



PLIEGO DE PRESCRIPCIONES TÉCNICAS

**ADQUISICIÓN DE UN PORTAL DIGITAL EN LA
MODALIDAD SAAS PARA EL CONSEJO DE
ADMINISTRACIÓN DE CANAL DE ISABEL II S.A.**

Nº CONTRATO: 163/2022

Área: Aplicaciones Informáticas

Empresa Canal de Isabel II, S.A.	Contrato ADQUISICIÓN DE UN PORTAL DIGITAL EN LA MODALIDAD SAAS PARA EL CONSEJO DE ADMINISTRACIÓN DE CANAL DE ISABEL II S.A. 163/2022	
Elaborado por Área de Aplicaciones Informáticas	Documento Pliego de Prescripciones Técnicas	Versión V02

Índice

1. INTRODUCCIÓN	3
2. ALCANCE	4
2.1. Requisitos funcionales	4
2.2. Niveles de servicio	5
2.3. Otros servicios	6
2.4. Otras condiciones del servicio	6
3. REQUISITOS DE SEGURIDAD MÍNIMOS DEL SOFTWARE COMO SERVICIO	7
4. Formato de la Oferta técnica	10

Empresa Canal de Isabel II, S.A.	Proyecto ADQUISICIÓN DE UN PORTAL DIGITAL EN LA MODALIDAD SAAS PARA EL CONSEJO DE ADMINISTRACIÓN DE CANAL DE ISABEL II S.A. 163/2022	
Elaborado por Área de Aplicaciones Informáticas	Documento Pliego de Prescripciones Técnicas	Versión V02

1. INTRODUCCIÓN

El objeto del presente contrato es la adquisición de una herramienta software en modalidad Saas, para gestionar un nuevo portal digital para la organización de las reuniones del Consejo de Administración de Canal de Isabel II S.A. y sus comisiones especializadas. Entre las funciones que se esperan conseguir de esta herramienta estarían las siguientes:

- Portal digital de acceso seguro
- Repositorio común de documentación
- Comunicación de convocatorias
- Gestor de notificaciones

Y todas aquellas funcionalidades que ayuden a que la organización de estos eventos se desarrolle de forma más eficaz y segura, facilitando el acceso a la información, la comunicación, y el envío y la gestión de documentación.

Empresa Canal de Isabel II, S.A.	Proyecto ADQUISICIÓN DE UN PORTAL DIGITAL EN LA MODALIDAD SAAS PARA EL CONSEJO DE ADMINISTRACIÓN DE CANAL DE ISABEL II S.A. 163/2022	
Elaborado por Área de Aplicaciones Informáticas	Documento Pliego de Prescripciones Técnicas	Versión V02

2. ALCANCE

2.1. Requisitos funcionales

A continuación, se enumeran los requisitos funcionales que debe tener la herramienta.

1. Gestión de Consejos y de sus comisiones especializadas:

- Para la organización de los diferentes consejos y de sus comisiones especializadas y con el objeto de garantizar la confidencialidad, la herramienta deberá contemplar la creación de espacios diferenciados a los que se le concederá acceso a todos o a parte de los usuarios consejeros. Se deben, al menos poder configurar 4 espacios/sedes (Consejo de Administración, Comisión de Auditoría, Comisión de Nombramientos y Retribuciones + espacio de reserva).
- Se podrán efectuar envíos de convocatorias de las reuniones a los distintos órganos sociales, divididos en espacios, con notificación a los correspondientes usuarios de cada espacio.

1.1. Gestión documental:

- La herramienta contará con un repositorio documental que permita el almacenamiento de los documentos digitales de forma estructurada, la gestión de versiones y el control de acceso.
- Se podrá subir tanto documentación relacionada con una convocatoria, como documentación complementaria (ejemplo, estatutos sociales, Reglamento del Consejo, Plan Estratégico y cualesquiera otros).
- Información histórica: se podrá subir documentación correspondiente a reuniones del Consejo y sus comisiones anteriores al inicio de la utilización de la herramienta por Canal.
- Marca de agua: se podrá configurar una marca de agua tanto en la pantalla como en la impresión y descarga de la documentación.
- Anotaciones: se podrá realizar anotaciones en documentos sin necesidad de modificar el original.
- Almacenamiento ilimitado: el repositorio no tendrá límite de almacenamiento.

2. Gestión de usuarios

Empresa Canal de Isabel II, S.A.	Proyecto ADQUISICIÓN DE UN PORTAL DIGITAL EN LA MODALIDAD SAAS PARA EL CONSEJO DE ADMINISTRACIÓN DE CANAL DE ISABEL II S.A. 163/2022	
Elaborado por Área de Aplicaciones Informáticas	Documento Pliego de Prescripciones Técnicas	Versión V02

- Roles de usuario: se proporcionará roles de usuario administrador para configurar el sistema, y otros roles, consumidores de la información.
- Gestión de permisos: se podrá configurar en virtud del usuario, tanto los permisos de acceso a los espacios virtuales, como los diferentes niveles de permisos de acceso a la documentación: lectura, modificación, eliminación, descarga, impresión, cambio de ubicación de los documentos, etc.

Concurrencia de usuarios: se deberá permitir, al menos, el acceso a 25 usuarios. A estos efectos se considerará “usuario” a cada una de las personas que tenga acceso al portal, con independencia del número de espacios diferenciados a los que tenga permiso para acceder.

En este sentido, a continuación, se indica el número de personas que habrán de tener acceso a los diferentes espacios:

Consejo de Administración: 25.

Comisión de Auditoría: 17.

Comisión de Nombramientos y Retribuciones: 17.

Espacio de reserva: 18.

3. Otras características

- Personalización de la interfaz: se deberá poder personalizar la interfaz de usuario con la inserción, al menos, de la imagen corporativa en el menú principal (“home”).
- Acceso multidispositivo: el acceso a la plataforma deberá poderse realizar desde cualquier dispositivo: PC, móvil y Tablet.
- Buscadores: la herramienta contará con un buscador avanzado de caracteres alfanuméricos, tanto en la interfaz como en la documentación subida a la plataforma.
- Posibilidad de descargar todo el contenido almacenado una vez finalizado la relación contractual.

2.2. Niveles de servicio

Los niveles de servicio que se establecen para la resolución de consultas, incidencias o problemas de carácter técnico desde su notificación serán las siguientes:

Empresa Canal de Isabel II, S.A.	Proyecto ADQUISICIÓN DE UN PORTAL DIGITAL EN LA MODALIDAD SAAS PARA EL CONSEJO DE ADMINISTRACIÓN DE CANAL DE ISABEL II S.A. 163/2022	
Elaborado por Área de Aplicaciones Informáticas	Documento Pliego de Prescripciones Técnicas	Versión V02

- Plazo máximo de tiempo de resolución de incidencias y consultas críticas: < 10 horas naturales
- Plazo máximo de tiempo de resolución de incidencias y consultas graves: < 24 horas naturales
- Plazo máximo de tiempo de resolución de incidencias y consultas leves: < 48 horas naturales

La criticidad de las incidencias será determinada por Canal de Isabel II, S.A. Los cambios de categorización de las mismas se coordinarán entre Canal de Isabel II, S.A. y el responsable del soporte técnico de la empresa adjudicataria.

Criticidad de incidencias y consultas:

- Leve: Es deseable su resolución, no impide el normal funcionamiento con el sistema.
- Grave: Es necesaria su resolución, ya que impide el normal funcionamiento con el sistema, aunque existen alternativas funcionales que lo cubren.
- Crítica: Es obligada su resolución ya que impide el normal funcionamiento con el sistema, y no existen alternativas funcionales que lo cubren.

2.3. Otros servicios

Adicionalmente se contratará:

- La instalación, configuración y puesta en marcha del software.
- Formación inicial, que podrá ser remota o presencial, tanto a usuarios como a administradores del software.
- Actualización de versiones y revisiones del producto.

2.4. Otras condiciones del servicio

Debido a la naturaleza del contrato no aplican como requerimientos específicos las consideraciones sociales, ambientales y de innovación, más allá de lo establecido como condiciones especiales de ejecución en el apartado 9.3 del Anexo 1 del Pliego de Cláusulas Administrativas Particulares.

Empresa Canal de Isabel II, S.A.	Proyecto ADQUISICIÓN DE UN PORTAL DIGITAL EN LA MODALIDAD SAAS PARA EL CONSEJO DE ADMINISTRACIÓN DE CANAL DE ISABEL II S.A. 163/2022	
Elaborado por Área de Aplicaciones Informáticas	Documento Pliego de Prescripciones Técnicas	Versión V02

3. REQUISITOS DE SEGURIDAD MÍNIMOS DEL SOFTWARE COMO SERVICIO

a) El acceso se produce exclusivamente bajo un protocolo seguro que cifre de forma robusta los datos transmitidos entre el cliente y el servidor, con el objeto de garantizar su confidencialidad, integridad y disponibilidad (por ejemplo, uso exclusivo de TLS 1.2 o superior, y utilizando sólo suites de cifrado robustas para evitar vulnerabilidades de tipo BEAST (RC4), Lucky13 (CBC), 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.).

b) Todos los formularios, incluidos los de inicio de sesión, tienen que estar protegidos contra ataques de fuerza bruta (uso de CAPTCHA, disociación de los campos “usuario” y “contraseña” en pasos distintos, pero dependientes y controlados, dentro del proceso de inicio de sesión, etc.) y tienen que controlar completamente los caracteres introducidos por el usuario para evitar ataques de tipo Cross-Site Scripting, Cross-Site Request Forgery (CSRF), Remote File Inclusion (RFI), Remote Code Execution (RCE), Inyección SQL, etc.

c) El uso de un esquema de BBDD propio para la información propiedad de Canal de Isabel II, S.A.

d) 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.

e) 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).

f) Almacenamiento de todos los datos de autenticación de los usuarios en la BBDD mediante el uso de funciones criptográficas seguras 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)), establecer un periodo máximo de vigencia y validez de las contraseñas (recomendado un máximo de 60 días) y de implementar un histórico de contraseñas (con un mínimo de 6). Es obligatorio el uso de funciones de derivación de claves basadas en contraseña (Password-Based Key Derivation Functions) para el almacenamiento de las contraseñas consideradas como seguras (por ejemplo, PBKDF2 utilizando al menos un generador de números pseudoaleatorios basado en HMAC-SHA1, 5.000 iteraciones para la parte cliente y 100.000 iteraciones para la parte servidora, versiones modernas de bcrypt con un work factor de al menos 12, versiones modernas no vulnerables de Argon2 (Argon2d), etc.).

g) Exista 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 como framework de autorización y OpenID Connect (OIDC) como protocolo de autenticación en las APIs existentes.

Empresa Canal de Isabel II, S.A.	Proyecto ADQUISICIÓN DE UN PORTAL DIGITAL EN LA MODALIDAD SAAS PARA EL CONSEJO DE ADMINISTRACIÓN DE CANAL DE ISABEL II S.A. 163/2022	
Elaborado por Área de Aplicaciones Informáticas	Documento Pliego de Prescripciones Técnicas	Versión V02

- SCIM como modelo para automatizar el intercambio de información de identidad de los usuarios entre distintos dominios de identidad.

h) En caso de existir Web Services que puedan ser consumidos desde Canal de Isabel II, S.A., deben estar securizados a nivel de mensaje, especificando la forma de firmar y cifrar los mensajes de tipo SOAP, a través de la especificación WS-Security. Por tanto:

- Los servicios deben estar autenticados, preferentemente con WS-Security Tokens
- Los usuarios deben ser autenticados vía SAML 2.0.
- La integridad de la información ha de estar garantizada a través del uso de protocolos seguros (HTTPS 1.2 o superior) o vía WS-Signature.
- El no repudio debe estar garantizado a través del uso de WS-Signature o WS-Addressing.
- La confidencialidad de la información ha de estar garantizada a través del uso de protocolos seguros (HTTPS 1.2 o superior) o vía WS-Encryption.
- Debe hacerse uso de una política de seguridad (WS-Policy).

i) Exista la posibilidad de habilitar al menos un segundo factor de autenticación (2FA) para garantizar la identidad de los usuarios del servicio, ya sea mediante el uso de certificados electrónicos reconocidos (como, por ejemplo, DNle), contraseñas de un único uso (OTP), uso de tokens (hardware o software), etc.

j) 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, WASC) para comprobar que existen y que han sido implementadas correctamente.

k) Se almacenará de forma segura (garantía de acceso, recuperación y no modificación) y se revisará de forma regular el registro de eventos de las actividades de los usuarios (errores y eventos de seguridad). Estos registros deberán mantenerse al menos durante cinco (5) años.

l) El proveedor comunicará inmediatamente a Canal de Isabel II, S.A. todas aquellas vulnerabilidades reportadas de forma privada o hechas públicas que afecten a sus sistemas, así como las acciones que están siendo llevadas a cabo para eliminar o mitigar dichas vulnerabilidades.

m) El proveedor del servicio Cloud, en caso de que haya evidencias demostrables de que un incidente de seguridad en Canal de Isabel II, S.A. es imputable a él, se compromete a elaborar un informe pormenorizado y exhaustivo del incidente en el que hará constar, como mínimo, la siguiente información:

- Descripción del incidente.
- Origen del incidente.
- Descripción cronológica de los hechos del incidente.

Empresa Canal de Isabel II, S.A.	Proyecto ADQUISICIÓN DE UN PORTAL DIGITAL EN LA MODALIDAD SAAS PARA EL CONSEJO DE ADMINISTRACIÓN DE CANAL DE ISABEL II S.A. 163/2022	
Elaborado por Área de Aplicaciones Informáticas	Documento Pliego de Prescripciones Técnicas	Versión V02

- Descripción de las acciones preventivas/correctivas llevadas a cabo por el proveedor del servicio Cloud.
- Evaluación de los recursos humanos pertenecientes al equipo de trabajo asignado a la prestación del servicio Cloud contratado por Canal de Isabel II, S.A. y que han sido necesarios para el análisis y resolución del incidente.

Dicho informe, una vez finalizado, se remitirá al responsable del proveedor en Canal de Isabel II, S.A. quien a su vez lo remitirá a la Dirección de Seguridad.

Los sistemas de información en los que se sustenten los servicios SaaS prestados por el Adjudicatario, deberán ser conformes con el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS) o cumplir con las medidas desarrolladas en las correspondientes guías del CCN-STIC o, en caso contrario, deberán adecuarse a ello en el plazo indicado por la disposición transitoria única del RD 311/2022 de 3 de mayo.

Empresa Canal de Isabel II, S.A.	Proyecto ADQUISICIÓN DE UN PORTAL DIGITAL EN LA MODALIDAD SAAS PARA EL CONSEJO DE ADMINISTRACIÓN DE CANAL DE ISABEL II S.A. 163/2022	
Elaborado por Área de Aplicaciones Informáticas	Documento Pliego de Prescripciones Técnicas	Versión V02

4. Formato de la Oferta técnica

La oferta técnica se atenderá al formato establecido en el apartado 6 del Anexo I del Pliego de Cláusulas Administrativas del presente procedimiento.

Firmado electrónicamente por
JUAN RODRIGUEZ HERRADURA
el día 08-08-2022 11:12:25

Delegación por Ausencia.

Jefe de ÁREA DE APLICACIONES INFORMÁTICAS

Firmado electrónicamente por
ÁNGEL RODRÍGUEZ GARCÍA
el día 08-08-2022 13:03:27

Subdirector de SISTEMAS INFORMÁTICOS

Firmado electrónicamente por
MÓNICA FIERRO MARTÍN
el día 09-08-2022 13:10:39

Directora de RECURSOS

Empresa Canal de Isabel II, S.A.	Proyecto ADQUISICIÓN DE UN PORTAL DIGITAL EN LA MODALIDAD SAAS PARA EL CONSEJO DE ADMINISTRACIÓN DE CANAL DE ISABEL II S.A. 163/2022	
Elaborado por Área de Aplicaciones Informáticas	Documento Pliego de Prescripciones Técnicas	Versión V02

ANEXO I

Los requisitos de seguridad se rellenarán conforme al anexo “requisitos de seguridad.xls”.