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 EVALUACIÓN DE PRODUCTOS INDUSTRIALES CONECTADOS CONFORME AL CYBER RESILIENCE ACT (CRA) Y OTRAS NORMATIVAS SECTORIALES E INTERNACIONALES"

NOVIEMBRE 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 regirán la contratación de un **"Servicio de Evaluación de ciberseguridad de Productos Industriales Conectados conforme al Cyber Resilience Act y otras Normativas Sectoriales e Internacionales",** 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.

El servicio tendrá por finalidad:

- Facilitar la interpretación y correcta aplicación de los requisitos legales exigidos por el **Cyber Resilience Act (CRA)** y demás marcos regulatorios sectoriales e internacionales aplicables (ej. **IEC 62443, regulaciones médicas, automoción, etc.**).
- Prestar asistencia en la implantación de procedimientos internos y medidas que garanticen el cumplimiento normativo.
- Impulsar la capacitación y sensibilización del personal de las empresas para asegurar el cumplimiento continuado.
- Proporcionar servicios de evaluación, a través de herramientas, metodologías y entornos de laboratorio que favorezcan la verificación técnica, la mejora continua y la adaptación a cambios regulatorios futuros.

El servicio se dirigirá a **empresas de Navarra**, y tendrá como finalidad reforzar la **competitividad**, el **cumplimiento normativo** y la **ciberresiliencia** en la **Comunidad Foral de Navarra**.

2.2 Objetivos

El principal objetivo de la contratación de un **"Servicio de Evaluación de Ciberseguridad de Productos Industriales Conectados conforme al Cyber Resilience Act y otras Normativas Sectoriales e Internacionales"** es poner a disposición del tejido empresarial navarro un servicio integral que facilite el cumplimiento y la evaluación en materia de ciberseguridad, elevando de esta manera el nivel de madurez técnica y normativa en las empresas de la Comunidad Foral de Navarra.

La **Ley de Ciberresiliencia (CRA)** establece obligaciones de ciberseguridad para todos los productos con componentes digitales, imponiendo a fabricantes y distribuidores la responsabilidad de garantizar su seguridad durante todo el ciclo de vida de sus productos. Este reglamento europeo introduce obligaciones en planificación, diseño, desarrollo, mantenimiento y actualización, afectando a todos los productos conectados directa o indirectamente a redes, salvo exclusiones específicas. A partir del **11 de diciembre de 2027**, estas obligaciones serán exigibles en la Unión Europea.

El objetivo principal es proteger a consumidores y empresas frente a productos inseguros o sin actualizaciones adecuadas, facilitando la identificación y uso de hardware y software con garantías de ciberseguridad. Los productos deberán contar con marcado CE, lo que reequilibra la responsabilidad hacia los fabricantes y permitirá decisiones de compra más seguras y transparentes en el mercado europeo.

Junto al CRA, cobran relevancia otros marcos como la **serie IEC 62443** para la ciberseguridad industrial y normativas sectoriales específicas (salud, automoción, aeronáutica, entre otros), que imponen requisitos adicionales de evaluación y certificación. El servicio objeto de este pliego está diseñado para dar cobertura a estas exigencias, ayudando a las empresas navarras a integrar la ciberseguridad desde la concepción del producto hasta su puesta en el mercado.

Este contexto normativo constituye asimismo una **oportunidad estratégica** para el tejido empresarial navarro, en la medida en que impulsa la innovación orientada al desarrollo de productos conectados más seguros y contribuye a reforzar la competitividad de las empresas, favoreciendo su adaptación a los requisitos de los mercados nacionales e internacionales.

En este contexto, los objetivos concretos del servicio son los siguientes:

1. **Facilitar el cumplimiento normativo** de las empresas navarras en relación con el **Cyber Resilience Act (CRA)** y otras regulaciones sectoriales e internacionales, a través de un servicio especializado de asesoría, evaluación y acompañamiento técnico.

2. **Impulsar la competitividad y la ciberresiliencia** del tejido empresarial de Navarra, promoviendo la adopción de prácticas de seguridad digital alineadas con la normativa europea, estatal y autonómica en materia de ciberseguridad.

3. **Reducir riesgos legales, técnicos y económicos** derivados del incumplimiento normativo y de fallos de seguridad, aportando seguridad jurídica, confianza de mercado y protección reputacional a las empresas participantes.

2.3 Alcance

El alcance de la presente contratación comprende los siguientes aspectos y se estructurará en dos bloques complementarios, cuyos requisitos técnicos se detallan en el punto 3 DESCRIPCIÓN DEL SERVICIO.

- **Servicio Fijo** cuya prestación será continua durante toda la vigencia del contrato:

    - Destinado a las tareas de oficina técnica que incluyen la gestión y coordinación del servicio, el asesoramiento técnico especializado, la formación y sensibilización, el seguimiento normativo y la elaboración de informes de reporting ejecutivo para el NavCC. Dentro de este bloque se elaborará, además, un informe de estimación del impacto del CRA en el tejido empresarial navarro, identificando los sectores, empresas y productos más afectados por la normativa.

- **Servicio Variable** de evaluación técnica de productos industriales conectados conforme al Cyber Resilience Act (CRA) y otras normativas sectoriales e internacionales:

    - Incluye la realización de evaluaciones y auditorías de ciberseguridad sobre productos industriales conectados, aplicando pruebas técnicas específicas y emitiendo los correspondientes informes de resultados.

    - La ejecución de los trabajos asociados al Servicio Variable se organizará a través de una bolsa de horas que actuará como mecanismo de referencia para planificar y controlar las distintas evaluaciones que se desarrollen a lo largo del contrato. La adjudicataria deberá presentar, antes de cada evaluación, una estimación previa de las horas necesarias, que será revisada y validada por el Navarra Cybersecurity Center (NavCC). Una vez finalizada la evaluación, se ajustará el consumo real, garantizando en todo momento la trazabilidad y la transparencia en el uso de los recursos pertinentes. Todas las horas deberán integrar, de manera global, los recursos técnicos, humanos y materiales necesarios para la prestación del servicio.

Este esquema permitirá ofrecer un servicio integral que combine el acompañamiento permanente con la ejecución de evaluaciones prácticas, garantizando a las empresas navarras el cumplimiento del CRA y de otras normativas sectoriales e internacionales de referencia.

La oferta presentada por la empresa adjudicataria deberá contemplar la totalidad de los costes asociados a la prestación del servicio, incluyendo gastos generales, financieros, de transporte, dietas, desplazamientos, seguros, herramientas, licencias, así como los derivados del personal técnico y cualquier otro concepto necesario para la correcta ejecución del contrato. Asimismo, el NavCC será el responsable de validar las empresas y productos que participarán en el proceso, validar las estimaciones de horas a invertir en cada evaluación, así como en cualquier otro aspecto técnico.

En todo caso, las empresas cuyos productos sean objeto de evaluación de ciberseguridad, a consecuencia de la prestación del servicio licitado, deberán disponer de su domicilio fiscal en Navarra.

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

- **FASE 0: Puesta en marcha (Oficina Técnica y Preparación del Servicio)**

    Esta fase incluye el establecimiento de la Oficina Técnica y definición de procedimientos operativos con la correspondiente validación inicial de los trabajos por parte del NavCC. Durante esta fase se elaborará el **"Informe de estimación del impacto del CRA en el tejido empresarial navarro"**, que identificará los sectores y empresas más afectados y servirá de base para orientar el servicio. Esta fase deberá quedar completada tras el primer mes del inicio del servicio.

- **FASE 1: Prestación del Servicio Fijo (continuo durante toda la vigencia del contrato)**

  En esta fase se incluirá el desarrollo de las actividades recurrentes de asesoramiento, formación, sensibilización, seguimiento y reporting ejecutivo al NavCC. Se prestará de manera continua durante toda la vigencia del contrato.

- **FASE 2: Ejecución del Servicio Variable (evaluaciones de productos industriales conectados)**

  En esta fase se desarrollarán las evaluaciones de seguridad solicitadas según la metodología aprobada. Asimismo, se ejecutarán las pruebas técnicas necesarias con sus respectivos análisis de resultados y, elaboración de informes específicos para cada caso. Esta fase se desarrollará en paralelo al Servicio Fijo hasta la finalización del contrato.

- **FASE 3: Cierre del Proyecto y Entrega de Resultados Finales**

  Esta fase incluirá la presentación de un informe ejecutivo global, con resultados consolidados, conclusiones y comparativas sectoriales anonimizadas. Adicionalmente, se realizará una validación de todos los entregables previstos por parte del NavCC.

  Esta fase deberá quedar entregada y aprobada antes del **31 de mayo de 2026**.

3 DESCRIPCIÓN DEL SERVICIO

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

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

El adjudicatario deberá aportar y describir en su oferta las funcionalidades del servicio a prestar, que consistirá en un **acompañamiento integral a las empresas de Navarra para el cumplimiento de la normativa CRA y otras normativas sectoriales e internacionales**, combinando asesoramiento técnico, apoyo operativo, capacitación práctica y evaluación técnica especializada.

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

Para la adecuada prestación del servicio, la adjudicataria pondrá a disposición de las empresas un equipo especializado que actuará como punto de referencia en materia de CRA y otras normativas sectoriales e internacionales, proporcionando asistencia a lo largo de todo el ciclo de desarrollo del servicio.

La prestación del servicio se articulará en torno a las siguientes líneas de actuación principales:

- **Proporcionar a las empresas navarras un entorno de asesoramiento técnico y metodológico,** que actúe como punto de referencia durante toda la vigencia del contrato. Este soporte permitirá la interpretación y conocimiento de la normativa, resolución de dudas y poner a disposición del tejido empresarial navarro criterios técnicos para orientar sus decisiones, garantizando una base para su adaptación regulatoria.

- **Ofrecer la posibilidad de someter productos industriales conectados a evaluaciones técnicas conforme al Cyber Resilience Act (CRA) y otras normativas sectoriales e internacionales** aplicables. De este modo, las empresas podrán conocer el estado de sus productos conectados y recibir orientación práctica para implementar mejoras, asegurando que sus soluciones cumplen con los requisitos normativos y de mercado.

- **Favorecer la generación de capacidades internas en las empresas navarras**, a través de acciones de formación, sensibilización y transferencia de conocimiento adaptadas a distintos perfiles profesionales. El objetivo es dotar al tejido

empresarial de los recursos y competencias necesarios para integrar la ciberseguridad en sus procesos y consolidar una cultura organizacional orientada a la seguridad.

- **Garantizar un seguimiento, control y actualización normativa**. Mediante la elaboración de análisis específicos que anticipen las consecuencias regulatorias en sectores y productos, el servicio permitirá mantener una visión actualizada del marco normativo aplicable. Además, se generarán informes periódicos de seguimiento y de resultados, que recogerán tanto el grado de avance alcanzado por las empresas en sus procesos de adaptación como la identificación de riesgos y oportunidades derivados de las exigencias normativas aplicables.

De esta forma, la prestación del servicio combinará una dimensión **estratégica** (alineación normativa), una dimensión **operativa** (apoyo práctico en la implantación de medidas e informes) y una dimensión **formativa** (generación de capacidades internas en las empresas), garantizando un impacto duradero más allá de la finalización del contrato.

3.1 Servicio Fijo

El **Servicio Fijo** se prestará de manera continua durante toda la vigencia del contrato y tendrá un alcance de **carácter global**, dirigido al conjunto del tejido empresarial navarro, con independencia de que una empresa participe o no en las evaluaciones de productos industriales conectados previstas en el Servicio Variable. Su finalidad es garantizar que todas las organizaciones dispongan de un marco de referencia en materia de impacto regulatorio y cumplimiento normativo, con acceso a asesoramiento técnico, formación, acciones de sensibilización y seguimiento continuo de la normativa aplicable a los diferentes productos industriales conectados.

En particular, el objetivo principal del Servicio Fijo es asegurar que las empresas navarras cuenten en todo momento con el respaldo necesario para comprender, interpretar y aplicar las exigencias del **Cyber Resilience Act (CRA)** y de otras normativas sectoriales de referencia.

Este bloque se materializa a través de la **Oficina Técnica**, concebida como punto de referencia y coordinación del proyecto, que asumirá tanto funciones de gestión y supervisión como de dinamización, formación y asesoramiento. De igual forma, la Oficina Técnica tendrá la responsabilidad de coordinar las actividades vinculadas al **Servicio Variable**, asegurando que la ejecución de evaluaciones de productos se lleve a cabo de manera coherente con los plazos, procedimientos y estándares establecidos.

En el marco del Servicio Fijo, el adjudicatario llevará a cabo las siguientes líneas de trabajo:

- **Gestión y coordinación del servicio:** la adjudicataria será responsable de la planificación, organización y control del servicio, supervisando la calidad de los trabajos y garantizando la correcta articulación entre el bloque fijo y el bloque variable. La figura del responsable del servicio actuará como enlace con la Dirección Técnica de NASERTIC y velará por la adecuada prestación en tiempo y forma de todas las actividades previstas.

- **Difusión y promoción de acciones de certificación:** se desarrollarán actividades de dinamización y promoción orientadas a dar visibilidad a la certificación de productos industriales conectados, de acuerdo con las normativas CRA, IEC 62443 y otros estándares aplicables. Estas acciones tendrán también como finalidad extender el alcance del proyecto a distintos ámbitos de interés en Navarra, favoreciendo que el tejido empresarial conozca dichas normativas y estándares.

- **Informe de estimación del impacto del CRA en el tejido empresarial navarro:** se elaborará un documento específico que identifique los sectores, tipologías de empresas y categorías de productos que se verán más afectados por la normativa, cuantificando en la medida de lo posible el esfuerzo de adaptación requerido. Este informe será un entregable clave en las fases iniciales del proyecto y servirá de base para orientar las actuaciones posteriores.

- **Exploración del entorno de evaluación y agentes relevantes:** se analizará el ecosistema de evaluación de ciberseguridad de producto industrial en Navarra, identificando casos de uso y organizaciones de especial interés. Al mismo tiempo, se fomentará la relación con centros de I+D, asociaciones empresariales y otros agentes expertos que puedan formar parte del ecosistema de soporte, garantizando así una respuesta integral a las necesidades que surjan durante la ejecución del servicio.

- **Asesoramiento técnico especializado y continuo:** la Oficina Técnica proporcionará soporte constante en la interpretación y aplicación del CRA y de otras normativas relevantes, resolviendo consultas técnicas, regulatorias y metodológicas. Se trata de asegurar que las empresas dispongan en todo momento de criterios homogéneos de aplicación y de orientación práctica para cumplir con los requisitos normativos.

- **Acompañamiento en la implantación de medidas de cumplimiento:** se elaborarán guías, protocolos y plantillas adaptadas al perfil de cada sector industrial, con el fin de facilitar la integración de requisitos de ciberseguridad en los procesos de diseño, desarrollo, mantenimiento y actualización de productos. Además, se prestará apoyo directo a las empresas en la aplicación práctica de dichas medidas.

- **Apoyo en la elaboración y validación de informes normativos:** la adjudicataria asistirá a las empresas en la preparación, revisión y validación de la documentación exigida por el CRA y por otras regulaciones sectoriales, garantizando su adecuación a los estándares requeridos. Para ello, se proporcionarán modelos normalizados y plantillas que simplifiquen el trabajo de las organizaciones beneficiarias.

- **Formación y sensibilización:** se pondrán en marcha programas de formación y talleres prácticos, tanto presenciales como en formato remoto, dirigidos a distintos perfiles profesionales dentro de las empresas. El objetivo será generar conocimiento interno y fomentar una cultura organizacional que incorpore la ciberseguridad como un elemento esencial y sostenible en el tiempo. En particular, la adjudicataria

deberá impartir un mínimo de **6 talleres presenciales de formación** durante la vigencia del contrato, con una **duración mínima de, al menos, 3 horas cada uno** de ellos y dirigidos a empresas navarras y orientados al conocimiento de la normativa relativa a la certificación de productos industriales conectados.

- **Seguimiento, control y reporting ejecutivo:** se definirán indicadores de cumplimiento y madurez que permitan monitorizar el avance de las empresas beneficiarias. Asimismo, se elaborarán informes periódicos con una visión global y sectorial anonimizada, que serán presentados al NavCC para su validación. Estas actividades de seguimiento garantizarán la trazabilidad del proyecto y permitirán introducir ajustes cuando sea necesario.

- **Actualización normativa y comunicación de cambios:** la adjudicataria se encargará de monitorizar de forma continua los cambios en la normativa europea, estatal y sectorial, emitiendo alertas y boletines informativos que aseguren que las empresas disponen siempre de información actualizada. Junto a la comunicación, se ofrecerán recomendaciones prácticas que faciliten una rápida adaptación a las nuevas exigencias regulatorias.

En conjunto, el **Servicio Fijo** constituye un marco integral de gestión, dinamización y apoyo a las empresas navarras, asegurando que cuentan con el respaldo técnico, organizativo y formativo necesario para avanzar en el cumplimiento de las obligaciones derivadas del CRA y de otras normativas internacionales y sectoriales en materia de ciberseguridad.

3.2 Servicio Variable

El **Servicio Variable** incluye la realización de evaluaciones técnicas de ciberseguridad sobre productos industriales conectados. Su finalidad es ofrecer a las empresas navarras la posibilidad de someter sus productos a pruebas de seguridad avanzadas, en coherencia con los requisitos establecidos por el **Cyber Resilience Act (CRA)**, la norma **IEC 62443** y otras regulaciones internacionales o sectoriales que resulten aplicables. De este modo, se asegura tanto la verificación técnica como la preparación de evidencias necesarias para procesos de certificación.

Cada evaluación se desarrollará en coordinación con el **Navarra Cybersecurity Center (NavCC)**, que validará junto con la adjudicataria los productos candidatos a ser evaluados. Para cada caso, se tendrán en cuenta las particularidades del sector correspondiente y se aplicarán los marcos normativos que resulten exigibles.

El adjudicatario deberá ofrecer, como mínimo, las siguientes líneas de actuación:

- **Evaluación de la seguridad de productos industriales conectados**, verificando el cumplimiento de los requisitos aplicables.

- **Auditorías de componentes y dispositivos industriales**, que incluyan la revisión de hardware, firmware y protocolos de comunicación.

- **Análisis y gestión de vulnerabilidades**, con identificación de riesgos y propuesta de medidas correctivas.
- **Acompañamiento a la certificación**.

Las pruebas deberán llevarse a cabo en laboratorios especializados que cuenten con herramientas adecuadas para la evaluación de la ciberseguridad industrial, incluyendo como mínimo:

- Plataformas para test de penetración en aplicaciones web.
- Herramientas para el testeo de protocolos de comunicación.
- Herramientas específicas para protocolos de comunicación industrial.

El coste de todo el equipamiento y de las licencias de software o hardware necesarias será asumido íntegramente por la adjudicataria.

Asimismo, en cada evaluación se deberán ejecutar, como mínimo, las siguientes pruebas:

1. **Verificación de los requisitos de seguridad** del producto bajo análisis.
2. **Test de mitigación de amenazas**, comprobando la eficacia de las medidas implementadas.
3. **Test de vulnerabilidades**, que incluirá:
    - Escaneo de puertos.
    - Escaneo de vulnerabilidades de red.
    - Ejercicios de fuzzing.
    - Pruebas de estrés en red.
4. **Test de penetración**, mediante simulaciones de ataques controlados.
5. **Revisión de independencia de los evaluadores**, asegurando objetividad y fiabilidad de los resultados.

La propuesta de la adjudicataria deberá detallar la metodología que se aplicará en las evaluaciones, así como el plan de trabajo asociado a cada producto, indicando fases, pruebas, recursos y plazos de ejecución. El servicio dará lugar, al menos, a los siguientes entregables:

- **Definición inicial de los trabajos de la Oficina Técnica:** Documento en el que se especificarán de forma detallada las funciones, procedimientos y responsabilidades de la oficina técnica en el marco del servicio. Este entregable debe ser validado y revisado por el NavCC antes de continuar con la ejecución del servicio.

- **Servicio de preparación y acompañamiento a la evaluación:** acciones iniciales dirigidas a orientar a las empresas participantes en la comprensión del proceso de evaluación.
- **Documentación del entorno de evaluación:** Elaboración de un informe que describa el alcance y escenario de pruebas, los recursos empleados, la configuración utilizada y las condiciones en las que se llevará a cabo la evaluación.
- **Parámetros de operación consensuados:** Acuerdo con cada empresa evaluada sobre los parámetros de funcionamiento del producto en el entorno de pruebas con el fin de garantizar la validez y representatividad de los resultados obtenidos.
- **Selección y diseño de pruebas:** Documento que refleje las pruebas que se realizarán en la evaluación, adaptando la metodología propuesta a las características del producto y a la normativa aplicable en cada caso.
- **Informe de resultados de pruebas**, con evidencias obtenidas, vulnerabilidades detectadas y conclusiones técnicas.
- **Informe técnico de evaluación completa**, con valoración global del cumplimiento normativo.
- **Servicio de apoyo a la remediación**, acompañando a las empresas en la implantación de las mejoras propuestas en los planes de remediación.

La ejecución de los trabajos asociados al **Servicio Variable** se gestionará mediante una **bolsa de horas** que permitirá atender las distintas evaluaciones de productos industriales conectados durante la vigencia del contrato. Esta bolsa constituirá el mecanismo de referencia para ejecutar los trabajos, asegurando en todo momento la trazabilidad de los consumos y la validación de los mismos por parte del Navarra Cybersecurity Center (NavCC).

En particular, el funcionamiento de dicha bolsa será el siguiente:

- **Estimación previa:** antes de iniciar cada evaluación, la adjudicataria elaborará una estimación de las horas necesarias, que deberá ser validada por el NavCC.
- **Consumo real:** una vez realizada la evaluación, se registrará el consumo real de horas.
- **Desviaciones relevantes:** si durante la ejecución se prevé una desviación significativa respecto a la planificación inicial, será obligatorio obtener la aprobación expresa del NavCC antes de continuar con el trabajo.
- **Control y trazabilidad:** la adjudicataria deberá documentar de forma transparente las horas dedicadas a cada tarea y facilitar al NavCC los informes de seguimiento necesarios para validar el consumo de horas.
- **Recursos incluidos:** todas las horas consumidas deberán contemplar, de forma integrada, los recursos técnicos, humanos, de equipamiento y software necesarios para la correcta realización de las tareas descritas en el servicio.

4 METODOLOGÍA Y PLAN DE TRABAJO

La empresa licitadora deberá proponer de manera clara la metodología a seguir durante el desarrollo del proyecto, cumpliendo los objetivos y características fijados en el presente pliego (3 DESCRIPCIÓN DEL SERVICIO). En la metodología la empresa licitadora deberá detallar la forma en la que abordará cada uno de los servicios definidos para el proyecto. El nivel de detalle aportado será el necesario para expresar que el método propuesto permitirá alcanzar los objetivos fijados.

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

5 EQUIPO DE TRABAJO

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

- **Gestor del Proyecto**: punto único de contacto para el control de la operativa del servicio con el Navarra Cybersecurity Center (NavCC). Será responsable de la coordinación global del contrato, de la supervisión de la calidad de los trabajos y de la integración entre el Servicio Fijo y el Servicio Variable. Deberá contar con una formación superior y una experiencia mínima de tres (3) años en la gestión de proyectos de naturaleza similar al del presente servicio.

- **Equipo Servicio Fijo:** encargado de proporcionar servicios de asesoramiento, dinamización, acompañamiento y formación a empresas, así como de elaborar el reporting y la coordinación técnica con el Navarra Cybersecurity Center (NavCC). El personal asignado al Servicio Fijo deberá contar con una experiencia mínima acreditada de dos (2) años en la gestión de proyectos tecnológicos, actividades de normalización técnica o coordinación de iniciativas de carácter formativo.

- **Equipo Servicio Variable**: encargados de ejecutar las evaluaciones técnicas de productos industriales conectados, incluyendo análisis, pruebas técnicas y, de la ejecución relativa al servicio variable. Deberán contar con, al menos, dos años de experiencia como técnicos/as de pruebas en proyectos similares al objeto del contrato. Deberán ser proyectos en los que se hayan llevado a cabo, con empresas, servicios de evaluación de ciberseguridad de productos industriales y, que, como consecuencia, tengan experiencia en el uso de las herramientas de laboratorio necesarias para la ejecución del servicio.

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.