

NOTA INFORMATIVA RELATIVA A LA SOLICITUD DE ACLARACIONES A LA DOCUMENTACIÓN DE ESPECIFICACIONES TÉCNICAS APORTADA POR LOS LICITADORES PARA EL PROCEDIMIENTO DE LICITACIÓN N.º 163/2022 PARA “ADQUISICIÓN DE UN PORTAL DIGITAL EN LA MODALIDAD SAAS PARA EL CONSEJO DE ADMINISTRACIÓN DE CANAL DE ISABEL II S.A.”

De conformidad con lo indicado en el Acta S01 de 20 de Septiembre 2022, una vez analizada la documentación presentada por los licitadores, la Mesa Permanente de Contratación asistida por los servicios técnicos de Canal de Isabel II, S.A. procederá a solicitar las aclaraciones necesarias en los términos y condiciones previstas en los pliegos del procedimiento.

Los **aspectos susceptibles de aclaración** encontrados en la documentación de Especificaciones Técnicas presentada por los licitadores son los siguientes:

DILITRUST IBÉRICA S.L.

Aspecto susceptible de aclaración 1: la empresa licitadora no ha presentado anexo I del PPT “requisitos de seguridad.xls” cumplimentado, tal y como se requiere en el apartado 6.A).8. del Anexo I del Pliego de Cláusulas Administrativas Particulares (en adelante, “PCAP”), donde se pone de manifiesto el grado de cumplimiento de los requisitos de seguridad del apartado 3 del PPT. Los licitadores deberán, en la columna de Consideraciones explicar cómo lo cumplen y en su caso dar pruebas de su cumplimiento (que pueden ser explicación de cómo lo cumplen, capturas, documentos, arquitectura, informes de auditoría, análisis de riesgos realizados, etc.) que permitan verificar el cumplimiento de los mismos.

PERFORMANCE MANAGEMENT PARTNERS SL

Aspecto susceptible de aclaración 1: en el alcance de requisitos funcionales del pliego recogido en el apartado 2.1. del Pliego de Prescripciones Técnicas (en adelante, “PPT”), se establece que el almacenamiento debe ser ilimitado. Sin embargo, en la oferta aparece: “Almacenamiento ilimitado de los datos de Diligent Boards en los centros de datos de Diligent Almacenamiento de 1Tb en Secure File Sharing”.

Aclaración: la empresa licitadora deberá aclarar si el almacenamiento es efectivamente ilimitado o si existe una limitación de 1Tb.

Aspecto susceptible de aclaración 2: en el anexo I del PPT, requisitos de seguridad, punto a y b, Evaluación objetiva del requisito en base a los dominios, objetivos de control y controles del anexo A ISO/IEC 27001:2013 (ISO/IEC 27002:2013), presentado por la empresa licitadora se responde lo siguiente:

Sí. HTTPS, TLS y SSL.

Se incluye certificado ISO 270001.

Todas las comunicaciones entre los servidores y los clientes se realizan a través de conexiones cifradas TLS 1.2. Los servidores están protegidos por una defensa de red multicapa que utiliza firewalls de perímetro, un sistema de prevención de intrusiones, proxies inversos, firewalls de aplicaciones web, equilibrio de carga y firewalls internos.

Toda la comunicación interna entre los componentes del sistema (es decir, entre servidores y centros de datos) está cifrada. Además, los centros de datos están protegidos por una seguridad física y electrónica de última generación y están sometidos a pruebas realizadas por terceros para garantizar que no surjan vulnerabilidades. Asimismo, utilizamos la colocación redundante en nuestros centros de datos para garantizar un tiempo de actividad superior al 99,5 %, incluso en caso de desastre u otra posible interrupción.

Aclaración: Se solicita evidencias del uso de suites de cifrado no vulnerables y no débiles. Si no es posible aportar evidencias, deben proporcionar la URL de acceso a Boards, para que sea Canal quien lo verifique.

Se entiende que el apartado b) lo cumplen a través de las "pruebas realizadas por terceros para garantizar que no surjan vulnerabilidades". Se solicita que nos hagan llegar evidencias del cumplimiento de este requisito, pudiendo ser:

- La última auditoría de seguridad del servicio objeto de contratación y el plan de remediación de los problemas detectados, bajo NDA (acuerdo de confidencialidad)
- Un informe con capturas de pantalla que evidencie el cumplimiento.

Aspecto susceptible de aclaración 3: en el anexo I del PPT, requisitos de seguridad, punto f, se indica:

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.).

La empresa licitadora ha respondido lo siguiente:

Sí.

Se incluye certificado ISO 270001.

Diligent ofrece una política de contraseña configurable por el cliente (longitud, número y conjunto de caracteres necesarios, excluir palabras en inglés, excluir nombres de usuario, caducidad, reutilización, opción de restablecimiento de contraseña [responder a preguntas de seguridad] y tiempos de inactividad forzados definidos por el cliente [cierre de sesión]). Los parámetros relacionados con la contraseña configurable del sitio también incluyen el número de inicios de sesión incorrectos antes del bloqueo y la activación de un autoservicio para el restablecimiento de contraseñas .

Los nombres de inicio de sesión tienen un máximo de 50 caracteres, y las contraseñas tienen un máximo de 32 caracteres.

Los clientes también pueden activar la Autorización del dispositivo, disponible en dispositivos iOS, Tienda de Windows, dispositivos Mac, dispositivos Android y ordenadores que ejecuten la aplicación de escritorio para Windows de Diligent Boards (OneClick). Esta función permite a los administradores asociar el acceso de usuario a uno o varios dispositivos específicos, por lo que limita el acceso a la aplicación desde cualquier dispositivo que no esté autenticado. Además, desactiva el acceso a Boards a través de navegador.

Aclaración: la empresa licitadora deberá aclarar si los datos de autenticación se cifran también con SHA-256 o se utiliza alguna función de derivación de claves basadas en contraseña.

Aspecto susceptible de aclaración 4: en el anexo I, requisitos de seguridad del PPT, último punto, se indica: 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.

La empresa licitadora ha respondido lo siguiente:

“No”.

Aclaración: la empresa licitadora deberá aclarar si la respuesta “no” se refiere a que los sistemas de información en los que se sustentan los servicios SaaS ofertados por la misma el licitador no son conformes con el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS), a que no cumplen con las medidas desarrolladas en las correspondientes guías CCN-STIC; o a que no se comprometen a adecuarse al ENS en el plazo indicado por la disposición transitoria única del RD 311/2022 de 3 de mayo.

Las aclaraciones solicitadas deben presentarse a través de la Plataforma Electrónica de Licitación, **antes de las 14.00 horas del tercer día hábil computado a partir del día hábil siguiente a la publicación en el tablón de anuncios electrónico del Portal de la Contratación Pública de la Comunidad de Madrid.**



Fecha:
2022.09.28
14:59:53 +02'00'

La Secretaria de la Mesa Permanente de Contratación