

**FORMALIZACIÓN DEL ACUERDO RELATIVO A LA MODIFICACIÓN DEL CONTRATO 194/2024
RELATIVO AL "SERVICIO DE COORDINACIÓN DE ACTIVIDADES INSTITUCIONALES DE CANAL DE
ISABEL II, S.A., M.P."**

Fecha: La fecha y hora del sellado de tiempo de la firma electrónica de la parte que haya firmado en último lugar.

----- **REUNIDOS** -----

De una parte, **D. GONZALO JOSÉ BARDÓN FERNÁNDEZ-PACHECO**, Subdirector de Contratación de Canal de Isabel II, Sociedad Anónima, M.P. (en adelante, "**Canal de Isabel II, S.A., M.P.**").

Y de otra parte, **D^a. ISABEL MATEOS DEL NOZAL**, en nombre y representación de TELECYL, S.A.

----- **INTERVIENEN** -----

El primero en nombre y representación de Canal de Isabel II S.A., M.P., en virtud de las facultades que le corresponden, conferidas según Poder otorgado a su favor por el Consejo de Administración de Canal de Isabel II S.A., M.P., en su sesión celebrada el día 29 de septiembre de 2022, elevado a documento público firmado por el Notario de Madrid, D. JUAN JOSÉ DE PALACIO RODRÍGUEZ, el día 6 de octubre de 2022, con el nº 6.543 de su protocolo.

La segunda en nombre y representación de la Sociedad Mercantil **TELECYL, S.A.** con domicilio social en Valladolid, calle Enrique Cubero nº 9. Ostenta dicha representación según Poder otorgado ante el Notario **D. IGNACIO CUADRADO ZULOAGA**, el día **5 de abril de 2019**, bajo el núm. **944** de su protocolo.

Ambas partes se reconocen recíprocamente capacidad suficiente para la celebración del presente Acuerdo y,

----- **EXPONEN** -----

Que con fecha **21 de enero de 2026** el Consejero Delegado de Canal de Isabel II, S.A. aprobó la primera modificación con incremento de precio del contrato n.º **194/2024** con aumento de precio de conformidad con lo dispuesto en los artículos 203 y 205.2 c) de la Ley 9/2017, de 8 de noviembre, de contratos del Sector Público, por la que se transponen al ordenamiento jurídico español las Directivas del Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014.

Que las partes, mediante el presente documento, formalizan el acuerdo relativo a la referida modificación del contrato n.º 194/2024, con sujeción a las siguientes:

----- CLÁUSULAS -----

PRIMERA. – MODIFICACIÓN Nº 1 DEL CONTRATO

Las partes acuerdan la **primera modificación del contrato**, con la finalidad de incorporar al contrato la creación de un microsite específico bajo el subdominio *175aniversario.canaldeisabelsegunda.es*, recurso digital imprescindible para centralizar y difundir las distintas acciones previstas con motivo de la conmemoración del 175 aniversario de Canal de Isabel II, constituyendo un elemento estratégico de comunicación institucional, referido en el informe de la Subdirección de Apoyo y Relaciones Institucionales que se adjunta como Anexo I.

La modificación propuesta incrementa el precio del contrato en la cantidad de 18.000,00 euros, IVA excluido, lo que supone un incremento del 5,09 % sobre el importe de adjudicación del contrato (353.389,00 euros, IVA excluido). El importe vigente del contrato tras la modificación nº 1 es de 371.389,00 €, excluido el IVA.

SEGUNDA. – FINAL

En todos aquellos aspectos que no hayan sido modificados por el presente Acuerdo, seguirán resultando de aplicación las cláusulas de los pliegos relativas a la aceptación de la adjudicación suscrita en fecha 28 de noviembre de 2025.

Siendo cuanto antecede expresión de la voluntad de ambas partes, así lo otorgan y, en prueba de conformidad, lo firman:

Firmado electrónicamente por
BARDÓN (R:A86488087) FIRMA
30.01.2026 14:38:09 CET

GONZALO JOSÉ

POR CANAL DE ISABEL II, S.A, M.P.,

ISABEL
MATEOS (R:
A47310941)

Firmado
digitalmente
por
ISABEL MATEOS
(R: A47310941)
Fecha:
2026.01.30
13:53:06 +01'00'

TELECYL, S.A.

ANEXO I
INFORME DE LA SUBDIRECCIÓN DE APOYO Y RELACIONES INSTITUCIONALES

**INFORME Y PROPUESTA DE LA MODIFICACIÓN DEL
CONTRATO N.º 194/2024 RELATIVO AL SERVICIO DE
COORDINACIÓN DE ACTIVIDADES INSTITUCIONALES DE
CANAL ISABEL II, S.A., M.P.**

MODIFICACIÓN N.º 1

Relaciones Externas

Subdirección de Apoyo y Relaciones Institucionales

ÍNDICE

| | |
|---|----------|
| MODIFICACIÓN N.º 1 | 1 |
| 1. Objeto | 3 |
| 2. Causa y justificación de la modificación del contrato: interés público de la modificación | 3 |
| 3. Análisis del cumplimiento de los requisitos necesarios para modificar el contrato | 3 |
| 3. 2 Introducción de las variaciones estrictamente indispensables | 5 |
| 3. 3 Análisis de las condiciones establecidas en el artículo 205.2 de la LCSP | 5 |
| 3. 4 Audiencia al redactor del especificaciones técnicas | 6 |
| 3. 5 Consentimiento del contratista y determinación de los precios contradictorios | 6 |
| 4. Intervención de la Subdirección de Contratación | 6 |
| 5. Propuesta de modificación | 6 |

1. Objeto

El objeto del presente documento es:

- a. El informe sobre la modificación nº 1 del contrato n.º 194/2024 “SERVICIO DE COORDINACIÓN DE ACTIVIDADES INSTITUCIONALES DE CANAL ISABEL II, S.A., M.P. no prevista en la documentación que rige la licitación debido a la necesidad de incorporar las unidades no previstas en dicha documentación que se indican a continuación:
 1. Creación de un microsite específico bajo el subdominio *175aniversario.canaldeisabelsegunda.es* para difundir las distintas acciones que se llevarán a cabo con motivo de la conmemoración del 175 aniversario de Canal de Isabel II S.A., M.P.
- b. Recabar informe de la Subdirección de Contratación sobre la conformidad a Derecho de dicha modificación con carácter previo a su aprobación por parte del Consejero Delegado, órgano competente para acordar la modificación en virtud de las facultades concedidas a su favor por el Consejo de Administración de Canal de Isabel II S.A., M.P. al suponer dicha modificación aumento del precio del contrato.

2. Causa y justificación de la modificación del contrato: interés público de la modificación

Tras la adjudicación y puesta en marcha del contrato 194/2024, y en el marco de la ejecución de los trabajos descritos en el pliego, se ha identificado la necesidad de incorporar la creación de un microsite específico bajo el subdominio **175aniversario.canaldeisabelsegunda.es**, recurso digital imprescindible para centralizar y difundir las distintas acciones previstas con motivo de la conmemoración del 175 aniversario de Canal de Isabel II, constituyendo un elemento estratégico de comunicación institucional.

La creación de este microsite permitirá disponer de un espacio web independiente con arquitectura y diseño adaptados a la temática conmemorativa, garantizar la escalabilidad y flexibilidad necesarias para integrar contenidos multimedia, agenda de eventos, noticias y documentación histórica, optimizar la experiencia de usuario mediante una navegación diferenciada del portal corporativo principal y facilitar la gestión y actualización autónoma de contenidos. La modificación atiende a razones de interés público en tanto que refuerza la transparencia y la difusión de las actividades conmemorativas asegurando el acceso a la información, contribuye a poner en valor los 175 años de historia, evolución y servicio público de Canal de Isabel II y favorece la participación ciudadana y la proyección de la entidad.

3. Análisis del cumplimiento de los requisitos necesarios para modificar el contrato

Al tratarse de una modificación no prevista en el PCAP, debe analizarse el cumplimiento de los requisitos previstos en los artículos 205 y 207 de la ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, por la que se transponen al ordenamiento jurídico español las Directivas del Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014 (LCSP) y debe recabarse el preceptivo consentimiento del contratista.

3.1 Circunstancias que justifican la modificación

El artículo 205.2 de la LCSP establece las siguientes circunstancias que permiten realizar una modificación no prevista en el PCAP, siempre que se limite a introducir las variaciones estrictamente indispensables para responder a la causa objetiva que la haga necesaria:

*c) Cuando las modificaciones no sean sustanciales. En este caso se tendrá **que justificar especialmente la necesidad de las mismas, indicando las razones por las que esas prestaciones no se incluyeron en el contrato inicial.***

*Una modificación de un contrato se considerará sustancial cuando tenga como resultado un contrato de naturaleza materialmente diferente al celebrado en un principio. En cualquier caso, una modificación **se considerará sustancial cuando se cumpla una o varias de las condiciones siguientes:***

1.º Que la modificación introduzca condiciones que, de haber figurado en el procedimiento de contratación inicial, habrían permitido la selección de candidatos distintos de los seleccionados inicialmente o la aceptación de una oferta distinta a la aceptada inicialmente o habrían atraído a más participantes en el procedimiento de contratación.

En todo caso se considerará que se da el supuesto previsto en el párrafo anterior cuando la obra o el servicio resultantes del proyecto original o del pliego, respectivamente, más la modificación que se pretenda, requieran de una clasificación del contratista diferente a la que, en su caso, se exigió en el procedimiento de licitación original.

2.º Que la modificación altere el equilibrio económico del contrato en beneficio del contratista de una manera que no estaba prevista en el contrato inicial.

En todo caso se considerará que se da el supuesto previsto en el párrafo anterior cuando, como consecuencia de la modificación que se pretenda realizar, se introducirían unidades de obra nuevas cuyo importe representaría más del 50 por ciento del presupuesto inicial del contrato.

3.º Que la modificación amplíe de forma importante el ámbito del contrato.

En todo caso se considerará que se da el supuesto previsto en el párrafo anterior cuando:

- (i) El valor de la modificación suponga una alteración en la cuantía del contrato que exceda, aislada o conjuntamente, del 15 por ciento del precio inicial del mismo, IVA excluido, si se trata del contrato de obras o de un 10 por ciento, IVA excluido, cuando se refiera a los demás contratos, o bien que supere el umbral que en función del tipo de contrato resulte de aplicación de entre los señalados en los artículos 20 a 23 de la LCSP.*
- (ii) Las obras, servicios o suministros objeto de modificación se hallen dentro del ámbito de otro contrato, actual o futuro, siempre que se haya iniciado la tramitación del expediente de contratación.*

Pues bien, de conformidad con lo dispuesto en el apartado 2 del presente informe, la circunstancia que justifica la incorporación de las unidades referidas en el apartado 1 responde al supuesto establecido en el art. 205.2 c) de la LCSP. En efecto, ya que esta modificación es necesaria para el correcto desarrollo del aniversario y del objeto de contrato (las actividades institucionales) para poder reforzar la transparencia y la difusión de las actividades conmemorativas asegurando el acceso a la información, contribuyendo a poner en valor los 175 años de historia, evolución y servicio público de Canal de Isabel II y favoreciendo la participación ciudadana y la proyección de la entidad.

Dicha prestación no se incluyó en el contrato inicial porque se trata de una necesidad que surgió una vez iniciados los trabajos de coordinación de las actividades institucionales. En ese momento se evidenció que era imprescindible contar con un microsite específico que permitiera centralizar de manera uniforme toda la información, documentación y materiales relacionados con el próximo aniversario de Canal de Isabel II. Esta necesidad no pudo preverse con anterioridad, ya que responde a un requerimiento de carácter técnico derivado directamente de la organización de las actividades.

3. 2 Introducción de las variaciones estrictamente indispensables

Se hace constar que, de acuerdo con lo dispuesto en el artículo 205.1 b) de la LCSP, la modificación se limita a introducir las variaciones estrictamente indispensables para responder a la causa objetiva que la hace necesaria.

3. 3 Análisis de las condiciones establecidas en el artículo 205.2 de la LCSP

Se hace constar que se cumple lo dispuesto en la letra c) del artículo 205.2 de la LCSP. En particular, se pone de manifiesto que:

Dicha modificación es necesaria ya que, a raíz del comienzo de los trabajos de la coordinación de actividades institucionales, se ha evidenciado la necesidad de utilizar un microsite específico bajo el subdominio 175aniversario.canaldeisabelsegunda.es para difundir las distintas acciones que se llevarán a cabo con motivo de la conmemoración del 175 aniversario de Canal de Isabel II S.A., M.P. que no estaba contemplado en el contrato inicial al haber derivado de manera inesperada de estas actuaciones y cuya función es necesario para finalizar satisfactoriamente la coordinación de los trabajos contemplados en los pliegos.

Además, se debe explicar que no concurre ninguna de las siguientes circunstancias:

1.º Que la modificación introduzca condiciones que, de haber figurado en el procedimiento de contratación inicial, habrían permitido la selección de candidatos distintos de los seleccionados inicialmente o la aceptación de una oferta distinta a la aceptada inicialmente o habrían atraído a más participantes en el procedimiento de contratación.

2.º Que la modificación altere el equilibrio económico del contrato en beneficio del contratista de una manera que no estaba prevista en el contrato inicial.

3.º Que la modificación amplíe de forma importante el ámbito del contrato, debido a que el valor de la modificación supone una alteración en la cuantía del contrato de un 5,09 %, sin exceder aislada o conjuntamente, el 10 por ciento del precio inicial del mismo, IVA excluido.

A continuación, se representa el comparativo económico respecto a las unidades recogidas en el Pliego de Prescripciones Técnicas que, con la modificación en sus mediciones, suponen la siguiente repercusión presupuestaria:

| | UNIDADES | PRECIO UNITARIO | TOTAL |
|--------------------|----------|-----------------|-------------|
| Creación microsite | 1 | 18.000,00 | 18.000,00 |
| TOTAL IVA EXCLUIDO | | | 18.000,00 € |
| TOTAL IVA | | | 3.780,00 € |
| TOTAL IVA INCLUIDO | | | 21.780,00 € |

La introducción de las unidades supone el 5,09% del presupuesto e incrementa el precio del contrato debido a las razones anteriormente comentadas.

3. 4 Audiencia al redactor del especificaciones técnicas

No ha resultado necesario proceder, de conformidad con lo dispuesto en el artículo 207.2 de la LCSP, a dar audiencia al redactor de las especificaciones técnicas, toda vez que las especificaciones técnicas han sido redactadas por CANAL DE ISABEL II, S.A., M.P.

3. 5 Consentimiento del contratista y determinación de los precios contradictorios

Se ha procedido, en un plazo no inferior a tres días, a recabar el preceptivo consentimiento del contratista TELECYL, S.A, para incorporar las nuevas unidades referidas en el apartado 1.

El contratista ha manifestado en el documento que se adjunta como Anexo I su consentimiento a incorporar al contrato las nuevas unidades referidas en el apartado 1. En dicho documento se hacen constar los precios de las nuevas unidades que han acordado contradictoriamente CANAL DE ISABEL II, S.A., M.P. y el contratista.

| <u>Código</u> | <u>Ud.</u> | <u>Descripción</u> | <u>Importe en letra</u> | <u>Importe</u> |
|---------------|------------|--------------------|-------------------------|----------------|
| - | 1 | Creación microsite | Dieciocho mil euros | 18.000,00 € |

Para la generación del precio que se plasma en este informe se han contrastado con valores reales en base al precio de mercado.

4. Intervención de la Subdirección de Contratación

El presente informe se remitirá a la Subdirección de Contratación para que, según las Instrucciones Regulatorias de la Ejecución de los Contratos aprobadas por el Consejero Delegado el 2 de junio de 2022, se pronuncie sobre la conformidad a Derecho de la modificación propuesta con carácter previo a su aprobación por parte del Consejero Delegado, órgano competente para acordar la modificación en virtud de las facultades concedidas a su favor por el Consejo de Administración de CANAL DE ISABEL II, S.A., M.P., al suponer dicha modificación aumento del precio del contrato.

5. Propuesta de modificación

Cumplíndose los requisitos establecidos en los artículos 205.2 c) y 207 de la LCSP se propone la modificación nº 1 del Contrato 194/2024 de “SERVICIO DE COORDINACIÓN DE ACTIVIDADES INSTITUCIONALES DE CANAL ISABEL II, S.A., M.P.”

Firmado electronicamente por: Fernando Arlandis Pérez
En la fecha y hora 07.01.2026 15:04:29 CET

Fernando Arlandis Pérez
Subdirector de Apoyo y Relaciones Institucionales.

ANEXO I Consentimiento del contratista

CONSENTIMIENTO DEL CONTRATISTA
A CANAL DE ISABEL II, S.A., M.P.

CONTRATO N.º 194/2024: SERVICIO DE COORDINACIÓN DE ACTIVIDADES INSTITUCIONALES DE CANAL ISABEL II, S.A., M.P.

Asunto: CONSENTIMIENTO A MODIFICACIÓN CONTRACTUAL por parte de TELECYL, S.A.

Tras la adjudicación y puesta en marcha del contrato N° 194/2024, y en el marco de la ejecución de los trabajos descritos en el pliego, se ha identificado la necesidad de incorporar la creación de un microsite específico bajo el subdominio 175aniversario.canaldeisabelsegunda.es, recurso digital imprescindible para centralizar y difundir las distintas acciones previstas con motivo de la conmemoración del 175 aniversario de Canal de Isabel II, constituyendo un elemento estratégico de comunicación institucional.

A) REQUISITOS TÉCNICOS.

Esta propuesta apostará por un diseño limpio y minimalista, donde la información se presente de forma clara y ordenada. El diseño utilizará la paleta presentada en la línea gráfica de la identidad del 175 aniversario tonos azules y verdes. Las imágenes protagonistas reflejarán la conexión entre naturaleza, tecnología e infraestructura, transmitiendo la esencia de Canal Isabel II como una empresa innovadora y comprometida con el futuro que impulsa.

Como texto principal “El impulso del agua” junto con el nombre “Canal Isabel II” en la transición entre una sección y otra. Presenta la identidad de la marca y su propósito. Elementos visuales: Se incluirá un lottie para mejorar la experiencia de usuario que indique el desplazamiento de la pantalla.

Habrán diferentes secciones, destacando la sección “175 años impulsando el futuro de Madrid” destaca la experiencia y el legado de la empresa, generando confianza al mostrar la solidez y relevancia histórica de Canal Isabel II y posicionándola como una entidad con tradición y compromiso. Con una imagen representativa, que introduce la línea temporal. Esta sección incluirá contenidos segmentados que explican cada año, combinando texto e imágenes para facilitar la lectura y comprensión, ofreciendo información clara y atractiva para el usuario. El apartado mostrará hitos históricos mediante una línea temporal que acompañe todo el recorrido y se complementa con un bloque dedicado a la agenda de próximos eventos. Finalmente, mediante imágenes panorámicas y mensajes como “175 años”, se reforzarán los valores institucionales y la conexión con el público.

En conclusión se prioriza la usabilidad y la lectura fácil. Las secciones estarán organizadas en bloques simples con tipografía clara y espacios amplios. Comenzando con un encabezado impactante que presente la identidad de la marca, seguido de secciones que destacan los 175 años de trayectoria, proyectos emblemáticos y próximos eventos. Incluye un bloque dedicado a la innovación y la tecnología, reforzando la visión de futuro y otro a las últimas noticias. El diseño busca equilibrio entre lo institucional y lo moderno, ofreciendo una navegación clara y visualmente atractiva.

Para la puesta en marcha de dicho microsite, se deberá llevar a cabo la implementación de medidas antiDDoS para proteger la página en caso de ataque de tipo DDoS (volumétrico, de protocolo y aplicación), por ello debe contemplar los siguientes aspectos:

- Consideraciones de seguridad para el diseño y construcción de aplicaciones web para Canal de Isabel II, Sociedad Anónima, M.P.
- Requisitos de seguridad para la confección del Microsite (aspectos técnicos de seguridad mínimos a tener en cuenta).
- Guía de seguridad en entornos y aplicaciones web.

B) AUTORIZACIÓN DE USO DE DOMINIO WEB Y CESIÓN DE CERTIFICADO DEL MICROSITE 175aniversario.canaldeisabelsegunda.es

Además, se deberá firmar la siguiente autorización de uso de dominio web y cesión de certificado del microsite 175aniversario.canaldeisabelsegunda.es

En relación con el modificado del contrato de referencia, se adjuntan las condiciones que deben introducirse en el mismo objeto de regular autorización de uso y cesión del certificado del dominio referenciado.

12.- Autorización de uso de dominio web

12.1 - Se otorga autorización de uso del dominio "175aniversario.canaldeisabelsegunda.es", a favor del adjudicatario para los exclusivos fines de la ejecución del Contrato, sin perjuicio de la posibilidad de subcontratación de ciertas tareas siempre que se realice al amparo de lo dispuesto en el Contrato.

12.2 - La autorización entrará en vigor en la fecha en que se formalice el contrato, quedando su duración condicionada a la vigencia del Contrato.

Finalizada la duración de la autorización de uso del dominio, Canal de Isabel II, S.A., M.P. redireccionará los dominios a sus DNS corporativos y revertirá las configuraciones indicadas por el contratista, no pudiendo el autorizado tener acceso ni reservarse facultad alguna sobre dichos dominios.

12.3 - El adjudicatario deberá estar adherido a las buenas prácticas internacionales en lo relativo al envío de correos masivos (bulk mailing).

12.4 - El adjudicatario, para minimizar el riesgo de que el dominio "175aniversario.canaldeisabelsegunda.es", titularidad de Canal de Isabel II, S.A., M.P. sea incluido dentro de listas negras de SPAM:

- a) Realizará todas las tareas, acciones y gestiones necesarias tanto en sus sistemas de información como en los que estén bajo su responsabilidad, así como en aquellos servicios de terceros que sean necesarios para la realización de los trabajos contemplados dentro del alcance del Contrato.
- b) Proporcionará, de forma clara, completa y precisa, toda la información técnica necesaria acerca de las configuraciones a realizar en los sistemas de información bajo responsabilidad de Canal de Isabel II, S.A., M.P.
- c) Realizará las gestiones que correspondan de revisión del contenido de los mensajes, fraccionamiento de los envíos, numeración contratos de seguimiento, etc.

12.5 - El adjudicatario dispondrá de un servicio de monitorización que permita comprobar si el dominio "175aniversario.canaldeisabelsegunda.es", titularidad de Canal de Isabel II, S.A., M.P., es incluido dentro de listas negras de SPAM. En tal caso, avisará a la mayor brevedad posible a Canal de Isabel II, S.A., M.P. de esta situación y de las listas negras en las que está incluido el dominio y prestará asistencia técnica a Canal de Isabel II, S.A., M.P. en las gestiones que Canal de Isabel II, S.A., M.P., como propietario del dominio, tenga que realizar para tramitar la exclusión del dominio de todas las listas negras en las que esté incluido.

12.6 - El adjudicatario realizará todas las tareas y acciones necesarias para evitar un potencial abuso del servicio contratado por Canal de Isabel II, S.A., M.P. por parte de terceros impacte negativamente en el servicio que el

contratista presta a Canal de Isabel II, S.A., M.P. En todo caso, en cuanto a los requisitos de seguridad, se estará asimismo a lo dispuesto en el PPT del Contrato.

12.7. - El adjudicatario dispondrá de un servicio de anonimización de correos electrónicos mediante la correcta configuración de los distintos protocolos de envío de correos electrónicos con el fin de evitar que las direcciones IP utilizadas puedan acabar en una lista negra.

12.8. - La presente autorización se otorga dejando a salvo la titularidad del dominio "175aniversario.canaldeisabelsegunda.es", que corresponde a Canal de Isabel II, S.A., M.P. y sin perjuicio de derechos de terceros. La presente autorización no podrá ser invocada para excluir o disminuir la responsabilidad civil o penal en la que hubiere incurrido el titular de la presente autorización en el ejercicio de las actuaciones objeto de la misma. No se permite remitir emails sin utilización del campo oculto.

13.- Cesión del Certificado de autenticación web

13.1. - Canal de Isabel II, S.A., M.P. cede el uso del certificado digital del dominio "175aniversario.canaldeisabelsegunda.es". Dicha cesión es de carácter exclusivo e intransferible, salvo en lo relativo al alojamiento del dominio mencionado, que podrá ser realizado de conformidad con las instrucciones de Canal de Isabel II, S.A., M.P. y en virtud de lo dispuesto en el Contrato, previa comunicación a Canal de Isabel II, S.A., M.P.

13.2. - De conformidad con el Reglamento (UE) Nº 910/2014, un certificado de autenticación de sitio web es una declaración que permite autenticar un sitio web y vincula el sitio web con la persona física o jurídica a quien se ha expedido el certificado. El certificado se empleará para comprobar que la clave pública que presenta Canal de Isabel II, S.A., M.P. en la página web "175aniversario.canaldeisabelsegunda.es", pertenece efectivamente a Canal de Isabel II, S.A., M.P.

13.3. - El certificado identifica al titular del dominio como persona jurídica. Sin perjuicio de la posible subcontratación de ciertas tareas en virtud de lo dispuesto en el Contrato, el adjudicatario no podrá transferir la utilización del certificado a otros sistemas informáticos o a otras entidades distintas.

13.4. - El adjudicatario será el responsable del cumplimiento del contenido del presente acuerdo. En cuanto a los requisitos de seguridad, se estará asimismo a lo dispuesto anexo de la modificación del contrato.

13.5. - En ningún caso, Canal de Isabel II, S.A., M.P. será responsable ante el adjudicatario o terceras partes, de cualquier daño directo o indirecto, incluida pérdida de beneficios, pérdida de ahorro o cualquier tipo de perjuicio surgido como consecuencia de la utilización normal o anormal de los certificados cedidos, siendo el uso del mismo a riesgo y ventura del contratista.

13.6. - El adjudicatario se compromete a introducir en todo acuerdo que firme con tercero relacionado directa o indirectamente con el uso del certificado, las cláusulas o estipulaciones que eximan de toda responsabilidad a Canal de Isabel II, S.A., M.P. en los términos expresados conforme lo dispuesto en las presentes Condiciones. El contratista indemnizará y mantendrá indemne a Canal de Isabel II, S.A., M.P. por cualquier daño que ésta pudiera sufrir por el cumplimiento total, parcial o defectuoso de las obligaciones asumidas en este documento y en base a toda reclamación dirigida contra ella por cualquier tercero con el que el contratista hubiera contratado. El contratista acepta y se compromete a aceptar con las condiciones impuestas por el prestador de servicios de confianza.

A continuación, se representa la partida presupuestaria:

| Ud. | Descripción | Importe en letra | Importe |
|-----|--------------------|---------------------|-------------|
| 1 | Creación microsite | Dieciocho mil euros | 18.000,00 € |

C) CONSENTIMIENTO.

Que TELECYL, S.A., en sede del trámite de audiencia que se confiere en su calidad de contratista de los referidos servicios, manifiesta expresamente su consentimiento a la modificación de este Contrato número 194/2024 en los términos y condiciones indicados anteriormente.

Y para que surta los efectos oportunos, en la tramitación de la Modificación del contrato N.º 194/2024, se firma el presente escrito y SOLICITA que, tras los trámites legales oportunos, sea tenido en consideración en la tramitación de la Modificación del Contrato de referencia.

TELECYL, S.A
CONTRATISTA

Fdo: 12404709 G ISABEL MATEOS (R: A47310941)
Firmado digitalmente por 12404709G ISABEL MATEOS (R: A47310941)
Fecha: 2026.01.07 11:19:08 +01'00'

ANEXO II

Resumen de la modificación a efectos de su publicación en el perfil del contratante
por la Subdirección de Contratación

| |
|--|
| Licitación 194/2024 SERVICIO DE COORDINACIÓN DE ACTIVIDADES INSTITUCIONALES DE CANAL ISABEL II, S.A., M.P. |
| Nif del contratista: A47310941 |
| Nombre o razón social del contratista: TELECYL, SA |
| Importe modificación (sin IVA): 18.000,00 euros |
| Importe modificación (con IVA): 21.780,00 euros |
| Variación plazo de ejecución: Sin variación del plazo del contrato |
| % que supone la modificación respecto al precio inicial del contrato: 5,09 % |
| Justificación de la modificación: dicha modificación es necesaria ya que, a raíz del comienzo de los trabajos de la coordinación de actividades institucionales, se ha evidenciado la necesidad de utilizar un microsite específico bajo el subdominio 175aniversario.canaldeisabelsegunda.es para difundir las distintas acciones que se llevarán a cabo con motivo de la conmemoración del 175 aniversario de Canal de Isabel II S.A., M.P. que no estaba contemplado en el contrato inicial al haber derivado de manera inesperada de estas actuaciones y cuya función es necesario para finalizar satisfactoriamente la coordinación de los trabajos contemplados en los pliegos. |
| Artículo de la normativa en que se basa la modificación: 205.2 letra c) de la LCSP |



**CONSIDERACIONES DE SEGURIDAD PARA
EL DISEÑO Y CONSTRUCCIÓN DE
APLICACIONES WEB PARA CANAL DE
ISABEL II, SOCIEDADA ANÓNIMA, M.P.**

Área: Seguridad Informática
Estado: Aprobado
Versión: v1.1
Clasificación: Difusión Limitada
Fecha de creación: 29.11.2011
Fecha de revisión: 30.11.2023

I. HISTORIAL DE CAMBIOS.

| Fecha | Versión | Nombre | Detalles |
|------------|---------|-------------------|--|
| 29.11.2010 | 0.1 | Alberto Escribano | Versión inicial |
| 16.12.2010 | 0.2 | Alberto Escribano | Se completan las metodologías de pruebas de seguridad en el apartado VI |
| 07.11.2011 | 0.3 | Alberto Escribano | Se completan aspectos del apartado V (administración de sesiones) |
| 18.11.2011 | 0.4 | Alberto Escribano | Se añade el apartado VII |
| 12.01.2012 | 0.5 | Alberto Escribano | Se completan aspectos del apartado V (control de procesamiento interno) |
| 18.10.2012 | 0.6 | Alberto Escribano | Se completan aspectos del apartado V (validación de datos de entrada) |
| 01.10.2017 | 0.7 | Alberto Escribano | Actualización IVC Actualización denominación razón social Canal de Isabel II, S.A. Actualización aspectos del apartado VI (validación de una aplicación web desde el punto de vista de la seguridad) |
| 04.11.2017 | 0.8 | Alberto Escribano | Se incluyen las cabeceras de seguridad (monitorización CERTSI) |
| 20.03.2018 | 0.9 | Alberto Escribano | Correcciones menores en la redacción |
| 13.12.2018 | 1.0 | Alberto Escribano | Se añaden consideraciones de seguridad para Google Analytics |
| 13.04.2020 | 1.1 | Alberto escribano | Correcciones menores en la redacción Actualización del uso de TLS 1.2 o superior en la parte del cifrado, utilizando siempre suites de cifrado robustas (ni débiles ni vulnerables). |
| 24.08.2023 | 1.2 | Alberto Escribano | CVSS V3.x Referrer-Policy: strict-origin-when-cross-origin Pragma: no-cache |
| 30.11.2023 | 1.3 | Alberto Escribano | Inclusión de las suites de cifrado Inclusión de la referencia a componentes de terceros |

II. TABLA DE CONTENIDOS.

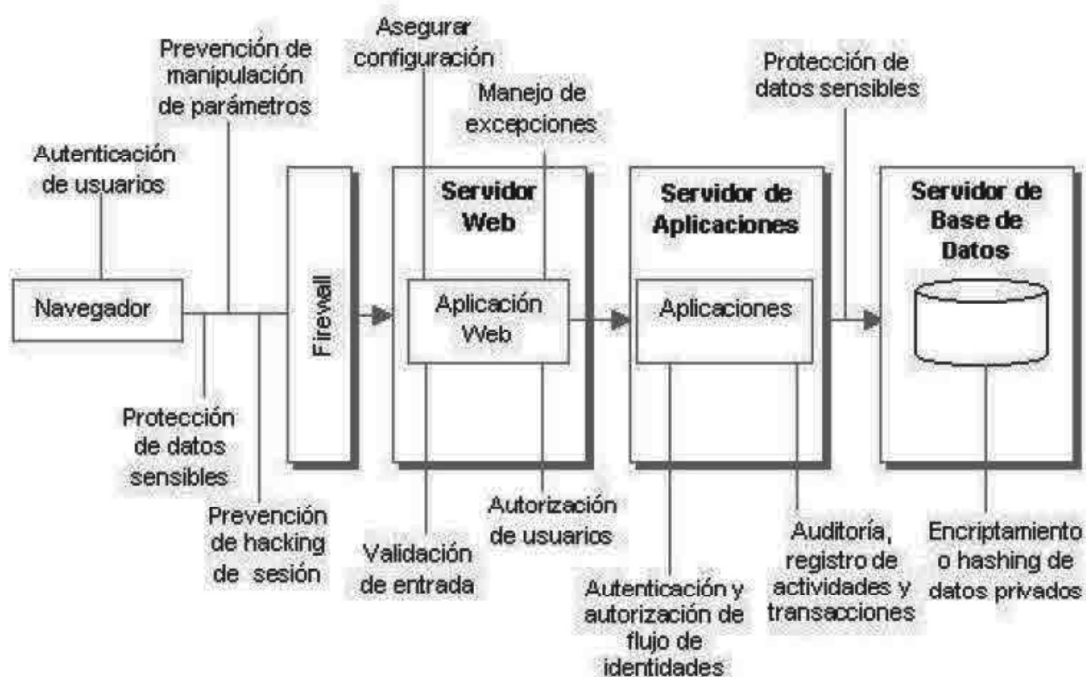
| | | |
|--------------------|---|------------------|
| <u>I.</u> | <u>HISTORIAL DE CAMBIOS.....</u> | <u>2</u> |
| <u>II.</u> | <u>TABLA DE CONTENIDOS.....</u> | <u>3</u> |
| <u>III.</u> | <u>INTRODUCCIÓN.</u> | <u>4</u> |
| <u>IV.</u> | <u>CONSIDERACIONES DE SEGURIDAD PARA EL DISEÑO DE UNA APLICACIÓN WEB.....</u> | <u>5</u> |
| <u>V.</u> | <u>CONSIDERACIONES DE SEGURIDAD Y VULNERABILIDADES ASOCIADAS.....</u> | <u>6</u> |
| <u>VI.</u> | <u>VALIDACIÓN DE UNA APLICACIÓN WEB DESDE EL PUNTO DE VISTA DE LA SEGURIDAD.....</u> | <u>9</u> |
| <u>VII.</u> | <u>CRONOGRAMA PARA LAS AUDITORÍAS DE SEGURIDAD.....</u> | <u>10</u> |

III. INTRODUCCIÓN.

Las aplicaciones Web presentan complejos aspectos de seguridad que deben ser cubiertos tanto a nivel de arquitectura y diseño como a nivel de desarrollo y construcción. Las aplicaciones Web más estables, seguras y resistentes a la intrusión son aquellas en las que los aspectos de seguridad se tuvieron en cuenta en todas las etapas del proyecto.

IV. CONSIDERACIONES DE SEGURIDAD PARA EL DISEÑO DE UNA APLICACIÓN WEB.

Es necesario considerar diferentes aspectos de seguridad existentes en cada parte de la arquitectura de una aplicación Web:



Esto se especifica a continuación en una tabla que relaciona las distintas consideraciones de seguridad con las vulnerabilidades asociadas.

V. CONSIDERACIONES DE SEGURIDAD Y VULNERABILIDADES ASOCIADAS.

| Consideración de seguridad | Vulnerabilidades asociadas |
|----------------------------------|--|
| Validación de datos de entrada | <p>La aplicación no está configurada para valores de entrada codificados, internacionalizados o en Unicode, no está definido un conjunto válido de caracteres, no se comprueban:</p> <ul style="list-style-type: none"> a) las longitudes de las cadenas de entrada b) los datos de entrada provenientes de variables de entorno del sistema c) los campos obligatorios d) el uso de valores por defecto o establecidos (listas que contenga sólo las entradas permitidas) en lugar entradas que se puedan realizar libremente por el usuario e) la comprobación de parámetros vacíos f) la comprobación del formato de los datos de entrada para aceptar sólo los formatos aceptados y evitar la inserción de cadenas de texto especialmente diseñadas/manipuladas o maliciosas en <i>query strings</i> (uso de <i>mime-types</i>, <i>content-type</i>, <i>magic numbers</i>, etc.) g) la comprobación del <i>file size</i> <p>La incorrecta validación en la entrada de datos a un sistema o aplicación aumenta el riesgo de realización de ataques al sistema a través de vulnerabilidades de tipo <i>HTTP Request Smuggling</i>, <i>heap overflow</i> (<i>use-after-free</i>, <i>double free</i>, <i>dereference after free</i>), <i>off-by-one</i>, <i>format string</i>, <i>integer overflows/underflows</i>, <i>memory leaks</i>, <i>buffer overflow</i>, etc.</p> |
| Control de procesamiento interno | Condiciones de carrera (<i>race conditions</i>). |
| Autenticación | Suplantación de identidad, <i>password cracking</i> , elevación de privilegios y accesos no autorizados. |
| Autorización | Acceso a datos confidenciales o restringidos, ejecución de operaciones no autorizadas. |
| Administración de configuración | Acceso no autorizado a consolas de administración, alteración de datos de configuración, acceso no autorizado a cuentas de usuario y perfiles de cuentas de usuarios, etc. |
| Datos sensibles | <p>Acceso a información confidencial o por terceros no autorizados.</p> <p>Pérdida de integridad de los datos.</p> <p>Ejemplos:</p> <ul style="list-style-type: none"> • Acceso a la estructura del sitio web (403 Forbidden) • Enlaces de terceros <code>target="_blank"</code> sin el atributo <code>rel="noopener noreferrer"</code> |

| | |
|-------------------------------------|---|
| Administración de sesiones | <p>Captura de identificadores de sesión. Tiempo excesivo de expiración de la sesión. Ejemplos:</p> <ul style="list-style-type: none"> • Cookies sin los atributos "HttpOnly", "Secure" • Cookies persistentes en lugar de cookies temporales de un solo uso • Configuración insegura de "crossdomain.xml" |
| Cifrado | <p>Uso prioritario del cifrado TLS 1.2 o superior en toda la aplicación para proteger el acceso a los datos (datos personales, datos confidenciales, credenciales de cuentas de usuario, etc.).</p> |
| Manipulación de parámetros | <p>Ejecución de comandos, elevación de privilegios, denegación de servicios (DoS y DDoS), etc.</p> |
| Gestión de excepciones | <p>Denegación de servicio y acceso a información específica de los sistemas base (sistema operativo, servidor web y de aplicaciones, base de datos, etc.). Ejemplos:</p> <ul style="list-style-type: none"> • Versiones concretas de servidores web, aplicación, componentes, etc. • Errores internos del servidor con volcado de pila |
| Auditoría y registro de actividades | <p>Fallos en el registro de pruebas de intrusión, acciones realizadas por el intruso y dificultades para diagnosticar problemas</p> |
| Componentes de terceros | <p>Uso de componentes de terceros fuera de soporte y/o vulnerables (jQuery, Bootstrap, etc.)</p> |

Uso de cabeceras de seguridad en los servidores web que alberguen *sites* o información de Canal de Isabel II

Debido a que Canal de Isabel II es Operador Esencial y sus sistemas están monitorizados por el CCN-CERT, todos los servidores web que sirvan *sites* de Canal de Isabel II se configurarán al menos con las siguientes cabeceras de seguridad, a las que aplican las consideraciones indicadas:

- Header set X-Frame-Options DENY | SAMEORIGIN | ALLOW-FROM
 - Consideración: el desarrollador tendrá que elegir el valor más restrictivo que permita que la página web funcione correctamente.
- Header set X-XSS-Protection "1; mode=block"
- Header set X-Content-Type-Options nosniff

Content Security Policy (CSP):

- Header set Content-Security-Policy "default-src 'self'; script-src 'self'; img-src 'self'; media-src 'self'; font-src 'self'; style-src 'self'; object-src 'self|none'"
 - Consideración: partiendo de esta configuración, el desarrollador deberá identificar la configuración más restrictiva posible que permita que la página web funcione correctamente

Si la página utiliza HTTPS, se incluirá HSTS:

- Header always set Strict-Transport-Security "max-age=31536000; includeSubdomains;"
- Referrer-Policy: strict-origin-when-cross-origin

Caché:

- Cache-Control: max-age=31536000, private, no-cache, no-store, must-revalidate
- Pragma: no-cache

Configuración de Google Analytics.

1. Añadir la entrada **`"ga('set', 'forceSSL', true);"`** en el código para que los emisores beacon, en cualquier caso, vayan siempre bajo TLS
2. Explicitar la llamada a **`'https://www.google-analytics.com/analytics.js'`** en lugar de dejar que sea la propia función la que decida según el protocolo de la página desde donde se invoque (`'//www.google-analytics.com/analytics.js'`)

VI. VALIDACIÓN DE UNA APLICACIÓN WEB DESDE EL PUNTO DE VISTA DE LA SEGURIDAD.

Para poder validar correctamente una aplicación Web, desde el punto de vista de la seguridad, previamente a su entrega a Canal de Isabel II, S.A. y a su puesta en producción, es necesario confrontarla contra el estándar de buenas prácticas de seguridad UNE-ISO/IEC 27002 en su publicación más actual, a través de la utilización de metodologías de pruebas de seguridad en sus últimas versiones publicadas:

Para Sistemas Operativos y Servicios:

1. OSSTM (Open Source Security Testing Methodology).
2. NIST (National Institute of Standards and Technology).

Para Aplicaciones Web:

1. OWASP (Open Web Application Security Project).
2. CWE (Common Weakness Enumeration).
3. WASC (Web Application Security Consortium).

Para Código Fuente:

1. OWASP (Open Web Application Security Project).
2. ISSAF (Information System Security Assessment Framework).
3. CVSS v3.x (Common Vulnerability Scoring System).

Adicionalmente, es necesario tener en cuenta los requisitos de seguridad establecidas por Canal de Isabel II, S.A. en los pliegos técnicos y administrativos en los que se recogen, a través de la Oficina de Proyectos de Canal de Isabel II, S.A., todos los aspectos necesarios para la realización del proyecto.

Por lo tanto, todo contratista que desarrolle una aplicación Web para Canal de Isabel II, S.A. deberá contrastar su desarrollo contra el estándar de seguridad arriba referenciado a través de su verificación en las pruebas realizadas con las metodologías de comprobación de seguridad antes mencionadas, además de aquellos requisitos de seguridad establecidos por Canal de Isabel II, S.A.

VII. CRONOGRAMA PARA LAS AUDITORÍAS DE SEGURIDAD.

Las auditorías de seguridad deberán planificarse dentro del cronograma de proyecto como tareas asociadas al mismo y con entregables definidos (resultados de las auditorías y tareas de corrección). Es conveniente realizar una auditoría en cuanto existan entregables que puedan ser revisados, lo que permitirá detectar de forma temprana posibles vulnerabilidades y proceder a su resolución con tiempo suficiente.

A la entrega definitiva del proyecto, se realizará la auditoría previa a la puesta en producción, donde se comprobará si se han solucionado vulnerabilidades detectadas con anterioridad y se reportarán aquellas que sigan apareciendo, como no solucionadas o como nuevas. Se abrirá entonces un periodo de resolución de las vulnerabilidades detectadas y se realizará una auditoría de verificación para comprobar que la aplicación entregada está libre de vulnerabilidades conocidas y se puede proceder a la puesta en producción de esta.

Para la realización de las auditorías, es conveniente tener acceso restringido (a través del control de acceso vía direccionamiento IP y autenticación y autorización de usuarios a los paneles o contextos de administración) al aplicativo en su fase de desarrollo y en su fase final de validación, así como en las fases posteriores de verificación de las correcciones. Dichas restricciones para el acceso a la parte administrativa de la aplicación (en caso de que exista) se deberán mantener una vez que el aplicativo esté publicado y en producción.

Aspectos técnicos de seguridad mínimos a tener en cuenta

RD 311/2022 por el que se regula el Esquema Nacional de Seguridad / Evaluación objetiva del requisito en base a los dominios, objetivos de control y controles del anexo A ISO/IEC 27001 (ISO/IEC 27002):

- 9.2.4. Gestión de información confidencial de autenticación de usuarios.
- 9.3.1. Uso de información confidencial para la autenticación.
- 9.4.1. Restricción del acceso a la información.
- 9.4.2. Procedimientos seguros de inicio de sesión.
- 13.1.1. Controles de red.
- 13.1.2. Mecanismos de seguridad asociados a servicios en red.

RD 311/2022 por el que se regula el Esquema Nacional de Seguridad / Evaluación objetiva del requisito en base a los dominios, objetivos de control y controles del anexo A ISO/IEC 27001 (ISO/IEC 27002):

- 9.2.1. Gestión de altas/bajas de usuarios
- 9.2.2. Gestión de los derechos de acceso asignados a usuarios
- 9.2.5. Revisión de los derechos de acceso de los usuarios.
- 9.2.6. Retirada o adaptación de los derechos de acceso

9.4.1. Restricción del acceso a la información

RD 311/2022 por el que se regula el Esquema Nacional de Seguridad / Evaluación objetiva del requisito en base a los dominios, objetivos de control y controles del anexo A ISO/IEC 27001 (ISO/IEC 27002):

- 10.1.1. Política de uso de los controles criptográficos.
- 10.1.2. Gestión de claves criptográficas.

RD 311/2022 por el que se regula el Esquema Nacional de Seguridad / Evaluación objetiva del requisito en base a los dominios, objetivos de control y controles del anexo A ISO/IEC 27001 (ISO/IEC 27002):

- 10.1.1. Política de uso de los controles criptográficos.
- 10.1.2. Gestión de claves criptográficas.

RD 311/2022 por el que se regula el Esquema Nacional de Seguridad / Evaluación objetiva del requisito en base a los dominios, objetivos de control y controles del anexo A ISO/IEC 27001 (ISO/IEC 27002):

- 9.2.4. Gestión de información confidencial de autenticación de usuarios.
- 9.3.1. Uso de información confidencial para la autenticación.
- 9.4.1. Restricción del acceso a la información.
- 9.4.2. Procedimientos seguros de inicio de sesión.
- 13.1.1. Controles de red.
- 13.1.2. Mecanismos de seguridad asociados a servicios en red.

| |
|---|
| <p>RD 311/2022 por el que se regula el Esquema Nacional de Seguridad / Evaluación objetiva del requisito en base a los dominios, objetivos de control y controles del anexo A ISO/IEC 27001 (ISO/IEC 27002):</p> <p>9.2.4. Gestión de información confidencial de autenticación de usuarios.</p> <p>9.3.1. Uso de información confidencial para la autenticación.</p> <p>9.4.1. Restricción del acceso a la información.</p> <p>9.4.2. Procedimientos seguros de inicio de sesión.</p> <p>13.1.1. Controles de red.</p> <p><u>13.1.2. Mecanismos de seguridad asociados a servicios en red.</u></p> |
| <p>RD 311/2022 por el que se regula el Esquema Nacional de Seguridad / Evaluación objetiva del requisito en base a los dominios, objetivos de control y controles del Anexo A ISO/IEC 27001 (ISO/IEC 27002):</p> <p>12.6.1. Gestión de las vulnerabilidades técnicas.</p> <p>12.6.2. Restricciones en la instalación de software</p> <p>18.2.1. Revisión independiente de la seguridad de la información.</p> <p>18.2.2. Cumplimiento de las políticas y normas de seguridad.</p> <p><u>18.2.3. Comprobación del cumplimiento.</u></p> |
| <p>RD 311/2022 por el que se regula el Esquema Nacional de Seguridad / Evaluación objetiva del requisito en base a los dominios, objetivos de control y controles del Anexo A ISO/IEC 27001 (ISO/IEC 27002):</p> <p>12.4.1. Registro y gestión de eventos de actividad</p> <p>Pueden existir requisitos legales adicionales en lo relativo a la conservación de los registros y eventos. Consultar con el DPD.</p> |
| <p>RD 311/2022 por el que se regula el Esquema Nacional de Seguridad / Evaluación objetiva del requisito en base a los dominios, objetivos de control y controles del Anexo A ISO/IEC 27001 (ISO/IEC 27002):</p> <p>12.6.1. Gestión de las vulnerabilidades técnicas.</p> <p>12.6.2. Restricciones en la instalación de software</p> <p>18.2.1. Revisión independiente de la seguridad de la información.</p> <p>18.2.2. Cumplimiento de las políticas y normas de seguridad.</p> <p><u>18.2.3. Comprobación del cumplimiento.</u></p> |
| <p>RD 311/2022 por el que se regula el Esquema Nacional de Seguridad / Evaluación objetiva del requisito en base a los dominios, objetivos de control y controles del Anexo A ISO/IEC 27001 (ISO/IEC 27002):</p> <p>12.1.3 – Capacity management</p> <p>12.4.1 – Event logging</p> <p>14.1 y 14.2 - System acquisition, development and maintenance</p> <p>12.6 - Technical vulnerability management</p> <p>13.1 - Network security management</p> <p>15.1.3 – Information and communication technology supply chain</p> <p>16 - Information security incident management</p> <p><u>17 - Information security aspects of business continuity management</u></p> |
| <p>RD 311/2022 por el que se regula el Esquema Nacional de Seguridad / Evaluación objetiva del requisito en base a los dominios, objetivos de control y controles del Anexo A ISO/IEC 27001 (ISO/IEC 27002):</p> <p>12.1.3 – Capacity management</p> <p>12.4.1 – Event logging</p> <p>14.1 y 14.2 - System acquisition, development and maintenance</p> <p>12.6 - Technical vulnerability management</p> <p>13.1 - Network security management</p> <p>15.1.3 – Information and communication technology supply chain</p> <p>16 - Information security incident management</p> <p><u>17 - Information security aspects of business continuity management</u></p> |
| <p>RD 311/2022 por el que se regula el Esquema Nacional de Seguridad / Evaluación objetiva del requisito en base a los dominios, objetivos de control y controles del Anexo A ISO/IEC 27001 (ISO/IEC 27002):</p> <p>12.1.3 – Capacity management</p> <p>12.4.1 – Event logging</p> <p>14.1 y 14.2 - System acquisition, development and maintenance</p> <p>12.6 - Technical vulnerability management</p> <p>13.1 - Network security management</p> <p>15.1.3 – Information and communication technology supply chain</p> <p>16 - Information security incident management</p> <p><u>17 - Information security aspects of business continuity management</u></p> |

RD 311/2022 por el que se regula el Esquema Nacional de Seguridad / Evaluación objetiva del requisito en base a los dominios, objetivos de control y controles del Anexo A ISO/IEC 27001 (ISO/IEC 27002):

12.1.3 – Capacity management

12.4.1 – Event logging

14.1 y 14.2 - System acquisition, development and maintenance

12.6 - Technical vulnerability management

13.1 - Network security management

15.1.3 – Information and communication technology supply chain

16 - Information security incident management

17 - Information security aspects of business continuity management

RD 311/2022 por el que se regula el Esquema Nacional de Seguridad / Evaluación objetiva del requisito en base a los dominios, objetivos de control y controles del Anexo A ISO/IEC 27001 (ISO/IEC 27002):

13.1.1. Comunicación de eventos en seguridad.

13.1.2. Comunicación de debilidades en seguridad.

13.2.1. Identificación de responsabilidades y procedimientos.

13.2.2. Evaluación de incidentes en seguridad.

13.2.3. Recogida de pruebas.

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.).

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., M.P.

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., M.P. 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). Las recomendaciones para el almacenamiento seguro de contraseñas son:

f.1) Utilizar Argon2id con una configuración mínima de 19 MB de memoria, 2 iteraciones y 1 grado de paralelismo

f.2) Si Argon2id no está disponible, usar sCrypt con un parámetro de coste mínimo de CPU/memoria de 217, un tamaño de bloque de 8 (1024 bytes) y un parámetro de paralelización de 1.

f.3) Para sistemas legacy que usan bcrypt usar un factor de trabajo ≥ 10 , con un límite de contraseña de 72 bytes.

f.4) Si se requiere cumplimiento FIPS-140, sería necesario utilizar PBKDF2 con un factor de trabajo ≥ 600.000 y configurarlo con una función has interna de HMAC-SHA-256 o superior

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) Cuando la naturaleza de la solución del adjudicatario requiera del uso de Servicios Web (WS) que utilicen mensajes de tipo SOAP, se requerirá que estén protegidos a nivel de mensaje, especificando la forma de firmar y el cifrado de los mensajes de tipo SOAP, a través de la especificación WS-Security.

- La integridad y confidencialidad de la información ha de estar garantizada a través del uso de protocolos de transporte seguros (TLS 1.2 o superior) y suites de cifrado robustas (ni débiles ni vulnerables).

Para la autenticación y autorización de los servicios se utilizará SAML 2.0. y WS-Security tokens.

- La integridad, autenticidad y confidencialidad de la información ha de estar garantizada mediante el uso de procesos de firma (XML Signature) y cifrado (XML Encryption) de mensajes.

Debe hacerse uso de una política de seguridad (WS-Policy).

i) Cuando la naturaleza de la solución del adjudicatario requiera del uso de servicios web (WS) que utilicen mensajes de tipo REST, se requerirá que estén convenientemente protegidos implementando, al menos, las siguientes características:

- La integridad y confidencialidad de la información ha de estar garantizada a través del uso de protocolos de transporte seguros (TLS 1.2 o superior) y suites de cifrado robustas (ni débiles ni vulnerables).
- Para la autenticación y autorización de los servicios se utilizarán los estándares OAuth 2.0 y OpenID Connect, permitiendo la emisión de tokens de acceso en formato JWT (RFC 7519).
- La integridad, autenticidad y confidencialidad de la información ha de estar garantizada mediante el uso de tokens JWT (RFC7519) para los procesos de firma (JWS) y cifrado (JWE) de mensajes

j) 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.

k) 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

l) 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

m) El proveedor comunicará inmediatamente a Canal de Isabel II, S.A., M.P. 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

n) El proveedor debe disponer de un Plan de Continuidad del Negocio, para las contingencias que puedan producirse en la prestación de servicio Cloud

o) El proveedor deberá disponer de proceso de devolución de la información propiedad de Canal de Isabel II en caso de resolución del contrato. Adicionalmente deberá aportar las certificaciones oportunas de destrucción segura de toda la información propiedad de Canal de Isabel II, que recogerán, al menos, la siguiente información:

al menos, la siguiente información:

I.Fecha de recogida del material.

II.Personal proveedor encargado de la recogida y transporte.

III.Procedimiento detallado empleado en el borrado/destrucción realizada.

IV.Fecha de la destrucción de la información

p) El proveedor habrá analizado el impacto que puede tener sobre los sistemas que soportan el servicio Cloud un incidente accidental o deliberado que tenga su origen en la cadena de suministro

q) El proveedor del servicio Cloud debe tener activas protecciones Anti-DDoS

S.A., M.P. 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., M.P. 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., M.P. quien a su vez lo remitirá a la Dirección de Seguridad.

Siempre

Siempre, en base a la clasificación de los activos de información dentro del alcance de los servicios cloud objeto de contratación por parte de Canal de Isabel II, S.A., M.P.

Siempre

Siempre

Siempre que:

- exista la posibilidad de integrar la autenticación y/o la autorización del servicio con proveedores de identidad de terceros
- existencia de Web Services / APIs que puedan ser consumidas

Siempre

Siempre

Siempre

Siempre

Siempre

Siempre

Siempre

Siempre

Siempre

· Evidencia del uso protocolos de comunicaciones fuertes, seguros y no vulnerables para proteger la confidencialidad, integridad y disponibilidad de los activos de información propiedad de Canal de Isabel II, S.A., M.P.

· Evidencia de la implantación de medidas de aislamiento y control de acceso (autenticación y autorización) a los activos de información propiedad de Canal de Isabel II, S.A., M.P. para la protección de su confidencialidad, integridad y disponibilidad

· Evidencia de implantación de medidas de seguridad que garanticen el control de acceso y la confidencialidad de los activos de información propiedad de Canal de Isabel II, S.A., M.P.

· Evidencia de la implantación de medidas de seguridad para la protección de los datos de autenticación de los usuarios del servicio con el objeto de proteger la confidencialidad, integridad y disponibilidad de los activos de información propiedad de Canal de Isabel II, S.A., M.P.

· Evidencia de la implantación de medidas de seguridad en la posible integración con proveedores de identidad de terceros y en el mecanismo de autorización de las APIs existentes, para la protección de los datos de autenticación de los usuarios del servicio con el objeto de proteger la confidencialidad, integridad y disponibilidad de los activos de información propiedad de Canal de Isabel II, S.A., M.P.

| |
|--|
| <p>· Evidencia de la implantación de medidas de seguridad adicionales y contrastadas para la protección de las cuentas de los usuarios en el servicio, con el objeto de minimizar el riesgo existente de suplantación, y proteger así la confidencialidad, integridad y disponibilidad de los activos de información propiedad de Canal de Isabel II, S.A., M.P.</p> |
| <p>· Evidencia de que existe y está implementada un gestión de vulnerabilidades que contemple metodologías dedicadas a la protección de aplicaciones web, al menos en los servicios cloud objeto de contratación por Canal de Isabel II, S.A., M.P.</p> |
| <p>· Evidencia de que existe y está implementados sistemas seguros de monitorización continua, correlación y gestión de eventos y alertas, con el objeto de garantizar la identificación y resolución temprana de posibles problemas e incidentes de seguridad que puedan afectar a los activos de información de Canal de Isabel II, S.A., M.P.</p> |
| <p>· Evidencia de que existen y están implementados procedimientos para el mantenimiento, actualización y securización de toda la infraestructura dedicada a la prestación del servicio cloud objeto de contratación por parte de Canal de Isabel II, S.A., M.P., con el objeto de proteger los activos de información propiedad de Canal de Isabel II, S.A., M.P.</p> |
| |
| |
| |

· Evidencia de que existen y están implementadas protecciones anti-DDoS para garantizar la prestación del servicio cloud objeto de contratación por parte de Canal de Isabel II, S.A., M.P.

· Evidencia de que existen y están implementados procedimientos para la comunicación de incidentes de seguridad en toda la infraestructura dedicada a la prestación del servicio cloud objeto de contratación por parte de Canal de Isabel II, S.A., M.P., con el objeto de proteger los activos de información propiedad de Canal de Isabel II, S.A., M.P.

Teniendo en cuenta los riesgos anteriormente mencionados:

· Por medio de ataques conocidos a protocolos de comunicación débiles, inseguros y/o vulnerables, la confidencialidad, integridad y disponibilidad de los activos de información propiedad de Canal de Isabel II, S.A., M.P. almacenados y gestionados en el servicio cloud están en riesgo cierto de poder ser accedidos por terceros no autorizados (directamente o por impersonación de usuarios legítimos a través de la obtención de sus credenciales), de ser modificados y/o eliminados y de no poder ser accedidos.

Teniendo en cuenta los riesgos anteriormente mencionados:

· Posibilidad cierta de accesos no controlados de terceros no autorizados a la información propiedad de Canal de Isabel II, S.A., M.P., que puedan poner en peligro su confidencialidad (acceso por terceros no autorizados, robo de información), integridad (alteración/manipulación de la información) y disponibilidad (eliminación de permisos, borrado de información)

Teniendo en cuenta los riesgos anteriormente mencionados:

· Posibilidad cierta de accesos no controlados de terceros no autorizados a la información propiedad de Canal de Isabel II, S.A., M.P., que puedan poner en peligro su confidencialidad (acceso por terceros no autorizados, robo de información), integridad (alteración/manipulación de la información) y disponibilidad (eliminación de permisos, borrado de información)

Teniendo en cuenta los riesgos anteriormente mencionados:

· Posibilidad cierta de accesos no controlados de terceros no autorizados, por impersonación o suplantación de identidad, a la información propiedad de Canal de Isabel II, S.A., M.P., que puedan poner en peligro su confidencialidad (acceso por terceros no autorizados, robo de información), integridad (alteración/manipulación de la información) y disponibilidad (eliminación de permisos, borrado de información)

Teniendo en cuenta los riesgos anteriormente mencionados:

· Posibilidad de accesos no controlados de terceros no autorizados, por impersonación o suplantación de identidad, a la información propiedad de Canal de Isabel II, S.A., M.P., que puedan poner en peligro su confidencialidad (acceso por terceros no autorizados, robo de información), integridad (alteración/manipulación de la información) y disponibilidad (eliminación de permisos, borrado de información)

| |
|---|
| <p>Teniendo en cuenta los riesgos anteriormente mencionados:</p> <ul style="list-style-type: none">· Posibilidad cierta de accesos no controlados de terceros no autorizados, por impersonación o suplantación de identidad, a la información propiedad de Canal de Isabel II, S.A., M.P., que puedan poner en peligro su confidencialidad (acceso por terceros no autorizados, robo de información), integridad (alteración/manipulación de la información) y disponibilidad (eliminación de permisos, borrado de información) |
| <p>Además de lo anteriormente mencionado:</p> <ul style="list-style-type: none">· Posibilidad cierta de existencia de vulnerabilidades específicas no identificados y, por lo tanto, no gestionadas, que terminen materializándose en incidentes de seguridad que afecten negativamente a la confidencialidad, integridad y disponibilidad de los activos de información propiedad de Canal de Isabel II, S.A., M.P. |
| <p>Teniendo en cuenta los riesgos anteriormente mencionados:</p> <ul style="list-style-type: none">· Posibilidad cierta de ocurrencia de incidentes de seguridad no identificados y, por lo tanto, no gestionados, que terminen materializándose en problemas de seguridad que afecten negativamente a la confidencialidad, integridad y disponibilidad de los activos de información propiedad de Canal de Isabel II, S.A., M.P. |
| <p>Teniendo en cuenta los riesgos anteriormente mencionados:</p> <ul style="list-style-type: none">· Posibilidad cierta de vulnerabilidades, sistemas operativos y software (tanto de las aplicaciones como de la infraestructura) no parcheado ni actualizado, infección por malware en general (virus, troyanos, ransomware, etc.), configuraciones incorrectas o inadecuadas y otros problemas de seguridad no identificados y, por lo tanto, no gestionados, que terminen materializándose en problemas de seguridad que afecten negativamente a la confidencialidad, integridad y disponibilidad de los activos de información propiedad de Canal de Isabel II, S.A., M.P. |
| |
| |
| |

Teniendo en cuenta los riesgos anteriormente mencionados:

- Posibilidad cierta de ocurrencia de incidentes de seguridad que afecten negativamente a la disponibilidad del servicio objeto de contratación por parte de Canal de Isabel II, S.A., M.P.

Teniendo en cuenta los riesgos anteriormente mencionados:

- Posibilidad cierta de ocurrencia de incidentes de seguridad materializados, que afecten negativamente a la confidencialidad, integridad y disponibilidad de los activos de información propiedad de Canal de Isabel II, S.A., M.P. y que requiera de notificación oficial de Canal de Isabel II a la autoridad competente o al CSIRT de referencia.