

APÉNDICE 2. REQUERIMIENTOS MÍNIMOS DE SEGURIDAD DE LOS SERVICIOS

INDICE

Apartado 1. Objeto del documento.	3
Apartado 2. Aspectos técnicos de seguridad.	3

Apartado 1. Objeto del documento.

El presente Apéndice tiene por objeto recoger los requisitos mínimos en cuanto a seguridad de la información y, en particular, en el caso de emplearse herramientas y servicios alojados en la nube que deben cumplir obligatoriamente los servicios ofertados a Canal de Isabel II en la presente licitación.

A tal efecto, el licitador deberá comprometerse, en caso de resultar adjudicatario, a cumplir e implementar todos estos requerimientos, antes de transcurridos los 6 primeros meses desde la fecha del Acta de Inicio de los trabajos.

Apartado 2. Aspectos técnicos de seguridad mínimos de carácter obligatorio.

El licitador deberá garantizar, mediante la presentación de evidencias fehacientes, basadas en informes de cumplimiento realizados y firmados (fecha completa, nombre completo del firmante, empresa y cargo ostentado por el firmante en ella) por un tercero independiente o referencias a la documentación técnica oficial de la solución ofertada, el cumplimiento de los siguientes requisitos de seguridad:

- El acceso a todas las herramientas que formen parte de la solución ofertada se realizará exclusivamente bajo un protocolo seguro que cifre de forma robusta los datos transmitidos entre origen y destino, 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.).
- Todos los formularios, incluidos los de inicio de sesión, estarán 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 deberán 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.
- En cada herramienta que pudiera tratar datos personales, la Dirección de los Trabajos podrá requerir que se haga uso de un esquema de BBDD propio para la información propiedad de Canal de Isabel II, S.A., por lo que la solución ofertada deberá permitir el uso de distintos esquemas de BBDD.
- Salvo que pueda garantizarse que el servicio se presta de manera exclusiva a Canal, dicho esquema de BBDD será 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.
- En cada herramienta que pudiera tratar datos personales, la Dirección de los Trabajos podrá requerir 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).
- 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.)

- En caso de existir Web Services que puedan ser consumidos desde Canal de Isabel II, S.A., estos deberán 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 deberán estar autenticados, preferentemente con WS-Security Tokens.
 - Los usuarios deberán ser autenticados vía SAML 2.0.
 - La integridad de la información ha deberá estar garantizada a través del uso de protocolos seguros (HTTPS 1.2 o superior) o vía WS-Signature.
 - El no repudio deberá estar garantizado a través del uso de WS-Signature o WS-Addressing.
 - La confidencialidad de la información deberá estar garantizada a través del uso de protocolos seguros (HTTPS 1.2 o superior) o vía WS-Encryption.
 - Deberá hacerse uso de una política de seguridad (WS-Policy).
- Deberá existir la posibilidad de habilitar al menos un segundo factor de autenticación (2FA) para garantizar la identidad de los usuarios que accedan al 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. En caso de que no exista la posibilidad de habilitar al menos un segundo factor de autenticación (2FA) para garantizar la identidad de los usuarios que accedan al servicio, será obligatorio que la solución ofertada pueda restringir el acceso al servicio a los rangos IP públicos de navegación de Canal de Isabel II.
- Todas las funciones de la aplicación relacionadas con la autenticación, la gestión de las sesiones y la autorización (control del acceso) deberán haber sido auditadas contra estándares de seguridad internacionalmente reconocidos (por ejemplo, OWASP, WASC) para comprobar que existen y que han sido implementadas correctamente.
- 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.

Mediante la presentación de la correspondiente declaración responsable, el proveedor del servicio deberá establecer el compromiso de llevar a cabo las siguientes acciones:

- 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 como de las acciones que están siendo llevadas a cabo para eliminar o mitigar dichas vulnerabilidades
- 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 comprometerá 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.