LICITACION 02/2019

Elaboración del Plan de Adecuación de los sistemas de información y los tratamientos de datos del Colegio de Ingenieros de Caminos, Canales y Puertos al Esquema Nacional de Seguridad, y su ejecución.

1. PROPÓSITO DE ESTE DOCUMENTO

Los colegios profesionales desde la aprobación de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDyGDD) están obligados a aplicar las medidas de seguridad previstas en el Esquema Nacional de Seguridad (en adelante ENS, según la disposición adicional primera y el artículo 77.1 LOPDyGDD), en relación a los tratamientos de datos personales y cuando las finalidades del tratamiento se relacionen con el ejercicio de potestades de derecho público.

El objetivo de esta convocatoria es seleccionar a un proveedor que lleve a cabo los trabajos necesarios para evaluar el impacto del ENS en la organización y las aplicaciones del Colegio,

determinar los controles y las medidas de seguridad aplicables al Colegio de Ingenieros de Caminos Canales y Puertos, en relación a los tratamientos recogidos en el Registro de Actividades de Tratamiento, disponible en http://www.ciccp.es/rgpd/rat/RAT_Web_v1_0.htm; la redacción de un plan de adecuación al ENS; la elaboración de una Política de Seguridad de la Información y de los documentos necesarios para la adecuación al ENS; la revisión del sistema documental de protección de datos personales a tal fin; y, finalmente, la ejecución del plan.

En este documento se describe de forma general el alcance de los servicios que debe ofertar el futuro proveedor para la adecuación del Colegio al ENS.

2. ESQUEMA DE PLAZOS DEL PROCESO

Evento	Fecha Prevista
Publicación del anuncio	21/01/2019
Fecha límite para la recepción de la oferta	11/02/2019

3. ANTECEDENTES – SITUACIÓN ACTUAL

Hasta la aprobación de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDyGDD) los colegios profesionales no estaban estaba obligados a implementar las medidas de seguridad del Esquema Nacional de Seguridad.

De acuerdo con la disposición adicional primera de la LOPDyGDD, en relación con el artículo 77.1 g LOPDyGDD, los colegios profesionales deben aplicar a los tratamientos de datos personales, cuando las finalidades del tratamiento se relacionen con el ejercicio de potestades de derecho público, las medidas de seguridad que correspondan de las previstas en el Esquema Nacional de Seguridad, así como impulsar un grado de implementación de medidas equivalentes en las empresas o fundaciones vinculadas a los mismos sujetas al Derecho privado.

El Esquema Nacional de Seguridad se regula en el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad.

La Junta de Gobierno del Colegio en su sesión de 26 de noviembre de 2018 acordó evaluar el impacto de la aplicación del Esquema Nacional de Seguridad en la organización y en las aplicaciones del Colegio y solicitar ofertas para la elaboración un Plan de Adecuación del Colegio al Esquema Nacional de Seguridad.

En esa sesión también designó como Responsable de Seguridad de la Información a D. Jesús Martos Ariza y acordó formar a los trabajadores que tengan que ver directa o indirectamente con la seguridad de la información en el Esquema Nacional de Seguridad.

Actualmente el Colegio no tiene adoptada una política expresa de seguridad de la información, tiene elaborado un Registro de Actividades de Tratamiento, con 23 actividades identificadas, disponible en

http://www.ciccp.es/rgpd/rat/RAT_Web_v1_0.htm . De estas actividades unas están relacionadas con el ejercicio de potestades de derecho público y otra responden al ejercicio de funciones privadas.

4. NECESIDADES

El Colegio ha de adecuar su funcionamiento, su sistema de información, las aplicaciones y las actividades de tratamiento al ENS, por lo que necesita evaluar el impacto de la aplicación del ENS, un Plan de Adecuación al ENS e implementarlo.

Toda vez que la estructura, la plantilla, las instalaciones, las aplicaciones respecto de los tratamientos de datos para el ejercicio de funciones públicas y privadas son comunes, la obligación establecida en la LOPDyGDD determina que el ENS y las medidas que implica se apliquen a todas las actividades de tratamiento llevadas por los Colegio.

5. SERVICIOS SOLICITADOS

-Evaluación del impacto del ENS en el Colegio: estudio y diagnóstico del estado actual de la organización en lo que respecta a la gestión de la seguridad de los sistemas de información y de las actividades de tratamiento de datos personales.
- Inventario de la información, de los servicios y de las actividades de tratamiento.
-Categorización de los sistemas, según los criterios el Anexo I del RD 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad.
- Inventario y valoración de activos.
-Análisis GAP o diferencial: determinar qué controles del ENS ya se encuentran implantados en la organización.
-Análisis de riesgos: Identificación y valoración de activos, amenazas, vulnerabilidades, cálculo del riesgo, nivel de riesgo aceptable y riesgo residual. Se hará de acuerdo a la metodología MAGERIT y mediante el uso de la aplicación PILAR o bien las alternativas que proponga el proveedor.
-Redacción del plan de adecuación, con las tareas a realizar y los plazos de ejecución para la completa aplicación de lo exigido por el ENS, contemplando todos los aspectos exigidos en la Guía de Seguridad CCN-STIC 806, documentando cuáles son las medidas del Anexo II del RD 3/2010 que deben ser aplicadas, teniendo en cuenta la categoría de los sistemas y los requisitos planteados para la protección de los datos de carácter personal, así como las insuficiencias del sistema.
-Elaboración de la Política de Seguridad de la Información, cumpliendo los requisitos del ENS y de la normativa de protección de datos.
-Redacción de todos los documentos que sean necesarios para cumplir con el ENS, incluyendo las normativas de seguridad y los procedimientos de seguridad y de gestión del sistema.

-Implantación del Plan de Adecuación siguiendo las pautas de las Guías CCN-STIC 821 y CCN-STIC 822 y sus anexos.
-Realización de acciones formativas a los empleados del Colegio.
-Ejecución de una auditoría interna conforme los aspectos exigidos en la Guía CCN- 802 Auditoria ENS y emisión del informe de auditoría

El proveedor seleccionado para prestar los servicios deberá coordinar sus trabajos con el Responsable de Seguridad de la Información, el Delegado de Protección de Datos y los proveedores de las aplicaciones del Colegio y del centro de proceso de datos.

Para mayor detalle sobre dichos servicios se puede concertar entrevista y contactar con D. Jesús Martos Ariza en la dirección de correo electrónico 17jma@ciccp.es .

6. PLAZO DE PRESTACIÓN DE LOS SERVICIOS

Está previsto que la Junta de Gobierno resuelva sobre la adjudicación en la sesión que prevé celebrar el 25 de febrero de 2019.

El servicio se prestará en el plazo de dos meses desde la firma del contrato. El plazo será un término esencial del contrato, que preverá penalizaciones por el retraso.

7. PRESENTACIÓN DE LA PROPUESTA

Las propuestas deberán presentarse en formato PDF (sin superar 15 páginas) incluyendo todos los servicios solicitados además del escenario económico (precios, hitos de pago…) de la oferta presentada.

La propuesta debe contener un esquema de fases y un cronograma de ejecución y especificar expresamente los documentos entregables.

También deberá incluirse persona de contacto, referencias y cualquier información relevante para la valoración de la oferta.

Las propuestas serán remitidas (**hasta el 11 de febrero de 2019**) a las siguientes direcciones de correo electrónico: secretariogeneral@ciccp.es y 17jma@ciccp.es .

8. PROCESO DE SELECCIÓN. NORMAS APLICABLES.

La contratación se rige por el Reglamento de Régimen Económico y Patrimonial del Colegio de Ingenieros de Caminos, Canales y Puertos, aprobado por el Consejo General del Colegio el 21 de junio de 2018.

La selección del proveedor se llevará a cabo mediante negociación con los proveedores que presenten oferta y es discrecional, atendiendo a la oferta técnica y económicamente más ventajosa.

La participación en el proceso implica la aceptación de las normas aplicables y de la decisión de la selección y de la contratación. La decisión sobre la selección del proveedor no reviste carácter administrativo y no será recurrible.

Con el proveedor seleccionado se formalizará un contrato que será el documento de carácter obligacional que rija la relación entre las partes.

Dicho contrato implicará un acuerdo de encargo del tratamiento de datos personales acorde con la normativa de protección de datos de carácter personal.

En el contrato se someterá a arbitraje de la Corte de Arbitraje del Colegio de Abogados de Madrid la resolución de las controversias que pudieran surgir.

9. DATOS DE CARÁCTER PERSONAL

Los datos personales incluidos en las ofertas podrán ser tratados por el Colegio, con la finalidad de gestionar la selección y, en su caso, la contratación.

El Colegio informa en relación a dicho tratamiento de lo siguiente:

-Finalidades: Gestión de la actividad contractual y convencional del Colegio. Gestión de la relación con proveedores de servicios o productos.

-Legitimación del tratamiento:

RGPD (art. 6.1.a) Consentimiento del interesado.

RGPD (art. 6.1.b) El tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales.

-Cesiones o comunicaciones: No se prevén.

-Derechos: Acceder, rectificar y suprimir los datos, solicitar la portabilidad de los mismos, oponerse al tratamiento y solicitar la limitación de éste. Se pueden ejercer mediante correo electrónico dirigido a: derechosdatos@ciccp.es .