PLIEGO DE PRESCRIPCIONES TÉCNICAS PARTICULARES PARA EL SERVICIO DE EVALUACIÓN EN MATERIA DE CIBERSEGURIDAD DEL DISEÑO DE PRODUCTOS INDUSTRIALES DEL SECTOR IoT DE GIPUZKOA PARA ZIUR FUNDAZIOA (Exp. ZIUR2024-015)

I. 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 Fundazioa como pieza clave* de esta integración.

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

ZIUR está llevando a cabo otro proyecto, asociado a la licitación ZIUR2024-018, en el que se lleva a cabo el proceso de adaptación de la metodología definida por ZIUR Fundazioa, basada en la norma IEC 62443, a las necesidades del sector IOT, usando como base la Ley CRA. Una vez dicha metodología se haya adoptado se pondrá a disposición de la empresa adjudicataria.

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

- Identificar el grado de cumplimiento y madurez de la ciberseguridad de los productos industriales del sector de IoT analizados.
- Identificar las capacidades de evaluación de productos industriales de tejido empresarial del territorio.
- Ayudar al sector de IoT 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 2 productos industriales de 2 empresas diferentes del sector de IoT**, siendo las fases inicialmente previstas las siguientes:

1. Reunión con la empresa adjudicataria de la licitación ZIUR2024-018 para la compartición y puesta en común de la adecuación de la metodología de evaluación, adaptada al sector IoT
2. Servicio previo de preparación a la evaluación y acompañamiento a las empresas evaluadas
3. Documentación del escenario de evaluación
4. Consensuar parámetros de operación de producto
5. Selección de las pruebas a realizar y diseño de las evaluaciones
6. Análisis de los resultados arrojados durante las pruebas llevadas a cabo en los puntos anteriores y propuesta de mejora en el diseño
7. 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 adjudicataria, incluidos los asociados a transporte y desplazamientos que puedan derivarse del servicio, tales como:

- Desplazamientos del personal de las 2 empresas participantes a las instalaciones del laboratorio evaluador. Las 2 empresas estarán ubicadas en Gipuzkoa.
- Transporte de las máquinas bajo estudio de las 2 empresas participantes al laboratorio evaluador.

II. 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 Fundazioa, 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 - empresa participante (agente distinto a la adjudicataria)** - 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 2 fabricantes que participarán en el proceso. En base a la norma de aplicación, se analizan en profundidad las características del producto y sus particularidades.
- **Laboratorio evaluador (adjudicataria)** - Se llevan a cabo los ensayos establecida para verificar el cumplimiento de los controles pertinentes en un laboratorio independiente.

Respecto al marco de referencia y la metodología de evaluación, desde ZIUR Fundazioa se ha llevado a cabo un proyecto anterior en el que, partiendo de un framework de referencia, de evaluación y testeo desarrollado por ZIUR Fundazioa, basado en la IEC 63443 4-1 y 62443 4-2, se está llevando a cabo una adaptación de dicho framework a la normativa de aplicación para este proyecto. Dicho framework se pone a disposición de los licitantes, previa petición expresa a través del correo electrónico ziur@ziur.eus, para que se use como referencia para la elaboración de esta propuesta. Una vez se disponga del resultado de la adaptación, anteriormente comentada, el resultado se compartirá con la empresa adjudicataria de este proyecto.

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 las y los técnicos/as de pruebas.

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

III. REQUISITOS TÉCNICOS

Los requisitos técnicos del laboratorio de pruebas son los que se describen a continuación.

Para la correcta realización de las pruebas, con la calidad esperada por ZIUR Fundazioa, 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 adjudicataria, debe disponer de las herramientas suficientes para ofrecer las siguientes funcionalidades. La empresa adjudicataria debe detallar las características de la herramienta propuestas para el proyecto y, como mínimo, deben disponer del siguiente equipamiento:

- 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 testo 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 las licitadoras 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.

La empresa licitadora debe proponer un plan de pruebas detallado, donde especifique todas las pruebas que llevará a cabo, y las herramientas que usará para cada una de las pruebas, con las que cumpla todos los requisitos de la norma.

En la propuesta debe detallarse, de manera clara, las pruebas y tests que se llevarán a cabo en cada una de las fases y tareas.

En la propuesta también debe detallarse manera clara (por ejemplo, en formato de tabla) el procedimiento interno que se usará para la comprobación de cada control del framework de evaluación de ZIUR.

IV. 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:

E.1 - Documentación del escenario de evaluación

Inicialmente, el fabricante de producto proporcionará a la empresa adjudicataria 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.

E.2 - Consensuar parámetros de operación de producto

Una vez las y los técnicos/as 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 técnicos/as de pruebas y el fabricante de producto.

E.3 - 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 III 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.

E.4 - Ejecución de las pruebas a realizar

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

E.5 - 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 Fundazioa. 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.

E.6 - 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 2 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 2 evaluaciones contempladas en el proyecto.

V. 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.

Firmado digitalmente por MARIA PENILLA AZCUENAGA el día 05/11/2024 con certificado emitido por AC DNIE 004

María Penilla Azcuenaga
DIRECTOR GENERAL DE ZIUR FUNDAZIOA