

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.:

En relación con el apartado 6.A).8. del Anexo I del PCAP los licitadores deberán presentar anexo I del PPT “requisitos de seguridad.xls”, donde se ponga 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 cumplen los requisitos exigidos y, en su caso, presentar prueba de su cumplimiento. Una vez revisado el Anexo I del PPT presentado por la empresa licitadora, se han observado los siguientes aspectos que deben ser objeto de aclaración:

Aspecto susceptible de aclaración 1: en relación con el apartado 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 (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.),* se ha comprobado que la empresa licitadora no indica nada relativo a las suites de cifrado utilizadas, si son o no débiles y/o vulnerables.

Aclaración 1: la empresa licitadora deberá aclarar el referido aspecto, indicando si las suites de cifrado utilizadas, son o no débiles y/o vulnerables.

Aspecto susceptible de aclaración 2: en relación con el apartado 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.*

Se entiende que se cumple al indicar en su documento “DiliTrust y la Seguridad” que, a través de pruebas de seguridad semanales, el servicio objeto de contratación “ha sido testado para aprobar con éxito todas las recomendaciones de seguridad provenientes de auditorías externas de vulnerabilidad a través de las siguientes organizaciones: “... OWASP TOP 10 Most Critical Web Application...”. no obstante, es necesario que el licitador confirme que se aplica también a todos los formularios del servicio, incluidos los de inicio de sesión.

Aclaración 2: la empresa licitadora deberá aclarar el referido aspecto, confirmando que se aplica también a todos los formularios del servicio, incluidos los de inicio de sesión.

Aspecto susceptible de aclaración 3: en relación con el apartado c) *el uso de un esquema de BBDD propio para la información propiedad de Canal de Isabel II, S.A.*, se ha comprobado que la empresa licitadora no indica nada al respecto de lo solicitado en los requisitos.

Aclaración 3: la empresa licitadora deberá aclarar el referido aspecto, indicando la información solicitada en los requisitos.

Aspecto susceptible de aclaración 4: en relación con el apartado 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*, se ha comprobado que la empresa licitadora no indica nada al respecto de lo solicitado en los requisitos.

Aclaración 4: la empresa licitadora deberá aclarar el referido aspecto indicando la información solicitada en los requisitos.

Aspecto susceptible de aclaración 5: en relación con el apartado 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.)*, se solicita que la empresa licitadora aclare los siguientes aspectos:

1. Sobre la obligatoriedad de utilizar caracteres alfanuméricos (mezcla de mayúsculas, minúsculas y números) y no alfanuméricos (por ejemplo, signos de puntuación y ortográficos), se solicita aclarar si es posible configurar la política de contraseñas en la aplicación para uso de los cuatro caracteres de distinto tipo (minúsculas, mayúsculas, cifras y puntuación).

Aclaración 5.1: la empresa licitadora deberá aclarar el referido aspecto indicando si es posible configurar la política de contraseñas en la aplicación para uso de los cuatro caracteres de distinto tipo (minúsculas, mayúsculas, cifras y puntuación).

2. Sobre el establecimiento de un periodo máximo de vigencia y validez de las contraseñas (recomendado un máximo de 60 días), no se indica nada con respecto al cumplimiento de este requisito.

Aclaración 5.2: la empresa licitadora deberá aclarar el referido aspecto indicando la información relativa al cumplimiento de este requisito.

3. Sobre el histórico de contraseñas (con un mínimo de 6), no se indica nada con respecto al cumplimiento de este requisito.

Aclaración 5.3: la empresa licitadora deberá aclarar el referido aspecto indicando la información relativa al cumplimiento de este requisito.

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:
2022.10.04
13:59:29 +02'00'

La Secretaría de la Mesa Permanente de Contratación