PLIEGO DE PRESCRIPCIONES TÉCNICAS

SERVICIO DE IMPLANTACIÓN DE UN SISTEMA DE MONITORIZACIÓN DEL PUESTO DE TRABAJO Y EXPERIENCIA DIGITAL DE USUARIO PARA CANAL DE ISABEL II, S.A.

CONTRATO Nº: 215/2020

Área: **Planificación, Control y Seguridad**

Canal de Isabel II, S.A. inscrita en el Registro Mercantil de Madrid al Tomo 29.733, Folio 86, Sección 8, Hoja M-534929 e Inscripción 1ª, NIF A86488087, Domicilio Social: C/ Santa Engracia, 125, 28003 Madrid

ÍNDICE

1. INTRODUCCIÓN 3
2. OBJETO DEL PLIEGO 3
3. ALCANCE 3
4. REQUISITOS FUNCIONALES Y TÉCNICOS DE LA SOLUCIÓN 4
5. PRUEBAS DE LOS EQUIPOS 8
6. CONDICIONES DEL SUMINISTRO 9
7. SERVICIO POSTVENTA 9
8. ANS SERVICIO 10

Canal de Isabel II, S.A. inscrita en el Registro Mercantil de Madrid al Tomo 29.733, Folio 86, Sección 8, Hoja M-534929 e Inscripción 1ª, NIF A86488087, Domicilio Social: C/ Santa Engracia, 125, 28003 Madrid

1. INTRODUCCIÓN

El Área de Atención al Usuario da servicio a 2800 equipos y 1.700 portátiles asignados a usuarios, cuyas incidencias y solicitudes se están gestionando de forma reactiva, sin herramientas que ayuden a determinar la causa del fallo, solo actuando en función de los problemas con los que se van encontrando los usuarios.

Con la llegada del teletrabajo, y la futura implantación del portátil como puesto de trabajo, se ha evidenciado la necesidad de disponer de una solución única, para monitorizar los puestos de usuario, independientemente de su localización y poder proporcionar una atención adecuada que garantice al usuario la disponibilidad de los medios de trabajo necesarios para ser productivos.

2. OBJETO DEL PLIEGO

El objeto del presente pliego es la implantación de un sistema software como servicio (SaaS - *Software as a Service*) de gestión del puesto de trabajo, para monitorizar todos los aspectos de las herramientas de productividad en el lugar de trabajo, sea dispositivo, red o aplicación.

El servicio proporcionará, en tiempo real, la visibilidad necesaria para que, a partir de métricas objetivas combinadas con la percepción subjetiva del empleado, permita al Área de Atención al Usuario actuar de forma proactiva y así poder dar un mejor servicio y satisfacer las expectativas de los empleados de Canal.

Se pretende:

- Reducir el número de incidencias de usuario, siendo proactivos.
- Reducir el tiempo de resolución de incidencias.
- Identificar software instalado en equipos de usuario y el uso de este, para licenciar solo aquel software realmente utilizado por el usuario.
- Mantener las versiones al día y unificadas.
- Mejorar el cumplimiento de las políticas de seguridad de TI.
- Aumentar la calidad de servicio de TI.
- Disponer de un sistema de valoración objetivo de la experiencia de empleado.

3. ALCANCE

El alcance del proyecto vendrá establecido por los siguientes servicios:

Servicio S1. Suministro de las Suscripciones al servicio SaaS acorde a los requisitos exigidos.

Servicio S2. Servicios de Implantación la solución, incluyendo Plan de Gestión de Proyecto previo a la realización de los trabajos, presentado por el adjudicatario y aprobado por Canal de Isabel II, S.A.

Servicio S3. Formación de la herramienta. A propuesta del adjudicatario y/o demanda formal por parte de Canal de Isabel II, S.A.

Canal de Isabel II, S.A. inscrita en el Registro Mercantil de Madrid al Tomo 29.733, Folio 86, Sección 8, Hoja M-534929 e Inscripción 1ª, NIF A86488087. Domicilio Social: C/ Santa Engracia, 125, 28003 Madrid

Servicio S4. Soporte y mantenimiento durante el periodo de la suscripción.

4. REQUISITOS FUNCIONALES Y TÉCNICOS DE LA SOLUCIÓN

A continuación, se describen los requisitos que debe cumplir la solución propuesta:

4.1 Requisitos Generales

- El servicio deberá proveerse en modo SaaS - Software as a Service desde una plataforma en Cloud, cuyos servidores estén ubicados en territorio del Espacio Económico Europeo (EEE).

- No se permitirá la subcontratación del tratamiento alguno de la información o cesión de datos con terceros fuera del ámbito establecido para la ubicación de servidores.

- El Sistema será capaz de recoger en tiempo real datos de dispositivos de usuario final y servidores físicos o virtuales basados en Windows y macOS.

- La solución deberá poder comunicar con los usuarios de manera personalizada para enviar notificaciones y recibir feedback sobre la experiencia de usuario.

- El sistema deberá dar la posibilidad de ejecutar acciones remotas sobre los dispositivos finales para automatizar la resolución de incidencias.

4.2 Requisitos técnicos

4.2.1 Requisitos de la Solución

- La solución no debe requerir ningún software de pago de terceros, por ejemplo, bases de datos o middleware. Debe venir integrado en el software.

- La solución debe ser capaz de gestionar y monitorizar más de 4000 puestos de trabajo y 600 servidores concurrentemente.

- La solución debe ser compatible e integrable con Azure AD de Microsoft.

Canal de Isabel II, S.A. inscrita en el Registro Mercantil de Madrid al Tomo 29.733, Folio 86, Sección 8, Hoja M-534929 e Inscripción 1ª, NIF A86488087, Domicilio Social: C/ Santa Engracia, 125, 28003 Madrid

- La solución no debe exigir el remplazo de la infraestructura existente, ni su actualización o ampliación hardware o software.
- La solución debe crear una relación entre los múltiples eventos de los dispositivos: el usuario, el dispositivo, la aplicación, el puerto, el protocolo, el destino y la solicitud web de cada actividad que se produce en los dispositivos.

- La solución debe disponer de un cliente de consulta y analítica de datos con interfaz gráfica que permita explotar la información almacenada en la misma sin necesidad de utilizar ningún lenguaje de programación o consulta. La exportación se debe poder realizar en diferentes formatos, requeridos como mínimo en csv, xls, pdf.

- La solución debe incluir un portal web para la creación y consulta de cuadros de mando.
- La solución debe tener datos accesibles a través de una API web para poder integrarse con otras plataformas;
- La solución debe tener un lenguaje de consulta para recuperar información a través de la API.
- La solución debe proveer indicadores sobre a experiencia digital del empleado y la comparativa con otras empresas de tamaño similar
- La solucion debe tener representación de flujos de tráfico entre clientes-servidores y drill-down.

4.2.2 Requisitos del agente

- La solución debe estar basada en un agente ligero que soporte los sistemas operativos Windows 7, Windows 10, Windows Server 2008, 2012, 2016 y 2019.

- El consumo del agente no debe exceder un 0,05% de CPU y 40 Mb de RAM de media.

- El agente no realizará ningún tipo de almacenamiento de datos en los dispositivos de usuario para no penalizar el rendimiento de estos.

- El agente debe comunicarse con la plataforma mediante tráfico cifrado. Este tráfico no debe exceder de 50 MB por día por dispositivo en condiciones normales.

Canal de Isabel II, S.A. inscrita en el Registro Mercantil de Madrid al Tomo 29.733, Folio 86, Sección 8, Hoja M-534929 e Inscripción 1ª, NIF A86488087, Domicilio Social: C/ Santa Engracia, 125, 28003 Madrid

4.3 Requisitos Funcionales

- La solución debe recopilar en tiempo real datos sobre:
  - Usuarios
  - Dispositivos
  - Paquetes instalados
  - Aplicaciones (aplicación, ejecutables que la componen y diferentes versiones de los ejecutables)
  - Puertos y Destinos de conexión
  - Dominios web visitados

- La solución debe recopilar en tiempo real datos sobre la actividad que se produce en el dispositivo:
  - Arranque del equipo
  - Login de usuario
  - Ejecución de procesos
  - Conexiones UDP, TCP y HTTP
  - Instalación de paquetes, actualizaciones y parches

- La solución debe recopilar en tiempo real inventario hardware y software de los equipos y servidores y caracterizar las aplicaciones de negocio de Canal de cara a inventariar su despliegue en los equipos y utilización en los mismos.

- La solución debe proporcionar un nivel de riesgo de las aplicaciones identificadas en el inventario de estas.

- La solución debe recopilar y habilitar investigaciones sobre eventos que afectan al usuario, como pantallas azules, crash de aplicaciones y eventos de aplicación que no responden, etc.

- Se deberán poder configurar servicios de negocio y aplicaciones en la plataforma para entender la experiencia de los usuarios en el acceso a dichos servicios.

- Se deberá disponer de la capacidad de tener una línea de tiempo en la que examinar los principales eventos que afectan a la experiencia del usuario de forma que se pueda analizar en el tiempo los eventos causantes de una mala experiencia.

Canal de Isabel II, S.A. inscrita en el Registro Mercantil de Madrid al Tomo 29.733, Folio 86, Sección 8, Hoja M-534929 e Inscripción 1ª, NIF A86488087, Domicilio Social: C/ Santa Engracia, 125, 28003 Madrid

- Se deberá disponer de diagramas de comunicación en los que se relacionen dispositivos, usuarios, aplicaciones, puertos y destinos de comunicación de forma gráfica.

- La solución debe habilitar las comunicaciones dinámicas con los empleados, desencadenadas por los eventos recopilados por la plataforma. Estas comunicaciones serán en forma de pop-ups.

- Se deberá poder realizar encuestas de tipo NPS a los usuarios.

  El sistema deberá proporcionar una métrica de experiencia digital que combine datos técnicos obtenidos del dispositivo y la actividad del usuario con datos subjetivos obtenidos de encuestas a los usuarios.

  Los parámetros de cálculo de la métrica tienen que poder ser modificables.

- La solución debe ser capaz de comparar las instancias de software instaladas en los dispositivos con el uso real de las mismas, de forma que se pueda reducir el gasto en licencias en función de su utilización real.

- La solución ha de basarse en una plataforma que permita monitorizar el cumplimiento y solucionar problemas relacionados, independientemente de las herramientas implementadas.

- La solución, debe contemplar caracterizados en aplicaciones y tipologías de estas los programas instalados y/o usados en los equipos

- La solución debe permitir analizar la información a partir de las diferentes redes de acceso desde los distintos centros de trabajo

- La solución debe permitir monitorizar las redes a partir de su uso desde los dispositivos de los usuarios

- La solución debe contar con diferentes niveles de reporting: cuadros de mando global, detalle operacional y nivel de detalle por usuario/dispositivo

Canal de Isabel II, S.A. inscrita en el Registro Mercantil de Madrid al Tomo 29.733, Folio 86, Sección 8, Hoja M-534929 e Inscripción 1ª, NIF A86488087. Domicilio Social: C/ Santa Engracia, 125, 28003 Madrid

4.4 Requisitos de seguridad

Con carácter general, el software debe cumplir con los siguientes requisitos:

- La solución debe ejecutarse en un entorno *cloud* en modo de *tenant* único.

- La comunicación entre los agentes y el entorno *cloud* deberá estar cifrada como mínimo con el protocolo TLS 1.2 para garantizar la seguridad de los datos.

- Se debe proporcionar un mecanismo de integración con SAML 2.0 para poder tener Single Sign On con el gestor de identidades de Canal de Isabel II y Office 365.

- Todas las acciones remotas que se quieran ejecutar en los dispositivos deberán estar firmadas digitalmente por el fabricante o por Canal de Isabel II.

- El software deberá garantizar los requisitos de seguridad detallados en el Anexo I (y relacionados en el documento adjunto "215-2020-UX-Requisitos_de_Seguridad.xlsx" o disponer de certificación del Esquema Nacional de Seguridad nivel medio.

5. PRUEBAS DE LOS EQUIPOS

Canal se reserva la posibilidad de solicitar a los licitadores un pequeño piloto del producto de una semana de duración, en el que se requerirá tener licencias cliente y acceso al software para comprobar que el producto ofertado cumple con los requisitos mínimos del Pliego de Prescripciones Técnicas. En cuyo caso el adjudicatario deberá entregar un plan de pruebas detallado, que será consensuado con Canal de Isabel Segunda.

El piloto será realizado sobre un parque de 200 equipos y 4 servidores ubicados en diferentes centros de trabajo de Canal de Isabel Segunda.

El licitador tendrá 5 días laborables desde la solicitud del piloto por parte de Canal para ponerlo en marcha.

No serán tomadas en consideración en el presente procedimiento de licitación las ofertas de los licitadores cuyo piloto no esté preparado para sus pruebas en el plazo señalado al efecto, o incumpla alguno de los requisitos del apartado 4 de este Pliego de Prescripciones Técnicas. Tampoco se tendrán en cuenta las ofertas de los licitadores cuyos equipos no superen las pruebas indicadas.

Canal de Isabel II, S.A. inscrita en el Registro Mercantil de Madrid al Tomo 29.733, Folio 86, Sección 8, Hoja M-534929 e Inscripción 1ª, NIF A86488087. Domicilio Social: C/ Santa Engracia, 125, 28003 Madrid

6. CONDICIONES DEL SUMINISTRO

El Adjudicatario deberá:

- Instalar y configurar la herramienta con personal de Canal.

- Impartir formación de la herramienta.

  Se impartirán dos sesiones de formación con una duración mínima de 25 horas. Estas se podrán hacer online en las oficinas de Canal de Isabel Segunda o de forma online, a criterio de Canal.

  El temario del curso será consensuado con Canal.

- Entregar manuales y documentación de la herramienta.

  Manuales Técnicos y funcionales de la herramienta.

  Manual de formación que incluya todo el temario del curso impartido.

  Documento de Instalación/Configuración inicial.

  Documento de operación que englobe las operaciones habituales

  Documento de *troubleshooting*

- Soporte y Resolución de incidencias

  El adjudicatario, deberá contar con técnicos especializados en la herramienta, para atender a las incidencias producidas durante el periodo del contrato. Proveerá de un número de teléfono o dirección de correo donde registrar las incidencias

  Mantener actualizado del documento de troubleshooting durante el ciclo de vida del contrato.

7. SERVICIO POSTVENTA

- A lo largo de la vida del contrato el Adjudicatario está obligado a suministrar todas las actualizaciones y parches que requiera la herramienta.
- Dar soporte sobre las nuevas actualizaciones y los cambios que se hayan producido.
- Cualquier actualización que se produzca en el software y que pueda impactar en el servicio, se ha de acordar con Canal antes de proceder a su actualización.
- Mantener actualizado del documento de troubleshooting durante el ciclo de vida del contrato.

Canal de Isabel II, S.A. inscrita en el Registro Mercantil de Madrid al Tomo 29.733, Folio 86, Sección 8, Hoja M-534929 e Inscripción 1ª, NIF A86488087, Domicilio Social: C/ Santa Engracia, 125, 28003 Madrid

8. ANS SERVICIO

- El tiempo de atención de las incidencias deber ser inferior a 1 hora.
- El tiempo de resolución de las incidencias debe ser inferior a 24 horas.
- Cuando la actualización de la plataforma SaaS tenga impacto sobre las versiones cliente soportadas, deberá ser comunicado con 7 días de antelación

9. ACLARACIONES

Para cualquier consulta sobre el presente procedimiento de licitación, deben ponerse en contacto con el **Área de Atención al Usuario de Canal o enviar un correo electrónico** a consultas_contratacion@canal.madrid **indicando en el asunto el número de procedimiento al que se refiere.**

Firmado electrónicamente por
Jesus Plaza Rubio
el día 17-08-2021 11:25:06

Firma: Jefe Área Proponente, Jesús Plaza Rubio
ÁREA DE PLANIFICACIÓN, CONTROL Y SEGURIDAD

Firmado electrónicamente por
Angel Rodriguez Garcia
el día 17-08-2021 12:07:12

Firma: Subdirector de SISTEMAS INFORMÁTICOS Ángel Rodríguez García
SUBDIRECCIÓN SISTEMAS INFORMÁTICOS

Firmado electrónicamente por
Monica Fierro Martin
el día 18-08-2021 18:32:54

Firma: Directora de RECURSOS Mónica Fierro Martín
DIRECCIÓN DE RECURSOS

Canal de Isabel II, S.A. inscrita en el Registro Mercantil de Madrid al Tomo 29.733, Folio 86, Sección 8, Hoja M-534929 e Inscripción 1ª, NIF A86488087, Domicilio Social: C/ Santa Engracia, 125, 28003 Madrid

10. ANEXO I. REQUISITOS DE SEGURIDAD

El software deberá garantizar los requisitos de seguridad relacionados en apartado o disponer de certificación del Esquema Nacional de Seguridad nivel medio, en cuyo caso deberá adjuntarse como documento de la oferta.

Junto con este pliego, se proporciona el documento 215-2020-UX-Analisis_de_Requisitos_de_Seguridad.V1.0.xlsx con el fin de que el licitador lo presente cumplimentado como un documento más de su oferta.

Canal de Isabel II, S.A. inscrita en el Registro Mercantil de Madrid al Tomo 29.733, Folio 86, Sección 8, Hoja M-534929 e Inscripción 1ª, NIF A86488087, Domicilio Social: C/ Santa Engracia, 125, 28003 Madrid

Consideraciones	Requisito	Cuando aplica
	Certificación de los servicios cloud a contratar por Canal de Isabel II S.A. en la Norma Internacional de Seguridad ISO/IEC 27001:2013, aplicando los objetivos de control y dominios de la Norma ISO/IEC 27002:2013	Siempre
	Certificación ISO/IEC 27017:2015 “Directrices para los controles de seguridad de la información basados en dicha Norma ISO/IEC 27002:2013 (incluyendo Cor 1:2014 y Cor 2:2015) para servicios en la nube” de los servicios cloud a contratar por Canal de Isabel II S.A.	Siempre
	Certificación ISO/IEC 27018:2014 “Requisitos para la protección de la información de identificación personal (PII) en sistemas cloud” de los servicios cloud a contratar por Canal de Isabel II S.A.	**Cuando exista tratamiento de datos de carácter personal**
	Certificación en el programa STAR (Cloud Security Alliance (CSA), Trust and Assurance Registry), al menos, en el nivel 2 (CSA STAR Certification) de los servicios cloud a contratar por Canal de Isabel II S.A.	Siempre (https://www.incibe.es/protege-tu-empresa/sellos-con-fianza/cloud/csa-star)

olio 86, Sección 8, Hoja M-534929 e Inscripción 1ª, NIF A86488087, Domicilio Social: C/ Santa Engracia, 125, 28003 Madrid

Consideraciones	Requisito	Cuando aplica
Se requerirá en base a los requisitos de disponibilidad que haya establecido Negocio (análisis de riesgos basado en ISO/IEC 27001:2013, BIA, etc.) para los activos de información dentro del alcance de los servicios cloud a contratar por parte de Canal de Isabel II, S.A. 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): 17.2.1. Disponibilidad de instalaciones para el procesamiento de la información	Certificación vigente en BS 25999 o ISO 22301:2012 "Sistema de Gestión de la Continuidad de Negocio" en los servicios cloud contratados por Canal de Isabel II, S.A.	Siempre
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): 12.6.1. Gestión de las vulnerabilidades técnicas. 12.6.2. Restricciones en la instalación de software 18.2.1. Revisión independiente de la seguridad de la información. 18.2.2. Cumplimiento de las políticas y normas de seguridad. 18.2.3. Comprobación del cumplimiento.	Disponer del resultado de la última auditoría de seguridad independiente por parte de terceros del servicio o servicios Cloud contratados por Canal de Isabel II, S.A., vulnerabilidades encontradas y estado el plan de acción identificado y definido para la resolución de las mismas	Siempre
Dado que los riesgo no son algo estático, pues evolucionan, es necesario revisarlos periódicamente y conocerlos, para que Negocio pueda tomar una decisión informada en cuanto a la contratación (asunción de los riesgos identificados) o no (no se asumen los riesgos identificados) de los servicios Cloud. 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): 8.1.1. Inventario de activos. 8.1.2. Propiedad de los activos. 8.1.3. Uso aceptable de los activos. 8.1.4. Devolución de activos.	Proporcionar el resultado de la revisión del último análisis de riesgos	Siempre

Hoja 86, Sección 8, Hoja M-534929 e Inscripción 1ª, NIF A86488087, Domicilio Social: C/ Santa Engracia, 125, 28003 Madrid

Consideraciones	Requisito	Cuando aplica
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): Dominio 9. Control de Accesos. Dominio 11. Seguridad física y ambiental. La Dirección de Seguridad puede dar información adicional al respecto de normativa de seguridad física existente y aplicable para la protección de infraestructuras, centros de trabajo y/o localizaciones físicas	Proporcionar una relación de las medidas de seguridad físicas implementadas en sus instalaciones (control de acceso a las instalaciones, a los CPDs, etc.)	Siempre
La seguridad en un entorno multi-cliente se verifican a través de la segmentación: hypervisor, aplicaciones y bases de datos. Aplicaría la 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): 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	Proporcionar una relación de las medidas de seguridad multi-cliente (multi-tenant) implementadas	Siempre que el servicio cloud sea compartido con otros clientes y no se preste en exclusiva
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): 12.4.1. Registro y gestión de eventos de actividad 16.1.2. Notificación de los eventos de seguridad de la información 16.1.3. Notificación de puntos débiles de la seguridad. 16.1.4. Valoración de eventos de seguridad de la información y toma de decision 16.1.5. Respuesta a los incidentes de seguridad. 16.1.6. Aprendizaje de los incidentes de seguridad de la información. 16.1.7. Recopilación de evidencias 18.2.2. Cumplimiento de las políticas y normas de seguridad. 18.2.3. Comprobación del cumplimiento.	Proporcionar una relación de los procedimientos de monitorización, alerta y reporting establecidos, incluyendo los de los análisis de incidentes de seguridad y de los análisis forenses	Siempre

Inscrita en el Registro Mercantil de Madrid, Tomo 986, Sección 8, Hoja M-534929 e Inscripción 1ª, NIF A86488087, Domicilio Social: C/ Santa Engracia, 125, 28003 Madrid

Consideraciones	Requisito	Cuando aplica
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): 12.2.1. Controles contra el código malicioso 12.6.1. Gestión de las vulnerabilidades técnicas 12.6.2. Restricciones en la instalación de software. 18.2.2. Cumplimiento de las políticas y normas de seguridad. 18.2.3. Comprobación del cumplimiento.	Proporcionar una relación de los procedimientos de bastionado y securización, tanto de la arquitectura de la infraestructura tecnológica como de servidores, comunicaciones, aplicaciones y servicios	Siempre
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): 12.1.4. Separación de entornos de desarrollo, prueba y producción 14.1. Requisitos de seguridad de los sistemas de información 14.2. Seguridad en los procesos de desarrollo y soporte. 14.3. Datos de prueba	Proporcionar información sobre el nivel de protección y exposición de los entornos o sistemas no productivos (desarrollo, test, calidad, formación, etc.) y de la información propiedad de Canal de Isabel II, S.A. que contienen y gestionan	Siempre que existan entornos no productivos (desarrollo, test, pruebas, calidad, formación, etc.)
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): 9.4.5. Control de acceso al código fuente de los programas. 14.1.1. Análisis y especificación de los requisitos de seguridad. 14.1.2. Seguridad de las comunicaciones en servicios accesibles por redes públicas. 14.1.3. Protección de las transacciones por redes telemáticas. 14.2.1.Política de desarrollo seguro de software. 14.2.4. Restricciones a los cambios en los paquetes de software. 14.2.5. Uso de principios de ingeniería en protección de sistemas. 14.2.6. Seguridad en entornos de desarrollo. 14.2.7. Externalización del desarrollo de software. 14.2.8. Pruebas de funcionalidad durante el desarrollo de los sistemas. 14.2.9. Pruebas de aceptación	Proporcionar evidencias sobre el aseguramiento de la calidad de los desarrollos software realizados por el proveedor (por ejemplo, proporcionando las correspondientes certificaciones ISO/IEC 15504 SPICE, ISO/IEC 33000, modelo de madurez CMMI, etc.) y evidencias de que la seguridad es tenida en cuenta desde el diseño	Siempre que existan desarrollos

Hoja 86, Sección 8, Hoja M-534929 e Inscripción 1ª, NIF A86488087, Domicilio Social: C/ Santa Engracia, 125, 28003 Madrid

Consideraciones	Requisito	Cuando aplica
Evaluación objetiva del requisito en base a los dominios, objetivos de control y controles del anexo ISO/IEC 27001:27002:2013: 14.2.2. Procedimientos de control de cambios en los sistemas. 14.2.3. Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo. 14.2.4. Restricciones a los cambios en los paquetes de software.	Proporcionar información sobre los cambios que potencialmente pudieran afectar al servicio objeto de contratación por parte de Canal de Isabel II, S.A.: - Categoría del cambio - Fecha y hora del cambio - Impacto esperado. - Funcionalidades afectadas - Tiempo real de interrupción del servicio - Descripción técnica del cambio en el servicio o en los sistemas que lo soportan o en los que se basa, así como el procedimiento detallado del plan de marcha atrás que se aplicará en caso de que fuera necesario. - Notificación del inicio, del fin del cambio y del resultado de las pruebas de validación del cambio realizadas para su aceptación Nota: el tener certificado el servicio objeto de contratación por parte de Canal de Isabel II, S.A. en la norma ISO/IEC 20000-1 (estándar de calidad para la certificación de los servicios de gestión y soporte TI) haría que se cumpliera este requisito	Siempre
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): 9.2.3. Gestión de los derechos de acceso con privilegios especiales. 12.4.1. Registro y gestión de eventos de actividad. 12.4.2. Protección de los registros de información. 12.4.3. Registros de actividad del administrador y operador del sistema.	Registrar las actividades realizadas por parte de los operadores y administradores de los sistemas que soportan o en los que se basa el servicio en relación con la información propiedad de Canal de Isabel II, S.A. que se gestiona y/o almacena en él	Siempre
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): 8.1.1. Inventario de activos. 8.1.2. Propiedad de los activos. 8.1.3. Uso aceptable de los activos. 8.1.4. Devolución de activos	Existen y se aplican procedimientos para la reversión del servicio a los clientes, la devolución a los mismos de la información de su propiedad en el mínimo tiempo posible y en un formato tratable por ellos, y la garantía de acceso a la información devuelta	Siempre

Hoja 86, Sección 8, Hoja M-534929 e Inscripción 1ª, NIF A86488087, Domicilio Social: C/ Santa Engracia, 125, 28003 Madrid

Consideraciones	Requisito	Cuando aplica
Evaluación objetiva. 1) LOPD (Art. 92.4 y Art 112.2) para datos personales y la información de identificación personal (PII). Consultar con DPD. 2) Del requisito en base a los dominios, objetivos de control y controles del anexo A ISO/IEC 27001:2013 (ISO/IEC 27002:2013): 8.1.4. Devolución de activos. 8.3.2. Eliminación de soportes. 18.2.2. Cumplimiento de las políticas y normas de seguridad. 18.2.3. Comprobación del cumplimiento.	Existen y se aplican procedimientos para el borrado (seguro y certificado cuando proceda) de la información propiedad de Canal de Isabel II, S.A. una vez se haya revertido el servicio, la información haya sido accedida y verificada en su totalidad por el Responsable del Tratamiento y/o Dueño de los Datos en Canal de Isabel II, S.A., tanto en la completitud como en la corrección de los datos devueltos, y una vez finalizada la prestación contractual	Siempre
Aspectos técnicos de seguridad mínimos a tener en cuenta		
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): 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.	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.).	Siempre
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): 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	b) El uso de un esquema de BBDD propio para la información propiedad de Canal de Isabel II, S.A. c) 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.	Siempre, en base a la clasificación de los activos de información dentro del alcance de los servicios cloud a contratar por parte de Canal de Isabel II, S.A.

Hoja 86, Sección 8, Hoja M-534929 e Inscripción 1ª, NIF A86488087, Domicilio Social: C/ Santa Engracia, 125, 28003 Madrid

Consideraciones	Requisito	Cuando aplica
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): 10.1.1. Política de uso de los controles criptográficos. 10.1.2. Gestión de claves criptográficas.	d) 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)	Siempre
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): 10.1.1. Política de uso de los controles criptográficos. 10.1.2. Gestión de claves criptográficas.	e) 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.)	Siempre
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): 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.	f) Exista la posibilidad de uso de: f.1. 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. f.2. OAuth 2.0 como framework de autorización y OpenID Connect (OIDC) como protocolo de autenticación en las APIs existentes. f.3. SCIM como modelo para automatizar el intercambio de información de identidad de los usuarios entre distintos dominios de identidad	Siempre que: · exista la posibilidad de integrar la autenticación y/o la autorización del servicio con proveedores de identidad de terceros · existencia de APIs que puedan ser consumidas

Hoja 86, Sección 8, Hoja M-534929 e Inscripción 1ª, NIF A86488087, Domicilio Social: C/ Santa Engracia, 125, 28003 Madrid

Consideraciones	Requisito	Cuando aplica
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): 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.	g) 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), contra-señas de un único uso (OTP), uso de tokens (hardware o software), etc.	Siempre
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): 12.6.1. Gestión de las vulnerabilidades técnicas. 12.6.2. Restricciones en la instalación de software 18.2.1. Revisión independiente de la seguridad de la información. 18.2.2. Cumplimiento de las políticas y normas de seguridad. 18.2.3. Comprobación del cumplimiento.	h) Todas las funciones de la aplicación relacionadas con la autenticación, la gestión de las sesiones y la autorización (con-trol 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	Siempre
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): 12.4.1. Registro y gestión de eventos de actividad Pueden existir requisitos legales adicionales en lo relativo a la conserva-ción de los registros y eventos. Consultar con el DPD.	i) 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 mante-nerse al menos durante cinco (5) años	Siempre

Sección 8, Hoja M-534929 e Inscripción 1ª, NIF A86488087, Domicilio Social: C/ Santa Engracia, 125, 28003 Madrid

Consideraciones	Requisito	Cuando aplica
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): 12.6.1. Gestión de las vulnerabilidades técnicas. 12.6.2. Restricciones en la instalación de software 18.2.1. Revisión independiente de la seguridad de la información. 18.2.2. Cumplimiento de las políticas y normas de seguridad. 18.2.3. Comprobación del cumplimiento.	j) 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	Siempre

Folio 86, Sección 8, Hoja M-534929 e Inscripción 1ª, NIF A86488087, Domicilio Social: C/ Santa Engracia, 125, 28003 Madrid