Diseño del plan general de campañas**, que contemple la segmentación del público destinatario, los objetivos de comunicación, los mensajes clave, las sesiones (presenciales y digitales), el cronograma y los formatos de los contenidos.
- **Diseño de las sesiones presenciales y on-line:** El técnico especialista (con el apoyo del técnico) será el encargado de diseñar la estructura, agenda y materiales de apoyo para las diferentes sesiones, de manera que se cumplan los objetivos marcados y se adapten a las necesidades de los diferentes públicos.
- **Elaboración de materiales de apoyo:** El técnico especialista (con el apoyo del técnico) se encargará de la elaboración de los materiales de apoyo necesarios para las sesiones presenciales y on-line que se planifiquen dentro de una campaña, tales como: presentaciones, infografías, gráficos, juegos, informes, etc.
- **Impartición de las sesiones presenciales y online:** El técnico especialista (junto con el técnico) se encargará de la impartición de las sesiones planificadas en las diferentes campañas. Para ello, el equipo técnico dispuesto deberá tener disponibilidad para desplazarse hasta las ubicaciones, dentro de la geografía navarra, donde vayan a celebrarse las sesiones presenciales. En el caso de las sesiones online, deberán asegurar que se realizan desde un lugar y con los medios adecuados para la grabación y emisión online de la sesión, garantizando una correcta visualización y sonido, que aseguren la calidad de la emisión. Por último, el equipo técnico deberá de poder garantizar la flexibilidad horaria necesaria para cumplir con los horarios que se hayan comprometido en el cronograma de las campañas.
- **Feedback y mejora continua:** el equipo técnico será el encargado de recoger el feedback de cada una de las sesiones impartidas (tanto presencial como online), que permita analizar y valorar la calidad e impacto de la misma, así como recoger y proponer propuestas de mejora continua que permitan la adecuación y evolución de las futuras sesiones.

3.2.3 Perfil de Técnico en Ciberseguridad

El perfil de Técnico en Ciberseguridad debe ser un perfil de apoyo al técnico especialista, con buenos conocimientos técnicos, normativos y habilidades de comunicación.

Este perfil deberá apoyar al Técnico Especialista en Ciberseguridad para cumplir con sus responsabilidades y funciones, tal y como se han definido en este pliego, siempre contando con la supervisión de este último. Se requiere, sin embargo, que tenga la capacidad suficiente como para poder impartir sesiones presenciales y on-line de forma autónoma.

3.3 Comunicación Digital, Creación de Contenidos y Gestión de Canales

El adjudicatario deberá prestar un servicio integral de comunicación digital asociado a las actuaciones del Navarra Cybersecurity Center (NavCC), que abarque tanto la **comunicación digital** como la **difusión y apoyo comunicativo de las actuaciones presenciales** desarrolladas en el marco del contrato.

El servicio comprenderá la planificación, creación, adaptación, publicación y difusión de contenidos y materiales de comunicación digital destinados a los distintos públicos objetivo de la sociedad navarra, tanto en el portal web como en redes sociales, con el objetivo de.

- Incrementar el alcance y notoriedad de las actuaciones de sensibilización y concienciación en ciberseguridad.
- Favorecer la participación de los públicos objetivo en campañas, sesiones, jornadas y demás actividades desarrolladas en el marco del servicio.
- Difundir conocimientos, recomendaciones, recursos y buenas prácticas en materia de ciberseguridad.
- Reforzar el posicionamiento del NavCC como iniciativa de referencia en materia de ciberseguridad en Navarra.
- Dar visibilidad a los servicios, recursos y contenidos disponibles a través del portal web del NavCC.
- Garantizar una comunicación coherente y coordinada entre las actuaciones digitales y presenciales desarrolladas durante la ejecución del contrato.

La planificación y ejecución de las actuaciones de comunicación se realizará en coordinación con el equipo del NavCC, con el equipo de Comunicación de NASERTIC y, cuando resulte necesario por la naturaleza de la actuación, con los responsables de comunicación institucional que NASERTIC determine.

Para ello el Adjudicatario deberá poner a disposición del servicio los siguientes perfiles:

- **Perfil de Responsable de Comunicación Digital y Gestión de Contenidos**
- **Perfil de Diseño Multimedia y Producción Audiovisual**

3.3.1 Estrategia de Comunicación Digital y materiales audiovisuales

A través de los perfiles anteriormente definidos, el adjudicatario deberá garantizar la definición y ejecución de un **plan de comunicación digital global**, vinculado a los objetivos del servicio y coordinado con la planificación general de campañas de concienciación y sensibilización.

Este plan deberá contemplar tanto los canales digitales del NavCC como las necesidades de difusión asociadas a campañas, jornadas, sesiones presenciales y on-line, eventos y demás actuaciones desarrolladas en el marco del contrato.

El plan deberá identificar, al menos:

- Públicos objetivo y segmentación de audiencias.
- Objetivos de comunicación.
- Líneas temáticas y mensajes clave.
- Canales y formatos propuestos.
- Planificación y frecuencia orientativa de las publicaciones.
- Actuaciones de difusión asociadas a campañas, jornadas y eventos.
- Criterios de adaptación de los mensajes a los diferentes colectivos.
- Indicadores que permitan evaluar el alcance, interacción y efectividad de las actuaciones de comunicación.

El adjudicatario deberá garantizar la generación de contenidos originales y materiales gráficos, multimedia y audiovisuales adaptados a los distintos públicos y canales.

Como mínimo, durante la ejecución del contrato se deberá contemplar la elaboración de contenidos de las siguientes tipologías:

- Vídeos y piezas audiovisuales de sensibilización y concienciación.
- Infografías, fichas, guías visuales y materiales divulgativos sobre buenas prácticas en materia de ciberseguridad.
- Contenidos interactivos o gamificados orientados a incrementar la participación y el alcance de las campañas.
- Podcasts u otros formatos de contenido sonoro.
- Boletines mensuales relacionados con la actualidad y las actuaciones de ciberseguridad de interés para los públicos objetivo.
- Noticias, recomendaciones y alertas de seguridad, con una frecuencia suficiente para mantener actualizados los canales de comunicación.
- Piezas y materiales específicos para la promoción, difusión y cobertura de campañas, sesiones, jornadas y eventos, tanto presenciales como on-line.
- Materiales susceptibles de utilización en soportes digitales o físicos cuando las necesidades de las actuaciones presenciales así lo requieran.

En respuesta a la presente licitación, el adjudicatario deberá presentar una propuesta de **estrategia global de comunicación digital y contenidos**, identificando los objetivos de concienciación perseguidos y cómo se alcanzan con los distintos contenidos propuestos.

La estrategia presentada por el adjudicatario constituirá el punto de partida del servicio y deberá evolucionar durante la ejecución del contrato en función de las prioridades establecidas por el NavCC, los resultados obtenidos, los indicadores de impacto, las necesidades detectadas y la evolución de los diferentes públicos objetivo.

Los contenidos y materiales deberán ser sometidos a los mecanismos de revisión y validación que establezca NASERTIC antes de su publicación o difusión. Ningún contenido que pueda considerarse comunicación institucional podrá publicarse o difundirse sin la correspondiente validación.

Todos los materiales específicamente desarrollados en ejecución del contrato, así como los correspondientes archivos fuente y versiones editables cuando proceda, serán entregados a NASERTIC en los términos establecidos en el presente Pliego.

3.3.2 Perfil de Responsable de Comunicación Digital y Gestión de Contenidos.

El perfil Responsable de Comunicación Digital y Gestión de Contenidos deberá cumplir con las siguientes responsabilidades y funciones:

- **Planificación y estrategia de comunicación:** El responsable de Comunicación Digital se encargará de definir y desarrollar un plan estratégico de comunicación para las redes sociales y portal web del NavCC, incluyendo:
 - Definición de las líneas temáticas, tipos de contenidos, formatos, canales y frecuencia de publicación.
 - Planificación y coordinación de la periodicidad de las publicaciones, asegurando su alineación con la estrategia de comunicación del NavCC y evitando periodos prolongados sin actualizaciones.
 - Coordinación con el equipo del NavCC para la validación de las líneas temáticas y contenidos antes de su publicación.
- **Creación, publicación y gestión de contenidos.** Corresponderá a este perfil la definición, publicación y gestión periódica de los contenidos de los distintos canales digitales, incluyendo:
 - Noticias breves, recomendaciones, materiales educativos, encuestas, mensajes de campañas, boletines, noticias y alertas de seguridad y demás contenidos necesarios.
 - Adaptación de los contenidos al canal, al público objetivo y a la actualidad, pudiendo incorporar hashtags temáticos y elementos visuales que refuercen la identidad del proyecto.
 - Gestión de la publicación de los materiales y contenidos en las redes sociales y portal web del NavCC.

- **Comunicación y difusión de campañas y actuaciones.** Coordinará la comunicación digital asociada a las campañas, jornadas, eventos y demás actuaciones desarrolladas en el marco del contrato, incluyendo:
 - Planificación de contenidos antes, durante y después de cada actuación.
 - Difusión de las actuaciones a través de los diferentes canales digitales con el objetivo de favorecer su visibilidad y alcance.
- **Coordinación de la producción de materiales.** Coordinará con el perfil de Diseño Multimedia y Producción Audiovisual la elaboración de los recursos gráficos, multimedia y audiovisuales necesarios para las campañas, jornadas y demás actuaciones de comunicación.
- **Seguimiento de resultados.** Realizará el seguimiento de los contenidos publicados y de los principales indicadores asociados a su alcance e impacto, proponiendo las adaptaciones que resulten necesarias.

3.3.3 Perfil de Diseño Multimedia y Producción Audiovisual

El perfil de Diseño Multimedia y Producción Audiovisual asumirá, entre otras, las siguientes funciones:

- **Diseño y producción de materiales.** El perfil de diseño multimedia será responsable de diseñar y producir los recursos gráficos, multimedia y audiovisuales necesarios de las campañas y actuaciones de comunicación y concienciación del NavCC, incluyendo:
 - Vídeos de concienciación y piezas audiovisuales.
 - Infografías y guías visuales sobre buenas prácticas en materia de ciberseguridad.
 - Retos y contenidos gamificados destinados a su difusión en redes sociales.
 - Podcasts y otros contenidos audiovisuales.
- **Adaptación de los materiales.** El perfil de diseñador deberá hacer accesibles y adaptará los contenidos a los diferentes canales, formatos, niveles de conocimiento y públicos destinatarios, desde público general hasta colectivos específicos como estudiantes, personas mayores o profesionales de diferentes sectores.
- **Calidad gráfica e identidad visual.** Garantizará la calidad gráfica y comunicativa de los contenidos y su coherencia con la identidad corporativa del NavCC, así como su correcta adaptación a los diferentes canales de difusión.
- **Producción y validación.** Será responsable de la propuesta de guion, diseño y producción de los materiales, coordinando su validación previa con el Responsable de Comunicación Digital y Gestión de Contenidos y con el equipo del NavCC.

- **Formatos y accesibilidad.** 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 cuando así lo requiera el NavCC. En particular, la elaboración de contenido audiovisual podrá ir acompañada de los subtítulos necesarios, cuando así lo requiera el NavCC, y los audios deberán acompañarse de una breve transcripción o resumen, de acuerdo con las necesidades de difusión y accesibilidad determinadas por el NavCC.

3.4 Gestión, mantenimiento y evolución del portal web del NavCC

El adjudicatario deberá garantizar la correcta gestión, mantenimiento y evolución del portal web del NavCC, como plataforma digital de referencia para la difusión de servicios, recursos, campañas, actividades y contenidos de sensibilización en materia de ciberseguridad dirigidos a la ciudadanía, el entorno educativo y el tejido empresarial navarro.

Para ello deberá poner a disposición del servicio los siguientes perfiles:

- **Perfil de Soporte y Administración del Portal Web.**
- **Perfil de Desarrollo y Mantenimiento Evolutivo del Portal Web.**

3.4.1 Portal Web del NavCC

A través de los perfiles anteriormente definidos, el adjudicatario proporcionará un servicio de gestión, mantenimiento y evolución integral del portal web del NavCC, que deberá prestarse de forma continuada durante todo el periodo de ejecución del contrato.

Actualmente, el portal web del NavCC se encuentra desarrollado sobre un sistema de gestión de contenidos (Drupal) e integra diferentes funcionalidades, entre ellas un agente conversacional basado en inteligencia artificial destinado a facilitar el acceso a la información y a los contenidos del portal. El código fuente es propiedad del NavCC y se pondrá a disposición del adjudicatario.

El servicio deberá incluir tres tipos de **mantenimiento** distintos (**preventivo**, **correctivo** y **evolutivo**), orientados a garantizar de forma proactiva el correcto funcionamiento del portal, así como a corregir defectos o fallos encontrados y promover la adecuada evolución del portal web en el tiempo.

- **Mantenimiento preventivo.** Se denomina mantenimiento preventivo al conjunto de actuaciones planificadas y periódicas destinadas a garantizar la estabilidad, disponibilidad, rendimiento, seguridad, accesibilidad y correcto funcionamiento de la página web, reduciendo la probabilidad de aparición de incidencias, vulnerabilidades o degradaciones del servicio.

Este servicio contempla todas aquellas acciones orientadas a anticipar posibles problemas técnicos, funcionales o de seguridad, así como a mantener actualizados y en condiciones óptimas los componentes que integran la solución web.

- **Mantenimiento correctivo.** Se denomina mantenimiento correctivo al conjunto de actuaciones destinadas a corregir incidencias, errores, defectos o fallos detectados en la página web, ya sea derivados de tareas de supervisión y mantenimiento preventivo, de comunicaciones realizadas por usuarios o de cualquier otro evento que afecte al correcto funcionamiento de la plataforma.

Este servicio incluirá la resolución de cualquier incidencia que pueda afectar a la disponibilidad, accesibilidad, integridad o correcto funcionamiento del portal, incluyendo, entre otras, errores funcionales, incidencias de integración, fallos de rendimiento, problemas de visualización, errores de contenido, incidencias de seguridad, fallos en formularios o servicios conectados.

Las actuaciones se mantendrán hasta el restablecimiento completo del servicio y la recuperación de las condiciones normales de funcionamiento de los componentes afectados.

- **Mantenimiento evolutivo.** Se denomina mantenimiento evolutivo al conjunto de actuaciones destinadas a adaptar, ampliar o mejorar la página web mediante la incorporación de nuevas funcionalidades, modificaciones de las existentes o adecuaciones derivadas de cambios tecnológicos, normativos, organizativos o estratégicos que afecten a la plataforma.

Este servicio contempla el análisis, diseño, desarrollo, configuración, integración, implantación y validación de mejoras o nuevas capacidades sobre la plataforma web, siempre que dichas actuaciones no constituyan una nueva licitación independiente ni supongan una transformación sustancial de la solución inicialmente contratada.

El servicio deberá cumplir con lo descrito en el apartado 8 ACUERDO DE NIVEL DE SERVICIO (SLA) – REQUISITOS SEGURIDAD PORTAL WEB.

El adjudicatario deberá generar un informe periódico que exponga todas las actividades de mantenimiento (**preventivo, correctivo y evolutivo**) realizadas. Estas acciones deberán estar ordenadas por fecha de ejecución y deberán plasmar de manera concisa el por qué de las mismas, así como los objetivos logrados con cada una de ellas. Asimismo, dichos informes deberán incorporar los indicadores y evidencias necesarios para acreditar el cumplimiento de los niveles de servicio (SLA) establecidos en el presente Pliego, incluyendo, cuando resulte de aplicación, los tiempos de respuesta y resolución de incidencias, la disponibilidad del servicio y cualquier otro indicador asociado a los SLA.

3.4.2 Perfil de Soporte y Administración del Portal Web.

El perfil de Soporte y Administración del Portal Web deberá garantizar la correcta administración y operativa diaria de la plataforma, asegurando su disponibilidad,

rendimiento, seguridad y correcto funcionamiento. Asimismo, será responsable de las actuaciones asociadas al mantenimiento preventivo y correctivo del portal.

Deberá cumplir con las siguientes responsabilidades y funciones:

- **Supervisión y mantenimiento operativo de la plataforma.** Deberá supervisar periódicamente el estado general del portal, sus componentes, integraciones y servicios asociados, así como monitorizar su rendimiento.
- **Actualización y seguridad del portal.**
 - Aplicar actualizaciones de seguridad, correcciones y nuevas versiones de los componentes software utilizados, siempre que resulten compatibles con la solución implantada, incluyendo CMS, base de datos, librerías de terceros y demás componentes asociados.
 - Revisar la seguridad del portal, identificando posibles vulnerabilidades y aplicando las medidas preventivas o correctivas necesarias para su mitigación.
- **Gestión y resolución de incidencias.**
 - Analizar y resolver las incidencias detectadas conforme a los niveles de servicio (SLA) establecidos.
 - Realizar las pruebas necesarias y verificar el restablecimiento de las condiciones normales de funcionamiento, rendimiento, seguridad y accesibilidad de la plataforma.
 - Documentar las incidencias, actuaciones realizadas y medidas adoptadas para evitar su repetición cuando proceda.
- **Seguimiento del servicio.**
 - Elaborar los informes periódicos correspondientes a las actuaciones de mantenimiento preventivo y correctivo realizadas.

3.4.3 Perfil de Desarrollo y Mantenimiento Evolutivo del Portal Web.

El perfil de Desarrollo y Mantenimiento Evolutivo del portal web será responsable de la evolución funcional del portal durante la vigencia del contrato, mediante el desarrollo, integración e implantación de mejoras y nuevas funcionalidades, incluyendo la evolución de los componentes y funcionalidades integrados en el portal, como el agente conversacional basado en inteligencia artificial, y asumirá, entre otras, las siguientes funciones:

- **Análisis, diseño y desarrollo de mejoras.** Analizar los requisitos y ejecutar las mejoras y nuevas funcionalidades solicitadas, evaluando previamente su impacto técnico y funcional y realizando su diseño, desarrollo e implantación.

- **Evolución funcional y tecnológica de la plataforma.** Se deberá evolucionar y optimizar la plataforma y sus integraciones, incluyendo procesos, navegación, experiencia de usuario y conexiones con sistemas, plataformas o servicios de terceros.
- **Gestión del agente conversacional basado en inteligencia artificial.** Se deberán realizar las actuaciones necesarias para la configuración, mantenimiento y evolución del agente conversacional y sus integraciones con el portal.
- **Validación y documentación de cambios.**
 - Realizar pruebas funcionales, técnicas, de seguridad y aceptación antes de la puesta en producción de los cambios.
 - Actualizar la documentación técnica y funcional asociada a las actuaciones realizadas.
 - Elaborar los informes periódicos correspondientes al mantenimiento evolutivo.

4 METODOLOGÍA Y PLAN DE TRABAJO

La empresa adjudicataria deberá proponer de manera clara la metodología a seguir durante el desarrollo del proyecto, cumpliendo los objetivos y características fijados en el presente pliego (0

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.

El adjudicatario 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

Para la correcta ejecución de los servicios descritos en los apartados anteriores, el adjudicatario deberá disponer de los perfiles profesionales descritos que son necesarios para garantizar la adecuada prestación de los trabajos objeto del contrato.

El Licitador deberá presentar en su oferta un organigrama del servicio en el que se especifiquen claramente los perfiles asociados a la ejecución del contrato, la cualificación y experiencia de sus integrantes.

Los profesionales responsables de la ejecución del contrato deberán disponer de la **cualificación y experiencia necesarias** para llevar a cabo de forma satisfactoria los trabajos planificados y alcanzar los objetivos establecidos. En particular, el equipo de trabajo deberá estar compuesto, como mínimo, por los siguientes perfiles, para los que se establecen las siguientes bolsas máximas de horas por anualidad completa de ejecución del contrato:

Perfil	Horas máximas anuales
Coordinador del Servicio	1.700 h
Técnico Especialista en Ciberseguridad	1.700 h
Técnico en Ciberseguridad	1.700 h
Responsable Comunicación Digital	720 h
Diseño Multimedia/Audiovisual	1.000 h
Soporte y Administración del Portal Web	300 h
Desarrollo y Mantenimiento Evolutivo del Portal Web	300 h
TOTAL	7.420 h

Las horas indicadas tienen la consideración de máximas para cada anualidad completa de ejecución del contrato y se consumirán en función de las necesidades efectivas del servicio y de los trabajos requeridos durante su ejecución. NASERTIC no estará obligada a consumir la totalidad de las horas previstas para cada perfil, siendo objeto de facturación únicamente las horas correspondientes a trabajos efectivamente realizados y debidamente acreditados.

Para periodos de ejecución inferiores a una anualidad completa, no resultará exigible el consumo proporcional de las bolsas de horas previstas, facturándose exclusivamente las horas correspondientes a los trabajos efectivamente realizados durante dicho periodo.

El adjudicatario deberá mantener durante la prestación de los servicios el personal comprometido en su oferta. En caso de bajas, ausencias o cualquier otra variación, deberá informar al NavCC y garantizar, cuando resulte necesaria su sustitución, la incorporación de profesionales con cualificación y experiencia equivalentes o superiores a las ofertadas.

Cuando existan causas objetivas relacionadas con la correcta ejecución del contrato, NASERTIC podrá requerir motivadamente a la empresa adjudicataria la sustitución de cualquiera de los profesionales adscritos al servicio, debiendo esta proceder a su sustitución por otro profesional con cualificación y experiencia equivalentes o superiores, sin coste adicional para NASERTIC. Los incumplimientos en la ejecución del contrato podrán dar lugar a la aplicación de las penalidades previstas en el Pliego de Cláusulas Administrativas Particulares.

El personal asignado al contrato dependerá exclusivamente de la empresa adjudicataria. En ningún supuesto podrá considerarse que existe relación laboral, contractual, funcional o de cualquier otra naturaleza entre dicho personal y NASERTIC, tanto durante la vigencia del contrato como a su finalización.

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.
- Como mecanismo ordinario de coordinación del servicio, se celebrará, como mínimo, **una reunión semanal de coordinación técnica y operativa** entre el Coordinador del Servicio y la Dirección de Proyecto de NASERTIC, así como **una reunión mensual de seguimiento del servicio** con el Equipo Director del Proyecto, en la que se revisará el grado de ejecución de los trabajos, los indicadores de seguimiento, las incidencias detectadas y la planificación de las actuaciones previstas. Sin perjuicio de ello, la Dirección de Proyecto podrá convocar cuantas reuniones adicionales considere oportunas para asegurar el cumplimiento del calendario del proyecto y la correcta consecución de los objetivos propuestos. El adjudicatario será responsable de la redacción y distribución de los informes de seguimiento y de 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, operación, mantenimiento, soporte y protección del 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 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 durante el mantenimiento y evolución del sistema.

8.3 GESTIÓN DE VULNERABILIDADES

El adjudicatario se compromete a detectar, notificar, analizar y corregir los fallos de seguridad identificados durante la ejecución del contrato, de acuerdo con los siguientes tiempos máximos de remediación:

Criticidad	Tiempo remediación
Crítica	≤ 24 horas (dentro del horario de soporte)
Alta	≤ 3 días (dentro del horario de soporte)
Media	≤ 7 días (dentro del horario de soporte)
Baja	≤ 15 días (dentro del horario de soporte)

A estos efectos, el tiempo de remediación se entenderá como el periodo comprendido entre la identificación y comunicación de la vulnerabilidad y la aplicación de una solución correctiva, mitigación o medida equivalente aceptada por NASERTIC.

Asimismo, deberán presentarse informes detallados que incluyan las vulnerabilidades detectadas, su criticidad, evolución y estado de corrección.

8.4 SOPORTE TÉCNICO DE ATENCIÓN A INCIDENCIAS

8.4.1 Cobertura del soporte

El adjudicatario deberá disponer de un servicio de soporte técnico para la atención, gestión y resolución de incidencias relacionadas con los servicios objeto del contrato.

El servicio de soporte deberá garantizar la correcta gestión de las incidencias desde su comunicación hasta su cierre, incluyendo su registro, clasificación, análisis seguimiento, resolución y documentación. La cobertura mínima exigida será la siguiente:

- **Horario estándar de soporte:** de lunes a viernes de 08:00 a 16:00 (en horario local)
- **Cobertura mínima para incidencias críticas:** atención en modalidad 8x5 dentro del horario estándar.

El adjudicatario deberá proporcionar y gestionar un sistema de Service Desk para la recepción, registro, seguimiento y gestión de incidencias, peticiones y consultas relacionadas con el servicio. Adicionalmente, se habilitará un canal de comunicación mediante correo electrónico.

8.4.2 Tiempos de atención y resolución de incidencias

A efectos del presente Pliego, se entenderá por tiempo de atención el tiempo transcurrido desde la comunicación o detección de una incidencia hasta que el adjudicatario registra la incidencia y comunica las primeras actuaciones realizadas o previstas. A efectos del presente Pliego, se entenderán los siguientes conceptos:

- **Tiempo de atención:** tiempo transcurrido desde la comunicación o detección de una incidencia hasta que el adjudicatario registra la incidencia, inicia su análisis y comunica las primeras actuaciones realizadas o previstas.

- **Tiempo de resolución:** tiempo transcurrido desde la comunicación o detección de una incidencia hasta la recuperación completa del servicio afectado o la aplicación de una solución definitiva o medida correctiva que permita restablecer las condiciones normales de funcionamiento.

Los tiempos máximos de atención exigidos serán los siguientes:

Nivel de incidencia	Tiempo de atención
Crítica	≤ 1 hora dentro del horario de soporte
Alta	≤ 4 horas dentro del horario de soporte
Media/Baja	≤ 1 día hábil

En aquellas incidencias en las que no sea posible aplicar una solución definitiva en un tiempo razonable, el adjudicatario deberá aplicar medidas de contingencia que permitan recuperar o mantener la operatividad del servicio, justificando las actuaciones realizadas y el plan previsto para la resolución definitiva.

8.5 INDICADORES DE NIVEL DE SERVICIO

Se establecen los siguientes indicadores clave que deberán cumplirse durante la ejecución del contrato:

- **Disponibilidad del portal web:** ≥ 99,5%.
- **Cumplimiento de los tiempos máximos de atención de incidencias:** ≥ 95%.
- **Cumplimiento de la aplicación de parches de seguridad dentro de los plazos establecidos:** ≥ 90%.
- **Ejecución correcta de copias de seguridad:** ≥ 99%.

8.6 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.

8.7 DOCUMENTACIÓN Y EVIDENCIAS REQUERIDAS

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.

El cumplimiento de los niveles de servicio tendrá carácter obligatorio durante toda la vigencia del contrato y deberá acreditarse mediante la información contenida en los informes periódicos de seguimiento, sin perjuicio de las comprobaciones que pueda realizar NASERTIC en cualquier momento.