

**PLIEGO DE PRESCRIPCIONES TÉCNICAS PARTICULARES PARA LA EVALUACIÓN Y LA CREACIÓN DE UNA
FUTURA CERTIFICACIÓN DE CIBERSEGURIDAD DE PRODUCTOS INDUSTRIALES DEL SECTOR DE LA
MÁQUINA HERRAMIENTA DE GIPUZKOA (EXPTE. ZIUR2023-02)**

I.- CONTEXTO DEL PLIEGO DE PRESCRIPCIONES TÉCNICAS

El objeto del presente pliego, conforme al artículo 124 de la Ley 9/2017 de Contratos del Sector Público, es definir las prescripciones técnicas particulares que han de regir la realización de las prestaciones, pormenorizando su alcance objetivo, así como los requisitos mínimos y condiciones técnicas generales que deberán considerarse para la prestación del servicio de asesoramiento.

II.- OBJETO Y ALCANCE DEL SERVICIO

Los objetivos de ZIUR con este proyecto se centran en desarrollar una iniciativa dirigida a la evaluación, para una futura certificación de producto industrial ciberseguro. Para ello, desde ZIUR se ha definido una *metodología* que permite la *evaluación y certificación de productos industriales* según la norma IEC 62443, siguiendo sus requisitos de seguridad y niveles de seguridad.

A la hora del diseño de la metodología, se han tenido en cuenta los siguientes aspectos clave:

- Que *aporte valor para la demanda* de modo que se fomente la certificación de productos por la oferta.
- Que sea una *metodología solvente* que fomente un sistema de *evaluación colaborativa* especializada que integre el ecosistema del territorio.
- Que *posicione a Ziur como pieza clave* de esta integración.

El **objeto** de la presente licitación es la obtención de un servicio de evaluación de productos industriales específicamente del sector de la Máquina Herramienta, evaluación realizada por un laboratorio evaluador con las capacidades técnicas y humanas que se definirán en el presente pliego de prescripciones técnicas, siguiendo la metodología definida por ZIUR y que se pondrá a disposición de las empresas licitantes, previa petición expresa durante los quince primeros días del plazo para presentar las proposiciones de la licitación.

Junto con el laboratorio evaluador, se valorará positivamente mediante criterio a valorar mediante juicio de valor, que la propuesta presentada por las empresas licitadoras incluya un servicio de preparación a la evaluación y de acompañamiento a la empresa evaluada, prestado por una empresa independiente al laboratorio evaluador.

Es decir, se otorgará una puntuación superior en el supuesto en el que la empresa que lleve a cabo los servicios asociados a la preparación/acompañamiento sea diferente a la que lleva a cabo los servicios

asociados a la figura del laboratorio evaluador, con el fin de mantener la independencia en ambos procesos.

En el caso en el que tanto la fase de preparación a la evaluación y de acompañamiento a la empresa evaluada como la fase a desempeñar por el laboratorio evaluador sea realizada por la misma empresa, los componentes de los dos equipos de trabajo involucrados deberán estar compuestos por personas distintas.

Los **objetivos** del proyecto son los siguientes:

- Realizar un piloto sobre la metodología de evaluación definida por ZIUR y analizar su validez como herramienta futura para la evaluación de ciberseguridad de productos industriales
- Identificar el grado de cumplimiento y madurez de la ciberseguridad de los productos industriales analizados.
- Identificar las capacidades de evaluación de productos industriales de tejido empresarial del territorio.
- Ayudar al sector de la máquina herramienta a conocer las necesidades que en materia de ciberseguridad le va a exigir tanto su mercado, como los diferentes requerimientos normativos.

Como resultado del proyecto, las empresas industriales de Gipuzkoa tendrán los siguientes **beneficios**:

- Alinear capacidades científico - tecnológicas e industriales
- Fortalecer la competitividad de nuestro tejido industrial
- Dar los pasos para que Gipuzkoa sea un referente en Ciberseguridad Industrial – Evaluación Producto Industrial

Alcance

Dentro del servicio, se contempla la **evaluación de seguridad de 4 productos industriales de 4 empresas diferentes del sector de la Máquina Herramienta**, siendo las fases inicialmente previstas las siguientes:

1. Servicio previo de preparación a la evaluación y acompañamiento a las empresas evaluadas
2. Documentación del escenario de evaluación
3. Consensuar parámetros de operación de producto
4. Selección de las pruebas a realizar y diseño de las evaluaciones
5. Análisis de los resultados arrojados durante las pruebas llevadas a cabo en los puntos anteriores y propuesta de mejora en el diseño
6. Servicio técnico de apoyo a cada empresa, para ayudarles a implementar las mejoras propuestas en el plan de remediación

Todos los costes asociados al servicio serán a cuenta de la licitadora, incluidos los asociados a transporte y desplazamientos que puedan derivarse del servicio, tales como:

- **Desplazamientos del personal de las 4 empresas participantes a las instalaciones del laboratorio evaluador. Las 4 empresas estarán ubicadas en Gipuzkoa.**
- **Transporte de las máquinas bajo estudio, de las 4 empresas participantes, al laboratorio evaluador.**

III.- DESCRIPCION DEL SERVICIO

En este apartado se describen las características técnicas que conforman el objeto del contrato y que la adjudicataria 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 ZIUR, cubriendo los aspectos de tareas a realizar y resultados esperados.

La adjudicataria deberá aportar y describir en su oferta los conocimientos, metodologías, herramientas y equipo humano en el que se apoyará para asegurar el resultado óptimo del proyecto, en los términos establecidos en el Cuadro de características y en el clausulado general del Pliego de Cláusulas Administrativas Particulares.

En el servicio se contempla la intervención de diferentes actores:

- **Fabricante** - Para dar comienzo al proceso de evaluación, la fabricante solicita la certificación del producto y facilita la documentación necesaria para ello. Será el personal de ZIUR el que seleccionará los 4 fabricantes que participarán en el proceso. En base a la norma IEEC62443, se analizan en profundidad las características del producto y sus particularidades
- **Servicio de preparación/acompañamiento** - Se lleva a cabo el ajuste de la normativa al caso particular de la evaluación aterrizándolo en controles.
- **Laboratorio evaluador** - Se llevan a cabo los ensayos establecida para verificar el cumplimiento de los controles pertinentes en un laboratorio independiente

Tal y como se ha indicado más arriba, el equipo de trabajo que lleve a cabo los servicios asociados a la preparación/acompañamiento debe ser diferente al que lleva a cabo los servicios asociados a la figura del laboratorio evaluador, con el fin de mantener la independencia en ambos procesos.

Respecto al marco de referencia y la metodología de evaluación, desde ZIUR se ha definido un *framework* de referencia, de evaluación y testeo basado en la IEC 63443 4-1 y 62443 4-2, que se pone a disposición de los licitantes, previa petición expresa a través del correo electrónico ziur@ziur.eus, con objeto de que conozcan la metodología y pruebas a realizar.

Mediante las evaluaciones de ciberseguridad (*security testing*), se busca validar que los controles de seguridad funcionan con respecto a lo esperado. Partiendo del documento de requisitos de seguridad, se evalúa, para cada una de las dimensiones, si dicho producto cumple con la especificación. Con el objeto de realizar dichas evaluaciones de una manera procedimentada, repetible y verificable por un agente externo; la norma IEC 62443 define una serie de niveles de seguridad (*security levels*), además de las prácticas a evaluar.

Indicar que la metodología definida por ZIUR establece al igual que la norma IEC62443 diferentes niveles de seguridad (SL – Security Levels), según el origen del ataque y sus posibles consecuencias.

- Nivel 0: no se requieren protecciones de seguridad para el producto.
- Nivel de seguridad 1: requiere de protección contra incidentes no intencionados.
- Nivel de seguridad 2: requiere de protección contra incidentes intencionados, con medios que evitan a atacantes que poseen una baja motivación o conocimiento.
- Nivel de seguridad 3: requiere de protección contra incidentes intencionados, los cuales podrían ser ocasionados por atacantes con conocimientos de IACS, tales como hacktivistas y ciberterroristas, entre otros.
- Nivel de seguridad 4: requiere de protección contra incidentes intencionados, mediante medios muy avanzados, grandes recursos, conocimientos avanzados y motivación alta, como ser organizaciones criminales y ciberejércitos.

A este respecto, el alcance de la evaluación de los productos industriales, se establece la evaluación de acuerdo con lo definido para el nivel de seguridad 1 – SL1.

Dicha evaluación se realiza en diversos ámbitos; desde ámbitos más generalistas donde se evalúan los protocolos de uso industrial (OPC-UA, Profinet, Modbus, etc.); hasta los ámbitos más concretos de un producto industrial, como pueden ser las aplicaciones desarrolladas por el propio fabricante. Realizar esta distinción permite, que, para las pruebas generalistas, se haga uso de herramientas de testeo existentes; mientras que el resultado de la evaluación de aplicación de fabricante dependerá del conocimiento y experiencia de los ingenieros de pruebas.

Todas las licencias de hardware y software, requeridos para realizar la evaluación, correrán a cargo de la licitadora.

IV.- REQUISITOS TÉCNICOS DEL LABORATORIO DE PRUEBAS

Para la correcta realización de las pruebas, con la calidad esperada por ZIUR, y con el fin de ser capaces de realizar una evaluación procedimentada, repetible, verificable por un agente externo y contenida en costes; es necesario el uso de herramientas de evaluación comerciales.

Teniendo en cuenta el estado del arte de las herramientas de evaluación de ciberseguridad industrial, el laboratorio acreditado por la licitadora, debe disponer de las herramientas suficientes para ofrecer las siguientes funcionalidades:

- Herramienta de testeo de penetración Web
 - Esta herramienta debe utilizar un marco de referencia estandarizado o de facto para llevar a cabo el testeo, por ejemplo, Open Web Application Security Project (OWASP) o similar.
- Herramienta de testeo de protocolos de comunicación
 - Esta herramienta debe analizar los protocolos de comunicación de propósito general. El resultado de este análisis deberá estar ligado con el reporte estandarizado de vulnerabilidades CVE (Common Vulnerabilities and Exposures).

- Herramienta de testeo de protocolos de comunicación industrial
 - Esta herramienta debe cubrir el testeo de comunicaciones inválidas o malformados (conocido como fuzzing), el testeo de tráfico elevado (conocido como pruebas de Denegación de Servicio); y la comprobación de vulnerabilidades conocidas en protocolos OT.
 - Debe soportar, al menos, los siguientes protocolos de comunicación:
 - EtherNet/IP (CIP)
 - Foundation Fieldbus (FF-HSE)
 - MMS
 - Modbus TCP/IP
 - OPC UA
 - PROFINET IO
 - DNP3
 - MMS (IEC 61850/ICCP)
 - Modbus TCP/IP
 - SES-92
 - ZigBee SE (802.15.4)

En cualquier caso, con el fin de comprobar que el laboratorio propuesto por el licitador para la ejecución de las pruebas cumple los requisitos mínimos para el objetivo del proyecto, la propuesta debe incluir el listado detallado de las herramientas HW y SW que componen el laboratorio donde se llevará a cabo la evaluación, así como su ubicación física.

Los servicios de laboratorio a realizar, teniendo como referencia la norma IEC62443, debe contemplar, como mínimo, llevar a cabo los siguientes tests:

- Prueba 1: Test de los requerimientos de seguridad del producto bajo estudio
 - Prueba funcional: test que teniendo en cuenta los requisitos de la norma, evalúa manera objetiva su cumplimiento (evidencias de pasa/no pasa) tanto de **manera externa como interna**
- Prueba 2: Test de mitigación de amenazas
 - Pruebas de Penetración: test que evalúa, de manera semiautomática, la **funcionalidad interna**, y para ello se simula una situación de ataque de manera controlada mediante técnicas de acceso no autorizado con el objetivo de conocer las brechas reales de seguridad
- Prueba 3: Test de Vulnerabilidades
 - Escaneo de puertos: test que evalúa la **conectividad externa del producto**; identificación posibles canales en desuso, pudiendo servir estos como punto de interacción con el sistema de manera no controlada

- Escaneo de vulnerabilidades de red: test que evalúa la conectividad externa del producto; **identificando los fallos conocidos** en la implementación de los protocolos de comunicación
- Fuzzing: test que evalúa la funcionalidad externa del producto, **identificando los fallos NO conocidos** en la implementación de los protocolos de comunicación.
- Test de stress de red: test que evalúa la **conectividad externa del producto**, *stressando* sus interfaces, y de esta manera afectar a su funcionamiento, similar a las técnicas usadas en los ataques de tipo de denegación de servicio (Denegación de Servicio). Esta prueba es de gran valor ya que con podemos detectar si el comportamiento de control del sistema (disponibilidad) se ve afectado ante ataques no muy sofisticados.
- Prueba 4: Test de Penetración
 - Test de penetración lógica: test que evalúa, de manera manual, la **funcionalidad interna**, y para ello se simula una situación de ataque de manera controlada mediante técnicas de acceso no autorizado con el objetivo de conocer las brechas reales de seguridad
- Prueba 5: Independencia de los testeadores
 - La independencia de los testeadores se consigue debido a que no existe ninguna relación de filiación entre las empresas fabricantes de los productos y los ingenieros de pruebas.

V.- METODOLOGIA Y PLAN DE TRABAJO

La empresa licitadora deberá realizar una propuesta que incluya tanto la metodología, como el plan de trabajo, reflejando los hitos más relevantes del servicio con sus respectivas fechas. Así mismo, se deberá especificar el listado de entregables con una descripción y estructura aproximada de lo que incluirá cada uno de ellos, siendo condición mínima la realización de los siguientes entregables:

V.1.- Servicio previo de preparación a la evaluación y acompañamiento a las empresas evaluadas

La evaluación comienza con un proceso previo de preparación por parte de la fabricante, en el que se definen parámetros esenciales que condicionan el alcance y aplicabilidad de los requisitos en el ámbito de la evaluación con el objetivo de diseñar los controles que se testarán.

En resumen, la evaluación debe ser acotada de manera que se establezca de forma clara el ámbito y el objetivo de la evaluación. Como resultado del proceso llevado a cabo por la fabricante, se obtendrá el conjunto de controles a evaluar.

Dentro de esta primera fase se contemplan las siguientes subfases:

1. Establecimiento del Alcance - El primer paso al comenzar la evaluación es definir el alcance, es decir, se debe delimitar aquello que se va a tener en consideración en el proceso. El alcance debe

- definir al menos las unidades organizacionales sometidas al mismo, los procesos o componentes a evaluar y la cobertura normativa de la evaluación.
2. Declaración de Aplicabilidad - Además del alcance, para los requerimientos que no son aplicables, debido a la naturaleza o condiciones del objeto de la evaluación, se deben marcar como no aplicables y ser comunicados al evaluador de manera motivada.
 3. Nivel de seguridad deseado - Se debe definir el nivel de seguridad a considerar en el momento de realizar la evaluación. Debe considerarse un nivel de seguridad general para toda la normativa sin perjuicio de los niveles de seguridad diferentes que se puedan marcar para subsecciones de la misma.
 4. Declaración de conformidad - Se facilitará al evaluador una declaración de conformidad para cada requisito del ámbito de aplicación. La declaración de conformidad explicará cómo se cumple el requisito correspondiente en el ámbito de aplicación para el nivel de seguridad solicitado.
 5. Provisión de Evidencias - Para el proceso de evaluación, se proporcionarán las evidencias ajustadas al nivel de rigurosidad exigido por el nivel de seguridad, de manera que el evaluador las considere posteriormente para examinar si se cumple el requisito relacionado. La provisión de evidencias no será necesaria para los requisitos que no aplican.

De cara a realizar las actividades descritas en los puntos anteriores es importante tener en cuenta que:

- Todos los puntos mencionados deben ser entregados de forma escrita al evaluador y a la organización de servicios auxiliares. Dichos informes deben estar escritos en euskera y en castellano.
- Parte de los objetivos a evaluar cuentan con criterios de aplicabilidad predefinidos según las características del producto, y solo serán evaluados si procede.
- La provisión de evidencias se realizará una vez la organización de servicios auxiliares defina los controles a evaluar.

V.2.- Documentación del escenario de evaluación

Inicialmente, el fabricante de producto proporcionará a la empresa adjudicadora información sobre los activos/dispositivos a testear (también conocido como Device Under Test, DUT); como puede ser: el funcionamiento de control normal, el funcionamiento de control excepcional y un listado de los mecanismos de interacción con el dispositivo. El DUT debe estar configurado con toda la funcionalidad posible que puede soportar, para garantizar la mayor cobertura posible de la evaluación y así, sacarle el máximo partido.

V.3.- Consensuar parámetros de operación de producto

Una vez las y los ingenieros de pruebas tengan acceso a dicha documentación, la analizarán y propondrán un documento de métodos de testeo y criterios para la monitorización de las funciones de control. Los parámetros de este documento serán acordados entre las y los ingenieros de pruebas y el fabricante de producto.

V.4.- Selección de las pruebas a realizar y diseño de las evaluaciones

Teniendo en cuenta las especificidades del producto a evaluar, se elegirán los tests que aplican en cada caso y se describirá como se va a realizar dicho test (entorno operativo, herramientas de medida, método de medida, valores resultado, etc.).

Dichos tests tienen que cumplir con los requisitos marcados en el apartado IV de este Pliego de Prescripciones Técnicas, de acuerdo con la norma IEC 62443 en su parte 4-1 práctica 5. Cada tipo de test deberá estar cubierto, al menos por una prueba, siendo recomendable hacer el mayor número de tipos de pruebas posible.

V.5.- Selección de las pruebas a realizar y diseño de las evaluaciones

Una vez realizado el diseño, se procederá a realizar la mencionada evaluación por las y los ingenieros de pruebas en su laboratorio.

V.6.- Análisis de los resultados arrojados durante las pruebas llevadas a cabo en los puntos anteriores y propuesta de mejora en el diseño

Una vez realizadas las pruebas, se procederá a analizar toda la información recogida en los tests para elaborar los informes de resultados, que se presentarán a la empresa bajo evaluación y a ZIUR. Todos los informes tienen que presentarse en Euskera y en Castellano.

En dichos informes, a la vista de los resultados obtenidos, debe incluirse una propuesta de mejoras en el diseño del producto, con el fin de mejorar su madurez de ciberseguridad.

V.7 - Servicio técnico de apoyo a cada empresa, para ayudarles a implementar las mejoras propuestas en el plan de remediación

La empresa adjudicataria encargada de la evaluación, debe incluir en el proyecto un servicio técnico de apoyo, para ayudar a cada una de las 4 empresas bajo evaluación, a implementar, en su producto, las mejoras propuestas en el apartado anterior.

Estas son las fases que, como mínimo, deben contemplarse para cada una de las 4 evaluaciones contempladas en el proyecto.

VI.- REQUISITOS DEL EQUIPO DE TRABAJO

Además de lo establecido para la adscripción obligatoria de medios personales:

- El equipo de trabajo del servicio de la Fase 1, descrita en el pliego técnico, de preparación y acompañamiento a las empresas evaluadas, deberá presentar un equipo de trabajo, independiente del servicio de evaluación. Dicho equipo de trabajo debe constar, como mínimo, de 2 profesionales con experiencia en servicios similares.
- El equipo de trabajo del servicio asociado a las Fase 2, 3, 4, 5, 6 y 7, asociadas el servicio de evaluación, con el objetivo de no demorar la ejecución de la evaluación y poder gestionar las diferentes evaluaciones en paralelo; cumpliendo los tiempos establecidos para la ejecución del proyecto, debe constar de, al menos, 4 ingenieros de pruebas.

VII.- INSPECCIÓN Y CONTROL DE LOS TRABAJOS

La empresa adjudicataria deberá facilitar el ejercicio de las funciones de inspección y control que sobre el desarrollo de los trabajos corresponden a ZIUR Fundazioa, dando estricto cumplimiento a las observaciones y recomendaciones que reciba.

Quedará en todo caso a criterio de ZIUR Fundazioa la modificación de la forma de seguimiento (reuniones, actas, informes, ...) en caso de que lo considere necesario.

Del mismo modo, deberá prestar, sin derecho a pago suplementario, los servicios que se estimen necesarios para el correcto desarrollo y cumplimiento del contrato, en lo referido a la asistencia a reuniones de trabajo o informativas. Esta obligación se mantendrá hasta la finalización del periodo de garantía.

Donostia-San Sebastián, 10 de Febrero de 2023.



Koldo PECIÑA TXINTXURRETA
ZIUR FUNDAZIOA