



**PLIEGO DE PRESCRIPCIONES TÉCNICAS PARA LA
CONTRATACIÓN DEL SERVICIO DE CONTROL Y GES-
TIÓN DOCUMENTAL EN MATERIA DE PREVENCIÓN
DE EMPRESAS CONTRATISTAS Y SUBCONTRATIS-
TAS DE CANAL DE ISABEL II S.A.**

Contrato N.º 18/2018

FECHA: 16/07/2018

INDICE

1. OBJETIVOS DEL CONTRATO

2. CARACTERÍSTICAS DE LOS SERVICIOS

2.1 Alcance del contrato.

2.2 Ámbito temporal.

3. CONDICIONES DE LOS SERVICIOS

3.1 Documentación general del contrato a revisar, controlar y archivar.

3.2 Documentación específica de prevención de riesgos laborales del contrato a revisar, controlar y archivar.

3.3 Documentación específica de prevención de riesgos laborales de trabajadores.

3.4 Documentación específica de maquinaria.

3.5 Requisitos funcionales

3.6 Requisitos técnicos y seguridad

3.7 Requisitos proveedor

3.8 Obligaciones del adjudicatario.

4. SEGUIMIENTO DEL CONTRATO

5. FACTURACIÓN

1. OBJETIVOS DEL CONTRATO.

El objeto de este contrato es la prestación del servicio de control y gestión de documentación legal y de Prevención de Riesgos Laborales de empresas contratistas y subcontratistas que Canal de Isabel II S.A. considere oportunos, en las condiciones establecidas en los pliegos del presente procedimiento de licitación.

2. CARACTERÍSTICAS DEL CONTRATO.

2.1 ALCANCE DEL CONTRATO.

El alcance debe cubrir los requisitos exigidos por la legalidad vigente en cuanto a la documentación a presentar por las empresas contratistas y subcontratistas desde el inicio de los trabajos a realizar para Canal de Isabel II S.A. hasta la finalización de los mismos.

2.2 ÁMBITO TEMPORAL.

El periodo de prestación de las actividades será de tres años a contar desde la firma del contrato.

3. CONDICIONES DEL CONTRATO.

En los siguientes apartados se desarrollan las características y estructura del objeto del contrato, que tendrán la consideración de requisitos mínimos del mismo y que serán parametrizados en función del tipo de contrato para cada expediente, debiendo ser respetados por las ofertas técnicas de los licitadores, que podrán ofertar elementos adicionales y compatibles a dichos requisitos mínimos. Los requisitos mínimos siempre deberán ser ofertados.

En el supuesto de que la oferta de algún licitador no contemple los requisitos mínimos y estructura descritos en el apartado 3.1, 3.2, 3.3, 3.4 y 3.5 su oferta no será tomada en cuenta en el presente procedimiento de licitación.

3.1 DOCUMENTACIÓN GENERAL DEL CONTRATO A CONTROLAR Y ARCHIVAR.

EMPRESA CONTRATISTA - SUBCONTRATISTAS

- Situación de cotización a la Seguridad Social de las empresas contratistas.
- Certificados de estar al corriente de pago con la Agencia Tributaria.
- Coberturas de las pólizas de responsabilidad Civil.
- DCL y RNT (TC1 y TC2)
- REA.
- RERA.
- Certificados de modalidades del Servicio de Prevención.

3.2 DOCUMENTACIÓN ESPECÍFICA DE PREVENCIÓN DE RIESGOS LABORALES DEL CONTRATO A CONTROLAR Y ARCHIVAR.

EMPRESA CONTRATISTA

- Evaluaciones de riesgos y Planificación de actividad preventiva.
- Plan de emergencia/ Plan de Autoprotección.
- Nombramiento de Consejero de Seguridad.
- Nombramiento de Coordinador de Seguridad.
- Copia del Libro de Subcontratación.
- Apertura de Centro de Trabajo
- Acta de reuniones de Coordinación.
- Documentos de Calidad de Canal de Isabel II (Cuestionario de evaluación de contratistas, Cartas de entrega y solicitud de documentación, acreditación de trabajadores y la información de riesgos).
- Listado de trabajadores especificando las autorizaciones necesarias para la realización de las tareas o funciones de su puesto de trabajo.
- Listado de Recursos Preventivos.
- Libro de Incidencias.

EMPRESAS SUBCONTRATISTAS

- Evaluación de riesgos o adhesión a la de la contrata principal.
- Listado de trabajadores especificando las autorizaciones necesarias para la realización de las tareas de su puesto de trabajo.

3.3 DOCUMENTACIÓN ESPECÍFICA DE PREVENCIÓN DE RIESGOS LABORALES DE TRABAJADORES.

- Documentación de cada trabajador
 - Apto médico.
 - Certificados de Formación.
 - Certificados de Información.
 - Entrega de equipos de protección individual.
 - Certificados de trabajadores cualificados o autorizados para trabajos de especial riesgo (eléctricos,...)
 - Jefe riesgo eléctrico.
 - Nombramientos de Recurso Preventivo.
 - Espacios confinados.
 - Formación en Montaje de Andamios.
 - Uso de Puentes Grúa.
 - Plataformas Elevadoras.
 - Trabajos en Altura/Verticales.
 - Actividades subacuáticas.
 - Manipulación Productos Fitosanitarios.
 - Atmósferas Explosivas (ATEX).
 - Vigilante Armado.

- Manipulación de Productos Químicos.
- Autorización para uso de maquinaria.

3.4 DOCUMENTACIÓN ESPECÍFICA DE MAQUINARIA.

- Listado de maquinaria y debiendo aportar:
 - Documentación de conformidad
 - Libro de mantenimiento de revisiones
 - ITV
 - Manual de Instrucciones
 - Seguro de la máquina.
 - Otra documentación.

3.5 REQUISITOS FUNCIONALES.

- Permitir la carga de documentación de PRL por parte de Empresas Contratistas (propia y de las subcontratas a su cargo)
- Permitir la separación de documentación por tipología:
 - Datos identificativos de cada empresa/contrato (expediente).
 - Documentación del expediente.
 - Documentación de los trabajadores.
 - Documentación de la maquinaria.
- Se debe diseñar un sistema claro, que permita saber con una primera pantalla de visualización en la herramienta, si la situación general de un contrato es de cumplimiento total o no, y en este caso, conocer de inmediato las causas del incumplimiento.
- Establecer niveles de jerarquía de acceso a la documentación:
 - Cada área del Canal solo podrá visualizar los contratos de su responsabilidad.
 - Cada contratista deberá visualizar sólo los expedientes, empleados, maquinaria y documentación a su cargo.
 - Creación de un entorno de acceso independiente para coordinadores de Seguridad y Salud.
- Fijación clara de la unidad operativa responsable de cada contrato.
- Establecer una lista de tipos de documentos posibles que aplican a las entidades del sistema, y que debe ser parametrizable, permitiendo la inclusión de nuevos tipos de documentos, si así se requiere.
- El sistema dispondrá de la información de riesgos de las diferentes instalaciones, la cual proporcionará Canal de Isabel I S.A. previamente a dicha plataforma, de forma que se permita la descarga de forma automática por las empresas responsables de mencionado contrato.

- Identificación clara de todas las personas que cargan la documentación en la aplicación de cada contratista o subcontratista, así como direcciones de correos y teléfonos para poder contactar con ellos.
- Al dar de alta un contrato debe permitir seleccionar la documentación que aplica al expediente, para que así se muestre tanto en pantalla como en los informes.
- Poder asociar a cada tipo de documento una fecha de carga y una fecha de caducidad del mismo, acorde a su tipología.
- Permitir fijar una fecha de inicio y final para la duración del contrato y sus posibles prórrogas.
- Disponer de un sistema de identificación del estado de la documentación por colores o semáforos, de manera individualizada para cada bloque, y para cada uno de los documentos que integran los mismos, el estado de la documentación:
 - Verde (correcto): está todo correcto.
 - Ámbar (pendiente de validación): la empresa está validando la documentación.
 - Rojo (incorrecto): la documentación está incompleta o ha caducado
 - Campo "Observaciones" para poder incluir comentarios durante la validación o rechazo de la misma.

Si un contratista o subcontratista, tiene documentos pendientes de validar en alguno de los bloques, su situación debe de ser pendiente, y señalizarse como tal, hasta que el adjudicatario no valide de forma positiva o negativa la documentación objeto de validación, pero manteniendo la situación de pendiente sólo en ese bloque, sin que dicha situación afecte al resto de la documentación.

- Visualización, filtro y acceso directo por parte de las Contratas a la documentación que no está correcta, sin necesidad de tener que acceder a cada uno de los bloques para comprobar la documentación pendiente aportada.
- En el caso de documentación errónea, se deben mostrar los motivos por los que se ha rechazado, para facilitar su identificación.
- Permitir el envío de notificaciones automáticas vía email a empresas contratistas:
 - Cada 15 - 30 días antes de que la documentación vaya a caducar.
 - En el momento en que caduque.
 - Posteriormente recordatorios semanales de la documentación que tienen caducada hasta que se actualice.
- Funcionalidad para remitir, de forma automática, información a las contratas, coordinadores de seguridad y salud y responsables del contrato de Canal de Isabel II S.A. con los documentos que incumplen. Deberá figurar el número de contrato, el nombre de la empresa contratista y el Área responsable del mismo. En dicho informe no deben aparecer los contratos cuya documentación esté correcta o actualizada.
- Funcionalidad para remitir, de forma automática, información a las contratas y coordinadores de seguridad y salud con los documentos próximos a caducar, además de figurar el número de contrato, el nombre de la empresa contratista y el Área responsable del mismo. Deberá permitir seleccionar el intervalo de días con el que se quieren notificar los documentos próximos a caducar.

- La plataforma tiene que permitir migrar trabajadores, documentación asociada y el estado de la misma de un contrato a otro (Subrogación de personal).
Cuando una contrata principal sea adjudicataria de dos o más contratos diferentes, la documentación correspondiente a la empresa y trabajadores se podrá reutilizar y extrapolar a los restantes contratos, evitando al contratista tener que cargar los datos en la aplicación varias veces.
- El sistema repercutirá en el “el control de acceso” a las instalaciones de Canal de Isabel II S.A. en relación a la situación de su documentación; de forma que en el caso de que la documentación de aquel personal que vaya a ejecutar trabajos en la instalación no esté actualizada/completa en la plataforma, no se permitida el acceso a la misma.
- Permitir dar de baja empresas, y que no aparezcan en pantalla, pero permanecerá accesible para determinados perfiles.
- Dispondrá de un generador de informes para editarlos con los campos y la periodicidad que se consideren oportunos como pueden ser: la documentación pendiente por expediente o por trabajador, listado de documentos caducados por expediente, unidades operativas, listado de números de accesos con fecha y hora por expediente. Los listados se deben exportar en formato Excel.
Los informes Excel deberán contemplar todos los campos incluidos en la base de datos, contemplándose la posibilidad de incrementar/modificar los campos, acorde a la evolución de las necesidades de Canal de Isabel II S.A.
- Generar gráficos e informes que permitan, tanto a usuarios externos como internos, conocer el estado de la documentación del contrato, aplicando los filtros que se consideren necesarios.
- El proceso de extracción de informes deber incluir filtros configurables.
- Dispondrá de un sistema de búsqueda avanzado: que permita buscar por múltiples campos y entidades (expedientes, empleados, empresas,...). Los filtros para búsquedas deben ser parametrizables. No se requiere búsqueda por contenido del documento.
- El comportamiento del botón de retroceso será volver a la pantalla anterior y no a la de inicio.

3.6 REQUISITOS TÉCNICOS Y SEGURIDAD.

- Visualización directa de documentos en pantalla (sin necesidad de descargarlos)
- Tipo de documento a gestionar: PDF; pudiendo cargar varios archivos en un mismo apartado, sin que implique la anulación del anterior.
- Capacidad para gestionar un mínimo de 1000 empresas (entre contratas y subcontratas) y 10.000 trabajadores.
- Capacidad para gestionar un rango de 135.000 – 150.000 documentos.
- Capacidad para gestionar la carga de documentos pesados (>3 Mb)

- El Área de Prevención deberá tener la posibilidad a nuevos contratos sin pasar por el administrador del programa.
- El acceso desde dispositivos móviles es suficiente con que sea vía Web.
- Se podrá contemplar la posibilidad de desarrollar una APP móvil.
- Se evaluará que presente un diseño "responsive" (este tipo de diseño permite su visualización web correcta en distintos dispositivos).
- Acceso a diferentes vistas dependiendo del perfil y permisos del usuario.
- La plataforma tiene que ser rápida, ágil, sencilla de utilizar y visualmente funcional.
- La plataforma debe disponer de una Guía de Ayuda o Manual de Usuario accesible para todas las contratas y restantes usuarios de la aplicación.
- Localización geográfica de los servidores dentro del Espacio Económico Europeo (EEE).
- Certificación del servicio en la norma ISO/IEC 27001 (gestión de seguridad de la información).
- Almacenamiento de traza con IP origen, contexto URL accedido, usuario, fecha de todos los accesos a la herramienta (no es necesario que incluya registro de las acciones que ha realizado dentro de la plataforma).
- Certificado en BS25999 o ISO22301 (gestión de sistema para evitar incidentes que causen interrupción de la actividad).
- La comunicación debe tener la seguridad para que la comunicación se realice bajo un protocolo robusto (p.e. TLS1.2) y haciendo uso de suites de cifrado seguras que eviten vulnerabilidades de tipo Logjam.
- El licitador deberá proporcionar el resultado de la última auditoría de seguridad independiente por parte de terceros del servicio o servicios contratados por Canal de Isabel II, S.A., vulnerabilidades encontradas y estado el plan de acción identificado y definido para la resolución de las mismas.
- El licitador deberá, al menos:
 - ✓ Proporcionar una relación de las medidas de seguridad físicas implementadas en sus instalaciones (control de acceso a las instalaciones, a los CPDs, etc.).
 - ✓ Proporcionar una relación de las medidas de seguridad multi-cliente (multi-tenant) implementadas, dado que el compartir recursos y servicios entre múltiples clientes (entre ellos, Canal de Isabel II, S.A.) obliga a garantizar una segregación física y/o lógica eficiente, y la implementación de controles que aseguren que un cliente, deliberada o inadvertidamente, interfiera en la confidencialidad, integridad y disponibilidad de la información propiedad de otros.

- ✓ Proporcionar una relación de los procedimientos de monitorización, alerta y reporting establecidos, incluyendo los de los análisis de incidentes de seguridad y de los análisis forenses.
- ✓ Proporcionar una relación de los procedimientos de bastionado y securización, tanto de la arquitectura de la infraestructura tecnológica como de servidores, comunicaciones, aplicaciones y servicios.
- ✓ Proporcionar información sobre el nivel de protección y exposición de los sistemas no productivos (desarrollo, test, calidad, formación, etc.) y de la información que contienen y gestionan (por ejemplo, protección de datos reales en entornos no productivos, disociación de datos reales, ofuscación de datos reales, etc.).
- ✓ Garantizar con evidencias que existen y se aplican procedimientos para la reversión del servicio a los clientes, la devolución en el mínimo tiempo posible de la información propiedad de los clientes a los mismos en un formato tratable por ellos y la garantía de acceso a la información devuelta.
- ✓ Garantizar con evidencias que existen y se aplican procedimientos para el borrado seguro certificado (y características del mismo) de la información de los clientes una vez se haya revertido el servicio, una vez haya sido accedida la información y verificada en su totalidad por el Responsable del Tratamiento y/o Dueño de los Datos tanto la completitud como la corrección de los datos devueltos, y una vez finalizada la prestación contractual.
- ✓ Garantizar que todo acceso al servicio se produce exclusivamente bajo protocolos que cifren de forma robusta los datos transmitidos entre el cliente y el servidor, con el objeto de garantizar su confidencialidad e integridad (por ejemplo, uso exclusivo de TLS 1.2 y utilizando sólo suites de cifrado robustas para evitar vulnerabilidades de tipo BEAST (RC4), Lucky13 (RC4), POODLE (SSL 3.0 y TLS 1.0), CRIME (TLS 1.0 compression), SWEET32 (3DES), Logjam (intercambio de claves de menos de 2048 en DH), DROWN (TLS 1.x con soporte a SSLv2), etc.).
- ✓ Garantizar el uso de un esquema de BBDD propio para la información propiedad de Canal de Isabel II, S.A., y que dicho esquema de BBDD sea accedido única y exclusivamente por el/los usuarios de aplicación que vayan a ser utilizados en la conexión del servicio Cloud a dicho esquema de BBDD.
- ✓ Garantizar el cifrado robusto de los datos propiedad de Canal de Isabel II, S.A. en la propia BBDD y modelo (cifrado completo o cifrado del dato).
- ✓ Garantizar que el almacenamiento de los datos de autenticación de los usuarios (por ejemplo, el par usuario/contraseña) en la BBDD mediante el uso de funciones resumen (hash) robustas (al menos, SHA-256) conjuntamente con la obligación de utilizar contraseñas complejas (longitud mínima de 10 caracteres, con obligatoriedad de utilizar caracteres alfanuméricos (mezcla de mayúsculas, minúsculas y números) y no alfanuméricos (por ejemplo, signos de puntuación y ortográficos)). Es obligatorio el uso de funciones de derivación de claves basadas en contraseña (Password-Based Key Derivation Functions) para el almacenamiento de las contraseñas (por ejemplo, PBKDF2).
- ✓ Garantizar que existe la posibilidad de uso de:
 - ❖ Un esquema XML para el intercambio de datos de autenticación y autorización (por ejemplo, SAML 2.0) e implementaciones de seguridad a nivel del mensaje.

- ❖ OAuth 2.0 u OpenID Connect como modelos de autorización segura para consumo de servicios web.
 - ❖ SCIM como modelo para automatizar el intercambio de información de identidad de los usuarios entre distintos dominios de identidad.
 - ✓ Garantizar que exista la posibilidad de habilitar un segundo factor de autenticación (2FA) mediante el uso de certificados electrónicos reconocidos (como, por ejemplo, DNle), certificados electrónicos reconocidos, contraseñas de un único uso (OTP), soft-tokens, etc.
 - ✓ Garantizar que todas las funciones de la aplicación relacionadas con la autenticación, la gestión de las sesiones y la autorización (control del acceso) han sido auditadas contra estándares de seguridad internacionalmente reconocidos (por ejemplo, OWASP) para comprobar que existen y que han sido implementadas correctamente.
 - ✓ Se comunicará inmediatamente a Canal de Isabel II, S.A. acerca de todas aquellas vulnerabilidades reportadas de forma privada o hechas públicas que afecten a sus sistemas y de las acciones que están siendo llevadas a cabo para eliminar o mitigar dichas vulnerabilidades
- La documentación deberá archiversse durante un periodo mínimo de 6 años.
 - La plataforma debe contemplar la migración de los datos desde el sistema actual que utiliza Canal de Isabel II.
 - Los accesos deben estar condicionados en base al perfil y permisos de usuario.
 - El Sistema debe disponer de la seguridad necesaria para que toda la información y acceso a la plataforma, alojamiento, revisión del servicio y control de indisponibilidades no cause ningún perjuicio a Canal de Isabel II S.A. debiendo cumplir con todas las medidas.

3.7 REQUISITOS PROVEEDOR.

- Soporte técnico ofrecido en español.
- La solución debe permitir contemplar pequeños evolutivos y adaptaciones a nuevas normativas legales, o bien que sea parametrizable por el usuario.
- Disponibilidad: 99,5%.
- Permite la realización de Backups diarios (24 h.).
- Disponer de un SLA para atención de incidencias.
- Resolución de incendias en 48 horas y notificación de las mismas al usuario.

3.8 OBLIGACIONES DEL ADJUDICATARIO.

El adjudicatario deberá solicitar en cada expediente la documentación parametrizada según el tipo de contrato de las indicadas de los apartados 3.1, 3.2, 3.3 y 3.4 a las empresas y verificarla una vez cargada en un plazo máximo de 48 horas, confirmando su validez o en caso contrario indicando un breve comentario para su subsanación. Toda la documentación deberá ser archivada y mantenerse actualizada.

Toda esta documentación será puesta a disposición de Canal de Isabel II S.A. a través de una base de datos de internet, de acceso exclusivo para los usuarios autorizados que dispondrán de una clave de acceso personalizada. La documentación de las subcontratas se incluirán con la del contratista principal del expediente.

Quincenalmente se enviará un email indicando la documentación que tenga pendiente cada expediente a las personas responsable Canal de Isabel II y de la empresa Contratista.

La empresa adjudicataria del contrato se compromete a traspasar la documentación de las empresas contratistas y subcontratistas existentes actualmente en la base de datos del actual adjudicatario de Canal de Isabel II SA a su base de datos en el plazo máximo de 15 días.

La documentación de empresas contratistas incorporada por el adjudicatario en la herramienta Web es propiedad del Canal de Isabel II S.A. debiendo ser devuelta al mismo en caso de rescisión o finalización del contrato.

En cuanto a legislación de protección de datos, el adjudicatario deberá cumplir con lo establecido en el PCAP.

Los datos de carácter personal facilitados por los licitadores serán incluidos en los ficheros de Canal de Isabel II, S.A. con la finalidad de gestionar el objeto del presente procedimiento y a efectos de adjudicación y seguimiento del mismo y de futuros procesos de licitación en los que pudieran participar. Los licitadores deberán contar con los consentimientos necesarios para facilitar datos de terceros a Canal de Isabel II, S.A. Pueden acceder, rectificar, oponerse o cancelar sus datos en la dirección social de Canal de Isabel II, S.A. con la referencia LOPD. Toda la información que se entregue al adjudicatario para la ejecución del contrato tendrá el carácter de confidencial.

El adjudicatario queda expresamente obligado a mantener absoluta confidencialidad y reserva sobre cualquier dato que pudiera conocer o le fuesen facilitados con ocasión del cumplimiento o realización de este Contrato, especialmente los de carácter personal o empresarial, que no podrá copiar o utilizar con fin distinto al que figura en este Contrato, ni tampoco ceder a otros ni siquiera a efectos de conservación. La obligación de preservar la confidencialidad rige durante el desarrollo del Contrato y con posterioridad al mismo. El adjudicatario sólo podrá revelar la información confidencial a sus empleados, con la finalidad de realizar el trabajo objeto de este Contrato y será responsable de los actos de los mismos. Canal de Isabel II, S.A. tendrá derecho a exigir en cualquier momento que la información confidencial y todas las copias, proporcionadas o accedidas por el adjudicatario, sean devueltas o destruidas dando prueba de

ello, ya sea antes, durante o después de la celebración de este Contrato. La devolución o destrucción de la información no eximirá al adjudicatario del cumplimiento de confidencialidad aquí reflejado.

El adjudicatario se obliga a indemnizar a Canal de Isabel II, S.A. por cualesquiera daños y perjuicios que sufra directamente, o por toda reclamación, acción o procedimiento, que traiga su causa de un incumplimiento o cumplimiento defectuoso por parte del adjudicatario de lo dispuesto tanto en el Contrato, esté o no vigente, como en lo dispuesto en la normativa reguladora de protección de datos de carácter personal.

El adjudicatario queda, igualmente, obligado al cumplimiento de lo dispuesto en las leyes vigentes sobre protección de datos de carácter personal, en particular a lo recogido en:

- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD).
- Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica de protección de datos de carácter personal (RLOPD).

Las obligaciones de confidencialidad establecidas en el Contrato son de carácter indefinido. En el supuesto de que para efectuar la prestación objeto del Contrato, el adjudicatario tuviera que acceder a datos de carácter personal de cuyo tratamiento sea responsable Canal de Isabel II, S.A., aquél tendrá la consideración de encargado del tratamiento. En este supuesto, el acceso a esos datos por parte del adjudicatario no se considerará comunicación de datos, sino acceso a datos por cuenta de terceros.

Los productos de software que pudieran ser destinados al tratamiento y documentación de datos de carácter personal deberán incluir en su descripción técnica el nivel de seguridad básico, medio o alto, que permitan alcanzar de acuerdo con lo establecido en el título VIII del RLOPD, debiendo incluir la descripción técnica en la oferta. Los productos de software, en cualquier caso, deberán permitir el cumplimiento del nivel de seguridad en función del tratamiento de datos a realizar o acceso de datos que se pudiera producir y la tipología de datos. La duración del encargo del tratamiento estará vinculada a la duración del Contrato. El adjudicatario actuará en el tratamiento de los datos únicamente de conformidad con las instrucciones que le señale Canal de Isabel II, S.A.

En caso de que el adjudicatario destine los datos a otra finalidad, los comunique, los utilice incumpliendo las estipulaciones del Contrato o bien, la normativa objeto de aplicación, así como cuando no adopte las medidas correspondientes para el almacenamiento y custodia de los mismos, será considerado también responsable del tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente.

A tal efecto, el adjudicatario responderá directamente frente al órgano sancionador y/o frente a Canal de Isabel II, S.A. y/o terceros de las consecuencias que se deriven del incumplimiento o cumplimiento defectuoso por parte del adjudicatario de lo dispuesto en la presente cláusula, así como en lo dispuesto en la normativa reguladora de protección de datos de carácter personal, exonerando a Canal de Isabel II, S.A. de cualquier responsabilidad.

El adjudicatario deberá aplicar, en función de la tipología de los datos de carácter personal que pudiera en su caso tratar y/o acceder, de conformidad con lo establecido en el artículo 81 del RLOPD e incorporar en su documento de seguridad, las medidas de seguridad que resulten de aplicación en virtud de la naturaleza de los datos tratados, que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural. A estos efectos, se relacionan las medidas de seguridad de nivel básico que resultan de aplicación:

NIVEL BÁSICO

- Documento de seguridad. Art. 88 RLOPD
- Funciones y obligaciones del Personal. Art. 89 RLOPD
- Registro de incidencias. Art. 90 RLOPD
- Control de acceso. Art. 91 RLOPD
- Gestión de soportes y documentos. Art. 92 RLOPD
- Identificación y autenticación. Art. 93 RLOPD
- Copias de respaldo y recuperación. Art. 94 RLOPD

El adjudicatario, en su caso, deberá aplicar las medidas técnicas y organizativas que garanticen el registro y la auditoría de las operaciones de tratamiento de datos de carácter personal.

Sin perjuicio de lo anterior, Canal de Isabel II, S.A. podrá imponer al adjudicatario la implantación de medidas de seguridad adicionales a las exigidas por la normativa de protección de datos. Si los datos personales tratados se almacenasen por el adjudicatario en dispositivos portátiles o se tratasen fuera de los locales de Canal de Isabel II, S.A., será preciso que exista una autorización previa escrita de Canal de Isabel II, S.A. y, en todo caso, deberá garantizarse como mínimo el nivel de seguridad correspondiente al tipo de fichero tratado.

El tratamiento y/o acceso a datos de carácter personal que en su caso pudiera realizar el adjudicatario y, en su caso, las personas subcontratadas por el adjudicatario (si este ha sido autorizado), deberá efectuarse en el Espacio Económico Europeo.

En el supuesto que el adjudicatario, a través de sistemas de información, accediera a datos de carácter personal de Canal de Isabel II, S.A. de forma remota, se prohíbe la incorporación de los datos de carácter personal a sistemas o soportes distintos de los autorizados expresamente por Canal de Isabel II, S.A., quien estará facultado para instruir al adjudicatario del modo y de las medidas de seguridad que se deberán implantar para ejecutar los accesos remotos a los propios recursos de Canal de Isabel II, S.A. en caso de que existieren.

El adjudicatario deberá notificar a Canal de Isabel II, S.A. cualquier indicio o situación que pudiera suponer violaciones de seguridad de los datos de carácter personal. El adjudicatario y, en su caso, las personas con las que subcontrate si ha sido debidamente autorizado, deberán tener los registros oportunos para verificar los fallos de seguridad, mantener actualizados los registros de incidencias, impedir un nuevo fallo o violación de seguridad, etc. En cualquier caso, el adjudicatario y, en su caso, las personas con las que este subcontrate (si hubiera sido debidamente autorizado), implementarán inmediatamente las medidas de seguridad correspondientes para impedir un nuevo fallo o violación de seguridad, respondiendo de las consecuencias que pudieran ocasionar en caso de incumplimiento de estas medidas.

Canal de Isabel II, S.A. tendrá derecho a obtener del adjudicatario en un plazo de 24 horas información relativa a dónde, cómo, cuándo y quién ha tratado, alojado, procesado o accedido a los datos de carácter personal y las condiciones de seguridad en que se han producido esos accesos o tratamientos.

Cuando finalice la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos a Canal de Isabel II, S.A., o al encargado de tratamiento que éste en su caso, hubiese designado. En caso de resultar de aplicación, el adjudicatario conservará debidamente bloqueados los datos en tanto pudieran derivarse responsabilidades de su relación con Canal de Isabel II, S.A. En cualquier caso, el adjudicatario y, en su caso, las personas que subcontrate (si este ha sido autorizado), deberán garantizar que son capaces de efectuar una supresión segura irreversible de los datos de carácter personal en función de estándares de seguridad. El adjudicatario no podrá subcontratar la totalidad o parte del tratamiento de los datos que deba efectuarse en cumplimiento del Contrato salvo autorización expresa y escrita de Canal de Isabel II, S.A.

El adjudicatario deberá garantizar únicamente el acceso a los soportes que contienen datos de carácter personal al personal que estuviera autorizado al efecto en sus respectivos documentos de seguridad. El adjudicatario y su personal guardarán secreto profesional sobre toda la información, documentos o datos a los que tenga acceso o de los que tengan conocimiento con ocasión de la ejecución del servicio, incluso después de finalizar el mismo, obligándose a no hacer pública cualquier información o datos que hubieran podido obtener y/o acceder durante la duración del contrato.

Será responsabilidad exclusiva del adjudicatario el comunicar a su personal, por cualquier medio de prueba admisible en derecho, las obligaciones y prohibiciones establecidas en la presente cláusula, incluido el deber de confidencialidad. Además, el adjudicatario garantizará que ha informado debidamente a los titulares (empleados del adjudicatario o de los terceros con los que el adjudicatario, en su caso, subcontrate si hubiera sido autorizado) de los datos de carácter personal que se hayan generado como consecuencia de los registros de las operaciones del servicio que se hayan encomendado, de la posibilidad de que sean utilizados por Canal de Isabel II, S.A. para un adecuado control del cumplimiento de la normativa de protección de datos (por ejemplo, registros de accesos, auditorías, etc.) y de seguridad.

El adjudicatario deberá implantar medidas que aseguren el cumplimiento de las obligaciones de confidencialidad e integridad de los datos, la obligación de que los mismos no van a ser utilizados para fines distintos del contratado, así como cualquier otra medida que se vaya a adoptar para el cumplimiento efectivo de los principios de protección de datos, debiendo aportar pruebas documentales. En este sentido, Canal de Isabel II, S.A. directamente o a través de tercero designado al efecto, podrá realizar controles para verificar el cumplimiento de las mismas, pudiendo ordenar, en su caso, la adopción de mecanismos que garanticen la confidencialidad y la integridad de los datos del servicio contratado.

El adjudicatario y, en su caso, los terceros con los que pudiera subcontratar (si hubiera sido debidamente autorizado), deberán realizar auditorías por empresa externa especialista en seguridad informática para verificar el cumplimiento de la normativa y de las medidas de seguridad para el tratamiento, acceso, encargo relativo a los datos y entregar en su caso, una copia del resultado de las auditorías y/o controles.

Sin perjuicio de las obligaciones indicadas anteriormente, a partir del 25 de mayo de 2018, el adjudicatario tendrá, asimismo, que atender las obligaciones derivadas de la aplicación del Reglamento 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 (en adelante, RGPD), y en concreto:

Canal de Isabel II, S.A. pondrá a disposición del adjudicatario algunos datos de carácter personal relativos al personal de las empresas contratistas que pueden prestar servicios en las instalaciones y/o locales de Canal de Isabel II, S.A.

El adjudicatario únicamente tratará los datos de carácter personal para la prestación de lo contratado. El tratamiento de los datos se realizará siguiendo las instrucciones documentadas de Canal de Isabel II, S.A. que este podrá poner a disposición del adjudicatario a partir del 25 de mayo de 2018, y en cualquier caso las dispuestas en este documento que serán consideradas como obligaciones de mínimo aplicables. En caso de aplicar, los productos de software que se pudieran destinar al tratamiento de datos deberán incluir en su descripción técnica el nivel de seguridad que permitan alcanzar en función de la evaluación de impacto de los tratamientos que el proveedor prevé realizar. Los productos de software, en cualquier caso, deberán garantizar la seguridad de los datos. El adjudicatario podrá consultar, conservar, extraer y utilizar los datos de carácter personal facilitados por Canal de Isabel II, S.A. en la medida necesaria para la prestación de lo contratado. En ningún caso, el adjudicatario podrá utilizar los datos para finalidades propias y/o diferentes de las establecidas, ni podrá comunicarlos a terceros. El tratamiento de los datos de carácter personal que realice el adjudicatario y, en su caso, las personas subcontratadas por el adjudicatario (si hubiera sido debidamente autorizado), deberá efectuarse en el Espacio Económico Europeo.

La duración del encargo del tratamiento está vinculada a la duración del Contrato. El adjudicatario, cuando finalice el contrato que provoca el tratamiento de los datos, deberá devolver o destruir los datos de carácter personal a los que haya tenido acceso y/o sobre los que haya realizado algún tratamiento en ejecución del Contrato. El adjudicatario y, en su caso, las personas con las que subcontrate si ha sido debidamente autorizado, garantizarán que han sido capaces de efectuar una supresión segura irreversible de las copias efectuadas de los datos de carácter personal.

De conformidad con el RGPD, el adjudicatario llevará, por escrito, un registro de todas las categorías de actividades de tratamiento efectuadas por cuenta de Canal de Isabel II, S.A. que deberá contener los siguientes extremos:

- El nombre y los datos de contacto del encargado o encargados.
- Las categorías de tratamientos efectuados por cuenta de Canal de Isabel II, S.A. En este supuesto se entenderá que las categorías de datos son las especificadas en párrafos precedentes.
- Una descripción general de las medidas técnicas y organizativas de seguridad que se implementarán en los sistemas y ubicaciones en los que se almacenarán los datos contenidos en los soportes.

El adjudicatario para garantizar un nivel de seguridad adecuado al riesgo deberá adoptar las medidas de seguridad necesarias, de conformidad con lo establecido en el artículo 32 RGPD y que, en su caso, incluirá entre otros:

- La implementación por el proveedor de las medidas de seguridad enumeradas en el anterior RLOPD.
- Restaurar la disponibilidad y el acceso a los datos personales de forma rápida, en caso de incidente físico o técnico.
- Verificar, evaluar y valorar regularmente, la eficacia de las medidas técnicas y organizativas implantadas para garantizar la seguridad de los soportes.
- El adjudicatario no podrá subcontratar la totalidad o parte del tratamiento de los datos que deba efectuarse en cumplimiento del Contrato salvo autorización expresa y escrita de Canal de Isabel II, S.A.

El adjudicatario notificará inmediatamente a Canal de Isabel II, S.A. cualquier indicio o situación que pudiera suponer violaciones de seguridad de los datos de carácter personal o pérdidas de soportes durante el traslado de las que tenga conocimiento. En este sentido, el adjudicatario y, en su caso, personas con las que subcontrate que hayan sido debidamente autorizadas, deberán tener los registros oportunos para verificar los fallos de seguridad, pérdidas, mantener actualizados los registros de incidencias, impedir un nuevo fallo o violación de seguridad, etc. y deberán implementar inmediatamente las medidas de seguridad correspondientes para impedir un nuevo fallo o violación de seguridad, respondiendo de las consecuencias que pudieran ocasionar en caso de incumplimiento de esta medida.

El adjudicatario junto con la comunicación de la incidencia deberá aportar, si fuera posible, toda la información y documentación relevante, y en concreto, la siguiente información:

- Descripción de la naturaleza de la violación de la seguridad de los datos personales.
- 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.
- Descripción de las posibles consecuencias de la violación de la seguridad de los datos personales.
- Descripción de las medidas adoptadas o propuestas para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, una copia de la oportuna denuncia ante la autoridad competente y/o la indicación de las medidas propuestas para mitigar los posibles efectos negativos.

Si no es posible facilitar la información en tiempo real, la información se facilitará de manera gradual sin dilación indebida.

El adjudicatario ayudará a que Canal de Isabel II, S.A. pueda notificar a la autoridad de control una violación de seguridad. Si el adjudicatario debe designar o bien decide designar a un delegado de protección de datos, tendrá que comunicar su identidad y datos de contacto a Canal de Isabel II, S.A.

Si el adjudicatario debe 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 a Canal de Isabel II, S.A. de esa exigencia legal de manera previa, salvo que tal Derecho lo prohíba por razones importantes de interés público.

El adjudicatario deberá poner a disposición de Canal de Isabel II, S.A. toda la información necesaria para demostrar el cumplimiento de las obligaciones que le impone el RGPD, así como para confirmar, permitir y contribuir a la realización de auditorías, incluidas inspecciones, por parte de Canal de Isabel II, S.A., de cualquier otro auditor designado. Esta última obligación también recaerá sobre los terceros que hayan sido subcontratados por el adjudicatario (si hubiera sido autorizado).

Canal de Isabel II, S.A. tendrá derecho a obtener del adjudicatario en un plazo de 24 horas información relativa a dónde, cómo, cuándo y quién ha manejado o accedido a los soportes de datos de carácter personal y las condiciones de seguridad en que se han producido esos accesos.

El adjudicatario deberá incluir en su oferta las medidas utilizadas para el cumplimiento de las obligaciones de confidencialidad e integridad de los datos, la obligación de que los mismos no van a ser utilizados para fines distintos del contratado, así como cualquier otra medida que se vaya a adoptar para el cumplimiento efectivo de los principios de protección de datos, debiendo aportar pruebas documentales. En este sentido, Canal de Isabel II, S.A., directamente o a través de terceros, podrán realizar controles para verificar el cumplimiento de las mismas, pudiendo ordenar, en su caso, la adopción de mecanismos que garanticen la confidencialidad y la integridad de los datos del servicio contratado.

El adjudicatario deberá mantener el deber de secreto respecto a los datos de carácter personal que maneje como consecuencia de lo contratado, incluso después de que finalice el contrato. Será responsabilidad exclusiva del adjudicatario el comunicar a su personal, por cualquier medio de prueba admisible en derecho, las obligaciones y prohibiciones establecidas en la presente cláusula. Además, el adjudicatario garantizará que ha informado debidamente a los titulares (empleados del adjudicatario o de los terceros con los que el adjudicatario, en su caso, subcontrate si hubiera sido autorizado) de los datos de carácter personal que se hayan generado como consecuencia de los registros de las operaciones del servicio, de la posibilidad de que sean utilizados por Canal de Isabel II, S.A. para un adecuado control del cumplimiento de la normativa de protección de datos (por ejemplo, registros de accesos, auditorías, etc.) y de seguridad.

Asimismo, el adjudicatario debe garantizar que las personas autorizadas para tratar los datos de carácter personal se han comprometido a respetar el deber de confidencialidad y que el personal a su cargo ha recibido la formación necesaria en materia de protección de datos para manejar los datos adecuadamente. El adjudicatario informará inmediatamente a Canal de Isabel II, S.A. si considera que alguna de las instrucciones contenidas en esta cláusula infringe el RGPD. Canal de Isabel II, S.A. cumplirá con las obligaciones que el RGPD le impone en cuanto responsable del tratamiento, y estará facultado para supervisar, directamente o a través de terceros, el tratamiento que realice el adjudicatario, incluida la realización de inspecciones y auditorías.

4. SEGUIMIENTO DEL CONTRATO.

Canal de Isabel II S.A. designará a un Responsable que velará por el cumplimiento de las actividades exigidas y ofertadas.

A tal efecto, el adjudicatario designará un Representante de la empresa, el cual coordinará con el Responsable del Contrato del Canal de Isabel II S.A., aquellas incidencias objeto del desarrollo de las actividades contratadas.

Durante la duración del contrato se realizará una reunión mensual con el responsable de contrato y con los técnicos encargados de revisar la documentación para realizar un seguimiento del contrato. Se elaborará un informe mensual con las estadísticas y datos solicitado por Canal de Isabel II S.A.

El adjudicatario deberá hacer un recordatorio mensual a las contratas con el texto e indicaciones que Canal de Isabel II S.A le solicite.

5. FACTURACION.

La facturación de las distintas actividades prestadas se realizará mensualmente en base a los contratos que figuren dados de alta en ese mes. Sólo se facturarán aquellos contratos en los que se revise documentación.

Para cualquier aclaración o consulta relacionada con el contrato del presente Pliego de Prescripciones Técnicas, se deberá contactar con el Área de Prevención del Canal de Isabel II, telf.: 91.545.10.00 ext. 1620 o a través del correo electrónico en la dirección contratación@canaldeisabelsegunda.es.

Todas las dudas planteadas por los licitadores en relación con las características de este proceso serán contestadas por escrito y de forma conjunta a las entidades que hayan retirado el Pliego de Prescripciones Técnicas y se realizará con forme a lo fijado en la Ley.

El presente Pliego de Prescripciones Técnicas Particulares del procedimiento de licitación por procedimiento abierto para la contratación del “**SERVICIO DE CONTROL Y GESTIÓN DOCUMENTAL DE EMPRESAS CONTRATISTAS Y SUBCONTRATISTAS DE CANAL DE ISABEL II S.A.**” consta de 18 páginas.



Firma: Santiago Ciruelos Soriano
JEFE ÁREA PREVENCIÓN



Firma: Pablo Galán González
DIRECTOR RECURSOS