PLIEGO DE PRESCRIPCIONES TÉCNICAS

LICENCIAS SERVICIO SAAS ARCHIBUS ON DEMAND DE CANAL DE ISABEL II, S.A.

Nº CONTRATO: 151/2022

Área: Planificación, Control y Seguridad

Empresa	Contrato	
Canal de Isabel II, S.A.	**LICENCIAS SERVICIO SAAS ARCHIBUS ON DEMAND DE CANAL DE ISABEL II, S.A. CONTRATO 151/2022**	
Elaborado por	Documento	Versión
Área de Planificación, Control y Seguridad	Pliego de Prescripciones Técnicas	V02

Índice

1. INTRODUCCIÓN 3

2. ALCANCE 4

2.1. Servicios incluidos en el Contrato 4

2.2. Niveles de servicio 5

2.3. Otros servicios 5

2.4. Otras condiciones del servicio 5

3. REQUISITOS DE SEGURIDAD MÍNIMOS DEL SOFTWARE COMO SERVICIO 6

4. Formato de la Oferta técnica 9

1. INTRODUCCIÓN

Canal de Isabel II (CANAL) utiliza el software Archibus On Demand una plataforma Saas (Software as a Services) para la gestión de espacios por parte del Área de Mantenimiento de Edificios.

2. ALCANCE

2.1. Servicios incluidos en el Contrato

Los servicios objeto del contrato son los que se detallan a continuación:

Servicio 1 (Si}. Renovación de suscripciones incluido el mantenimiento y soporte técnico:

Renovación de las suscripciones a las aplicaciones que dispone actualmente Canal de Isabel II, S.A. licenciado el acceso para cinco usuarios de forma simultánea. Estas aplicaciones son:

- Space Inventory & Performance
- Space Personnel & Occupancy
- Asset Management
- Enterprise Move Management.
- tres licencias de acceso para Smartclient para AutoCAD y Revit

El servicio incluye:

- 25 Gb de espacio de almacenamiento para base de datos
- 2 Gb de espacio de almacenamiento para archivos o planos

El soporte técnico incluirá:

- Asistencia técnica ante incidencias y problemas
- Actualización de versiones y revisiones
- Remisión periódica -trimestral- de copias de seguridad de la base de datos

El Soporte Técnico consistirá en:

La tramitación de las incidencias relativas a cualquier vicio oculto o fallo del sistema se realizará a través del Centro de Soporte Técnico de Archibus con el fin de que se proceda a su resolución acorde al nivel de servicio indicado en el apartado 2.2. de este documento. Con este objeto, el personal asignado al Centro de Soporte Técnico estará capacitado para realizar los siguientes servicios:

- Asistencia Técnica Telefónica a los Administradores Funcionales y Técnicos de ARCHIBUS.
- Registro y seguimiento de cualquier incidencia o problema con el Servicio ARCHIBUS ON DEMAND, proporcionando, si es posible, alternativas de trabajo (medidas paliativas), mientras se soluciona el problema.
- Corrección de disfunciones de cualquier personalización del software que pudiera realizarse.
- Adaptación de las personalizaciones existentes sobre las nuevas versiones o revisiones de ARCHIBUS.

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:

- 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 en 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:

- Paquete de formación Continua: Canal de Isabel II, S.A. contará con un paquete de 32 horas, de las que podrá disponer bajo demanda para impartir formación sobre la herramienta y nuevas versiones.
- Servicio parametrización: Canal de Isabel II, S.A. contará con un paquete de 40 horas de las que podrá disponer bajo demanda para servicios de administración y actualización de planos e inventarios de espacios normalizados.

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.

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.

- 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-Adressing.
- 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, DNIe), 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. acerca de todas aquellas vulnerabilidades reportadas de forma privada o hechas públicas que afecten a sus sistemas, así de 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.

- 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.

4. Formato de la Oferta técnica

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

Firmado electronicamente por: Jesus Plaza Rubio
En la fecha y hora 04.11.2022 12:09:24 CET

Jefe de ÁREA DE PLANIFICACIÓN, CONTROL Y SEGURIDAD

Firmado electronicamente por: Ángel Rodríguez García
En la fecha y hora 04.11.2022 14:18:56 CET

Subdirector de SISTEMAS INFORMÁTICOS

Firmado electronicamente por: JUAN SÁNCHEZ GARCÍA
En la fecha y hora 06.11.2022 23:25:11 CET

Director de INNOVACIÓN E INGENIERÍA