

# REALIZACIÓN DE UN DIAGNÓSTICO DE CIBERSEGURIDAD

Pliego de Condiciones Particulares



# ÍNDICE

# Contenido

1	1	Antecedentes	2
2		Objeto	
3	1	Alcance	2
	3.1	1 Auditorías Técnicas en los sistemas de IT	3
	3.2	2 Auditorías Técnicas de seguridad entorno OT	3
	3.3	B Plan de Mejora	4
	3.4	4 Entregables	4
4	F	Plazo de entrega	5
5	F	Precio y forma de pago	5
6	(	Criterios de valoración de ofertas y adjudicación	6
	6.1	Puntuación de la oferta económica:	6
	6.2	Puntuación de la oferta técnica:	7
7	(	Cumplimiento condiciones del servicio	7
8		Documentación para formular la oferta	7
	8.1	Memoria técnica	7
	8.2	Proposición económica	8



#### 1 Antecedentes

La presente especificación técnica se elabora tras haber realizado EBHISA un análisis del estado de sus sistemas informáticos, constatado el incremento de los ciberataques a nivel mundial y valorado la importancia de mantener dichos sistemas protegidos para garantizar la continuidad de la actividad.

## 2 Objeto.

El objeto de este pliego es establecer las condiciones técnicas y económicas necesarias para la presentación de ofertas para el desarrollo de los trabajos de asistencia técnica que permitirán la elaboración de un Diagnóstico de Ciberseguridad.

Más concretamente los trabajos consisten en el análisis de seguridad de los sistemas IT y OT de EBHI y la elaboración de un plan de acción y mejora, que comprende:

- La realización de auditorías técnicas en los sistemas de IT con objeto de verificar el cumplimiento con los requerimientos de Seguridad en sus sistemas y redes, y minimizar el riesgo de sufrir un compromiso de seguridad de la información.
- 2) El análisis técnico de ciberseguridad de los Sistemas de Operación (OT) mediante la realización de un conjunto de pruebas técnicas sin riesgo para la operativa diaria de la instalación, así como mediante entrevistas y revisión de diagramas y manuales técnicos.
- 3) Elaboración de un plan de acción con sugerencias de mejoras de seguridad para los sistemas IT y OT analizados y de la arquitectura general.

#### 3 Alcance.

Como ya se ha mencionado anteriormente, el servicio planteado tiene por objeto realizar un análisis de la seguridad de los sistemas de información,



automatización y control industrial de EBHISA, con objeto de determinar las acciones y medidas que deberían ser implantadas para mejorar el nivel de seguridad de estos sistemas y arquitecturas que conforman.

A continuación se detalla el alcance de los trabajos a realizar. Las propuestas deben incluir las fases, metodología y herramientas utilizadas para realizar cada uno de estos trabajos.

#### 3.1 Auditorías Técnicas en los sistemas de IT

Esta auditoría debe incluir:

- Estudio y propuesta de arquitectura de red desde un punto de vista de la seguridad, identificando las segmentaciones necesarias y los elementos necesarios para proteger las distintas redes.
- Test de Intrusión externo sobre 5-10 IP's.
- Test de intrusión interno en las 5 redes principales de tipo medio (clase C) de la organización.
- Test de intrusión en las 3 redes WIFI de la organización.
- Auditoría de aplicativo web con un enfoque de caja gris.

## 3.2 Auditorías Técnicas de seguridad entorno OT

En el caso del entorno OT la auditoría se centrará en la identificación de las principales deficiencias técnicas mediante la revisión de diagramas y manuales de productos, el análisis técnico de archivos de configuración de los equipos, la realización y análisis de capturas de tráfico en el entorno de producción y la realización de entrevistas con técnicos especialistas.

Asimismo se realizará un estudio de la arquitectura de red actual para identificando los flujos de datos existentes y realizar una propuesta de segmentación por capas incluyendo los elementos necesarios para proteger cada una de ellas.

PCP C2017-00108 Página 3 de 7



## 3.3 Plan de Mejora

El objetivo último del proyecto es plantear un Plan de Acción en el que se detallan los controles y medidas técnicas de seguridad que se recomienda implantar. Para ello se contará como referencia con las siguientes normativas:

La norma ISO/IEC 27002:2013.

El estándar IEC 63443-2.

La guía de referencia NIST SP 800-82.

#### 3.4 Entregables

Los entregables de los servicios solicitados serán los siguientes:

## 1) Auditorías técnicas en los sistemas de IT:

Informes técnicos sobre las pruebas realizadas, vulnerabilidades encontradas, riesgos potenciales.

Recomendaciones (que se incluirán en el plan de mejora) tanto de arquitectura de red como de dispositivos hardware y/o software necesarios.

## 2) Auditorías Técnicas de seguridad en entorno OT:

Informe técnico que recoge las vulnerabilidades detectadas durante los análisis de tráfico y de configuraciones.

Propuesta de arquitectura de red incluyendo los dispositivos hardware y/o software necesarios que se incluirán en el plan de mejora.

Informe de limitaciones técnicas para la implementación de mejoras en el área OT, el cual se tendrá en cuenta en el plan de mejora.

## Plan de mejora:

Informe técnico que recoge las propuestas de mejora a nivel de IT y de OT, y que permitirá corregir las deficiencias encontradas en los análisis técnicos. Dicho plan de mejora debe separar las acciones en corto, medio y



largo plazo en función de su criticidad e incluir una valoración coste, duración y esfuerzo necesario para su implementación.

Resumen Ejecutivo del Proyecto, detallando los principales resultados obtenidos en el marco del proyecto, tanto desde el punto de vista organizativo y procedimental como desde el punto de vista técnico

Todos los entregables serán aportados en dos formatos, uno de ellos será un documento impreso y el otro formato será uno editable digitalmente. Word y/o Excel para documentos de texto, listados etc.

## 4 Plazo de entrega

Para la realización de los trabajos objeto de la licitación se establece un plazo **máximo de 4 meses** a contar desde la fecha de adjudicación.

# 5 Precio y forma de pago.

El importe del Contrato será el de adjudicación. En ningún caso el importe de adjudicación podrá ser superior a **30.000 euros** (IVA no incluido).

Este importe comprende la totalidad de los gastos que tenga que hacer el adjudicatario para la ejecución de este Contrato, es decir, incluye todos los gastos necesarios para desarrollar los trabajos, los gastos de desplazamiento y los trabajos necesarios para la elaboración de los documentos correspondientes.

La forma de pago será transferencia bancaria a la cuenta del adjudicatario en el plazo de 60 días tras la recepción de la factura. Se realizarán las siguientes facturaciones:

Facturaciones a la recepción de los trabajos.

Para el abono del precio será imprescindible la presentación de la correspondiente factura por parte del adjudicatario y previa conformidad de la misma por el responsable designado por EBHISA.



# 6 Criterios de valoración de ofertas y adjudicación

Los criterios que se utilizarán para ponderar las proposiciones de los licitadores son los que se indican a continuación:

- Oferta económica para la propuesta. Con una ponderación del 25%.
- Consideraciones técnicas. Con una ponderación del 75%.

#### 6.1 Puntuación de la oferta económica:

Se asignarán 25 puntos a la oferta más económica, a las restantes ofertas se le asignará la puntuación obtenida mediante la siguiente fórmula:

Poi = Pmax - Pr x ((Oi - Omb) / Omb)\*100

Siendo,

Poi: Puntuación de la oferta a valorar.

Pmax: Puntuación máxima a obtener (en este caso Pmax=25).

Pr: Puntos que se restan en relación al incremento porcentual respecto a la mejor oferta (en este caso Pr=0,33).

Oi: Importe de la oferta a valorar.

Omb: Importe de la oferta más baja.

Las ofertas anormalmente bajas podrán ser desestimadas. Una oferta será considerada anormalmente baja cuando:

BOi > BMO + 10 %

Siendo:

BOi: Bajada porcentual de la oferta respecto al importe máximo de adjudicación (30.000 €). BOi = (Oi-30.000)/30.000\*100

BOM: Media aritmética de las BO de todas las ofertas presentadas que cumplan los requisitos mínimos exigidos en los pliegos de condiciones.



#### 6.2 Puntuación de la oferta técnica:

Se valorará en este apartado y con una puntuación de hasta 75 puntos y con el siguiente reparto:

- 30 puntos. Detalle técnico de la metodología a seguir para obtener los objetivos marcados en cada fase del proyecto.
- 25 puntos. Equipo de proyecto. Titulación y experiencia acreditada de los medios humanos asignados al contrato en proyectos similares.
- 10 puntos por mejoras o ampliaciones al alcance propuesto y que contribuyan a los objetivos descritos.
- 10 puntos Planificación y organización propuesta. Cronograma de los trabajos

# 7 Cumplimiento condiciones del servicio

El adjudicatario queda obligado al cumplimiento de las condiciones del servicio en los términos de su oferta y en las condiciones establecidas en el presente pliego de condiciones particulares.

Si el adjudicatario incumpliese alguna de las condiciones de su oferta o de las establecidas en el pliego citado, será facultad de EBHISA resolver el contrato.

# 8 Documentación para formular la oferta

El licitador deberá presentar una memoria técnica y una proposición económica:

#### 8.1 Memoria técnica

El licitador presentará una memoria técnica con la siguiente información mínima:

- Presentación de la empresa licitadora.
- Experiencia del licitador.
- Descripción técnica detalla del proyecto. Metodología y herramientas.
- Planificación y organización propuesta. Cronograma de los trabajos.
- Equipo de proyecto. Titulación y experiencia acreditada de los medios humanos asignados al contrato en proyectos similares.

PCP C2017-00108 Página 7 de 7



# 8.2 Proposición económica

La oferta económica, manifestando tomar parte en la licitación, debe realizarse según el modelo que se detalla en el Anexo I.

Gijón, 3 de Octubre de 2017

EL TECNICO DE SISTEMAS DE INFORMACION

Javier González Cotera

## ANEXO I. MODELO DE PROPOSICIÓN ECONÓMICA

D.D <sup>a</sup> , con domicilio en
calle, con NIF nº, en nombre propio/en nombre y representación de la empresa y de la que se indica domicilio social en y CIF nº
vista la licitación convocada por la Sociedad EBHISA para la "REALIZACION DE UN DIAGNOSTICO DE CIBERSEGURIDAD" por procedimiento negociado con publicidad, y enterado de las condiciones y requisitos que se exigen para la adjudicación del servicio, se compromete a la realización del citado servicio por importe de € IVA no incluido (en letra y en cifra), con sujeción a los Pliego de Condiciones, que conoce y acepta expresamente, haciendo constar que no ha presentado más de una proposición en la misma licitación, ya sea individualmente, ya en unión temporal con otro empresario, comprometiéndose además, al riguroso cumplimiento de todas las obligaciones que impone la legislación vigente y en especial las de carácter fiscal, laboral y seguridad social,
En de 2017.
(Fecha y firma del proponente)