

Número de expediente: 2024032 Armonizado

Objeto de la contratación: Acuerdo Marco para la prestación de servicios de simulacros de incidentes de Ciberseguridad en el marco del Plan de Recuperación, Transformación y Resiliencia
- Financiado por la Unión Europea – NextGenerationEU

Documento: Pliego de prescripciones técnicas.

1. INTRODUCCIÓN

La “Estrategia para la Transformación Digital de Euskadi 2025” es la herramienta básica del Gobierno Vasco para impulsar la transformación digital de Euskadi, y fue aprobada por el Consejo de Gobierno en fecha 30 de marzo de 2021.

Dicha estrategia, liderada por el Departamento de Industria, Transición Energética y Sostenibilidad del Gobierno Vasco, acompañará con un apoyo sinérgico, proactivo y coordinado de todos los agentes involucrados, el reto que impone un nuevo modelo de transformación digital.

Las tecnologías digitales están destinadas a impulsar el crecimiento presente y futuro de todas las organizaciones, así como a aumentar la demanda de nuevas funciones, conjuntos de aptitudes y perfiles laborales. Las empresas esperan reestructurar su fuerza de trabajo en respuesta a la creciente automatización, reduciendo los perfiles más tradicionales y sustituyéndolos por otros más tecnológicos o ampliando la subcontratación para trabajos especializados.

La ETDE2025 se estructura en tres dimensiones que permiten definir los elementos sobre los que el Gobierno Vasco ha puesto su foco y sus prioridades durante el periodo de vigencia de la Estrategia. Estas dimensiones son las **palancas tecnológicas**, los **habilitadores de apoyo** y los **ámbitos de aplicación**. Estas tres dimensiones no actúan de forma aislada sino como un sistema y debe contemplarse desde la perspectiva de la generación de valor para Euskadi. A partir de ahí, la selección de las palancas tecnológicas se ha llevado a cabo teniendo en cuenta el papel disruptivo que están llamadas a tener a corto, medio y largo plazo en los retos que se plantean en las tres transiciones. Los habilitadores se conforman como los medios, canales o capacidades que favorecen y aceleran el despliegue de las tecnologías digitales.

Una de estas “palancas tecnológicas” identificadas es la “CIBERSEGURIDAD Y CONFIANZA DIGITAL”.



La ciberseguridad agrupa un conjunto de medidas y actuaciones asociadas a proteger redes, dispositivos, programas y datos de ataques, daños o accesos no autorizados. El impulso y desarrollo de la digitalización de la actividad productiva, y en particular el incremento exponencial de dispositivos conectados a la red, así como la creciente sofisticación de las tecnologías de la información y las comunicaciones hacen necesario incidir en la seguridad digital de las empresas mejorando las herramientas de protección.

La ciberseguridad es una práctica consolidada en el desarrollo de aplicaciones y sistemas informáticos y se ha incorporado como una función esencial dentro de las propias empresas

usuarias. Por ello, surgen nuevas tendencias que tienen un amplio impacto en la industria y un potencial significativo de disrupción tal y como se detalla a continuación:

- Nuevas soluciones de detección y respuestas extendidas, que mejoran la detección de amenazas y proporcionan una mayor capacidad de respuesta a incidentes.
- Automatización de los procesos de seguridad.
- Nuevas responsabilidades de seguridad a través del uso de la IA.
- Surgió la figura Chief Security Officer, CSO, persona encargada de la seguridad de la organización, física y tecnológica.
- Mayor importancia de la privacidad en las organizaciones.
- Equipos de confianza y seguridad digitales para garantizar la integridad en todas las interacciones con clientes y proveedores.
- Servicios de seguridad en la nube cada vez más populares.
- Misma protección para todo el ciclo de vida de la organización, pero teniendo en cuenta los requisitos de las aplicaciones nativas de la nube o cloud native apps.
- Las VPN o Redes Privadas Virtuales, comienzan a ser reemplazadas por redes de confianza cero, Zero Trust, en las cuales es necesaria una estricta verificación de identidad, independientemente de su ubicación, y tanto si se trata de personas como de dispositivos.

Los problemas o retos asociados a la ciberseguridad están en constante cambio ya que los ciberataques aumentan en volumen y complejidad, por lo que la capacidad de la ciberseguridad y los desarrollos evolucionan en la misma medida. El desarrollo, uso o la aparición de otras tecnologías presenta oportunidades y retos para la ciberseguridad. Por un lado, la IA, que contribuye al aumento de la rapidez en la respuesta, y a una mejor detección de las anomalías que permiten detectar y bloquear automáticamente los ciberataques. Por otra parte, la computación cuántica trae nuevos retos asociados a la criptografía cuántica que busca reducir las vulnerabilidades ante ataques que también utilicen esta tecnología. La llamada ciberseguridad cuántica plantea medidas como la distribución de claves cuánticas, los algoritmos de seguridad cuántica y los generadores de números aleatorios cuánticos. Del mismo modo, la ciberseguridad resulta fundamental para la interoperabilidad de los sistemas de información o los Centros de Procesamiento de Datos, CPD, debido al almacenamiento e intercambio de datos sensibles.

Finalmente, las capacidades de la ciberseguridad se están adaptando a las redes 5G, que se están convirtiendo en la espina dorsal de muchas aplicaciones cruciales como el vehículo autónomo, por lo que la integridad y la disponibilidad de estas redes tiene importantes puntos de vulnerabilidad.

En todo este contexto, se hace necesario que las empresas estén entrenadas para gestionar los incidentes de ciberseguridad que puedan sufrir. Se vislumbra que en este ámbito las empresas se pueden clasificar en una doble tipología. Las que ya han sufrido un incidente de ciberseguridad, y las que los van a sufrir.

El proyecto actual consiste en realizar un “Simulacro de incidentes de Ciberseguridad”, en entorno controlado, y que esto nos permita identificar los puntos débiles que tenga la empresa para posteriormente tomar decisiones para reducir la vulnerabilidad de nuestros sistemas y equipos. Estas decisiones no eliminarán las posibilidades de sufrir un incidente de ciberseguridad, pero es seguro que nos servirán para mitigar sustancialmente los daños que estos incidentes puedan causar a nuestra empresa.

Este servicio está enmarcado dentro del CONVENIO DE COLABORACIÓN EN EL ÁMBITO DE LA CONVOCATORIA RETECH (REDES TERRITORIALES DE ESPECIALIZACIÓN TECNOLÓGICA) DE LA SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL formalizado en noviembre del 2023 entre otros por SPRI-AGENCIA VASCA DE DESARROLLO EMPRESARIAL e INCIBE (S.M.E. INSTITUTO NACIONAL DE CIBERSEGURIDAD DE ESPAÑA M.P., S.A.)

Los objetivos estratégicos que se marcaron dentro el proyecto presentado por el Gobierno Vasco a esta convocatoria, y denominado PROYECTO RED-ARGOS, son, entre otros, los siguientes:

- Fortalecer la industria de ciberseguridad con un ecosistema de innovación público-privado a través del desarrollo de actividades de I+D+i para la experimentación y la generación de una red de infraestructuras lógicas o físicas de conocimiento distribuido que ofrezca complementariedad, la transferencia a empresas, la especialización tecnológica, la llegada al mercado de soluciones y la creación de productos en toda la cadena de valor.
- Mejorar la permeabilidad de la ciberseguridad a todos los sectores económicos, para así aumentar su adopción global.
- Promover, hacer crecer y consolidar la colaboración interregional, apoyándose en las fortalezas de cada comunidad autónoma participante en la propuesta para conseguir un mayor efecto tractor en el campo de la ciberseguridad como oportunidad económica, profesional y empresarial.
- Mejorar las capacidades con las que ya se cuenta a nivel regional, incorporando nuevas infraestructuras, equipamientos y recursos que permitan su especialización.
- Incrementar la adopción global de medidas de ciberseguridad, desde el diseño y en el resto de etapas. Desarrollo de nuevas soluciones.
- Atraer y generar talento con el desarrollo de estrategias de captación y capacitación en ciberseguridad, tanto a nivel de oferta como de demanda a través de planes de formación e itinerarios especializados con competencias y perfiles profesionales, que aceleren el desarrollo de la Ciberseguridad.
- Impulsar el emprendimiento en ciberseguridad, y la aceleración especialmente de las PYMEs, con una mejor visibilidad y llegada al mercado.

2. OBJETO DE LA CONTRATACIÓN

El presente Acuerdo Marco tiene por objeto la selección de empresas especializadas en Ciberseguridad para la prestación de los servicios de simulacros de incidentes de Ciberseguridad, para SPRI-Agencia Vasca de Desarrollo Empresarial (en adelante, "SPRI"), durante el plazo de duración del mismo.

La prestación de los servicios por los adjudicatarios de este concurso público se realizará a demanda de SPRI y al mismo tiempo, en parte, como respuesta a las solicitudes que SPRI reciba de las empresas con actividad en la CAE para la organización de jornadas de "Simulacros de incidentes de Ciberseguridad" que se podrán celebrar tanto "in company" para equipos directivos/as de una empresa como en formato abierto a diferentes empresas, en las instalaciones que SPRI ponga a disposición de estas actividades, en condiciones de igualdad para todas las empresas con centro de actividad en la CAE. Estos simulacros estarán orientados principalmente a personas de los equipos de dirección, con capacidad en la toma de decisiones que permitan reducir las vulnerabilidades de la empresa en el ámbito de ciberseguridad. Las personas del área de Tecnologías de la Información y las Comunicaciones deberán participar siempre en estos simulacros. También se podrán organizar desde SPRI simulacros que impliquen a personas del ámbito técnico. Los servicios serán prestados por los adjudicatarios a demanda de SPRI y esta los requerirá atendiendo a su demanda y, en parte, a la demanda previa de las empresas a través del SERVICIO DE INCIDENTES DE CIBERSEGURIDAD de SPRI de su página Web. Estos simulacros podrán ser organizados por SPRI también en convocatoria abierta para diferentes empresas de manera conjunta, pudiendo tener que prestarse simulacros de incidentes específicos den relación con los 17 Clusters empresariales de la CAE.

El precio de cada simulacro estará determinado por las diferentes "tipologías de simulacro de incidentes de ciberseguridad", y por el número de horas máximas asignadas por SPRI para la gestión e impartición de cada uno de estos tipos de simulacro de incidentes de ciberseguridad en función de las características de cada empresa o colectivo de empresas y de sus necesidades en este ámbito. La tipología de simulacros de incidentes podrá ir variando en función de la evolución tecnológica y también de la situación global de ciberseguridad en los diferentes sectores empresariales. Se tendrá en cuenta en el diseño y evolución de la tipología de simulacros de incidentes las necesidades específicas de los 17 clusters existentes en la CAE.

La dedicación no superará las 7 horas por persona consultora, hasta un máximo de dos personas, por simulacro. Las adjudicatarias estarán obligadas a ejecutar los simulacros de incidentes de ciberseguridad siguiendo las instrucciones y estructura básica que SPRI determine para cada tipo de simulacro de incidente de Ciberseguridad.

A su vez, ninguna empresa contratista seleccionada podrá ejecutar servicios por importe superior a 350.000 euros (IVA no incluido). En caso de que el número de contratistas fuera inferior a 10, el importe máximo de adjudicación de contratos basados por contratista será el resultado de dividir el valor estimado del contrato entre el número de contratistas (ej. 8 contratistas, valor máximo de adjudicación 437.500 euros).

Se seleccionará un máximo de 20 contratistas.

Las actividades objeto del Acuerdo Marco y de cada uno de los contratos se llevarán a cabo en el ámbito de la CAE.

El alcance temporal será hasta el 31 de marzo de 2026, desde el día hábil siguiente a la fecha de formalización del Acuerdo Marco. Los contratos basados serán adjudicados dentro de la duración del Acuerdo Marco, pudiendo tener una duración superior, de hasta tres meses más.

3. OBJETIVOS Y DESCRIPCIÓN DE LAS ACTIVIDADES A DESARROLLAR

3.1. Objetivo

La prestación de servicios de simulacros de incidentes de Ciberseguridad.

3.2. Actividades objeto del contrato

Las tareas que se encomendarán a los adjudicatarios serán todas las necesarias para la gestión y ejecución de simulacros de incidentes de ciberseguridad. Éstas serán, sin ánimo exhaustivo, las siguientes:

- Conocer los objetivos de cada servicio, identificar sus necesidades y definir la tipología de simulacro que mejor se adapte a sus necesidades.
- Colaborar con SPRI en la definición de la tipología de simulacros de incidentes de ciberseguridad.
- Gestionar y ejecutar los simulacros de incidentes de ciberseguridad que organice SPRI en convocatoria abierta a las empresas de la CAE en las instalaciones que SPRI habilite al efecto.
- Gestionar y ejecutar los simulacros de incidentes de ciberseguridad en las empresas que de manera individual así se lo soliciten a SPRI, bien *in company*, bien en las instalaciones que SPRI habilite al efecto, dentro de la CAE.
- Elaborar informe del resultado de los simulacros realizados así como propuestas de actuaciones a realizar por las mismas para reducir sus vulnerabilidades.
- Elaboración de informes para SPRI, sobre el resultado de los simulacros realizados.
- Ejecutar la tipología de simulacros de ciberseguridad que le sean solicitados. La tipología será definida y diseñada por SPRI. Se establecerá para cada simulacro el número de horas máximo a imputar de cada uno de los dos perfiles profesionales requeridos en el Acuerdo Marco. La dedicación no superará las 7 horas por persona consultora, hasta un máximo de dos personas, por simulacro.
- A modo de ejemplo, y sin perjuicio de su necesaria actualización y ajuste a las necesidades que plantee SPRI en cada caso, los simulacros podrán ser de estos tipos:
 - Ransomware.
 - Infraestructura crítica.
 - Ataques dirigidos.
 - Otros.
- Se diseñarán tipos de simulacros de manera acorde al tamaño de las empresas así como a sus sectores de actividad, haciendo especial esfuerzo en diseñar simulacros dirigidos a las pequeñas y medianas empresas, especialmente las de los sectores industriales y de servicios avanzados así como las del ámbito de la energía.
- Realizar para SPRI acciones de difusión del servicio.

- Las empresas adjudicatarias del acuerdo marco deberán ajustar la ejecución de los simulacros a la metodología que establezca SPRI para cada tipología de simulacro. A modo de ejemplo, se tendrá en cuenta aspectos tales como:
 - Diseñar simulacros específicos para los equipos de dirección, y siempre involucrando en el mismo a los equipos del Área TIC.
 - Los simulacros deben estar dirigidos a equipos de comité de crisis y enfocado a la toma de decisiones.
 - Posibilidad de benchmark y búsqueda de sinergias con las acciones que realizan entidades como INCIBE o ZIUR.
 - Revisar actuaciones dirigidas también a perfiles Técnicos, Role play, etc.
 - Diseñar simulacros con diferentes formatos: simulacro de incidente en una planta productiva mediante juego de rol narrativo (storytelling), simulacros para diferentes perfiles, en formatos con dedicaciones horarias en una o varias sesiones.
- Colaboración con SPRI en el establecimiento y gestión de cuadros de mando del servicio.
- Colaboración con los Clusters en el ámbito de este contrato cuando SPRI así lo solicite.

En la ejecución de los diferentes contratos basados en el Acuerdo Marco se deberá garantizar la prestación de los servicios en ambas lenguas oficiales, toda vez que la prestación deberá poder ejecutarse en comunicación con cualquier empresa o colectivos de empresas con centro de actividad en la CAE. Asimismo, el contratista garantizará en todas las acciones, un uso no sexista del lenguaje y del tratamiento de imágenes. Todo ello en función de lo previsto en la Decreto 19/2024, de 22 de febrero, de normalización del uso del euskera en el Sector Público Vasco, así como en la Ley Orgánica 3/2007, de 22 de marzo, para la igualdad efectiva de mujeres y hombres.

El cumplimiento de las obligaciones de cooficialidad lingüística y del uso no sexista del lenguaje y de las imágenes, es imprescindible y esencial para la correcta prestación del Servicio. De esta forma, se configuran como condiciones esenciales de ejecución de cada uno de los contratos basados en el Acuerdo Marco, así como del propio Acuerdo Marco, y su incumplimiento, entendiéndose por tal la no prestación de un Servicio en cualquiera de las lenguas oficiales tras haberlo solicitado SPRI o una empresa, o un uso del lenguaje y de las imágenes no ajustado a lo señalado en la Ley Orgánica 3/2007, de 22 de marzo, para la igualdad efectiva de mujeres y hombres, podrá:

- Ser objeto de una penalidad, de hasta el 10% del importe correspondiente al contrato basado en el que se constate el incumplimiento en cuanto al uso no sexista del lenguaje y de las imágenes.
- Ser causa de resolución del acuerdo marco en el caso de que el contratista al que se le asigne el contrato basado no pueda ejecutar una prestación en la lengua oficial requerida por SPRI o por la empresa.

4. EQUIPO DE TRABAJO Y PERFILES PROFESIONALES REQUERIDOS

El equipo de trabajo que las licitadoras oferten en su propuesta deberá incluir personal cualificado y estar compuesto por técnicos especialistas en Ciberseguridad. En particular, el equipo de trabajo que se proponga deberá cumplir con, al menos, las siguientes condiciones:

- a-** Designación de una persona (consultor/a jefe/a del proyecto) que ejerza como responsable general de los Servicios a prestar e interlocutor con la persona responsable en SPRI, con conocimiento y experiencia suficientes en labores de naturaleza similar a la del objeto del presente pliego, esto es, en el ámbito de Ciberseguridad.
- b-** Para la ejecución de las labores descritas en el apartado 3º anterior, además de la persona que ejerza como consultor/a jefe/a de proyecto, se estima necesario, por cada adjudicatario, un equipo adicional mínimo de 2 personas (2 Consultores/as Técnicos/as especialistas, que operarán como técnicos de apoyo) con experiencia en el ámbito de Ciberseguridad.

- c- Al menos una de las personas del equipo de trabajo propuesto deberá poder prestar el Servicio en euskera, cuando SPRI y/o las empresas así lo soliciten. Por ello, en la oferta se deberá acreditar el dominio, a nivel C1 o equivalente de euskera por, al menos, 1 miembro del equipo de trabajo propuesto.

Los trabajos desarrollados serán supervisados por el responsable del contrato de SPRI.

SPRI podrá indicar a la contratista, que se compromete a valorarlo, la incorporación de personas adicionales a los servicios, en función de las necesidades puntuales, siempre que sus perfiles sean similares a los de las personas propuestas en el equipo de trabajo.

En cualquier caso, el equipo de trabajo deberá estar compuesto, al menos, de los siguientes perfiles profesionales:

- Una persona, con formación superior en Ingeniería Industrial, Ingeniería Informática, Ingeniería de Telecomunicaciones, Física, Matemáticas o equivalentes, con formación específica en Ciberseguridad, que ejerza como consultor/a jefe/a del proyecto e interlocutor principal con SPRI.
- Dos personas, al menos una de ellas con formación superior en Ingeniería Industrial, Ingeniería Informática, Ingeniería de Telecomunicaciones, Física, Matemáticas, o similares, con formación específica en Ciberseguridad, que ejerza como consultor/a experto/a especialista, a modo de técnico de apoyo. A la segunda persona no le será exigible contar con formación superior, pero sí acreditar conocimientos en el ámbito de la Ciberseguridad.

Los miembros del equipo propuesto deberán disponer de la siguiente experiencia mínima y cumplir con los roles a continuación detallados:

Perfil profesional	Roles y años de experiencia
1-Consultor/a Jefe/a del proyecto	Experiencia en consultoría y gestión de proyectos, con al menos 5 años de experiencia en el campo objeto de este servicio. Liderazgo: Debe ser capaz de liderar equipos multidisciplinares y dirigir proyectos desde la concepción hasta la implementación. Habilidades de gestión: Debe tener habilidades sólidas en gestión de proyectos, incluyendo planificación, asignación de recursos, gestión de riesgos y presupuesto y disponer de habilidades de descargo del proyecto con el equipo de SPRI. Excelentes habilidades comunicativas: Debe ser capaz de comunicarse eficazmente con clientes, equipos internos y otros stakeholders. Orientado a resultados: Se espera que este perfil tenga un enfoque orientado a resultados y sea capaz de cumplir con los objetivos del proyecto dentro de los plazos y presupuestos establecidos. Capacidad analítica: Debe ser capaz de analizar problemas complejos y desarrollar soluciones efectivas para resolverlos.

2-Consultores/as Técnicos/as especialista	Experiencia en consultoría de al menos 2 años en el campo específico relacionado con el proyecto. Habilidades técnicas: Debe tener un sólido conocimiento técnico en su área de especialización y ser capaz de aplicar este conocimiento en la resolución de problemas que surjan en la ejecución del servicio con SPRI. Autonomía: Se espera que pueda trabajar de manera autónoma en tareas asignadas, aunque también pueda colaborar eficazmente en equipos formados entre el adjudicatario y SPRI. Habilidades de comunicación: Debe ser capaz de comunicarse claramente con el equipo de SPRI, tanto verbalmente como por escrito. Adaptabilidad: Debe ser capaz de adaptarse a diferentes entornos de trabajo y ser flexible en su enfoque para abordar los desafíos del proyecto.
--	---

El equipo mínimo se entenderá sin perjuicio de la obligación de la adjudicataria de destinar el personal que sea necesario para la correcta ejecución del contrato y cumplir con las condiciones generales y específicas en cuanto a competencia técnica y profesional contenidas en la legislación vigente y requeridas en el presente Pliego, todo ello por cuanto los medios humanos constituyen un factor determinante en la calidad del servicio. Las personas que durante el período de duración de contrato resulten precisas para el desarrollo del mismo tendrán el nivel curricular requerido según el perfil al que se adscriban.

5. SUPERVISIÓN Y CONTROL DEL SERVICIO

Los servicios a prestar serán supervisados por el Área de Transformación Digital de SPRI, y en particular por la persona responsable del contrato, que podrá pedir las explicaciones e informaciones que considere oportunas al objeto de verificar el correcto desarrollo de los trabajos contratados.

6. ASIGNACIÓN DE LOS CONTRATOS BASADOS ENTRE LOS CONTRATISTAS SELECCIONADOS

La prestación de los Servicios se plantea como una sucesión de contratos basados derivados del Acuerdo Marco, uno para cada "Simulacro de incidente de ciberseguridad", que se ejecutarán a demanda de SPRI:

- (i) En el caso de los servicios in company, sobre la base de la demanda previa de las empresas, SPRI solicitará tres ofertas, y se podrán utilizar uno o varios de los criterios de adjudicación utilizados en la adjudicación del Acuerdo Marco, pudiendo ser las ponderaciones distintas.
- (ii) En cuanto a la realización de jornadas de simulación de incidentes de ciberseguridad abiertas a diferentes empresas, SPRI garantizará un reparto mediante un turno rotatorio, de forma que se adjudicará un contrato basado a cada empresa siguiendo el orden en el que hubieran quedado clasificadas las propuestas (esto es, se comenzará adjudicando el primer servicio a la empresa clasificada en primer lugar, y así sucesivamente según el orden de clasificación). En caso de empates en la puntuación global, se adjudicará siguiendo un orden alfabético en atención a la denominación

social de la adjudicataria. En caso de coincidir en fechas la jornada con otra jornada previamente adjudicada, se adjudicará el contrato basado a la siguiente empresa siguiendo el mismo orden y turno rotatorio.

En todo caso, ningún contratista seleccionado podrá ejecutar servicios por importe superior a 350.000 euros (IVA no incluido). En caso de que el número de contratistas fuera inferior a 10, el importe máximo de adjudicación de contratos basados por contratista será el resultado de dividir el valor estimado del contrato entre el número de contratistas (ej. 8 contratistas, valor máximo de adjudicación 437.500 euros).

En ningún caso el contratista seleccionado para la ejecución de un contrato basado podrá de forma no justificada renunciar a su ejecución, y vendrá obligado a prestar todos los servicios solicitados por SPRI. Se entenderá por causa justificada la coincidencia en fechas con jornadas previamente convocadas en el marco del presente acuerdo, así como la superación del umbral económico máximo por contratista antes indicado.