8.3.5. POLÍTICA DE PRIVACIDAD

1. INTRODUCCIÓN

1.1. Objetivo

El objetivo de la presente política es definir el compromiso que los profesionales de la estructura del Colegio de Ingenieros de Caminos, Canales y Puertos (CICCP) deben cumplir en relación con el tratamiento de datos de carácter personal en el desempeño de sus funciones en o para el Colegio, y en el marco en que se establece dicho compromiso.

1.2. Ámbito de aplicación

Esta política es de aplicación a todos/as los/as profesionales que se integran en la estructura del Colegio, en cualquiera de sus centros directivos (Sede Central y Demarcaciones) porque desempeñan cargos o son personal del CICCP, con acceso a la información de la que es responsable el Colegio, y que también puede hacer extensiva, de conformidad con los acuerdos de encargo de tratamiento que se suscriban, a cualquier otro profesional vinculado con el CICCP, colaborador habitual o puntual, cuya actuación pueda afectar de alguna manera a la responsabilidad o reputación del Colegio.

1.3. Normativa

El presente documento está basado en el cumplimiento de la siguiente normativa:

• Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).

• Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

• Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

• Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.

• Ley 19/2013, de 9 de diciembre, de Transparencia, acceso a la información pública y buen gobierno.

• Ley 16/1985, de 25 de junio, del Patrimonio Histórico Español.

1.4. Principios del tratamiento de datos y de la seguridad de la información

El Colegio, su estructura orgánica y plantilla tratarán la información y los datos personales bajo su responsabilidad conforme a los siguientes principios de protección de datos y seguridad de la información:

• Licitud, lealtad y transparencia: los datos de carácter personal serán tratados de manera lícita, leal y transparente en relación con el/la interesado/a.

• Legitimación en el tratamiento de datos personales: sólo se tratarán los datos de carácter personal cuando dicho tratamiento se encuentre amparado en alguna de las causas de legitimación establecidas en los artículos 6 y 9 del RGPD.

• Limitación de la finalidad: los datos de carácter personal serán tratados para el cumplimiento de fines determinados, explícitos y legítimos u no serán tratados ulteriormente de manera incompatible con dichos fines.

• Minimización de datos: los datos de carácter personal serán adecuados, pertinentes y limitados a los necesario en relación con los fines para los que son tratados.

• Limitación del plazo de conservación: los datos de carácter personal serán mantenidos de forma que se permita la identificación de los/as interesados/as durante no más tiempo del necesario para los fines que justificaron su tratamiento.

• Integridad y confidencialidad: los datos de carácter personal serán tratados de tal manera que se garantice su seguridad, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas. Quienes intervengan en el tratamiento de los datos están sujetos.

• Responsabilidad proactiva: el Colegio y su estructura serán responsables del cumplimento de los principios anteriormente señalados y adoptarán las medidas técnicas u organizativas que permitan estar en condiciones de demostrar dicho cumplimiento.

• Atención a los derechos de los/as afectados/as: se adoptarán medidas en la organización que garanticen el adecuado ejercicio de los derechos de acceso, rectificación, supresión, oposición, limitación del tratamiento y portabilidad respecto de sus datos de carácter personal.

• Alcance estratégico: la protección de datos y la seguridad de la información debe contar con el compromiso y apoyo de todos los niveles estratégicos y directivos de forma que pueda estar coordinada e integrada con el resto de las iniciativas estratégicas del Colegio para conformar un todo coherente y eficaz.

• Responsabilidad diferenciada: en los sistemas de información responsabilidad del Colegio se observará el principio de responsabilidad diferenciada de forma que se delimiten las diferentes responsabilidades y roles.

• Seguridad integral: la seguridad tenderá a la preservación de la confidencialidad, la integridad y la disponibilidad de la información, pudiendo, además abarcar otras propiedades como la autenticidad, la responsabilidad, la fiabilidad y el no repudio. La seguridad se entiende como un proceso integral constituido por todos los elementos técnicos, humanos, materiales, organizativos, relacionados con el sistema, evitando, salvo en los casos de urgencia o necesidad, cualquier actuación puntual o tratamiento coyuntural.

• Gestión de Riesgos: la gestión de riesgos es el conjunto de actividades coordinadas que el Colegio desarrolla para dirigir y controlar el riesgo, entendiendo como riesgo el efecto de la incertidumbre sobre la consecución de objetivos que, en el marco del RGPD, es la protección de los derechos y libertades de los titulares de los datos que trata el Colegio. El análisis y la gestión de riesgos con parte especial del proceso de protección de datos y de seguridad de la información del Colegio, de forma que permita el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. La reducción de estos niveles se realizará mediante el despliegue de medidas de seguridad, que establecerá un equilibrio entre la naturaleza de los datos y los tratamientos, el impacto y probabilidad de los riesgos a los que estén expuestos y la eficacia y el coste de las medidas de seguridad. Al evaluar el riesgo el Colegio tendrá en cuenta los riesgos que se derivan para los derechos de las personas con respecto al tratamiento de sus datos personales.

• Proporcionalidad: el Colegio establecerá las medidas de protección, detección y recuperación de forma que resulten proporcionales a los potenciales riesgos y a la criticidad y valor de la información, de los tratamientos de datos personales y de los servicios afectados.

• Proceso de verificación: el Colegio implantará un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad de los tratamientos.

2. OBLIGACIÓN DE CONOCER Y CUMPLIR

Todo profesional del CICCP debe conocer la presente Política y actuar conforme a los principios y comportamientos definidos, comunicando a su responsable directo o director de servicio cualquier duda respecto a su cumplimiento o cualquier indicio de actuación en contra de este.

La presente Política, así como los procedimientos posteriores que de la misma pudieran emanar se encontrarán permanentemente actualizados en la Intranet para ser consultados posteriormente cuando se requiera.

Todos/as los/as directores/as tienen obligación de velar por el cumplimiento de la Política en sus diferentes áreas, liderar su cumplimiento, resolver las dudas o inquietudes que le transmitan los/as profesionales, y establecer los mecanismos que aseguren su cumplimiento contando para ello con el asesoramiento del Delegado de Protección de Datos.

Las dudas sobre seguridad de la información y protección de datos se podrán trasladar al Comité de Seguridad que a su vez podrá trasladarlas al Delegado de Protección de Datos.

El incumplimiento de las normas contenidas en la presente Política estará sujeto a la potestad disciplinaria y sancionadora del CICCP, con sujeción a los principios y reglas previstas por la legislación vigente. Por lo tanto, cualquier incumplimiento relacionado deberá ponerse en conocimiento del Delegado de Protección de Datos. La gestión de dudas e incumplimientos se realizará aplicando rigurosamente los principios de independencia y rigurosidad.

2.1. Compromiso de confidencialidad por escrito

En el marco de la relación que los/as profesionales de la estructura de CICCP con el mismo, aquellos se comprometerán expresamente, en un documento que firmarán a:

• No revelar a persona ajena al CICCP, sin su consentimiento, la información a la que haya tenido acceso en el desempeño de sus funciones en el Colegio, excepto en el caso de que ello sea necesario para dar cumplimiento a las obligaciones propias o de la organización impuestas por las leyes o normas que resulten de aplicación, o cuando sea requerido para ello por mandato de una Autoridad competente con arreglo a Derecho.

• Utilizar la información a que alude el apartado anterior, únicamente en la forma que exija el desempeño de sus funciones en el CICCP y no disponer de ella de ninguna otra forma o finalidad. Está prohibida la copia y envío de cualquier información obtenida o generada como consecuencia del trabajo para fines distintos de este.

• No utilizar en forma alguna, cualquier otra información que hubiese podido obtener prevaliéndose de su condición de profesional de la estructura del Colegio y que no sea necesaria para el desempeño de sus funciones en el CICCP.

• Cumplir en el desarrollo de sus funciones en el CICCP con la normativa vigente nacional y comunitaria, relativa a la protección de datos de carácter personal, y en particular con el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales y cualquier otra que la sustituya o complemente en el futuro.

• Cumplir las Políticas de Seguridad de la Información y sus sistemas, así como del correo electrónico y otros sistemas de comunicación, los procedimientos que establezca y le comunique la dirección de la Corporación.

• No hacer uso personal de los sistemas y equipos de información titularidad del Colegio que interfiera con sus funciones en la estructura del Colegio, de los/as demás trabajadores/as o de la Corporación.

• En internet, adoptar las precauciones oportunas para proceder a la descarga de archivos, asegurándose, antes de hacerlo, de la confianza o acreditación del sitio web desde el que se realizará.

• Cumplir los compromisos anteriores incluso después de extinguida, por cualquier casusa, la relación que le une con el CICCP.

• Asumir las consecuencias del incumplimiento de los anteriores compromisos, conociendo que la infracción de los deberes adquiridos puede dar lugar a sanciones conforme al RGPD y a sanción disciplinaria laboral o deontológica, si corresponde, y a responsabilidad civil y penal.

Están sujetos a un compromiso de confidencialidad escrito además de a los empleados/as los siguientes colectivos:

- Órganos de gobierno del Colegio y las Demarcaciones
- Miembros del Consejo General
- Representantes internacionales.
- Miembros de Comisiones, Comités, Grupos de Trabajo.

Para regular el compromiso de confidencialidad con los colectivos referenciados, el CICCP dispone de un documento especifico.

2.2. Uso de los medios digitales del colegio por los empleados

Los/as trabajadores/as deberán cumplir las políticas o instrucciones de uso aceptable o de seguridad de la información y sus sistemas, así como el correo electrónico y otros sistemas de comunicación, que establezca y le comunique la dirección del Colegio. No deberán hacer un uso personal de los sistemas y equipos de información titularidad del CICCP que interfiera con el trabajo del empleado/a, de los/as demás trabajadores/as o de la Corporación. Los/as trabajadores/as serán informados/as de que no se permite el acceso a páginas web no ligadas al trabajo como páginas de chat, redes sociales no profesionales, juegos, juegos de azar, viajes, compras por Internet, venta de acciones, de contenido ilegal o de carácter pornográfico, etc. También está prohibido expresamente la difusión y descarga de material ilegal, vulnerador de derechos, así como el uso, la copia o envío ilegal de software o material que esté protegido por leyes protectoras de la propiedad intelectual o industrial. En internet, deberán adoptar las precauciones oportunas antes de proceder a la descarga de archivos asegurándose, antes de hacerlos, de la confianza o acreditación del sitio web desde el que se realizará.

El Colegio podrá acceder a los contenidos derivados del uso de medios digitales facilitados a los/as trabajadores/as a los efectos de controlar el cumplimiento de las obligaciones laborales o estatutarias y de garantizar la integridad de dichos dispositivos.

Por todo ello, ningún/a trabajador/a del CICCP puede esperar a que sus comunicaciones con medios del Colegio o uso de los sistemas informáticos del Colegio sean confidenciales, ni tampoco privados, estando sometidos al control del empleador.

El/la trabajador/a será informado que en los equipos y sistemas informáticos propiedad de CICCP se podrán instalar aplicaciones que analicen el tráfico enviado y recibido de Internet y lo

permita o prohíba en función de una serie de reglas específicas definidas por los administradores de los sistemas.

2.3. Decálogo de buenas prácticas

Los principios y obligaciones básicas de los/as empleados/as se recogerán en un documento denominado Decálogo de Buenas Prácticas de Protección de Datos, que será difundido periódicamente entre los/as empleados/as, así como actualizado.

En el ANEXO A que recogen las CUESTIONES RELATIVAS AL PERSONAL

3. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

La seguridad de la información se rige por la Política de Seguridad de la Información del CICCP, acorde con las medidas de seguridad del Esquema Nacional de Seguridad, y una serie de documentos, procedimientos y medidas de desarrollo de la misma (Normativa de Seguridad; Procedimientos de Seguridad; Procesos de Autorización; Medidas de Seguridad del Marco Operacional y de Protección), que las personas responsables de su aplicación deben conocer.

La seguridad de los sistemas estará atendida, revisada y auditada por personal cualificado, dedicado e instruido en todas las fases de su ciclo de vida: instalación, mantenimiento, gestión de incidencias y desmantelamiento.

El personal del Colegio recibirá la formación específica necesaria para garantizar la seguridad de las tecnologías de la información aplicables a los sistemas y servicios del Colegio.

La Política de Seguridad se encuentra a disposición de los interesados en el Portal de Transparencia de la página web del Colegio.

4. SISTEMA DOCUMENTAL DE PROTECCIÓN DE DATOS

El sistema documental de protección datos del CICCP recoge de forma ordenada los documentos que sobre la protección de datos de carácter personal genera el CICCP como responsable de tratamiento de datos de carácter personal para cumplir con el RGPD; la LOPDGDD y la normativa que pueda dictarse en su desarrollo.

El Colegio, como responsable de tratamiento de datos de carácter personal, es responsable del cumplimiento de los principios del RGPD y de la LOPDGDD y de las obligaciones que le incumben, y ha de ser capaz de demostrarlo de acuerdo con el principio de responsabilidad proactiva.

El sistema documental de protección de datos está bajo la custodia del CICCP y en particular del Secretario General del CICCP.

El sistema documental se compone de:

- Documentos Públicos (publicados en la web de transparencia en (http://www3.ciccp.es/transparencia/)
• Registro de Actividades de Tratamiento (RAT)
• Políticas de Seguridad (modelos y procedimientos)

- Documentos Internos (Intranet del Colegio para empleados)
• Documentación para empleados (Obligaciones / Buenas prácticas / Ejercicio de derechos/ Actuación ante brechas de seguridad detectadas)
Documentos Privados (únicamente a disposición del comité de seguridad)
• Política de Privacidad. Documento general que incluye la totalidad de anexos y procedimientos

5. TRATAMIENTO DE DATOS PERSONALES

5.1. Contenido

Se entiende por “datos personales” toda aquella información sobre una persona física identificada o identificable (“el/la interesado/a”). Se considera persona física identificable toda persona cuya identidad pueda determinarse directa o indirectamente, en particular mediante un identificador, como por ejemplo, un número de identificación (DNI, nº de la Seguridad Social), datos de localización (ej.: domicilio), un identificador en línea (ej.: cuentas de correo electrónico), o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural, social de dicha persona (ej.: datos biométricos). En adelante, “Datos personales”.

Ejemplos de datos personales serían el nombre completo, número de DNI o pasaporte, dirección profesional o personal, nacionalidad, profesión, datos financieros, de salud, genéticos, biométricos, de una persona física identificada o identificable.

5.2. Alcance

Únicamente aplica a las personas físicas, ya que la citada normativa no resultaría aplicable a los datos de las personas jurídicas.

5.3. Formato de los datos

Para que los datos se consideren como de carácter personal, es indiferente el formato en el que se faciliten, ya sea en formato electrónico/digital de cualquier tipo (Excel, Word, Access, Power Point, aplicación, archivo de audio o vídeo, etc.) o formato físico (documento en papel, fotografías, etc.

Las medidas de seguridad implementar variarán en función del formato en que los datos estén disponibles.

5.4. Registro de actividades de tratamiento – Uso de datos

El Colegio mantendrá actualizado el Registro de Actividades de Tratamiento con datos de carácter personal de las que sea responsable, que incluirá toda la información a la que se refiere el artículo 30 del RGPD.

Las finalidades que habilitan el tratamiento de datos de carácter personal son las contenidas en cada actividad de la recogida en el Registro de Actividades de Tratamiento.

El Registro de Actividades de Tratamiento se mantendrá continuamente actualizado y podrá consultarse en la página web del Colegio, de conformidad con lo dispuesto en la LOPDGDD. Cualquier duda sobre las finalidades del tratamiento se planteará al Delegado de Protección de Datos.

Los datos personales han de ser adecuados, pertinentes y no excesivos con relación a la finalidad para la que se recogen. No se recabarán más datos de los necesarios y no se utilizarán datos personales recogidos para finalidades distintas y/o incompatibles con aquellas para las que se recogieron.

5.5. Habilitación para el tratamiento de datos. Recogida de datos. Gestión del consentimiento.

Se considera tratamiento cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de estos, ya sea por procedimientos manuales, automatizados, o mixtos, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo, interconexión, limitación, supresión o destrucción.

Se entiende que existe tratamiento de datos personales desde que se conocen o se dispone de acceso de visualización a dichos datos, incluso si es un acceso potencial (es decir, se pueda o no, desde el momento que se puede acceder, se está produciendo un tratamiento de datos personales).

La habilitación o legitimación para el tratamiento de datos personales se fundará en alguna de las causas de legitimación establecidas en los artículos 6 y 9 del RGPD.

Las concretas habilitaciones para cada una de las actividades de tratamiento que lleva a cabo el Colegio son las recogidas en su documento “Registro de Actividades de Tratamiento”

El CICCP no recabará datos de carácter personal de los interesados/as sin su conocimiento. La inclusión de datos en formularios será voluntaria y debidamente anunciada, mostrándose las pertinentes cláusulas informativas conformadas en dos capas. Las capas informativas y sus niveles de detalle tendrán el contenido indicado por la Guía para el cumplimiento del deber de Informar (2018) editada por la AEPD.

Siempre que se recaben datos se informará por escrito, o mediante locución si se recaban telefónicamente, con la primera capa de información básica, en forma de tabla, con los epígrafes de “responsable”; ”finalidades”; “legitimación”; “cesiones/destinatarios”; y “derechos”, donde se informará de que se pueden ejercer los derechos en mediante correo electrónico a derechosdatos@ciccp.es , poniéndose en contacto con el Delegado de Protección de Datos del CICCP mediante correo electrónico dirigido a dpo@ciccp.es o bien mediante comunicación escrita con acuse de recibo a c/ Almagro, 42 – 1ª Planta ,Madrid 28010.

Se añadirá, en su caso, el epígrafe “procedencia” únicamente cuando los datos no procedan del propio interesado/a. También se indicará la fecha de la versión de la cláusula y habrá una extensión de la información (+info), con los dos enlaces, uno a la segunda capa detallada, con información adicional, otro a un extracto del Registro de Actividades de Tratamiento.

Los datos de carácter personal que se pudieran recabar directamente del interesado/a de forma informada quedarán incorporados a la correspondiente actividad de tratamiento titularidad del CICCP.

Cuando la legitimación del tratamiento se base en el consentimiento y haya que recabar éste se podrán utilizar los métodos establecidos en los Procedimientos de Obtención y Conservación del Consentimiento, que forman parte del sistema documental de protección de datos de carácter personal del CICCP y se identificará por actividades del tratamiento los sistemas utilizados en cada caso, guardando el debido registro de la prestación del consentimiento, de los datos proporcionados y de las cláusulas informativas mostradas.

El procedimiento de obtención y gestión del consentimiento se incluye como ANEXO B.

5.6. Forma de acceso

Para considerar que se está realizando un tratamiento de datos personales, es indiferente la forma en la que se tenga acceso a los mismos (ya sea en formato electrónico/digital o en formato físico), de modo que se deberá cumplir con el procedimiento establecido en todos los casos.

Del mismo modo, se está ante un tratamiento de datos personales si el acceso a los mismos se produce incorporando dichos datos a los sistemas informáticos o instalaciones del CICCP.

5.7. Nivel de seguridad

Los/as profesionales de la estructura de CICCP deben conocer y aplicar las medidas de seguridad conforme al ENS, que se recogen en el Registro de Actividades de Tratamiento y en el sistema de seguridad de la información.

Para conocer más acerca de los niveles de seguridad en materia de protección de datos personales se deberá contactar con el Comité de Seguridad.

5.8. Política de tratamiento de datos de carácter personal y de privacidad

La "Política de Privacidad web", documento que se integra dentro del sistema documental de protección de datos de carácter personal del CICCP y está orientado a cumplir con el deber de información en relación a toda la actividad del Colegio como segunda capa complementaria al resto de cláusulas informativas a las que se ha aludido en epígrafes anteriores. En dicha política se integrará también el tratamiento de cookies.

La política de tratamiento de datos de carácter personal y de privacidad web deberán ser conocidas por las personas de la estructura del Colegio y se publicará para general conocimiento en la página web.

5.9. Periodo de conservación. Bloqueo de datos. Patrimonio documental

Según la normativa de protección de datos, los datos personales se conservarán mientras dure la finalidad para la cual fueron recogidos. En el Registro de Actividades de Tratamiento consigna los plazos o criterios.

Posteriormente se conservarán debidamente bloqueados. El bloqueo de los datos consiste en la identificación y reserva de los mismos, adoptando medidas técnicas y organizativas, para impedir su tratamiento incluyendo su visualización, excepto para la puesta a disposición de los datos a jueces y tribunales, el Ministerio Fiscal o las Administraciones Públicas competentes, en particular de las autoridades de protección de datos, para la exigencia de posibles responsabilidades derivadas del tratamiento y sólo por el plazo de prescripción de las mismas. Transcurrido ese plazo deberá procederse a la destrucción de los datos.

Los datos bloqueados no podrán ser tratados para ninguna finalidad distinta de la señalada. Para la eliminación de documentos con datos personales, que nos sean copias auxiliares, las personas de la estructura del Colegio consultarán previamente con el Comité de Seguridad el procedimiento a seguir.

Dichos criterios deberán ser tenidos en cuenta por el colegio a la hora de facilitar el ejercicio de los derechos de conformidad con el procedimiento establecido al efecto.

Los criterios de conservación de los/as Colegiados/as definidos por CICCP se incluyen en el ANEXO C

5.10. Destinatarios de los datos

Los datos podrán ser cedidos o comunicados a otros destinatarios según las habilitaciones previstas en el RGPD. Las concretas cesiones o comunicaciones son las que se recogen en el Registro de Actividades de Tratamiento para cada actividad de y todas ellas deben figurar en las cláusulas informativas y de recogida del consentimiento cuando éste sea el fundamento legitimador del consentimiento.

5.11. Derechos de información los interesados

El derecho a la información es el derecho que tienen los interesados a ser informados por el responsable acerca de los fines y demás circunstancias del tratamiento de sus datos. Por tanto, al derecho de información de los interesados le corresponde un correlativo deber de información a cargo del responsable del tratamiento.

De acuerdo a la normativa de protección de datos, el interesado tiene, además, un derecho a la transparencia de toda información recibida del responsable sobre el tratamiento de sus datos, de manera que dicha información le sea facilitada en forma concisa, transparente, inteligible y de fácil acceso, utilizando un lenguaje claro y sencillo.

Requisitos establecidos para cumplir con el derecho de información

Conforme a la normativa, será necesario informar sobre los siguientes extremos:

Cuando los datos personales se obtengan directamente del propio interesado, el responsable del tratamiento, en el momento en que estos se obtengan, le facilitará toda la información indicada a continuación:

a) la identidad y los datos de contacto del responsable y, en su caso, de su representante;

b) los datos de contacto del Delegado de Protección de Datos, en su caso;

c) los fines del tratamiento a que se destinan los datos personales y la base jurídica del tratamiento;

d) en su caso, los intereses legítimos del responsable o de un tercero en que se base el tratamiento;

e) los destinatarios o las categorías de destinatarios de los datos personales, en su caso;

f) en su caso, la intención del responsable de transferir datos personales a un tercer país u organización internacional y la existencia o ausencia de una decisión de adecuación de la Comisión Europea o, en caso de transferencias basadas en los arts. 46, 47 o 49 (apdo. 1, párrafo 2º), referencia a las garantías adecuadas;

g) el plazo durante el cual se conservarán los datos personales o, cuando no sea posible, los criterios utilizados para determinar este plazo;

h) la existencia del derecho a solicitar al responsable del tratamiento el acceso a los datos personales relativos al interesado, y su rectificación o supresión, o la limitación de su tratamiento, o a oponerse al tratamiento, así como el derecho a la portabilidad de los datos;

i) cuando el tratamiento esté basado en el consentimiento, la existencia del derecho a retirar el consentimiento en cualquier momento, sin que ello afecte a la licitud del tratamiento basado en el consentimiento previo a su retirada;

j) el derecho a presentar una reclamación ante una autoridad de control;

k) si la comunicación de datos personales es un requisito legal o contractual, o un requisito necesario para suscribir un contrato, y si el interesado está obligado a facilitar los datos personales y está informado de las posibles consecuencias de que no facilitar tales datos;

l) la existencia de decisiones automatizadas, incluida la elaboración de perfiles, y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado.

Cuando los datos personales no se obtengan directamente del interesado, el responsable del tratamiento le facilitará la información indicada en el apartado anterior y, además, la siguiente información:

a) las categorías de datos personales de que se trate;

b) la fuente de la que proceden los datos personales y, en su caso, si proceden de fuentes de acceso público;

En este caso, el responsable del tratamiento facilitará la información indicada:

• dentro de un plazo razonable, una vez obtenidos los datos personales, y a más tardar dentro de un mes, habida cuenta de las circunstancias específicas en las que se traten dichos datos;

• si los datos personales han de utilizarse para comunicación con el interesado, a más tardar en el momento de la primera comunicación a dicho interesado, o

• si está previsto comunicarlos a otro destinatario, a más tardar en el momento en que los datos personales sean comunicados por primera vez.

Cuando el responsable del tratamiento proyecte el tratamiento ulterior de los datos personales para un fin que no sea aquel para el que se obtuvieron, proporcionará al interesado, antes de dicho tratamiento ulterior, información sobre ese otro fin y cualquier otra información pertinente.

Las disposiciones anteriores no serán aplicables cuando y en la medida en que:

a) el interesado ya disponga de la información;

b) la comunicación de dicha información resulte imposible o suponga un esfuerzo desproporcionado, en particular para el tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, a reserva de las condiciones y garantías indicadas en el artículo pueda imposibilitar u obstaculizar gravemente el logro de los objetivos de tal tratamiento. En tales casos, el responsable adoptará

medidas adecuadas para proteger los derechos, libertades e intereses legítimos del interesado, inclusive haciendo pública la información;

c) la obtención o la comunicación esté expresamente establecida por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento y que establezca medidas adecuadas para proteger los intereses legítimos del interesado, o

d) cuando los datos personales deban seguir teniendo carácter confidencial sobre la base de una obligación de secreto profesional regulada por el Derecho de la Unión o de los Estados miembros, incluida una obligación de secreto de naturaleza estatutaria.

Las cláusulas informativas del CICCP se encuentran en el ANEXO D

5.12. Encargados del tratamiento

Un encargado del tratamiento es una persona o entidad que presta un servicio al responsable, que conlleva necesariamente el tratamiento de datos personales por cuenta de éste.

El RGPD establece 2 obligaciones fundamentales en la relación establecida entre responsable-encargado:
• Diligencia del CICCP en la elección del encargado;
• Formalización de la relación entre el Colegio-y los encargados mediante contrato escrito.

5.12.1. Diligencia en la elección de encargado

La primera obligación del Colegio en cuanto a su relación con un encargado del tratamiento es previa a su contratación. De hecho, dicha obligación consiste en elegir únicamente un encargado que ofrezca garantías suficientes de que, a la hora de tratar los datos por cuenta del responsable, aplicará medidas técnicas y organizativas de conformidad al RGPD, garantizando los derechos de las personas afectadas.

Por tanto, se exige al responsable un deber de diligencia en la elección del encargado. En este sentido, es importante subrayar que por el hecho de que el Colegio contrate un servicio a un encargado que conlleva el tratamiento de datos personales, el primero no pierde la consideración de responsable, por lo que responderá ante el interesado titular de los datos de cualquier irregularidad cometida por el encargado en dicho tratamiento de datos.

Para cumplir con esta obligación de diligencia, antes de contratar al encargado, CICCP deberá solicitarle documentalmente evidencias que acrediten las medidas adoptadas para cumplir con las disposiciones del RGPD, en relación al tratamiento a realizar por cuenta del responsable. Otra manera de demostrar las garantías exigidas por el RGPD se produce cuando el encargado pueda acreditar su adhesión a códigos de conducta (art. 40 RGPD) u obtener una certificación (art. 42 RGPD).

Es importante subrayar que el deber de diligencia se extiende igualmente al encargado cuando subcontrate cualquier operación de tratamiento con otro subencargado.

5.12.2. Formalización de contrato escrito

El artículo 28 del RGPD establece que la relación entre responsables y encargados deberá formalizarse mediante un contrato o acto jurídico que vincule a ambos.

En este sentido, contamos con el documento “Directrices para la elaboración de contratos entre responsables y encargados del tratamiento” de la AEPD. Como mínimo, dicho contrato deberá establecer el objeto, la duración, la naturaleza y la finalidad del tratamiento, el tipo de datos personales y categorías de interesados, y las obligaciones y derechos del responsable. En particular, el contrato incluirá:

El artículo 28 del RGPD establece que la relación entre responsables y encargados deberá formalizarse mediante un contrato o acto jurídico que vincule a ambos.

En este sentido, contamos con el documento “Directrices para la elaboración de contratos entre responsables y encargados del tratamiento” de la AEPD. Como mínimo, dicho contrato deberá establecer el objeto, la duración, la naturaleza y la finalidad del tratamiento, el tipo de datos personales y categorías de interesados, y las obligaciones y derechos del responsable. En particular, el contrato incluirá:

• Instrucciones del responsable del tratamiento: es necesario identificar de forma clara cuáles son los tratamientos a realizar por el encargado, atendiendo al tipo de servicio prestado y a la forma de prestarlo.

• Deber de confidencialidad: el encargado debe garantizar que las personas autorizadas para el tratamiento se han comprometido a respetar un deber de confidencialidad en el tratamiento de los datos.

• Medidas de seguridad: se debe establecer la obligación del encargado de adoptar todas las medidas de seguridad necesarias, de conformidad con el artículo 32 RGPD.

• Régimen de subcontratación: el RGPD exige autorización previa por escrito del responsable del tratamiento para que el encargado pueda recurrir a otro encargado (subencargado), para desarrollar total o parcialmente el servicio o tratamiento encomendado. La autorización puede ser específica o general. El subencargado, en todo caso, debe estar sujeto a las mismas condiciones que el encargado (instrucciones, obligaciones, medidas de seguridad, etc.), y en la misma forma (formalizando contrato escrito con el encargado).

• Derechos de los interesados: hay que establecer la forma en la que el encargado, en su caso, asistirá al responsable en el cumplimiento de la obligación de responder a las solicitudes de ejercicio de los derechos del interesado.

• Violaciones de seguridad: debe regularse el deber del encargado de informar al responsable de toda brecha de seguridad detectada respecto del tratamiento de los datos personales a su cargo.

• Destino de los datos: hay que prever si, una vez finalice la prestación de servicios, debe el encargado suprimir los datos o devolvérselos al responsable, a elección de éste.

• Colaboración del encargado: el contrato debe reflejar la obligación del encargado de poner a disposición del responsable toda la información necesaria para demostrar el cumplimiento de sus obligaciones, incluso para permitir la realización de auditorías.

De acuerdo a la LOPDGDD, los contratos de encargo formalizados antes del 25/05/2018 al amparo de la normativa anterior, mantienen su vigencia hasta la fecha de vencimiento señalada en los mismos y, en caso de haberse pactado con duración indefinida, hasta el 25/05/2022. No obstante, durante dichos plazos cualquiera de las partes puede exigir a la otra la modificación del contrato para adaptarlo a la nueva normativa.

Los modelos de contrato utilizado por CICCP para regular el tratamiento de datos con sus proveedores se encuentra en el ANEXO E

5.13. Derechos de los/as interesados/as

Los derechos reconocidos en los artículos 15 a 22 del RGPD podrán ejercerse directamente o por medio de representante legal o voluntario. Los/as titulares de la patria potestad podrán ejercitar en nombre y representación de los menores de catorce años los derechos de acceso, rectificación, supresión, limitación del tratamiento, oposición y portabilidad o cualesquiera otros que pudieran corresponderles en el contexto de la normativa sobre protección de datos de carácter personal.

Cualquier persona tiene derecho a obtener confirmación sobre si el CICCP trata datos que le concierne, o no.

Las personas interesadas tienen derecho a acceder a sus datos personales y a obtener una copia de los datos personales objeto de tratamiento, a actualizarlos, así como a solicitar la rectificación de los datos inexactos, o en su caso, solicitar su supresión cuando, entre otros motivos, los datos ya no sean necesarios para los fines para los que fueron recogidos.

En determinadas circunstancias previstas en el art. 18 del RGPD, los/as interesados/as podrán solicitar la limitación del tratamiento de sus datos, en cuyo caso únicamente el Colegio los conservará para el ejercicio o la defensa de reclamaciones.

Como consecuencia de la aplicación del derecho a la supresión u oposición al tratamiento de datos personales en el entorno online, los/as interesados/as tienen derecho al olvido según la jurisprudencia del Tribunal de Justicia de la Unión Europea.

Los/as interesados/as podrán oponerse al tratamiento de sus datos con fines de mercadotecnia, incluida la elaboración de perfiles. En particular los colegiados tienen derecho a que el Colegio indique gratuitamente respecto de los datos personales que se publican en la ventanilla única que no puede utilizarse para fines de publicidad o prospección comercial.

En virtud del derecho de portabilidad, los/as interesados/as tienen derecho a obtener los datos personales que les incumben en un formato estructurado de uso común y lectura mecánica y a transmitirlos a otro responsable.

Todo interesado/a tiene derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar, salvo las excepciones previstas en el art. 22.1 del RGPD. El Colegio no trata datos adoptando decisiones automatizadas sin intervención humana.

El / la interesado/a tiene derecho a la supresión de sus datos, por la desaparición de la finalidad que motivó el tratamiento o la recogida, por revocación del consentimiento cuando sea éste el que legitime el tratamiento, o por el resto de motivos contenidos en el art. 17 RGPD.

5.14. Atención a los derechos de los/las interesados/as

El CICCP tiene establecido un procedimiento sencillo de ejercicio de los derechos de protección de datos de carácter personal, disponiendo de una dirección de correo electrónico para el ejercicio de derechos derechosdatos@ciccp.es, definido en el documento "Procedimiento para el ejercicio de derechos" que todos/as los/as empleados/as del Colegio deben conocer y aplicar. Cualquier petición de ejercicio de derechos de protección de datos recibida en el Colegio por cualquier vía o canal se remitirá por los/as empleados/as del Colegio a derechosdatos@ciccp.es

Esta norma se incluirá en el decálogo de protección de datos para empleados/as.

En el caso de los Colegiados, podrán presentar sus solicitudes de ejercicio de derechos a través de su área privada en la sede electrónica, por ello, las comunicaciones en este sentido se realizarán a través de esta vía.

Se responderá a las solicitudes de el resto de los/as interesados/as, por correo electrónico con confirmación de lectura si la solicitud se ha recibido por ese medio o por correo postal certificado con acuse de recibo si la solicitud se ha recibido por medios diferentes al correo electrónico, sin dilación indebida y a más tardar en el plazo de un mes.

La prueba del cumplimiento del deber de responder a la solicitud de ejercicio de derechos formulando por el/la afectado/a recae sobre el Colegio por lo que se conservará copia de todas las respuestas y de la justificación de envío y recepción.

El procedimiento para el ejercicio de derechos se encuentra en el ANEXO F.

5.15. Gestión de brechas de seguridad

El procedimiento para la gestión de brechas de seguridad, que se integra en el sistema documental de protección de datos, se establece con la finalidad de la correcta identificación, registro y resolución, con minimización de daños, de las brechas de seguridad que afecten a los datos de carácter personal.

La gestión de la brecha se realizará según el procedimiento establecido por el que se rige el Colegio, que contempla aspectos de prevención, detección y corrección, para conseguir que las amenazas sobre la información no se materialicen y, si ello sucede, no afecten gravemente a la información que maneja o a los servicios que se prestan por CICCP.

La existencia de este procedimiento se hará constar en el decálogo de buenas prácticas en protección de datos dirigido a los/as empleados/as del Colegio, a los que se instruirá en cómo actuar ante brechas de seguridad y de las responsabilidades que correspondan.

El procedimiento de brechas de seguridad se encuentra en el ANEXO G.

5.16. Transparencia y acceso a la información pública

El Colegio está sometido a la Ley 19/2013, de 9 de diciembre, de Transparencia, acceso a la información pública y buen gobierno. De conformidad con la Guía de Transparencia (2016), editada por el Consejo de Transparencia y Buen Gobierno y Unión Profesional, la publicidad activa alcanza:

• A las funciones que desarrolla la Corporación, la normativa que les sea de aplicación, así como a su estructura organizativa. A estos efectos, incluirán un organigrama actualizado que identifique a los/as responsables de la Junta de Gobierno y su perfil y trayectoria profesional.

• La siguiente información económica:

o Contratos: deberán ser objeto de publicación, de oficio, los contratos sujetos a derecho administrativo, previstos en la Ley de Contratos del Sector Público, cuyo objeto sea la proyección del ejercicio de una función pública. Respecto de estos contratos, y siguiendo lo expresamente previsto por la Ley de Transparencia, se publican los siguientes aspectos:
- Objeto
- Duración
- Importe de la licitación y de adjudicación
- Procedimiento utilizado para su celebración e instrumentos de publicidad
- Número de licitadores y la identidad del adjudicatario
- Modificaciones, desistimiento y renuncia.

o Convenios: deberán publicarse los convenios firmados por CICCP en ejercicio de las funciones públicas que le hayan sido conferidas. Dicha publicidad incluirá los siguientes conceptos:
- Partes firmantes
- Objeto
- Plazo de duración
- Modificaciones realizadas
- Obligaciones, incluidas también en caso de que las hubiera, las económicas derivadas de los mismos.

o Encomiendas de gestión: en caso de que la corporación de derecho público, en ejercicio de las funciones públicas que desempeñe, realice una encomienda de gestión, esta deberá ser publicada con los siguientes datos:
- Objeto
- Presupuesto
- Duración
- Obligaciones económicas
- Subcontrataciones que eventualmente se realicen con mención a los adjudicatarios, procedimiento seguido para la adjudicación y su importe.

La publicación de esta información al amparo de la Ley de Transparencia y Buen Gobierno se hará teniendo en cuenta el derecho a la protección de datos. Si hubiera datos de categorías especiales (de conformidad con el art. 9 RGPD) no se publicarán estos.

Respecto a la publicación de la información de carácter personal contenida en los contratos y convenios que sean publicados, debe atenerse a lo dispuesto en el criterio interpretativo nº 4 de 2015 firmado conjuntamente por el Consejo de Transparencia y Buen Gobierno y la Agencia Española de Protección de Datos (no publicación del nº de DNI ni de la firma manuscrita).

En cuanto al derecho de acceso a la información pública referida al ejercicio de funciones públicas, si la información solicitada contuviera datos de carácter personal de categorías especiales (art. 9 RGPD) el acceso únicamente se podrá autorizar en caso de que se contase con el consentimiento expreso y por escrito del afectado, a menos que dicho afectado hubiese hecho manifiestamente públicos los datos con anterioridad a que se solicitase el acceso.

Si la información incluyese datos personales que hagan referencia al origen racial, a la salud o a la vida sexual, incluyese datos genéticos o biométricos o contuviera datos relativos a la comisión de infracciones penales o administrativas que no conllevasen la amonestación pública al infractor, el acceso solo se podrá autorizar en caso de que se cuente con el consentimiento expreso del afectado o si aquel estuviera amparado por una norma con rango de ley.

Con carácter general, y salvo que en el acceso concreto prevalezca la protección de datos personales u otros derechos constitucionalmente protegidos sobre el interés público en la divulgación que lo impida, se concederá el acceso a la información que contenga los datos meramente identificativos relacionados con la organización, funcionamiento o actividad pública del Colegio.

Cuando la información solicitada no contuviera datos especialmente protegidos, el órgano al que se dirija la solicitud concederá el acceso previa ponderación suficientemente razonada del interés público en la divulgación de la información y los derechos de los afectados cuyos datos aparezcan en la información solicitada, en particular su derecho fundamental a la protección de datos de carácter personal.

Para la realización de la citada ponderación, dicho órgano tomará particularmente en consideración los siguientes criterios:

a) El menor perjuicio a los afectados derivados del transcurso de los plazos establecidos en el artículo 57 de la Ley 16/1985, de 25 de junio, del Patrimonio Histórico Español.

b) La justificación por los solicitantes de su petición en el ejercicio de un derecho o el hecho de que tengan la condición de investigadores y motiven el acceso en fines históricos, científicos o estadísticos.

c) El menor perjuicio de los derechos de los afectados en caso de que los documentos únicamente contuviesen datos de carácter meramente identificativo de aquéllos.

d) La mayor garantía de los derechos de los afectados en caso de que los datos contenidos en el documento puedan afectar a su intimidad o a su seguridad, o se refieran a menores de edad.

5.17. Evaluación de impacto relativa a la protección de datos

Una Evaluación de Impacto relativa a la protección de datos (EIPD) es un proceso en el que, por un lado, se analizan los riesgos que un producto o servicio puede implicar para la protección de datos de los afectados y, por otro, se gestionan dichos riesgos mediante la adopción de las medidas necesarias para eliminarlos o mitigarlos. Se trata, por tanto, de una metodología que evalúa el impacto en la privacidad de un proyecto, programa, servicio, producto o cualquier iniciativa que implique el tratamiento de datos personales, y adopta las medidas necesarias para evitar o minimizar los impactos negativos.

En el Reglamento General de Protección de datos se establece que existirá la obligación de realizar una Evaluación de Impacto cuando el tratamiento entrañe un alto riesgo para los derechos y libertades de las personas físicas.

El análisis de la necesidad de llevar a cabo Evaluaciones de Impacto relativas a la protección de datos se encuentra en el ANEXO H.

5.18. Delegado de Protección de Datos

En cumplimiento de lo establecido en la normativa de protección de datos, el CICCP procedió a la designación de Don Alberto Pecci como Delegado de Protección de Datos por acuerdo de la Junta de Gobierno de fecha ____

6. GOBIERNO DEL MODELO

6.1. Titularidad

La aprobación de este documento y sus modificaciones corresponde a la Junta de Gobierno del Colegio de Ingenieros de Caminos, Canales y Puertos.

La aprobación de los Anexos y sus modificaciones corresponde al Secretario General del Colegio.

6.2. Interpretación

Corresponde al Secretario General, asesorado por el Delegado de Protección de Datos y la Dirección Jurídica la interpretación de esta Política.

6.3. Validez y revisión

Este modelo entrará en vigor desde la fecha de su aprobación y publicación. Su contenido será objeto de revisión periódica, realizándose los cambios o modificaciones que se consideren convenientes.

ANEXOS

ANEXO A.
CUESTIONES RELATIVAS AL PERSONAL

Todo profesional del CICCP debe conocer la presente Política y actuar conforme a los principios y comportamientos definidos, comunicando a su responsable directo o director de servicio cualquier duda respecto a su cumplimiento o cualquier indicio de actuación en contra de este.

La presente Política, así como los procedimientos posteriores que de la misma pudieran emanar se encontrarán permanentemente actualizados en la Intranet para ser consultados posteriormente cuando se requiera.

Todos/as los/as directores/as tienen obligación de velar por el cumplimiento de la Política en sus diferentes áreas, liderar su cumplimiento, resolver las dudas o inquietudes que le transmitan los/as profesionales, y establecer los mecanismos que aseguren su cumplimiento contando para ello con el asesoramiento del Delegado de Protección de Datos.

Las dudas sobre seguridad de la información y protección de datos se podrán trasladar al Comité de Seguridad que a su vez podrá trasladarlas al Delegado de Protección de Datos.

El incumplimiento de las normas contenidas en la presente Política estará sujeto a la potestad disciplinaria y sancionadora del CICCP, con sujeción a los principios y reglas previstas por la legislación vigente. Por lo tanto, cualquier incumplimiento relacionado deberá ponerse en conocimiento del Delegado de Protección de Datos. La gestión de dudas e incumplimientos se realizará aplicando rigurosamente los principios de independencia y rigurosidad.

Compromiso de confidencialidad por escrito

En el marco de la relación que los/as profesionales de la estructura de CICCP con el mismo, aquellos se comprometerán expresamente, en un documento que firmarán a:

• No revelar a persona ajena al CICCP, sin su consentimiento, la información a la que haya tenido acceso en el desempeño de sus funciones en el Colegio, excepto en el caso de que ello sea necesario para dar cumplimiento a las obligaciones propias o de la organización impuestas por las leyes o normas que resulten de aplicación, o cuando sea requerido para ello por mandato de una Autoridad competente con arreglo a Derecho.

• Utilizar la información a que alude el apartado anterior, únicamente en la forma que exija el desempeño de sus funciones en el CICCP y no disponer de ella de ninguna otra forma o finalidad. Está prohibida la copia y envío de cualquier información obtenida o generada como consecuencia del trabajo para fines distintos de este.

• No utilizar en forma alguna, cualquier otra información que hubiese podido obtener prevaliéndose de su condición de profesional de la estructura del Colegio y que no sea necesaria para el desempeño de sus funciones en el CICCP.

• Cumplir en el desarrollo de sus funciones en el CICCP con la normativa vigente nacional y comunitaria, relativa a la protección de datos de carácter personal, y en particular con el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales

y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales y cualquier otra que la sustituya o complemente en el futuro.

• Cumplir las Políticas de Seguridad de la Información y sus sistemas, así como del correo electrónico y otros sistemas de comunicación, los procedimientos que establezca y le comunique la dirección de la Corporación.

• No hacer uso personal de los sistemas y equipos de información titularidad del Colegio que interfiera con sus funciones en la estructura del Colegio, de los/as demás trabajadores/as o de la Corporación.

• En internet, adoptar las precauciones oportunas para proceder a la descarga de archivos, asegurándose, antes de hacerlo, de la confianza o acreditación del sitio web desde el que se realizará.

• Cumplir los compromisos anteriores incluso después de extinguida, por cualquier casusa, la relación que le une con el CICCP.

• Asumir las consecuencias del incumplimiento de los anteriores compromisos, conociendo que la infracción de los deberes adquiridos puede dar lugar a sanciones conforme al RGPD y a sanción disciplinaria laboral o deontológica, si corresponde, y a responsabilidad civil y penal.

Están sujetos a un compromiso de confidencialidad escrito además de a los empleados/as los siguientes colectivos:
- Órganos de gobierno
- Consejo General
- Junta de decanos
- Representantes internacionales.

Para regular el compromiso de confidencialidad con los colectivos referenciados, el CICCP dispone de un documento específico.

Compromiso de confidencialidad para Miembros de la Junta de Gobierno

D/Dª……., mayor de edad y DNI: ……., (en adelante, la persona firmante) interviniendo en este acto en su condición de persona integrante de la Junta de Gobierno del Colegio de Ingenieros De Caminos, Canales y Puertos (CICCP),

MANIFIESTA:

1. Que ostenta el siguiente cargo en la Junta de Gobierno de CICCP (marcar la que corresponda:)

Decano /a		Tesorero/a	
Vicedecano/a		Interventor/a	
Secretario/a		Vocal	
Vicesecretario/a			

2. Que conoce que, con motivo del desempeño de sus funciones en CICCP, puede tener acceso a información diversa, ya sea en soporte automatizado o no automatizado, en la que se contengan datos de carácter personal.

3. Que ha sido informado/a por CICCP de que los datos personales deben tratarse de un modo que se garantice su seguridad y su confidencialidad, de conformidad lo establecido en el Reglamento (UE) 2016/679, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales a la libre circulación de estos datos (en adelante, RGPD).

4. Que asimismo conoce que CICCP debe tomar medidas para garantizar que cualquier persona que integre la Junta de Gobierno y tenga acceso a datos personales, solo pueda tratar dichos datos para cumplir las funciones derivadas de su cargo.

5. Que, en consecuencia y al objeto de formalizar el compromiso por parte de la persona firmante de observar un deber de seguridad y confidencialidad en el tratamiento de datos personales, suscribe el presente documento que se regirá por las siguientes,

CLÁUSULAS

Primera. - Objeto y ámbito de aplicación

1.1.- Este documento tiene por objeto formalizar el compromiso por parte de persona firmante, en su condición de integrante de la Junta de Gobierno de CICCP, respecto del cumplimiento de un deber de seguridad y confidencialidad en el tratamiento de datos personales, con motivo del desempeño de sus funciones.

1.2.- Esta obligación se entenderá referida a la totalidad de la información que contenga datos personales a la que pueda tener acceso la persona firmante durante el desempeño de sus funciones, en cualquier tipo de soporte y a través de cualquier medio.

1.3- En este sentido, la Secretaría Técnica de CICCP limitará el acceso a los sistemas de información al objeto de garantizar el cumplimiento de las obligaciones antedichas.

1.4.- Cualquier información que contenga datos de carácter personal deberá ser solicitada por escrito con identificación de la persona solicitante y el motivo de dicha solicitud.

Segunda. - Alcance del compromiso

2.1.- En cumplimiento del objeto del presente documento, la persona firmante se compromete a tratar los datos personales a los que tenga acceso durante el desempeño de sus funciones de un modo que garantice una seguridad y confidencialidad adecuadas, inclusive para impedir el acceso o uso no autorizados de dichos datos y del equipo utilizado en el tratamiento. A tal efecto, se compromete a no revelar ni dar a conocer los datos personales a cualquier persona que no tenga acceso autorizado a los mismos y observando en todo caso las instrucciones del Colegio, incluyendo las medidas técnicas y organizativas de seguridad en el tratamiento de datos personales que le sean comunicadas sin destinarlos en ningún caso a cualquier otra finalidad.

2.2.- La persona firmante conoce y acepta que la totalidad de la información relativa a las actividades de CICCP a la que pueda tener acceso con motivo del desempeño de sus funciones para la misma, en cualquier tipo de soporte y a través de cualquier medio, pertenece y/o es responsabilidad de CICCP, sin que tal acceso otorgue a la persona firmante derecho o título alguno sobre dicha información.

Tercera. - Vigencia del deber de confidencialidad

3.1.- La persona firmante conoce que el deber de confidencialidad adquirido en el tratamiento de datos personales subsistirá aun después de finalizar el desempeño de su cargo en la Junta de Gobierno de CICCP, comprometiéndose al término de dichas relaciones a guardar dicho deber sin límite temporal, así como a cesar en toda operación de tratamiento de los datos personales que hubiera conocido durante el desempeño de sus funciones para CICCP, y a no conservar copia alguna de dichos datos.

Cuarta. - Responsabilidad

4.1.- La persona firmante conoce y acepta que el cumplimiento del deber de seguridad y confidencialidad en el tratamiento de datos personales forma parte de sus deberes como integrante de la Junta de Gobierno, por lo que, en caso de cualquier vulneración de este, incurriría en responsabilidad personal, pudiendo ser sancionado por CICCP conforme a los Estatutos del Colegio.

Y para que así conste, y en prueba de aceptación y conformidad con el contenido del presente documento, lo firma por duplicado en el lugar y fecha al principio expresados.

Fdo.: D/Dª……

Uso de los medios digitales del colegio por los empleados
Los/as trabajadores/as deberán cumplir las políticas o instrucciones de uso aceptable o de seguridad de la información y sus sistemas, así como el correo electrónico y otros sistemas de comunicación, que establezca y le comunique la dirección del Colegio. No deberán hacer un uso personal de los sistemas y equipos de información titularidad del CICCP que interfiera con el trabajo del empleado/a, de los/as demás trabajadores/as o de la Corporación. Los/as trabajadores/as serán informados/as de que no se permite el acceso a páginas web no ligadas al trabajo como páginas de chat, redes sociales no profesionales, juegos, juegos de azar, viajes, compras por Internet, venta de acciones, de contenido ilegal o de carácter pornográfico, etc. También está prohibido expresamente la difusión y descarga de material ilegal, vulnerador de derechos, así como el uso, la copia o envío ilegal de software o material que esté protegido por leyes protectoras de la propiedad intelectual o industrial. En internet, deberán adoptar las precauciones oportunas antes de proceder a la descarga de archivos asegurándose, antes de hacerlos, de la confianza o acreditación del sitio web desde el que se realizará.

El Colegio podrá acceder a los contenidos derivados del uso de medios digitales facilitados a los/as trabajadores/as a los efectos de controlar el cumplimiento de las obligaciones laborales o estatutarias y de garantizar la integridad de dichos dispositivos.

Por todo ello, ningún/a trabajador/a del CICCP puede esperar a que sus comunicaciones con medios del Colegio o uso de los sistemas informáticos del Colegio sean confidenciales, ni tampoco privados, estando sometidos al control del empleador.

El/la trabajador/a será informado que en los equipos y sistemas informáticos propiedad de CICCP se podrán instalar aplicaciones que analicen el tráfico enviado y recibido de Internet y lo permita o prohíba en función de una serie de reglas específicas definidas por los administradores de los sistemas.

Decálogo de buenas prácticas
Los principios y obligaciones básicas de los/as empleados/as se recogerán en un documento denominado Decálogo de Buenas Prácticas de Protección de Datos, que será difundido periódicamente entre los/as empleados/as, así como actualizado.

Cláusula informativa para el personal de la estructura del CICCP
En cumplimiento de lo establecido en la Ley Orgánica de Protección de Datos de Carácter Personal y Garantía de Derechos Digitales ("LOPDGDD") y el Reglamento Europeo EU 2016/679 de Protección de Datos personales ("RGPD") COLEGIO DE INGENIEROS DE CAMINOS CANALES Y PUERTOS (en adelante, "El Colegio" o "CICCP") informa al abajo firmante (en adelante el TRABAJADOR), que los datos personales suministrados por éste serán incorporados a ficheros del Colegio con la finalidad de gestionar los diversos aspectos derivados de su relación con el Colegio y el desempeño de su trabajo en las instalaciones de ésta, y entre otras, en su caso las relaciones laborales, la nómina, la prevención de los riesgos laborales, la formación, las obligaciones tributarias y las necesarias para cumplir con la legislación en protección de datos tanto durante la vigencia del contrato como una vez extinguido.

El TRABAJADOR es responsable de la veracidad de los datos suministrados, así como de notificar cualquier cambio que se produzca.

El TRABAJADOR reconoce así y acepta que los datos personales suministrados u obtenidos en el curso de su relación contractual con el Colegio, incluidos sus datos identificativos, académicos y profesionales, así como su imagen, serán tratados por el Colegio acorde a la legislación laboral vigente y la normativa de protección de datos de carácter personal anteriormente citada.

El Colegio puede necesitar proceder a la comunicación de datos personales profesionales, de nómina y/o curriculares, de sus trabajadores en determinados casos, según sea necesario, a:

a) A administraciones públicas competentes, por razones de cumplimiento normativo diverso.

b) Servicios de prevención externos, Mutua de Accidentes de Trabajo y Enfermedades Laborales y Compañías de seguros que el Colegio contrate con el objeto de cumplir con sus obligaciones legales, proteger a sus trabajadores y demás establecidas en los convenios colectivos.

c) Empresas de formación contratadas por el Colegio y administraciones públicas y organismos encargados de la bonificación de la formación continua o subvenciones de otro tipo para la formación.

d) Bancos para el pago de nómina, complementos y gastos en cada caso.

e) Empresas aseguradoras para la gestión del seguro.

f) Empresas y entidades con las que, el Colegio tenga relaciones comerciales, al efecto de gestionar adecuadamente la relación con el trabajador.

g) Clientes del Colegio, cuando la información personal sea requerida para la ejecución de los proyectos u otros servicios contratados, en especial cuando es requerido en la Coordinación de Actividades Empresariales.

h) Consultores y asesores externos contratados por el Colegio para realizar auditorías, así como asesoría y consultoría.

i) Gestorías para la gestión de las nóminas de los trabajadores.

j) Empresas de mantenimiento informático con las que el Colegio trabaje para el correcto funcionamiento de los sistemas.

De este modo, el TRABAJADOR abajo firmante ACEPTA haber recibido esta información respecto al tratamiento de sus datos personales.

Datos personales de terceros y allegados
En el supuesto de que el TRABAJADOR aporte datos de terceros (por ejemplo, familiares) que resulten necesarios para la gestión de sus datos, el Colegio podrá requerir el consentimiento de éstos cuando sea necesario y en términos análogos al presente.

Deber de confidencialidad
Con carácter general, si El TRABAJADOR tuviera acceso a datos personales de clientes, proveedores o personal del Colegio deberá tener presente su obligación de preservar la confidencialidad de los mismos, lo cual implica no divulgarlos

a terceros y custodiar debidamente los registros de dichos datos personales.

Por consiguiente, se compromete a cumplir con el deber de confidencialidad que incluye:

• No revelar a persona ajena al CICCP, sin su consentimiento, la información a la que haya tenido acceso en el desempeño de sus funciones en el Colegio, excepto en el caso de que ello sea necesario para dar cumplimiento a las obligaciones propias o de la organización impuestas por las leyes o normas que resulten de aplicación, o cuando sea requerido para ello por mandato de una Autoridad competente con arreglo a Derecho.

• Utilizar la información a que alude el apartado anterior, únicamente en la forma que exija el desempeño de sus funciones en el CICCP y no disponer de ella de ninguna otra forma o finalidad. Está prohibida la copia y envío de cualquier información obtenida o generada como consecuencia del trabajo para fines distintos de este.

• No utilizar en forma alguna, cualquier otra información que hubiese podido obtener prevaliéndose de su condición de profesional de la estructura del Colegio y que no sea necesaria para el desempeño de sus funciones en el CICCP.

• Cumplir en el desarrollo de sus funciones en el CICCP con la normativa vigente nacional y comunitaria, relativa a la protección de datos de carácter personal, y en particular con el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales y cualquier otra que la sustituya o complemente en el futuro.

• Cumplir las Políticas de Seguridad de la Información y sus sistemas, así como del correo electrónico y otros sistemas de comunicación, los procedimientos que establezca y le comunique la dirección de la Corporación.

• No hacer uso personal de los sistemas y equipos de información titularidad del Colegio que interfiera con sus funciones en la estructura del Colegio, de los/as demás trabajadores/as o de la Corporación.

• En internet, adoptar las precauciones oportunas para proceder a la descarga de archivos, asegurándose, antes de hacerlo, de la confianza o acreditación del sitio web desde el que se realizará.

• Cumplir los compromisos anteriores incluso después de extinguida, por cualquier casusa, la relación que le une con el CICCP.

• Asumir las consecuencias del incumplimiento de los anteriores compromisos, conociendo que la infracción de los deberes adquiridos puede dar lugar a sanciones conforme al RGPD y a sanción disciplinaria laboral o deontológica, si corresponde, y a responsabilidad civil y penal.

Derechos
El TRABAJADOR podrá acceder y en su caso, rectificar, suprimir, oponerse y limitar el tratamiento de sus datos en cualquier momento, así como revocar el consentimiento cuando proceda ejercitando sus derechos en la siguiente dirección dpo@ciccp.es.

El Colegio informa, no obstante, que el ejercicio de los derechos de supresión, así como la revocación o la oposición pueden suponer diversas consecuencias en los tratamientos que el Colegio realiza sobre los datos registrados, por lo que, en todo caso, se recomienda encarecidamente que el TRABAJADOR consulte previamente su situación y los tratamientos en particular que le afectan al solicitar el ejercicio de los derechos que le asisten.

D./Dña. _____

En _____a___de___del____
Firma:

ANEXO B
OBTENCIÓN Y CONSERVACIÓN DEL CONSENTIMEINTO

Objeto
El Reglamento General de Protección de datos impone la adopción de medidas técnicas y organizativas orientadas a garantizar que el uso de la información personal por parte de las organizaciones es conforme con la citada normativa.

Todos los tratamientos de datos personales que se realicen en una organización deben quedar identificados y definidos en el documento denominado Registro de Actividades de Tratamiento, según el artículo 30 del RGPD.

Cuando los tratamientos de datos personales tengan como base de legitimación, el consentimiento del titular de los datos se hace necesario por parte del responsable, establecer un conjunto de medidas tendentes a asegurar que la gestión del consentimiento cumple con los requisitos establecidos en la normativa.

El presente documento tiene por objeto establecer e informar de las condiciones y requisitos que debe tener la gestión del consentimiento de conformidad con la citada normativa. Para ello, y con carácter previo se van a definir los roles que ocupan los sujetos y los tratamientos de datos implicados en dicha gestión.

Alcance

El presente documento alcanza al conjunto de actividades de tratamientos de datos definidos en el epígrafe 2.1; y cuya legitimación esté basada en la obtención del consentimiento del interesado de la siguiente entidad:

Organización	Dirección SEDE CENTRAL
Colegio de Ingenieros de Caminos, Canales y Puertos, incluyendo: • Su sede central • Cada una de las demarcaciones que forman parte del Colegio	Almagro, 42 - 1ª Planta, Madrid 28010

Gestión del consentimiento

Definición de los roles y sujetos de datos:
En este epígrafe se definen los roles que ocupan los participantes en la recogida de datos personales.

RGPD	
Rol	**Definición**
Responsable de tratamiento	La persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento, … (Art. 4 RGPD) • CICCP, como Colegio Profesional único. Dicha posición, se hace extensiva a cada una de las demarcaciones.
Encargados de tratamiento	La persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento. (Art. 4 RGPD)
Interesados	• Titulares de los datos personales que trata el responsable. • Colegiados. • Socios Administradores • Colegiados denunciados • Interesados que presenten quejas • Miembros del Comité De Deontología y de su Comisión de Admisión • Colegiados solicitantes de visado. • Clientes de los colegiados • Peritos • Miembros de los órganos colegiales • ...
Destinatarios	La persona física o jurídica, autoridad pública, servicio u otro organismo al que se comuniquen datos personales, se trate o no de un tercero (Art. 4 RGPD)

Es necesario que se defina y asigne claramente todas las responsabilidades para gestión del consentimiento y la garantía de seguridad de la información.

Por ello, se deben segregar tareas y las áreas de responsabilidad ante posibles conflictos de interés con el fin de reducir las oportunidades de una modificación no autorizada o no intencionada, o el de una mala gestión en la obtención del consentimiento.

Identificación de tratamientos afectados:
Se incluye a continuación, la relación de tratamientos identificados y definidos en el documento "Registro de Actividades de Tratamiento v1.3" como tratamientos basados únicamente en el consentimiento de los interesados.

Tratamiento	Finalidades
Gestión Colegial	Colegiación y gestión de las funciones legalmente previstas derivadas de la colegiación. Alta, cobro de cuota. Gestión de las relaciones Colegio-colegiados. Envío de información colegial. Prestación de servicios colegiales. Llevanza del registro de colegiados. Elaboración de listas de colegiados y publicación de sus datos en ventanilla única. Publicación del Anuario o Lista de colegiados. Registro de actuaciones profesionales para licitaciones. Tramitación de procedimientos derivados del ejercicio de funciones públicas del Colegio. Gestión de la participación en procesos electorales. Gestión de la relación derivada de la condición de representante internacional. Emisión de dictámenes sobre honorarios en los procedimientos de tasación de costas cuando a tales efectos lo soliciten los órganos judiciales. Emisión de Certificados Encuestas sobre prestación de servicios

Tratamiento	Finalidades
Registro de peritos y expertos CICCP	Gestión del registro de peritos ingenieros de caminos, canales y puertos. Elaboración de listados. Gestión de otros registros de expertos Comunicación a juzgados y tribunales y otras partes y designación de peritos Si lo autoriza, sus datos podrán utilizarse para edición, publicación y distribución pública de los listados. Emisión de Certificados
Agencia de colocación	Gestión de la agencia de colocación: anuncio de empleos y envío de CV a empresas solicitantes. En el caso de ser demandante de empleo, gestión de la Agencia de Colocación, la comunicación de sus datos a ofertantes de empleo y la remisión de información relativa a la búsqueda y mejora del empleo. En el caso de ser ofertante de empleo, gestión de la Agencia de Colocación, la comunicación de sus datos a demandantes de empleo y la gestión de la oferta de empleo. Emisión de Certificados
Antiguos colegiados	Gestión de la relación con antiguos colegiados. Envío de información colegial y relevante para los Ingenieros de caminos, canales y puertos. Emisión de Certificados
Precolegiados	Precolegiación. Gestión de la relación con el precolegiado, envío de información sobre actividades colegiales y de formación, así como prestación de servicios. Realización de encuestas, sobre el Colegio, sobre la calidad y satisfacción de los servicios y aspectos relacionados con la titulación y profesión. Emisión de Certificados

Tratamiento	Finalidades
Gestión de cursos, formación y eventos	Gestión de asistencia a jornadas y eventos o como alumno en cursos o actividades organizadas por el Colegio, incluyendo en dicha finalidad, si procede, la facturación de los cursos en los que se matricula, el envío de comunicaciones relacionadas con las jornadas o cursos en los que se inscribe, así como la de conocer la satisfacción y opinión sobre la calidad de las jornadas celebradas y de los cursos impartidos. En el caso de cursos y actividades formativas, sus datos se tratarán para la evaluación y calificación. Sus datos podrán ser utilizados, si lo autoriza, para el envío por el Colegio de información relativa a la actividad formativa y a la realización de jornadas y eventos. Gestión de becas. Realización de encuestas de calidad. Emisión de Certificados
Gestión de publicaciones y suscripciones	Gestión de contenidos de la revista. Gestión de envío de la revista. Gestión de suscripciones. Gestión de envío de información sobre licitaciones. Venta de publicaciones, material técnico o didáctico.
Gestión de convenio con la AEAT	Intermediación para que colegiados y sociedades profesionales representen a terceros en gestiones con Hacienda.
Gestión de premios y distinciones	Gestión de Premios promovidos por el CICCP. Emisión de Certificados
Gestión de encuestas	Realización de Encuestas sobre el ejercicio profesional. Realización de encuestas de calidad y sobre la gestión de la prestación de servicios por el Colegio
Gestión contractual y convencional del Colegio	Gestión de las relaciones negociales con el Colegio, bien sea actividad contractual, convencional (suscripción de convenios) o con proveedores de servicios o productos.
Gestión de emprendedores	Gestión del programa de asesoría y apoyo a emprendedores
Gestión de registros y listados voluntarios de colegiados y profesionales	Gestión de registros y listados voluntarios de colegiados y profesionales con finalidades concretas. Gestión de listados para contratación Emisión de Certificados
Fondo de Solidaridad	Gestión del Fondo de Solidaridad Gestión de las aportaciones y emisión de certificados Tramitación de ayudas

Condiciones legales del consentimiento

Los anteriores tratamientos de datos personales tienen como base de legitimación el consentimiento del interesado. A continuación se describen las condiciones establecidas en el art. 7 RGPD y en el art. 6 LOPDGDD que debe reunir los siguientes requisitos para ser válido:

• Debe ser libre, es decir, ha de prestarse de manera voluntaria, sin condicionamiento alguno.

• También debe ser específico, es decir, debe ir referido a una finalidad concreta.

• Ha de ser informado, de manera que antes de prestar su consentimiento el interesado debe recibir una información mínima sobre qué datos van a tratarse, por quién y para qué. Esta condición se cumple mostrando las cláusulas informativas generadas por la organización.

• Debe prestarse de manera inequívoca, es decir, mediante una declaración o una clara acción afirmativa. Por el contrario, el RGPD prohíbe:
o El consentimiento tácito
o El consentimiento obtenido mediante silencio o basado en la inacción
o El consentimiento negativo u “opt-out”
o Las casillas premarcadas

• A su vez, ha de ser demostrable, por lo que la carga de la prueba de que el interesado dio su consentimiento recae sobre el responsable que lo afirma.

• Por otra parte, el interesado tendrá derecho a retirar el consentimiento en cualquier momento, debiendo ser informado de tal circunstancia antes de dar su consentimiento. Por tanto, el consentimiento debe ser revocable.

• Por último, en determinados casos el consentimiento ha de ser explícito:
o Cuando el consentimiento sea la base para el tratamiento de categorías especiales de datos;
o Cuando ampare la toma de decisiones automatizadas que produzcan efectos jurídicos en el interesado o le afecten significativamente;
o Cuando habilite una transferencia internacional de datos en ausencia de una decisión de adecuación y de garantías adecuadas.

Cuando el tratamiento de los datos personales se efectúe por medios automatizados, debe permitirse que los interesados que hubieran facilitado sus datos personales puedan solicitar el ejercicio de sus derechos, incluyendo que reciban sus datos en un formato estructurado, de uso común, de lectura mecánica e interoperable, y los transmitan a otro responsable del tratamiento. Debe partirse de formatos interoperables que permitan la portabilidad de los datos personales.

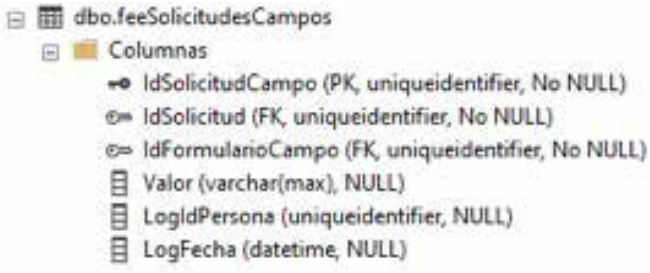
Aplicabilidad de los requisitos legales
El ejercicio de derechos por parte de los interesados se ve afectado cuando el tratamiento está basado en el consentimiento, de tal manera que obliga al responsable a tomar acciones sobre la gestión de sus bases de datos al objeto de controlar las condiciones en las que se prestó dicho consentimiento y su posibilidad de revocación.

Para dar una respuesta técnica a los requisitos legales, CICCP ha realizado un estudio sobre todas las aplicaciones tecnológicas que soportan todos los tratamientos cuya base de legitimación sea el consentimiento del interesado, así:

Gescol
La web de GESCOL permite construir formularios a medida, especificando los campos, como los del RGPD. Esos formularios guardan siempre en la misma tabla (modelado de datos donde se guardan los datos recogidos por un programa) los valores rellenados por los usuarios.

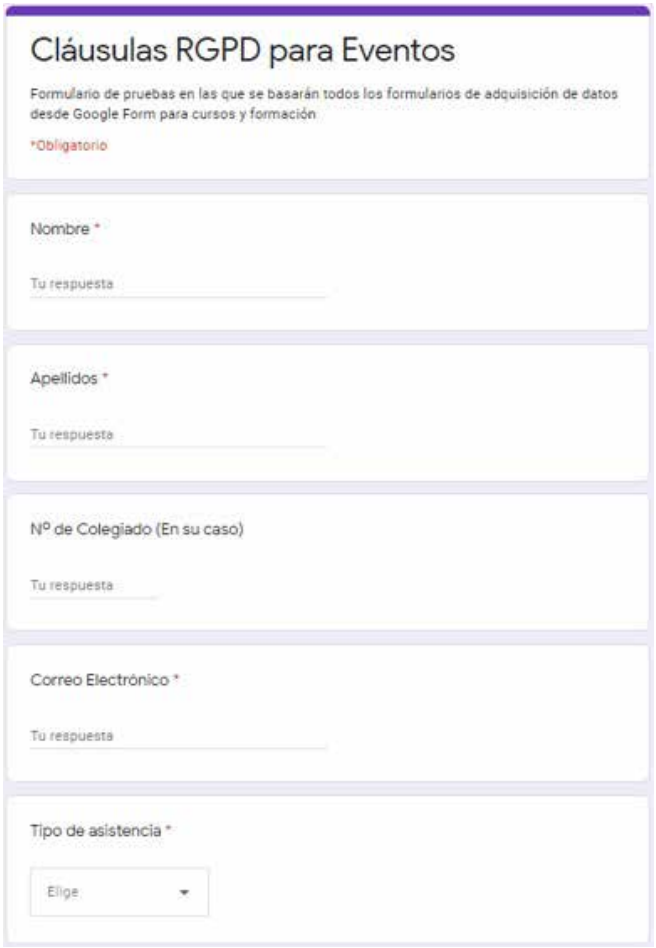
En concreto, la tabla en la que se almacenan los valores correspondientes a la gestión de los diferentes consentimientos es "feeSolicitudesCampos" y la tabla que contiene configuración de esos campos es "feeFormulariosCampos", ambas de la base de datos "GesColCICCP". El valor guardado en el campo para las casillas es un 1 o 0, que indican si se marca o no.

Se acompaña imagen del diseño de la tabla:



A continuación, se muestra un screenshot del formulario y las casillas de marcación de consentimiento RGPD:

Google Forms
La herramienta Google Forms es utilizada por CICCP para la recogida de datos vía web en la parte de acceso público de la página, se incluye screenshot del formulario:



Cláusulas RGPD para Eventos

Formulario de pruebas en las que se basarán todos los formularios de adquisición de datos desde Google Form para cursos y formación

*Obligatorio

Nombre *

Tu respuesta

Apellidos *

Tu respuesta

Nº de Colegiado (En su caso)

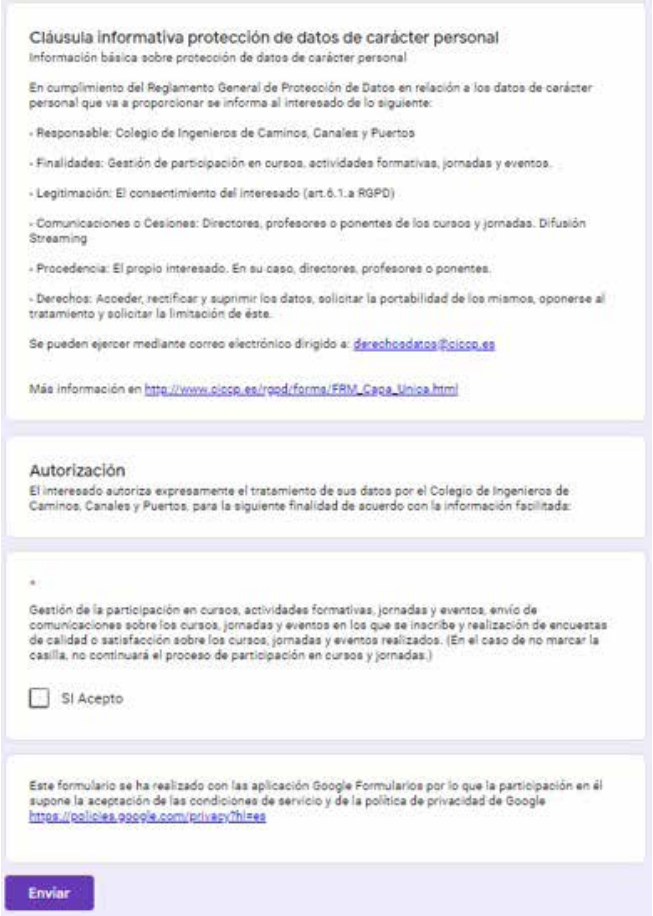
Tu respuesta

Correo Electrónico *

Tu respuesta

Tipo de asistencia *

Elige



Cláusula informativa protección de datos de carácter personal

Información básica sobre protección de datos de carácter personal

En cumplimiento del Reglamento General de Protección de Datos en relación a los datos de carácter personal que va a proporcionar se informa al interesado de lo siguiente:

- Responsable: Colegio de Ingenieros de Caminos, Canales y Puertos
- Finalidades: Gestión de participación en cursos, actividades formativas, jornadas y eventos.
- Legitimación: El consentimiento del interesado (art.6.1.a RGPD)
- Comunicaciones o Cesiones: Directores, profesores o ponentes de los cursos y jornadas. Difusión Streaming
- Procedencia: El propio interesado. En su caso, directores, profesores o ponentes.
- 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

Más información en http://www.ciccp.es/rgpd/forms/FRM_Capa_Unica.html

Autorización

El interesado autoriza expresamente el tratamiento de sus datos por el Colegio de Ingenieros de Caminos, Canales y Puertos, para la siguiente finalidad de acuerdo con la información facilitada:

*

Gestión de la participación en cursos, actividades formativas, jornadas y eventos, envío de comunicaciones sobre los cursos, jornadas y eventos en los que se inscribe y realización de encuestas de calidad o satisfacción sobre los cursos, jornadas y eventos realizados. (En el caso de no marcar la casilla, no continuará el proceso de participación en cursos y jornadas.)

SI Acepto

Este formulario se ha realizado con las aplicación Google Formularios por lo que la participación en él supone la aceptación de las condiciones de servicio y de la política de privacidad de Google https://policies.google.com/privacy?hl=es

Enviar

ANEXO C
CRITERIOS DE CONSERVACIÓN DE LOS DATOS DE LOS COLEGIADOS

A continuación, se incluyen los criterios adoptados por el CICCP en relación a la conservación y destrucción de los datos de carácter personal de los/as Colegiados/as:

• En los casos de baja hay que comprobar si tiene deudas o hay procedimientos disciplinarios en marcha. En ese caso habría que conservar los datos necesarios por los plazos de prescripción (5 años cuotas; 3 años procedimientos disciplinarios).

• Colegiados con deudas: se conservan además los datos necesarios para reclamaciones, datos de contacto, datos bancarios y relativos al estado de cobro de cuotas y facturación de servicios, mientras estén vigentes las deudas y no hayan prescrito (5 años).

• Si no tiene deudas ni procedimientos pendientes: hay que conservar nombre, apellidos, nº de DNI, datos relativos al título habilitante y de pertenencia al Colegio y bloquear el resto de los datos por tres años. Bloquear significa que sólo tenga acceso una persona habilitada a tal fin.

• Se conservan también los datos de los trabajos profesionales visados, los relativos a la inscripción en el listado de Peritos y en MediaCaminos y del Registro de Sociedades Profesionales.

• Colegiados con procedimientos disciplinarios en tramitación o pendientes de ejecución, si continúa abierto y se da de baja, se conservan además todos los datos mientras están en tramitación, y en su caso una vez haya sanción, durante 2 años.

• Hay que pedir consentimiento para conservar los datos referentes a la formación, o a otras actividades del Colegio.

Los anteriores criterios deberán ser tenidos en cuenta por el Colegio a la hora de facilitar el ejercicio de los derechos de conformidad con el procedimiento establecido al efecto.

ANEXO D
CLÁUSULAS INFORMATIVAS

Gestión colegial

¿Quién es el responsable del tratamiento de sus datos?
Identidad: Colegio de Ingenieros de Caminos, Canales y Puertos
CIF: Q-2867009-I
Dirección Postal: c/Almagro 42, 28010 Madrid
Teléfono: 91.308.19.88
Correo electrónico: atencioncolegial@ciccp.es
Web: http://www.ciccp.es
Contacto Delegado de Protección de Datos: dpo@ciccp.es
Ventanilla única: http://www3.ciccp.es/ventanilla-unica

¿Con qué finalidad tratamos sus datos personales?
El Colegio de Ingenieros de Caminos, Canales y Puertos tratará sus datos con el fin de gestionar la colegiación, las funciones legalmente derivadas de la colegiación, incluida la del control de deontológico y el ejercicio de la facultad disciplinaria, el cargo de la cuota colegial, la gestión de la participación en procesos electorales, el envío de información colegial, así como la prestación de servicios colegiales.

Los datos podrán ser tratados para la emisión de dictámenes sobre honorarios en los procedimientos de tasación de costas cuando a tales efectos lo soliciten los órganos judiciales.

De acuerdo con la redacción vigente de la Ley 2/1974 de Colegios Profesionales determinados datos (nombre y apellidos, número de colegiación, títulos oficiales de los que estén en posesión, datos profesionales de domicilio, teléfono y dirección de correo electrónico, y situación de habilitación profesional) serán publicados en la ventanilla única. La previsión de la publicación del registro de colegiados en la ventanilla única de la página web de los colegios profesionales responde a las potestades de ordenación profesional que las leyes atribuyen a estas Corporaciones de Derecho Público, resultando obligatorio para éstas, mantener actualizado el registro de colegiados en la ventanilla única de su web, con la finalidad de protección de los intereses de los ciudadanos y clientes.

Sus datos podrán ser utilizados, si lo autoriza, para el envío por el Colegio de información relativa a formación o de interés profesional.

También podrán ser utilizados sus datos para la realización de encuestas de calidad y satisfacción sobre la prestación de servicios, si así lo ha autorizado.

Sus datos podrán ser utilizados para la emisión de certificados

¿Cuánto tiempo conservaremos sus datos?
Los datos personales proporcionados se conservarán mientras se mantenga su condición de colegiado, no se solicite su supresión por el interesado o cuando los datos dejen de ser necesarios -incluyendo la necesidad de conservarlos durante los plazos de prescripción aplicables o pertinentes para la finalidad para la cual hubieran sido recabados o registrados.

La supresión, eliminación o destrucción de los datos tratados en el ejercicio de funciones públicas se realizará de conformidad con lo establecido en la Ley 16/1985, de 25 de junio, del Patrimonio Histórico Español y sólo pueden ser destruidos previa regulación de un procedimiento que salvaguarde el valor probatorio de derechos y obligaciones y los valores artísticos e históricos que puedan tener los documentos, por acuerdo del órgano competente.

Legitimación
La base legal del tratamiento es la siguiente:

RGPD: 6.1.a) Consentimiento del interesado. La base legal para el envío de información no colegial relativa a formación o de interés profesional y para la realización de encuestas de calidad y satisfacción sobre la prestación de servicios es el consentimiento que usted presta que podrá retirar en cualquier momento.

RGPD: 6.1.c) Tratamiento necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento.

La base legal de las finalidades principales del tratamiento de sus datos asociados a la colegiación, para la gestión de las funciones derivadas de la colegiación, el cargo de la cuota colegial, la elaboración de las listas de colegiados y publicación de datos en la ventanilla única, así como el envío de información colegial es la Ley 2/1974, de 13 de febrero, sobre Colegios Profesionales.

Ley 25/2009, de 22 de diciembre, de modificación de diversas leyes para su adaptación a la Ley sobre el libre acceso a las actividades de servicio y su ejercicio

Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

RGPD: 6.1.e) Tratamiento necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento. El tratamiento para las finalidades principales no está supeditado al consentimiento para el tratamiento de los datos que no sean necesarios para dichas finalidades.

¿A qué destinatarios se comunicarán sus datos?
En la ventanilla única en la web del Colegio, de acceso público, se van a publicar sus datos de nombre, apellidos, número de colegiado y los datos de la dirección profesional (incluyendo teléfono, fax y correo electrónico si los ha facilitado) de conformidad con el artículo 10 de la redacción vigente Ley 2/1974, de 13 de febrero, sobre Colegios Profesionales

A los órganos judiciales podrá comunicarse, en su caso, los datos referidos a los incidentes de tasación de costas.

Si lo ha autorizado, la cesión de datos de identificativos y de contacto se podrán proporcionar a las siguientes entidades:
- Asociación de Ingenieros de Caminos, Canales y Puertos (CIF - G-78416252)
- FAM Caminos S.A. (CIF A80617707)
- Compañía de Seguros y Reaseguros S.A (CASER, con CIF-A 28013050)
- Mutualidad de Previsión Social Fondo de Asistencia Mutua del Colegio de Ingenieros de Caminos, Canales y Puertos (CIF V78293719)
- Banco Caminos S.A. (CIF A28520666)
- Almagro Sociedad Cooperativa de Consumidores y Usuarios (NIF F2839881)

¿Cuál es la procedencia de los datos?
Los datos personales que tratará el Colegio son los que usted proporcione, en el formulario de inscripción o en otros momentos posteriores.

¿Qué categorías de datos trata el Colegio?
El Colegio tratará los datos que nos suministre, que pueden ser de las siguientes categorías:
- Datos de carácter identificativo
- Características personales
- Datos académicos y profesionales
- Datos de detalle del empleo
- Datos bancarios y económico-financieros y seguros

No se tratarán categorías especiales de datos.

¿Cuáles son sus derechos?
Cualquier persona tiene derecho a obtener confirmación sobre si el Colegio de Ingenieros de Caminos, Canales y Puertos trata datos personales que le conciernen, o no.

Las personas interesadas tienen derecho a acceder a sus datos personales y a obtener una copia de los datos personales objeto del tratamiento, a actualizarlos, así como a solicitar la rectificación de los datos inexactos o, en su caso, solicitar su supresión cuando, entre otros motivos, los datos ya no sean necesarios para los fines para los que fueron recogidos.

En determinadas circunstancias previstas en el artículo 18 RGPD, los interesados podrán solicitar la limitación del tratamiento de sus datos, en cuyo caso únicamente los conservaremos para el ejercicio o la defensa de reclamaciones.

Como consecuencia de la aplicación del derecho a la supresión u oposición al tratamiento de datos personales en el entorno on-line los interesados tienen, en su caso, el derecho al olvido según la jurisprudencia que el Tribunal de Justicia de la UE.

Los interesados podrán oponerse al tratamiento de sus datos con fines de mercadotecnia, incluida la elaboración de perfiles. En particular, los colegiados tienen derecho a que el Colegio indique gratuitamente respecto de los sus datos personales que se publican en la ventanilla única que no pueden utilizarse para fines de publicidad o prospección comercial.

El colegiado sólo se puede oponer a la publicación de sus datos, los que proceda según la Ley de Colegios Profesionales, en la ventanilla única por motivos fundados y legítimos, por ejemplo por amenaza terrorista o de violencia de género.

Si se editara el registro de colegiados en otro tipo de fuente accesible al público diferente a la ventanilla única (p.ej. en papel), el colegiado se puede oponer a la publicación si coincide con el domicilio personal.

En virtud del derecho a la portabilidad, los interesados tienen derecho a obtener los datos personales que les incumben en un formato estructurado de uso común y lectura mecánica y a transmitirlos a otro responsable

El interesado tiene el derecho a la supresión de sus datos, por la desaparición de la finalidad que motivó el tratamiento o la recogida, por revocación del consentimiento cuando sea éste el que legitime el tratamiento, o por el resto de motivos contenidos en el artículo 17 RGPD.

¿Cómo se pueden ejercer los derechos?
- Mediante un escrito dirigido a Colegio de Ingenieros de Caminos, Canales y Puertos. Calle Almagro, 42, 28010 Madrid.
- Mediante correo electrónico dirigido a: secretariogeneral@ciccp.es

¿Qué vías de reclamación existen?
Si considera que sus derechos no se han atendido debidamente, tiene derecho a presentar una reclamación ante la Agencia Española de Protección de Datos, cuyos datos de contacto son:

Teléfonos: 901 100 099 / 91.266.35.17
Dirección Postal: C/ Jorge Juan, 6, 28001 Madrid
Sede Electrónica:
https://sedeagpd.gob.es/sede-electronica-web/
Página web: http://www.agpd.es

Gestión de sociedades profesionales

¿Quién es el responsable del tratamiento de sus datos?
Identidad: Colegio de Ingenieros de Caminos, Canales y Puertos
CIF: Q-2867009-I
Dirección Postal: c/Almagro 42, 28010 Madrid
Teléfono: 91.308.19.88
Correo electrónico: atencioncolegial@ciccp.es
Web: http://www.ciccp.es
Contacto Delegado de Protección de Datos: dpo@ciccp.es
Ventanilla única: http://www3.ciccp.es/ventanilla-unica

¿Con qué finalidad tratamos sus datos personales?
El Colegio de Ingenieros de Caminos, Canales y Puertos tratará sus datos con el fin de gestionar el Registro de Sociedades Profesionales, sus altas, modificaciones y bajas.

¿Cuánto tiempo conservaremos sus datos?
Los datos personales proporcionados se conservarán mientras sean necesarios y pertinentes -incluyendo la necesidad de conservarlos durante los plazos de prescripción aplicables- para la finalidad para la cual hubieran sido proporcionados, recabados o registrados.

La supresión, eliminación o destrucción de los datos tratados en el ejercicio de funciones públicas se realizará de conformidad con lo establecido en la Ley 16/1985, de 25 de junio, del Patrimonio Histórico Español y sólo pueden ser destruidos previa regulación de un procedimiento que salvaguarde el valor probatorio de derechos y obligaciones y los valores artísticos e históricos que puedan tener los documentos, por acuerdo del órgano competente.

Legitimación
El tratamiento de sus datos tiene el siguiente amparo en el Reglamento General de Protección de Datos:

RGPD: 6.1.a) Consentimiento del interesado.

RGPD: 6.1.e) Tratamiento necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento.

RGPD: 6.1.c) Tratamiento necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento

Así, la legitimación inicial del tratamiento de sus datos personales es el consentimiento expreso que presta y la base legal del tratamiento posterior, así como de las posibles comunicaciones a terceros, es la que proporcionan la Ley 2/2007, de 15 de marzo, de Sociedades Profesionales; la Ley 2/1974, de 13 de febrero, sobre Colegios Profesionales, y la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

¿A qué destinatarios se comunicarán sus datos?
Sus datos podrán comunicarse al Registro Mercantil, al Ministerio de Justicia, a la Comunidad de Madrid, a otros colegios profesionales, y a los administradores y representantes de la sociedad profesional, así como a quienes sean interesados legítimos de acuerdo con la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, y a quien tenga derecho de acceso a la información pública, con los límites que apliquen, de conformidad con la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno

El Registro de Sociedades Profesionales se publica en la ventanilla única del Colegio, en la página web www.ciccp.es.

¿Cuál es la procedencia de los datos?
Los datos personales que tratará el Colegio son los que usted proporcione y aquellos que le comunique el Registro Mercantil o terceros (colegios profesionales; representantes o administradores de la sociedad profesional; etc.) para la correcta llevanza del Registro de Sociedades Profesionales.

¿Qué categorías de datos trata el Colegio?
El Colegio tratará los datos que nos suministre y los que se incorporen al Registro de Sociedades Profesionales, según lo establecido en el artículo 8 de la Ley de Sociedades Profesionales.

¿Cuáles son sus derechos?
Cualquier persona tiene derecho a obtener confirmación sobre si el Colegio de Ingenieros de Caminos, Canales y Puertos trata datos personales que le conciernen, o no.

Las personas interesadas tienen derecho a acceder a sus datos personales y a obtener una copia de los datos personales objeto del tratamiento, a actualizarlos, así como a solicitar la rectificación de los datos inexactos o, en su caso, solicitar su supresión cuando, entre otros motivos, los datos ya no sean necesarios para los fines para los que fueron recogidos.

En determinadas circunstancias previstas en el artículo 18 RGPD, los interesados podrán solicitar la limitación del tratamiento de sus datos, en cuyo caso únicamente los conservaremos para el ejercicio o la defensa de reclamaciones.

Como consecuencia de la aplicación del derecho a la supresión u oposición al tratamiento de datos personales en el entorno on-line los interesados tienen, en su caso, el derecho al olvido según la jurisprudencia que el Tribunal de Justicia de la UE.

Los interesados podrán oponerse al tratamiento de sus datos con fines de mercadotecnia, incluida la elaboración de perfiles. En particular, los colegiados tienen derecho a que el Colegio indique gratuitamente respecto de los sus datos personales que se publican en la ventanilla única que no pueden utilizarse para fines de publicidad o prospección comercial.

El colegiado sólo se puede oponer a la publicación de sus datos, los que proceda según la Ley de Colegios Profesionales, en la ventanilla única por motivos fundados y legítimos, por ejemplo por amenaza terrorista o de violencia de género. Si se editara el registro de colegiados en otro tipo de fuente accesible al público diferente a la ventanilla única (p.ej. en papel), el colegiado se puede oponer a la publicación si coincide con el domicilio personal.

En virtud del derecho a la portabilidad, los interesados tienen derecho a obtener los datos personales que les incumben en un formato estructurado de uso común y lectura mecánica y a transmitirlos a otro responsable

El interesado tiene el derecho a la supresión de sus datos, por la desaparición de la finalidad que motivó el tratamiento o la recogida, por revocación del consentimiento cuando sea éste el que legitime el tratamiento, o por el resto de motivos contenidos en el artículo 17 RGPD.

¿Cómo se pueden ejercer los derechos?
- Mediante un escrito dirigido a Colegio de Ingenieros de Caminos, Canales y Puertos. Calle Almagro, 42, 28010 Madrid.
- Mediante correo electrónico dirigido a: secretariogeneral@ciccp.es

¿Qué vías de reclamación existen?
Si considera que sus derechos no se han atendido debidamente, tiene derecho a presentar una reclamación ante la Agencia Española de Protección de Datos, cuyos datos de contacto son:

Teléfonos: 901 100 099 91.266.35.17
Dirección Postal: C/ Jorge Juan, 6, 28001 Madrid
Sede Electrónica:
https://sedeagpd.gob.es/sede-electronica-web/
Página web: http://www.agpd.es

Archivo de expedientes deontológicos

¿Quién es el responsable del tratamiento de sus datos?
Los datos de identificación y contacto del Colegio son:
- Identidad: Colegio de Ingenieros de Caminos, Canales y Puertos
- CIF: Q-2867009I
- Dirección postal: Calle Almagro,42 28010 Madrid
- Teléfono: 91 308 19 88
- Correo electrónico: atencioncolegial@ciccp.es
- Página web: http://www.ciccp.es
- Ventanilla Única: http://www3.ciccp.es/ventanilla-unica/
- Contacto Delegado de Protección de Datos: dpo@ciccp.es

El Colegio de Ingenieros de Caminos, Canales y Puertos tratará sus datos con el fin de gestionar las quejas interpuestas, la

tramitación de los preceptivos procedimientos, expedientes y recursos, así como la gestión de las funciones legalmente previstas de control deontológico y de aplicación del régimen disciplinario. Los datos personales se conservarán mientras sean necesarios y pertinentes -incluyendo la necesidad de conservarlos durante los plazos de prescripción aplicables- para la finalidad para la cual hubieran sido proporcionados, recabados o registrados.

La legitimación del tratamiento deriva del artículo 6 RGPD, apartados letra c (el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento) y letra e (el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento). La queja, los documentos que se acompañen, los escritos que se produzcan y los datos personales contenidos en ellos se incorporarán a un expediente administrativo al que tendrán acceso los interesados legítimos de acuerdo con la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas. En la tramitación de recursos los datos personales contenidos en el expediente podrán comunicarse a Juzgados y Tribunales. En su caso, el dato de situación de habilitación profesional, o no, se publicará en la ventanilla única del Colegio según la Ley 2/1974, de 13 de febrero, sobre Colegios Profesionales.

Puede ejercer los derechos que procedan según el RGPD a acceder, rectificar y suprimir los datos, solicitar la portabilidad de los mismos, oponerse al tratamiento y solicitar la limitación de éste, mediante correo electrónico dirigido a: derechosdatos@ciccp.es.

Si considera que sus derechos no se han atendido debidamente, tiene derecho a presentar una reclamación ante la Agencia Española de Protección de Datos, cuyos datos de contacto son: teléfonos: 901 100 099; 91.266.35.17, dirección postal: C/ Jorge Juan, 6 28001-Madrid; sede electrónica: https://sedeagpd.gob.es/sede-electronica-web/; página web: http://www.agpd.es

¿Con qué finalidad tratamos sus datos personales?
El Colegio de Ingenieros de Caminos, Canales y Puertos tratará sus datos con el fin de gestionar la queja que interpone, la tramitación de los preceptivos procedimientos, expedientes y recursos, así como la gestión de las funciones legalmente previstas de control deontológico y de aplicación del régimen disciplinario.

¿Cuánto tiempo conservaremos sus datos?
Los datos personales proporcionados se conservarán mientras sean necesarios y pertinentes -incluyendo la necesidad de conservarlos durante los plazos de prescripción aplicables- para la finalidad para la cual hubieran sido proporcionados, recabados o registrados.

La supresión, eliminación o destrucción de los datos tratados en el ejercicio de funciones públicas se realizará de conformidad con lo establecido en la Ley 16/1985, de 25 de junio, del Patrimonio Histórico Español y sólo pueden ser destruidos previa regulación de un procedimiento que salvaguarde el valor probatorio de derechos y obligaciones y los valores artísticos e históricos que puedan tener los documentos, por acuerdo del órgano competente.
.
Legitimación
El tratamiento de sus datos tiene el siguiente amparo en el Reglamento General de Protección de Datos:

· RGPD: 6.1.a) Consentimiento del interesado.

· RGPD: 6.1.e) Tratamiento necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento.

· RGPD: 6.1.c) Tratamiento necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento.

La legitimación inicial del tratamiento de sus datos personales es el consentimiento expreso que presta al presentar la queja y la base legal del tratamiento posterior, así como de las posibles comunicaciones a terceros, es la que proporcionan la Ley 2/1974, de 13 de febrero, sobre Colegios Profesionales y la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

¿A qué destinatarios se comunicarán sus datos?
Su queja, los documentos que acompañe y los datos personales contenidos en ellos se incorporarán a un expediente administrativo al que tendrán acceso el o los denunciados y quienes sean interesados legítimos de acuerdo con la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, así como quien tenga derecho de acceso a la información pública, con los límites que apliquen, de conformidad con la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno

En la tramitación de recursos los datos personales contenidos en el expediente podrán comunicarse a Juzgados y Tribunales.

En su caso, el dato de situación de habilitación profesional, o no, se publicará en la ventanilla única del Colegio según la Ley 2/1974, de 13 de febrero, sobre Colegios Profesionales.

¿Cuál es la procedencia de los datos?
Los datos personales que tratará el Colegio son los que usted proporcione, incorporados a su queja, a los documentos anexos o a otros escritos que formule en el procedimiento. También se tratarán los datos que respecto de su persona puedan aportar otras partes en el procedimiento al que dé lugar la queja o los que provengan de terceras personas como resultado de las pruebas que se practiquen en el procedimiento.

¿Qué categorías de datos trata el Colegio?
El Colegio tratará los datos que nos suministre y los que se incorporen al expediente, que pueden ser, entre otras, de las siguientes categorías:
- Datos de carácter identificativo
- Características personales
- Circunstancias sociales
- Datos académicos y profesionales
- Datos de detalle del empleo, datos económico-financieros y seguros, etc...

¿Cuáles son sus derechos?
Cualquier persona tiene derecho a obtener confirmación sobre si el Colegio de Ingenieros de Caminos, Canales y Puertos trata datos personales que le conciernen, o no.

Las personas interesadas tienen derecho a acceder a sus datos personales y a obtener una copia de los datos personales objeto del tratamiento, a actualizarlos, así como a solicitar la rectificación de los datos inexactos o, en su caso, solicitar su supresión cuando, entre otros motivos, los datos ya no sean necesarios para los fines para los que fueron recogidos.

En determinadas circunstancias previstas en el artículo 18 RGPD, los interesados podrán solicitar la limitación del tratamiento de sus datos, en cuyo caso únicamente los conservaremos para el ejercicio o la defensa de reclamaciones.

Como consecuencia de la aplicación del derecho a la supresión u oposición al tratamiento de datos personales en el entorno on-line los interesados tienen, en su caso, el derecho al olvido según la jurisprudencia que el Tribunal de Justicia de la UE.

Los interesados podrán oponerse al tratamiento de sus datos con fines de mercadotecnia, incluida la elaboración de perfiles. En particular, los colegiados tienen derecho a que el Colegio indique gratuitamente respecto de los sus datos personales que se publican en la ventanilla única que no pueden utilizarse para fines de publicidad o prospección comercial.

El colegiado sólo se puede oponer a la publicación de sus datos, los que proceda según la Ley de Colegios Profesionales, en la ventanilla única por motivos fundados y legítimos, por ejemplo por amenaza terrorista o de violencia de género.

Si se editara el registro de colegiados en otro tipo de fuente accesible al público diferente a la ventanilla única (p.ej. en papel), el colegiado se puede oponer a la publicación si coincide con el domicilio personal.

En virtud del derecho a la portabilidad, los interesados tienen derecho a obtener los datos personales que les incumben en un formato estructurado de uso común y lectura mecánica y a transmitirlos a otro responsable.

El interesado tiene el derecho a la supresión de sus datos, por la desaparición de la finalidad que motivó el tratamiento o la recogida, por revocación del consentimiento cuando sea éste el que legitime el tratamiento, o por el resto de motivos contenidos en el artículo 17 RGPD.

¿Cómo se pueden ejercer los derechos?
- Mediante un escrito dirigido a Colegio de Ingenieros de Caminos, Canales y Puertos. Calle Almagro, 42, 28010 Madrid.
- Mediante correo electrónico dirigido a: secretariogeneral@ciccp.es

¿Qué vías de reclamación existen?
Si considera que sus derechos no se han atendido debidamente, tiene derecho a presentar una reclamación ante la Agencia Española de Protección de Datos, cuyos datos de contacto son:

Teléfonos: 901 100 099 91.266.35.17
Dirección Postal: C/ Jorge Juan, 6, 28001 Madrid
Sede Electrónica:
https://sedeagpd.gob.es/sede-electronica-web/
Página web: http://www.agpd.es

GESTIÓN DE VISADOS

Gestión de órganos colegiales

¿Quién es el responsable del tratamiento de sus datos?
Identidad: Colegio de Ingenieros de Caminos, Canales y Puertos
CIF: Q-2867009-I
Dirección Postal: c/Almagro 42, 28010 Madrid
Teléfono: 91.308.19.88
Correo electrónico: atencioncolegial@ciccp.es
Web: http://www.ciccp.es
Contacto Delegado de Protección de Datos: dpo@ciccp.es
Ventanilla única: http://www3.ciccp.es/ventanilla-unica

¿Con qué finalidad tratamos sus datos personales?
El Colegio de Ingenieros de Caminos, Canales y Puertos tratará los datos con la finalidad de gestionar los órganos colegiales y la secretaría de los mismos, incluyendo la convocatoria a las sesiones y confección y archivo de actas.

¿Cuánto tiempo conservaremos sus datos?
Los datos personales proporcionados se conservarán mientras se mantenga su condición de colegiado, no se solicite su supresión por el interesado o cuando los datos dejen de ser necesarios -incluyendo la necesidad de conservarlos durante los plazos de prescripción aplicables- o pertinentes para la finalidad para la cual hubieran sido recabados o registrados.

La supresión, eliminación o destrucción de los datos tratados en el ejercicio de funciones públicas se realizará de conformidad con lo establecido en la Ley 16/1985, de 25 de junio, del Patrimonio Histórico Español y sólo pueden ser destruidos previa regulación de un procedimiento que salvaguarde el valor probatorio de derechos y obligaciones y los valores artísticos e históricos que puedan tener los documentos, por acuerdo del órgano competente.

Legitimación
La base legal del tratamiento es la siguiente:

RGPD: 6.1.a) Consentimiento del interesado

RGPD: 6.1.e) Tratamiento necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento.

RGPD: 6.1.c) Tratamiento necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento.

Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno

Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

Ley 2/1974, de 13 de febrero, sobre Colegios Profesionales.

Real Decreto 1271/2003, de 10 de octubre por el que se aprueban los Estatutos del Colegio de Ingenieros de Caminos, Canales y Puertos.

¿A qué destinatarios se comunicarán sus datos?
En su caso y si procede legalmente
- Publicación de datos identificativos en la web del Colegio y su ventanilla única.
- Registros y Administraciones Públicas competentes.
- Distribución de actas de órganos colegiales a interesados legítimos.

¿Cuál es la procedencia de los datos?
Los datos que tratará el Colegio son las que proporciona el interesado y los resultantes de la incorporación de datos a las actas de los órganos colegiales.

¿Qué categorías de datos trata el Colegio?
El Colegio tratará datos identificativos, datos profesionales y de contacto de los miembros de los órganos colegiales, así como aquellos datos que se incorporen a las actas de éstos.

¿Cuáles son sus derechos?
Cualquier persona tiene derecho a obtener confirmación sobre si el Colegio de Ingenieros de Caminos, Canales y Puertos trata datos personales que le conciernen, o no.

Las personas interesadas tienen derecho a acceder a sus datos personales y a obtener una copia de los datos personales objeto del tratamiento, a actualizarlos, así como a solicitar la rectificación de los datos inexactos o, en su caso, solicitar su supresión cuando, entre otros motivos, los datos ya no sean necesarios para los fines para los que fueron recogidos.

En determinadas circunstancias previstas en el artículo 18 RGPD, los interesados podrán solicitar la limitación del tratamiento de sus datos, en cuyo caso únicamente los conservaremos para el ejercicio o la defensa de reclamaciones.

Como consecuencia de la aplicación del derecho a la supresión u oposición al tratamiento de datos personales en el entorno on-line los interesados tienen, en su caso, el derecho al olvido según la jurisprudencia que el Tribunal de Justicia de la UE.

Los interesados podrán oponerse al tratamiento de sus datos con fines de mercadotecnia, incluida la elaboración de perfiles. En particular, los colegiados tienen derecho a que el Colegio indique gratuitamente respecto de los sus datos personales que se publican en la ventanilla única que no pueden utilizarse para fines de publicidad o prospección comercial.

El colegiado sólo se puede oponer a la publicación de sus datos, los que proceda según la Ley de Colegios Profesionales, en la ventanilla única por motivos fundados y legítimos, por ejemplo por amenaza terrorista o de violencia de género. Si se editara el registro de colegiados en otro tipo de fuente accesible al público diferente a la ventanilla única (p.ej. en papel), el colegiado se puede oponer a la publicación si coincide con el domicilio personal.

En virtud del derecho a la portabilidad, los interesados tienen derecho a obtener los datos personales que les incumben en un formato estructurado de uso común y lectura mecánica y a transmitirlos a otro responsable.

El interesado tiene el derecho a la supresión de sus datos, por la desaparición de la finalidad que motivó el tratamiento o la recogida, por revocación del consentimiento cuando sea éste el que legitime el tratamiento, o por el resto de motivos contenidos en el artículo 17 RGPD.

¿Cómo se pueden ejercer los derechos?
- Mediante un escrito dirigido a Colegio de Ingenieros de Caminos, Canales y Puertos. Calle Almagro, 42, 28010 Madrid.
- Mediante correo electrónico dirigido a: secretariogeneral@ciccp.es

¿Qué vías de reclamación existen?
Si considera que sus derechos no se han atendido debidamente, tiene derecho a presentar una reclamación ante la Agencia Española de Protección de Datos, cuyos datos de contacto son:

Teléfonos: 901 100 099 91.266.35.17
Dirección Postal: C/ Jorge Juan, 6, 28001 Madrid
Sede Electrónica:
https://sedeagpd.gob.es/sede-electronica-web/
Página web: http://www.agpd.es

Registro de peritos ICCP

¿Quién es el responsable del tratamiento de sus datos?
Identidad: Colegio de Ingenieros de Caminos, Canales y Puertos
CIF: Q-2867009-I
Dirección Postal: c/Almagro 42, 28010 Madrid
Teléfono: 91.308.19.88
Correo electrónico: atencioncolegial@ciccp.es
Web: http://www.ciccp.es
Contacto Delegado de Protección de Datos: dpo@ciccp.es
Ventanilla única: http://www3.ciccp.es/ventanilla-unica

¿Con qué finalidad tratamos sus datos personales?
Según la finalidad que se haya autorizado el Colegio de Ingenieros de Caminos, canales y Puertos, tratará los datos con la finalidad de:

La gestión del Registro de Peritos y Expertos Ingenieros de Caminos, Canales y Puertos, según las Normas Generales del Registro de Peritos aprobadas por el Consejo General del Colegio en su sesión del día 5 de marzo de 2014. El listado derivado del registro se envía a la Administración de Justicia, Juzgados y Tribunales, Consejo General del Notariado, Colegios Notariales.

La gestión de los registros de expertos a los que el colegiado se inscriba.

Sus datos podrán ser utilizados para el envío por el Colegio a su dirección de correo electrónico o postal de comunicaciones relativas a tales finalidades.

Si el colegiado lo autoriza y así lo acordarán los órganos colegiales competentes, los listados, en su caso, se podrán editar, publicar y distribuir públicamente.

¿Cuánto tiempo conservaremos sus datos?
Los datos personales proporcionados se conservarán mientras se mantenga su condición de perito , no se solicite su supresión por el interesado y ésta proceda, y mientras sean necesarios -incluyendo la necesidad de conservarlos durante los plazos de prescripción aplicables- o pertinentes para la finalidad para la cual hubieran sido recabados o registrados.

La supresión, eliminación o destrucción de los datos tratados en el ejercicio de funciones públicas se realizará de conformidad con lo establecido en la Ley 16/1985, de 25 de junio, del Patrimonio Histórico Español y sólo pueden ser destruidos previa regulación de un procedimiento que salvaguarde el valor probatorio de derechos y obligaciones y los valores artísticos e históricos que puedan tener los documentos, por acuerdo del órgano competente

Legitimación
El tratamiento de sus datos tiene el siguiente amparo en el Reglamento General de Protección de Datos:

· RGPD: 6.1.a) Consentimiento del interesado.

· RGPD: 6.1.e) Tratamiento necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento.

· RGPD: 6.1.c) Tratamiento necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento.

Así, la base legal del tratamiento de sus datos es el consentimiento prestado inicialmente con su solicitud de alta en el listado de Contadores-Partidores, y posteriormente la habilitación legal de la Ley de Enjuiciamiento Civil, de 7 de enero de 2000 y de la Ley del Notariado de 28 de mayo de 1862. según Ley 15/2015, de 2 de julio, para la designación de contadores partidores por Jueces y Tribunales y Notarios.

La base legal del tratamiento de sus datos para la gestión del registro de peritos será el consentimiento.

El consentimiento puede ser revocado.

¿A qué destinatarios se comunicarán sus datos?
Como consecuencia de la gestión del listado derivado del Registro podrán comunicarse datos personales a la Administración de Justicia, a los Órganos Judiciales, al Consejo General del Notariado, a Colegios Notariales y a Notarios, así como otras instituciones que requieran los listados de peritos y expertos

Como consecuencia de la gestión de otros registros podrán comunicarse datos a los solicitantes de expertos.

Si lo autoriza el interesado y los órganos colegiales lo acordaran, se podrán editar listados en formato papel y digital, así como distribuir públicamente.

¿Cuál es la procedencia de los datos?
Los datos personales que tratará el Colegio son los que usted proporcione, en el formulario de alta o en otros momentos posteriores.

¿Qué categorías de datos trata el Colegio?
El Colegio tratará los datos que nos suministre, que pueden ser de las siguientes categorías:

- Datos de carácter identificativo
- Datos académicos y profesionales.
No se tratarán categorías especiales de datos.

¿Cuáles son sus derechos?
Cualquier persona tiene derecho a obtener confirmación sobre si el Colegio de Ingenieros de Caminos, Canales y Puertos trata datos personales que le conciernen, o no.

Las personas interesadas tienen derecho a acceder a sus datos personales y a obtener una copia de los datos personales objeto del tratamiento, a actualizarlos, así como a solicitar la rectificación de los datos inexactos o, en su caso, solicitar su supresión cuando, entre otros motivos, los datos ya no sean necesarios para los fines para los que fueron recogidos.

En determinadas circunstancias previstas en el artículo 18 RGPD, los interesados podrán solicitar la limitación del tratamiento de sus datos, en cuyo caso únicamente los conservaremos para el ejercicio o la defensa de reclamaciones.

Como consecuencia de la aplicación del derecho a la supresión u oposición al tratamiento de datos personales en el entorno on-line los interesados tienen, en su caso, el derecho al olvido según la jurisprudencia que el Tribunal de Justicia de la UE.

Los interesados podrán oponerse al tratamiento de sus datos con fines de mercadotecnia, incluida la elaboración de perfiles. En particular, los colegiados tienen derecho a que el Colegio indique gratuitamente respecto de los sus datos personales que se publican en la ventanilla única que no pueden utilizarse para fines de publicidad o prospección comercial.

El colegiado sólo se puede oponer a la publicación de sus datos, los que proceda según la Ley de Colegios Profesionales, en la ventanilla única por motivos fundados y legítimos, por ejemplo por amenaza terrorista o de violencia de género. Si se editara el registro de colegiados en otro tipo de fuente accesible al público diferente a la ventanilla única (p.ej. en papel), el colegiado se puede oponer a la publicación si coincide con el domicilio personal.

En virtud del derecho a la portabilidad, los interesados tienen derecho a obtener los datos personales que les incumben en un formato estructurado de uso común y lectura mecánica y a transmitirlos a otro responsable.

El interesado tiene el derecho a la supresión de sus datos, por la desaparición de la finalidad que motivó el tratamiento

o la recogida, por revocación del consentimiento cuando sea éste el que legitime el tratamiento, o por el resto de motivos contenidos en el artículo 17 RGPD.

¿Cómo se pueden ejercer los derechos?
- Mediante un escrito dirigido a Colegio de Ingenieros de Caminos, Canales y Puertos. Calle Almagro, 42, 28010 Madrid.
- Mediante correo electrónico dirigido a: secretariogeneral@ciccp.es

¿Qué vías de reclamación existen?
Si considera que sus derechos no se han atendido debidamente, tiene derecho a presentar una reclamación ante la Agencia Española de Protección de Datos, cuyos datos de contacto son:

Teléfonos: 901 100 099 91.266.35.17
Dirección Postal: C/ Jorge Juan, 6, 28001 Madrid
Sede Electrónica:
https://sedeagpd.gob.es/sede-electronica-web/
Página web: http://www.agpd.es

Gestión MediaCaminos y cortes de arbitraje

¿Quién es el responsable del tratamiento de sus datos?
Identidad: Colegio de Ingenieros de Caminos, Canales y Puertos
CIF: Q-2867009-I
Dirección Postal: c/Almagro 42, 28010 Madrid
Teléfono: 91.308.19.88
Correo electrónico: atencioncolegial@ciccp.es
Web: http://www.ciccp.es
Contacto Delegado de Protección de Datos: dpo@ciccp.es
Ventanilla única: http://www3.ciccp.es/ventanilla-unica

¿Con qué finalidad tratamos sus datos personales?
El Colegio de Ingenieros de Caminos, Canales y Puertos, a través de la institución de mediación colegial MediaCAMINOS, tratará sus datos con la finalidad de gestionar la institución de mediación MediaCAMINOS, el censo de mediadores, la designación de mediadores y los procedimientos de mediación.

Sus datos podrán ser utilizados, si lo autoriza, para el envío por el Colegio de información relativa a la mediación, a cursos, actos o eventos que pudiese organizar MediaCAMINOS, así como terceros, todos ellos relacionados con la mediación.

¿Cuánto tiempo conservaremos sus datos?
Los datos personales proporcionados se conservarán mientras sean necesarios y pertinentes -incluyendo la necesidad de conservarlos durante los plazos de prescripción aplicables- para la finalidad para la cual han sido proporcionados, recabados o registrados.

La supresión, eliminación o destrucción de los datos tratados en el ejercicio de funciones públicas se realizará de conformidad con lo establecido en la Ley 16/1985, de 25 de junio, del Patrimonio Histórico Español y sólo pueden ser destruidos previa regulación de un procedimiento que salvaguarde el valor probatorio de derechos y obligaciones y los valores artísticos e históricos que puedan tener los documentos, por acuerdo del órgano competente.

Legitimación
El tratamiento de sus datos tiene el siguiente amparo en el Reglamento General de Protección de Datos:

- RGPD: 6.1.a) Consentimiento del interesado.

- RGPD: 6.1.e) Tratamiento necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento.

- RGPD: 6.1.c) Tratamiento necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento.

Así, la legitimación inicial del tratamiento de sus datos personales es el consentimiento expreso que presta al solicitar el alta en MediaCAMINOS y la base legal del tratamiento posterior, así como de la publicidad de los datos y las posibles comunicaciones a terceros, es la que proporcionan la Ley 2/1974, de 13 de febrero, sobre Colegios Profesionales y la Ley 5/2012, de 6 de julio, de mediación en asuntos civiles y mercantiles.

La legitimación para las finalidades adicionales (de envío de información relativa a la mediación, a cursos, actos y/o eventos que pudiese organizar MediaCAMINOS, así como terceros, todos ellos relacionados con la mediación) es el consentimiento.

El consentimiento puede ser revocado en cualquier momento.

¿A qué destinatarios se comunicarán sus datos?
Sus datos se pueden comunicar a las partes en los procedimientos de mediación.

De conformidad con el artículo 5 de la Ley 5/2012, de 6 de julio, de mediación en asuntos civiles y mercantiles, MediaCAMINOS dará a conocer la identidad de los mediadores que actúen dentro de su ámbito, informando, al menos, de su formación,

especialidad y experiencia en el ámbito de la mediación a la que se dediquen.

De conformidad con el Real Decreto 980/2013, de 13 de diciembre, por el que se desarrollan determinados aspectos de la Ley 5/2012, de 6 de julio, de mediación en asuntos civiles y mercantiles, se comunicará Registro de Mediadores e Instituciones de Mediación (Ministerio de Justicia) la identidad de los mediadores.

¿Cuál es la procedencia de los datos?
Los datos personales que tratará el Colegio son los que usted proporcione, incorporados a su solicitud, o que comunique posteriormente.

¿Qué categorías de datos trata el Colegio?
El Colegio tratará los datos que nos suministre, que pueden ser, entre otras, de las siguientes categorías: Datos de carácter identificativo
- Características personales
- Datos académicos y profesionales
- Datos de detalle del empleo
- Datos bancarios y económico-financieros y seguros, etc.

¿Cuáles son sus derechos?
Cualquier persona tiene derecho a obtener confirmación sobre si el Colegio de Ingenieros de Caminos, Canales y Puertos trata datos personales que le conciernen, o no.

Las personas interesadas tienen derecho a acceder a sus datos personales y a obtener una copia de los datos personales objeto del tratamiento, a actualizarlos, así como a solicitar la rectificación de los datos inexactos o, en su caso, solicitar su supresión cuando, entre otros motivos, los datos ya no sean necesarios para los fines para los que fueron recogidos.

En determinadas circunstancias previstas en el artículo 18 RGPD, los interesados podrán solicitar la limitación del tratamiento de sus datos, en cuyo caso únicamente los conservaremos para el ejercicio o la defensa de reclamaciones.

Como consecuencia de la aplicación del derecho a la supresión u oposición al tratamiento de datos personales en el entorno on-line los interesados tienen, en su caso, el derecho al olvido según la jurisprudencia que el Tribunal de Justicia de la UE.

Los interesados podrán oponerse al tratamiento de sus datos con fines de mercadotecnia, incluida la elaboración de perfiles.

En particular, los colegiados tienen derecho a que el Colegio indique gratuitamente respecto de los sus datos personales que se publican en la ventanilla única que no pueden utilizarse para fines de publicidad o prospección comercial.

El colegiado sólo se puede oponer a la publicación de sus datos, los que proceda según la Ley de Colegios Profesionales, en la ventanilla única por motivos fundados y legítimos, por ejemplo por amenaza terrorista o de violencia de género.

Si se editara el registro de colegiados en otro tipo de fuente accesible al público diferente a la ventanilla única (p.ej. en papel), el colegiado se puede oponer a la publicación si coincide con el domicilio personal.

En virtud del derecho a la portabilidad, los interesados tienen derecho a obtener los datos personales que les incumben en un formato estructurado de uso común y lectura mecánica y a transmitirlos a otro responsable.

El interesado tiene el derecho a la supresión de sus datos, por la desaparición de la finalidad que motivó el tratamiento o la recogida, por revocación del consentimiento cuando sea éste el que legitime el tratamiento, o por el resto de motivos contenidos en el artículo 17 RGPD.

¿Cómo se pueden ejercer los derechos?
- Mediante un escrito dirigido a Colegio de Ingenieros de Caminos, Canales y Puertos. Calle Almagro, 42, 28010 Madrid.
- Mediante correo electrónico dirigido a: secretariogeneral@ciccp.es

¿Qué vías de reclamación existen?
Si considera que sus derechos no se han atendido debidamente, tiene derecho a presentar una reclamación ante la Agencia Española de Protección de Datos, cuyos datos de contacto son:

Teléfonos: 901 100 099 91.266.35.17
Dirección Postal: C/ Jorge Juan, 6, 28001 Madrid
Sede Electrónica:
https://sedeagpd.gob.es/sede-electronica-web/
Página web: http://www.agpd.es

Asesoría jurídica
Agencia de colocación

¿Quién es el responsable del tratamiento de sus datos?
Identidad: Colegio de Ingenieros de Caminos, Canales y Puertos
CIF: Q-2867009-I

Dirección Postal: c/Almagro 42, 28010 Madrid
Teléfono: 91.308.19.88
Correo electrónico: atencioncolegial@ciccp.es
Web: http://www.ciccp.es
Contacto Delegado de Protección de Datos: dpo@ciccp.es
Ventanilla única: http://www3.ciccp.es/ventanilla-unica

¿Con qué finalidad tratamos sus datos personales?
Si es usted demandante de empleo el Colegio de Ingenieros de Caminos, Canales y Puertos tratará sus datos de carácter personal para la gestión de la Agencia de Colocación, la comunicación de sus datos a ofertantes de empleo y la remisión de información relativa a la búsqueda y mejora del empleo.

Si es usted ofertante de empleo el Colegio de Ingenieros de Caminos, Canales y Puertos tratará sus datos de carácter personal para la gestión de la Agencia de Colocación, la comunicación de sus datos a demandantes de empleo y la gestión de la oferta de empleo.

Sus datos podrán ser utilizados para la emisión de certificados

¿Cuánto tiempo conservaremos sus datos?
Los datos personales proporcionados se conservarán mientras sean necesarios y pertinentes -incluyendo la necesidad de conservarlos durante los plazos de prescripción aplicables- para la finalidad para la cual han sido proporcionados, recabados o registrados.

Si es usted demandante de empleo y no actualizara su datos, el curriculum o no realizara gestión alguna de búsqueda de empleo por el plazo de un año sus datos serán suprimidos, implicando el bloqueo de los mismos.

La supresión, eliminación o destrucción de los datos tratados en el ejercicio de funciones públicas se realizará de conformidad con lo establecido en la Ley 16/1985, de 25 de junio, del Patrimonio Histórico Español y sólo pueden ser destruidos previa regulación de un procedimiento que salvaguarde el valor probatorio de derechos y obligaciones y los valores artísticos e históricos que puedan tener los documentos, por acuerdo del órgano competente.

Legitimación
El tratamiento de sus datos tiene el siguiente amparo en el Reglamento General de Protección de Datos:

- RGPD: 6.1.a) Consentimiento del interesado.

El consentimiento puede ser revocado en cualquier momento.

¿A qué destinatarios se comunicarán sus datos?
Si es usted demandante de empleo, como consecuencia de la gestión de las finalidades autorizadas sus datos podrán ser comunicados a ofertantes de empleo.

Si es usted ofertante de empleo, como consecuencia de la gestión de las finalidades autorizadas sus datos podrán ser comunicados a demandantes de empleo.

¿Cuál es la procedencia de los datos?
Los datos personales que tratará el Colegio son los que usted proporcione, incorporados al formulario o solicitud, o que comunique posteriormente con las finalidades autorizadas.

Podrá tratar también datos que proporcionen los ofertantes o los demandantes de empleo, relativos a la selección o contratación.

¿Qué categorías de datos trata el Colegio?
El Colegio tratará los datos que nos suministre, que pueden ser de las siguientes categorías:
- Datos de carácter identificativo
- Características personales
- Circunstancias sociales
- Datos académicos y profesionales
- Datos de detalle del empleo
- Datos económico-financieros

También podrá tratar datos relativos a la selección o contratación.

¿Cuáles son sus derechos?
Cualquier persona tiene derecho a obtener confirmación sobre si el Colegio de Ingenieros de Caminos, Canales y Puertos trata datos personales que le conciernen, o no.

Las personas interesadas tienen derecho a acceder a sus datos personales y a obtener una copia de los datos personales objeto del tratamiento, a actualizarlos, así como a solicitar la rectificación de los datos inexactos o, en su caso, solicitar su supresión cuando, entre otros motivos, los datos ya no sean necesarios para los fines para los que fueron recogidos.

En determinadas circunstancias previstas en el artículo 18 RGPD, los interesados podrán solicitar la limitación del tratamiento de sus datos, en cuyo caso únicamente los conservaremos para el ejercicio o la defensa de reclamaciones.

Como consecuencia de la aplicación del derecho a la supresión u oposición al tratamiento de datos personales en el en-

torno on-line los interesados tienen, en su caso, el derecho al olvido según la jurisprudencia que el Tribunal de Justicia de la UE.

Los interesados podrán oponerse al tratamiento de sus datos con fines de mercadotecnia, incluida la elaboración de perfiles. En particular, los colegiados tienen derecho a que el Colegio indique gratuitamente respecto de los sus datos personales que se publican en la ventanilla única que no pueden utilizarse para fines de publicidad o prospección comercial.

El colegiado sólo se puede oponer a la publicación de sus datos, los que proceda según la Ley de Colegios Profesionales, en la ventanilla única por motivos fundados y legítimos, por ejemplo por amenaza terrorista o de violencia de género.

Si se editara el registro de colegiados en otro tipo de fuente accesible al público diferente a la ventanilla única (p.ej. en papel), el colegiado se puede oponer a la publicación si coincide con el domicilio personal.

En virtud del derecho a la portabilidad, los interesados tienen derecho a obtener los datos personales que les incumben en un formato estructurado de uso común y lectura mecánica y a transmitirlos a otro responsable

El interesado tiene el derecho a la supresión de sus datos, por la desaparición de la finalidad que motivó el tratamiento o la recogida, por revocación del consentimiento cuando sea éste el que legitime el tratamiento, o por el resto de motivos contenidos en el artículo 17 RGPD.

¿Cómo se pueden ejercer los derechos?
- Mediante un escrito dirigido a Colegio de Ingenieros de Caminos, Canales y Puertos. Calle Almagro, 42, 28010 Madrid.
- Mediante correo electrónico dirigido a: secretariogeneral@ciccp.es

¿Qué vías de reclamación existen?
Si considera que sus derechos no se han atendido debidamente, tiene derecho a presentar una reclamación ante la Agencia Española de Protección de Datos, cuyos datos de contacto son:

Teléfonos: 901 100 099 91.266.35.17
Dirección Postal: C/ Jorge Juan, 6, 28001 Madrid
Sede Electrónica:
https://sedeagpd.gob.es/sede-electronica-web/
Página web: http://www.agpd.es

Antiguos colegiados (colegiados dados de baja y precolegiados)

¿Quién es el responsable del tratamiento de sus datos?
Identidad: Colegio de Ingenieros de Caminos, Canales y Puertos
CIF: Q-2867009-I
Dirección Postal: c/Almagro 42, 28010 Madrid
Teléfono: 91.308.19.88
Correo electrónico: atencioncolegial@ciccp.es
Web: http://www.ciccp.es
Contacto Delegado de Protección de Datos: dpo@ciccp.es
Ventanilla única: http://www3.ciccp.es/ventanilla-unica

¿Con qué finalidad tratamos sus datos personales?
El Colegio de Ingenieros de Caminos, Canales y Puertos tratará sus datos con el fin de gestionar la relación con sus antiguos colegiados.

Sus datos podrán ser utilizados, si lo autoriza, para el envío por el Colegio de información colegial y relevante para los Ingenieros de Caminos, Canales y Puertos.

Sus datos podrán ser utilizados para la emisión de certificados

¿Cuánto tiempo conservaremos sus datos?
Los datos personales proporcionados se conservarán mientras se mantenga su condición de colegiado, no se solicite su supresión por el interesado o cuando los datos dejen de ser necesarios -incluyendo la necesidad de conservarlos durante los plazos de prescripción aplicables- o pertinentes para la finalidad para la cual hubieran sido recabados o registrados.

La supresión, eliminación o destrucción de los datos tratados en el ejercicio de funciones públicas se realizará de conformidad con lo establecido en la Ley 16/1985, de 25 de junio, del Patrimonio Histórico Español y sólo pueden ser destruidos previa regulación de un procedimiento que salvaguarde el valor probatorio de derechos y obligaciones y los valores artísticos e históricos que puedan tener los documentos, por acuerdo del órgano competente.

Legitimación
La base legal del tratamiento es la siguiente:

RGPD: 6.1.a) Consentimiento del interesado. La base legal para el envío de información no colegial relativa a formación o de interés profesional y para la realización de encuestas de calidad y satisfacción sobre la prestación de servicios es el consentimiento que usted presta que podrá retirar en cualquier momento.

¿A qué destinatarios se comunicarán sus datos?
No se prevé comunicación de datos

¿Cuál es la procedencia de los datos?
Los datos personales que tratará el Colegio son los que usted proporcione, en el formulario de baja o en otros momentos posteriores.

¿Qué categorías de datos trata el Colegio?
El Colegio tratará los datos que nos suministre, que pueden ser de las siguientes categorías:
- Datos de carácter identificativo
- Características personales
- Datos académicos y profesionales
- Datos de detalle del empleo
No se tratarán categorías especiales de datos.

¿Cuáles son sus derechos?
Cualquier persona tiene derecho a obtener confirmación sobre si el Colegio de Ingenieros de Caminos, Canales y Puertos trata datos personales que le conciernen, o no.

Las personas interesadas tienen derecho a acceder a sus datos personales y a obtener una copia de los datos personales objeto del tratamiento, a actualizarlos, así como a solicitar la rectificación de los datos inexactos o, en su caso, solicitar su supresión cuando, entre otros motivos, los datos ya no sean necesarios para los fines para los que fueron recogidos.

En determinadas circunstancias previstas en el artículo 18 RGPD, los interesados podrán solicitar la limitación del tratamiento de sus datos, en cuyo caso únicamente los conservaremos para el ejercicio o la defensa de reclamaciones.

Como consecuencia de la aplicación del derecho a la supresión u oposición al tratamiento de datos personales en el entorno on-line los interesados tienen, en su caso, el derecho al olvido según la jurisprudencia que el Tribunal de Justicia de la UE.

Los interesados podrán oponerse al tratamiento de sus datos con fines de mercadotecnia, incluida la elaboración de perfiles. En particular, los colegiados tienen derecho a que el Colegio indique gratuitamente respecto de los sus datos personales que se publican en la ventanilla única que no pueden utilizarse para fines de publicidad o prospección comercial.

El colegiado sólo se puede oponer a la publicación de sus datos, los que proceda según la Ley de Colegios Profesionales, en la ventanilla única por motivos fundados y legítimos, por ejemplo por amenaza terrorista o de violencia de género.

Si se editara el registro de colegiados en otro tipo de fuente accesible al público diferente a la ventanilla única (p.ej. en papel), el colegiado se puede oponer a la publicación si coincide con el domicilio personal.

En virtud del derecho a la portabilidad, los interesados tienen derecho a obtener los datos personales que les incumben en un formato estructurado de uso común y lectura mecánica y a transmitirlos a otro responsable.

El interesado tiene el derecho a la supresión de sus datos, por la desaparición de la finalidad que motivó el tratamiento o la recogida, por revocación del consentimiento cuando sea éste el que legitime el tratamiento, o por el resto de motivos contenidos en el artículo 17 RGPD.

¿Cómo se pueden ejercer los derechos?
- Mediante un escrito dirigido a Colegio de Ingenieros de Caminos, Canales y Puertos. Calle Almagro, 42, 28010 Madrid.
- Mediante correo electrónico dirigido a: secretariogeneral@ciccp.es

¿Qué vías de reclamación existen?
Si considera que sus derechos no se han atendido debidamente, tiene derecho a presentar una reclamación ante la Agencia Española de Protección de Datos, cuyos datos de contacto son:

Teléfonos: 901 100 099 91.266.35.17
Dirección Postal: C/ Jorge Juan, 6, 28001 Madrid
Sede Electrónica:
https://sedeagpd.gob.es/sede-electronica-web/
Página web: http://www.agpd.es

¿Con qué finalidad tratamos sus datos personales?
El Colegio de Ingenieros de Caminos, Canales y Puertos tratará sus datos con el fin de gestionar la precolegiación y la relación del Colegio con el precolegiado, envío de información sobre actividades colegiales y de formación, así como la prestación de servicios. Realización de encuestas, sobre el Colegio, sobre la calidad y satisfacción de los servicios y aspectos relacionados con la titulación y profesión. Sus datos podrán ser utilizados para la emisión de certificados

¿Cuánto tiempo conservaremos sus datos?
Los datos personales proporcionados se conservarán mientras no revoque su consentimiento, se mantenga su condición

de precolegiado, no se solicite su supresión por el interesado o cuando los datos dejen de ser necesarios -incluyendo la necesidad de conservarlos durante los plazos de prescripción aplicables- o pertinentes para la finalidad para la cual hubieran sido recabados o registrados.

La supresión, eliminación o destrucción de los datos tratados en el ejercicio de funciones públicas se realizará de conformidad con lo establecido en la Ley 16/1985, de 25 de junio, del Patrimonio Histórico Español y sólo pueden ser destruidos previa regulación de un procedimiento que salvaguarde el valor probatorio de derechos y obligaciones y los valores artísticos e históricos que puedan tener los documentos, por acuerdo del órgano competente.

Legitimación
La base legal del tratamiento de sus datos es el consentimiento que usted presta y que podrá retirar en cualquier momento.

El tratamiento para las finalidades principales no está supeditado al consentimiento para el tratamiento de los datos que no sean necesarios para dichas finalidades.

¿A qué destinatarios se comunicarán sus datos?
No se prevén cesiones.

¿Cuál es la procedencia de los datos?
Los datos personales que tratará el Colegio son los que usted proporcione, en el formulario de inscripción o en otros momentos posteriores.

¿Qué categorías de datos trata el Colegio?
El Colegio tratará los datos que nos suministre, que pueden ser de las siguientes categorías:
- Datos de carácter identificativo
- Datos académicos y profesionales
No se tratarán categorías especiales de datos.

Gestión de cursos y formación

¿Quién es el responsable del tratamiento de sus datos?
Identidad: Colegio de Ingenieros de Caminos, Canales y Puertos
CIF: Q-2867009-I
Dirección Postal: c/Almagro 42, 28010 Madrid
Teléfono: 91.308.19.88
Correo electrónico: atencioncolegial@ciccp.es
Web: http://www.ciccp.es
Contacto Delegado de Protección de Datos: dpo@ciccp.es
Ventanilla única: http://www3.ciccp.es/ventanilla-unica

¿Con qué finalidad tratamos sus datos personales?
El Colegio de Ingenieros de Caminos, Canales y Puertos tratará sus datos con la finalidad principal de gestionar su asistencia a jornadas y eventos o como alumno en cursos o actividades organizadas por el Colegio, incluyendo en dicha finalidad, si procede, la facturación de los cursos en los que se matricula, el envío de comunicaciones relacionadas con las jornadas o cursos en los que se inscribe, así como la de conocer la satisfacción y opinión sobre la calidad de las jornadas celebradas y de los cursos impartidos.

En el caso de cursos y actividades formativas, sus datos se tratarán para la evaluación y calificación.

Sus datos podrán ser utilizados, si lo autoriza, para el envío por el Colegio de información relativa a la actividad formativa y a la realización de jornadas y eventos.

Sus datos podrán ser utilizados para la emisión de certificados

¿Cuánto tiempo conservaremos sus datos?
Los datos personales proporcionados se conservarán mientras se mantenga su condición de alumno o haya obligaciones pendientes de cumplimiento, no se solicite su supresión por el interesado o cuando los datos dejen de ser necesarios -incluyendo la necesidad de conservarlos durante los plazos de prescripción aplicables- o pertinentes para la finalidad para la cual hubieran sido recabados o registrados

Legitimación
La base legal del tratamiento es la siguiente:

RGPD: 6.1.a) Consentimiento del interesado.

El tratamiento para la finalidad principal (gestión de la participación en cursos, jornadas y eventos) no está supeditado al consentimiento para el tratamiento de los datos que no sean necesarios para dicha finalidad (envío de información relativa a la actividad de otros cursos, jornadas y eventos organizados por el Colegio).

¿A qué destinatarios se comunicarán sus datos?
En el caso de inscripciones a cursos y actividades formativas, sus datos identificativos se podrán comunicar a los directores, profesores o ponentes de los cursos o actividades formativas en los que se matricule o inscriba.

En el caso de eventos y jornadas que se retransmitan en streaming, las imágenes y el sonido podrán retransmitirse y/o publicarse en redes sociales

En el caso en el que se participe en programas de becas o de prácticas, sus datos identificativos se podrán comunicar a las empresas que formen parte de dichos programas

En el caso de eventos y jornadas en las que se realicen fotografías, las imágenes podrán publicarse en medios escritos o digitales.

En el caso de inscripciones a eventos y jornadas, no se prevén cesiones.

¿Cuál es la procedencia de los datos?
Los datos personales que tratará el Colegio son los que usted proporcione, en el formulario de inscripción o en otros momentos posteriores.

También podrá tratar los datos que le proporcionen terceras personas (como directores, profesores o ponentes de los cursos) en el ámbito del desarrollo de los cursos y del control, evaluación y calificación de su participación y desempeño.

¿Qué categorías de datos trata el Colegio?
El Colegio tratará los datos que nos suministre, que pueden ser de las siguientes categorías:
- Datos de carácter identificativo
- Otros datos identificativos (firma, imagen, voz)
- Características personales
- Datos académicos y profesionales
- Datos de detalle del empleo
- Datos bancarios y económico-financieros.

El Colegio tratará los datos derivados de su participación en las jornadas, en los cursos o actividades en los que se matricule y de, en su caso, la correspondiente evaluación y calificación. No se tratarán categorías especiales de datos.

¿Cuáles son sus derechos?
Cualquier persona tiene derecho a obtener confirmación sobre si el Colegio de Ingenieros de Caminos, Canales y Puertos trata datos personales que le conciernen, o no.

Las personas interesadas tienen derecho a acceder a sus datos personales y a obtener una copia de los datos personales objeto del tratamiento, a actualizarlos, así como a solicitar la rectificación de los datos inexactos o, en su caso, solicitar su supresión cuando, entre otros motivos, los datos ya no sean necesarios para los fines para los que fueron recogidos.

En determinadas circunstancias previstas en el artículo 18 RGPD, los interesados podrán solicitar la limitación del tratamiento de sus datos, en cuyo caso únicamente los conservaremos para el ejercicio o la defensa de reclamaciones.

Como consecuencia de la aplicación del derecho a la supresión u oposición al tratamiento de datos personales en el entorno on-line los interesados tienen, en su caso, el derecho al olvido según la jurisprudencia que el Tribunal de Justicia de la UE.

Los interesados podrán oponerse al tratamiento de sus datos con fines de mercadotecnia, incluida la elaboración de perfiles. En particular, los colegiados tienen derecho a que el Colegio indique gratuitamente respecto de los sus datos personales que se publican en la ventanilla única que no pueden utilizarse para fines de publicidad o prospección comercial.

El colegiado sólo se puede oponer a la publicación de sus datos, los que proceda según la Ley de Colegios Profesionales, en la ventanilla única por motivos fundados y legítimos, por ejemplo por amenaza terrorista o de violencia de género.

Si se editara el registro de colegiados en otro tipo de fuente accesible al público diferente a la ventanilla única (p.ej. en papel), el colegiado se puede oponer a la publicación si coincide con el domicilio personal.

En virtud del derecho a la portabilidad, los interesados tienen derecho a obtener los datos personales que les incumben en un formato estructurado de uso común y lectura mecánica y a transmitirlos a otro responsable

El interesado tiene el derecho a la supresión de sus datos, por la desaparición de la finalidad que motivó el tratamiento o la recogida, por revocación del consentimiento cuando sea éste el que legitime el tratamiento, o por el resto de motivos contenidos en el artículo 17 RGPD.

¿Cómo se pueden ejercer los derechos?
- Mediante un escrito dirigido a Colegio de Ingenieros de Caminos, Canales y Puertos. Calle Almagro, 42, 28010 Madrid.
- Mediante correo electrónico dirigido a: secretariogeneral@ciccp.es

¿Qué vías de reclamación existen?
Si considera que sus derechos no se han atendido debidamente, tiene derecho a presentar una reclamación ante la Agencia Española de Protección de Datos, cuyos datos de contacto son:

Teléfonos: 901 100 099 91.266.35.17
Dirección Postal: C/ Jorge Juan, 6, 28001 Madrid
Sede Electrónica:
https://sedeagpd.gob.es/sede-electronica-web/
Página web: http://www.agpd.es

Gestión de publicaciones y suscripciones

¿Quién es el responsable del tratamiento de sus datos?
Identidad: Colegio de Ingenieros de Caminos, Canales y Puertos
CIF: Q-2867009-I
Dirección Postal: c/Almagro 42, 28010 Madrid
Teléfono: 91.308.19.88
Correo electrónico: atencioncolegial@ciccp.es
Web: http://www.ciccp.es
Contacto Delegado de Protección de Datos: dpo@ciccp.es
Ventanilla única: http://www3.ciccp.es/ventanilla-unica

¿Con qué finalidad tratamos sus datos personales?
El Colegio de Ingenieros de Caminos, Canales y Puertos tratará sus datos con la finalidad de gestionar:
- Publicaciones.
- Suscripciones.
- Venta de publicaciones, material técnico o didáctico.

¿Cuánto tiempo conservaremos sus datos?
Los datos personales proporcionados se conservarán mientras sean necesarios y pertinentes -incluyendo la necesidad de conservarlos durante los plazos de prescripción aplicables- para la finalidad para la cual han sido proporcionados, recabados o registrados.

La supresión, eliminación o destrucción de los datos tratados en el ejercicio de funciones públicas se realizará de conformidad con lo establecido en la Ley 16/1985, de 25 de junio, del Patrimonio Histórico Español y sólo pueden ser destruidos previa regulación de un procedimiento que salvaguarde el valor probatorio de derechos y obligaciones y los valores artísticos e históricos que puedan tener los documentos, por acuerdo del órgano competente.

Legitimación
El tratamiento de sus datos tiene el siguiente amparo en el Reglamento General de Protección de Datos:

RGPD: 6.1.a) Consentimiento del interesado.

El consentimiento puede ser revocado en cualquier momento.

¿A qué destinatarios se comunicarán sus datos?
En su caso, entidades bancarias, para la tramitación de pagos y cobros.

¿Cuál es la procedencia de los datos?
Los datos personales que tratará el Colegio son los que usted proporcione, incorporados a su solicitud, o que comunique posteriormente con las finalidades autorizadas.

¿Qué categorías de datos trata el Colegio?
El Colegio tratará los datos que nos suministre, que pueden ser, entre otras, de las siguientes categorías:
-Datos de carácter identificativo y de contacto.
-Datos académicos y profesionales.
-Datos bancarios y económicos.

¿Cuáles son sus derechos?
Cualquier persona tiene derecho a obtener confirmación sobre si el Colegio de Ingenieros de Caminos, Canales y Puertos trata datos personales que le conciernen, o no.

Las personas interesadas tienen derecho a acceder a sus datos personales y a obtener una copia de los datos personales objeto del tratamiento, a actualizarlos, así como a solicitar la rectificación de los datos inexactos o, en su caso, solicitar su supresión cuando, entre otros motivos, los datos ya no sean necesarios para los fines para los que fueron recogidos.

En determinadas circunstancias previstas en el artículo 18 RGPD, los interesados podrán solicitar la limitación del tratamiento de sus datos, en cuyo caso únicamente los conservaremos para el ejercicio o la defensa de reclamaciones.

Como consecuencia de la aplicación del derecho a la supresión u oposición al tratamiento de datos personales en el entorno on-line los interesados tienen, en su caso, el derecho al olvido según la jurisprudencia que el Tribunal de Justicia de la UE.

Los interesados podrán oponerse al tratamiento de sus datos con fines de mercadotecnia, incluida la elaboración de perfiles. En particular, los colegiados tienen derecho a que el Colegio indique gratuitamente respecto de los sus datos personales que se publican en la ventanilla única que no pueden utilizarse para fines de publicidad o prospección comercial.

El colegiado sólo se puede oponer a la publicación de sus datos, los que proceda según la Ley de Colegios Profesiona-

les, en la ventanilla única por motivos fundados y legítimos, por ejemplo por amenaza terrorista o de violencia de género.

Si se editara el registro de colegiados en otro tipo de fuente accesible al público diferente a la ventanilla única (p.ej. en papel), el colegiado se puede oponer a la publicación si coincide con el domicilio personal.

En virtud del derecho a la portabilidad, los interesados tienen derecho a obtener los datos personales que les incumben en un formato estructurado de uso común y lectura mecánica y a transmitirlos a otro responsable

El interesado tiene el derecho a la supresión de sus datos, por la desaparición de la finalidad que motivó el tratamiento o la recogida, por revocación del consentimiento cuando sea éste el que legitime el tratamiento, o por el resto de motivos contenidos en el artículo 17 RGPD.

¿Cómo se pueden ejercer los derechos?
- Mediante un escrito dirigido a Colegio de Ingenieros de Caminos, Canales y Puertos. Calle Almagro, 42, 28010 Madrid.
- Mediante correo electrónico dirigido a: secretariogeneral@ciccp.es

¿Qué vías de reclamación existen?
Si considera que sus derechos no se han atendido debidamente, tiene derecho a presentar una reclamación ante la Agencia Española de Protección de Datos, cuyos datos de contacto son:
Teléfonos: 901 100 099 91.266.35.17
Dirección Postal: C/ Jorge Juan, 6, 28001 Madrid
Sede Electrónica:
https://sedeagpd.gob.es/sede-electronica-web/
Página web: http://www.agpd.es

Gestión del convenio con la AEAT
Actividades corporativas y relaciones institucionales
Atención a los derechos de las personas

¿Quién es el responsable del tratamiento de sus datos?
Identidad: Colegio de Ingenieros de Caminos, Canales y Puertos
CIF: Q-2867009-I
Dirección Postal: c/Almagro 42, 28010 Madrid
Teléfono: 91.308.19.88
Correo electrónico: atencioncolegial@ciccp.es
Web: http://www.ciccp.es
Contacto Delegado de Protección de Datos: dpo@ciccp.es
Ventanilla única: http://www3.ciccp.es/ventanilla-unica

¿Con qué finalidad tratamos sus datos personales?
El Colegio de Ingenieros de Caminos, Canales y Puertos tratará sus datos con el fin de dar respuesta a las solicitudes de los interesados en el ejercicio de los derechos que establece el Reglamento General de Protección de Datos.

¿Cuánto tiempo conservaremos sus datos?
Los datos personales proporcionados se conservarán mientras sean necesarios y pertinentes -incluyendo la necesidad de conservarlos durante los plazos de prescripción aplicables- para la finalidad para la cual hubieran sido proporcionados, recabados o registrados.

La supresión, eliminación o destrucción de los datos tratados en el ejercicio de funciones públicas se realizará de conformidad con lo establecido en la Ley 16/1985, de 25 de junio, del Patrimonio Histórico Español y sólo pueden ser destruidos previa regulación de un procedimiento que salvaguarde el valor probatorio de derechos y obligaciones y los valores artísticos e históricos que puedan tener los documentos, por acuerdo del órgano competente.

Legitimación
El tratamiento de sus datos tiene el siguiente amparo en el Reglamento General de Protección de Datos:

RGPD: 6.1.c) Tratamiento necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento

¿A qué destinatarios se comunicarán sus datos?
Su solicitud, los documentos que acompañe y los datos personales contenidos en ellos se podrán comunicar a la Agencia Española de Protección de Datos o al Defensor del Pueblo si así fuera requerido

¿Cuál es la procedencia de los datos?
Los datos personales que tratará el Colegio son los que usted proporcione, incorporados a su solicitud.

¿Qué categorías de datos trata el Colegio?
El Colegio tratará los datos que nos suministre y los que se incorporen al expediente de mediación, que pueden ser, entre otras, de las siguientes categorías:
- Datos de carácter identificativo

¿Cuáles son sus derechos?
Cualquier persona tiene derecho a obtener confirmación sobre si el Colegio de Ingenieros de Caminos, Canales y Puertos trata datos personales que le conciernen, o no.

Las personas interesadas tienen derecho a acceder a sus datos personales y a obtener una copia de los datos personales objeto del tratamiento, a actualizarlos, así como a solicitar la rectificación de los datos inexactos o, en su caso, solicitar su supresión cuando, entre otros motivos, los datos ya no sean necesarios para los fines para los que fueron recogidos.

En determinadas circunstancias previstas en el artículo 18 RGPD, los interesados podrán solicitar la limitación del tratamiento de sus datos, en cuyo caso únicamente los conservaremos para el ejercicio o la defensa de reclamaciones.

Como consecuencia de la aplicación del derecho a la supresión u oposición al tratamiento de datos personales en el entorno on-line los interesados tienen, en su caso, el derecho al olvido según la jurisprudencia que el Tribunal de Justicia de la UE.

Los interesados podrán oponerse al tratamiento de sus datos con fines de mercadotecnia, incluida la elaboración de perfiles. En particular, los colegiados tienen derecho a que el Colegio indique gratuitamente respecto de los sus datos personales que se publican en la ventanilla única que no pueden utilizarse para fines de publicidad o prospección comercial.

El colegiado sólo se puede oponer a la publicación de sus datos, los que proceda según la Ley de Colegios Profesionales, en la ventanilla única por motivos fundados y legítimos, por ejemplo por amenaza terrorista o de violencia de género.

Si se editara el registro de colegiados en otro tipo de fuente accesible al público diferente a la ventanilla única (p.ej. en papel), el colegiado se puede oponer a la publicación si coincide con el domicilio personal.

En virtud del derecho a la portabilidad, los interesados tienen derecho a obtener los datos personales que les incumben en un formato estructurado de uso común y lectura mecánica y a transmitirlos a otro responsable.

El interesado tiene el derecho a la supresión de sus datos, por la desaparición de la finalidad que motivó el tratamiento o la recogida, por revocación del consentimiento cuando sea éste el que legitime el tratamiento, o por el resto de motivos contenidos en el artículo 17 RGPD.

¿Cómo se pueden ejercer los derechos?
- Mediante un escrito dirigido a Colegio de Ingenieros de Caminos, Canales y Puertos. Calle Almagro, 42, 28010 Madrid.
- Mediante correo electrónico dirigido a: secretariogeneral@ciccp.es

¿Qué vías de reclamación existen?
Si considera que sus derechos no se han atendido debidamente, tiene derecho a presentar una reclamación ante la Agencia Española de Protección de Datos, cuyos datos de contacto son:

Teléfonos: 901 100 099 91.266.35.17
Dirección Postal: C/ Jorge Juan, 6, 28001 Madrid
Sede Electrónica:
https://sedeagpd.gob.es/sede-electronica-web/
Página web: http://www.agpd.es

Transparencia y acceso a la información
Gestión de registro de entrada y salida
Videovigilancia

¿Quién es el responsable del tratamiento de sus datos?
Identidad: Colegio de Ingenieros de Caminos, Canales y Puertos
CIF: Q-2867009-I
Dirección Postal: c/Almagro 42, 28010 Madrid
Teléfono: 91.308.19.88
Correo electrónico: atencioncolegial@ciccp.es
Web: http://www.ciccp.es
Contacto Delegado de Protección de Datos: dpo@ciccp.es
Ventanilla única: http://www3.ciccp.es/ventanilla-unica

¿Con qué finalidad tratamos sus datos personales?
El Colegio de Ingenieros de Caminos, Canales y Puertos, tratará sus datos con el fin de ejercer si legítimo derecho a la vigilancia de sus instalaciones.

¿Cuánto tiempo conservaremos sus datos?
Las imágenes se mantendrán durante un plazo máximo de 30 días desde su captación, salvo que sirvan de prueba para la denuncia de delitos o infracciones, las cuales serán conservadas por el tiempo necesario para ser entregadas a las Fuerzas y Cuerpos de Seguridad del Estado o Jueces y Tribunales, las cuales podrán ser solicitadas únicamente mediante requerimiento al responsable del tratamiento y solamente en el marco de actuaciones judiciales o policiales.

Legitimación
El tratamiento de sus datos tiene el siguiente amparo en el Reglamento General de Protección de Datos:

· RGPD: 6.1.f) Interés legítimo.

Instrucción 1/2006, de 8 de noviembre, de la Agencia Española de Protección de Datos, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras.
Legislación vigente en Materia de Seguridad Privada

¿A qué destinatarios se comunicarán sus datos?
Las imágenes recogidas por las cámaras de videovigilancia podrán comunicarse a las Fuerzas y Cuerpos de Seguridad del Estado o Jueces y Tribunales cuando sirvan de prueba para la denuncia de delitos o infracciones

¿Cuál es la procedencia de los datos?
Los datos personales que tratará el Colegio son los recogidos por las cámaras de videovigilancia instaladas en las zonas de paso de la primera y tercera planta de su edificio de c/ Almagro, 42
¿Qué categorías de datos trata el Colegio?
El Colegio tratará datos personales de las siguientes categorías:
- Imágenes

¿Cuáles son sus derechos?
Cualquier persona tiene derecho a obtener confirmación sobre si el Colegio de Ingenieros de Caminos, Canales y Puertos trata datos personales que le conciernen, o no.
Las personas interesadas tienen derecho a acceder a sus datos personales y a obtener una copia de los datos personales objeto del tratamiento, a actualizarlos, así como a solicitar la rectificación de los datos inexactos o, en su caso, solicitar su supresión cuando, entre otros motivos, los datos ya no sean necesarios para los fines para los que fueron recogidos.
En determinadas circunstancias previstas en el artículo 18 RGPD, los interesados podrán solicitar la limitación del tratamiento de sus datos, en cuyo caso únicamente los conservaremos para el ejercicio o la defensa de reclamaciones.
Como consecuencia de la aplicación del derecho a la supresión u oposición al tratamiento de datos personales en el entorno on-line los interesados tienen, en su caso, el derecho al olvido según la jurisprudencia que el Tribunal de Justicia de la UE.
Los interesados podrán oponerse al tratamiento de sus datos con fines de mercadotecnia, incluida la elaboración de perfiles.
En particular, los colegiados tienen derecho a que el Colegio indique gratuitamente respecto de los sus datos personales que se publican en la ventanilla única que no pueden utilizarse para fines de publicidad o prospección comercial.
El colegiado sólo se puede oponer a la publicación de sus datos, los que proceda según la Ley de Colegios Profesionales, en la ventanilla única por motivos fundados y legítimos, por ejemplo por amenaza terrorista o de violencia de género.
Si se editara el registro de colegiados en otro tipo de fuente accesible al público diferente a la ventanilla única (p.ej. en papel), el colegiado se puede oponer a la publicación si coincide con el domicilio personal.
En virtud del derecho a la portabilidad, los interesados tienen derecho a obtener los datos personales que les incumben en un formato estructurado de uso común y lectura mecánica y a transmitirlos a otro responsable
El interesado tiene el derecho a la supresión de sus datos, por la desaparición de la finalidad que motivó el tratamiento o la recogida, por revocación del consentimiento cuando sea éste el que legitime el tratamiento, o por el resto de motivos contenidos en el artículo 17 RGPD.

¿Cómo se pueden ejercer los derechos?
- Mediante un escrito dirigido a Colegio de Ingenieros de Caminos, Canales y Puertos. Calle Almagro, 42, 28010 Madrid.
- Mediante correo electrónico dirigido a: secretariogeneral@ciccp.es

¿Qué vías de reclamación existen?
Si considera que sus derechos no se han atendido debidamente, tiene derecho a presentar una reclamación ante la Agencia Española de Protección de Datos, cuyos datos de contacto son:

Teléfonos: 901 100 099 91.266.35.17
Dirección Postal: C/ Jorge Juan, 6, 28001 Madrid
Sede Electrónica:
https://sedeagpd.gob.es/sede-electronica-web/
Página web: http://www.agpd.es

GESTIÓN DE PREMIOS Y DISTINCIONES

¿Quién es el responsable del tratamiento de sus datos
Identidad: Colegio de Ingenieros de Caminos, Canales y Puertos
CIF: Q-2867009-I
Dirección Postal: c/Almagro 42, 28010 Madrid
Teléfono: 91.308.19.88
Correo electrónico: atencioncolegial@ciccp.es
Web: http://www.ciccp.es
Contacto Delegado de Protección de Datos: dpo@ciccp.es
Ventanilla única: http://www3.ciccp.es/ventanilla-unica

¿Con qué finalidad tratamos sus datos personales?
El Colegio de Ingenieros de Caminos, Canales y Puertos tratará sus datos con el fin de gestionar los premios y distinciones promovidos por el CICCP.

¿Cuánto tiempo conservaremos sus datos?
Los datos personales proporcionados se conservarán mientras se mantenga su condición de colegiado, no se solicite su supresión por el interesado o cuando los datos dejen de ser necesarios -incluyendo la necesidad de conservarlos durante los plazos de prescripción aplicables- o pertinentes para la finalidad para la cual hubieran sido recabados o registrados.

La supresión, eliminación o destrucción de los datos tratados en el ejercicio de funciones públicas se realizará de conformidad con lo establecido en la Ley 16/1985, de 25 de junio, del Patrimonio Histórico Español y sólo pueden ser destruidos previa regulación de un procedimiento que salvaguarde el valor probatorio de derechos y obligaciones y los valores artísticos e históricos que puedan tener los documentos, por acuerdo del órgano competente.

Legitimación
La base legal del tratamiento es la siguiente:

RGPD: 6.1.a) Consentimiento del interesado.

RGPD: 6.1.f) el tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento.

El tratamiento para las finalidades principales no está supeditado al consentimiento para el tratamiento de los datos que no sean necesarios para dichas finalidades.

¿A qué destinatarios se comunicarán sus datos?
El Colegio de Ingenieros de Caminos, Canales y Puertos podrá publicar datos académicos y profesionales de los premiados y finalistas tanto en la página web del Colegio o en otros medios con la finalidad de dar publicidad al premio.

En el caso de eventos sobre premios que se retransmitan en streaming, la imágenes y el sonido podrán retransmitirse y/o publicarse en redes sociales.

En el caso de eventos sobre premios en los que se realicen fotografías, las imágenes podrán publicarse en medios escritos o digitales.

¿Cuál es la procedencia de los datos?
Los datos personales que tratará el Colegio son los que usted proporcione, en el formulario de inscripción o en otros momentos posteriores así como el de terceras personas que presenten a candidatos para los distintos premios.

¿Qué categorías de datos trata el Colegio?
El Colegio tratará los datos que nos suministre, que pueden ser de las siguientes categorías:
- Datos de carácter identificativo
- Otros datos identificativos (firma, imagen, voz)
- Características personales
- Datos académicos y profesionales

No se tratarán categorías especiales de datos.

¿Cuáles son sus derechos?
Cualquier persona tiene derecho a obtener confirmación sobre si el Colegio de Ingenieros de Caminos, Canales y Puertos trata datos personales que le conciernen, o no.

Las personas interesadas tienen derecho a acceder a sus datos personales y a obtener una copia de los datos personales objeto del tratamiento, a actualizarlos, así como a solicitar la rectificación de los datos inexactos o, en su caso, solicitar su supresión cuando, entre otros motivos, los datos ya no sean necesarios para los fines para los que fueron recogidos.

En determinadas circunstancias previstas en el artículo 18 RGPD, los interesados podrán solicitar la limitación del tratamiento de sus datos, en cuyo caso únicamente los conservaremos para el ejercicio o la defensa de reclamaciones.

Como consecuencia de la aplicación del derecho a la supresión u oposición al tratamiento de datos personales en el entorno on-line los interesados tienen, en su caso, el derecho al olvido según la jurisprudencia que el Tribunal de Justicia de la UE.

Los interesados podrán oponerse al tratamiento de sus datos con fines de mercadotecnia, incluida la elaboración de perfiles. En particular, los colegiados tienen derecho a que el Colegio indique gratuitamente respecto de los sus datos personales que se publican en la ventanilla única que no pueden utilizarse para fines de publicidad o prospección comercial.

El colegiado sólo se puede oponer a la publicación de sus datos, los que proceda según la Ley de Colegios Profesionales, en la ventanilla única por motivos fundados y legítimos, por ejemplo por amenaza terrorista o de violencia de género.

Si se editara el registro de colegiados en otro tipo de fuente accesible al público diferente a la ventanilla única (p.ej. en papel), el colegiado se puede oponer a la publicación si coincide con el domicilio personal.

En virtud del derecho a la portabilidad, los interesados tienen derecho a obtener los datos personales que les incumben en un formato estructurado de uso común y lectura mecánica y a transmitirlos a otro responsable

El interesado tiene el derecho a la supresión de sus datos, por la desaparición de la finalidad que motivó el tratamiento o la recogida, por revocación del consentimiento cuando sea éste el que legitime el tratamiento, o por el resto de motivos contenidos en el artículo 17 RGPD.

¿Cómo se pueden ejercer los derechos?
- Mediante un escrito dirigido a Colegio de Ingenieros de Caminos, Canales y Puertos. Calle Almagro, 42, 28010 Madrid.
- Mediante correo electrónico dirigido a: secretariogeneral@ciccp.es

¿Qué vías de reclamación existen?
Si considera que sus derechos no se han atendido debidamente, tiene derecho a presentar una reclamación ante la Agencia Española de Protección de Datos, cuyos datos de contacto son:

Teléfonos: 901 100 099 91.266.35.17
Dirección Postal: C/ Jorge Juan, 6, 28001 Madrid
Sede Electrónica:
https://sedeagpd.gob.es/sede-electronica-web/
Página web: http://www.agpd.es

Gestión de encuestas
Gestión contractual y convencional del Colegio

¿Quién es el responsable del tratamiento de sus datos?
Identidad: Colegio de Ingenieros de Caminos, Canales y Puertos
CIF: Q-2867009-I
Dirección Postal: c/Almagro 42, 28010 Madrid
Teléfono: 91.308.19.88
Correo electrónico: atencioncolegial@ciccp.es
Web: http://www.ciccp.es
Contacto Delegado de Protección de Datos: dpo@ciccp.es
Ventanilla única: http://www3.ciccp.es/ventanilla-unica

¿Con qué finalidad tratamos sus datos personales?
El Colegio de Ingenieros de Caminos, Canales y Puertos tratará sus datos con el fin de gestionar las relaciones negociales con el Colegio, bien sea actividad contractual, convencional (suscripción de convenios) o con proveedores de servicios o productos

¿Cuánto tiempo conservaremos sus datos?
Los datos personales proporcionados se conservarán mientras se mantenga su condición de colegiado, no se solicite su supresión por el interesado o cuando los datos dejen de ser necesarios -incluyendo la necesidad de conservarlos durante los plazos de prescripción aplicables- o pertinentes para la finalidad para la cual hubieran sido recabados o registrados.

La supresión, eliminación o destrucción de los datos tratados en el ejercicio de funciones públicas se realizará de conformidad con lo establecido en la Ley 16/1985, de 25 de junio, del Patrimonio Histórico Español y sólo pueden ser destruidos previa regulación de un procedimiento que salvaguarde el valor probatorio de derechos y obligaciones y los valores artísticos e históricos que puedan tener los documentos, por acuerdo del órgano competente.

Legitimación
La base legal del tratamiento es la siguiente:

RGPD: 6.1.a) Consentimiento del interesado.

El tratamiento para las finalidades principales no está supeditado al consentimiento para el tratamiento de los datos que no sean necesarios para dichas finalidades.

¿A qué destinatarios se comunicarán sus datos?
A la Agencia Tributaria se le podrán comunicar los datos de transacciones económicas en cumplimiento de una obligación legal.

A las entidades bancarias, se le podrán comunicar los datos de las transacciones económicas necesarias para el pago de productos o servicios

¿Cuál es la procedencia de los datos?
Los datos personales que tratará el Colegio son los que usted proporcione.

¿Qué categorías de datos trata el Colegio?
El Colegio tratará los datos que nos suministre, que pueden ser de las siguientes categorías:
- Datos de carácter identificativo
- Datos de transacciones
- Datos académicos y profesionales
- Datos bancarios y económico-financieros y seguros

No se tratarán categorías especiales de datos.

¿Cuáles son sus derechos?
Cualquier persona tiene derecho a obtener confirmación sobre

si el Colegio de Ingenieros de Caminos, Canales y Puertos trata datos personales que le conciernen, o no.

Las personas interesadas tienen derecho a acceder a sus datos personales y a obtener una copia de los datos personales objeto del tratamiento, a actualizarlos, así como a solicitar la rectificación de los datos inexactos o, en su caso, solicitar su supresión cuando, entre otros motivos, los datos ya no sean necesarios para los fines para los que fueron recogidos.

En determinadas circunstancias previstas en el artículo 18 RGPD, los interesados podrán solicitar la limitación del tratamiento de sus datos, en cuyo caso únicamente los conservaremos para el ejercicio o la defensa de reclamaciones.

Como consecuencia de la aplicación del derecho a la supresión u oposición al tratamiento de datos personales en el entorno on-line los interesados tienen, en su caso, el derecho al olvido según la jurisprudencia que el Tribunal de Justicia de la UE.

Los interesados podrán oponerse al tratamiento de sus datos con fines de mercadotecnia, incluida la elaboración de perfiles. En particular, los colegiados tienen derecho a que el Colegio indique gratuitamente respecto de los sus datos personales que se publican en la ventanilla única que no pueden utilizarse para fines de publicidad o prospección comercial.

El colegiado sólo se puede oponer a la publicación de sus datos, los que proceda según la Ley de Colegios Profesionales, en la ventanilla única por motivos fundados y legítimos, por ejemplo por amenaza terrorista o de violencia de género.

Si se editara el registro de colegiados en otro tipo de fuente accesible al público diferente a la ventanilla única (p.ej. en papel), el colegiado se puede oponer a la publicación si coincide con el domicilio personal.

En virtud del derecho a la portabilidad, los interesados tienen derecho a obtener los datos personales que les incumben en un formato estructurado de uso común y lectura mecánica y a transmitirlos a otro responsable

El interesado tiene el derecho a la supresión de sus datos, por la desaparición de la finalidad que motivó el tratamiento o la recogida, por revocación del consentimiento cuando sea éste el que legitime el tratamiento, o por el resto de motivos contenidos en el artículo 17 RGPD.

¿Cómo se pueden ejercer los derechos?
- Mediante un escrito dirigido a Colegio de Ingenieros de Caminos, Canales y Puertos. Calle Almagro, 42, 28010 Madrid.
- Mediante correo electrónico dirigido a: secretariogeneral@ciccp.es

¿Qué vías de reclamación existen?
Si considera que sus derechos no se han atendido debidamente, tiene derecho a presentar una reclamación ante la Agencia Española de Protección de Datos, cuyos datos de contacto son:

Teléfonos: 901 100 099 91.266.35.17
Dirección Postal: C/ Jorge Juan, 6, 28001 Madrid
Sede Electrónica:
https://sedeagpd.gob.es/sede-electronica-web/
Página web: http://www.agpd.es

Gestión de emprendedores

¿Quién es el responsable del tratamiento de sus datos?
Identidad: Colegio de Ingenieros de Caminos, Canales y Puertos
CIF: Q-2867009-I
Dirección Postal: c/Almagro 42, 28010 Madrid
Teléfono: 91.308.19.88
Correo electrónico: atencioncolegial@ciccp.es
Web: http://www.ciccp.es
Contacto Delegado de Protección de Datos: dpo@ciccp.es
Ventanilla única: http://www3.ciccp.es/ventanilla-unica

¿Con qué finalidad tratamos sus datos personales?
El Colegio de Ingenieros de Caminos, Canales y Puertos tratará los datos de carácter personal que nos facilite con el fin de gestionar su participación en el programa de asesoría y apoyo a emprendedores del Colegio de Ingenieros de Caminos, Canales y Puertos.

La información y documentación que proporcione será tratada de forma confidencial, pudiendo tener acceso a ella los empleados del Colegio de Ingenieros de Caminos, Canales y Puertos y los colaboradores voluntarios del Área de Emprendedores.

¿Cuánto tiempo conservaremos sus datos?
Los datos personales proporcionados se conservarán mientras sean necesarios y pertinentes -incluyendo la necesidad de conservarlos durante los plazos de prescripción aplicables- para la finalidad para la cual hubieran sido proporcionados, recabados o registrados.

Legitimación
La legitimación del tratamiento de sus datos personales, incluyendo las posibles comunicaciones a terceros, es el consentimiento expreso que presta personalmente, así como el consentimiento de terceras personas que usted manifiesta tener para el tratamiento de los datos.

¿A qué destinatarios se comunicarán sus datos?
Los datos personales facilitados, de acuerdo con el consentimiento prestado, podrán comunicarse a terceras personas o instituciones a las que se les presente el proyecto en el ámbito de la gestión del asesoramiento y apoyo al emprendedor. Estas comunicaciones serán previamente autorizadas por el interesado.

En el caso de que la información facilitada no deba llegar alguna persona o institución en concreto debe comunicarlo al Colegio.

¿Cuál es la procedencia de los datos?
Los datos personales que tratará el Colegio son los que usted proporcione, incorporados al formulario de participación en el programa o contenidos en los documentos o escritos que nos facilite.

También se trataran los datos que respecto de su persona puedan aportar otras personas en el desarrollo del programa. También se tratarán los datos de otras personas que usted nos facilite, para lo que debe contar con el consentimiento expreso.

¿Qué categorías de datos trata el Colegio?
El Colegio tratará la documentación y los datos que nos suministre y los que se incorporen al expediente, que pueden ser, entre otras, de las siguientes categorías: datos de carácter identificativo, características personales, circunstancias sociales datos académicos y profesionales; datos de detalle del empleo, datos económico-financieros y seguros, etc..

¿Cuáles son sus derechos?
Cualquier persona tiene derecho a obtener confirmación sobre si el Colegio de Ingenieros de Caminos, Canales y Puertos trata datos personales que le conciernen, o no.

Las personas interesadas tienen derecho a acceder a sus datos personales y a obtener una copia de los datos personales objeto del tratamiento, a actualizarlos, así como a solicitar la rectificación de los datos inexactos o, en su caso, solicitar su supresión cuando, entre otros motivos, los datos ya no sean necesarios para los fines para los que fueron recogidos.

En determinadas circunstancias previstas en el artículo 18 RGPD, los interesados podrán solicitar la limitación del tratamiento de sus datos, en cuyo caso únicamente los conservaremos para el ejercicio o la defensa de reclamaciones.

Como consecuencia de la aplicación del derecho a la supresión u oposición al tratamiento de datos personales en el entorno on-line los interesados tienen, en su caso, el derecho al olvido según la jurisprudencia que el Tribunal de Justicia de la UE.

Los interesados podrán oponerse al tratamiento de sus datos con fines de mercadotecnia, incluida la elaboración de perfiles. En particular, los colegiados tienen derecho a que el Colegio indique gratuitamente respecto de los sus datos personales que se publican en la ventanilla única que no pueden utilizarse para fines de publicidad o prospección comercial.

El colegiado sólo se puede oponer a la publicación de sus datos, los que proceda según la Ley de Colegios Profesionales, en la ventanilla única por motivos fundados y legítimos, por ejemplo, por amenaza terrorista o de violencia de género. Si se editara el registro de colegiados en otro tipo de fuente accesible al público diferente a la ventanilla única (p.ej. en papel), el colegiado se puede oponer a la publicación si coincide con el domicilio personal.

En virtud del derecho a la portabilidad, los interesados tienen derecho a obtener los datos personales que les incumben en un formato estructurado de uso común y lectura mecánica y a transmitirlos a otro responsable

El interesado tiene el derecho a la supresión de sus datos, por la desaparición de la finalidad que motivó el tratamiento o la recogida, por revocación del consentimiento cuando sea éste el que legitime el tratamiento, o por el resto de motivos contenidos en el artículo 17 RGPD.

¿Cómo se pueden ejercer los derechos?
- Mediante un escrito dirigido a Colegio de Ingenieros de Caminos, Canales y Puertos. Calle Almagro, 42, 28010 Madrid.
- Mediante correo electrónico dirigido a: secretariogeneral@ciccp.es

¿Qué vías de reclamación existen?
Si considera que sus derechos no se han atendido debidamente, tiene derecho a presentar una reclamación ante la Agencia Española de Protección de Datos, cuyos datos de contacto son:

Teléfonos: 901 100 099 91.266.35.17
Dirección Postal: C/ Jorge Juan, 6, 28001 Madrid
Sede Electrónica:
https://sedeagpd.gob.es/sede-electronica-web/
Página web: http://www.agpd.es

Fondo de solidaridad

¿Quiénes son los corresponsables del tratamiento de sus datos?
Identidad: Colegio de Ingenieros de Caminos, Canales y Puertos
CIF: Q-2867009-I
Dirección Postal: c/Almagro 42, 28010 Madrid
Teléfono: 91.308.19.88
Correo electrónico: atencioncolegial@ciccp.es
Web: http://www.ciccp.es
Contacto Delegado de Protección de Datos: dpo@ciccp.es
Ventanilla única: http://www3.ciccp.es/ventanilla-unica

Identidad: Fundación Ingenieros de Caminos, Canales y Puertos
CIF: G-80680630
Dirección Postal: c/Almagro 42, 28010 Madrid
Teléfono: 91.308.19.88
Correo electrónico: secretariogeneral@ciccp.es
Web: http://www.fundacioncaminos.es

¿Con qué finalidad tratamos sus datos personales?
El Colegio de Ingenieros de Caminos, Canales y Puertos y la Fundación Caminos tratarán sus datos de carácter personal para la gestión del Fondo de Solidaridad y la tramitación de ayudas, de las aportaciones a dicho Fondo, la emisión de certificados y si se autoriza para la publicación y difusión de la identidad de los aportantes.

¿Cuánto tiempo conservaremos sus datos?
Los datos personales proporcionados se conservarán mientras se mantenga su condición de colegiado, no se solicite su supresión por el interesado o cuando los datos dejen de ser necesarios -incluyendo la necesidad de conservarlos durante los plazos de prescripción aplicables- o pertinentes para la finalidad para la cual hubieran sido recabados o registrados.

La supresión, eliminación o destrucción de los datos tratados en el ejercicio de funciones públicas se realizará de conformidad con lo establecido en la Ley 16/1985, de 25 de junio, del Patrimonio Histórico Español y sólo pueden ser destruidos previa regulación de un procedimiento que salvaguarde el valor probatorio de derechos y obligaciones y los valores artísticos e históricos que puedan tener los documentos, por acuerdo del órgano competente.

Legitimación
La base legal del tratamiento es la siguiente:

RGPD: 6.1.a) Consentimiento del interesado.

El tratamiento para las finalidades principales no está supeditado al consentimiento para el tratamiento de los datos que no sean necesarios para dichas finalidades.

¿A qué destinatarios se comunicarán sus datos?
A la Agencia Tributaria se le podrán comunicar los datos de transacciones económicas en cumplimiento de una obligación legal.

Si se autoriza por el interesado, se podrá publicar y difundir la identidad de los aportantes

Respecto de los solicitantes de ayudas no se prevén

¿Cuál es la procedencia de los datos?
Los datos personales que tratarán el Colegio y la Fundación son los que usted proporcione

¿Qué categorías de datos tratan el Colegio y la Fundación?
El Colegio tratará los datos que nos suministre, que pueden ser de las siguientes categorías:
- Datos de carácter identificativo
- Datos profesionales y de contacto
- Datos económicos, bancarios y de transacciones
No se tratarán categorías especiales de datos.

¿Cuáles son sus derechos?
Cualquier persona tiene derecho a obtener confirmación sobre si el Colegio de Ingenieros de Caminos, Canales y Puertos trata datos personales que le conciernen, o no.

Las personas interesadas tienen derecho a acceder a sus datos personales y a obtener una copia de los datos personales objeto del tratamiento, a actualizarlos, así como a solicitar la rectificación de los datos inexactos o, en su caso, solicitar su supresión cuando, entre otros motivos, los datos ya no sean necesarios para los fines para los que fueron recogidos.

En determinadas circunstancias previstas en el artículo 18 RGPD, los interesados podrán solicitar la limitación del trata-

miento de sus datos, en cuyo caso únicamente los conservaremos para el ejercicio o la defensa de reclamaciones.

Como consecuencia de la aplicación del derecho a la supresión u oposición al tratamiento de datos personales en el entorno on-line los interesados tienen, en su caso, el derecho al olvido según la jurisprudencia que el Tribunal de Justicia de la UE.

Los interesados podrán oponerse al tratamiento de sus datos con fines de mercadotecnia, incluida la elaboración de perfiles. En particular, los colegiados tienen derecho a que el Colegio indique gratuitamente respecto de los sus datos personales que se publican en la ventanilla única que no pueden utilizarse para fines de publicidad o prospección comercial.

El colegiado sólo se puede oponer a la publicación de sus datos, los que proceda según la Ley de Colegios Profesionales, en la ventanilla única por motivos fundados y legítimos, por ejemplo por amenaza terrorista o de violencia de género.

Si se editara el registro de colegiados en otro tipo de fuente accesible al público diferente a la ventanilla única (p.ej. en papel), el colegiado se puede oponer a la publicación si coincide con el domicilio personal.

En virtud del derecho a la portabilidad, los interesados tienen derecho a obtener los datos personales que les incumben en un formato estructurado de uso común y lectura mecánica y a transmitirlos a otro responsable

El interesado tiene el derecho a la supresión de sus datos, por la desaparición de la finalidad que motivó el tratamiento o la recogida, por revocación del consentimiento cuando sea éste el que legitime el tratamiento, o por el resto de motivos contenidos en el artículo 17 RGPD.

¿Cómo se pueden ejercer los derechos?
- Mediante un escrito dirigido a:
Colegio de Ingenieros de Caminos, Canales y Puertos. Calle Almagro, 42, 28010 Madrid
Fundación Caminos, Calle Almagro, 42, 1ª planta, 28010 Madrid
- Mediante correo electrónico a: derechosdatos@ciccp.es

¿Qué vías de reclamación existen?
Si considera que sus derechos no se han atendido debidamente, tiene derecho a presentar una reclamación ante la Agencia Española de Protección de Datos, cuyos datos de contacto son:

Teléfonos: 901 100 099 91.266.35.17
Dirección Postal: C/ Jorge Juan, 6, 28001 Madrid
Sede Electrónica:
https://sedeagpd.gob.es/sede-electronica-web/
Página web: http://www.agpd.es

ANEXO E
CONTRATOS CON TERCEROS

Acuerdo de encargo de tratamiento de datos de carácter personal

C O M P A R E C E N
De otra parte, el COLEGIO DE INGENIEROS DE CAMINOS, CANALES Y PUERTOS, con domicilio corporativo a estos efectos en Madrid, calle Almagro, 42 [o dirección de la Demarcación] y con C.I.F.: Q2867009I, representado por D.……..., con DNI nº……en su calidad de……., en virtud de……..

De otra parte, AUTONOMO, con domicilio a estos efectos en…….. Y con D.N.I……..,

D I C E N Y A C U E R D A N
I.) Acuerdo de encargo del tratamiento
Que en la medida en que para la prestación de sus servicios profesionales al Colegio AUTONOMO podrá tener acceso a determinados datos de carácter personal de los que es responsable el Colegio, AUTONOMO y el Colegio, y de conformidad con el REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales, en adelante RGPD, y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDyGDD) pactan las siguientes cláusulas:

1. Objeto del encargo del tratamiento
Mediante las presentes cláusulas se habilita a AUTONOMO para tratar por cuenta del responsable del tratamiento, el Colegio de Ingenieros de Caminos, Canales y Puertos (en adelante se podrá referir a éste como el Colegio o el responsable), los datos de carácter personal necesarios para prestar el servicio que se contrata.

El tratamiento consistirá, exclusivamente y sin posibilidad de destino para otra finalidad, en el manejo de datos correspondientes a las actividades que correspondan a las funciones de Gestión Colegial del Registro de Actividades del Tratamiento

del Colegio disponible en http://www.ciccp.es/rgpd/rat/RAT_Web_v1_0.htm.

a) En particular:
- Actividad de tratamiento: Gestión de Publicaciones y Suscripciones
- Categoría de Datos: Nombre y apellidos, email, dirección postal
- Interesados: Suscriptores.

Los tratamientos concretos que podrá realizar AUTONOMO son la consulta, utilización y comunicación por transmisión, siguiendo las políticas y procedimientos de protección de datos y de seguridad de la información que establezca el Colegio. El encargado no podrá realizar transferencias internacionales de los datos que trate.

2. Identificación de la información afectada
Para la ejecución de las prestaciones derivadas del cumplimiento del objeto de este encargo, el responsable del tratamiento, podrá poner a disposición del encargado del tratamiento, los datos referidos a las actividades del registro de actividades del tratamiento indicadas.

3. Duración
El presente acuerdo de encargo del tratamiento tiene la duración pactada en el contrato.

Una vez finalice el presente contrato, el encargado del tratamiento debe devolver al responsable los datos personales y suprimir cualquier copia que esté en su poder.

4. Obligaciones del encargado del tratamiento
El encargado del tratamiento y todo su personal se obliga a:

a. Utilizar los datos personales objeto de tratamiento sólo para la finalidad objeto de este encargo. En ningún caso podrá utilizar los datos para fines propios.

b. Tratar los datos de acuerdo con las instrucciones del responsable del tratamiento.

Si el encargado del tratamiento considera que alguna de las instrucciones infringe el RGPD o cualquier otra disposición en materia de protección de datos de la Unión o de los Estados miembros, el encargado informará inmediatamente al responsable.

c. Llevar, por escrito, un registro de todas las categorías de actividades de tratamiento efectuadas por cuenta del responsable, que contenga:

1. El nombre y los datos de contacto del encargado o encargados y de cada responsable por cuenta del cual actúe el encargado y, en su caso, del representante del responsable o del encargado y del delegado de protección de datos.

2. Las categorías de tratamientos efectuados por cuenta de cada responsable.

3. Una descripción general de las medidas técnicas y organizativas de seguridad relativas a:

a) La capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento.

b) La capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida, en caso de incidente físico o técnico.

c) El proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

d) En su caso, a la seudonimización y el cifrado de datos personales

d. No comunicar los datos a terceras personas, salvo que cuente con la autorización expresa del responsable del tratamiento, en los supuestos legalmente admisibles.

El encargado puede comunicar los datos a otros encargados del tratamiento del mismo responsable, de acuerdo con las instrucciones del responsable. En este caso, el responsable identificará, de forma previa y por escrito, la entidad a la que se deben comunicar los datos, los datos a comunicar y las medidas de seguridad a aplicar para proceder a la comunicación.

Si el encargado debiera transferir datos personales a un tercer país o a una organización internacional, en virtud del Derecho de la Unión o de los Estados miembros que le sea aplicable, informará al responsable de esa exigencia legal de manera previa, salvo que tal Derecho lo prohíba por razones importantes de interés público.

e. No subcontratar ninguna de las prestaciones que formen parte del objeto de este contrato que comporten el tratamiento de datos personales, salvo los servicios auxiliares necesarios para el normal funcionamiento de los servicios del encargado. El encargado comunicará la identidad de los prestadores de

los servicios auxiliares que puedan tener acceso a los datos de carácter personal objeto de este encargo.

f. Mantener el deber de secreto respecto a los datos de carácter personal a los que haya tenido acceso en virtud del presente encargo, incluso después de que finalice su objeto.

g. Garantizar que las personas autorizadas para tratar datos personales se comprometan, de forma expresa y por escrito, a respetar la confidencialidad y a cumplir las medidas de seguridad correspondientes, de las que hay que informarles convenientemente.

h. Mantener a disposición del responsable la documentación acreditativa del cumplimiento de la obligación establecida en el apartado anterior.

i. Garantizar la formación necesaria en materia de protección de datos personales de las personas autorizadas para tratar datos personales.

j. Asistir al responsable del tratamiento en la respuesta al ejercicio de los derechos de:
1. Acceso, rectificación, supresión y oposición
2. Limitación del tratamiento
3. Portabilidad de datos
4. A no ser objeto de decisiones individualizadas automatizadas (incluida la elaboración de perfiles)

Cuando las personas afectadas ejerzan los derechos de acceso, rectificación, supresión y oposición, limitación del tratamiento, portabilidad de datos y a no ser objeto de decisiones individualizadas automatizadas, ante el encargado del tratamiento, éste debe comunicarlo por correo electrónico a la dirección derechosdatos@ciccp.es. La comunicación debe hacerse de forma inmediata y en ningún caso más allá del día laborable siguiente al de la recepción de la solicitud, juntamente, en su caso, con otras informaciones que puedan ser relevantes para resolver la solicitud.

k. Derecho de información
Corresponde al responsable facilitar el derecho de información en el momento de la recogida de los datos.

l. Notificación de violaciones de la seguridad de los datos
El encargado del tratamiento notificará al responsable del tratamiento, sin dilación indebida, y en cualquier caso antes del plazo máximo de 24 horas, y a través del correo electrónico dpo@ciccp.es, debiéndose asegurarse de su recepción, las violaciones de la seguridad de los datos personales a su cargo de las que tenga conocimiento, juntamente con toda la información relevante para la documentación y comunicación de la incidencia.

No será necesaria la notificación cuando sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas.

Las violaciones de seguridad se entienden que, en todo caso, se producen en los siguientes supuestos:

-Brecha de confidencialidad: Tiene lugar cuando partes que no están autorizadas, o no tienen un propósito legítimo para acceder a la información, acceden a ella.

-Brecha de integridad: se produce cuando se altera la información original y la sustitución de datos puede ser perjudicial para el individuo.

-Brecha de disponibilidad: su consecuencia es que no se puede acceder a los datos originales cuando es necesario.
Si se dispone de ella se facilitará, como mínimo, la información siguiente:

a) Descripción de la naturaleza de la violación de la seguridad de los datos personales, inclusive, cuando sea posible, las categorías y el número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados.

b) El nombre y los datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información.

c) Descripción de las posibles consecuencias de la violación de la seguridad de los datos personales.

d) Descripción de las medidas adoptadas o propuestas para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.

m. Dar apoyo al responsable del tratamiento en la realización de las evaluaciones de impacto relativas a la protección de datos, cuando proceda.

n. Dar apoyo al responsable del tratamiento en la realización de las consultas previas a la autoridad de control, cuando proceda.

o. Poner a disposición del responsable toda la información necesaria para demostrar el cumplimiento de sus obligaciones, así como para la realización de las auditorías o las inspecciones que realicen el responsable u otro auditor autorizado por él.

p. Implantar las medidas de seguridad necesarias para:

a) Garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento.

b) Restaurar la disponibilidad y el acceso a los datos personales de forma rápida, en caso de incidente físico o técnico.

c) Verificar, evaluar y valorar, de forma regular, la eficacia de las medidas técnicas y organizativas implantadas para garantizar la seguridad del tratamiento.

d) Seudonimizar y cifrar los datos personales, en su caso.

q. En su caso, si estuviera obligado por el RGPD, designar un delegado de protección de datos según el RGPD y comunicar su identidad y datos de contacto al responsable.

r. Devolver al responsable del tratamiento los datos de carácter personal y, si procede, los soportes donde consten, una vez cumplida la prestación. La devolución debe comportar el borrado total de los datos existentes en los equipos informáticos utilizados por el encargado. No obstante, el encargado puede conservar una copia, con los datos debidamente bloqueados, mientras puedan derivarse responsabilidades de la ejecución de la prestación.

5. Obligaciones y derechos del responsable del tratamiento
Corresponde al responsable del tratamiento velar, de forma previa y durante todo el tratamiento, por el cumplimiento del RGPD por parte del encargado y supervisar el tratamiento, incluida la realización de inspecciones y auditorías.

II) Información sobre datos personales vinculados al presente contrato.
Respecto de los datos de AUTONOMO incluidos en este contrato, con motivo de su ejecución serán incluidos en tratamientos, titularidad del Colegio, cuya finalidad es la gestión contractual y la derivada del desarrollo de la función para la que se le contrata.

El Registro de Actividades del Tratamiento del Colegio y las finalidades del tratamiento de datos está disponible en http://www.ciccp.es/rgpd/rat/RAT_Web_v1_0.htm.

En particular el Colegio informa del tratamiento de datos en relación a la siguiente actividad:

-Gestión contractual y convencional del Colegio:
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 éste, de medidas precontractuales.
Cesiones o comunicaciones: Ministerio para la Transición Ecológica. Publicación de la contratación en la página web.
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

Fdo.……. POR EL COLEGIO

Fdo.……..… POR EL AUTONOMO

Acuerdo para el tratamiento de datos personales entre responsables del tratamiento

C O M P A R E C E N
De otra parte, el COLEGIO DE INGENIEROS DE CAMINOS, CANALES Y PUERTOS, con domicilio corporativo a estos efectos en Madrid, calle Almagro, 42 [o dirección de la Demarcación] y con C.I.F.: Q2867009I, representado por D.……..., con DNI nº.……en su calidad de……., en virtud de……..

Y
De otra parte, D. /Dña._____ con DNI _____ como representante legal de _____ con NIF _____ y con domicilio sito en _____(de ahora en adelante, “Responsable del Tratamiento”).

INTERVIENEN ambas Partes en el nombre y la representación indicada, reconociéndose mutuamente capacidad legal necesaria para suscribir el presente contrato y obligarse en la condición con que intervienen, y a tal efecto

D I C E N Y A C U E R D A N
Que de conformidad con el contrato de fecha [INDICAR FECHA], los Responsables del tratamiento acordaron la presta-

ción de los siguientes servicios, para lo que es necesario el tratamiento de datos personales.
- Prestación de servicios correspondientes a [ESTABLECER DESCRIPCIÓN DE LOS SERVICIOS].

Que los Responsables del tratamiento tratarán los datos personales acorde con lo establecido en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (en adelante, "RGPD") y en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales y resto de normativa de protección de datos que pudiera resultar de aplicación.

Que los Responsables de tratamiento acuerdan suscribir el presente contrato de acuerdo con las siguientes,

CLÁUSULAS

1. DEFINICIONES
Normativa sobre Protección de Datos: Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los Derechos Digitales.

Datos personales: toda información sobre una persona física identificada o identificable; se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica genética, psíquica, económica, cultural o social de dicha persona.

Autoridad de Protección de Datos: Autoridad de protección de datos en los territorios donde se encuentran ubicadas las Partes.

Violación de la seguridad: Toda violación de la seguridad que ocasione la destrucción pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.

Responsable de Tratamiento: la persona física o jurídica autoridad pública, servicio u otro organismo que, solo o junto con otros determine los fines y medios del tratamiento.

Encargado de Tratamiento: la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del Responsable del tratamiento.

Tratamiento: cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no como la recogida, registro, organización, estructuración, conservación adaptación o modificación, extracción. consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción.

2. OBJETO
El objeto de este contrato es regular el tratamiento de datos personales por las Partes como Responsables del tratamiento en virtud del contrato de prestación de servicios formalizado entre ambas.

Los tratamientos de datos personales incluirán los siguientes tratamientos: Recogida Registro Estructuración Modificación Conservación Extracción · Consulta Comunicación Difusión Interconexión Cotejo Limitación Supresión · Destrucción Conservación Comunicación por transmisión.

Las Partes acuerdan tratar exclusivamente los datos personales a los efectos de este contrato para el desarrollo del objeto del mismo.

3. DURACIÓN
El presente contrato tendrá una duración igual a la duración del contrato principal.

4. GARANTÍAS DE OBTENCIÓN LEGÍTIMA DE LOS DATOS OBTENIDOS
Las Partes, en base a sus propias actuaciones, garantizarán que los datos han sido obtenidos legítimamente y que los interesados han sido informados y se ha solicitado su consentimiento para su tratamiento, cuando éste sea necesario, y proceder a la comunicación o comunicaciones subsiguientes derivadas del cumplimiento del presente contrato, disponiendo de elementos probatorios de la atención al derecho de información como del registro del consentimiento si procede.

5. CUMPLIMIENTO DE LA NORMATIVA SOBRE PROTECCIÓN DE DATOS
Cada una de las Partes deberá garantizar que cumple con la normativa sobre Protección de Datos en todo momento durante la vigencia de este contrato.

Asimismo, cada una de las Partes será responsable de garantizar que su personal cumple con las obligaciones establecidas en la normativa de protección de datos aplicable. Las Partes pondrán a mutua disposición toda la información necesaria para demostrar el cumplimiento de sus obligaciones, así como para la realización de las auditorías o las inspecciones que se realicen.

A tales efectos, las Partes se comprometen a que el personal a su servicio que tenga acceso y trate los datos personales objeto del contrato suscrito por las Partes, se comprometan de forma expresa y por escrito a observar el secreto profesional y al deber de guardarlo respecto de los datos personales, independientemente del soporte o forma en la que tengan conocimiento de estos. Estas obligaciones subsistirán aún después de finalizar la relación contractual. Ambas Partes mantendrán a disposición de la otra Parte cuanta documentación acreditativa del cumplimiento de dicha obligación.

Ambas Partes se obligan a no comunicar los datos, ni siquiera a efectos de conservación, a otras personas no autorizadas.

Ambas Partes llevarán, por escrito, un registro de todas las categorías de actividades de tratamiento efectuadas de conformidad con la normativa sobre Protección de Datos.

Las Partes se prestarán apoyo en la realización de las evaluaciones de impacto relativas a la protección de datos, así como en la realización de consultas previas a la autoridad de control, cuando proceda.

Cuando se solicite, cada Parte pondrá a disposición de la otra toda la información necesaria para demostrar el cumplimiento de las obligaciones estipuladas en el presente contrato, así como en la normativa sobre Protección de Datos.

Ambas Partes se comprometen, cuando proceda, en designar un Delegado de Protección de Datos y comunicar su identidad y datos de contacto a la otra Parte.

6. TRANSFERENCIAS INTERNACIONALES DE DATOS
Ninguna de las Partes transferirá datos personales fuera del Espacio Económico Europeo sin el previo consentimiento expreso de la otra Parte.

Cuando la otra Parte consienta una transferencia fuera del Espacio Económico Europeo, esta adoptará las medidas que la otra Parte pueda requerir para garantizar una adecuada protección de los datos personales de conformidad con la normativa de Protección de Datos.

7. MEDIDAS DE SEGURIDAD
Cada una de las Partes se asegurará que cuenta con medidas técnicas y organizativas apropiadas para impedir accesos no autorizados, destrucción o pérdida de los datos personales, garantizando el cumplimiento de las obligaciones establecidas en la normativa de protección de datos de carácter personal en relación con los datos tratados.

Asimismo, y con carácter periódico las Partes realizarán una evaluación de riesgos en materia de seguridad de la información, de la que se derivarán la implantación de mecanismos para:

a) Garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento.

b) Restaurar la disponibilidad y el acceso a los datos personales de forma rápida, en caso de incidente físico o técnico.

c) Verificar, evaluar y valorar, de forma regular, la eficacia de las medidas técnicas y organizativas implantadas para garantizar la seguridad del tratamiento.

d) Seudonimizar y cifrar los datos personales, en su caso.

8. ENCARGADO DE TRATAMIENTO
Si se precisa contratar los servicios de un tercero para llevar a cabo todo o parte de los servicios objeto del contrato formalizado entre las Partes, se deberá garantizar que éste ofrece garantías suficientes para aplicar medidas técnicas y organizativas apropiadas, de manera que el tratamiento sea conforme con los requisitos establecidos en la normativa sobre Protección de Datos y garantice la protección de los derechos de los interesados.

Cuando se contraten los servicios de un tercero se deberá suscribir un contrato de encargado del tratamiento conforme al Derecho de la Unión o de los Estados miembros en el cual se regule el contenido mínimo exigido por la normativa de protección de datos.

9. VIOLACIONES DE SEGURIDAD
Cualquiera de las Partes que haya sufrido una violación de seguridad o sospeche que ésta pueda haber ocurrido, proporcionará sin dilación, y en todo caso antes del plazo máximo de 24 horas desde que se tuvo conocimiento, a la otra Parte una descripción detallada de la violación de seguridad, del número de afectados y del tipo de datos objeto de la violación de seguridad.

Se facilitará, como mínimo, la información siguiente:

a) Descripción de la naturaleza de la violación de la seguridad de los datos personales, inclusive, cuando sea posible, las categorías y el número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados.

b) Descripción de las posibles consecuencias de la violación de la seguridad de los datos personales.

c) Descripción de las medidas adoptadas o propuestas para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.

Si no es posible facilitar la información simultáneamente, y en la medida en que no lo sea, la información se facilitará de manera gradual sin dilación indebida.

Las comunicaciones se realizarán a través de los siguientes medios:

- En el caso del Colegio de Ingenieros de Canales Caminos y Puertos a través del correo electrónico: dpo@ciccp.es.

- En el caso de [ESTABLECER DENOMINACIÓN DE LA OTRA PARTE] a través del correo electrónico: [ESTABLECER DIRECCIÓN DE CORREO ELECTRÓNICO].

La Parte que haya sufrido la violación o sospeche que pueda haber ocurrido, debe iniciar acciones para investigarla con el objetivo de identificar, impedir y mitigar sus efectos.

Cuando proceda, cada Parte es responsable de comunicar a la Agencia Española de Protección de Datos y a los interesados las violaciones de seguridad que se produzcan.

10. INCUMPLIMIENTO Y RESPONSABILIDAD
El incumplimiento por cualquiera de las Partes de las obligaciones referidas en el presente contrato es extensible a su justa responsabilidad, respondiendo ante las Autoridades de Protección de Datos, o ante cualquier tercera persona de las infracciones que se puedan haber cometido derivadas de la ejecución del presente contrato y/o de la legislación vigente en materia de protección de datos de carácter personal.

Las Partes responderán de la totalidad de los daños y perjuicios que se irroguen a la otra parte en todos los supuestos de conducta negligente o culposa en el incumplimiento de las obligaciones que respectivamente les incumben, a tenor de lo pactado en el presente contrato.

11. DERECHOS
En caso de que un interesado ejerza sus derechos, las Partes deben comunicar a la otra parte el ejercicio de estos para realizar las acciones pertinentes atendiendo al tipo de derecho solicitado.

La comunicación o traslado de la solicitud del ejercicio de derechos entre las Partes deberá realizarse de forma inmediata, dentro del plazo de 24 horas a contar desde la recepción de la solicitud, y a través de los siguientes medios:

- En el caso del Colegio de Ingenieros de Canales Caminos y Puertos a través del correo electrónico: dpo@ciccp.es.

- En el caso de [ESTABLECER DENOMINACIÓN DE LA OTRA PARTE] a través del correo electrónico: [ESTABLECER DIRECCIÓN DE CORREO ELECTRÓNICO].

Cada parte resolverá las solicitudes de derechos que le sean recibidas en su posición de Responsable de Tratamiento de los datos.

12. CONFIDENCIALIDAD
Toda la información calificada de confidencial, que sea comunicada entre las Partes con motivo de la prestación de los servicios, solo podrá ser utilizada por estas para dar cumplimiento al contrato formalizado entre ambas. Ninguna de las partes revelará a terceros, ninguna información que reciba de la otra parte en relación con el presente contrato, sin el previo consentimiento por escrito de la otra.

Las anteriores restricciones no se aplicarán cuando la información sea accesible con carácter general para el público por un motivo diferente al incumplimiento de una obligación derivada de la presente cláusula, se obtenga de un tercero que no esté sujeto a la obligación de guardar confidencialidad, que fuese conocida por el tercero con anterioridad o la revelación de la información venga impuesta por la ley o responda al cumplimiento de una orden de naturaleza judicial o administrativa. En este último caso siempre que la parte que hubiera recibido la orden informe previamente por escrito a la otra parte acerca de la obligación de proceder a dicha revelación.

La obligación de confidencialidad permanecerá en vigor para ambas partes con carácter indefinido, incluso una vez finalizado el contrato.

13. DESTINO DE LOS DATOS
Una vez cumplida la prestación contractual, las Partes podrán conservar debidamente bloqueados, los datos mientras existan obligaciones legales de conservación o pudieran derivarse responsabilidades de la prestación del servicio y del tratamiento realizado. Tras la prescripción de dichos plazos, la información objeto del presente contrato, deberá ser destruida mediante un procedimiento que asegure las máximas garantías.

14. TRATAMIENTO DE DATOS PERSONALES DE LOS FIRMANTES
En virtud de lo establecido en la normativa aplicable en materia de protección de datos personales, los datos personales de los firmantes del presente contrato y de las personas de contacto de cada entidad, serán tratados por cada una de las Partes con la finalidad de dar cumplimiento a la relación que se establece entre estas en el presente contrato.

La base jurídica que legitima el tratamiento de los datos personales es la ejecución del contrato suscrito entre las partes y el interés legítimo.

Los datos personales no se cederán a terceros salvo que sea necesario para dar cumplimiento a una obligación legal que resulte de aplicación.

Los datos proporcionados se conservarán mientras se mantenga la relación comercial o durante los años necesarios para cumplir con las obligaciones legales comerciales y tributarias.

Las partes podrán ejercer los derechos de acceso, rectificación, oposición, supresión, portabilidad y limitación del tratamiento, dirigiendo una comunicación, acompañando a la solicitud de que se trate una copia del documento nacional de identidad o documento identificativo equivalente.

Para realizar las comunicaciones al Colegio de Ingenieros de Canales Caminos y puertos deberá dirigirse a la dirección dpo@ciccp.es.

Para realizar las comunicaciones a [ESTABLECER DENOMINACIÓN DE LA OTRA PARTE] deberá dirigirse a la dirección [ESTABLECER DIRECCIÓN DE CORREO ELECTRÓNICO]

Asimismo, le informamos que puede presentar una reclamación ante la Agencia Española de Protección de Datos, a través de su página web (www.aepd.es).

15. LEGISLACION Y FUERO APLICABLE
El presente contrato se regirá e interpretará de acuerdo con las leyes españolas.

Las Partes intervinientes tratarán de resolver mediante acuerdo amistoso cualquier discrepancia o conflicto relativo a la ejecución o interpretación de las disposiciones contenidas en este contrato, en base a los principios de buena fe.

En defecto de lo anterior, las Partes intervinientes aceptan someterse a la jurisdicción de los Juzgados y Tribunales de Madrid con renuncia expresa a cualquier otro fuero o jurisdicción que les pudiese corresponder.

Y en prueba de conformidad con cuanto antecede, firman ambas Partes todas las hojas del presente contrato por duplicado y a un solo efecto, en el lugar y la fecha al principio indicados

Fdo.…… POR EL COLEGIO
Fdo.…… POR EL PROVEEDOR

ANEXO F
PROCEDIMIENTO PARA EL EJERCICIO DE LOS DERECHOS

El CICCP tiene establecido un procedimiento sencillo de ejercicio de los derechos de protección de datos de carácter personal, disponiendo de una dirección de correo electrónico para el ejercicio de derechos derechosdatos@ciccp.es, definido en el documento "Procedimiento para el ejercicio de derechos" que todos/as los/as empleados/as del Colegio deben conocer y aplicar. Cualquier petición de ejercicio de derechos de protección de datos recibida en el Colegio por cualquier vía o canal se remitirá por los/as empleados/as del Colegio a derechosdatos@ciccp.es

Esta norma se incluirá en el decálogo de protección de datos para empleados/as.

En el caso de los Colegiados, podrán presentar sus solicitudes de ejercicio de derechos a través de su área privada en la sede electrónica, por ello, las comunicaciones en este sentido se realizarán a través de esta vía.

Se responderá a las solicitudes de el resto de los/as interesados/as, por correo electrónico con confirmación de lectura si la solicitud se ha recibido por ese medio o por correo postal certificado con acuse de recibo si la solicitud se ha recibido por

medios diferentes al correo electrónico, sin dilación indebida y a más tardar en el plazo de un mes.

La prueba del cumplimiento del deber de responder a la solicitud de ejercicio de derechos formulando por el/la afectado/a recae sobre el Colegio por lo que se conservará copia de todas las respuestas y de la justificación de envío y recepción.

Disposiciones comunes al ejercicio de derechos
Se señalan a continuación algunas cuestiones a tener en cuenta a la hora de atender todos o parte de los derechos del interesado.

Para todos los derechos: Los derechos del interesado pueden ejercerse directamente por el propio interesado o por medio de representante legal o voluntario. En el primer caso, el interesado deberá acreditar su identidad mediante copia de su DNI o pasaporte. En el segundo caso, el responsable deberá comprobar además la identidad del representante y la representación conferida al mismo por el interesado.

Para los derechos de rectificación, supresión y limitación del tratamiento: Cuando a solicitud del interesado, proceda el responsable a rectificar, suprimir o limitar el tratamiento de sus datos, dicho responsable deberá informar de ello a cada uno de los destinatarios a los que hubiera comunicado previamente los datos. Asimismo, el responsable informará al interesado acerca de dichos destinatarios, si este así lo solicita.

Para los derechos de rectificación y supresión (bloqueo de datos): El responsable que reciba una solicitud de rectificación o supresión debe proceder al bloqueo de los datos que sean objeto de corrección o supresión.

En la práctica, bloquear los datos supone para el responsable "marcarlos" (es decir, conservarlos, pero manteniéndolos "congelados"), de manera que no sean objeto de las operaciones de tratamiento habituales, ni sean accesibles al personal que tuviera habitualmente tal acceso (limitando su acceso a una persona). Para ello, deberán adoptarse medidas técnicas para que se indique claramente en el sistema que dichos datos han sido bloqueados, y para impedir que los datos puedan modificarse o ser objeto de operaciones de tratamiento ulterior. Algunos métodos para hacerlo (en tratamientos automatizados) serían los siguientes:

- trasladar temporalmente los datos a otro sistema
- impedir el acceso de usuarios a los datos
- retirar temporalmente los datos publicados de un sitio web

Los datos bloqueados únicamente podrán utilizarse para su puesta a disposición de jueces, tribunales, el Ministerio Fiscal o las Administraciones competentes (en particular, de las Autoridades de protección de datos), en caso de requerimiento de los mismos para la exigencia de posibles responsabilidades derivadas del tratamiento.

El plazo de conservación de los datos bloqueados será el plazo de prescripción de las citadas responsabilidades (de 1 a 3 años), por lo que deberá determinarse en cada caso en función de las circunstancias que concurran.

Cuestiones relativas a la Ley de Transparencia
La atención al ejercicio de derechos que se describe en este Anexo debe considerar las obligaciones establecidas en la Ley de Transparencia y Buen Gobierno a fecha 24 de junio de 2015 por lo que se incluyen menciones a la normativa anterior. (LOPD 15/1999)

En cuanto al derecho de acceso a la información pública referida al ejercicio de funciones públicas, si la información solicitada contuviera datos de carácter personal de categorías especiales (art. 9 RGPD) el acceso únicamente se podrá autorizar en caso de que se contase con el consentimiento expreso y por escrito del afectado, a menos que dicho afectado hubiese hecho manifiestamente públicos los datos con anterioridad a que se solicitase el acceso.

Si la información incluyese datos personales que hagan referencia al origen racial, a la salud o a la vida sexual, incluyese datos genéticos o biométricos o contuviera datos relativos a la comisión de infracciones penales o administrativas que no conllevasen la amonestación pública al infractor, el acceso solo se podrá autorizar en caso de que se cuente con el consentimiento expreso del afectado o si aquel estuviera amparado por una norma con rango de ley.

Con carácter general, y salvo que en el acceso concreto prevalezca la protección de datos personales u otros derechos constitucionalmente protegidos sobre el interés público en la divulgación que lo impida, se concederá el acceso a la información que contenga los datos meramente identificativos relacionados con la organización, funcionamiento o actividad pública del Colegio.

Cuando la información solicitada no contuviera datos especialmente protegidos, el órgano al que se dirija la solicitud concederá el acceso previa ponderación suficientemente razonada del interés público en la divulgación de la información

y los derechos de los afectados cuyos datos aparezcan en la información solicitada, en particular su derecho fundamental a la protección de datos de carácter personal.

Para la realización de la citada ponderación, dicho órgano tomará particularmente en consideración los siguientes criterios:

a) El menor perjuicio a los afectados derivados del transcurso de los plazos establecidos en el artículo 57 de la Ley 16/1985, de 25 de junio, del Patrimonio Histórico Español.

b) La justificación por los solicitantes de su petición en el ejercicio de un derecho o el hecho de que tengan la condición de investigadores y motiven el acceso en fines históricos, científicos o estadísticos.

c) El menor perjuicio de los derechos de los afectados en caso de que los documentos únicamente contuviesen datos de carácter meramente identificativo de aquéllos.

d) La mayor garantía de los derechos de los afectados en caso de que los datos contenidos en el documento puedan afectar a su intimidad o a su seguridad, o se refieran a menores de edad.

Se transcribe a continuación el Criterio interpretativo nº 2 adoptado por el Consejo de Transparencia y Buen Gobierno en relación al límite del derecho a la protección de datos de carácter personal en el cumplimiento de la transparencia pasiva o derecho de información pública.

Los artículos 14 y 15 de la Ley de Transparencia y Buen Gobierno establecen los límites del derecho de acceso a la información pública que, de conformidad con el artículo 5, número 3, de la Ley, resultan también aplicables a las obligaciones de publicidad activa regulados en la norma.

El proceso de aplicación de estas normas comprende las siguientes etapas o fases sucesivas:

I. Valorar si la información solicitada o sometida a publicidad activa contiene o no datos de carácter personal, entendiéndose por éstos los definidos en el artículo 3 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en adelante LOPD)

II. En caso afirmativo, valorar si los datos son o no datos especialmente protegidos en los términos del artículo 7 de la LOPD, esto es: a) Datos reveladores de la ideología, afiliación sindical, religión y creencias; b) Datos de carácter personal que hagan referencia al origen racial, a la salud y a la vida sexual, y c) Datos de carácter personal relativos a la comisión de infracciones penales o administrativas. Si contuviera datos de carácter personal especialmente protegidos, la información solo se podrá publicar o facilitar: a) En el supuesto de los datos de la letra a) anterior, cuando se cuente con el consentimiento expreso y por escrito del afectado, a menos que dicho afectado hubiese hecho manifiestamente públicos los datos con anterioridad a que se solicitase el acceso. b) En el supuesto de los datos de la letra b) anterior, cuando se cuente con el consentimiento expreso del afectado o estuviera amparado por una norma con rango de Ley, y c) En el supuesto de los datos de la letra c) anterior, y siempre que las correspondientes infracciones penales o administrativas no conlleven la amonestación pública al infractor, cuando se cuente con el consentimiento expreso del afectado o estuviera amparado por una norma con rango de Ley,

III. Si los datos de carácter personal contenidos en la información no fueran datos especialmente protegidos, valorar si son o no exclusivamente datos meramente identificativos relacionados con la organización, el funcionamiento o la actividad pública del órgano o entidad correspondiente. Si los datos contendidos son exclusivamente identificativos relacionados con la organización, el funcionamiento o la actividad pública del órgano o entidad, la información se publicará o facilitará con carácter general, salvo que en el caso concreto prevalezca la protección de datos personales y otros derechos constitucionalmente protegidos sobre el interés público en la divulgación.

IV. Si los datos de carácter personal no fueran meramente identificativos y relacionados con la organización, el funcionamiento o la actividad pública del órgano o no lo fueran exclusivamente, efectuar la ponderación prevista en el artículo 15 número 3 de la LTAIBG.

V. Finalmente, una vez realizados los pasos anteriores, valorar si resultan de aplicación los límites previstos en el artículo 14. Los límites a que se refiere el artículo 14 de la LTAIBG, a diferencia de los relativos a la protección de los datos de carácter personal, no se aplican directamente, sino que de acuerdo con la literalidad del texto del número 1 del mismo, “podrán” ser aplicados.

De esta manera, los límites no operan ni automáticamente a favor de la denegación ni absolutamente en relación a los contenidos.

La invocación de motivos de interés público para limitar el acceso a la información deberá estar ligada con la protección concreta de un interés racional y legítimo.

En este sentido su aplicación no será en ningún caso automática: antes al contrario deberá analizarse si la estimación de la petición de información supone un perjuicio (test del daño) concreto, definido y evaluable. Este, además no podrá afectar o ser relevante para un determinado ámbito material, porque de lo contrario se estaría excluyendo un bloque completo de información.

Del mismo modo, es necesaria una aplicación justificada y proporcional atendiendo a la circunstancia del caso concreto y siempre que no exista un interés que justifique la publicidad o el acceso (test del interés público).

CONCLUSIÓN:
En atención a lo analizado anteriormente, a juicio de este Consejo de Transparencia y Buen Gobierno y de esta Agencia Española de Protección de Datos procede concluir lo siguiente:

a) Los artículos 14 y 15 de la LTAIBG regulan los límites del derecho de acceso a la información que no operan de forma automática, sino que habrán de ser aplicados de acuerdo con las reglas de aplicación y los elementos de ponderación que establecen la citada Ley y la LOPD.

b) El orden de ponderación opera desde el artículo 15 al 14 con valoración de los elementos que modulan la toma de decisiones.

c) El artículo 14 no supondrá, en ningún caso una exclusión automática del derecho a la información, antes al contrario, deberá justificar el test del daño y el del interés público para ser aplicado.

d) Del mismo modo, su aplicación deberá justificar y motivar la denegación.

e) En cualquier caso si no cupiera el otorgamiento del acceso a la totalidad de la información una vez hechas las valoraciones anunciadas, se concederá acceso parcial previa omisión de la información afectada por el límite salvo que de ello resulte una información distorsionada o que carezca de sentido. En este caso, deberá indicarse al solicitante que parte de la información ha sido omitida.

f) Todas las resoluciones denegatorias, total o parcialmente, del acceso en aplicación de los límites previstos en el artículo 14 de la LTAIBG serán objeto de publicidad en los términos establecidos en el art. 14.3 de la misma.

Principios a observar para atender a las solicitudes
Como guía a seguir a la hora de atender los derechos de los interesados, se desarrollan a continuación los siguientes principios básicos:

A. Toda solicitud debe responderse en el plazo máximo de 1 mes a partir de su recepción. Dicho plazo únicamente podrá prorrogarse otros 2 meses en caso necesario, teniendo en cuenta la complejidad y el número de solicitudes.

B. Se contestará siempre por escrito y de forma gratuita.
Cuando el interesado presente su solicitud por medios electrónicos, se contestará también por medios electrónicos (salvo que el interesado solicite otro medio), activando la función de confirmación de lectura.
En caso de solicitud por correo postal, se contestará mediante correo certificado con acuse de recibo.
En caso de solicitud verbal, se informará al interesado de que su solicitud debe presentarse por escrito y acompañada de copia de su DNI.
En todos los casos, se conservará la solicitud recibida, la respuesta facilitada y el acuse de recibo.

C. Se facilitará la información de forma concisa y transparente, utilizando un lenguaje fácil de entender, claro y sencillo.

D. Deberá verificarse la identidad del solicitante, mediante copia de su DNI o pasaporte, para comprobar que quien ejercita el derecho es el titular de los datos. En caso de que el interesado no hubiera aportado su DNI o pasaporte junto a la solicitud, se le solicitará para poder atender su derecho.

En caso de que el interesado actúe mediante representante, se solicitará a éste que acredite su identidad y la representación otorgada a su favor. Igualmente, en el caso de tratarse de un menor de edad que actúe a través de sus padres o tutor legal, el representante legal deberá acreditar dicha condición.

E. Deben contestarse todas las solicitudes recibidas, sin excepción. Esto incluye:
- solicitudes de personas cuyos datos se compruebe que no constan en el sistema del responsable;
- solicitudes de personas que no acrediten su identidad;
- solicitudes que se reciban por medios distintos de los dispuestos para ello por el responsable del tratamiento;
- solicitudes que vayan a denegarse por algún motivo (ver apdo. siguiente).

F. En caso de que el responsable deniegue una solicitud, deberá:
- contestar, a más tardar, en el plazo de 1 mes desde la solicitud;
- concretar los motivos de la denegación;
- y, además, informar al interesado de la posibilidad de presentar una reclamación ante la Autoridad de control y de ejercitar acciones judiciales

G. Para que una solicitud se considere correctamente atendida, no sólo debe hacerse efectivo el derecho ejercitado, sino que, además, hay que contestar al interesado confirmando la acción realizada. Por ejemplo: si una persona solicita la rectificación de un dato inexacto, no basta con corregir dicho dato en el sistema, sino que también hay que contestar al interesado para confirmarle la corrección efectuada, dentro del plazo máximo de 1 mes.

H. Cuando el interesado haya solicitado la rectificación o la supresión de sus datos, se adoptarán las medidas técnicas necesarias para proceder al bloqueo de los datos. En ningún caso se procederá al borrado o eliminación de la información antes de que finalice el período de bloqueo, y sin haberse asegurado de que no concurre alguna de las circunstancias que impide dicho borrado (ej.: deber de conservación por obligación legal).

I. En los casos en que proceda limitar el tratamiento de los datos deberán analizarse las medidas técnicas a adoptar para hacerlo posible.

J. Si el interesado ejercita cualquiera de los derechos de rectificación, supresión o limitación del tratamiento, se deberá notificar la acción realizada a cada uno de los destinatarios a los que se hubieran cedido previamente los datos.

En caso de oposición del interesado al uso de sus datos con fines publicitarios o comerciales, deberán tomarse las medidas necesarias para impedir cualquier nuevo envío publicitario a dicho interesado

Protocolo de actuación
Para la correcta atención de los derechos, sugerimos seguir los pasos que se describen a continuación.

Los interesados deberán ejercitar sus derechos ante el Delegado de Protección de Datos (“DPO”) designado por la organización, Don. Alberto Pecci, mediante el envío de un correo electrónico a la dirección dpo@ciccp o mediante correo ordinario a la dirección Calle Almagro, 42, 20010, Madrid.

En el caso de que Don Alberto Pecci, se encuentre en alguna situación que le imposibilite la atención de los derechos de los interesados se designa a D./Dña. [_____] como responsable de atender las solicitudes.

Esta designación se comunicará a todo el personal del Colegio de Ingenieros de Caminos, Canales y Puertos.

Paso 1 - Recepción de la solicitud

1.1.- El empleado/a que reciba la solicitud (ya sea por correo postal, electrónico o de forma presencial), la comunicará inmediatamente al DPD de la organización.

1.2.- El DPD comprobará:

a. Si la solicitud va acompañada de copia del DNI u otro medio de identificación del interesado y, en su caso, del representante;

b. Si se especifica suficientemente en la solicitud cuál es el derecho ejercitado (acceso, rectificación, supresión, etc.), y a qué tratamiento de datos se refiere (tratamiento de datos de empleados, de clientes, de proveedores, etc.).

En caso de no cumplirse el requisito 1.2.a, se procederá según se describe en el Paso 4.1.b. En caso de no cumplirse el requisito 1.2.b, se procederá según se describe en el Paso 4.1.c.

En caso de cumplirse ambos requisitos, el DPD informará de la solicitud recibida a la persona responsable del Departamento afectado (ej.: si es un proveedor, al responsable del Dpto. de Compras), y la gestionará siguiendo los Pasos siguientes.

Paso 2 - Gestión de la solicitud

2.1.- En caso de concurrir los requisitos para atender la solicitud, el DPD solicitará al/la responsable del Departamento afectado que se compruebe la información disponible relacionada con el derecho ejercitado por el interesado.

2.2.- Si se tratara de una solicitud de acceso, se comprobará igualmente si la misma persona hubiera ejercitado el mismo derecho en los 6 meses anteriores.

2.3.- Si se tratara de una solicitud de rectificación, de supresión o de limitación del tratamiento, se verificará también si los datos del interesado hubieran sido comunicados a terceros.

Paso 3 - Atención del derecho ejercitado

3.1.- Una vez obtenida la información necesaria por parte del Departamento(s) afectado(s), el DPD dará las instrucciones internas necesarias para que se haga efectivo el derecho ejercitado por el interesado, antes del vencimiento del plazo de 1 mes a contar desde la recepción de la solicitud.

3.2.- El derecho ejercitado se hará efectivo mediante la adopción de las medidas técnicas y/o organizativas necesarias. Para la determinación de dichas medidas se analizará el alcance del derecho ejercitado y se observarán los principios definidos en este documento.

Paso 4 - Respuesta al interesado

4.1.- Antes del vencimiento del plazo de 1 mes desde la recepción de la solicitud se procederá a enviar al interesado la respuesta a su solicitud, de acuerdo a la opción que proceda de entre las siguientes:

a. Que la solicitud haya sido atendida, en cuyo caso se informará de ello al interesado.

Si la solicitud atendida tuviera por objeto cualquiera de los derechos de rectificación, supresión o limitación del tratamiento, se deberá igualmente notificar la acción realizada a cada uno de los destinatarios a los que, en su caso, se hubieran comunicado previamente los datos.

b. Que la solicitud haya sido denegada, en cuyo caso se informará de los motivos de la denegación, así como de la posibilidad de presentar una reclamación ante una autoridad de control y de ejercitar acciones judiciales.

c. Que la solicitud no sea suficientemente clara o existan dudas sobre el derecho ejercitado o sobre la identidad del interesado, en cuyo caso se le solicitarán las aclaraciones correspondientes (en caso de recibirse dichas aclaraciones, se retomará el Procedimiento en el Paso 2).

4.2.- Para la respuesta al interesado se utilizará alguno de los medios indicados anteriormente. A saber:

Se contestará siempre por escrito y de forma gratuita.
Cuando el interesado presente su solicitud por medios electrónicos, se contestará también por medios electrónicos (salvo que el interesado solicite otro medio), activando la función de confirmación de lectura.
En caso de solicitud por correo postal, se contestará mediante correo certificado con acuse de recibo.
En caso de solicitud verbal, se informará al interesado de que su solicitud debe presentarse por escrito y acompañada de copia de su DNI.
En todos los casos, se conservará la solicitud recibida, la respuesta facilitada y el acuse de recibo

Paso 5 - Archivo de la solicitud

5.1.- Una vez finalizada la gestión de cada solicitud, el DPD procederá a su archivo, incluyendo toda la documentación generada, las gestiones realizadas y las comunicaciones con el interesado (y sus acuses de recibo).

Modelo de respuesta

Estimado Sr. _____

Acusamos recibo de su correo electrónico de fecha ___ de _____ de 2018, por el que solicita la supresión de los datos de carácter personal referentes a ud.

El Colegio va a proceder a la supresión solicitada de sus datos con la excepción que procede y de acuerdo con los plazos y procedimiento siguiente:

-Conservaremos con fines de archivo de interés público (al amparo del artículo 17.3.e, en relación con el art. 17.3.b), del REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales, en adelante RGPD) sus datos de identificación (nombre, apellidos, nº de DNI) , datos referentes al título habilitante y de pertenencia al Colegio (fechas de alta y baja)

-Durante el plazo de tres años al amparo del artículo 17.3.e RGPD conservaremos, el resto de sus datos bloqueados quedando a disposición exclusiva de los jueces y tribunales, el Ministerio Fiscal o las Administraciones Públicas competentes, en particular de las autoridades de protección de datos, para la exigencia de posibles responsabilidades derivadas del tratamiento y por el plazo señalado de prescripción de las mismas. Los datos bloqueados no podrán ser tratados para ninguna finalidad distinta de la señalada en el apartado anterior. Transcurridos esos tres años los datos se suprimirán mediante su borrado, en el caso de datos en soportes informáticos, o destrucción, en el caso de soporte papel.

Le informamos que cuando proceda, tiene los derechos a acceder, rectificar y suprimir los datos, solicitar la portabilidad de los mismos, oponerse al tratamiento y solicitar la limitación de éste. Se pueden ejercer por correo electrónico en derechosdatos@ciccp.es . Le informamos que la dirección de contacto del Delegado de Protección de Datos del Colegio es dpo@ciccp.es y que la autoridad competente para tutelar el ejercicio de los derechos de protección de datos es la Agencia Española de Protección de Datos sita en Calle Jorge Juan, 6, 28001 Madrid, con página web www.agpd.es y sede electrónica en https://sedeagpd.gob.es/sede-electronica-web/.

Asimismo, en pie de página le informamos del posible tratamiento de sus datos de carácter personal en relación al ejercicio de derechos derivados del Reglamento General de Protección de Datos, pudiendo consultar todas las actividades de tratamiento que lleva a cabo el Colegio en http://www.ciccp.es/rgpd/rat/RAT_Web_v1_0.htm*

Atentamente,

(*)

En cumplimiento del Reglamento General de Protección de Protección de Datos (RGPD) en relación a los datos de carácter personal que el Colegio trata para atender su solicitud, se informa al interesado de lo siguiente:		
Responsable	Colegio de Ingenieros de Caminos, Canales y Puertos	
Finalidades	Atención de los derechos reconocidos en el Reglamento General de Protección de Datos de las Personas (art 5 RGPD) .	
Legitimación	RGPD: 6.1.c) Tratamiento necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento. Reglamento General de Protección de Datos Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.	
Cesiones	No se prevén, salvo, si procede, Agencia Española de Protección de Datos	
Procedencia	El propio interesado o su representante legal .	
Derechos	Acceder, rectificar y suprimir los datos, solicitar la portabilidad de los mismos, oponerse al tratamiento y solicitar la limitación de éste Los derechos se pueden ejercer en derechosdatos@ciccp.es	
Versión	2018.09	+ info Aquí puede consultar todas las actividades de tratamiento que lleva a cabo el Colegio: Registro de Actividades de Tratamiento

Modelo de informe de seguimiento
Se acompaña a continuación una propuesta organizativa para gestionar las solicitudes de ejercicio de derechos.

En la siguiente tabla puede llevarse un seguimiento de la atención de cada uno de los ejercicios de derecho:

Nº	COD.	NOMBRE Y APELLIDOS	FECHA SOLICITUD	DERECHO/S SOLICITADO/S	FECHA LIMITE RESPUESTA	FECHA/S DE RESPUESTA	TRAT.	CAT INTERESADO	CAT. DATOS
Número	Código	Nombre y apellidos del solicitante	Fecha entrada solicitud	Derecho/s que ejercita o contenido de su petición	= Fecha entrada solicitud + 30 días hábiles		Tratamiento identificado en el RAT	Ej. Colegiados	Ej. Datos identificativos

Posteriormente, por cada ejercicio se podrá redactar un informe en el que se incluyan la siguiente estructura:

I.- Antecedentes

a.- Fecha de entrada solicitud

b.- Se verifica que la solicitud constituye un ejercicio de derechos de datos personales, por lo que debe ser atendido por CICCP de conformidad con lo establecido en su procedimiento de atención a derechos.

c.- Se activa el procedimiento de atención al ejercicio de derechos

II.- Acciones desplegadas: donde se relacionen todas las medidas desplegadas en atención a la solicitud recibida, incluyendo pantallazos de las respuestas ofrecidas.

ANEXO G
PROCEDIMIENTO DE BRECHAS DE SEGURIDAD

Objeto

Este documento, que se integra en el sistema documental de Protección de Datos de carácter personal del CICCP, establece el procedimiento por el que se rige la gestión de brechas de seguridad relativas a la Protección de Datos personales de los que el colegio sea responsable del tratamiento. El RGPD Denomina a las brechas de seguridad como "violaciones de seguridad" y las define como "toda violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.

El procedimiento se establece, en cumplimiento del principio de responsabilidad proactiva previsto en el RGPD, con la finalidad de la correcta identificación, registro y resolución, con minimización de daños de las brechas de seguridad que afecten a datos de carácter personal.

La gestión de la brecha se realizará según la política de seguridad de la información del Colegio la normativa de seguridad los procedimientos de seguridad, los procesos de autorización y el marco operacional y de protección que establecen las medidas de seguridad de la información que rigen en el Colegio, y que contemplan los aspectos de prevención, detección y corrección para conseguir que las amenazas sobre la información no se materialicen, y si ello sucede, no afecten gravemente a la información que maneja o los servicios que se prestan por la corporación.

La existencia de este procedimiento de gestión de brechas de seguridad se hará constar en el decálogo de buenas prácticas en Protección de Datos dirigido a los/as empleados/as del Colegio a los que se les instruirá en cómo actuar ante brechas de seguridad y de las responsabilidades que les correspondan.

La brecha puede tener impacto en la corporación desde diferentes puntos de vista: la protección de la información, la prestación de los servicios, o el cumplimiento normativo o conformidad legal y la reputación e imagen públicas. Por ello, toda la organización debe ser consciente de cómo actuar ante una brecha de seguridad y responder para la minimización de los riesgos y daños.

La detección e identificación de un incidente que se califica como brecha de seguridad que afecte a datos de carácter personal dará lugar en el colegio a la apertura de un expediente de brecha de seguridad y a la conformación de un equipo de respuesta dirigido por:
- El Comité de Seguridad
- El Delegado de Protección de Datos

Dado el impacto y los perjuicios que las brechas pueden originar, los expedientes de brechas de seguridad se comunicarán

a otras direcciones. Las personas titulares de estas direcciones podrán integrarse en los equipos de respuesta.

Como consecuencia de dichas brechas o violaciones se puede comprometer al colegio, como responsable del tratamiento, en el cumplimiento de los principios y obligaciones del RGPD. Si no se toman a tiempo las medidas adecuadas coma las violaciones de seguridad de los datos personales pueden entrañar daños y perjuicios físicos, materiales o inmateriales para las personas físicas, como la pérdida de control sobre sus datos personales o restricción de sus derechos, discriminación, usurpación de identidad, pérdidas financieras, reversión no autorizada de la seudonimización , daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, o cualquier otro perjuicio económico o social significativo para la persona física en cuestión.

La gestión de una brecha de seguridad requiere determinar la peligrosidad potencial del incidente y la estimación de la magnitud del impacto potencial en los individuos. Para esta evaluación se deberá recurrir al análisis de riesgo su evaluación de impacto realizado antes de la puesta en marcha de las actividades de tratamiento y a una clasificación previa del incidente según procedimiento establecido. Una vez se ha detectado e identificado una brecha de seguridad es necesario poner en marcha un plan de actuación previamente definido y aprobado para solucionar el incidente. Durante el proceso de respuesta coma en una 1ª fase se intenta contener el incidente, tras lo cual se erradica la situación generada por el mismo y se termina con las acciones de recuperación oportunas.

De acuerdo con el RGPD, tan pronto como el la responsable del tratamiento tenga conocimiento de que se ha producido una violación de la seguridad de los datos personales, el/la responsable debe, sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, notificar la violación de la seguridad de los datos personales a la autoridad de control competente coma la Agencia Española de Protección de Datos coma a menos que el/la responsable pueda demostrar, atendiendo al principio de responsabilidad proactiva, la improbabilidad de que la violación de la seguridad de los datos personales entrañen un riesgo para los derechos y libertades de las personas físicas. Si dicha notificación no es posible en el plazo de 72 horas, debe acompañarse de una indicación de los motivos de la dilación, pudiendo facilitarse información por fases.

El/la responsable del tratamiento también debe comunicar al interesado/a sin dilación indebida la violación de la seguridad de los datos personales en caso de que puede entrañar un alto riesgo para sus derechos y libertades, y permitirle tomar las precauciones necesarias. La comunicación debe describir la naturaleza de la violación de la seguridad de los datos personales y las recomendaciones para que la persona física afectada mitigue los potenciales efectos adversos resultantes de la violación. Dichas comunicaciones a los/as interesados/as deben realizarse tan pronto como sea razonablemente posible y en estrecha cooperación con la autoridad de control, siguiendo sus orientaciones o por las de otras autoridades competentes. como las autoridades policiales. Así, por ejemplo, la necesidad de mitigar un riesgo de daños y perjuicios inmediatos justificaría una rápida comunicación con los interesados/as, mientras que cabe justificar que la comunicación lleve más tiempo por la necesidad de aplicar medidas adecuadas para impedir violaciones continuas de la seguridad de los datos personales o similares.

La gestión integral de las brechas de seguridad debe entenderse como parte de la proactividad del colegio como responsable del tratamiento, además de como una forma de dar cumplimiento a la obligación de mantener un registro documental de las incidencias y las notificaciones.

Para una buena gestión de las brechas de seguridad en la responsable debe documentar las debidamente según el artículo 33 RGPD, a tal efecto debe disponer de un registro de incidencias. La documentación de todo proceso de gestión y respuesta es importante de cara a comunicaciones a partes interesadas de carácter interno o externo, y a la elaboración de un informe de respuesta, que tras su análisis permita extraer conclusiones. Es necesario documentar los hechos efectos y las medidas correctivas adoptadas así como la propia notificación a las autoridades y afectados de modo que esta documentación permita a la autoridad de control verificar el cumplimiento de la obligación de notificación en todo su contenido. Este procedimiento se basa en la Guía para la Gestión y Notificación de Brechas de Seguridad (2018) editada por la Agencia Española de Protección de Datos, en colaboración con el Centro Criptológico Nacional y el Instituto Nacional de Ciberseguridad adaptado a las circunstancias del Colegio.

Procedimiento general

El procedimiento general de brechas de seguridad será gestionado por el Comité de Seguridad en el que se integrará el Delegado de Protección de Datos.

La existencia de este procedimiento se hará constar en el decálogo de buenas prácticas en Protección de Datos dirigidos a

los/as empleados/as del Colegio y se instruirá a toda la plantilla en las responsabilidades que derivan del mismo en la debida comunicación de la sospecha o conocimiento de incidencias en la seguridad de la información y la Protección de Datos de carácter personal al Delegado de Protección de Datos.

El procedimiento tiene 4 fases:
1. Detección, identificación y clasificación.
2. Respuesta.
3. Notificación.
4. Seguimiento y cierre.

Detección, identificación y clasificación.
Durante esta fase de detección e identificación se concretan las situaciones que se consideran incidentes de seguridad y las herramientas, mecanismos de detección o sistemas de alerta. Estos mecanismos permitirán a la Corporación identificar una brecha de seguridad en caso de que se produzca.

La identificación de un incidente de seguridad puede producirse a través de fuentes internas a la organización o fuentes externas.

Son fuentes internas las que provienen de controles y mecanismos de seguridad dentro y alrededor de las instalaciones de la corporación, así como los medios de acceso remoto a la información.

Desde el punto de vista de la seguridad física, la detección se produciría ante el incumplimiento o vulneración de las medidas de seguridad adoptadas por o respecto a:
• Políticas de accesos con usuario y contraseña;
• Políticas específicas del puesto de trabajo: mesas limpias, bloqueo de pantallas de los terminales informáticos.
• Controles físicos como alarmas (de detección de intrusos, de incendios, etc.) video vigilancia, control y registro de accesos a determinadas zonas de acceso restringido.
• Procedimientos establecidos en la materia, como por ejemplo, Procedimiento de atención a Derechos y los requisitos que de identificación de los/as interesados/as establece el procedimiento.

Es preciso tener en cuenta que un incidente y que tenga lugar en el ámbito de la seguridad física puede tener repercusión en el contexto de la ciberseguridad.

En cuanto a los controles de ciberseguridad, la fuente sobre la incidencia puede provenir de la notificación de problemas por parte del personal del Colegio o de sistemas automatizados de detección de diferentes tipos. Se pueden considerar las siguientes fuentes de información:
• Notificaciones de usuarios: presencia de archivos con caracteres inusuales; recepción de correos electrónicos con archivos adjuntos sospechosos; comportamiento extraño de dispositivos; imposibilidad de acceder a ciertos servicios; extravío o robo de dispositivos de almacenamiento o equipos con información.
• Alertas generadas por software antivirus.
• Consumos excesivos y repentinos de memoria o disco en servidores y equipos.
• Anomalías de tráfico de red o picos de tráfico en horas inusuales.
• Alertas de sistemas de detección/prevención de intrusión (IDS/IPS). Un IDS aporta a la red un grado de seguridad preventivo ante cualquier actividad sospechosa.
• Alertas de sistemas de correlación de eventos.
• Análisis de registros de conexiones realizadas a través de proxys corporativos o conexiones bloqueadas en cortafuegos.
• Análisis de registro de servidores y aplicaciones con intentos de acceso no autorizados.
• Análisis de registros en herramientas DLP (Data Loss Prevention).
• También se debe considerar cualquier posible indicio de la ocurrencia de un incidente de seguridad en el futuro como el análisis del resultado de un escáner de vulnerabilidades del sistema, el anuncio de un nuevo 'exploit' dirigido a atacar una vulnerabilidad que podría estar presente en el sistema o amenazas explícitas anunciando ataques a los sistemas de información de la corporación.

En muchas ocasiones es posible que la detección del incidente se produzca a través de una fuente externa, de la comunicación de un 3º proveedores de servicios informáticos proveedores de servicios de internet o fabricantes de soluciones de seguridad; por un colegiado/a o un usuario de los servicios del colegio; o un colaborador/a o encargado/a de tratamiento de este; o por la comunicación pública o las notificaciones que se pudieran realizar por el Colegio por los distintos organismos públicos como Agencia Española de Protección de Datos (AEPD), el Centro Criptológico Nacional (CCN); y el Instituto Nacional de Ciberseguridad (INCIBE); Fuerzas y cuerpos de Seguridad del Estado, o incluso mediante la información publicada en medios de comunicación.

El análisis de información recibida o manejada permitirá determinar si se está ante un incidente de seguridad o no, así como la naturaleza, clase, tipo, si dicho incidente ha afectado a datos de carácter personal y por tanto constituye una brecha

de los datos de carácter personal de las previstas en el RGPD, y el nivel de riesgo al que se enfrenta la corporación y los/as interesados/as de los que trata datos.

Se deberá documentar e incorporar al registro de incidencias que forma parte del sistema documental de Protección de Datos toda la información relevante: desde los síntomas y mecanismos de detección que permitieron identificarlo, hasta las acciones y medidas de control adoptadas en cada una de las fases de gestión del del incidente. En particular, se deberá mantener como mínimo un registro documental de los incidentes de seguridad que hayan afectado a los datos de carácter personal incluyendo el tipo de incidente, descripción del mismo, gravedad estado y medidas adoptadas para su resolución. Por otra parte, una de las ventajas de disponer de este registro documental de incidencias es que, en ocasiones, incidentes de pequeña entidad pueden revelar la ocurrencia de un problema mayor previamente no identificado.

Las incidencias deben ser I) tipificadas; II) clasificadas y III) valoradas por el equipo de gestión.

I.- Tipificación
Una brecha de seguridad puede ser, de alguno de los siguientes tipos:

- Brecha de confidencialidad: tiene lugar cuando partes (personas o aplicaciones) que no están autorizadas, o no tienen un propósito legítimo para acceder a la información acceden a ella. La severidad de la pérdida de confidencialidad varía según el alcance de la divulgación, es decir, el número potencial y el tipo de partes que pueden haber accedido ilegal o ilícitamente a la información.

- Brecha de integridad: se produce cuando se altera la información original y la sustitución de datos puede ser perjudicial para el/la interesado/a afectado/a. La situación más grave ocurre cuando existen serias posibilidades de que los datos alterados se hayan utilizado de una manera que pueda dañar al interesado/a.

- Brecha de disponibilidad: su consecuencia es que no se puede acceder a los datos originales cuando es necesario. Puede ser temporal (los datos son recuperables, pero tomará un periodo de tiempo y esto puede ser perjudicial para el/la interesado/a afectado/a), o permanente (los datos no pueden recuperarse).

II.- Clasificación
Los factores que se pueden considerar a la hora de establecer criterios de clasificación son, entre otros:

- Tipo de amenaza: código dañino, intrusiones, fraude etc. Se trata de una breve descripción del incidente en función de la información de la que se disponga.

- Contexto u origen de la amenaza: interna o externa.

- El perfil de los/as interesados/as afectados/as (colegiados/as; personal; usuarios de servicios del Colegio; ciudadanos/as; proveedores o colaboradores/as; etc.)

- Número y tipología de los sistemas afectados.

- Dimensión de la seguridad afectada (según ENS: disponibilidad, autenticidad, integridad, confidencialidad, trazabilidad.)

- Categoría del sistema de información: Según ENS: media.

El CICCP ha procedido a realiza la clasificación de su sistema de información en base a lo establecido por el ENS siendo el resultado que la totalidad de su sistema de información está categorizado como de seguridad “media” de conformidad con su art. 43.

- Vector de ataque o método: ruta, forma o medio por el que se ha materializado el incidente. Entre las tipologías de casos que pueden dar lugar a un incidente de seguridad, se puede citar:

o 0-day (vulnerabilidad no conocida): vulnerabilidad que permite a un atacante el acceso a datos en la medida en que es una vulnerabilidad desconocida. Esta vulnerabilidad existirá hasta que el fabricante o desarrollador la resuelva.

o APT (ataque dirigido): se refiere a diferentes tipos de ataques dirigidos normalmente a recabar información fundamental que permita continuar con ataques más sofisticados. En esta categoría se encuadraría por ejemplo una campaña de envío de email con software malintencionado a empleados/as hasta conseguir que alguno de ellos lo instale en su equipo y proporcione una puerta de salida al sistema.

o Denegación de servicio (DoS/DDoS): Consiste en inundar de tráfico un sistema hasta que no sea capaz de dar servicio a los/as usuarios/as legítimos del mismo.

o Acceso a cuentas privilegiadas: el atacante consigue acceder al sistema mediante una cuenta de usuario con privilegios

avanzados, lo que le confiere libertad de acciones previamente deberá haber conseguido el nombre de usuario y contraseña por algún método, por ejemplo, un ataque dirigido.

o Código malicioso: piezas de software cuyo objetivo es infiltrarse o dañar un ordenador, servidor u otro dispositivo de red con finalidades muy diversas. Una de las posibilidades para que el código dañino alcance a una organización es que un usuario lo instale de forma involuntaria.

o Compromiso de la información: recoge todos los incidentes relacionados con el acceso y fuga, modificación o borrado de información no pública.

o Robo y/o filtración de datos: se incluye en esta categoría la pérdida/robo de información de dispositivos de almacenamientos con información.

o Desfiguración (Defacement): Es un tipo de ataque dirigido qué consiste en la modificación de la página web corporativa con intención de colgar mensajes reivindicativos de algún tipo o cualquier otra intención la operativa normal de la web queda interrumpida como produciéndose además daños reputacionales.

o Explotación de vulnerabilidades de aplicaciones dos cuando un posible atacante logra explotar con éxito una vulnerabilidad existente en un sistema o producto consiguiendo comprometer una aplicación de la organización.

o Ingeniería social: son técnicas basadas en el engaño, normalmente llevadas a cabo a través de las redes sociales que se emplean para dirigir la conducta de una persona u obtener información sensible por ejemplo el usuario es inducido a pulsar sobre un enlace haciéndole pensar que es lo correcto.

1. Fundamentos para la determinación de la categoría de un sistema.

La determinación de la categoría de un sistema se basa en la valoración del impacto que tendría sobre la organización un incidente que afectara a la seguridad de la información o de los sistemas, con repercusión en la capacidad organizativa para:

a) Alcanzar sus objetivos.
b) Proteger los activos a su cargo.
c) Cumplir sus obligaciones diarias de servicio.
d) Respetar la legalidad vigente.
e) Respetar los derechos de las personas.

La determinación de la categoría de un sistema se realizará de acuerdo con lo establecido en el presente real decreto, y será de aplicación a todos los sistemas empleados para la prestación de los servicios de la Administración electrónica y soporte del procedimiento administrativo general.

2. Dimensiones de la seguridad.

A fin de poder determinar el impacto que tendría sobre la organización un incidente que afectara a la seguridad de la información o de los sistemas, y de poder establecer la categoría del sistema, se tendrán en cuenta las siguientes dimensiones de la seguridad, que serán identificadas por sus correspondientes iniciales en mayúsculas:

a) Disponibilidad [D].
b) Autenticidad [A].
c) Integridad [I].
d) Confidencialidad [C].
e) Trazabilidad [T].

3. Determinación del nivel requerido en una dimensión de seguridad.

Una información o un servicio pueden verse afectados en una o más de sus dimensiones de seguridad. Cada dimensión de seguridad afectada se adscribirá a uno de los siguientes niveles: BAJO, MEDIO o ALTO. Si una dimensión de seguridad no se ve afectada, no se adscribirá a ningún nivel.

a) Nivel BAJO. Se utilizará cuando las consecuencias de un incidente de seguridad que afecte a alguna de las dimensiones de seguridad supongan un perjuicio limitado sobre las funciones de la organización, sobre sus activos o sobre los individuos afectados.
Se entenderá por perjuicio limitado:

1.º La reducción de forma apreciable de la capacidad de la organización para atender eficazmente con sus obligaciones corrientes, aunque estas sigan desempeñándose.
2.º El sufrimiento de un daño menor por los activos de la organización.
3.º El incumplimiento formal de alguna ley o regulación, que tenga carácter de subsanable.
4.º Causar un perjuicio menor a algún individuo, que aún siendo molesto pueda ser fácilmente reparable.
5.º Otros de naturaleza análoga.

III.- Valoración
Se ha de valorar el alcance de la brecha de seguridad. La peligrosidad dependerá de los siguientes factores:

La categoría o nivel de criticidad respecto a la seguridad de los sistemas afectados:

- Crítico: cuando concurren los siguientes tres índices: i) cuando afecta a datos valiosos (incluyendo categorías especiales de datos de conformidad con el art. 9 RGPD); ii) gran volumen y iii) en poco tiempo.

IV.- Naturaleza, sensibilidad y categorías de datos afectados.
- Datos legibles/ilegibles: datos protegidos mediante algún sistema de pseudonimización (por ejemplo, cifrado o hash)

- Datos de categorías especiales del art. 9 RGPD: datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o la orientación sexual de una persona física.

- Datos relativos a condenas e infracciones penales o medidas de seguridad conexas.

- Datos relativos a infracciones administrativas o procedimientos disciplinarios.

- Datos confidenciales relativos a la relación laboral.

- Datos sobre características especiales de los individuos: si afectan a menores, a personas con características especiales o con necesidades especiales.

- Datos que permitan evaluar personalidad o comportamiento. Incluidos datos de localización, tráfico, hábitos y preferencias.

- Datos de solvencia patrimonial, financiera, o créditos. Incluyendo transacciones, posiciones, ingresos, cuentas, factura.

- Datos de escaso riesgo: datos básicos de identidad, de contacto o profesionales.

- Alto riesgo, o no, para los derechos y libertades de las personas físicas. La conclusión sobre esta valoración implicará la necesidad, o no, de comunicar la brecha a los/las interesados/as afectados/as. (art. 34 RGPD).

- Volumen de datos personales afectados: expresados en cantidad (registros ficheros, documentos) y/o periodos de tiempo.

- Facilidad de identificación de los/as interesados: facilidad con la que se puede deducir la identidad de los individuos a partir de los datos involucrados en la brecha.

- Severidad de las consecuencias para los individuos:

o Baja: Las personas no se verán afectadas o pueden encontrar algunos inconvenientes que superarán sin ningún problema (tiempo de reingreso de información, molestias, irritaciones, etc.)

o Media: Las personas pueden encontrar inconvenientes importantes que podrán superar a pesar de algunas dificultades (costos adicionales, denegación de acceso a servicios comerciales, miedo, falta de comprensión, estrés, dolencias físicas menores, etc.)

o Alta: las personas pueden enfrentar consecuencias importantes que deberían poder superar, aunque con serias dificultades (malversación de fondos, listas negras de los bancos, daños a la propiedad, pérdida de empleo, citación judicial, empeoramiento de la salud etc.)

o Muy alta: las personas pueden enfrentar consecuencias significativas o incluso irreversibles que no pueden superar (exclusión o marginación social, dificultades financieras tales como deudas considerables o incapacidad para trabajar, dolencias psicológicas o físicas a largo plazo, muerte, etc.)

- Número de individuos afectados: Dentro de uno de los siguientes niveles:
o Bajo: menos de 100.
o Medio: de 101 a 1000.
o Alto: de 1001 a 2.000.
o Muy alto: más de 2.000.

- Perfil de los/as usuarios/as afectados/as: su posición en la estructura organizativa de la entidad y, en su consecuencia, sus privilegios de acceso a información sensible o confidencial.

- El número y tipología de los sistemas afectados.

- El impacto que la brecha puede tener en la organización, desde los puntos de vista de la protección de la información, la prestación de los servicios, la conformidad legal y la imagen pública. Va a estar relacionado con la categoría o criticidad de los servicios afectados y personas afectadas. En este aspecto se diferencia entre los siguientes impactos:
o Bajo (perjuicio limitado)
o Medio (perjuicio grave)
o Alto (perjuicio muy grave)

- Valoración de los requerimientos legales y regulatorios, si procede, o no, notificación de la brecha a la autoridad de control y cualquier otra obligación de notificación, comunicación o denuncia a Fuerzas y Cuerpos de seguridad del Estado en caso de delito.

El análisis de detección su consideración como brecha de seguridad que afecta a datos de carácter personal y su tipificación clasificación y valoración se incorporará al registro de incidencias.

V.- Respuesta
Una vez que el incidente ha sido considerado como una brecha de seguridad que afecta a datos de carácter personal, y a efectos de una correcta y eficaz gestión de la misma cómo se abrirá un expediente al efecto y se conformará un equipo de respuesta coordinado por:
• El Departamento de Sistemas
• Y el Delegado de Protección de Datos.

En función de la incidencia, el equipo de respuesta podrá integrar a otros responsables.

A cada brecha de seguridad se le asignará un código de expediente EBS, consecutivo por años. Si fuera la primera incidencia en 2018, sería EBS 1/2018, y así correlativamente.

En las comunicaciones referidas a la incidencia, se indicará siempre el código, en especial en el asunto de los correos electrónicos para su fácil identificación y atención inmediata. La apertura del expediente será comunicada al Comité de Seguridad y, en su caso, a otras direcciones de CICCP que pudieran tener interés.

El equipo de respuesta se reunirá, si fuera posible, de forma presencial cuantas veces sea necesario. La comunicación y coordinación debe ser fluida y eficiente.

El equipo de respuesta analizará la información disponible, la tipificación, clasificación y valoración inicial, que a la vista de nuevos datos o evolución de la brecha podrán ser contempladas, actualizadas o modificadas.

Todos/as los/as empleados/as del Colegio responderán de forma inmediata a las solicitudes de información o colaboración que les realice el responsable.

El equipo de respuesta dependiendo del nivel de criticidad de la severidad de las consecuencias y del impacto podrá proponer a, equipo de gestión que la Resolución o investigación del incidente requiere de la contratación de servicios externos.

El equipo de respuesta adoptará la puesta en marcha de un plan de contingencia y respuesta para contener y mitigar o eliminar los daños que pudieran sufrir los/as interesados/as afectados/as, con especial atención a las primeras medidas más inmediatas de contención tratando de limitar en lo posible los daños causados por el incidente. Por ejemplo, si un ordenador está infectado, deberá ser desconectado de la red corporativa inmediatamente o, si una información ha sido difundida erróneamente a través de internet, deberá ser retirada. Estas medidas también proporcionan un tiempo para poder desarrollar una solución adecuada sin el factor tiempo.

Durante todo el ciclo de vida de procedimiento de gestión de la brecha de seguridad, y en especial en el proceso de respuesta, debe tenerse en cuenta la recolección y custodia de pruebas/evidencias que permitan disponer de información presentable ante terceros. En todo el proceso de gestión de la brecha se van a tomar las acciones necesarias para contener y revertir el impacto que haya podido tener una brecha de seguridad. estas acciones pueden incurrir en la modificación de evidencias, lo que puede imposibilitar el uso de la información registrada por los sistemas involucrados de cara a la presentación de esta información frente a terceros, y en especial su uso como prueba en procedimientos judiciales y administrativos.

VI.- Contención del incidente
Para tratar de garantizar que la información generada por los sistemas involucrados en una brecha de seguridad cumpla los objetivos de cumplimiento de la organización de cara a que dichos registros puedan ser utilizados frente a terceros y/o en litigios, es necesario tener en consideración dos aspectos para cada brecha de seguridad:

- Por una parte, definir la necesidad de uso de la información por parte de la organización en la propia fase de detección de la brecha de seguridad de cara a la recolección de evidencias.

Por otra establecer la cadena de custodia adecuada que satisfaga el uso de la información definido por la organización.

La contención del incidente proporciona tiempo para desarrollar una estrategia de respuesta a medida. Una parte esencial de la contención es la toma de decisiones rápidas como pueden ser cerrar un sistema, aislarlo de la red, deshabilitar ciertas funciones, etc.

Las medidas de contención podrán ser inmediatas o de aplicación progresiva en función del desarrollo de la solución del incidente. es conveniente determinar las medidas a implantar estableciendo:
- un orden de prioridad;
- los responsables asignados;
- tiempos estimados;
- efectos esperados.

Algunas medidas de contención serán sencillas y las podrá iniciar el usuario, sin embargo otras medidas son más complejas y deben estar en manos de personal especializado que se encargue de la seguridad tecnológica e informática.

En función de cada caso algunas de las medidas de contención que podrían ser de aplicación son las siguientes:

- Si es posible, impedir el acceso al origen de la divulgación: dominios, puertos, servidores, la fuente o los destinatarios de la divulgación. Dependiendo del vector de ataque, impedir el acceso al origen dos dominios, conexiones, equipos informá-

ticos o conexiones remotas, puertos, parches, actualización del software de detección, bloqueo de tráfico, deshabilitar dispositivos, servidores, etc.

- Suspender credenciales lógicas y físicas con acceso a información privilegiada. cambiar todas las contraseñas de usuarios privilegiadas o hacer que los usuarios lo hagan de manera segura.

- Aislar el sistema utilizado para revelar los datos con el fin de realizar un análisis forense más tarde.

- Si los datos han sido enviados a servidores públicos, solicitar al propietario/a (o al webmaster) que elimine los datos divulgados.

- Vigilar la difusión de los documentos/datos filtrados en los diferentes sitios web y redes sociales así como los comentarios y reacciones de usuarios en internet.

VII.- Solución/erradicación
Cuando se ha conseguido contener el incidente, la erradicación puede ser necesaria para solventar determinados efectos del incidente de seguridad, por ejemplo, eliminar malware o desactivar cuentas de usuarios vulneradas. También sirve para identificar y mitigar todas las vulnerabilidades que hubiesen sido explotadas.

Las tareas de erradicación deben contar con la descripción de alto nivel de las tareas, así como de la responsabilidad (equipo interno o externo e identificación del responsable del equipo) de cada una de ellas.

Algunos ejemplos de tareas de erradicación podrían ser las que se enumeran a continuación:

- Definir el proceso de desinfección basado en firmas, herramientas, nuevas versiones/revisiones de software, etc. y probarlo. Asegurar que el proceso de desinfección funciona adecuadamente sin dañar servicios.

- Comprobar la integridad de todos los datos almacenados en el sistema, mediante un sistema de hashes por ejemplo, que permita garantizar que los ficheros no han sido modificados, especial atención debe ser tenida con relación a los ficheros ejecutables.

- Revisar la correcta planificación y actualización de los motores y firmas de antivirus.

- Análisis con antivirus de todo el sistema, los discos duros y la memoria.

- Restaurar conexiones y privilegios paulatinamente. especial acceso restringido paulatino de máquinas remotas o no gestionadas.

Con el objeto de planificar la respuesta al incidente deberá fijarse un plazo para la implementación de las tareas de erradicación. en casos complejos que incluyen múltiples tareas y equipos de ejecución, deberá existir coordinación entre los distintos equipos.

Tras la aplicación de las medidas se debe verificar el correcto funcionamiento de éstas, confirmando su idoneidad para la erradicación del incidente. de ser así, se dará por terminada esta fase.

Se debe considerar también si las medidas aplicadas son de carácter temporal o si forman parte de una solución definitiva, y el sistema y/o la información afectada ha vuelto de nuevo de modo efectivo a su estado original.

Además, debe asegurarse que la misma vulnerabilidad no podrá ser explotada en el futuro, o dicho en otros términos, se deberá tomar medidas que eviten o eliminen la posibilidad de que un incidente vuelva a producirse.

VIII.- Recuperación
Solucionada la brecha de seguridad y verificada la eficacia de las medidas adoptadas, se entra en la fase de recuperación, que tiene como objetivo el restablecimiento del servicio en su totalidad confirmando su funcionamiento normal y evitando en la medida de lo posible que sucedan nuevos incidentes basados en la misma causa.

Esto puede implicar la adopción no solo de medias activas, sino también imple entando controles periódicos y eficaces que permiten el seguimiento pormenorizado en los procesos de mayor riesgo.

Se identificarán las distintas soluciones dirigidas a evitar nuevos incidentes de seguridad basados en la misma causa, así como la eficiencia y costes de las distintas opciones planteadas.

Teniendo en cuenta el riesgo, así como la eficiencia de los costes de las distintas opciones planteadas, el equipo de respuesta propondrá al Comité de Seguridad la estrategia que recomienda seguir a futuro.

Elaboración del informe de resolución
La elaboración del informe de resolución tiene como objetivo servir de base para realizar ejercicios futuros de lecciones aprendidas. Con carácter meramente interno, este informe, este informe debe facilitar a todos los equipos involucrados en la respuesta del incidente, el entendimiento de porqué de las acciones tomadas, así como las acciones marcadas para el seguimiento en el corto, medio y largo plazo. También serán tenidos en cuenta los cambios necesarios que deberían ser incluidos en el análisis de riesgos de la organización.

En la medida de lo posible, este informe debe incluir detalles técnicos sobre diferentes acciones llevadas a cabo. Se nutrirá en gran medida de la documentación elaborada durante el proceso de respuesta. El informe de resolución se debe presentar en forma de línea temporal, de modo que facilite el seguimiento de las diferentes acciones, y debería incluir al menos información relativa a los siguientes apartados:
- Alcance e impacto del incidente.
- Controles preventivos existentes.
- Acciones de respuesta tomadas sobre las diferentes alternativas consideradas para la resolución de la brecha.
- Acciones tomadas para la prevención de futuras brechas.
- Impacto en la resolución del incidente de las acciones de respuesta tomadas.
- Acciones definidas para el seguimiento.

Notificación

I.- Análisis del impacto
La Guía para la Notificación de brechas de Seguridad (2018) de la AEPD establece unos criterios orientativos para interpretar los conceptos jurídicos indeterminados que contiene el RGPD en orden a la toma de decisiones relacionada con la notificación de brechas de seguridad a la autoridad de control y para la comunicación a los interesados, basándose en tres parámetros: i) volumen de afección (nº de registros afectados); ii) tipología de los datos (sensibles/no sensibles); iii) impacto (exposición). A cada parámetro se le otorga un valor y en función de una fórmula [Riesgo = Volumen x Tipología x Impacto] se obtiene el resultado del posible riesgo y de la obligación o no de notificación y comunicación.

En la siguiente tabla figuran la valoración de los criterios y el valor a aplicar en cada caso:

Criterio	Valor a aplicar
VOLUMEN DE AFECCIÓN (P)	
Menos de 100 registros	1
Hasta 1.000	2
Entre 1.000 y 100.000	3
Mas de 100.000	4
Más de 1.000.000	5
TIPOLOGÍA DE DATOS (T)	
Datos no sensibles	X1
Datos sensibles	X2
IMPACTO (I)	
Nulo	X2
Interno (dentro de la empresa / controlado)	X4
Externo (perímetro proveedor / atacante)	X6
Pública (Accesible desde internet)	X8
Desconocido (10)	X10
Cálculo del posible riesgo = P x T x I	

Para que la comunicación sea efectiva se deba de superar el siguiente valor:
- Superior a 20 para la notificación a la Agencia.
- Superior a 40 para la notificación a los/as interesados/as.

II.- Notificación a la Autoridad de Control
Según el art. 33 RGPD, en caso de brecha de la seguridad que afecte a los datos personales, el/la responsable del tratamiento la notificará a la autoridad de control competente, la AEPD, sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, a menos que sea improbable que dicha brecha constituye un riesgo para los derechos y libertades de las personas físicas.

Se considera que se tiene constancia de una brecha de seguridad cuando haya una certeza de que se ha producido y se tiene conocimiento suficiente de su naturaleza y alcance.

El criterio a tener en cuenta para determinar si un incidente ha producido una "brecha de seguridad de los datos personales" se recoge en el propio RGPD, e incluye "todas aquellas brechas de la seguridad que ocasionen la destrucción, pérdida o

alteración incidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizado a dichos datos."

La notificación de la brecha de seguridad a la autoridad de control será realizada por el Delegado de Protección de Datos, toda vez que es el punto de contacto de contacto del responsable del tratamiento con dicha autoridad.

Esta comunicación se realizará con el modelo de comunicación previsto por las autoridades de control, y deberá contener la siguiente información:

- Datos identificativos y de contacto del responsable del tratamiento y del Delegado de Protección de Datos.

- Indicación de si se trata de una notificación completa o parcial. En caso de tratarse de una notificación parcial si se trata de una primera notificación o una notificación complementaria.

- Información sobre la brecha de seguridad de datos personales.

- Fecha y hora en la que se detecta.

- Fecha y hora en la que se produce el incidente y su duración.

- Circunstancias en que se haya producido la brecha de seguridad de datos personales (por ejemplo, pérdida, robo, copia, etc.)

- Naturaleza y contenido de los datos personales en cuestión.

- Resumen del incidente que ha causado la brecha de seguridad de datos personales (con indicación de la ubicación física y del soporte de almacenamiento)

- Posibles consecuencias y efectos negativos en los/as afectados/as.

- Posibles consecuencias y efectos negativos en los/as afectados/as.

- Medidas técnicas y organizativas que se hayan adoptado por parte del responsable del tratamiento.

- Categoría de los datos afectados y número de registros afectados.

- Categoría y número de individuos afectados.

- Posibles cuestiones de carácter transfronterizo, indicando la posible necesidad de notificar a otras autoridades de control.

Modelo de registro de incidentes

Fecha de notificación	__ / __ / ____
Descripción detallada de la naturaleza de la violación	
Categoría de interesados afectados	
Cálculo aproximado de registro de datos personales afectados	
Datos de contacto del DPD	
Descripción resumida de las posibles consecuencias.	
Descripción resumida de las medidas adoptadas para poner remedio a la violación de seguridad	

Si en el momento de la notificación, no fuese posible facilitar información, podrá facilitarse posteriormente, de manera gradual en distintas fases. La primera notificación se realizará en las primeras 72h, y al menos, se realizará una comunicación final o de cierre cuando se disponga de toda la información relativa al incidente.

Cuando el/la responsable realice la primera notificación deberá informar si proporciona más información a posteriori. También podrá adoptar información adicional mediante comunicaciones intermedias a la autoridad de control bajo petición de ésta, cuando el/la responsable considere adecuado actualizar la situación de ésta.

Cuando la notificación inicial no sea posible en el plazo de 72h, la notificación deberá realizarse igualmente, y en ella deberán constar y justificarse los motivos de la dilación.

Las notificaciones deben ser claras, concisas y que incluyan la información necesaria para que puedan ser analizadas adecuadamente.

No será necesaria la notificación a la autoridad de control si el cálculo del posible riesgo obtenido en el análisis de impacto es superior a 20.

III.- Identificación de la Autoridad de control
Cuando el incidente pueda afectar a los datos de personas en más de un Estado miembro, el/la responsable debe realizar

una evaluación sobre cuál es la autoridad principal a la que se deberá realizar la notificación y, en caso de duda, se debe, como mínimo, notificar a la autoridad de control local donde la brecha ha tenido lugar. Actuará como autoridad de control principal, la del establecimiento principal o la del único establecimiento del responsable.

Los criterios para identificar el establecimiento principal son:

- Lugar donde tenga la sede principal el/la responsable.

- Lugar donde se toman las decisiones sobre fines y medios.

- Por ello, en el caso de CICCP, la autoridad de control es la Agencia Española de Protección de Datos (AEPD).

IV.- Proceso de comunicación al interesado/a afectado/a
Así mismo, el art. 34 RGPD establece que cuando sea probable que la brecha de seguridad de los datos personales entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento comunicará a los/as afectados/as sin dilación indebida.

El equipo de respuesta, con el análisis de la situación realizado, decidirá si existe tal riesgo, teniendo en cuenta diversos factores a tener en consideración para decidir si se ha de realizar las comunicaciones a las personas afectadas:

- Cuáles son las obligaciones legales y/o contractuales.

- Riesgos que comporta la pérdida de datos: daños físicos, daños reputacionales. etc.

- Existe un riesgo razonable de suplantación de identidad o fraude (en función del tipo de información que se ha visto afectada y teniendo en cuenta si la información) estaba pseudonimizada o cifrada.

- Compromiso de datos de categorías especiales contemplada en el art. 9 RGPD.

- Hasta qué punto la persona afectada puede evitar o mitigar los posibles daños posteriores.

Si después del análisis correspondiente, es necesario realizar la notificación pero se prevé que la comunicación de los/as afectados/as puede comprometer el resultado de la investigación en curso, la comunicación podría posponerse siempre bajo la supervisión de la autoridad de control. La comunicación a los/as afectados/as se realizará a la mayor brevedad posible, en un lenguaje claro y sencillo y siempre en estrecha cooperación con la autoridad de control y las autoridades policiales, de acuerdo con sus orientaciones.

Esta comunicación será firmada por el Comité de Seguridad y el Delegado de Protección de Datos.

Y contendrá, al menos, la siguiente información:

- Descripción general del incidente y momento en que se ha producido.

- Las posibles consecuencias de la brecha de seguridad de los datos personales.

- Descripción de los datos e información personal afectada.

- Resumen de las medidas implantadas hasta el momento para controlar los posibles daños.

- Otras informaciones útiles a los afectados para proteger sus datos o prevenir posibles daños.

- Datos de contacto del Delegado de Protección de Datos.

Seguimiento y cierre
El plan de actuación para la gestión de brechas de seguridad requiere de determinadas tareas de seguimiento y cierre. Entre estas tareas cabe:

I.- Valoración de contratación de un análisis pericial
El equipo de respuesta valorará y propondrá al Comité de Seguridad la contratación de un análisis pericial. En determinados casos está justificado que la investigación sea conducida por un experto perito que tendrá como misión fundamental el análisis de los hechos y la recopilación de evidencias precisas. Su intervención puede resultar de gran utilidad para evidenciar lo sucedido tanto en vía administrativa como en sede judicial.

II.- Valoración de interposición de denuncias o adopción de medidas jurídicas
Se valorará la oportunidad de interposición de denuncias o de iniciación de procedimientos judiciales a los fines de exigencias de responsabilidades o de reparación de daños

III.- Cierre de la brecha de seguridad
Una vez las acciones derivadas de los procesos de Plan de Contingencia y Respuesta hayan concluido, se considerará

que se han alcanzado los objetivos y se procederá al cierre de la brecha de seguridad.

Revisión del procedimiento
Este procedimiento será revisado anualmente por:
• El Comité de seguridad.
• Y el Delegado de Protección de Datos.

Workflow procedimiento

ANEXO H
ANÁLISIS DE LA NECESIDAD DE EVALUACIÓN DE IMPACTO

Primer nivel de análisis
Esta primera fase del análisis consiste en analizar, en primer lugar, si el tratamiento encaja en alguno de los supuestos previstos en la lista publicada por la Agencia Española de Protección de Datos (en adelante, AEPD) de los tipos de tratamiento que NO requieren una EIPD (art. 35.5 del RGPD).

En caso negativo, se verificará, en segundo lugar, si el tratamiento encaja en el listado publicado por la AEPD de los tipos de operaciones de tratamiento que SÍ requieren una EIPD (art. 35.4 RPGD).

En dichos listados se recogen los siguientes tratamientos:

Listado de tratamientos que NO requieren EIPD (art. 35.5 RGPD)
1. Tratamientos que se realizan estrictamente bajo las directrices establecidas o autorizadas con anterioridad mediante circulares o decisiones emitidas por las Autoridades de Control, en particular la AEPD, siempre y cuando el tratamiento no se haya modificado desde que fue autorizado.
2. Tratamientos que se realizan estrictamente bajo las directrices de códigos de conducta aprobados por la Comisión Europea o las Autoridades de Control, en particular la AEPD, siempre y cuando una EIPD completa haya sido realizada para la validación del código de conducta y el tratamiento se implementa incluyendo las medidas y salvaguardas definidas en la EIPD.
3. Tratamientos que sean necesarios para el cumplimiento de una obligación legal, cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable, siempre que en el mismo mandato legal no se obligue a realizar una EIPD, y siempre y cuando ya se haya realizado una EIPD completa
4. Tratamientos realizados en el ejercicio de su labor profesional por trabajadores autónomos que ejerzan de forma individual, en particular médicos, profesionales de la salud o abogados, sin perjuicio de que pueda requerirse cuando el tratamiento que lleven a cabo cumpla, de forma significativa, con dos o más criterios establecidos en la lista de tipos de tratamientos de datos que requieren evaluación de impacto relativa a protección de datos publicada por la AEPD.
5. Tratamientos obligatorios por ley y realizados con relación a la gestión interna del personal de las PYMES con finalidad de contabilidad, gestión de recursos humanos y nóminas, seguridad social y salud laboral, pero nunca relativos a los datos de los clientes.
6. Tratamientos realizados por comunidades y subcomunidades de propietarios tal como se definen en el artículo 2 (a, b y d) de la Ley 49/1960 de Propiedad Horizontal.
7. Tratamientos realizados por colegios profesionales y asociaciones sin ánimo de lucro para la gestión de los datos personales de sus propios asociados y donantes, y en el ejercicio de su labor, siempre que no incluyan en el tratamiento de datos sensibles tales como los que se establecen en el artículo 9.1 del RGPD y no sea de aplicación el artículo 9.2(d) de dicho Reglamento.

Listado de tratamientos que requieren EIPD (art. 35.4 RGPD)	CICCP
1. Tratamientos que impliquen perfilado o valoración de sujetos, incluida la recogida de datos del sujeto en múltiples ámbitos de su vida (desempeño en el trabajo, personalidad y comportamiento), que cubran varios aspectos de su personalidad o sobre sobre sus hábitos.	NO
2. Tratamientos que impliquen la toma de decisiones automatizadas o que contribuyan en gran medida a la toma de tales decisiones, incluyendo cualquier tipo de decisión que impida a un interesado el ejercicio de un derecho o el acceso a un bien o un servicio o formar parte de un contrato.	NO
3. Tratamientos que impliquen la observación, monitorización, supervisión, geolocalización o control del interesado de forma sistemática y exhaustiva, incluida la recogida de datos y metadatos a través de redes, aplicaciones o en zonas de acceso público, así como el procesamiento de identificadores únicos que permitan la identificación de usuarios de servicios de la sociedad de la información como pueden ser los servicios web, TV interactiva, aplicaciones móviles, etc.	NO
4. Tratamientos que impliquen el uso de categorías especiales de datos a las que se refiere el artículo 9.1 del RGPD, datos relativos a condenas o infracciones penales a los que se refiere el artículo 10 del RGPD o datos que permitan determinar la situación financiera o de solvencia patrimonial o deducir información sobre las personas relacionada con categorías especiales de datos.	NO
5.Tratamientos que impliquen el uso de datos biométricos con el propósito de identificar de manera única a una persona física.	NO
6. Tratamientos que impliquen el uso de datos genéticos para cualquier fin.	NO
7. Tratamientos que impliquen el uso de datos a gran escala. Para determinar si un tratamiento se puede considerar a gran escala se considerarán los criterios establecidos en la guía WP243 “Directrices sobre los delegados de protección de datos (DPD)” del Grupo de Trabajo del Artículo 29.	NO
8. Tratamientos que impliquen la asociación, combinación o enlace de registros de bases de datos de dos o más tratamientos con finalidades diferentes o por responsables distintos.	NO
9. Tratamientos de datos de sujetos vulnerables o en riesgo de exclusión social, incluyendo datos de menores de 14 años, mayores con algún grado de discapacidad, discapacitados, personas que acceden a servicios sociales y víctimas de violencia de género, así como sus descendientes y personas que estén bajo su guardia y custodia.	NO
10. Tratamientos que impliquen la utilización de nuevas tecnologías o un uso innovador de tecnologías consolidadas, incluyendo la utilización de tecnologías a una nueva escala, con un nuevo objetivo o combinadas con otras, de forma que suponga nuevas formas de recogida y utilización de datos con riesgo para los derechos y libertades de las personas.	NO
11. Tratamientos de datos que impidan a los interesados ejercer sus derechos, utilizar un servicio o ejecutar un contrato, como por ejemplo tratamientos en los que los datos han sido recopilados por un responsable distinto al que los va a tratar y aplica alguna de las excepciones sobre la información que debe proporcionarse a los interesados según el artículo 14.5 (b,c,d) del RGPD.	NO

De acuerdo al criterio establecido por la AEPD, “será necesario realizar una EIPD en la mayoría de los casos en los que dicho tratamiento cumpla con dos o más criterios de la lista expuesta a continuación, salvo que el tratamiento se encuentre en la lista de tratamientos que no requieren EIPD a la que se refiere en artículo 35.5 del RGPD. Cuantos más criterios reúna el tratamiento en cuestión, mayor será el riesgo que entrañe dicho tratamiento y mayor será la certeza de la necesidad de realizar una EIPD”.

Por lo expuesto, se concluye que de este primer nivel de análisis no cabe considerar que CICCP tenga obligación de realizar EIPD sobre los tratamientos que lleva a cabo a la fecha de elaboración/revisión de este informe.

Segundo nivel de análisis

El segundo nivel de análisis consiste en verificar si el tratamiento está incluido en los supuestos previstos en el art. 35.3 del RGPD:

• evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones con efectos jurídicos para las personas físicas;

• tratamiento a gran escala de categorías especiales de datos o de datos relativos a condenas e infracciones penales;

• observación sistemática a gran escala de una zona de acceso público.

Como base para realizar esta fase del análisis, partimos de la respuesta de CICCP al cuestionario siguiente:

Elementos a analizar	SÍ	NO
¿Las operaciones de tratamiento implican una evaluación sistemática y amplia de aspectos personales relativa a personas físicas?		X
¿Con las operaciones de tratamiento, se pueden determinar hábitos, comportamientos, preferencias, gustos, intereses, etc. de personas identificadas o identificables?		X
A todos los efectos, ¿podemos considerar que una de las finalidades del tratamiento es elaborar perfiles personales o predecir comportamientos?		X
A partir del tratamiento de los datos, ¿se toman decisiones con efectos jurídicos para las personas afectadas?		X
A partir del tratamiento de los datos, ¿se toman decisiones que pueden afectar significativamente o perjudicar de alguna manera las personas afectadas?		X
¿Se tratan datos a gran escala de alguna categoría especial?		X
¿Se tratan datos relativos a condenas o infracciones penales?		X
¿El tratamiento implica un control sistemático, monitorización o supervisión a gran escala de áreas de acceso público?		X

Siendo negativa la respuesta a las cuestiones planteadas, podemos concluir que los tratamientos de datos llevados a cabo por CICCP no encajan en los supuestos previstos en el art. 35.3 del RGPD.

Tercer nivel de análisis

Para llevar a cabo esta fase del análisis deben considerarse los criterios para detectar el alto riesgo que propone el GT 29 en el WP 248, para lo cual partimos de las respuestas de CICCP a las cuestiones siguientes:

Existencia de factores de riesgo (criterios del WP 248)	SÍ	NO
¿El tratamiento implica la evaluación o puntuación de personas?		X
¿El tratamiento implica elaborar perfiles de personas o hacer predicciones sobre su comportamiento?		X
¿La finalidad del tratamiento es tomar decisiones de manera automatizada, que puedan tener efectos jurídicos?		X
¿La finalidad del tratamiento es tomar decisiones de manera automatizada, que puedan tener efectos similares a los jurídicos, o efectos significativos para las personas?		X
¿El tratamiento implica algún tipo de vigilancia sistemática? (observación, supervisión y control de personas)		X
¿Se tratan categorías especiales de datos?		X*
¿Se tratan datos relativos a condenas o infracciones penales?		X
¿Se traten datos que es puedan considerarse como muy personales?		X
¿Se tratan datos a gran escala?		X
¿El tratamiento implica combinar diferentes fuentes de información o datos relacionados con tratamientos diversos?		X
¿Se tratan datos relativos a personas en situación de vulneración o de desequilibrio respecto del responsable del tratamiento?		X
¿Se tratan datos de niños? (personas menores de 18 años)		X
¿Las operaciones de tratamiento utilizan o aplican soluciones tecnológicas u organizativas de forma innovadora?		X
¿El tratamiento puede impedir a las personas afectadas utilizar un servicio o ejecutar un contrato?		X

Teniendo en cuenta que todas las respuestas obtenidas a las cuestiones planteadas han sido negativas, cabe concluir que aplicando los criterios para detectar el alto riesgo que propone el GT 29 en el WP 248, los tratamientos de la organización no entrañan un alto riesgo para los derechos y libertades de las personas físicas.

Conclusión
Sobre la base de la información obtenida relativa a las operaciones de tratamiento existentes en CICCP, se concluye que NO requieren la realización de Evaluación de Impacto relativa a la Protección de Datos, al no entrañar un alto riesgo para los derechos y libertades de las personas físicas.

Esta conclusión deberá revisarse en el caso de que CICCP proyecte iniciar un nuevo tratamiento que pueda entrañar alto riesgo.