



**PLIEGO DE PRESCRIPCIONES TÉCNICAS PARA
LA IMPLANTACIÓN DEL SOFTWARE DE
CONTROL, SUPERVISIÓN Y ADQUISICIÓN DE
DATOS (SCADA) PARA EL CENTRO DE
CONTROL DE CANAL DE ISABEL II.**

CONTRATO N° 281/2021

Área de Aplicaciones Informáticas

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A.	NUEVO SCADA	Diciembre 2021
Elaborado por	Documento	Versión
Área de Aplicaciones Informáticas	Pliego de Prescripciones Técnicas	V1.0

Índice

1. INTRODUCCIÓN	5
1.1. Contexto y antecedentes	5
1.2. Planteamiento del proyecto	5
1.3. Objetivos del proyecto	7
2. ALCANCE DEL SERVICIO LICITADO	9
2.1. Fase 1: Proyecto de implantación básica (o Piloto).....	10
2.2. Fase 2: Suministro de licencias y software	11
2.3. Fase 3: Diseño e implantación de la arquitectura	12
2.4. Fase 4: Formación técnica al equipo de proyecto	13
2.5. Fase 5: Proyecto de implantación completa del nuevo SCADA	14
2.5.1. Servicios de gestión del cambio	15
2.5.2. Migración de la información	16
3. ENTORNO TECNOLÓGICO.....	19
4. REQUISITOS DEL SOFTWARE	20
4.1. Requisitos de Adquisición de Datos	21
4.2. Requisitos de Proceso de Señal.....	21
4.3. Requisitos de Proceso y Modelado de Datos	23
4.4. Requisitos de Gestión de Alarmas.....	25
4.5. Requisitos de Interfaz de Usuario (HMI).....	28
4.6. Requisitos de Herramientas de Desarrollo	31
4.7. Interfaces con otros sistemas	33
4.8. Requisitos de Arquitectura de Sistemas, Seguridad y Redes.....	35
4.9. Requisitos de Modo de Licenciamiento	36
4.10. Requisitos de Capacidad y Rendimiento	38
4.11. Requisitos del ecosistema de la plataforma.....	38
4.12. Requisitos del mantenimiento y soporte	39
4.13. Requisitos de Seguridad.....	40
5. PROYECTO DE IMPLANTACIÓN BÁSICA.....	44
5.1. Requisitos del Proyecto De implantación básica	44

5.2.	Gestión de implantación básica	48
5.3.	Validación del Proyecto de implantación básica.....	50
6.	PROYECTO DE DISEÑO E IMPLANTACIÓN	53
6.1.	Gestión del proyecto.....	53
6.2.	Plan de Pruebas	55
6.3.	Formación.....	55
6.4.	Gestión del Cambio	56
6.5.	Puesta en Producción.....	57
6.6.	Soporte post-implantación y Devolución del Servicio	57
7.	EJECUCIÓN DE LOS TRABAJOS	58
7.1.	Plazos de ejecución.....	58
7.2.	Equipos de trabajo.....	59
7.3.	Organización, Seguimiento y Control de los trabajos	62
7.4.	Lugar de realización de los trabajos	63
7.5.	Conectividad con Canal de Isabel II	63
8.	MODELO DE GOBIERNO	64
8.1.	Gestión de Servicios.....	64
8.2.	Gestión de la Relación.....	64
8.2.1.	Modelo de Referencia	64
8.2.2.	Comité de Dirección	65
8.2.3.	Comité de Seguimiento y control.....	66
8.2.4.	Comité Operacional	68
8.3.	Gestión del Contrato.....	69
8.4.	Sistema de Gestión Integrado	69
8.5.	Seguimiento e informes	70
9.	Fase de Devolución.....	71
9.1.	Principios clave.....	71
9.2.	Principios generales	71
9.3.	Elementos que se transferirán	73
9.4.	Planificación y plan de proyecto	74
9.5.	Gobierno de la finalización.....	75
9.6.	Actividades durante el periodo de Soporte	76
9.7.	Gestión de la seguridad y la conformidad.....	76
9.8.	Facturación y obligaciones durante la finalización.....	77
9.8.1.	Garantías durante la transferencia sobre los servicios a transferir.....	77
10.	AUDITORIA.....	78
10.1.	Principios	78
10.2.	Procedimientos de auditoría	79

10.2.1.	Organización de la auditoría.....	79
10.2.2.	Plan de Auditoría	79
10.2.3.	Notificación.....	79
10.2.4.	Reunión de arranque.....	80
10.2.5.	Trabajo de campo.....	80
10.2.6.	Informe de auditoría	81
10.2.7.	Seguimiento	81
10.2.8.	Software para la auditoría	81
10.2.9.	Documentación.....	82
10.2.10.	Auditorías realizadas por terceros	82
11.	ESTRUCTURA DE LAS OFERTAS	83
12.	CONDICIONES DE ACEPTACIÓN, GARANTÍA Y MANTENIMIENTO	84
	ANEXO 1. CUESTIONARIO PERSONAL	85
	ANEXO 2. METODOLOGÍA DE GESTIÓN DE PROYECTO DE CANAL DE ISABEL II	86
	ANEXO 3. CONSIDERACIONES DE SEGURIDAD DE APLICACIONES PARA CANAL DE ISABEL II, S.A.	88
	ANEXO 5. ESPECIFICACIÓN ENTORNOS TECNOLÓGICOS PARA NUEVOS DESARROLLOS.	120
1.	CONTEXTO.....	120
2.	OBJETIVOS DEL PROYECTO/ÁREA FUNCIONAL	120
3.	FASES DEL PROYECTO/ÁREA FUNCIONAL Y ENTREGABLES.....	120
4.	HITOS CLAVE	121
5.	FACTORES CRÍTICOS DE ÉXITO	121
6.	RESTRICCIONES	121
7.	DETALLE DE LOS REQUISITOS.....	121
	ANEXO 5. CONDICIONES PARA LA CONEXIÓN A LA RED CORPORATIVA DE DATOS Y DE SEGURIDAD DE CANAL DE ISABEL II	131
1.	Conexión única del operador de comunicaciones con la RCD de Canal de Isabel II ..	131
2.	Conexión de backup, contingencia o respaldo con la RCD de Canal de Isabel II	132
3.	Direccionamiento IP.....	132
4.	Monitorización de la conexión.....	132
5.	Contacto	132

1. INTRODUCCIÓN

1.1. Contexto y antecedentes

Canal de Isabel II comenzó a telecontrolar sus infraestructuras a finales de los años 80, montando un Centro de Control para la supervisión de la captación y aducción del agua. Para realizar estas tareas de telecontrol se dispone como plataforma el software SCADA (Sistema de Control, Supervisión y Adquisición de Datos) Aspentech Info-plus.21.

En el pasado, la funcionalidad del software y las limitaciones técnicas hicieron necesario desarrollar a medida muchas funcionalidades que hoy en día vienen de serie en todos los productos SCADA, así como diseñar el núcleo del sistema con una arquitectura de procesos en ejecución que no aprovechan los avances en tecnologías de la información ocurridos en los últimos 25 años.

En estos años se han realizado varios proyectos de reingeniería y renovación de la plataforma SCADA para asegurar su continuidad y ampliar su funcionalidad y capacidad de proceso. Sin embargo, gran parte del núcleo diseñado al principio se ha mantenido debido a las dependencias del resto de los procesos del mismo.

1.2. Planteamiento del proyecto

Para la consecución de este proyecto global de transformación Canal de Isabel II ha decidido dividir el proyecto en cinco fases:

- **Fase 1 (Implantación básica o Piloto):** cuyo objetivo es validar que los productos ofertados cubren suficientemente los requerimientos esenciales de Canal de Isabel II. Durante esta fase se deberán parametrizar, configurar y desarrollar todos los requerimientos, procesos e interfaces considerados obligatorios para la implantación básica de la solución. Durante la fase 1 se realizará la incorporación del 10% de la información histórica del sistema actual a la nueva solución para la validación de la implantación básica.
- **Fase 2 (Suministro de licencias y software):** cuyo objetivo es el suministro de todas las licencias de uso necesarias para todos los productos que formen parte de la solución ofertada y que deben cubrir las necesidades indicadas en este pliego para las diferentes fases del proyecto.
- **Fase 3 (Diseño e implantación de la arquitectura):** cuyo objetivo es el diseño e implantación de la arquitectura así como el dimensionamiento de la solución global, necesaria para soportar el software adquirido y su implantación.
- **Fase 4 (Formación técnica al equipo de proyecto):** cuyo objetivo es la formación adecuada del equipo de proyecto de Canal de Isabel II que participará en la construcción del nuevo SCADA.

- **Fase 5 (Implantación completa):** cuyo objetivo es la implantación completa y definitiva de la solución con todos los requerimientos de Canal de Isabel II. Durante esta fase se llevará a cabo la implantación completa de la solución y puesta en producción de la misma, llevando a cabo la configuración y desarrollos de todos los requerimientos, procesos e integraciones considerados necesarios para la puesta en producción de la solución. Durante la fase 5 se realizará la incorporación del 100% de la información histórica del sistema actual, que se haya identificado como necesaria para su migración al nuevo sistema, y se dejará en modo consulta el histórico actual en Oracle .

Se han identificado como factores críticos de éxito para este proyecto:

- Seleccionar un producto o conjunto de productos estándar del mercado que mejor se adapten a los requerimientos de Canal y que sus procesos utilicen las mejores prácticas para llevar a cabo los trabajos de telecontrol.
- La solución debe ser de un fabricante con capacidad de evolución en el mercado, innovación y adaptación a las nuevas normativas que surjan.
- Los productos que formen parte de la solución deben estar disponibles en español.
- Los productos ofertados deben disponer de un número suficiente de integradores certificados por el fabricante con gran experiencia en proyectos similares del sector. Para ello el/los fabricantes de los productos deben disponer de un programa de certificación de integradores y partners vigente que garantice la actualización, es decir que el programa de certificación requiera la revalidación periódica de la certificación para asegurar que los integradores y partners conocen las características últimas de sus productos.
- Oferta conjunta integrador-fabricante(s) que integre los productos del fabricante con las necesidades demandas por Canal de Isabel II, mediante la flexibilidad y capacidad del integrador
- Equipo de implantación por el integrador con conocimiento y experiencia en los procesos de telecontrol en una empresa que gestione el ciclo integral del agua.
- Servicios de acompañamiento del fabricante, que incluya servicios de asesoramiento, validación y apoyo durante el proyecto.
- Control de calidad del desarrollo para asegurar el uso de las mejores prácticas y metodologías.
- Definir un modelo de relación y gestión adecuado.
- Realizar una adecuada gestión del conocimiento del sistema asegurando su correcta transmisión dentro del equipo (estabilidad y formación).
- Flexibilidad a la hora de adaptarse a cambios en los sistemas derivados de los cambios en los procesos empresariales o regulatorios.
- Formación adecuada en los productos de la solución ofertada.
- Definir los procedimientos de trabajo adecuados con el resto de equipos de Canal.

- Polivalencia del equipo para poder trabajar con diferentes demandas de servicios.
- Correcta gestión del cambio.
- Solución con la mayor garantía en seguridad de la información y la protección de datos personales

1.3. Objetivos del proyecto

El objeto del presente concurso es la contratación del **“SUMINISTRO Y SERVICIOS PARA LA IMPLANTACIÓN DEL SOFTWARE DE CONTROL, SUPERVISIÓN Y ADQUISICIÓN DE DATOS (SCADA) PARA EL CENTRO DE CONTROL DE CANAL DE ISABEL II** durante un periodo de cuatro años.

A través de estos servicios Canal de Isabel II persigue conseguir:

- Implantar un nuevo sistema de SCADA que dé soporte a los procesos de Telecontrol de Canal de Isabel II asegurando su satisfacción.
- Supervisión y control en tiempo real de las infraestructuras incluidas en la plataforma.
- Gestionar la información de forma unificada, a partir de la consolidación y contextualización de los datos en un repositorio único.
- Proporcionar un sistema de información preciso y en tiempo real que permita la toma de decisiones, tanto en la parte operativa y de mantenimiento como para conocer los indicadores de referencia del estado de las instalaciones.
- Eliminar cualquier tipo de limitación acerca del tamaño del sistema, su número de variables, usuarios o interfaces, con una plataforma suficientemente escalable.
- Añadir funcionalidades que el sistema actual no permite o que suponen desarrollos muy complejos, como sistemas de validación, control de calidad y estimación de datos y automatización de procesos.
- Facilitar la integración con otros sistemas, como los de mantenimiento de infraestructuras, sistemas de información geográfica y herramientas de inteligencia de negocio.
- Aportar dentro de la plataforma características que permitan la utilización de software avanzado de proceso de datos en tiempo real, sistemas CEP o IA/ML.
- Definir un estándar tecnológico para homogeneizar y estandarizar los sistemas de supervisión y control.
- Disponer de una arquitectura tecnológica que proporcione un sistema totalmente abierto, modular y reutilizable que permita agregar nuevas funcionalidades e infraestructuras a la plataforma, al mismo tiempo que garantice la ciberseguridad, la alta disponibilidad y la escalabilidad de la solución.

- Fomentar la estandarización y reutilización de recursos hardware, software y de comunicaciones.
- Diseñar e implantar sobre el nuevo SCADA la base de datos en tiempo real , con la migración de los datos históricos y las configuraciones de adquisición de datos así como la adaptación y redefinición de los esquemas del sistema actual.
- Es esencial que Canal tenga control absoluto sobre el sistema. Para que esto sea posible, cualquier desarrollo sobre la plataforma debe estar abierto, y tanto la propiedad intelectual como el código fuente debe de pertenecer a Canal. El código fuente de cualquier sistema o dispositivo que contenga lógica programable debe ser enviado a Canal para evitar futuras dependencias de terceros.
- Que el sistema sea adaptable a las tendencias tecnológicas y funcionales del mercado.
- Asegurar una correcta solución de implantación y control de la ejecución de la misma, así como de mantenimiento, gestión, control y administración del sistema, procesos y usuarios.
- Garantizar una gestión eficiente del conocimiento de los sistemas, tanto dentro del equipo del adjudicatario como dentro del equipo de Canal de Isabel II. Para ello será objetivo primordial documentar y mantener actualizada la documentación de los sistemas, así como la formación y capacitación continua de los operadores de los sistemas.
- Cumplir con las normas y procedimientos definidos en Canal de Isabel II en relación con autorizaciones y permisos en los entornos, control de accesos, tareas de administración y en general Política de Seguridad de Sistemas de Información, así como las normativas y recomendaciones en materia de Protección de Datos.

2. ALCANCE DEL SERVICIO LICITADO

Dentro del plan estratégico de ampliación y mejora del telecontrol se encuentra la renovación y modernización del sistema SCADA. El primer paso de la renovación del sistema SCADA consiste en la selección de una nueva plataforma que cubra de serie gran parte de los requisitos que actualmente soportan procesos desarrollados a medida e incluya las tecnologías actuales de procesamiento paralelo, procesamiento avanzado de eventos CEP (Complex Event Processing) y herramientas de análisis de datos.

El alcance del contrato contempla los siguientes apartados:

- Elaboración de un proyecto de implantación básica que garantice la viabilidad y adecuación del producto a las necesidades de Canal de Isabel II. Se deberán parametrizar, configurar y desarrollar todos los requerimientos, procesos e interfaces considerados obligatorios para la implantación básica de la solución. Durante la fase 1 se realizará la incorporación del 10% de la información del sistema actual a la nueva solución para la validación de la implantación básica.
- Suministro de licencias y software de la plataforma SCADA seleccionada, así como mantenimiento y soporte del producto.
- Programa de formación técnica al equipo de proyecto y usuarios finales.
- Servicios de diseño e implantación de la arquitectura de la solución.
- Proyecto de implantación del nuevo SCADA. Implantación completa de la solución y puesta en producción de la misma, llevando a cabo la configuración y desarrollos de todos los requerimientos, procesos e integraciones considerados necesarios para la puesta en producción de la solución. En esta fase se realizará la incorporación del 100% de la información del sistema actual, que se haya identificado como necesaria para su migración al nuevo sistema y se debe ofrecer una solución de consulta bajo demanda para la información no migrada.
- El adjudicatario deberá prestar desde el inicio de los trabajos servicios de gestión del cambio.

2.1. Fase 1: Proyecto de implantación básica (o Piloto)

Para comprobar la adecuación del producto a los requisitos, se debe realizar un proyecto de implantación básica. A lo largo de este pliego, se denominará este proyecto tanto “Implantación básica” como “Piloto”.

En caso de que el mismo no supere la validación, Canal de Isabel II desestimará la adquisición de la plataforma software y el resto del alcance del proyecto.

La ejecución de la implantación básica tiene la consideración de proyecto y se ajustará a la metodología de gestión de proyectos implantada en Canal de Isabel II, por ello, al inicio de esta fase deberá realizarse un Plan de Implantación Básica, siguiendo la metodología de gestión de proyectos de Canal de Isabel II que figura en el Anexo 2 del presente pliego. Este plan deberá ser realizado por el adjudicatario con la colaboración de Canal de Isabel II para, posteriormente, aprobarse por parte de Canal de Isabel II.

El producto permitirá modelar las estructuras de datos según están definidas en el estándar unificado de Canal de Isabel II, así como replicar el comportamiento y simbología de los elementos gráficos representados en dicho estándar unificado

Las licencias para el proyecto de implantación básica deberán ser aportadas por adjudicatario.

El adjudicatario entregará a Canal la propuesta de arquitectura necesaria para la implantación completa, en la que se habrá tenido en cuenta las consideraciones de seguridad de la arquitectura definitiva.

Los entregables por parte del adjudicatario deben ser:

- Propuesta de arquitectura necesaria para la implantación completa
- Documentación de gestión del proyecto de implantación básica incluida la migración del 10% de la información histórica y las configuraciones necesarias de adquisición de datos, de acuerdo a la metodología de gestión de proyectos de Canal de Isabel II (Anexo 2)
- Sistema de implantación básica instalado y configurado
- Código fuente de las extensiones y personalizaciones realizadas al producto
- Ficheros de configuración modificados tras la instalación
- Scripts y programas para la validación de los requisitos de carga y rendimiento
- Análisis GAP con identificación de las adaptaciones necesarias para cubrir los requerimientos de Canal de Isabel II y que deberán realizarse para la implantación completa de la solución.

Una vez finalizado y aprobado el de implantación básica, el adjudicatario deberá prestar el resto de los servicios.

Los requisitos de la implantación básica y los criterios de validación de los mismos se especifican en el apartado PROYECTO DE IMPLANTACIÓN BÁSICA del presente pliego.

2.2. Fase 2: Suministro de licencias y software

Uno de los principales objetivos del contrato es la selección de un software SCADA que cumpla con los requisitos solicitados por Canal de Isabel II. En el apartado REQUISITOS DEL SOFTWARE del presente pliego se especifican estos requisitos.

Los requisitos están catalogados como Obligatorios, lo cual significa que el software debe cumplirlos para poder optar al concurso, o como Valorables, que reflejan características deseables del software que puntúan en la evaluación del mismo, pero no descalifican en caso de no cumplir.

En caso de que el cumplimiento del requisito marcado sea con extensiones, add-on del producto o servicios en la nube, dichas extensiones deberán estar incluidas en el licenciamiento ofertado, en caso contrario se considerará que “No cumple” con el requisito.

A través del presente procedimiento deberán ofertarse a Canal todas las licencias de uso necesarias para todos los productos que formen parte de la solución ofertada y que deben cubrir las necesidades indicadas en este pliego para las diferentes fases del proyecto.

Los entregables por parte del adjudicatario deben ser:

- Paquete instalable del software
- Documentación y manuales del producto en formato electrónico
- Licencias de uso del producto registradas a nombre de Canal de Isabel II
- Licencias de extensiones adicionales para el cumplimiento de requisitos no soportados por el producto base y ofertadas por el proveedor.
- Contrato de servicios en la nube, si procede, con sus correspondientes acuerdos de nivel de servicio, hasta el final de la duración del contrato.

Se contempla en este apartado la contratación del soporte correspondiente con el fabricante de la solución ofertada durante la duración del contrato.

El mantenimiento contratado ha de contemplar al menos los siguientes aspectos mínimos:

- Gestión de casos: La gestión de casos de soporte debe estar disponible en lo que se refiere a su creación, actualización y comprobación del estado de resolución de forma centralizada y preferiblemente a través de un sistema online (portal de soporte).
- Documentación: El soporte debe contemplar el acceso a la documentación del producto, ya sean manuales, guías técnicas o FAQs de los productos que componen la solución.

- Versiones y parches: Acceso a nuevas versiones de software y parches. En caso de bugs de producto que afecten a la instalación de Canal de Isabel II, el fabricante de la solución debe comprometerse a solucionar los mismos desarrollando un parche a medida o bien proporcionando un workaround que permita salvar la disfuncionalidad.
- Todas las correcciones o modificaciones que sean necesarias para cubrir la funcionalidad ofertada, y que se encuentren en el normal uso del sistema implantado durante la vigencia del contrato, serán subsanadas por el adjudicatario sin coste alguno para Canal de Isabel II, debiendo aportar el adjudicatario los recursos necesarios y en plazo para que sean subsanadas en el menor tiempo posible.
- Soporte: El soporte contratado debe cumplir con los requisitos que aparecen en el apartado “Requisitos del mantenimiento y soporte”

Los entregables por parte del adjudicatario deben ser:

- Credenciales de acceso a los portales de gestión de casos, documentación, versiones y parches.
- Teléfono de soporte para incidencias graves

2.3. Fase 3: Diseño e implantación de la arquitectura

En caso de validación de la implantación básica, el adjudicatario deberá llevar a cabo el diseño e implantación de la arquitectura, así como el dimensionamiento de la solución global, necesaria para soportar el software adquirido y su implantación.

El diseño de la arquitectura definitiva debe considerar los aspectos de seguridad, tanto de red y separación de la red de telecontrol de la red corporativa de datos a través de firewall, como de perfiles y permisos de los distintos tipos de usuarios en el sistema. Así mismo, debe contemplar tres entornos diferenciados con distintas parametrizaciones y recursos asignados (Entorno de Desarrollo para el desarrollo y prueba de desarrollos, Entorno de Integración para pruebas conjuntas y de estrés y para formación de usuarios, y Entorno de Producción para la operativa de la empresa).

Los sistemas de desarrollo e integración deben estar preparados para conectarse y desconectarse de las fuentes de datos reales, así como tener un sistema de simulación de eventos que permita forzar las situaciones a probar. Este mecanismo de simulación de eventos forma parte integral de la arquitectura a integrar.

El sistema productivo debe entregarse con las conexiones a los servidores OPC DA y UA que sirven de puente con los front-end configurados para la recepción de datos.

El entorno productivo debe cumplir con los requisitos de capacidad y rendimiento especificados en el apartado 4.10, y debe contar con un conjunto de monitores que permitan comprobar su funcionamiento y rendimiento.

Los entregables por parte del adjudicatario deben ser:

- Requerimientos de equipos para cada entorno (desarrollo, integración y producción)
- Manual de instalación y configuración del sistema
- Manual de backup & recovery
- Documento de arquitectura e integración con sistemas Canal de Isabel II, especialmente con los servidores OPC existentes. Debe incluir los flujos de datos y los servicios (protocolo y puerto) utilizados.
- Manual de operación con las operaciones habituales de mantenimiento y configuración
- Definición e implantación de la monitorización de la plataforma
- Mecanismo de simulación de eventos
- Procedimiento de paso entre entornos de objetos, desarrollos y refresco de configuración y datos
- Sistema de desarrollo instalado y configurado de acuerdo a la arquitectura definida
- Sistema de integración instalado y configurado de acuerdo a la arquitectura definida
- Sistema de producción instalado y configurado de acuerdo a la arquitectura definida
- Documento de seguridad, de acuerdo a la plantilla establecida en Canal de Isabel II.

2.4. Fase 4: Formación técnica al equipo de proyecto

Para la implantación de una nueva plataforma es imprescindible realizar una formación adecuada al equipo de proyecto de Canal de Isabel II que participará en la construcción del nuevo SCADA.

El proveedor especificará el temario de la Formación que considere necesaria para este proyecto, bien sea a través de cursos estándar del fabricante o a medida. A modo indicativo, el temario deberá ser consensuado con Canal y deberá cubrir al menos los siguientes aspectos:

- Interfaz de usuario, herramientas y personalización del entorno.
- Arquitectura de la plataforma SCADA
- Administración y operación del sistema
- Monitorización, depuración, logs de sistema
- Configuración de seguridad y permisos
- Adquisición de datos, configuración de conectores
- Procesamiento de datos
- Base de datos de equipos y señales, modelización de datos
- Programación de tareas, edición de flujos de trabajo
- Gestión de alarmas. Programación avanzada de alarmas.
- Creación de esquemas, dashboards y cambios al HMI
- Consulta y análisis de datos
- Instalación de nuevas versiones y/o parches.

La oferta debe incluir como mínimo 200 horas de formación técnica impartidas por ingenieros o formadores certificados en la solución.

2.5. Fase 5: Proyecto de implantación completa del nuevo SCADA

La ejecución de la implantación tiene la consideración de proyecto y se ajustará a la metodología de gestión de proyectos implantada en Canal de Isabel II. Por ello, al inicio de esta fase deberá realizarse un Plan de Implantación, siguiendo la metodología de gestión de proyectos de Canal de Isabel II. Este plan deberá ser realizado por el adjudicatario con la colaboración de Canal de Isabel II para, posteriormente, aprobarse por parte de Canal de Isabel II.

Los requisitos del mismo se establecerán en la fase de Análisis de Requisitos del proyecto, ofreciéndose una valoración inicial de los mismos en el apartado PROYECTO DE DISEÑO E IMPLANTACION del presente pliego.

Los entregables por parte del adjudicatario deben ser:

- Documentación de gestión del proyecto de implantación completa incluida la migración de la información histórica, de acuerdo a la metodología de gestión de proyectos de Canal de Isabel II (Anexo 2)
- Documentación de requisitos y análisis funcional
- Modelos de datos físico y lógico de la base de datos en tiempo real
- Documentación de configuración de los conectores de datos utilizados
- Modelos de los tipos de equipos y señales, y las jerarquías y relaciones entre ellos.
- Documentación de procesamientos de señales implantados en el sistema, generación de alarmas sencillas y complejas.
- Documentación de configuración y personalización del interfaz de usuario
- Esquemas de infraestructuras hidráulicas
- Documentación técnica de las extensiones y personalizaciones realizadas
- Código fuente de las extensiones y personalizaciones
- Documentación y diseño de los workflows y reglas de correlación de eventos
- Documentación y diseño de los interfaces con otros sistemas
- Scripts y programas para la validación de los requisitos de carga y rendimiento
- Manuales de formación para usuarios finales
- Cuadros de mando e informes
- Documento de seguridad, de acuerdo a la plantilla establecida en Canal de Isabel II.

A continuación, se describen los servicios de gestión del cambio y migración de la información, que estarán incluidos ambos en esta fase.

2.5.1. Servicios de gestión del cambio

Esta implantación conlleva una gestión del cambio inherente al proyecto de transformación de los procesos de Telecontrol y sus herramientas de soporte, y que afecta a todas las líneas horizontales y verticales de Canal de Isabel II. Sobre esta base, se establecen las siguientes líneas de consideración y/o actuaciones necesarias, que deberán considerar las empresas licitadoras, para garantizar con éxito la gestión del cambio adecuada al Proyecto.

Se deberán articular los mecanismos oportunos para que exista una relación fluida entre el equipo de Proyecto y el personal de la Subdirección de Telecontrol y Subdirección de Sistemas Informáticos de Canal de Isabel II, tanto al nivel de responsables de la toma de decisiones como de los integrantes de equipos de trabajo concretos que se establezcan para dar solución a problemas concretos del Proyecto.

El adjudicatario, deberá realizar también todas las labores necesarias para la Gestión del cambio y comunicación, todo ello bajo la supervisión y aceptación de Canal de Isabel II.

Las actividades mínimas a realizar serán las siguientes:

- Incorporar a especialistas en gestión del cambio a las sesiones de trabajo con el fin de identificar los principales riesgos asociados a los usuarios de los sistemas de información y poder elaborar acciones favorecedoras de la implantación de los nuevos sistemas.
- Realizar acciones de difusión y comunicación que permitan dar a conocer el proyecto a los diferentes agentes implicados de Canal de Isabel II.
- Inclusión en las fases iniciales del proyecto de los usuarios clave designados por la Subdirección de Telecontrol y la Subdirección de Sistemas Informáticos, especialmente en la definición de los siguientes aspectos:
 - Partiendo del as-is y definiendo el to-be conforme a las necesidades de Canal de Isabel II
 - Integración con el resto de los sistemas requeridos, tanto de los flujos de trabajo como de la arquitectura de la solución.
 - Etapas de validación continua por parte de los usuarios clave de los productos, validación de las especificaciones finales de diseño y pruebas de usuario durante la construcción y validación final.
 - Sesiones de Transferencia adecuadamente enmarcadas en la planificación dirigidas a Usuarios del sistema, Administradores y mantenedores en el ámbito informático de la solución y Soporte al Centro de Atención a Usuarios que recibe las llamadas e incidencias de usuarios internos de Canal.

La relación de entregables asociados a esta actividad será al menos la siguiente:

- Plan de gestión del cambio
- Plan de comunicación

2.5.2. Migración de la información

La migración total de la información del sistema actual al nuevo se llevará a cabo conforme al siguiente plan:

- Fase 1 - Implantación básica - se migrará el 10% de la información histórica del sistema actual y las configuraciones necesarias para la adquisición de datos a la nueva solución para la validación de la implantación básica, y se definirán las estrategias y planes para la migración final y puesta en producción.
- Fase 2 – Implantación Completa – en la que se construirán y validarán las herramientas necesarias para implementar las estrategias y planes definidos en la fase 1 para la migración y se migrará el 100% de la información histórica y las configuraciones de adquisición de datos.

Canal de Isabel II facilitará la información del modelo de datos del actual SCADA, y trabajará coordinadamente con el adjudicatario en aclarar todas las dudas que surjan sobre el modelo o singularidades en los datos.

El adjudicatario será el responsable de analizar el modelo de datos actual e identificar cómo realizar la extracción de la información, las transformaciones que la información precise, o información adicional de enriquecimiento que pudiera necesitar. Todas las tareas de extracción, limpieza, depuración, transformación y carga de la información serán llevadas a cabo por el adjudicatario.

Dado el impacto que las extracciones masivas de información pueden tener en los sistemas de Canal de Isabel II, el adjudicatario deberá validar el procedimiento de extracción con los técnicos de Canal de Isabel II, realizar pruebas parciales de extracción que permitan valorar el impacto de los procesos y coordinarse con los técnicos de Canal de Isabel II para definir las ventanas en las que la extracción podrá realizarse, y planificar los trabajos de extracción que sean precisos.

Formará parte de la validación de la implantación básica la extracción y transformación de la información correspondiente al 10% de la información histórica del sistema origen, así como su correcta carga en el sistema destino y verificación del funcionamiento de los procesos con esta información migrada.

Será necesario elaborar una estrategia y plan de migración global para todo el proyecto. Dentro de las estrategias será fundamental definir toda la información que es necesario migrar para el correcto funcionamiento de todos los procesos en el nuevo sistema, cumpliendo con los requerimientos y especificaciones establecidas. El plan de migración deberá contemplar los planes de pruebas y reporting—con al menos los siguientes entregables:

- Estrategia migración (cargas incrementales, sucesivas totales, etc.)

- Plan de migración y convivencia
- Plan de pruebas – debe incluir:
 - Pruebas de validación de la información
 - Reporting necesario para validar la migración
 - ⊖ Análisis y definición de datos a migrar-
 - Análisis de la calidad del dato origen (integridad referencial, datos duplicados, incumplimiento de reglas, etc.) y definir reglas para las correcciones necesarias.
 - Diseño del modelo de datos destino
 - Mapeo y transformación necesaria de la información

Durante esta fase de implantación completa, el adjudicatario deberá:

- Implementar todos los programas y procesos de migración definidos en el plan. Al menos deben incluir:
 - Procedimientos automatizados para la extracción de la información de los sistemas actuales
 - Conversiones y transformaciones de datos (formatos, códigos u otros cálculos precisos)
 - Depuración automatizada de la información. En aquellos casos donde no sea posible, se deberá suministrar a Canal de Isabel II las reglas para la depuración y toda la información necesaria para poder depurar en origen
 - Carga en el nuevo sistema
- Implementar el reporting necesario para validar la migración
- Realizar sucesivas pruebas de migración, con el objeto de validar la estrategia y los programas implementados sobre el entorno de integración
- Ajustar el plan de migración y el plan de pruebas conforme a las pruebas realizadas
- Pasar a producción todos los programas de migración y la solución para el acceso a información no migrada
- Se mantendrá durante un tiempo acordado los dos sistemas en paralelo (el antiguo y el nuevo) hasta que se pueda validar la información en el nuevo sistema, para lo cual se identificarán los ajustes y excepciones necesarias.
- Preparar un plan detallado para la puesta en producción (incluyendo tareas previas que permitan hacer una migración progresiva, reduciendo la cantidad de información a migrar durante esta fase)
- Acordar con Canal de Isabel II, la fecha para la ejecución del plan de puesta en producción, en base a las necesidades de negocio de Canal de Isabel II (minimizar el impacto de la indisponibilidad)
- Ejecutar el plan de puesta en producción, que incluya comprobación de la migración del 100% de la información histórica del sistema origen, y su correcta carga en el sistema destino
- Ejecutar los informes que permitan validar la información migrada

- Dar acceso al nuevo sistema de producción a los usuarios (no podrá hacerse hasta haber validado la información migrada)

3. ENTORNO TECNOLÓGICO

Los sistemas de información corporativos que dan servicio a la actividad diaria de la organización se encuentran centralizados y redundados en dos CPDs (Centros de Proceso de Datos) diferentes.

Estos Sistemas de Información, se enmarcan en lo que se denomina el entorno tecnológico de Canal de Isabel II , el cuál es fundamentalmente el siguiente:

- Estaciones de automatización Front-End Siemens, Rockwell Control Logix, PEGASUS y TESEOS, YCAROS, HYDRA (de diseño propio).
- Las informaciones de cada Front-End se ofrecen a través de servidores OPC DA y OPC UA .
- Estaciones cliente con Windows y navegadores Google Chrome y Microsoft Edge.
- Controladores de dominio basados en Windows, con un único dominio Windows Corporativo.Azure AD en algunos aplicativos.
- Servidores virtualizados en plataforma VMWare vSphere.
- Smartphones y Tablets Android y Apple.
- Gestión de aplicaciones móviles SOTI Mobicontrol
- Base de datos Oracle Exadata
- Sistema de desarrollo basado en control de versiones Subversion, integración continua Maven, Hudson y Jenkins y calidad de código Sonar.
- Sistema de ticketing y gestión de proyectos con software de CA , Service Desk y Clarity respectivamente.
- Sistema de documentación Confluence
- Suite de productos Scada de Aspentech.21.
- Aplicaciones de apoyo desarrolladas a medida en .net para boletines (informes complejos diarios sobre el ciclo integral del agua), gestión de límites (adaptación de límites a cambios de explotación o estacionales), sectorización (graficación y corrección histórica en sectores CAM)
- Desarrollo a medida Java para gestión inteligente de alarmas Scada, usando como BRMS Drools de Jboss.

4. REQUISITOS DEL SOFTWARE

Cada uno de los requisitos solicitados está catalogado como Obligatorio o como Valorable:

- Obligatorio: Indica que es necesario que el producto cumpla con el requisito. En caso de no cumplir o no ofrecer una solución satisfactoria al mismo, el producto quedará excluido del proceso de licitación.
- Valorable: Indica una característica de valor deseable del producto, pero no se excluirá al producto en caso de que no la incluya. El grado de cumplimiento de los requisitos Valorables, determinará la puntuación obtenida por los licitadores, tal y como se explica en el apartado 8 del PCAP.

En caso de que el cumplimiento del requisito marcado sea con extensiones o add-on del producto, o con servicios en la nube, dichas extensiones deberán estar incluidas en el licenciamiento ofertado, en caso contrario se considerará que “No cumple” con el requisito.

En el apartado 6 del PCAP, el licitador debe incluir un resumen técnico del cumplimiento de los requisitos obligatorios, que permita verificar el cumplimiento de dicho requisito. Además, debe incluir una referencia clara y accesible a la documentación oficial del producto que permita contrastar dicha información.

En el anexo II bis del PCAP, el licitador debe incluir un resumen técnico del cumplimiento de los requisitos valorables, que permita valorar el grado de adecuación a lo solicitado. Además, debe incluir una referencia clara y accesible a la documentación oficial del producto que permita contrastar dicha información.

4.1. Requisitos de Adquisición de Datos

El sistema se basa en la adquisición de datos de distintas fuentes, principalmente a través de OPC. Esta adquisición no es una importación de datos a demanda, sino una adquisición automática de los datos según se van generando a través de polling o respuesta a evento, por lo que el producto debe traer conectores que permitan dicha adquisición.

ID	Descripción	Tipo	Puntos
RAD1	OPC DA: El producto es cliente OPC DA para lectura y escritura de datos a través de este estándar.	Obligatorio	
RAD2	OPC HDA: El producto es cliente OPC HDA para lectura de datos a través de este estándar.	Obligatorio	
RAD3	OPC UA: El producto es cliente OPC UA para leer datos a través de este estándar.	Obligatorio	
RAD4	Base de datos Oracle: El producto permite cargar y obtener datos de BBDD relacionales Oracle.	Obligatorio	
RAD5	Base de datos SQL-Server: El producto permite cargar y obtener datos de BBDD relacionales Microsoft SQL-Server.	Obligatorio	
RAD6	Bases de datos relacionales: El producto permite cargar y obtener datos de BBDD relacionales genéricas, a través de estándares como ODBC, JDBC, etc.	Valorable	10
RAD7	Ficheros planos: El producto permite cargar datos a partir de ficheros de texto plano.	Obligatorio	
RAD8	Microsoft Excel: El producto permite cargar datos a partir de ficheros en formato Excel.	Valorable	8
RAD9	REST: El producto permite obtener datos de servicios web REST.	Obligatorio	
RAD10	SNMP: El producto permite obtener datos de protocolo de gestión de red SNMP v1 y SNMP v2.	Valorable	2
RAD11	SNMP Traps: El producto permite recibir Traps SNMP.	Valorable	2
RAD12	Mensajería: El producto permite la obtención de datos de sistemas de mensajería MQTT	Obligatorio	
RAD13	Mensajería: El producto permite la obtención de datos mediante sistemas de mensajería de colas y tópicos JMS, ActiveMQ o Kafka	Valorable	5

4.2. Requisitos de Proceso de Señal

ID	Descripción	Tipo	Puntos
RPS1	Diseño base de datos tiempo real: El producto permite la definición flexible y configurable de las características de cada uno de los tipos de señales diferentes que debe de tratar el	Obligatorio	

	sistema y los tratamientos a realizar al recibir la señal. A esta característica la denominamos actualmente "registro de definición", si bien puede considerarse que sean "clases" en el sentido de sistemas orientados al objeto. Considerando un registro de definición (analógico o digital) como un objeto, este debe de ser capaz de almacenar, tratar e historizar todas las medidas que hagan referencia a un determinado captador, las alarmas que pueden generarse y la apariencia dependiendo de su estado.		
RPS2	Herramienta definición de registros/clases: El producto está provisto de una herramienta intuitiva y ágil para crear las definiciones de los registros o clases.	Obligatorio	
RPS3	Medidas directas: El producto permite obtener a través del tratamiento de una medida analógica o una señal digital (dependiente del tipo de registro de definición) medidas directas del autómata.	Obligatorio	
RPS4	Medidas derivadas: El producto permite obtener a través del tratamiento de una única medida directa, una o varias medidas derivadas mediante cálculos en tiempo real. Las medidas que llegan del autómata pueden ser ya derivadas, en cuyo caso no sería necesario tratamiento alguno.	Obligatorio	
RPS5	Medidas calculadas analógicas: El producto permite obtener medidas analógicas calculadas en tiempo real a partir de la combinación de medidas directas de campo y derivadas. Desde simples combinaciones aritméticas hasta complejas fórmulas de cálculo como puedan ser curvas de gasto en aliviaderos.	Obligatorio	
RPS6	Medidas calculadas digitales 1: El producto permite obtener señales digitales calculadas en tiempo real a partir de la combinación lógica de señales digitales.	Obligatorio	
RPS7	Medidas calculadas digitales 2: El producto permite obtener señales digitales calculadas en tiempo real a partir de operaciones con valores analógicos de resultado digital (ej: $\text{caudal1} > \text{caudal2}$ and $\text{nivel1} < > 0$).	Obligatorio	
RPS8	Medidas calculadas analógico-digitales: El producto permite obtener medidas analógico-digitales calculadas en tiempo real a partir de la combinación de medidas analógicas y señales digitales (ej: tener en cuenta estado abierto/cerrado de una válvula de guarda para el cálculo de un caudal de un desagüe en función del nivel de un embalse y el grado de apertura de la válvula de regulación).	Obligatorio	
RPS9	Eliminación de valores anómalos: El producto permite la eliminación de valores anómalos puntuales en medidas analógicas (filtrado de la señal).	Obligatorio	
RPS10	Unidades de medida: El producto permite asociar a cada medida una unidad de medida.	Obligatorio	
RPS11	Conversión de unidades: El producto permite la conversión automática entre distintas unidades de medida (ej: de m ³ /s a litro/minuto) para permitir la representación gráfica en función de la escala.	Obligatorio	

RPS12	Desconexión de señales: El producto permite desconectar del sistema un equipo que tenga un comportamiento anómalo, permitiendo en caso necesario almacenar datos en logs diferenciados para su seguimiento.	Obligatorio	
RPS13	Contadores: El producto permite definir valores acumulativos tipo contador, por ejemplo horas de funcionamiento, número de arranques, contadores de volumen de agua y cálculo de caudales.	Obligatorio	

4.3. Requisitos de Proceso y Modelado de Datos

ID	Descripción	Tipo	Puntos
RPD1	Programas de tratamiento de la información por evento: El producto permite la creación de rutinas que se disparen como respuesta a un evento. Estos programas son los encargados de materializar el control y desaparición de las alarmas, realizar cálculos hidráulicos correspondientes y activar otras tareas o programas asociados. Los eventos deben poder encolarse y priorizarse en caso de llegada simultánea.	Obligatorio	
RPD2	Programas de activación cíclica: El producto permite la creación tareas que se activen cada cierto periodo de tiempo. Los ciclos de activación de cada rutina son distintos y están definidos tipo CRON o funcionalidad equivalente.	Obligatorio	
RPD3	Lenguaje programación no propietario: El producto permite que la programación de todas las tareas del sistema se realice con lenguajes y tecnologías estándar tales como Java, .Net o lenguajes de script (JavaScript, R, Python, etc.).	Valorable	10
RPD4	Lenguaje de consulta: El repositorio de información permite la consulta mediante lenguaje de consulta SQL o sus variantes para bases de datos NoSQL (CQL, HiveQL, Pig, etc.)	Valorable	10
RPD5	BPM: El producto permite la creación de workflows de trabajo BPM que se desencadenen al cumplirse las condiciones de ejecución definidas. Estas condiciones de ejecución serían distintas combinaciones de valores de señales procesadas, repetición de un mismo evento un determinado número de ocasiones, tratamientos complejos de múltiples señales o activaciones periódicas.	Valorable	8
RPD6	Límites dinámicos: El producto permite el cálculo de límites dinámicos en señales analógicas. Se entiende por límites dinámicos valores umbral de la señal para el disparo de alarma de límite calculados a partir de condiciones de contorno (día de la semana, festividad, mes, temperatura ambiente, precipitación esperada, ...).	Obligatorio	
RPD7	Estimación de valores: El producto permite la estimación de valores de señales analógicas. Se entiende por valores estimados el cálculo sustitutivo de un valor de campo por indisponibilidad de la señal calculados a partir de las condiciones de contorno (consumo esperado, temperatura, señales en la misma red,.....). También en caso necesario debe permitirse la imposición manual de valores. Los valores	Valorable	10

	estimados deben poder identificarse claramente en la ventana de detalle.		
RPD8	Predicción de valores: El producto permite calcular la predicción de valores (por ejemplo, consumos) en función de la historia del valor y condiciones definidas de contorno.	Valorable	5
RPD9	Cálculos por comparación de datos: El producto permite cálculos basados en la comparación de datos actuales con datos históricos y disparar alarmas en función de los resultados.	Valorable	8
RPD10	Históricos medias analógicas: El producto realiza el guardado de registros históricos de las señales analógicas para poder ser consultados y mostrados por la interfaz gráfica del SCADA. Los datos a historizar serán valores medio, máximo y mínimo durante el periodo definido. El periodo debe ser configurable y se debe permitir configurar varios periodos (cada X minutos, horario, diario).	Obligatorio	
RPD11	Históricos señales digitales: El producto permite el guardado de registros históricos de las señales digitales para poder ser consultados y mostrados por la interfaz gráfica del SCADA.	Obligatorio	
RPD12	Históricos telemandos: El producto permite el guardado de registros históricos de los telemandos para poder ser auditados. Una misma maniobra puede involucrar varios telemandos.	Obligatorio	
RPD13	Operadores temporales de Allen: El producto permite trabajar con operadores sobre intervalos temporales de Allen o funcionalidad similar: EQUALS (intervalos coincidentes), BEFORE (primer intervalo antes que el segundo), AFTER (primer intervalo posterior al segundo), MEETS (los intervalos son contiguos), OVERLAP (los dos intervalos tienen solape), BEGINS (el primer intervalo es el principio del segundo), ENDS (el primer intervalo es el final del segundo), MERGES (unir los dos intervalos en uno), INCLUDES (primer intervalo contiene el segundo) e INCLUDED_IN (primer intervalo contenido en el segundo).	Valorable	8
RPD14	Filtrado de ruido: El producto permite aplicar filtros (Kalman o técnicas similares) para suavizar la señal eliminando ruido en la señal.	Obligatorio	
RPD15	Modelado de datos: El producto permite modelar las estructuras de datos según están definidas en el estándar unificado de Canal de Isabel II, así como replicar el comportamiento y simbología de los elementos gráficos representados en dicho estándar unificado.	Obligatorio	
RPD16	Modelado de Señales: El producto permite modelar las señales que llegan al SCADA abstrayendo el tipo de medida de campo (porcentaje, lazo de corriente, unidades de ingeniería...) y parametrizando las distintas medidas calculadas, permitiendo reutilizar el modelo en todos las señales del mismo tipo (caudal, presión, potencia, nivel,...).	Obligatorio	
RPD17	Modelado de Equipos: El producto permite modelar equipos con varias señales analógicas y digitales (por ejemplo, analizadores de red eléctrica o bombas) y reutilizar el modelo en todos los equipos del mismo tipo.	Obligatorio	

RPD18	Modelado de Instalaciones: El producto permite modelar infraestructuras hidráulicas con varios componentes, equipos y señales, permitiendo configurar el número de elementos de cada tipo (por ejemplo, una Estación de Bombeo con N Equipos tipo Bomba) y reutilizar el modelo en todas las infraestructuras del mismo tipo.	Obligatorio	
RPD19	Jerarquía de Automatización: El producto permite modelar el sistema de telecontrol de la empresa, definiendo una jerarquía flexible (actualmente estaciones de comunicación primarias, estaciones de comunicación dependientes, autómatas locales, equipos y señales).	Valorable	10
RPD20	Jerarquía de Infraestructuras: El producto permite modelar el sistema hidráulico de la empresa, definiendo una jerarquía flexible (actualmente con sistemas formados por instalaciones, componentes, equipos y señales). La parte de equipos y señales es común en ambas jerarquías.	Valorable	10

4.4. Requisitos de Gestión de Alarmas

ID	Descripción	Tipo	Puntos
ALR1	Generación de alarmas 1: El producto permite la generación de alarmas para la supervisión del sistema a través de señales digitales procedentes de campo.	Obligatorio	
ALR2	Generación de alarmas 2: El producto permite la generación de alarmas para la supervisión del sistema a través de cambios en el valor de medidas analógicas: límites superiores e inferiores.	Obligatorio	
ALR3	Generación de alarmas 3: El producto permite la generación de alarmas para la supervisión del sistema a través de la rapidez de cambio de una medida analógica: gradientes.	Obligatorio	
ALR4	Generación de alarmas 4: El producto permite la generación de alarmas para la supervisión del sistema a través de la combinación aritmética y/o lógica de varias señales y/o alarmas activas.	Obligatorio	
ALR5	Generación de alarmas 5: El producto permite la generación de alarmas para la repetición N veces de un evento en un periodo de tiempo T.	Obligatorio	
ALR6	Generación de alarmas 6: El producto permite la generación de alarmas para la supervisión del sistema a través de programación de alarmas con operadores temporales: Antes, Después, En un intervalo T.	Valorable	10
ALR7	Generación de alarmas 7: El producto permite la generación de alarmas para la supervisión del sistema a través de programación de alarmas temporales: No cambia valor durante un tiempo T.	Valorable	10
ALR8	Histórico de alarmas: El producto permite el guardado de registros históricos de las alarmas generadas por el sistema para poder ser consultados. Se recogerá la siguiente información: código alarma, código del captador, regla, etc que la genera, texto de la alarma, fecha y hora de aparición de la alarma, fecha y hora de reconocimiento, fecha y hora de	Obligatorio	

	finalización, motivo de la finalización, usuario que ha reconocido la alarma, tipo de alarma y elemento, señal, regla, etc., que haya generado la alarma.		
ALR9	Temporización de alarmas: El producto permite temporizar alarmas para retrasar su aparición hasta un tiempo T configurable por tipo de alarma.	Obligatorio	
ALR10	Escenarios temporales para alarmas: El producto permite poder definir calendarios/escenarios tipo (configurables): horas valle, horas punta, fin de semana, día laborable, festivo, etc. De tal forma que se apliquen diferentes límites o reglas para la generación o no de alarmas según estos escenarios temporales.	Valorable	10
ALR11	Categorización de las alarmas: El producto permite la categorización de las alarmas, aplicando el mismo tratamiento a todas las alarmas del mismo de la misma categoría.	Obligatorio	
ALR12	Jerarquización de alarmas: El producto permite la jerarquización de las alarmas, existiendo una alarma principal y varias subordinadas, agrupando las subordinadas por debajo de la principal.	Valorable	10
ALR13	Inhibición de alarmas subordinadas: El producto permite la jerarquización de las alarmas, de tal forma que la aparición de una principal inhabilite la activación de las alarmas subordinadas.	Valorable	10
ALR14	Permanencia en el tiempo de las alarmas: El producto permite tipos de alarma que se resuelven automáticamente cuando la situación que las provoca desaparece (por ejemplo, límites) y alarmas que no se resuelven hasta ser atendidas por el operador aunque la causa que las generó haya desaparecido (por ejemplo, gradientes).	Obligatorio	
ALR15	Ciclo de vida de una alarma: El producto permite definir ciclos de vida para cada tipo de alarma.	Valorable	5
ALR16	Sumario de alarmas 1: El producto debe disponer de un sumario de alarmas personalizable dónde se recoge el estado de las diferentes alarmas generadas por el sistema.	Obligatorio	
ALR17	Sumario de alarmas 2: El producto debe permitir tener varios sumarios simultáneos para mostrar distintos tipos de alarmas (por ejemplo, alarmas del sistema de telecontrol y alarmas del sistema hidráulico / alarmas de abastecimiento y alarmas de saneamiento / alarmas de estaciones depuradoras, alarmas de bombes y alarmas de depósitos /)	Valorable	5
ALR18	Sumario de alarmas 3: La información a mostrar en el sumario de cada alarma simple (de una sola señal) debe poder contener información tanto de la alarma (código, tipo de alarma, prioridad, fecha y hora de inicio, estado,...) como de la señal que ha generado la alarma (tag del elemento, descripción del elemento,...).	Valorable	10
ALR19	Sumario de alarmas 4: En caso de alarmas compuestas debe mostrar la información de la alarma (código, tipo de alarma, prioridad, fecha y hora de inicio, estado,) y los valores de la combinación de señales que ha generado la alarma compuesta.	Valorable	10

ALR20	Sumario de alarmas 5: El sumario puede filtrarse por cualquiera de los campos que aparecen en él mediante campos seleccionables para los valores sujetos a dominio y por patrones LIKE %cadena% para los textuales no sujetos a dominio y combinaciones tipo >=< para valores numéricos.	Valorable	8
ALR21	Sumario de alarmas 6: El sumario debe refrescarse automáticamente para mostrar el estado actual de las alarmas haciendo push cuando salte una alarma.	Obligatorio	
ALR22	Sumario de alarmas 7: El sumario permite la selección de varias alarmas para realizar un tratamiento conjunto de todas las alarmas seleccionadas.	Valorable	7
ALR23	Sumario de alarmas 8: El operador puede marcar una alarma como “Relevante”, lo cual implicará un tratamiento y flujo distinto de dicha alarma y un sumario específico de alarmas relevantes.	Valorable	2
ALR24	Sumario de alarmas 9: Desde el sumario de alarmas se permite abrir la ventana de detalle de los objetos involucrados en la aparición de la alarma.	Valorable	10
ALR25	Sumario de alarmas 10: El sumario permite la visualización rápida de los últimos cambios de la señal a través de un micrográfico de la misma en el propio sumario o en tooltip.	Valorable	2
ALR26	Sincronización de alarmas y esquemas: La apariencia de los elementos afectados por alarma en todos los esquemas en que aparezca se modificará en consonancia con el estado de la alarma en tiempo real, mediante cambios en color, parpadeo incluso cambio del icono del elemento.	Obligatorio	
ALR27	Secuencia temporal de eventos: El producto permite definir secuencias temporales de eventos que deben producirse en un determinado orden y en un margen temporal definido, para la generación de alarmas dependiendo del caso no se cumpla o se cumpla. Ejemplo se produce el evento de apertura de compuerta X, después de un tiempo T1 (con un margen +-t) debe producirse un incremento de caudal en el medidor Y, después de un tiempo T2 debe producirse un incremento de nivel en el depósito Z.	Valorable	10
ALR28	Relaciones entre señales: El producto permite definir relaciones flexibles entre señales, de manera que pueda utilizarse esa relación para generar alarmas. Por ejemplo, debe permitirse relacionar una señal de caudal con una señal de presión, para generar una alarma de posible rotura si la señal de caudal aumenta y la de presión cae por debajo de un umbral.	Valorable	5
ALR29	El sistema deberá permitir al operador el silenciado temporal de alarmas si dispone de los privilegios correspondientes. Este silenciado temporal permitirá al operador evitar alarmas repetitivas al aparecer alguna incidencia, hasta que ésta sea convenientemente subsanada por mantenimiento.	Obligatorio	
ALR30	Las alarmas deben ser detectadas y comunicadas por un servicio de alarmas, que en caso de tormenta de alarma (cientos o miles de alarmas detectadas en un segundo), el servicio de alarmas propondrá alguna herramienta de ayuda a la gestión de las mismas y evitará el bloqueo de la visualización de las alarmas.	Obligatorio	

ALR31	El sistema tendrá la capacidad para que operadores autorizados eliminen temporalmente las alarmas seleccionadas de la lista de alarmas activas y/o que las suprimen durante un período determinado. El sistema debe pedir a los operadores que introduzcan un motivo para esta acción.	Obligatorio	
ALR32	El sistema debe poder generar alarma en base a los recursos del sistema (utilización de la CPU, memoria, etc.).	Valorable	5
ALR33	La plataforma deberá permitir una visualización de las alarmas a través de una herramienta de “estilos” donde estos se puedan modificar dependiendo de las necesidades del cliente.	Obligatorio	

4.5. Requisitos de Interfaz de Usuario (HMI)

ID	Descripción	Tipo	Puntos
RIU1	Interfaz web: El producto dispone de interfaz web basado en tecnologías estándar de internet.	Obligatorio	
RIU2	Diseño web adaptable: El producto permite un diseño web responsive.	Obligatorio	
RIU3	Esquema gráfico: El producto permite la visualización de la información de forma gráfica mediante una pantalla o esquema gráfico	Obligatorio	
RIU4	Valor señal analógica: El producto permite la representación de valores en tiempo real de las señales analógicas asociadas a cada esquema gráfico.	Obligatorio	
RIU5	Estado señales digitales: El producto permite la representación gráfica del estado de las distintas señales digitales asociadas a cada esquema gráfico mediante códigos de colores o cambios de iconos.	Obligatorio	
RIU6	Estado alarmas: El producto permite la representación gráfica del estado de las distintas alarmas asociadas a cada esquema gráfico mediante códigos de colores y/o simbología.	Obligatorio	
RIU7	Elemento representado: El producto permite que cada tipo de elemento sea representado por un icono de una biblioteca de símbolos, de manera que el mismo tipo de elemento tenga la misma representación en todos los esquemas gráficos.	Obligatorio	
RIU8	Color elemento representado: El producto permite la representación en varios colores de cada tipo de elemento, dependiendo del estado de la señal o alarma representada.	Obligatorio	
RIU9	Variación elemento representado: El producto permite la representación con diferentes iconos de cada tipo de elemento, dependiendo del estado de la señal o alarma representada.	Valorable	5
RIU10	Zoom: El producto permite acercar y alejar en los esquemas gráficos sin empeorar la visualización de los mismos.	Obligatorio	
RIU11	Desplazamiento: El producto permite el desplazamiento dentro de los esquemas gráficos.	Obligatorio	
RIU12	Gráfica comparativa de señales: El producto permite representar en una misma gráfica varias señales, permitiendo	Obligatorio	

	cambiar el eje temporal X, la representación de color y grosor de cada serie de señal, el rango de valores a mostrar en el eje Y de cada señal. La configuración de estas gráficas debe poder guardarse dentro del menú privado o compartido.		
RIU13	Menú: El producto permite la creación de un menú general configurable en forma de árbol jerárquico, pudiéndose cambiar, en modo diseño, las hojas entre las ramas del árbol y las ramas entre ellas arrastrándolas con el ratón.	Valorable	5
RIU14	Menú personalizado: El producto permite a cada usuario la creación de un menú personalizado donde pueda guardar los esquemas gráficos, cuadros de mando y gráficos de tendencias que desee.	Valorable	8
RIU15	Menú compartido: El producto permite la creación de un menú compartido entre los miembros de un mismo grupo de trabajo (basado en roles y/o grupos de seguridad definidos) donde guarden los esquemas gráficos, cuadros de mando y gráficos de tendencias que deseen.	Valorable	5
RIU16	Buscador pantallas: El producto posee un buscador de esquemas gráficos. La búsqueda se realizará en texto libre, siendo el buscador el responsable de analizar la consulta y devolver como resultado los esquemas que cumplen con los criterios de búsqueda.	Obligatorio	
RIU17	Buscador señales: El producto posee un buscador de señales al menos por tag y descripción, que devuelva las pantallas en las que se representen los valores de esa señal.	Obligatorio	
RIU18	La señal encontrada aparecerá resaltada en el esquema gráfico para su fácil localización	Valorable	5
RIU19	Configurabilidad del buscador: El producto permite una gestión sencilla de la configuración de los campos a indexar (pesos, prioridades, etc.).	Valorable	4
RIU20	Ventana detalle: El producto permite que cada elemento posea su propia ventana de detalle asociada.	Obligatorio	
RIU21	Tipos ventana detalles: El producto permite que la configuración de cada ventana de detalle dependa del tipo de elemento.	Obligatorio	
RIU22	Permisos ventana detalle: El producto permite aplicar diferentes permisos de acceso a la información mostrada en la ventana de detalle en función de los diferentes roles de usuarios definidos.	Obligatorio	
RIU23	Información ventana detalle 1: El producto permite que en la ventana de detalle se visualice el nombre y la descripción del elemento asociado.	Obligatorio	
RIU24	Información ventana detalle 2: El producto permite que en la ventana de detalle se visualicen las distintas jerarquías de la señal (Automatización, Infraestructuras) del elemento asociado.	Obligatorio	
RIU25	Información ventana detalle 3: El producto permite que en la ventana de detalle se visualice información adicional del elemento asociado, a través de enlaces web a otros sistemas.	Obligatorio	
RIU26	Información ventana detalle 4: El producto permite que en la ventana de detalle se visualice el estado del elemento asociado (conectado, desconectado, valor impuesto, etc.).	Obligatorio	

RIU27	Información ventana detalle 5: El producto permite que en la ventana de detalle se visualice el valor y la fecha de la última actualización del elemento asociado, auto refrescándose cuando varíen.	Obligatorio	
RIU28	Información ventana detalle 6: El producto permite que en la ventana de detalle se visualice el protocolo de actuación especiales, comentarios generales y de mantenimiento del elemento (campos del registro de definición).	Obligatorio	
RIU29	Información ventana detalle 7: El producto permite que en la ventana de detalle se visualice una gráfica de valores en el tiempo del elemento.	Obligatorio	
RIU30	Información ventana detalle 8: El producto permite que la gráfica y el resto de valores del elemento asociado se refresquen automáticamente.	Obligatorio	
RIU31	Información ventana detalle 9: El producto permite que la gráfica de valores en el tiempo del elemento asociado, presente escalado automático de los ejes.	Valorable	8
RIU32	Información ventana detalle 10: El producto permite que la gráfica de valores en el tiempo del elemento asociado, presente escalado ajustable manualmente de los ejes.	Valorable	8
RIU33	Información ventana detalle 11: El producto permite que el escalado del eje horizontal (eje de tiempo) determine qué detalle de dato mostrar: hasta un tiempo X muestra valores en tiempo real, para un tiempo entre X e Y muestra medias minutas, para un tiempo entre Y y Z muestra medias horarias y para un tiempo mayor que Z muestra medias diarias.	Valorable	5
RIU34	Información ventana detalle 12: El producto permite que en la ventana de detalle se visualice la información de los valores de la gráfica temporal del elemento asociado en formato tabla a través de un botón.	Valorable	10
RIU35	Información ventana detalle 13: El producto permite que en la ventana de detalle se enlace hacia otras ventanas de detalle otros elementos derivados o relacionados.	Valorable	10
RIU36	Información ventana detalle 14: El producto permite que en la ventana de detalle se visualice información relacionada con el PLC de campo (dirección, etc.) únicamente para usuarios con permisos avanzados.	Valorable	10
RIU37	Información ventana detalle 15: El producto permite que en la ventana de detalle se pueda cambiar diferentes parámetros ajustables (límites, gradientes, márgenes de sensibilidad y coeficientes de conversión) con un registro de cambios, únicamente para usuarios con permisos avanzados.	Obligatorio	
RIU38	Información ventana detalle 16: El producto permite que en la ventana de detalle se pueda desconectar el equipo de la señal que se recibe de campo con un registro de cambios, únicamente para usuarios con permisos avanzados.	Obligatoria	
RIU39	Información ventana detalle 17: El producto permite desde la ventana de detalle asociar un estado de conectado o no conectado con subestados asociados a cada uno (ejemplo: desconectado puede tener como subestado: mantenimiento, sin servicio, reparación o no instalado) de forma que determinadas rutinas de cálculo de valores o alarmas se	Valorable	10

	detengan y se activen otras tareas como pueden ser ordenes de trabajo.		
RIU40	Cuadro de mando: El producto permite la creación de cuadros de mando configurables por el usuario.	Obligatorio	
RIU41	Layout de cuadros de mando: El producto ofrece plantillas para crear distintos tipos de cuadros de mando.	Valorable	1
RIU42	Roles: El producto restringe el acceso a los cuadros de mando dependiendo del rol o grupo de usuario.	Obligatorio	
RIU43	Esquemas gráficos en CM: El producto permite que se pueda incorporar a los cuadros de mando esquemas gráficos ya existentes. Los esquemas son enlaces y no copias. Presentan las mismas utilidades y/o enlaces del original.	Valorable	2
RIU44	Gráficas temporales en Cuadros de Mando: El producto permite crear composiciones de gráficas temporales con cualquier tag o información tipo fecha-valor, aunque no esté historizada.	Obligatorio	
RIU45	Marcadores: El producto permite incluir/guardar marcadores en los cuadros de mando.	Valorable	1
RIU46	Fórmulas y combinaciones: El producto permite aplicar fórmulas/combinaciones de diferentes señales en los cuadros de mando.	Obligatorio	
RIU47	Indicadores KPI: El producto permite definir indicadores KPI, actualizables en tiempo real, en los cuadros de mando.	Obligatorio	
RIU48	Gráficas básicas: El producto para los cuadros de mando permite diferentes tipos de gráficas para la representación de los indicadores KPI y demás elementos (diagrama de líneas, columnas o barras, circulares, velocímetros)	Obligatorio	
RIU49	Gráficas avanzadas: El producto para los cuadros de mando permite diferentes tipos de gráficas avanzadas (diagrama radial de Kiviatt, dispersión de puntos con ajuste polinómico, mapas de calor, gráficos de rectángulos, proyección solar, etc.).	Valorable	5
RIU50	Desplazamiento temporal: El producto permite el desplazamiento temporal sobre las gráficas temporales de los cuadros de mando.	Valorable	2
RIU51	Configuración de ejes: El producto trae utilidades para la configuración de los ejes de las gráficas de indicadores.	Valorable	1
RIU52	Ayuda: El producto tiene una ayuda contextual accesible desde el HMI	Valorable	5
RIU53	La plataforma de visualización deberá disponer de una funcionalidad de playback. Esto es, ser capaz de reproducir, sobre los gráficos y sinópticos habituales, la visualización retrospectiva de la instalación en un tiempo anterior y permitir, desde ese punto, la reproducción a velocidades seleccionables por el usuario.	Valorable	5

4.6. Requisitos de Herramientas de Desarrollo

El producto debe permitir la extensión de funcionalidad, para lo cual debe ofrecer un conjunto de herramientas coherente para dichas ampliaciones. La forma en que se realicen dichas extensiones puede no ser la misma a la descrita en los requisitos, pero deben poder

conseguirse los mismos objetivos (personalización de funcionalidad, facilidad de depuración y simulación, ...).

ID	Descripción	Tipo	Puntos
HER1	Application Programming Interface: El producto tiene un API documentado para permitir la extensión de funcionalidad del producto.	Obligatorio	
HER2	Hooks: El producto tiene definidos puntos de enganche para ampliar la funcionalidad del producto en esos puntos (respuesta a eventos, callback, ...)	Obligatorio	
HER3	Entorno de programación 1: La herramienta de programación para extensión de funcionalidad debe contener las facilidades de un Integrated Development Environment tales como coloreado de sintaxis, sugerencias de métodos de clase, etc. En caso del uso de lenguajes estándar, se entiende cumplido este requisito si el entorno de desarrollo que utiliza el producto es un IDE habitual de dicho lenguaje (Eclipse, NetBeans, Visual Studio,...).	Obligatorio	
HER4	Entorno de programación 2: El entorno de programación debe ofrecer facilidades para la depuración y simulación de código (fijar valores, variables, vigilar variables, breakpoints, step over o step into un componente).	Obligatorio	
HER5	Control de versiones: El producto debe permitir el control de versiones de las extensiones de código, reglas, workflows y esquemas, a través de interfaces con herramientas open source de tal propósito (Subversion, GitHub,...).	Valorable	3
HER6	Interfaz creación reglas y workflows 1: El producto presenta un interfaz gráfico que permite representar y codificar los distintos procesos en un diagrama de flujo.	Valorable	4
HER7	Interfaz creación reglas y workflows 2: El interfaz de creación de reglas y workflows posee componentes parametrizables reutilizables.	Valorable	2
HER8	Interfaz creación reglas y workflows 3: El interfaz de creación de reglas y workflows permite crear nuevos componentes parametrizables reutilizables	Obligatorio	
HER9	Interfaz creación reglas y workflows 4: El interfaz de creación de reglas y workflows posee una herramienta de depuración que permite realizar pruebas de los workflows (fijar valores, variables, vigilar variables, breakpoints, step over o step into un componente).	Valorable	4
HER10	Interfaz creación de esquemas 1: El producto presenta un interfaz gráfico para la creación de esquemas.	Obligatorio	
HER11	Interfaz creación de esquemas 2: El interfaz de creación de esquemas gráficos contiene una biblioteca de símbolos definible y ampliable.	Obligatorio	
HER12	Interfaz creación de esquemas 3: El interfaz de creación de esquemas gráficos contiene plantillas (partes de esquemas) reutilizables y puede crearlas.	Valorable	2
HER13	Interfaz creación de esquemas 4: El interfaz de creación de esquemas gráficos permite de forma sencilla ubicar los diferentes símbolos y conexiones entre ellos.	Obligatorio	
HER14	Interfaz creación de esquemas 5: El interfaz de creación de esquemas gráficos permite de forma sencilla enlazar cada	Obligatorio	

	símbolo, caja o punto de datos con el valor de la señal deseada.		
HER15	Interfaz creación de esquemas 6: El interfaz de creación de esquemas gráficos permite de forma sencilla enlazar cada símbolo, caja o punto de datos con el valor de un dato extraído de una fuente de datos externa, normalmente otra base de datos.	Valorable	2
HER16	Interfaz creación de esquemas 7: El interfaz de creación de esquemas gráficos permite de forma sencilla enlazar cada símbolo, caja o punto de datos con el valor de una fórmula de cálculo especificada.	Obligatorio	
HER17	Interfaz creación de esquemas 8: El interfaz de creación de esquemas gráficos permite de forma sencilla dibujar a partir de figuras básicas (flechas, líneas, cuadrados, círculos, etc.).	Obligatorio	
HER18	Interfaz creación de esquemas 9: El interfaz de creación de esquemas gráficos permite de forma sencilla insertar etiquetas.	Obligatorio	
HER19	Interfaz creación de esquemas 10: El interfaz de creación de esquemas gráficos permite de forma sencilla incorporar dibujos en formato vectorial.	Valorable	4
HER20	Interfaz creación de esquemas 11: El interfaz de creación de esquemas gráficos permite de forma sencilla incorporar imágenes bitmap.	Valorable	2
HER21	Interfaz creación de esquemas 12: El interfaz de creación de esquemas gráficos permite de forma sencilla diseñar animaciones en función de los valores de señales digitales y analógicas.	Valorable	2
HER22	Interfaz creación de esquemas 13: El interfaz de creación de esquemas gráficos crea como resultado un fichero no binario (JSON, XML o similar) de manera que pueda ser tratado con programas externos.	Valorable	5
HER23	Interfaz con base de datos: El producto permite la conexión a su base de datos a través de un interfaz tipo SQL o similar.	Valorable	10
HER24	Simulación de escenarios: El producto permite la simulación de escenarios a través de flujos de eventos simulados y respondiendo consistentemente a dicho flujo.	Valorable	6
HER25	Moviola: El producto permite la repetición de flujos de eventos para revisar los hechos ocurridos en un momento dado.	Valorable	5
HER26	Data Mining básico: El producto trae implementados algoritmos básicos de Data Mining, como correlaciones, clasificaciones y clustering.	Valorable	6
HER27	Data Mining ampliable: El producto permite la incorporación de nuevos algoritmos de búsqueda de patrones.	Valorable	6

4.7. Interfaces con otros sistemas

ID	Descripción	Tipo	Puntos
INT1	REST: El producto permite llamadas a sistemas externos a través de protocolo REST.	Obligatorio	

INT2	SOAP: El producto permite llamadas a servicios web SOAP.	Valorable	5
INT3	Exportación de datos: El producto permite exportar los datos mostrados en los cuadros de mando y ventanas de detalle a formato Excel y/o CSV.	Obligatorio	
INT4	ArcGIS : El producto permite la conexión a servicios de mapa y servicios geográficos de ESRI.	Valorable	10
INT5	Servicios de mapa: El producto permite la conexión a servicios de mapa OGC, Azure Maps y Google Maps.	Valorable	5
INT6	EAM: El producto permite la integración con software EAM a través de servicios web.	Valorable	2
INT7	Conector de base de datos 1: El producto permite la conexión a su base de datos a través de tecnología de conectores estándar ODBC.	Valorable	5
INT8	Conector de base de datos 2: El producto permite la conexión a su base de datos a través de tecnología de conectores estándar JDBC.	Valorable	5
INT9	Telemandos: El producto debe implementar los mecanismos necesarios (end to end) para el envío de telemandos y su posterior confirmación, identificando de forma unívoca las transacciones entre el producto y el PLC remoto.	Obligatorio	
INT10	OPC UA Server: El producto es capaz de ofrecer datos a través del estándar OPC UA	Obligatorio	
INT11	BIM: La plataforma dispondrá de un módulo de integración de formatos BIM que permita la visualización dinámica en 3D.	Valorable	6
INT 12	API de Consulta de datos: La plataforma dispondrá de un API de consulta para consultar datos desde sistemas externos.	Valorable	10
INT 13	Telemandos: debe integrar el protocolo/driver de telecontrol y telemando actual (S7 Sinaut). La comunicación entre el controlador SCADA y los nodos (estaciones) de Telecontrol se deberá realizar vía TCP/IP a través de un Módulo de comunicaciones (TIM) maestro como puerta de enlace. Dicho protocolo garantiza directamente la redundancia del SCADA, por lo tanto, se deberá poder configurar una conexión redundante al driver en el proyecto para cada TIM maestro que se comunicará con el controlador. En base a esta compatibilidad, el SCADA debe de soportar la recepción de Trama Ethernet según IEEE 802.3, sobre Protocolo TCP/IP en las capas 3 y 4 en el Puerto TCP usado por defecto empaquetado en un marco de protocolo S7 y enviado como Payload sobre TCP/IP.	Valorable	10

4.8. Requisitos de Arquitectura de Sistemas, Seguridad y Redes

ID	Descripción	Tipo	Puntos
SSR1	Modelo de seguridad de base de datos: El producto permite establecer unos niveles de seguridad en función de los cuales se tienen mayores o menores privilegios para la visualización, modificación y el borrado de registros en la base de datos en tiempo real.	Obligatorio	
SSR2	Seguridad menú: El producto permite aplicar permisos de acceso en cada rama o esquema del menú en función de los roles de usuario.	Obligatorio	
SSR3	Seguridad buscador: El buscador permite aplicar permisos de acceso a los resultados del menú en función de los distintos roles de usuario, no mostrando aquellos resultados a los que no se tenga permisos.	Valorable	10
SSR4	Seguridad funcional: El producto permite restringir la funcionalidad en función de los roles de los distintos usuarios, de forma que se pueda controlar la modificación de valores desde la ventana de detalle, la ejecución de telemandos, la desconexión de equipos y cualquier otra función.	Obligatorio	
SSR5	Trazabilidad de accesos: El producto permite realizar la auditoria y trazabilidad de acceso de usuarios al sistema, de forma configurable.	Valorable	10
SSR6	Trazabilidad de cambios en valores de la señal: El producto registra los cambios realizados en los distintos parámetros de la señal (límites, descripciones, porcentaje del gradiente, ...) registrando al menos fecha, usuario, parámetro modificado, valor antiguo, valor nuevo y opcionalmente comentarios con el motivo del cambio.	Valorable	10
SSR7	Configuración del sistema: Las labores de configuración y administración del sistema están restringidas a roles específicos y los cambios realizados son trazables.	Obligatorio	
SSR8	Oracle: El producto soporta como base de datos la BBDD corporativa Oracle	Valorable	10
SSR9	Separación de redes: La arquitectura de la solución debe permitir la separación de la RED Industrial/Enterprise DMZ (donde residirá el producto y la base de datos en tiempo real), por un lado de la Red Corporativa de Datos (Enterprise Network) y por otro de la Red de Telecontrol (Industrial Network, donde están los autómatas Front-End del sistema de telecontrol y el resto de PLC y sensores).	Valorable	10
SSR10	Alta disponibilidad: La arquitectura de la solución debe ser de alta disponibilidad, constando de varios nodos de forma que la caída de cada uno de ellos no suponga pérdida de servicio total o parcial del sistema.	Obligatorio	
SSR11	Escalabilidad horizontal: La arquitectura de la solución debe ser escalable horizontalmente, de forma que soporte un incremento en el número de señales, en la frecuencia de las	Obligatorio	

	mismas y/o en los procesamientos a realizar mediante la adición de nuevos nodos de proceso.		
SSR12	Arquitectura x86_64: El producto funciona sobre plataformas hardware de arquitectura x86_64	Obligatorio	
SSR13	Virtualización: El producto funciona sobre plataformas de virtualización de hardware VMWare.	Obligatorio	
SSR14	Autodiagnóstico: El producto permite monitorizarse a sí mismo, mostrando alertas de fallos de funcionamiento o degradación del sistema.	Valorable	5
SSR15	Actualizaciones en caliente: El producto permite realizar actualizaciones de versión y parches sin necesidad de interrumpir el servicio, tanto de adquisición de datos como de servicio a los usuarios.	Valorable	10
SSR16	La comunicación entre el interfaz HMI y la base de datos en tiempo real se realizará mediante protocolos seguros. En caso del interfaz web, se soportará HTTPS permitiendo configurar los protocolos (por ejemplo TLS 1.2) y las suites de cifrado.	Valorable	10
SSR17	Autenticación en Active Directory: El producto permite la autenticación integrada de usuarios con Microsoft Active Directory o Azure Active Directory	Valorable	10
SSR18	Roles en Active Directory: El producto permite la definición de roles y/o autorizaciones a través de grupos de Microsoft Active Directory.	Valorable	10
SSR19	Soporte del sistema a una arquitectura híbrida. Posibilidad de que la arquitectura pueda verse modificada y trasladar alguno de sus componentes a cualquiera de las principales plataformas cloud, ya sea el histórico o el tiempo real.	Obligatorio	

4.9. Requisitos de Modo de Licenciamiento

ID	Descripción	Tipo	Puntos
LIC1	Todas las licencias de la plataforma deberán estar dentro de una lista de precios pública en España con precios indicados en Euros.	Obligatorio	
LIC2	La compra de licencias sólo podrá llevarse a cabo por medio de unas de las tres modalidades siguientes: <ol style="list-style-type: none"> 1. Las licencias podrán ser en la modalidad Perpetuas, es decir, ser adquiridas por Canal con un pago único al inicio del proyecto. En esta modalidad de licenciamiento, las extensiones pueden implicar la adquisición de nuevas licencias o ampliación de las existentes, por incremento en el número de señales, incremento en el número de usuarios, incremento de datos históricos etc 	Obligatorio	

	<p>2. Las licencias podrán ser en la modalidad por Suscripción, es decir, realizando un pago anual en el que estará integrado el uso de licencias acordado y su mantenimiento.</p> <p>3. Las licencias podrán ser en la modalidad por Créditos en el que el proveedor deberá permitir al cliente la compra de una bolsa de créditos que podrá canjear por cualquiera de las licencias integradas en el portfolio de soluciones. La forma de adquirirlos será la siguiente:</p> <ul style="list-style-type: none"> • El usuario adquiere paquetes de créditos anualmente. Pago anual. • Cada licencia supone un nº de créditos determinado • El número de créditos puede incrementarse o reducirse al fin de contrato • No requiere compromiso de software. Posible utilización de cualquier software incluido dentro de la modalidad por créditos • Está incluida la actualización de software y soporte 		
LIC3	Al ser un sistema clasificado como crítico para la continuidad de negocio de Canal de Isabel II, S.A., el modo licenciamiento permitirá la continuidad del servicio en el caso de que se produjera la circunstancia de que cumpliera el plazo de vigencia del contrato y la renovación del mismo estuviera en trámite pero no formalizada. Si se produjera esta circunstancia Canal de Isabel II, S.A. solicitaría formalmente al fabricante del software la continuidad del servicio durante al menos 3 meses comprometiéndose a la renovación del mismo. Para ello, el licitador deberá incluir en su oferta un compromiso por parte del fabricante a la continuidad de servicio para el software contratado, en caso de retraso en la renovación de las licencias tras el vencimiento del contrato	Valorable	10
LIC4	El licenciamiento debe estar dimensionado para un número de usuarios estimado de al menos 1.500.	Obligatorio	
LIC5	Licencias de punto fijo para ciertos usuarios: En caso de que el modo de licenciamiento tenga limitación de usuarios, debe permitir la fijación de licencias en ciertos equipos o para ciertos usuarios, de forma que siempre estén disponibles en el Centro de Control. En caso de no existir limitación de usuarios, este requisito se marcará en la plantilla como "Cumple".	Valorable	5

4.10. Requisitos de Capacidad y Rendimiento

ID	Descripción	Tipo	Puntos
CAP1	Número de valores a historizar: El sistema debe ser capaz de mantener un histórico accesible desde el producto de 100.000.000.000 (cien mil millones) de valores de señales.	Obligatorio	
CAP2	Tiempo de consulta de un valor único: El tiempo de consulta de un valor único del histórico para una señal en un instante de tiempo dado debe ser inferior a 3 segundos.	Obligatorio	
CAP3	Tiempo de consulta de un rango de valores de una señal: El tiempo de consulta de un rango de valores de un día para una señal debe ser inferior a 10 segundos.	Obligatorio	
CAP4	Número de señales a tratar: El sistema debe ser capaz de gestionar un flujo de 10.000 señales por segundo.	Obligatorio	
CAP5	Tiempo de refresco del interfaz 1: El tiempo de refresco del interfaz de usuario para mostrar los valores en una pantalla con menos de 10 señales debe ser inferior a 3 segundos.	Obligatorio	
CAP6	Tiempo de refresco del interfaz 2: El tiempo de refresco del interfaz de usuario para mostrar los valores en una pantalla con menos de 75 señales debe ser inferior a 5 segundos.	Obligatorio	
CAP7	Tiempo de refresco del interfaz 3: El tiempo de refresco del interfaz de usuario para mostrar los valores en una pantalla con menos de 200 señales debe ser inferior a 7 segundos.	Obligatorio	
CAP8	Carga del sistema: El sistema debe soportar una carga sostenida de 300 usuarios trabajando on-line concurrentes lanzando una petición de datos al sistema cada 10 segundos manteniendo de media los tiempos de respuesta de los requisitos anteriores.	Obligatorio	

4.11. Requisitos del ecosistema de la plataforma

ID	Descripción	Tipo	Puntos
REP1	El fabricante de software deberá disponer de un programa de certificación de empresas y personas, que permita evaluar a través de exámenes presenciales en España su nivel de conocimiento.	Obligatorio	
REP2	El fabricante del software deberá contar con una red de al menos más de un integrador en España	Obligatorio	

	certificado y con conocimiento sobre las herramientas a implementar.		
REP3	El fabricante del software deberá contar con una red de al menos 10 integradores en España certificados y con conocimiento sobre las herramientas a implementar.	Valorable	5
REP4	El fabricante del software deberá contar con una red de al menos 30 integradores en España certificados y con conocimiento sobre las herramientas a implementar.	Valorable	10
REP5	El fabricante deberá disponer de un calendario de formación para integradores de sistema y usuarios finales sobre las herramientas objeto de este pliego.	Valorable	3
REP6	El soporte técnico de fabricante deberá tener varios niveles de soporte, siendo como mínimo el primer nivel en castellano, desde España. El resto de los niveles podrán ser ejecutados desde otras regiones, en inglés.	Obligatorio	
REP7	El fabricante supervisará la instalación y configuración del sistema, asegurando así la calidad del producto implantado	Obligatorio	

4.12. Requisitos del mantenimiento y soporte

ID	Descripción	Tipo	Puntos
RMS1	<p>El soporte contratado debe contemplar un tiempo de atención máximo para las distintas categorías de incidencias. Las categorías de incidencias y los plazos de atención a las mismas son los siguientes:</p> <ul style="list-style-type: none"> Emergencias: Aquellas que supongan una parada o inactividad del funcionamiento del sistema o que provoquen la imposibilidad de algún proceso de supervisión crítico. Se atenderán en un plazo no superior a 2h. La resolución de la reclamación deberá 	Obligatorio	

	<p>realizarse en un plazo no superior a 24h y en servicio 24x7.</p> <ul style="list-style-type: none"> • Incidencias o errores: Disfunciones que producen información o resultados erróneos, o que provoquen la imposibilidad de algún proceso no crítico. Se atenderán dentro de la jornada de trabajo en que se notifiquen si ésta se ha realizado antes de las 13:00 horas y serán atendidas el siguiente día laborable en caso contrario. La resolución de la anomalía deberá realizarse en un plazo no superior a 48h y en servicio de 8x5 al menos. • Consultas o anomalías menores: se atenderán y resolverán en un plazo no superior a 72h desde su comunicación con atención de servicio en 8x5. 		
RMS2	<p>Cuando una anomalía urgente requiera una intervención en las instalaciones de Canal, el tiempo de atención y desplazamiento no podrá exceder las 3 horas (incluyendo las 2 horas de atención), por lo que el licitante deberá acreditar que dispone de personal técnico y de una oficina de atención o soporte técnico en la Comunidad de Madrid o provincias limítrofes a fin de cumplir el requerimiento de atención de anomalías urgentes.</p>	Obligatorio	

4.13. Requisitos de Seguridad

ID	Descripción	Tipo	Puntos
SE01	<p>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 (suites de cifrado que hagan uso del modo de cifrado de cadena de bloques (CBC)), POODLE (SSL 3.0 y TLS 1.0), CRIME (TLS 1.0 compression), SWEET32 (3DES), Logjam (intercambio de claves de menos de 2048 en DH), DROWN (TLS 1.x con soporte a SSLv2), etc.).</p>	Obligatorio	
SE02	<p>Todos los formularios, incluidos los de inicio de sesión, tienen que estar protegidos contra</p>	Obligatorio	

	ataques de fuerza bruta (uso de reCAPTCHA, 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), XML External Entity Injection, (XXE), Inyección SQL, etc.		
SE03	El uso de un esquema de BBDD propio para la información propiedad de Canal de Isabel II, S.A.	Obligatorio	
SE04	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.	Obligatorio	
SE05	Cifrado robusto de los datos propiedad de Canal de Isabel II, S.A. en la propia BBDD, ya sea como cifrado completo o cifrado del dato.	Obligatorio	
SE06	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, scrypt, versiones modernas no vulnerables de Argon2 (por ejemplo, Argon2d), etc.).	Obligatorio	
SE07	Exista la posibilidad de uso de, al menos: a. Un esquema XML para el intercambio de datos de autenticación y autorización (por	Obligatorio	

	<p>ejemplo, SAML 2.0) e implementaciones de seguridad a nivel del mensaje.</p> <p>b. OAuth 2.0 como framework de autorización y OpenID Connect (OIDC) como protocolo de autenticación en las APIs existentes.</p> <p>c. SCIM como modelo para automatizar el intercambio de información de identidad de los usuarios entre distintos dominios de identidad.</p>		
SE08	<p>En caso de existir Web Services que puedan ser consumidos desde Canal de Isabel II, S.A., deben estar securizados a nivel de mensaje, especificando la forma de firmar y cifrar los mensajes de tipo SOAP, a través de la especificación WS-Security. Por tanto:</p> <p>a. Los servicios deben estar autenticados, preferentemente con WS-Security Tokens</p> <p>b. Los usuarios deben ser autenticados vía SAML 2.0.</p> <p>c. La integridad de la información ha de estar garantizada a través del uso de protocolos seguros (TLS 1.2 o superior) o vía WS-Signature.</p> <p>d. El no repudio debe estar garantizado a través del uso de WS-Signature o WS-Addressing.</p> <p>e. La confidencialidad de la información ha de estar garantizada a través del uso de protocolos seguros (TLS 1.2 o superior) o vía WS-Encryption.</p> <p>f. Debe hacerse uso de una política de seguridad (WS-Policy).</p>	Obligatorio	
SE09	<p>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. Es recomendable que la aplicación del 2FA se fuerce a nivel de administración del aplicativo y que no pueda ser deshabilitado por el propio usuario. En caso de que el 2FA sí pueda ser deshabilitado por el propio usuario, es obligatorio que existan y se implementen, al menos, los siguientes controles compensatorios adicionales: notificación automática de eventos</p>	Obligatorio	

	(usuario que deshabilita el 2FA, inicio de sesión e inicio de sesión desde direcciones IP extranjeras) y por distintos medios (SMS, correo, etc.), posibilidad de generación de informes periódicos con el listado del estado de configuración de los usuarios (por ejemplo, usuarios que tienen habilitado o deshabilitado el 2FA) y restricción de acceso al servicio desde los rangos IP públicos de Canal de Isabel II, S.A.		
SE10	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, etc.) para comprobar que existen y que han sido implementadas correctamente.	Obligatorio	
SE11	El proveedor del servicio Cloud almacenará, de forma detallada (al menos, fecha y hora, usuario y dirección IP origen, acción realizada, resultado de la acción (correcto, error) y componente(s) afectados por la acción) y segura (garantía de acceso, recuperación y no modificación), tanto todos los eventos con las actividades realizadas por los usuarios como los eventos sobre la información propiedad de Canal de Isabel II, S.A. (al menos, creación, modificación y borrado), y revisará de forma regular dichos eventos para detectar posibles errores y posibles problemas de seguridad en el servicio. Estos registros deberán mantenerse por el proveedor al menos durante cinco (5) años.	Obligatorio	

5. PROYECTO DE IMPLANTACIÓN BÁSICA

5.1. Requisitos del Proyecto De implantación básica

Para la validación del producto, el implantador o fabricante debe realizar una implantación básica que permita demostrar la adecuación del producto a los requerimientos. Esta implantación básica tendrá un plazo máximo de ejecución de 4 meses desde la firma del Acta de Inicio de los trabajos a partir de que Canal de Isabel II ponga a disposición del adjudicatario los servidores con los requerimientos del producto para el desarrollo del de implantación básica.

La implantación básica deberá cumplir los siguientes requisitos:

PIL0: El producto permitirá modelar las estructuras de datos según están definidas en el estándar unificado de Canal de Isabel II, así como replicar el comportamiento y simbología de los elementos gráficos representados en dicho estándar unificado

PIL1: Conexión a través de OPC a las estaciones primarias redundadas en el centro de respaldo y adquisición y persistencia del flujo de datos de las mismas.

PIL2: Filtrado, procesamiento y almacenado (en base de datos en tiempo real) de las señales analógicas (necesarias para la generación de los esquemas de pruebas) para la obtención de medidas calculadas a partir de la señal de campo. Estos tipos de señales son fácilmente identificables por el valor del tipo de equipo de su registro de definición. El filtrado consiste en procesar y almacenar el valor solamente si ha cambiado más de un porcentaje configurable respecto al valor anterior. Se deberán configurar, al menos, dos tipos de procesamiento de señal, por un lado, señales que llegan de campo con el valor de ingeniería y señales que llegan de campo con el resultado de la conversión analógico-digital (pesos), las cuales requieren la conversión a porcentaje sobre un fondo de escala y la aplicación de un coeficiente para obtener el valor en unidades de ingeniería. Todos los coeficientes que se apliquen deberán ser configurables.

PIL3: Almacenado de todos los cambios de las señales digitales simples y dobles, sin procesamiento, en base de datos en TR y en BD relacional.

PIL4: Procesamiento y almacenado (en base de datos en tiempo real) de las medidas de presión, aplicando un procesamiento polinómico

PIL5: Generación de medias temporales con la frecuencia acordada de las señales de caudal y nivel, en BD relacional, persistiendo tanto el valor medio como el valor máximo, mínimo e instantáneo del periodo.

PIL6: Sumario de alarmas en el que deben aparecer las alarmas generadas por el sistema, especialmente las definidas en estos requisitos. En caso de que la alarma sea producida por una única señal, debe de poder abrirse la Ventana de Detalle de la señal que genera la alarma. Todas las alarmas deben historizarse, tanto en base de datos en

TR como en BD relacional, indicando hora de inicio de alarma, hora de fin de alarma y todas las actuaciones manuales que realicen los operadores sobre ellas.

PIL7: Creación de un simulador de eventos que permita introducir medidas simuladas en el sistema para probar las condiciones de alarma.

PIL8: Generación de alarmas de límites en las señales de caudal y nivel. Se establecerán para todas estas señales un Límite Superior del 80% del valor máximo y un Límite Inferior del 10% del valor máximo por defecto.

PIL9: Generación de alarmas de gradientes (cambio de valor entre dos valores consecutivos en un intervalo de tiempo configurable) para las señales de caudales y niveles de PIL2. Se establecerá para estas señales un gradiente del 5% que se aplicará sobre el valor actual.

PIL10: Generación de alarmas de Avería en Sensor para las señales que estando implementadas en campo en lazo de corriente 4-20 mA, se envíen con los pesos correspondientes a 0-20mA, cuando el valor de los pesos sea inferior al que corresponde a 4 mA o superior a 20 mA. con una tolerancia del 2%.

PIL11: Generación de alarmas de señales digitales simples cuyo tipo de equipo sea GEN0 (señales digitales). Estas señales indican alarma cuando pasan a valor 1.

PIL12: Generación de alarma de Avería en Sensor Reiterada cuando sobre la misma señal se producen N alarmas en un periodo T de tiempo (inicialmente N=3 y T=24 horas).

PIL13: Generación de alarma de una señal digital, simple o doble, por permanencia temporal (La alarma se disparará cuando la señal esté activa por lo menos durante un tiempo configurable)

PIL14: Generación de alarma de Valor Estacionario sobre todas las señales de caudal cuando un caudal no varíe durante un periodo T de tiempo (inicialmente T=30 minutos).

PIL15: Generación de 5 alarmas compuestas como combinación AND y OR de varias señales digitales (por ejemplo, fallo de suministro en planta a partir de varias señales de fallo en CCM individuales).

PIL16: Generación de 5 alarmas compuestas como combinación AND y OR de señales digitales y comparaciones analógicas, sin componente temporal ($\text{caudal1} < \text{caudal2}$, $\text{caudal1} < 1\text{m}^3/\text{s}$ OR $\text{caudal1} \geq 1.5\text{m}^3/\text{s}, \dots$).

PIL17: Generación de 3 alarmas con componente temporal:

- Variación de caudal1 mayor a X% en un periodo T
- No se produce incremento de caudal1 tras un periodo T desde la apertura de compuerta 1
- Decremento de presión1 mayor que P y decremento de caudal1 mayor que Q durante un periodo T.

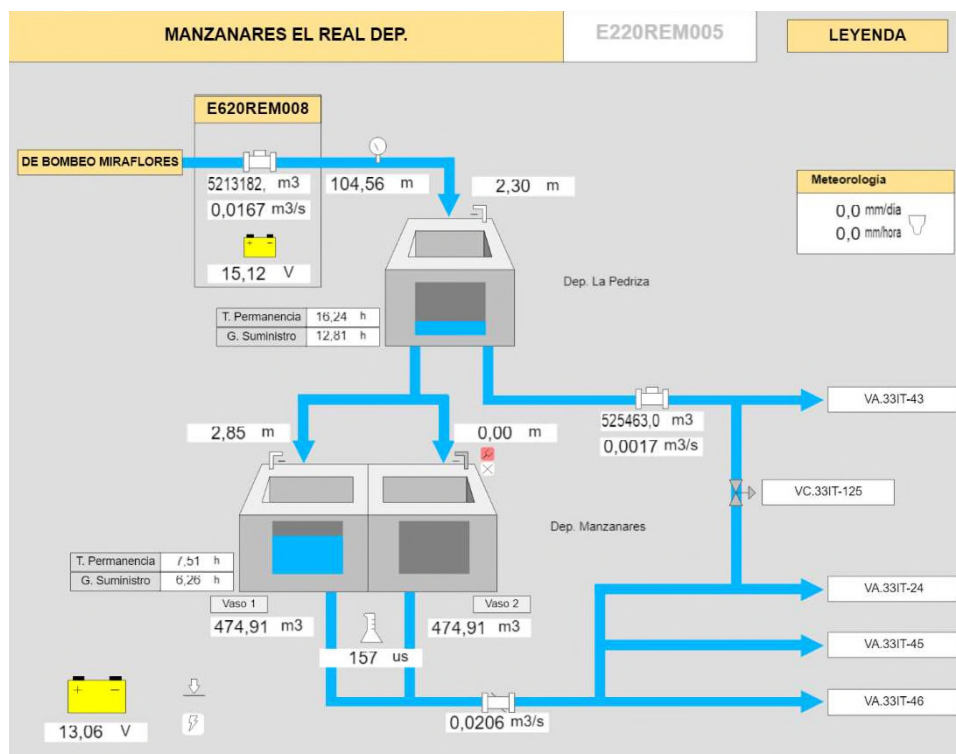
PIL18: Simulación de ejecución de un telemando por parte de un usuario con un perfil de seguridad adecuado, mediante escritura OPC en el front-end de telemandos. Para

ello se tendrá un interfaz de usuario que muestre el valor actual de un telemando del sistema y permita introducir el nuevo valor de consigna.

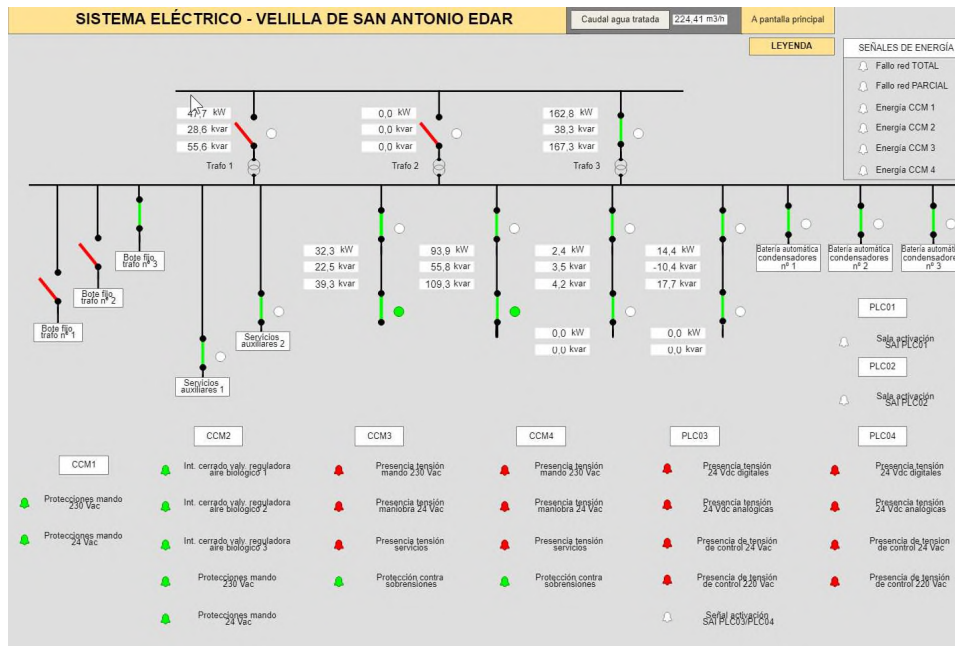
PIL19: Workflow desencadenado como respuesta a una de las alarmas de PIL14 que llame a un servicio REST para crear un aviso en un sistema externo y envíe un correo electrónico a una lista de distribución.

PIL20: Modelado de un equipo analizador de red eléctrica Sentron con las distintas señales de tensión, intensidad, potencia, energía y coseno de phi.

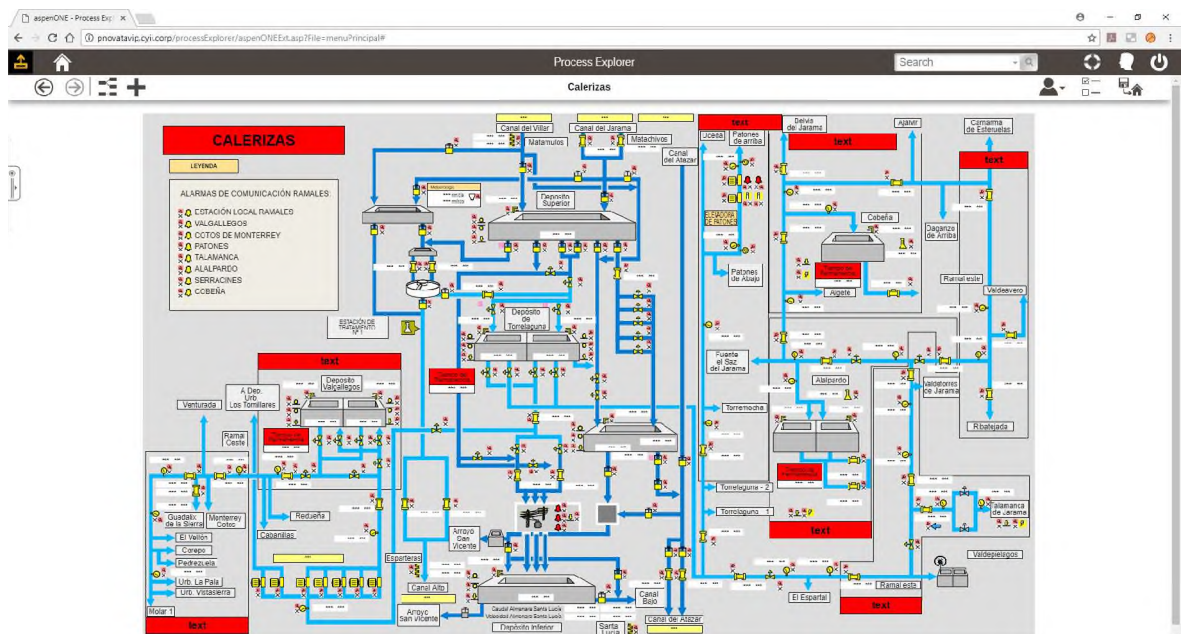
PIL21: Generación de un esquema sencillo con representación de pocas señales, como el que se muestra a continuación.



PIL22: Generación de un esquema medio con la representación de un sistema Eléctrico, como el que se muestra a continuación.



PIL23: Generación de un esquema complejo con la representación de un nudo de distribución, como el que se muestra a continuación.



PIL24: Generación de interfaz básica de usuario con menú de acceso a las instalaciones. En el menú se replicarán 500 veces cada uno de los tres esquemas de la implantación básica (modificando el nombre en cada copia) con una profundidad de 3 niveles (10 carpetas de primer nivel, con 10 carpetas de segundo nivel cada una y 15 esquemas en cada una) Se probará el cambio de hojas y de ramas del árbol arrastrándolas con el ratón.

PIL25: Buscador con parametrización para buscar esquemas, códigos de señales, descripciones de equipos y señales. La paginación de resultados será de 10 elementos.

PIL26: Ventana de Detalle de señal con código, descripción, datos básicos, gráfica de evolución temporal de la señal con posibilidad de ajuste de la escala temporal (por defecto 48 horas con campos “Desde” y “Hasta” que permitan indicar nuevas fechas y horas) y de la escala de valores (por defecto desde cero hasta el valor del fondo de escala, con campos máximo y mínimo para cambiar la escala). La ventana de detalle debe contener también campos editables para modificación de Límite Superior, Límite Inferior y Gradiente, además de poder poner a off el equipo para que no introduzca datos en la base de datos en tiempo real.

PIL27: Exportación a Excel de los datos de la gráfica de la ventana de detalle.

PIL28: El tiempo de respuesta de la pantalla compleja deberá ser de un máximo de 5 segundos. Entendiendo como tiempo de respuesta tanto la pantalla como los valores asociados a todas las señales.

PIL29: El tiempo de repuesta de la pantalla media deberá estar entre 2 y 4 segundos.

PIL30: El tiempo de respuesta de la pantalla sencilla deberá estar entre 1 y 3 segundos.

PIL31: El tiempo de respuesta de la Ventana de Detalle deberá ser de un máximo de 4 segundos. Entendiendo como tiempo de respuesta tanto la pantalla como los valores asociados a todas las señales

PIL32: El sistema deberá soportar una carga de 100 usuarios concurrentes lanzando una petición de datos cada 5 segundos, correspondiendo un 20% de las peticiones a esquemas complejos, un 20% a esquemas medios, un 20% a esquemas sencillos y un 40% a ventanas de detalle.

PIL33: Prueba esquema de seguridad en función de Roles y permisos definidos para distintos usuarios.

5.2. Gestión de implantación básica

Para el adecuado control del Proyecto de implantación básica (o Piloto), se realizará la gestión del mismo a través de la metodología de gestión de proyectos implantada en Canal de Isabel II.

Las áreas de gestión del proyecto necesarias para su adecuado seguimiento y control son las detalladas a continuación:

- Plan de Recursos
- Plan de Tiempo/Cronograma
- Plan de Costes
- Plan de Comunicación
- Plan de Calidad
- Plan de Riesgos/Contingencias

Será necesaria la aportación, por parte del proveedor en la oferta, de los planes correspondientes a dichas áreas de gestión. El conjunto de todos estos planes conformará el Plan de Proyecto.

El proveedor también deberá identificar en su oferta la infraestructura necesaria para el proyecto de implantación básica, con la que Canal de Isabel II deberá contar.

Se proporciona la documentación necesaria de la metodología y las plantillas de los documentos necesarios en el Anexo 2 del presente pliego.

La entrega de la documentación se realizará en formato Microsoft Word o Acrobat (pdf). Deben mantenerse todas las versiones de la documentación entregada, contemplando el control de los cambios. Todos los productos resultantes del trabajo quedarán en posesión de Canal.

El alcance de la implantación básica comprende, dependiendo de las particularidades de la plataforma software, las siguientes tareas:

1 Análisis básico requerimientos

- P1.1 Análisis conexión a orígenes de datos
- P1.2 Análisis tipos lecturas de campo asociada y modelado de sensor
- P1.3 Análisis procesamiento de lecturas de campo
- P1.4 Análisis Sumario Alarmas
- P1.5 Análisis Proceso Generación alarmas para piloto
- P1.6 Análisis VD Piloto
- P1.7 Análisis Sumario Alarmas Piloto
- P1.8 Análisis Simulador Eventos Piloto
- P1.9 Análisis Simulador Telemandos piloto
- P1.10 Análisis Generación workflow piloto
- P1.11 Análisis diseño interfaz básica y menú acceso a esquemas piloto
- P1.12 Análisis diseño esquemas sencillo, medio, complejo

2 Diseño básico requerimientos y arquitectura

- P2.1 Diseño conexión piloto para lectura de orígenes de datos
- P2.2 Diseño tipos lecturas de campo piloto asociada y modelos de sensor
- P2.3 Diseño procesamiento piloto de lecturas de campo
- P2.4 Diseño proceso Generación alarmas para piloto
- P2.5 Diseño VD Piloto
- P2.6 Diseño Sumario Alarmas Piloto
- P2.7 Diseño Simulador Eventos Piloto
- P2.8 Diseño Simulador Telemandos piloto
- P2.9 Diseño Generación workflow piloto
- P2.10 Diseño diseño interfaz básica y menú acceso a esquemas piloto
- P2.11 Diseño diseño esquemas sencillo, medio, complejo

3 Configuración e Implementación piloto

- P3.1 Instalación y configuración servidores piloto
- P3.2 Implementación de modelos de sensores y lecturas de campo
- P3.3 Implementación procesamiento piloto de lecturas de campo
- P3.4 Implementación sistema Generación alarmas para piloto distintas tipologías
- P3.5 Implementación VD Piloto
- P3.6 Implementación Sumario Alarmas Piloto
- P3.7 Implementación Simulador Eventos Piloto
- P3.8 Implementación Simulador Telemandos piloto
- P3.9 Implementación Generación workflow piloto
- P3.10 Implementación diseño esquemas sencillo, medio, complejo
- P3.10 Implementación diseño interfaz básica y menú acceso a esquemas piloto con esquemas replicados

4 Aprobación

La facturación de la implantación básica se llevará a cabo del siguiente modo:

Bloques de actividades	Facturación	Método de facturación
1 y 2 Análisis y diseño	20%	Hito entregables
3 Configuración e implementación	60%	Incremento valor ganado
3 Aprobación (*)	20%	Hito validación

(*) Si la implantación básica no supera la validación de Canal, no podrá ser facturada por parte del adjudicatario

El porcentaje anteriormente indicado es sobre el importe indicado en la oferta referente al concepto de “Fase 1 – Implantación básico (Piloto)” en el Anexo II del PCAP.

5.3. Validación del Proyecto de implantación básica

El Proyecto de implantación básica debe cumplir cada uno de los requisitos solicitados y que serán verificados por parte del equipo de proyecto de Canal de la forma indicada en este apartado. También se deberá cargar el 10% de la información histórica del sistema actual a la nueva solución para la validación de la implantación básica.

Los requisitos de adquisición de datos PIL1 a PIL4 serán verificados a partir de los datos persistidos en el sistema durante 24 horas, comparando la cantidad de datos obtenidos con los esperados en cuanto a número de señales y valores a tener de cada señal. Será validado por personal de Canal.

El equipo de proyecto exportará los valores de 20 señales de caudal y nivel del SCADA actual y del nuevo sistema, comparando con Excel los valores obtenidos en ambos sistemas. Será validado por personal de Canal.

El requisito de medias dosminutales y horarias de PIL5 se realizará comparando con Excel las medias de esas 20 señales en el nuevo sistema con las obtenidas por el SCADA actual, admitiendo diferencias de un 5% en dosminutales y un 2% en el caso de horarias.

La validación del sumario de alarmas de PIL6 consta de una validación de la funcionalidad solicitada de apertura de ventana de detalle, así como comprobación del log de alarmas que debe registrar, y que se verificará en consonancia con los requisitos de generación de alarmas.

El simulador de eventos de PIL7 se probará introduciendo valores forzados de diversas señales para la realización de las pruebas de generación de alarmas.

Los límites PIL8 se comprobarán mediante cruce en Excel de los valores registrados y valores de límites de las medidas de caudal y nivel, comprobando en el log de alarmas la generación de las mismas. Así mismo, se comprobarán que todas las alarmas de límites registradas en el log de alarmas correspondieron efectivamente a la situación de superación de límite.

Los gradientes PIL9 se comprobarán mediante cruce en Excel de los valores registrados y variaciones entre valores, comprobando en el log de alarmas la generación de las mismas. Así mismo, se comprobarán que todas las alarmas de gradiente registradas en el log de alarmas correspondieron efectivamente a la situación de superación del umbral de variación de la señal.

Las Averías en Sensor PIL10 se comprobarán mediante comparación del log de alarmas del sistema de implantación básica con el log de alarmas del SCADA actual, debiendo coincidir ambos registros. En caso de discrepancias, se comprobará el motivo para determinar si el exceso o defecto de alarmas es debido a mal funcionamiento de la implantación básica o está justificado. Si no hay alarmas se forzarán con el simulador y se comprobará su correcto funcionamiento.

Las alarmas digitales simples para equipos tipo GEN0 de PIL11 se comprobarán mediante comparación del log de alarmas del sistema de implantación básica con el log de alarmas del SCADA actual, debiendo coincidir ambos registros. En caso de discrepancias, se comprobará el motivo para determinar si el exceso o defecto de alarmas es debido a mal funcionamiento de la implantación básica o está justificado. Si no hay alarmas se forzarán con el simulador y se comprobará su correcto funcionamiento.

Para las alarmas de Avería en Sensor Reiteradas de PIL12 se forzarán 20 con el simulador y se comprobará su correcto funcionamiento.

Para las alarmas de señales digitales por permanencia temporal, se provocará la situación de anomalía con el simulador, y se comprobará que se activa la alarma si la señal permanece en la situación anómala pasado el intervalo de tiempo configurado. Si se interrumpe la situación de anomalía antes de finalizar el intervalo de tiempo, la alarma no se debe activar.

En las alarmas de Valor Estacionario de PIL14 se forzarán 20 alarmas con el simulador y se comprobará su correcto funcionamiento.

Las alarmas complejas PIL15, PIL16 y PIL17 se validarán manualmente por el equipo de proyecto de Canal mediante el forzado de los valores necesarios con el simulador de eventos PIL7, comprobando que se generan las alarmas cuando se dan las condiciones para su disparo.

El telemando PIL18 se comprobará mediante el envío de 20 consignas al servidor OPC que conecta con el autómatas front-end a través del interfaz de usuario desarrollado en el proyecto de implantación básica, comprobando con el área de automatización que las consignas llegan correctamente al autómatas.

Para el workflow BPM PIL19 se comprobará que se dispara la ejecución del mismo al darse la condición de alarma definida, que se produce la llamada al servicio REST y el envío de correo.

El equipo de PIL20 debe cumplir ser un objeto reutilizable que tenga como atributos las diferentes señales, y se comprobará su correcto funcionamiento mostrándose en una ventana de detalle.

En los esquemas de PIL21, PIL22 y PIL23 se comprobará visualmente su correcto funcionamiento, que muestran los mismos valores que las pantallas del sistema actual y que los tiempos de carga cronometrados para el usuario están dentro de los rangos

definidos en PIL287, PIL298 y PIL30 para cada tipo de pantalla, con 20 repeticiones de carga de cada pantalla alternadas con navegación de menú.

El menú PIL31 se comprobará manualmente el plegado y replegado de los nodos del menú, que los enlaces funcionan correctamente y que soporta sin problemas el número de nodos.

El buscador PIL32 se comprobará manualmente introduciendo distintos criterios de búsqueda, con 20 repeticiones de cada tipo:

- La búsqueda por tag completo de señal debe dar como primer resultado esa señal.
- La búsqueda por tag parcial debe devolver todos los tag que contengan esa parte antes que el resto de resultados.
- La búsqueda por descripción debe devolver en la primera pantalla de resultados el elemento buscado, a no ser que todos los resultados sean más próximos a la descripción que el elemento buscado con lo que se invalidaría ese caso de prueba.

Se probarán manualmente los enlaces de las pantallas a la Ventana de Detalle PIL26, comprobando que se muestra la señal correcta, que la gráfica de señal cumple los requisitos solicitados, que se puede cambiar el escalado de tiempo y valor de acuerdo a lo solicitado, que la funcionalidad de cambio de límites, puesta a off del registro y gradientes está operativa, que se puede exportar a Excel los datos de la gráfica como se indica en PIL27 y que los tiempos de carga se ajustan a lo pedido en PIL31.

Se comprobarán los tiempos y las pruebas de carga del sistema, el software de análisis y rendimiento acordado entre el proveedor y Canal de Isabel II.

PIL28: Comprobación mediante el lanzamiento de 100 requests desde un único thread con un decalaje de un segundo.

PIL29: Comprobación mediante el lanzamiento de 100 requests desde un único thread con un decalaje de un segundo.

PIL30: Comprobación mediante el lanzamiento de 100 requests desde un único thread con un decalaje de un segundo.

PIL31: Comprobación mediante el lanzamiento de 100 requests desde un único thread con un decalaje de un segundo a ventanas de detalle de señales diferentes.

PIL32: Comprobación mediante el lanzamiento de 1 request cada 10 segundos desde 100 threads concurrentes durante 1 hora con llamadas alternas a esquemas y ventanas de detalle en los porcentajes especificados en el requisito.

PIL 33: Comprobación de la funcionalidad asignada a los distintos roles configurados en el producto, generando al menos un usuario por cada role o perfil.

6. PROYECTO DE DISEÑO E IMPLANTACIÓN

Una vez finalizada y validada la implementación básica, y con el Plan de Implantación completa aprobado, se procederá a la ejecución del plan que debe dar como entregable principal el sistema final construido y su pase a producción, incluyendo la migración de toda la información histórica y necesaria para el normal funcionamiento de los procesos, desde el sistema actual.

Deberá desarrollarse un Plan de Pruebas de la implantación completa. Recogerá para cada requisito, qué pruebas se van a realizar y los criterios de aceptación de dicha prueba. Este Plan deberá ser aprobado por Canal de Isabel II, así como cualquier cambio que se realice previo a su ejecución.

Las pruebas que se realicen durante la implantación deberán realizarse tanto con los datos migrados como con nuevos datos de alta en la solución que se está implantando.

6.1. Gestión del proyecto

Para el adecuado control del Proyecto, se realizará la gestión del mismo a través de la metodología de gestión de proyectos implantada en Canal de Isabel II.

Las áreas de gestión del proyecto necesarias para su adecuado seguimiento y control son las detalladas a continuación.

- Plan de Gestión del Alcance (Gestión de cambios)
- Plan de Recursos
- Plan de Tiempo/Cronograma
- Plan de Comunicación
- Plan de Calidad
- Plan de Riesgos/Contingencias
- Plan de Costes

Será necesaria la aportación, por parte del proveedor en la oferta, de los planes correspondientes a dichas áreas de gestión. El conjunto de todos estos planes conformará el Plan de Proyecto.

Es necesario establecer hitos de carácter funcional en el Plan de Proyecto, coincidentes con entregables.

Se proporciona la documentación necesaria de la metodología y las plantillas de los documentos necesarios en el Anexo 2 del presente pliego

La entrega de la documentación se realizará en formato Microsoft Word o Acrobat (pdf). Deben mantenerse todas las versiones de la documentación entregada, contemplando el control de los cambios. Todos los productos resultantes del trabajo quedarán en posesión de Canal.

El alcance comprende, dependiendo de las particularidades de la plataforma software, las siguientes tareas:

- 1 Modelo de Datos SCADA**
 - 1.1 Análisis modelo actual registros
 - 1.2 Definición nuevo modelo registros
 - 1.3 Definición de procesos de carga maestra
 - 1.4 Definición de procesos de migración información
 - 1.5 Definición de procesos de sincronización información
- 2 Procesamiento Datos SCADA**
 - 2.1 Análisis procesamiento actual información
 - 2.2 Definición nuevo procesamiento información
- 3 Interfaces SCADA otros Sistemas**
 - 3.1 Análisis interfaces actuales
 - 3.2 Definición nuevas interfaces
- 4 Modelo de Datos Oracle**
 - 4.1 Análisis modelo actual objetos
 - 4.2 Definición nuevo modelo
- 5 Interfaz Web de Supervisión**
 - 5.1 Análisis de Interfaz Web de Supervisión actual
 - 5.2 Definición de nueva Interfaz Web de Supervisión
- 6 Aplicaciones Auxiliares**
 - 6.1 Análisis de aplicaciones auxiliares actuales
 - 6.2 Definición/integración de aplicaciones/utilidades auxiliares
- 7 Instalación y configuración de servidores**
 - 7.1 Servidores SCADA
 - 7.2 Servidores OPC
 - 7.3 Servidores auxiliares
 - 7.4 Configurar conexiones entre servidores
 - 7.5 Probar comunicación entre servidores
- 8 Implementación modelo SCADA**
 - 8.1 Implementación procesos carga maestra Scada
 - 8.2 Carga maestra Scada Desarrollo
 - 8.3 Carga maestra Scada Integración
 - 8.4 Carga maestra Scada PRO
 - 8.5 Implementación procesos migración información a Scada nuevo
 - 8.6 Implementación procesos sincronización información migrada a nuevo Scada
 - 8.7 Migración información a Scada nuevo Desarrollo
 - 8.8 Activación procesos de sincronización
 - 8.9 Migración información a Scada nuevo PRO
- 9 Implementación modelo Oracle**
 - 9.1 Implementación procesos carga maestra Oracle
 - 9.2 Carga maestra Oracle Desarrollo
 - 9.3 Carga maestra Oracle Integración
 - 9.4 Carga maestra Oracle PRO
 - 9.5 Implementación procesos migración información a Oracle nuevo
 - 9.6 Implementación procesos sincronización información migrada a Oracle nuevo
 - 9.7 Migración información a Oracle nuevo Desarrollo
 - 9.8 Activación procesos de sincronización
 - 9.9 Copia de información a Oracle nuevo Integración
 - 9.10 Migración información a Oracle nuevo PRO
- 10 Seguridad BBDD's**
 - 10.1 Implementación seguridad BBDD Scada
 - 10.2 Implementación seguridad BBDD Oracle
- 11 Desarrollo tareas de procesamiento información SCADA y Oracle**
- 12 Desarrollo procesos interfaces SCADA**
- 13 Desarrollo interfaz Web de Supervisión**
 - 13.1 Desarrollo interfaz Web CDC Alarmas y Reglas
 - 13.2 Desarrollo interfaz Web Supervisión

- 13.3 Desarrollo cuadros de mando/informes
- 13.4 Securización
- 14 Desarrollo/Integración utilidades auxiliares**
- 15 Pruebas**
 - 15.1 Pruebas unitarias.
 - 15.2 Pruebas de integración entre los sistemas
 - 15.3 Pruebas de aceptación
 - 15.4 Pruebas de estrés y rendimiento
 - 15.5 Pruebas de seguridad de la plataforma
- 16 Formación**
- 17 Puesta en Producción y Estabilización**
 - 15.1 Plataforma disponible nuevas instalaciones incluyendo todo ABASTECIMIENTO y al menos un esquema de cada tipología de instalación (incluyendo SANEAMIENTO y DEPURACIÓN)
 - 15.2 Plataforma completa (mediante mantenimiento)

La facturación de la implantación se llevará a cabo del siguiente modo:

Bloques de actividades	Facturación	Método de facturación
1 a 16	80%	Incremento valor ganado
17 Puesta Producción y Estabilización	20%	Hito validación

El porcentaje anteriormente indicado es sobre el importe indicado en la oferta referente al concepto de “Fase 5 – Implantación completa” en el Anexo II del PCAP.

6.2. Plan de Pruebas

El adjudicatario definirá un plan de pruebas exhaustivo, considerando que se deben realizar:

- Pruebas unitarias.
- Pruebas de integración entre los sistemas
- Pruebas de aceptación
- Pruebas de estrés y rendimiento
- Pruebas de seguridad de la plataforma

Para la aceptación del proyecto por parte del CYII, la ejecución del plan de pruebas debe tener un resultado satisfactorio.

6.3. Formación

Antes de la puesta en producción del nuevo sistema, se realizará la formación para usuarios finales. El enfoque será principalmente de “formación para formadores”, de forma que el adjudicatario forme a personal de Canal de Isabel II para que sean éstos los que

impartan los cursos al resto de la empresa. No obstante, Canal de Isabel II se reserva el derecho de cambiar parte de las horas de la formación para formadores por formación directa a los usuarios finales, en caso de que la organización del trabajo así lo requiera.

A modo indicativo, el temario debe cubrir al menos los siguientes aspectos:

- Comunicación eficaz
- Organización del curso
- Preparación de ejercicios prácticos
- Vista general del interfaz de usuario
- Organización del menú
- Ventana de Detalle
- Gráficas de tendencias
- Personalización del menú. Favoritos y gráficas compartidas
- Exportación de datos
- Conexión desde Excel
- Informes y cuadros de mando

Dentro del plan de proyecto se deberá incluir un plan de formación para formadores y usuarios finales como mínimo de 200 horas, impartidas por formadores con experiencia.

Los entregables por parte del adjudicatario deben ser:

- Manuales de formación y ejercicios
- Formación presencial o telemática, a elección de Canal de Isabel II

6.4. Gestión del Cambio

La opción de transformación que conlleva el desarrollo e implantación del nuevo Sistema que es objeto de este contrato, hace necesario que a lo largo de la ejecución de todo el proyecto se gestione el cambio que esto supone en la organización.

En este sentido, las ofertas deberán incluir las propuestas que consideren convenientes, contemplando, al menos los siguientes aspectos:

- Se realizará la identificación de personal clave que por su implicación directa en el proyecto, o por sus conocimientos, deban participar de manera activa en el mismo. Dicho personal recibirá la formación necesaria en función de los roles que deban asumir. Estará contemplado en el Plan de Formación.
- Difusión del proyecto dentro de la organización en la forma que se estime más adecuada.
- Acciones que faciliten el arranque en productivo y el apoyo a los usuarios.

6.5. Puesta en Producción

Se desea una puesta en producción del nuevo sistema en dos fases, una con las características básicas que permita sustituir el sistema actual, y tras una fase de estabilización y corrección de errores, acometer el desarrollo de las características más avanzadas del sistema.

La entrega y puesta en producción del sistema incluirá:

- Su instalación y puesta a punto.
- Las cargas iniciales incluidas en los requisitos del sistema.
- Entrega de la documentación en los términos descritos en el apartado correspondiente.

Tras la puesta en producción el adjudicatario dedicará el equipo de trabajo necesario durante un periodo mínimo de dos meses a corregir los problemas que surjan tras la puesta en producción y ajustar el funcionamiento de los mismos.

6.6. Soporte post-implantación y Devolución del Servicio

Tanto el soporte y mantenimiento del sistema hasta la finalización del periodo contratado como el proyecto la devolución del servicio forman parte del contrato y deben completarse a todos los efectos en el plazo de ejecución del contrato.

La devolución del servicio consiste en un proyecto de traspaso del servicio de mantenimiento a personal de Canal de Isabel II y/o a otro proveedor seleccionado por Canal. En el apartado Fase de Devolución se describen los requisitos de esta fase.

7. EJECUCIÓN DE LOS TRABAJOS

7.1. Plazos de ejecución

El plazo de ejecución del contrato será de 4 años, teniendo como tiempo máximo para cada una de las fases definidas en el alcance, lo indicado a continuación:

1. Implantación básica (Proyecto Piloto): tendrá un plazo máximo de ejecución de 4 meses a partir de que Canal de Isabel II ponga a disposición del adjudicatario los servidores con los requerimientos del producto para el desarrollo del de implantación básica.
2. Suministro de licencias y software: Una vez que Canal de Isabel II haya validado y aprobado el proyecto piloto, solicitará los entregables de este apartado, que deberán entregarse en el plazo máximo de 2 meses. El software deberá incluir todas las características ofertadas por el licitante en la plantilla de cumplimiento de requisitos, lo que implica que todas las ampliaciones necesarias para cubrir la funcionalidad deben entregarse en dicho plazo. La fase de mantenimiento y soporte del producto software tendrá la misma duración de los 4 años de contrato.
3. Diseño e implantación de la arquitectura: Tras la aprobación del proyecto piloto, el adjudicatario deberá indicar en un plazo de 15 días las necesidades de servidores y equipamiento. Tras la entrega del equipamiento por parte del Área de Infraestructura Informática, el adjudicatario dispondrá de 2 meses para entregar toda la documentación e instalar los tres entornos de (desarrollo, integración y producción) con las conexiones a los Front-End de Automatización securizadas.
4. Programa de Formación: Tras la puesta en marcha del entorno de integración para pruebas y formación, se impartirá la formación ofertada al equipo de proyecto en un plazo máximo de 2 meses. Canal de Isabel II y el adjudicatario podrán de mutuo acuerdo adelantar parte de la formación utilizando para ello el entorno del proyecto piloto.
5. Diseño e implantación del nuevo SCADA: Tras la puesta en marcha del entorno de desarrollo, se comenzará la fase de diseño e implantación del nuevo sistema con una duración entre 36 y 40 meses, dependiendo del tiempo consumido en las fases anteriores. El adjudicatario dispondrá de 1 mes para realizar la planificación detallada del proyecto y la elaboración definitiva de la documentación de gestión de proyecto. Se desea una puesta en producción del nuevo sistema en dos fases, una con las características básicas que permita sustituir el sistema actual, y tras una fase de estabilización y corrección de errores, acometer el desarrollo de las características más avanzadas del sistema. La formación a formadores para el curso a usuarios se realizará 1 mes antes de la puesta en producción del sistema.

En caso de incumplimiento de estos plazos, el adjudicatario incurrirá en la penalización correspondiente prevista en el Anexo I del PCAP.

7.2. Equipos de trabajo

El licitador habrá de identificar de forma expresa los equipos de trabajo ofertados para el piloto, el diseño e implantación de la arquitectura, la formación y el soporte.

El licitador deberá proporcionar las características del equipo de trabajo debidamente detallado incluyendo:

- Descripción de las categorías profesionales necesarias, incluyendo las tareas y actividades a realizar por cada una, así como las responsabilidades a asumir.
- Número de personas dedicadas al proyecto por cada categoría profesional.
- Perfil profesional asociado a cada puesto de trabajo.
- Dedicación, en jornadas, de cada uno de los perfiles.

El equipo de proyecto debe constar al menos del siguiente personal, si bien dependiendo de la fase del mismo no todo el personal debe estar dedicado a él a tiempo completo. No obstante, todo el equipo ofertado debe estar disponible para corregir las desviaciones que puedan surgir en la ejecución del proyecto.

Perfil	Director de Proyecto
Formación de base	Titulado Superior
Cualificación	Responsable de la gestión y la coordinación del área de desarrollos de la empresa con capacidades de asignación/desasignación de recursos dentro de su propia empresa, así como de la resolución de problemas graves que afecten al desarrollo del proyecto.
Experiencia	Requeridos al menos 5 años de experiencia como Director de Proyecto o Jefe de Proyectos de servicios de AM.
Cantidad	1

Perfil	Jefe de Proyecto
Formación de base	Titulado Superior en ingeniería o ciencias
Formación específica	80 horas en gestión de proyectos de desarrollo de software o certificación PMP de PMI
Cualificación	Capacidad demostrable para la planificación y gestión de proyectos de desarrollo de software.
Experiencia	Requeridos al menos 4 años de experiencia como Jefe de Proyecto en proyectos de implantación del producto seleccionado.
Cantidad	1

Perfil	Arquitecto de sistemas
Formación de base	Titulado Superior o medio en Informática
Formación específica	<p>200 horas de formación en:</p> <ul style="list-style-type: none"> ▪ Bases de datos relacionales ▪ Web Services ▪ Redes TCP/IP ▪ Ciberseguridad ▪ Sistemas SCADA ▪ Arquitectura de la solución propuesta <p>Certificación emitida por el fabricante del producto en relación a arquitectura de la solución</p>
Experiencia	Al menos 3 años de experiencia en proyectos o servicios de este tipo y con el producto seleccionado, como arquitecto de sistemas.
Cantidad	1

Perfil	Consultor SCADA
Formación de base	Titulado Superior en ingeniería o ciencias
Formación específica	<p>100 horas en sistemas de control y adquisición de datos, OPC y automatización.</p> <p>Certificación en la plataforma SCADA propuesta por el adjudicatario, relacionada con el desarrollo y configuración sobre dicha plataforma.</p>
Cualificación	Capacidad demostrable para el diseño de bases de datos en tiempo real, configuración de la plataforma SCADA propuesta por el adjudicatario, programación de alarmas y reglas, configuración del HMI.
Experiencia	Al menos 3 años de experiencia en la plataforma SCADA propuesta por el adjudicatario.
Cantidad	4

Perfil	Analista programador SCADA
Formación de base	Titulado Superior o medio en Informática
Formación específica	<p>Formación en:</p> <ul style="list-style-type: none"> ▪ Plataforma SCADA propuesta por el adjudicatario (mínimo 50 horas).

	<ul style="list-style-type: none"> .Net, Java, lenguajes de scripting habilitados para desarrollos dentro de la plataforma seleccionada. (mínimo 50 horas) Base de datos Oracle y la que use la plataforma en alguno de sus módulos.(mínimo 50 horas)
Cualificación	Capacidad demostrable para diseñar aplicaciones, componentes y bases de datos a partir de los requisitos de usuario y para la generación de código en la plataforma SCADA.
Experiencia	Al menos 3 años de experiencia en la plataforma SCADA propuesta por el adjudicatario.
Cantidad	3

Perfil	Analista programador SCADA
Formación de base	Titulado Superior o medio en Informática
Formación específica	Formación en: <ul style="list-style-type: none"> Plataforma SCADA propuesta por el adjudicatario (mínimo 50 horas). .Net, Java, lenguajes de scripting habilitados para desarrollos dentro de la plataforma seleccionada. (mínimo 50 horas) Base de datos Oracle y la que use la plataforma en alguno de sus módulos. (mínimo 50 horas) UX Designer (20 horas)
Cualificación	Capacidad demostrable para diseñar aplicaciones, siguiendo guías de estilo , componentes y bases de datos a partir de los requisitos de usuario y para la generación de código en la plataforma SCADA.
Experiencia	Al menos 3 años de experiencia en la plataforma SCADA propuesta por el adjudicatario.
Cantidad	1

Perfil	Analista de datos
Formación de base	Titulado Superior en ingeniería o ciencias
Formación específica	Horas de formación : <ul style="list-style-type: none"> Herramientas Business Intelligence (mínimo 50 horas) Herramientas ETL (mínimo 50 horas) Bases de datos usadas en la arquitectura de la plataforma propuesta.(mínimo 50 horas) Machine Learning (deseable)

Cualificación	Capacidad demostrable para el análisis de grandes volúmenes de información, Data Mining, herramientas ETL y cuadros de mando.
Experiencia	Requeridos al menos 3 años de experiencia en proyectos o servicios de este tipo y en la plataforma propuesta como analista de datos
Cantidad	1 (segunda parte del proyecto)

Los datos se detallarán en el formulario adjunto como ANEXO 1 – CUESTIONARIO PERSONAL.

Canal de Isabel II se reserva el derecho de solicitar la sustitución de algún miembro del equipo de trabajo del adjudicatario, informando justificadamente de la necesidad del cambio.

7.3. Organización, Seguimiento y Control de los trabajos

La organización, seguimiento y control de los trabajos se llevarán a cabo de acuerdo al apartado modelo de gobierno.

Las fases técnicas del Proyecto Piloto y de Implantación de la Arquitectura tendrán una reunión de seguimiento cada 15 días, con objeto de detectar cualquier desviación sobre la planificación y poder decidir y ejecutar medidas correctoras en el menor plazo posible.

La fase de implantación del sistema SCADA será objeto de reuniones de seguimiento mensuales, en las que se revisará la marcha del proyecto respecto a la planificación y decidir en caso necesario las medidas correctoras para corregir las desviaciones. Este seguimiento se realizará mediante la técnica de “Valor Ganado” en la que se compara el valor del trabajo planificado del proyecto (PV) con el valor real ejecutado (EV).

Por tanto, en el Plan de Proyecto se establecerán los paquetes de trabajo y sus diferentes tareas con su peso en el proyecto total estableciendo hitos de carácter funcional coincidentes con entregables. El peso de los hitos en el Valor Ganado del paquete de trabajo será del 20% del total. Es decir, las tareas que conforman cada paquete de trabajo tendrán una valoración del 80% del Valor Ganado, y la aceptación del hito entregable por parte de Canal Gestión del 20% restante. Además, existirá un hito específico de Puesta en Producción del proyecto con una valoración del 20% del valor total del proyecto.

Si en los seguimientos periódicos del proyecto acordados se obtiene un índice de eficiencia de tiempo (SPI) inferior al 80% se incurrirá en una penalización, según se describe en el apartado 9.1 del Anexo I del PCAP. El cálculo del SPI se realizará dividiendo el valor ganado (EV) entre el valor planificado (EP) y multiplicándolo por 100.

7.4. Lugar de realización de los trabajos

Las fases técnicas del Proyecto Piloto y de Implantación de la Arquitectura se realizarán del modo en que Canal de Isabel II considere más idóneo en cada momento.

El Programa de Formación podrá impartirse tanto en modalidad on-line como presencial, ya sea en las aulas de formación de Canal de Isabel II sobre el entorno de integración, o en las instalaciones del adjudicatario si ambas partes lo estiman conveniente.

El Adjudicatario realizará el resto de trabajos en sus propias instalaciones, excepto los que por su naturaleza requieran presencia en las instalaciones de Canal de Isabel II.

7.5. Conectividad con Canal de Isabel II

El Adjudicatario deberá establecer una línea de comunicaciones y otra de backup con Canal de Isabel II a lo largo de la duración del contrato y sin coste adicional para Canal de Isabel II, que deberán cumplir las consideraciones de conectividad y seguridad incluidas dentro del Anexo 5 del presente documento.

8. MODELO DE GOBIERNO

Canal de Isabel II considera que, para el éxito de este proyecto, es imprescindible un Modelo de Gestión y de Relación con los Adjudicatarios sólido y consistente, capaz de evolucionar los servicios externalizados de acuerdo a la evolución del negocio y de la tecnología.

En este apartado describiremos el Modelo de Gestión requerido por Canal de Isabel II. La oferta del Adjudicatario deberá describir con detalle suficiente la organización de su equipo de trabajo, tanto para los servicios centralizados en sus instalaciones, como para aquellos técnicos que deban estar en ubicaciones de Canal de Isabel II. Esta descripción debe incluir el detalle de los procedimientos, políticas, guías y herramientas que utilizará durante la vigencia del contrato para la gestión y supervisión de los servicios, de los equipos de trabajo propios y de los de terceros o subcontratados implicados en la prestación de los servicios.

En su diseño, el Adjudicatario debe adaptarse al Modelo de Gestión que se describe a continuación. El Adjudicatario debe establecer y detallar en su propuesta, los requerimientos de su modelo organizativo respecto a la participación de personal de Canal de Isabel II.

8.1. Gestión de Servicios

El Adjudicatario es responsable de la gestión, ejecución, supervisión técnica y control diario de los servicios prestados y de que estos se presten de acuerdo a los niveles de calidad acordados con Canal de Isabel II.

Para completar estas actividades, el Adjudicatario deberá utilizar el modelo **ITIL-ITSM**. El objetivo que persigue Canal de Isabel II es disponer de un entorno de gestión estándar que permita realizar cambios o incorporaciones durante el Contrato o tomar decisiones a su finalización, sin impacto significativo en el usuario de los mismos.

8.2. Gestión de la Relación

Para la gestión de la relación se considera clave para el éxito de este proyecto asegurar que se dispone de la necesaria flexibilidad para responder a los cada vez más rápidos cambios en el entorno de negocio de Canal de Isabel II

Dicho modelo está basado en el Modelo de referencia que se expone a continuación.

8.2.1. Modelo de Referencia

El Modelo requerido se estructura en tres niveles.

- El **nivel estratégico** es el encargado de velar por que la estrategia y objetivos del proyecto estén alineados con los corporativos, y de controlar y garantizar que todas las decisiones y operaciones se ajustan a dicha estrategia.
- El **nivel táctico** se encarga de transformar las decisiones estratégicas en planes de operación y acción y de coordinar, dirigir y controlar los esfuerzos necesarios para su ejecución.
- El **nivel operacional** se responsabiliza de la gestión, ejecución, supervisión técnica y control diario de los servicios.

8.2.2. Comité de Dirección

Frecuencia	Comité	Responsabilidades	Asistentes	
			Canal de Isabel II	Adjudicatario
Semestral (o tras 10 días de la petición de cualquiera de las partes)	Dirección	<ul style="list-style-type: none"> ▪ Aprobar los cambios en ANS propuestos por el comité de Seguimiento y control ▪ Aprobar los cambios en el ámbito del servicio propuestos por el Comité de Seguimiento y Control ▪ Aprobar los cambios al contrato propuestos por el Comité de Seguimiento y Control ▪ Discutir cualquier incidencia o problema surgido durante la ejecución del servicio ▪ Ejecutar cualquier otra actividad relacionada con la dirección estratégica que pueda surgir a lo largo del Servicio ▪ Resolver cualquier conflicto continuado entre los participantes en el proyecto, que no haya sido posible resolver tras un periodo de tiempo razonable por otros niveles de gestión subordinados dentro del presente Modelo de Relación. 	<ul style="list-style-type: none"> ▪ Director ejecutivo (capacitado para asegurar el nivel de decisión y compromiso que requieren las decisiones estratégicas) (*) 	<ul style="list-style-type: none"> ▪ Gestor Estratégico (capacitado para asegurar el nivel de decisión y compromiso que requieren las decisiones estratégicas)

(*) Rol que preside el Comité

8.2.3. Comité de Seguimiento y control

Frecuencia	Comité	Responsabilidades	Asistentes	
			Canal de Isabel II	Adjudicatario
Mensual (o a petición de cualquiera de las partes)	Seguimiento y control	<ul style="list-style-type: none"> ▪ Asegurar que se consiguen los niveles de calidad acordados y, que en el caso de deficiencias no resueltas a nivel operativo, se desarrollen e implementen planes de resolución de problemas ▪ Monitorizar el estado de los servicios ▪ Revisar, actualizar y controlar el cumplimiento de la planificación ▪ Coordinar los grupos y personas asignados a la entrega del Servicio ▪ Discutir nuevos requerimientos o cambios. Revisar y aprobar las Peticiones de Cambio. ▪ En el caso de que el cambio requiera de cambios en el Contrato, revisar el informe de impacto correspondiente. Estos informes son los que deben ser enviados al Comité de Dirección de acuerdo a un Proceso de Gestión de Cambios en el Contrato ▪ Asegurar que el personal asignado para la ejecución de los servicios por el Adjudicatario está disponible y disponen de los recursos, formación y soporte necesarios para la correcta ejecución de sus tareas ▪ Revisar los niveles de servicio medidos en cada periodo, discutir las desviaciones sobre los valores objetivos acordados y calcular, en su caso, las penalizaciones aplicables ▪ Servir como punto único de contacto entre las organizaciones de Canal de Isabel II y del 	<ul style="list-style-type: none"> ▪ Director / Jefe de Proyecto (*) 	<ul style="list-style-type: none"> ▪ Responsable del Servicio/ Proyecto

Frecuencia	Comité	Responsabilidades	Asistentes	
			Canal de Isabel II	Adjudicatario
		<p>Adjudicatario para todos los asuntos relacionados nivel de gestión táctico del Servicio</p> <ul style="list-style-type: none"> ▪ Controlar que la facturación se está realizando conforme a los acuerdos y resolver cualquier problema relacionado con el precio o los pagos ▪ Revisar y facilitar al Comité de Dirección cualquier información que le sea solicitada 		

(*) Rol que preside el Comité

8.2.4. Comité Operacional

Frecuencia	Comité	Responsabilidades	Asistentes	
			Canal de Isabel II	Adjudicatario
Semanal/ A petición de cualquiera de las partes	Operativo	<ul style="list-style-type: none"> Elaborar planes de detalle semanales de actuación para las planificaciones mensuales acordadas y realizar su seguimiento Revisar la lista de incidencias y tareas pendientes y asignar prioridades Revisar y priorizar las peticiones recibidas Coordinar los grupos y personas asignados a la entrega del Servicio Discutir nuevos requerimientos o cambios. Revisar y aprobar las Peticiones de Cambio menores. En el caso de que el cambio sea significativo elaborar informe propuesta para el Comité de Seguimiento y Control. Verificar que el personal asignado para la ejecución de los servicios por el Adjudicatario está disponible y disponen de los recursos, formación y soporte necesarios para la correcta ejecución de sus tareas Revisar la tendencia de los niveles de servicio y establecer acciones correctoras 	<ul style="list-style-type: none"> Jefe de Proyecto / Responsable Operativo (*) 	<ul style="list-style-type: none"> Jefe de Proyecto / Responsable Operativo
		<ul style="list-style-type: none"> Servir como interlocutor entre las organizaciones de Canal de Isabel II y del Adjudicatario para todos los asuntos del día a día relacionados con el Servicio Revisar y facilitar al Comité de Seguimiento y Control cualquier información que le sea solicitada. 		

(*) Rol que preside el Comité

8.3. Gestión del Contrato

Canal de Isabel II considera como un requerimiento imprescindible contar con estructuras de contrato flexibles, que permitan los cambios en cualquier aspecto del servicio que sea preciso como consecuencia de cambios en la demanda de servicios a los usuarios o áreas de negocio de Canal de Isabel II, o cambios en el entorno de negocio de Canal de Isabel II. Además debe garantizar que el proyecto se beneficia del avance de la tecnología, tanto en mejoras de calidad de servicio o productividad como en su coste.

Un aspecto crítico para el éxito del proyecto y que, por lo tanto, será valorado especialmente, son los mecanismos para gestionar la variabilidad del ámbito de los Servicios a lo largo de la vida del contrato.

El adjudicatario debe describir los procedimientos, métodos y herramientas que propone implantar para la gestión de cambios en el contrato. El adjudicatario deberá proponer concretamente un Procedimiento de Gestión de Cambios al Contrato capaz de gestionar:

- Cambios mayores y menores al contrato
- Cambios en los documentos de Contrato y en los Apéndices
- Cambios en el Ámbito de los servicios contenido en el Contrato
- Cambios en los ANS
- Cambios como consecuencia de la implantación o ejecución de iniciativas de mejora o de los Planes de Transformación
- Cambios en las actividades de negocio (nuevos servicios, abandono de actividades) o en la organización de Canal de Isabel II que impactan en el ámbito, volúmenes o la forma de entrega de los servicios
- Cualquier otro cambio que pueda afectar a la estructura o contenido de los contratos que regulan la prestación de los servicios

8.4. Sistema de Gestión Integrado

Canal de Isabel II tiene como objetivo llevar a cabo una gestión activa e integrada de la entrega de los servicios, en dos niveles: estratégico y táctico-operativo. Para ello espera que el Adjudicatario implemente un Sistema de Gestión Integrado que permita a Canal de Isabel II realizar la gestión continua y en todos los niveles:

- **Nivel Estratégico.** Tener una visión global que permita:
 - Controlar el cumplimiento del contrato
 - Controlar que los niveles de servicio responden a las necesidades de negocio para mantener la alineación con los objetivos corporativos
 - Controlar el cumplimiento global de los niveles de servicio y que se produce una mejora continua de su calidad

- Controlar la evolución del consumo de servicio y su coste asociado (ratios de coste)
- Controlar y ajustar los precios
- **Niveles Táctico y Operativo.** Tener una visión detallada que permita:
 - Controlar el cumplimiento de los niveles de servicio
 - Monitorizar y ajustar los niveles de servicio
 - Seguimiento y control de fallos, incidencias y problemas
 - Control de las configuraciones y topologías de sistemas y redes
 - Control y seguimiento de la capacidad y de los planes e iniciativas relacionadas con la capacidad
 - Seguimiento, control y ajuste de la asignación de tareas y de recursos
 - Seguimiento y control de la ejecución de tareas y trabajos
 - Maximizar el uso de los servicios del Adjudicatario
 - Conocer el detalle de los consumos y precios de los servicios

El Adjudicatario debe detallar en el Plan de Gestión de la Comunicación dentro del Plan de Gestión del Proyecto las herramientas y procesos que componen el Sistema de Gestión Integrado que propone utilizar. El Adjudicatario incluirá en su descripción ejemplos de interfaces, informes, etc.

8.5. Seguimiento e informes

Se establecen como estándar los informes siguientes:

Informe mensual

Informe dirigido a los miembros del Comité de Seguimiento y Control para analizar la información requerida en dicho comité, en especial la actividad del periodo correspondiente, el cumplimiento de los indicadores de nivel de servicio y la identificación proactiva de problemas en el cumplimiento del ANS.

Informe anual

Informe dirigido a los miembros del Comité de Dirección para analizar la información requerida en dicho comité, en especial recogiendo la evolución de los indicadores de calidad y la información de los elementos que se consideren más críticos.

Adicionalmente a estos informes, y ante situaciones específicas, el Adjudicatario deberá presentar información requerida bajo demanda y en particular para cubrir los puntos descritos en el Comité Operacional.

9. Fase de Devolución

A continuación, se describen los requisitos para los servicios de finalización, incluido un Plan de Devolución que el Adjudicatario deberá redactar, mantener y actualizar anualmente de acuerdo con el contrato.

9.1. Principios clave

El objetivo del Plan de Devolución es permitir la finalización del contrato y el traspaso del conocimiento de los servicios que se estén prestando a Canal de Isabel II o al nuevo adjudicatario que pudiera ser adjudicatario del nuevo contrato para la prestación de estos servicios.

El Plan de Devolución detallará los tipos de procesos y actividades que el Adjudicatario prestará para la finalización ordenada y transferencia al nuevo adjudicatario que pasase a realizar los servicios que se estén prestando.

El Adjudicatario actualizará el Plan de Devolución de acuerdo a los análisis y resultados que se vayan produciendo a lo largo del contrato.

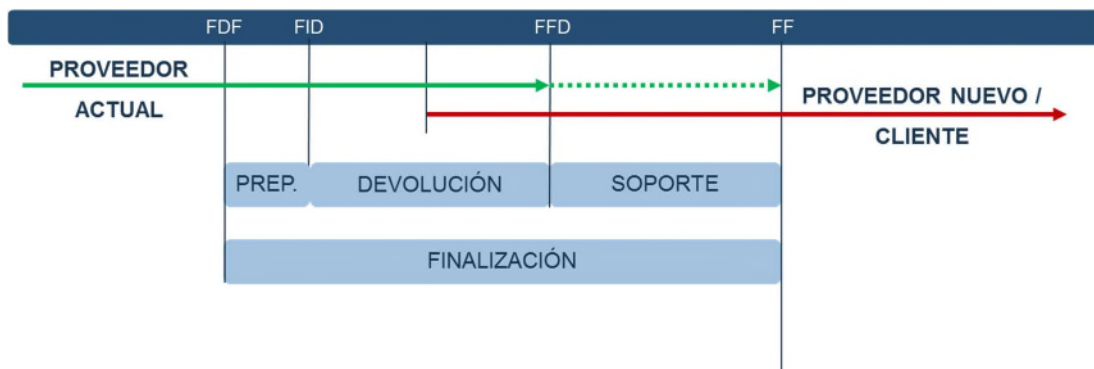
El Plan de Devolución deberá cubrir las siguientes cuestiones con detalle:

1. Principios generales.
2. Elementos que se transferirán.
3. Planificación y plan de proyecto.
4. Gobierno de la finalización.
5. Actividades durante el periodo de seguimiento
6. Gestión de la seguridad.
7. Facturación y obligaciones durante la finalización.
8. Garantías durante la transferencia sobre los servicios a transferir.

En el siguiente capítulo se explicarán con más detalle los requisitos para cada cuestión.

9.2. Principios generales

Se establecen los siguientes periodos de tiempo para la finalización de los servicios:



Nota: la relación de longitud entre las franjas no significa un espacio de tiempo determinado

Donde:

- Fecha de Decisión de la Finalización: fecha en la que el Adjudicatario y Canal de Isabel II deciden finalizar los servicios. A partir de esta fecha comienza el periodo de preparación, donde se comienza a elaborar el plan de proyecto de ejecución de la finalización en base al Plan de Devolución
- Fecha de Inicio de la Devolución: fecha en la que comienza el periodo de devolución donde se realiza el proyecto de ejecución de la finalización.
- Fecha de Fin de la Devolución: fecha a partir de la cual la responsabilidad, el conocimiento y los activos se han transferido y finaliza el contrato. A partir de esta fecha empieza un periodo de soporte por parte del Adjudicatario.
- Fecha de Finalización: que define el final del proyecto de ejecución de la finalización.

Durante el proyecto de finalización, el Adjudicatario asumirá la responsabilidad de ayudar a Canal de Isabel II y/o los posibles nuevos adjudicatarios comunicados por Canal de Isabel II, con la finalización de los servicios que se mencionan en el presente pliego y todos los puntos relacionados que se describen a continuación, sin interrupción alguna de los servicios ni de los niveles de calidad.

Durante el proyecto de finalización el Adjudicatario facilitará a Canal de Isabel II y a los posibles proveedores sustitutos acceso a:

- Los registros y la documentación que puedan ser necesarios.

Durante el proyecto de finalización el Adjudicatario garantizará que sus empleados relacionados con la entrega del servicio dedicarán tiempo suficiente a transferir su conocimiento a Canal de Isabel II o a los proveedores sustitutos.

Toda documentación necesaria para la prestación del servicio se mantendrá actualizada, lo que se auditará antes de la Fecha de Inicio de la Devolución. Si no están al día, será necesario actualizarlas. No se cobrará ninguna tarifa adicional a Canal de Isabel II por actualizar esta documentación.

9.3. Elementos que se transferirán

El Plan de Devolución deberá contener listas exhaustivas, correctas, actuales y ordenadas (tanto impresas como en electrónico) que incluyan toda la información disponible para el Adjudicatario, de todo el hardware, servicios, software y licencias, bases de datos y datos, documentación, ajustes de instalaciones, configuraciones y parametrizaciones y desarrollos realizados. El Adjudicatario será responsable de la recopilación y actualización de estas listas, así como de la precisión de estas listas. El Adjudicatario deberá cumplir los principios siguientes que apliquen en relación a los servicios demandados:

- Hardware. El Plan de Devolución contendrá una descripción de la arquitectura de la solución que está en producción.
- Software y aplicaciones. El Plan de Devolución contendrá una lista de todo el software, materiales y licencias en uso para la prestación de los servicios. Especificará la propiedad del software y las licencias, los licenciarios y los permisos para transferir las licencias. Toda la personalización del software para Canal de Isabel II debe ponerse a disposición de Canal de Isabel II sin coste adicional.
- Herramientas. El Plan de Devolución contiene una lista específica de todas las herramientas (herramientas de gestión del servicio y plantillas de cambios) usadas para la prestación de los servicios. También especificará la propiedad de las herramientas, las licencias, los licenciarios y los permisos para transferir las licencias. En caso de herramientas propietarias, el Plan de Devolución propone herramientas alternativas y describe, en general, la transición para la implementación de herramientas alternativas.
- Datos y bases de datos. El Plan de Devolución especifica todos los datos electrónicos e impresos, su propiedad y la ubicación de almacenamiento, y la propiedad del sistema de almacenamiento. El Adjudicatario también suministrará un registro de todos los cambios realizados y planificados como parte del procedimiento integral de gestión del cambio. Canal de Isabel II determina y debe aprobar el formato en que el Adjudicatario deberá transferir los datos.
- Documentación. El Plan de Devolución incluye una lista de toda la documentación, descripciones de procesos e instrucciones de trabajo utilizados por el Adjudicatario para la prestación de los servicios. El Adjudicatario garantiza que toda la documentación relevante sea exacta y esté actualizada en el momento de su transferencia a Canal de Isabel II o al Adjudicatario sustituto. La documentación se pondrá a disposición de Canal de Isabel II en formato electrónico e impreso.
- Transferencia de instalaciones. El Plan de Devolución incluye una lista con todas las ubicaciones de instalaciones, especificaciones ambientales y su inventario. También incluye una lista de todos los ajustes de instalaciones o cambios que deben realizarse en caso de finalización (como movimiento de hardware, personal o equipo de oficina).
- Transferencia de contratos de terceros. El Plan de Devolución incluye una lista de todos los contratos utilizados por el Adjudicatario y los subcontratistas para la

provisión de servicios a Canal de Isabel II. La lista deberá especificar qué contratos pueden transferirse a Canal de Isabel II. El Adjudicatario asegura que cualquier contrato transferible utilizado por el Adjudicatario y los subcontratistas en la provisión de los servicios se pueda asignar a Canal de Isabel II o al Adjudicatario sustituto, en la Fecha de Inicio de la Devolución o antes de ella sin cargos adicionales. Sin embargo, Canal de Isabel II también puede decidir que terminará los contratos de terceros sin cargo alguno.

- Transferencia de conocimiento. El Adjudicatario dedicará tiempo y recursos razonables durante la transición de finalización para garantizar la adecuada transferencia de conocimiento.

9.4. Planificación y plan de proyecto

El Plan de Devolución incluirá un plan de proyecto de finalización con la planificación de las actividades necesarias para realizar la finalización a partir de la Fecha de Inicio de la Devolución. Deberán especificarse para cada actividad las responsabilidades del Adjudicatario, de Canal de Isabel II y del Adjudicatario sustituto.

A partir de la Fecha de Decisión de la Finalización y durante el periodo de preparación se realizará una verificación del Plan de Devolución entre Canal de Isabel II y el Adjudicatario, se verificarán las hipótesis y los requisitos previos, y se actualizarán si se acuerda y es necesario. En virtud de tal revisión el Adjudicatario generará el plan de proyecto de ejecución de la finalización.

Durante el periodo de preparación, el Adjudicatario y Canal de Isabel II recopilarán y facilitarán toda la información necesaria para una devolución fluida de los servicios a partir de la Fecha de Inicio de la Devolución.

El periodo de preparación no podrá ser superior a 1 mes.

El plan de ejecución de la finalización se desglosará en procesos de trabajo manejables, que se detallarán cada semana y describirán en detalle las actividades y entregables necesarios del Adjudicatario, Canal de Isabel II, y (si corresponde) del Adjudicatario sustituto. Por cada proceso de trabajo se acordará una lista clara de hitos para cada etapa. En caso de que se aplique la transferencia de hardware, software y licencias, bases de datos y datos, documentación, contratos de terceros, ajustes de instalaciones y personal, cada grupo deberá tratarse como procesos de trabajo separados. Además, deberá especificarse la cantidad de recursos necesarios de Canal de Isabel II y, si corresponde, del Adjudicatario sustituto. Para cada proceso de trabajo, el plan de ejecución de la finalización incluirá los criterios de aceptación que deberán cumplirse.

Después de la Fecha de Fin de la Devolución, el Adjudicatario facilitará soporte y transferencia de conocimiento a Canal de Isabel II o a su Adjudicatario durante un periodo de tiempo acordado (periodo de soporte). El periodo de soporte no podrá ser inferior a 3 meses.

Al finalizar el periodo de soporte se realizará el cierre del proyecto de ejecución de la

finalización, dando por terminada la finalización de los servicios.

9.5. Gobierno de la finalización

El Plan de Devolución deberá contener una descripción detallada de la configuración organizativa, las personas implicadas, y las líneas de comunicación. Como referencia para el modelo de gobierno se considera lo especificado en el Modelo de Gobierno, en particular en lo que se refiere a los niveles estratégico, táctico y operativo y sus respectivos gestores.

Durante el periodo de preparación cada parte nombrará un Responsable de la Finalización, que será responsable de la coordinación y gestión de la finalización de los servicios y de la aplicación del Plan de Devolución.

Durante la fase de devolución seguirá vigente el modelo de gobierno indicado en el presente pliego. Los comités establecidos en dicho modelo podrán ir desapareciendo progresivamente, según el proyecto de ejecución de la finalización. Además, se establece el siguiente comité de nivel estratégico:

Frecuencia	Comité	Objetivos	Asistentes	
			Canal de Isabel II	Adjudicatario
Quincenal	Comité Estratégico de la Finalización	<ul style="list-style-type: none"> Revisar la calidad de la devolución y sus resultados clave Supervisar los criterios de aceptación de finalización acordados Ofrecer compromiso, apoyo y recursos para la finalización de las respectivas áreas de responsabilidad de cada parte para facilitar el éxito de la finalización Revisar y monitorizar el progreso según los hitos del proyecto de ejecución de la finalización Resolver problemas y riesgos clave escalados de las reuniones de Progreso de la Devolución Actuar como canal de relación con el negocio de Canal de Isabel II para cuestiones que le afecten. Revisar incidencias y registros de riesgos Revisar y aprobar cambios en el Plan de Devolución 	<ul style="list-style-type: none"> Gestor Estratégico (*) Responsable de la Finalización 	<ul style="list-style-type: none"> Gestor Estratégico Responsable de la Finalización

(*) Rol que preside el Comité

Durante la fase de devolución se establece además el siguiente comité de nivel táctico:

Frecuencia	Comité	Objetivos	Asistentes	
			Canal de Isabel II	Adjudicatario
Semanal	Progreso de la Devolución	<ul style="list-style-type: none"> Revisión del progreso de todas las actividades incluidas en el ámbito de la finalización Examinar las incidencias y los riesgos Revisar los cambios en el Plan de Devolución. Revisar las actividades y carga de trabajo para la siguiente semana. 	<ul style="list-style-type: none"> Responsable de la Finalización (*) Gestor Operativo 	<ul style="list-style-type: none"> Responsable de la Finalización Gestor Operativo

(*) Rol que preside el Comité

El Adjudicatario proporcionará a Canal de Isabel II los informes semanales de progreso de la devolución que describen:

1. El estado actual de la devolución.
2. El progreso del trabajo que se realiza.
3. Los problemas o retrasos reales o previstos de los cuales el Adjudicatario tenga conocimiento.
4. El impacto de este tipo de problemas o retrasos en el Plan de Devolución.
5. Todas las acciones que se están adoptando o que deban adoptarse para remediar ese tipo de problemas o retrasos.

9.6. Actividades durante el periodo de Soporte

Durante el periodo de soporte los Responsables de la Finalización de Canal de Isabel II y del Adjudicatario mantendrán la comunicación necesaria para la ejecución de las actividades de soporte definidas.

9.7. Gestión de la seguridad y la conformidad

En el Plan de Devolución, el Adjudicatario especificará cómo se garantiza la seguridad de los datos, sistemas e información durante la finalización. En un plazo de cuatro semanas después de la Fecha de Fin de la Devolución el Adjudicatario borrará cualquier copia (on line) restante de software de aplicación y juegos de datos, sin conservar ninguna copia de seguridad, a menos que Canal de Isabel II indique lo contrario.

9.8. Facturación y obligaciones durante la finalización

Aparte de los cargos que se indican en presente pliego, Canal de Isabel II no tendrá ninguna otra obligación hacia el Adjudicatario durante la finalización de los servicios, estando todos los trabajos de devolución incluidos en los servicios contratados.

Las partes reconocen que la finalización de los servicios del Adjudicatario al nuevo Adjudicatario o a Canal de Isabel II (según corresponda) puede producirse en fases, lo que puede provocar el cese gradual por parte del Adjudicatario de la provisión de partes de los servicios y su provisión por el nuevo Adjudicatario o el cliente. En este sentido, las partes acuerdan que los cargos variarán durante la migración de los servicios retirados. En el proyecto de ejecución de la finalización se detallará el plan de facturación de finalización, según se vaya produciendo la devolución de los servicios.

A partir de Fecha de Fin de la Finalización las responsabilidades para la prestación del servicio recaen en Canal de Isabel II o en el Adjudicatario sustituto. No se aceptarán facturas en relación con la prestación del servicio después de la Fecha de Fin de la Finalización.

Durante el periodo de soporte el Adjudicatario podrá facturar dicho servicio de soporte en base a las tarifas acordadas por perfiles según los precios propuestos en la oferta.

9.8.1. Garantías durante la transferencia sobre los servicios a transferir.

Durante los periodos de preparación y devolución el Adjudicatario deberá cumplir los niveles de servicio descritos en el presente pliego, estando vigente la aplicación de posibles penalizaciones.

10. AUDITORIA

Se definen los principios y procedimientos aplicables a las actividades de auditoría de Canal de Isabel II y terceros (auditores externos, reguladores, etc.) en los servicios proporcionados por el Adjudicatario.

10.1. Principios

Canal de Isabel II tendrá derecho a auditar los servicios prestados por el Adjudicatario durante la vigencia del presente contrato con el fin de determinar:

- El cumplimiento de los servicios según lo especificado en este pliego.
- El cumplimiento de los Acuerdos de Nivel de Servicio
- La integridad y exactitud de los informes.
- La exactitud de los costes facturados.
- La integridad, seguridad y tratamiento de los datos.
- Seguridad de los trabajos realizados

Canal de Isabel II tendrá derecho a realizar un máximo de 6 auditorías a lo largo de la vida del contrato, y dentro de este alcance, al menos una cada 2 años.

A título informativo, Canal de Isabel II podría llevar a cabo una auditoría en cualquiera de los siguientes momentos:

- Una vez al año.
- A la entrada en producción de diferentes nuevos sistemas
- Cuando circunstancias específicas den a Canal de Isabel II motivos razonables para el supuesto de que el Adjudicatario no cumple con sus obligaciones contractuales.

Los costes facturados por un auditor externo elegido por Canal de Isabel II serán pagados por Canal de Isabel II. Cualquier gasto incurrido por el Adjudicatario con respecto a la auditoría correrá a cargo del Adjudicatario.

Si el resultado de la auditoría demuestra que el Adjudicatario ha facturado sus servicios a Canal de Isabel II con un sobrecoste con respecto a los cargos acordados, el Adjudicatario reembolsará con prontitud las cantidades cobradas de más, más incurrirá en las penalizaciones indicadas en el apartado 9.1 del Anexo I del PCAP.

Sin perjuicio de cualquier otro derecho de Canal de Isabel II, si el resultado de la auditoría demuestra que el rendimiento real de Adjudicatario no cumple con el Catálogo de Servicios, los niveles de servicio, el Plan de Transición o el Plan de Transformación, o si la auditoría revela cualquier otro rendimiento insuficiente o falta de cumplimiento, el Adjudicatario definirá, planificará e implementará las mejoras necesarias para subsanar tal

incumplimiento que serán autorizadas por Canal de Isabel II. Se hará un Plan de Mejora de la auditoría como se describe en este documento.

10.2. Procedimientos de auditoría

10.2.1. Organización de la auditoría

Canal de Isabel II y el Adjudicatario asignarán un coordinador de auditoría en el Cliente y en el Adjudicatario.

10.2.2. Plan de Auditoría

No existe una planificación fija acordada para las auditorías. Cada año Canal de Isabel II preparará un Plan de Auditoría que refleje, al menos, lo siguiente:

- Universo de auditoría (en términos de potenciales objetos de auditoría).
- Lista no limitativa de auditorías que Canal de Isabel II llevará a cabo en el año en curso.
- Calendario previsto.
- Seguimiento de Auditorías.

Canal de Isabel II puede cambiar el Plan de Auditoría durante el año cuando Canal de Isabel II identifica la necesidad de hacerlo. Los cambios en el Plan de Auditoría se comunicarán al coordinador de auditoría del Adjudicatario.

El coordinador de auditoría de Canal de Isabel II gestionará el Plan de Auditoría. El Coordinador de Auditoría de Canal de Isabel II mantendrá relaciones con las partes pertinentes de auditoría fuera de Canal de Isabel II (auditores externos, reguladores, etc.), coordinará y supervisará las iniciativas de auditoría y actualizará los requisitos de auditoría y Plan de Auditoría con respecto a los servicios proporcionados por el Adjudicatario cuando sea necesario. El Coordinador de Auditoría de Canal de Isabel II comunicará el Plan de Auditoría anual al Coordinador de Auditoría del Adjudicatario.

10.2.3. Notificación

Canal de Isabel II notificará al Coordinador de Auditoría del Adjudicatario de una próxima auditoría con un mes de antelación. Dicha comunicación contendrá información sobre los requisitos de auditoría en los siguientes términos:

- Los objetivos de la auditoría.

- Alcance de la auditoría.
- Duración de la auditoría.
- Listado de información necesaria que debe estar disponible (este listado puede ser modificado durante la auditoría).
- Actividades especiales que los auditores necesiten realizar (ejecución de software de auditoría o scripts).
- Ubicación(es) de auditoría.
- Roles implicados y fechas en las que deben estar disponibles.
- Nombres de los auditores.

El Coordinador de Auditoría del Adjudicatario evaluará los requisitos de auditoría e informará al Coordinador de Auditoría de Canal de Isabel II sobre cualquier conflicto que afecte a la auditoría.

Para las auditorías causadas por circunstancias específicas que den a Canal de Isabel II motivos razonables para el supuesto de que el Adjudicatario no cumple con sus obligaciones contractuales, se notificará al Coordinador de Auditoría del Adjudicatario tan pronto como sea razonablemente posible. Si no hay tiempo para definir los requisitos de auditoría, la notificación puede ser informal.

En estos casos, el Adjudicatario proporcionará la información solicitada y el acceso a los datos con alta prioridad.

10.2.4. Reunión de arranque

La reunión de arranque se llevará a cabo el primer día de la auditoría, con el Adjudicatario, Canal de Isabel II y los auditores para comunicar a los participantes los requisitos de la auditoría a fin de eliminar cualquier confusión.

10.2.5. Trabajo de campo

El Coordinador de Auditoría del Adjudicatario facilita el trabajo de auditoría, poniendo a disposición del equipo auditor los distintos elementos expuestos en los requisitos de auditoría y haciendo que los roles implicados estén disponibles y con el propósito de acelerar el proceso de auditoría. Aquellos que participen en alguna reunión durante el proceso de auditoría resolverán la solicitud de información adicional (documentación, datos, procedimientos, etc.) y verificarán que las actas de las reuniones reflejan los puntos tratados y resultados obtenidos.

El Coordinador de Auditoría del Adjudicatario podrá asistir a cualquier reunión de trabajo de campo durante el proceso de auditoría.

El trabajo de campo incluye:

- Entrevistas con empleados del Adjudicatario o con terceros contratados por el Adjudicatario.
- Consulta de documentación.
- Pruebas de los procedimientos tomando muestras.
- Otras actividades que se requieran para ofrecer garantías suficientes sobre la calidad de los procesos y datos.

10.2.6. Informe de auditoría

Cada auditoría se traduce en un informe de auditoría donde se refleja el cumplimiento del servicio según el alcance establecido. El informe de auditoría se presentará en una reunión a la que asistirán el Coordinador de Auditoría de Canal de Isabel II y el Coordinador de Auditoría del Adjudicatario.

El Coordinador de Auditoría del Adjudicatario elaborará un Plan de Mejora para solventar las posibles no conformidades expuestas en el informe. En dicho Plan de Mejora se indicará, para cada no conformidad, las acciones a tomar, la fecha en la que acción será completada y la persona responsable de realizar la acción. El Plan de Mejora se entregará a Canal de Isabel II no más tarde de un mes después de la fecha del informe de auditoría. Canal de Isabel II aprobará el Plan de Mejora y lo remitirá al equipo auditor para su aprobación final.

10.2.7. Seguimiento

Se realizará un seguimiento del cumplimiento de las acciones del Plan de Mejora debido a la auditoría. Dicho seguimiento se realizará en las reuniones de seguimiento del servicio establecidas mensualmente según se indica en el Modelo de Gobierno.

10.2.8. Software para la auditoría

Con el fin de acelerar el proceso de auditoría mediante la automatización de actividades, el equipo auditor podrá solicitar la instalación y ejecución de cierto software de auditoría o de scripts relacionados. En ese caso se seguirá el proceso de Gestión de Cambios acordado. El software de auditoría y los scripts pueden incluir descarga de datos de Canal de Isabel II o del Adjudicatario o la extracción de la configuración de equipos. El Adjudicatario facilitará la implantación del software de auditoría o scripts.

10.2.9. Documentación

Canal de Isabel II puede acceder a toda la documentación necesaria que mantiene el Adjudicatario que está relacionada con los servicios. El Adjudicatario entregará una copia (electrónica) de la documentación pertinente si es necesario. Canal de Isabel II y el equipo auditor tratarán toda la documentación suministrada por el Adjudicatario con carácter confidencial.

10.2.10. Auditorías realizadas por terceros

Canal de Isabel II puede decidir delegar las actividades de auditoría a auditores independientes. El Adjudicatario tratará estos auditores independientes de manera similar a lo descrito en este documento y los considerará como si fueran empleados de Canal de Isabel II. En los casos auditorías realizadas por terceros, Canal de Isabel II seguirá siendo responsable de la Auditoría.

Canal de Isabel II puede decidir contratar a expertos en la materia para delegar actividades de auditoría específicas. El Adjudicatario podrá rechazar a estos expertos en la materia si concurren motivos razonables. Si el Adjudicatario rechaza el experto en la materia, propondrá un experto en la materia alternativo comparable al presentado por Canal de Isabel II. Estos expertos firmarán un acuerdo de confidencialidad aceptable para el Adjudicatario.

Canal de Isabel II será responsable de las acciones u omisiones de estos auditores independientes y asegurará que se adhieran a las obligaciones derivadas del Acuerdo Marco de Servicios, como si fueran parte del mismo (por ejemplo, en temas de confidencialidad), sin obstáculos o impedimentos.

El Coordinador de Auditoría del Adjudicatario y el Coordinador de Auditoría de Canal de Isabel II se mantendrán mutuamente informados acerca de las actividades previstas por el auditor independiente.

11. ESTRUCTURA DE LAS OFERTAS

Las empresas licitadoras deberán presentar de forma precisa, estructurada, clara y concisa sus propuestas.

Para facilitar su valoración, debe presentarse una copia digital de la oferta. En caso de discrepancia prevalecerá la copia en papel. No se valorarán las ofertas que no se ajusten a la estructura indicada.

No serán tomadas en consideración en el presente procedimiento de licitación las ofertas que no se ajusten a la estructura indicada o que no cumplan los requisitos mínimos establecidos en el presente Pliego.

La estructura de la oferta técnica se encuentra detalla en el **apartado 6 del anexo I del PCAP**.

12. CONDICIONES DE ACEPTACIÓN, GARANTÍA Y MANTENIMIENTO

El Adjudicatario comunicará por escrito a Canal de Isabel II la entrega de los trabajos objeto de cada una de las fases de este pliego en la reunión de control, la cual se mantendrá con el carácter periódico que se determine.

Canal de Isabel II revisará cada uno de los resultados del trabajo y comprobará su adecuación a los requisitos establecidos. Como consecuencia de ello, hará una propuesta de corrección o mejora, que el Adjudicatario deberá implantar, o dará su aceptación definitiva.

En todo caso, se establece un periodo de garantía de **6 meses**, durante el cual el Adjudicatario se comprometerá a resolver cualquier error o falta de adecuación a los requisitos detectados con posterioridad a la aceptación definitiva.

Firmado electronicamente por RODRIGUEZ
HERRADURA JUAN FIRMA

Firma: Juan Rodríguez Herradura
RESPONSABLE DE APLICACIONES

Firmado electronicamente por: RAFAEL EGIDO
BLÁNDEZ
En la fecha y hora 05.12.2022 14:49:24 CET

Firma: Rafael Egidio Blández
JEFE ÁREA APLICACIONES INFORMÁTICAS

Firmado electronicamente por: CESAR MARTÍN
MEGÍAS
En la fecha y hora 07.12.2022 10:11:59 CET

Firma: César Martín Megías
JEFE ÁREA OPERACIÓN CENTRO DE CONTROL

Firmado electronicamente por: Ángel Rodríguez
García
En la fecha y hora 05.12.2022 14:54:05 CET

Firma: Ángel Rodríguez García
SUBDIRECTOR SISTEMAS INFORMÁTICOS

Firmado electronicamente por: FRANCISCO JAVIER
FERNÁNDEZ DELGADO
En la fecha y hora 07.12.2022 11:14:14 CET

Firma: Francisco Javier Fernández Delgado
SUBDIRECTOR DE TELECONTROL

Firmado electronicamente por 02877981Z JUAN
SÁNCHEZ (R:A86488087)

Firma: Juan Sánchez García
DIRECTOR INNOVACIÓN E INGENIERÍA

ANEXO 1. CUESTIONARIO PERSONAL

Cuestionario por persona del equipo propuesto.

Apellidos, Nombre - identificador	
Perfil ofertado	

Formación Académica.

Título Académico	Centro	Años	F-expedición

Formación en Tecnologías de la Información y/o Consultoría.

Curso	Impartido por	Horas	Fecha inicio

Se consignarán aquí las certificaciones técnicas exigidas para la realización de los trabajos.

Certificaciones exigidas

Módulo	Fecha de Certificación	Nivel de Certificación

Experiencia Profesional (sólo en el perfil ofertado)

Proyecto	Empresa	Perfil Ofertado	Categoría profesional en la empresa	Fecha inicio	Fecha fin	Meses	Descripción funciones realizadas
						Total meses	

ANEXO 2. METODOLOGÍA DE GESTIÓN DE PROYECTO DE CANAL DE ISABEL II

El Área de Planificación, Control y Seguridad a través de la Oficina de Proyectos, pone a disposición de los licitadores que así lo requieran, a través del enlace:

https://www.canaldeisabelsegunda.es/documents/20143/3672224/Metodologia_de_Gestion_de_Proyectos_Proyecto_y_Servicio.zip

El licitador deberá utilizar para presentar el Plan de Proyecto en su oferta la plantilla:

ODP-G-Plan_de_Gestión_del_Proyecto.docx

que contiene todos los capítulos necesarios para describir los objetivos, alcance, modelo, solución y herramientas propuestas y para el adecuado seguimiento y control del proyecto. La no presentación del plan en la plantilla suministrada por Canal de Isabel II supondrá que la oferta no sea tomada en consideración en el presente procedimiento de licitación.

Consta de los siguiente capítulos:

- Introducción al Plan de Gestión del Proyecto
 - Propósito
 - Alcance
 - Preparación
 - Aprobación
 - Actualización
 - Periodicidad del control y revisión del Plan
- Introducción al Proyecto (Descripción general del Proyecto)
 - Descripción general
 - Descripción del Alcance
 - Descripción de la solución/modelo/herramientas
 - Descripción detallada del modelo y herramientas propuestos y de sus componentes.
 - Entorno tecnológico necesario.
 - Roles y Responsabilidades
- Planes para cada una de las áreas de Gestión
 - Plan de Gestión del Alcance (Gestión de Cambios) en el que se tendrán en cuenta las diferentes fases que conforman su alcance. En él se incluirá, para la fase 3, el ANS que el licitador propone o, en su caso, el acatamiento con carácter general del ANS que acompaña a este pliego.
 - Plan Gestión del Tiempo/Cronograma en el que se identifiquen las diferentes fases.

- Plan de Gestión de Costes. Las fases 1 y 2 se tratarán en cuanto a coste como un proyecto cerrado con un coste también cerrado e independiente. La fase 3 en función de la imputación de horas realizada al proyecto. La fase 4 se planificará durante las fase 1 y 2 con cargo al presupuesto de estas fases, ejecutándose al final del proyecto con cargo al presupuesto de la fase 3.
 - Plan de Gestión de Riesgos/Contingencias. De forma separada para cada una de las fases.
 - Plan de Gestión de Recursos. En este plan se tendrán en cuenta los diferentes equipos de trabajo que puedan participar en las diferentes fases del proyecto.
 - Plan de Gestión de la Comunicación. De la misma manera que en los planes anteriores, se tendrán en cuenta las diferentes fases y sus diferentes modelos de gestión (Proyecto y Servicio). En ésta se incluirán los modelos de Gestión del ANS, del Servicio, de la Relación y del Contrato que el licitador propone según las directrices contenidas en los sucesivos apartados de este pliego.
 - Plan de Gestión de la Calidad.
- Cierre del Proyecto

El ofertante deberá presentar la metodología prevista para el desarrollo de los trabajos de las fases de pleno servicio y, también, para la devolución del servicio, bien por rescisión del contrato tras reiterados incumplimientos de los niveles de servicio o por la finalización del mismo.

El Plan de Proyecto deberá ser ajustado por el Adjudicatario, una vez realizada la adjudicación, para su aprobación por parte de Canal de Isabel II. Deberá, por tanto, ser aprobado por Canal de Isabel II antes del inicio de los trabajos.

ANEXO 3. CONSIDERACIONES DE SEGURIDAD DE APLICACIONES PARA CANAL DE ISABEL II, S.A.

CONSIDERACIONES PARA EL DESARROLLO SEGURO DE APLICACIONES:

1.- OBJETO Y ÁMBITO DE APLICACIÓN

El objeto de este procedimiento general de seguridad es definir, independientemente de la tecnología, un conjunto de buenas prácticas de codificación y desarrollo seguro que se pueden integrar en el ciclo de vida del desarrollo de software como requisitos de codificación y cuya implementación permitiría mitigar las vulnerabilidades de software más comunes.

En general, es mucho menos costoso desarrollar software seguro que corregir los problemas de seguridad después de que la aplicación se ha completado, por no hablar de los costes, tangibles e intangibles, que pueden estar asociados a un fallo de seguridad.

El objetivo de la seguridad tanto en las aplicaciones como en los sistemas de información de Canal de Isabel II Gestión, S.A. (en adelante, Canal de Isabel II) es mantener la confidencialidad, integridad y disponibilidad de los activos de información que forman parte de los procesos de negocio y, a través de la implementación de los necesarios y adecuados controles de seguridad, permitir su ejecución satisfactoria.

2.- DEFINICIONES

Activo (de información).

Recurso perteneciente a Canal de Isabel II y que contiene algún tipo de información relevante para su negocio.

Puede presentarse en diferentes soportes (oral, impreso o electromagnético) y en cualquier estado de su ciclo de vida, debiendo ser protegido en cualquiera de estos estados con la misma diligencia y de forma acorde a su clasificación.

Adjudicatario.

Responsable del proyecto de desarrollo perteneciente a la empresa externa con la que Canal de Isabel II establece una relación contractual para la asistencia técnica o realización de un proyecto de desarrollo, designado específicamente por dicha empresa para ello.

Algoritmos de cifrado robusto.

Aquellos algoritmos de cifrado que han demostrado resistencia al criptoanálisis.

Amenaza

Causa potencial de un incidente no deseado, que puede ocasionar daño a un sistema u organización.

Aplicaciones.

Programa o conjunto de programas informáticos que soportan procesos de una o varias actividades de gestión o de apoyo para Canal de Isabel II.

Autenticación

Es la propiedad que permite comprobar la autenticidad de la identidad de la entidad, es decir, comprobar que una entidad es quien dice ser. Toda aplicación desarrollada para Canal de Isabel II realizará una comprobación de la autenticidad de las entidades que acceden a ella, verificando sus credenciales de acceso.

Autorización.

Es el proceso por el cual se autoriza al usuario identificado y autenticado a acceder sólo a aquellos recursos a los que se le ha permitido el acceso.

Canonicalizar.

Convertir distintas codificaciones y representaciones de datos a una forma estándar predefinida.

Certificados digitales.

Son claves criptográficas firmadas por una autoridad de certificación reconocida.

Ciclo de vida (de un activo).

Estados en los que un activo de información puede potencialmente presentarse. Son generación, transmisión, almacenamiento, compartición/publicación y eliminación.

Condiciones de carrera (*race conditions*).

Si los procesos que están en ejecución no son correctamente sincronizados, puede producirse un error de corrupción de datos, lo que puede ser aprovechado para vulnerar los sistemas

Confidencialidad.

Propiedad de un activo, por la que la información contenida debe ser protegida de la exposición fuera de una audiencia determinada, de una forma proporcional al daño que le causaría a Canal de Isabel II dicha exposición.

Control (salvaguarda, medida de seguridad o contramedida).

Medio de gestión del riesgo, que incluye políticas, procedimientos, directrices, prácticas o estructuras de la organización, y que pueden ser de naturaleza administrativa, técnica, de gestión o legal.

Cookie.

Pequeña información enviada por un sitio web y almacenada como un fichero en el equipo del usuario con el propósito de llevar el control de usuario, conseguir información sobre su actividad previa, hábitos de navegación, etc. Esto permite al sitio web ofrecer al usuario, entre otras cosas, una experiencia personalizada.

Disponibilidad.

Propiedad de un activo, por la que la información que contiene está a disposición (accesible y utilizable) de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones.

Entidad.

Todo usuario físico, programa, aplicación, servicio o sistema que accede y hace uso de la información.

Evento de seguridad de la información.

Es la presencia identificada de un estado del sistema, del servicio o de la red que indica un posible incumplimiento de la política de seguridad de la información, un fallo de controles, o una situación previamente desconocida que puede afectar a la seguridad.

Framework.

Conjunto estandarizado de conceptos, prácticas y criterios que sirve como referencia para enfocar un tipo de problemática particular.

Hash.

Funciones inyectivas sin inversa que se usan principalmente para generar un conjunto de datos resumen de un tamaño fijo como referencia unívoca del conjunto de datos de entrada. Las funciones hash o checksum pueden ser criptográficamente robustas o no, dependiendo de la facilidad para someterlas a criptoanálisis e identificar colisiones (identificar dos conjuntos de datos distintos que generan el mismo conjunto de datos resumen, desconociendo éste previamente) o ataques por preimagen (construir un conjunto de datos que generen el mismo conjunto conocido de datos resumen).

Integridad.

Propiedad de un activo de información, por la que la información que contiene está libre de modificaciones no autorizadas. Salvaguarda la exactitud y completitud de la información.

Identificación.

Es el proceso de verificación de la identidad de una entidad. Toda entidad deberá tener un identificador único para permitir la trazabilidad de las acciones que realice.

No repudio.

Protección contra la negación, por parte de alguna de las entidades implicadas, de haber participado en toda o en parte de la comunicación, evitando que el emisor o el receptor nieguen la transmisión de un mensaje.

Puesta en Producción.

Proceso de creación, verificación y puesta en marcha del entorno productivo y despliegue e implantación de la aplicación desarrollada.

Propietario o Dueño de los datos.

Es el principal usuario de los datos y dueño de los mismos.

Responsable de la Aplicación.

Responsable designado por la Unidad Organizativa a la que da servicio un Sistema de Información para aprobar las mejoras o informes y autorizar el acceso a la aplicación. En aquellos Sistemas de Información en los que se traten datos sujetos a la ley de Protección de Datos, este responsable será el Responsable Operativo del Fichero.

Riesgo.

Valoración de la frecuencia (probabilidad) de que una o más amenazas aprovechen una o más vulnerabilidades y la magnitud de la posible pérdida (impacto) de uno o más activos de información.

Salt.

Datos aleatorios que se usan como una entrada adicional a una función hash para obtener los datos resumen de una contraseña o frase de contraseña (passphrase).

Seguridad de la Información.

Es la protección de la información y de los sistemas de información contra el acceso no autorizado y/o la modificación de la información, ya sea en su almacenamiento, procesamiento o tránsito, y en su disponibilidad a los usuarios autorizados.

Sistema de Información.

Aplicación o conjunto de aplicaciones informáticas cuya finalidad es dar soporte a una unidad o proceso de negocio de Canal de Isabel II.

TLS.

Acronimo de Transport Layer Security.

3.- DESARROLLO

A lo largo del Ciclo de Vida del Desarrollo de los Sistemas de Información, se ha de contemplar la seguridad de una manera integrada. Por ello, en este Procedimiento General se abordan las actividades de seguridad en las diferentes fases del desarrollo de sistemas de información como se muestra en el siguiente diagrama:



3.1.- Fase de Diseño.

3.1.1.- Establecimiento de Requisitos de Seguridad.

La construcción de aplicaciones o sistemas requiere considerar la seguridad de la información y el mantenimiento de medidas apropiadas a lo largo de la fase de diseño del desarrollo. Los requisitos de seguridad de la información deberán ser tratados y considerados como una parte integral de los requisitos de negocio. Por ello, los requisitos de seguridad deben ser considerados al evaluar las distintas alternativas de diseño de las aplicaciones.

Se establecerán los requisitos de seguridad necesarios para mantener el riesgo a un nivel aceptable, considerando implicaciones de coste y eficiencia. Estos serán identificados teniendo en cuenta, al menos:

- Toda la información procesada por la aplicación.
- Obligaciones contractuales, reguladoras y legales.
- Los requisitos y objetivos de negocio de Canal de Isabel II

El Dueño de los Datos / Responsable de la Aplicación procederá a la valoración ACIDA de los activos de información que se gestionarán en la aplicación en caso de que sean activos de información nuevos. Para dicha valoración ACIDA será de aplicación el Procedimiento General de Clasificación y Tratamiento Seguro de la Información PGS-001. Si se trata de activos de información ya existentes, se informará de su valoración ACIDA actual.

Toda aplicación o sistema que se desarrolle en o para Canal de Isabel II, deberá cumplir, al menos, con los siguientes **Requisitos Generales de Seguridad**:

[RGS01] Arquitectura de seguridad.

Las aplicaciones desarrolladas en o para Canal de Isabel II deberán conseguir una integración óptima en el entorno tecnológico de Canal de Isabel II, en particular, deberán hacer uso de los servicios de seguridad ofrecidos por dicho entorno (control de accesos mediante mecanismos de seguridad perimetral e interna (cortafuegos, NAC, IPS, etc.) servicios de directorio, SSO, servicios de criptografía, etc.). Asimismo, deberán disponer de un diseño de arquitectura que facilite el comportamiento seguro de la aplicación (Seguridad por Diseño).

El responsable del proyecto deberá proporcionar inicialmente a la Dirección de Seguridad el documento **“Arquitectura de la Aplicación”** en el que se detallará el diseño de arquitectura de la aplicación. Este documento debe contemplar, al menos:

- Diagrama de arquitectura con indicación de los interfaces entre sus componentes.
- Descripción detallada de los componentes de la aplicación o sistema. Se reflejarán los componentes y elementos que formen parte de la arquitectura, conexiones de red entre ellos, flujos de los datos, protocolos y puertos previstos para las comunicaciones tanto entre los componentes, como con otros sistemas, así como los interfaces de usuario.

[RGS02] Modelado de amenazas.

Todas las aplicaciones desarrolladas en o para Canal de Isabel II tendrán un modelo de amenaza desarrollado y documentado basado en la evaluación del riesgo de la aplicación. El enfoque de evaluación del riesgo contemplará, al menos, lo siguiente:

- Descomponer la aplicación a través de un proceso de inspección manual, comprendiendo cómo funciona la aplicación, sus activos, funcionalidad y conectividad.
- Identificar los activos afectados, obtener su clasificación e inferir los controles que les aplican.
- Identificar, documentar y valorar las amenazas potenciales a través de un proceso de desarrollo de escenarios de amenaza, árboles de ataque que desarrollen una visión realista de potenciales vectores de ataque desde la perspectiva del atacante, así como la identificación de las condiciones necesarias para que un ataque se logre llevar a cabo con éxito.
- Explorar e identificar condiciones o vulnerabilidades potenciales (técnicas, operacionales y de gestión), proporcionando información relevante sobre cuáles serían las contramedidas más eficaces para contrarrestar un posible ataque y/o mitigar los efectos de la presencia de una vulnerabilidad en nuestro sistema/aplicación.
- Proveer información sobre cómo las medidas actuales previenen la consecución de ataques
- Crear estrategias sólidas de mitigación para las vulnerabilidades o brechas de seguridad encontradas: desarrollar controles de mitigación para cada una de las amenazas

que se consideran realistas. El resultado de un modelo de amenaza es, generalmente, una colección de listas y diagramas.

- Proporcionar una estrategia sólida para evitar posibles vulnerabilidades y brechas de seguridad.
- Simplificar la posterior actualización mediante el uso de componentes reutilizables.
- Transmitir al negocio la importancia de los riesgos tecnológicos en términos de impacto de negocio.
- Facilitar la comunicación y promover una mejor concienciación sobre la importancia de la seguridad.

Para la evaluación del riesgo se utilizará la metodología MAGERIT en su versión 2, aunque para aquellos aspectos no cubiertos por esta metodología se pueden contemplar otras como NIST 800-30, OCTAVE, CRAMM, etc., siempre que los criterios de evaluación puedan ser mapeables con los de MAGERIT v2 y los resultados estén alineados con ella.

[RGS03] Principio de Separación de Privilegios, Mínimos Privilegios, Segregación de Funciones y Mínimos Mecanismos Comunes.

Son cuatro principios relacionados:

1. Mínimos privilegios (*Least privilege*).

Cada usuario y proceso deberán tener un conjunto de derechos de acceso mínimo y suficiente para desempeñar sus tareas. El privilegio mínimo limita el daño que un usuario malicioso podrá ejercer si toma el control del programa. Los derechos de acceso deberán ser exigidos explícitamente, en lugar de ser dados a los usuarios por defecto.

2. Separación de privilegios (*Separation of Privileges*).

La separación de privilegios es una técnica que se usa para atenuar el daño potencial de un ataque.

Es muy importante diferenciar y separar los privilegios necesarios en cada momento en un programa y entre distintas rutinas o programas. De este modo, desde una parte del programa no se podrán ejecutar operaciones que no se tenían previstas en un principio. Un atacante no podrá aprovechar el control sobre un programa para efectuar tareas distintas o adicionales al propósito del mismo.

3. Segregación de funciones (*Segregation of Duties - SoD*).

3.a) En el aspecto funcional de la aplicación:

Ninguna persona o grupo de personas con funciones y/o responsabilidades comunes debe poder manejar todos los aspectos o fases de una misma transacción. Toda transacción debe ser realizada en cuatro etapas:

- i. Aprobación.
- ii. Autorización.
- iii. Ejecución.
- iv. Registro.

El control de las dichas etapas debe correr a cargo de empleados o grupos de empleados comunes relativamente independientes.

La finalidad de la segregación de funciones es tanto poder detectar los errores involuntarios como para que ninguna persona o grupo de personas se halle en posición de poder cometer un fraude y ocultar su acción por medio de la falsificación o modificación no autorizada de información sin confabularse con otros miembros de la organización.

3.b) En el aspecto de gestión:

Los roles de desarrollo, administración, operación y usuario final tienen que estar claramente diferenciados y existir mecanismos de identificación de pertenencia a cada grupo.

4. Mínimos mecanismo comunes (*Least common mechanisms*).

Los mecanismos comunes a más de un usuario, proceso y/o función no deben ser compartidos. Cada mecanismo compartido (especialmente las variables compartidas) por más de un usuario es potencialmente un camino de intercambio de información entre usuarios y debe ser evitado.

[RGS04] Validación de los datos.

Se deberá tratar la entrada, el procesamiento y la salida de los datos, para permitir explícitamente los datos válidos y no permitir ningún otro tipo de dato.

La validación de datos garantiza la estabilidad adecuada del sistema ya que realiza un control preventivo sobre aquellos datos que el sistema espera recibir, que va a procesar o que va a devolver como salida.

- Validación de datos de entrada.

Todos los datos de entrada deberán ser validados para garantizar que son correctos y apropiados. Esta validación se realizará siempre en un sistema confiable (como, por ejemplo, el servidor). Como norma general, la aplicación estará configurada adecuadamente para especificar un conjunto de caracteres definido (como, por ejemplo, UTF-8) para todas las fuentes de entrada. Antes de la validación, todos los datos de entrada serán convertidos y codificados a ese conjunto de caracteres definido (canonicalización) y cualquier fallo de validación dará como resultado el rechazo de los datos de entrada.

Se validarán y comprobarán obligatoriamente, al menos, los siguientes aspectos:

- a) las longitudes de las cadenas de datos de entrada.
- b) los datos de entrada provenientes de variables de entorno del sistema operativo.
- c) los campos obligatorios.
- d) los campos de formularios.
- e) los rangos de datos.
- f) la comprobación de parámetros vacíos.
- g) del formato de los datos de entrada para aceptar sólo los formatos aceptados: uso de *mime-types*, *content-type*, *magic numbers*, etc.
- h) todos los datos de entrada contra una "lista blanca" de caracteres permitidos, siempre que sea posible.
- i) si no es posible definir una "lista blanca" de caracteres permitidos, será obligatorio implementar controles adicionales, como, por ejemplo:
- j) codificación de los datos de salida

- k) APIs de seguridad para el tratamiento de los datos
- l) niveles de autorización y registro en el uso de los datos dentro de la aplicación
El objeto es controlar exhaustivamente caracteres identificados como potencialmente peligrosos (por ejemplo: < > " ' % () & + \ / \ ' \") para evitar la inserción de cadenas de texto especialmente diseñadas, manipuladas o maliciosas por parte de un potencial atacante.
- m) bytes nulos (%00).
- n) caracteres de nueva línea (%0d, %0a, \r, \n).
- o) caracteres de alteraciones de ruta "punto, punto, barra" (./ o ..\). En los casos en que se soporten conjuntos de caracteres extendidos (por ejemplo, UTF-8 extendido), será obligatorio contemplar representaciones alternativas, tales como: %c0%ae%c0%ae/ (es necesario utilizar la canonicalización como forma de implementar la doble codificación u otras formas de ofuscación de ataques).

Siempre que sea posible, se debe hacer uso de valores establecidos previamente por defecto (por ejemplo, listas desplegables que contengan sólo las entradas permitidas) en lugar entradas que se puedan realizar libremente por el usuario.

El objetivo es lograr una correcta validación en la entrada de datos a un sistema o aplicación minimizando el riesgo de realización de ataques al sistema a través de vulnerabilidades de tipo *HTTP request smuggling*, *heap overflow* (*use-after-free*, *double free*, *dereference after free*), *off-by-one*, *format string*, *integer overflows/underflows*, *memory leaks*, *buffer overflow*, etc.

- Control en el procesamiento interno de los datos.

Deberán incorporarse comprobaciones de validación para detectar información alterada. La validación de los datos durante su procesamiento está orientada a asegurar tanto su estabilidad e integridad como la del propio sistema ante posibles fallos en el procesamiento.

Los datos introducidos correctamente pueden verse alterados durante su procesamiento debido a errores o a actos deliberados. Se deberán incorporar filtros de comprobación y validación para detectar dicha alteración y poder llevar a cabo las acciones de remediación que se identifiquen. El diseño de las aplicaciones debe asegurar la implantación de mecanismos que minimicen el riesgo debido a fallos en el proceso que provoquen pérdidas de integridad.

Los aspectos a considerar son:

- Condiciones de carrera (*race conditions*): interacción entre hilos en un proceso, concurrencia de distintos procesos, uso de recursos compartidos, etc.
- Introducir controles tales como la gestión de los niveles de autorización de acceso a los datos, registros de auditoría de acceso a los mismos, uso de funciones resumen (hash) criptográficamente robustas, firma digital, etc.
- La ubicación y uso en los programas de funciones tipo 'añadir' y 'borrar' para cambiar los datos.
- Los procedimientos para evitar la ejecución de procesos en el orden equivocado o después de fallos en un proceso anterior.
- El uso de programas de recuperación de fallos para asegurar el correcto y adecuado procesamiento de los datos.

- El uso de procedimientos almacenados predefinidos o prediseñados en lugar de realizar construcción de sentencias.

- Validación de datos de salida:

Se deberán validar los datos de salida de una aplicación para garantizar que el proceso de la información ha sido correcto y apropiado a lo definido. La validación de salidas deberá comprobar, al menos:

- Que los datos de salida son los esperados y son verosímiles.
- Que se suministra suficiente información al usuario o a un sistema de proceso subsiguiente para poder permitir determinar la exactitud, completitud, precisión y clasificación de la información.

Todas las salidas, y códigos de retorno y de error deberán ser verificados y tratados. Se contemplará obligatoriamente la correcta codificación de los datos de salida a través de un sistema confiable (por ejemplo, el servidor) y utilizando preferiblemente funciones estándar o rutinas completamente verificadas. Dicha codificación se realizará en base a cómo los datos de salida serán utilizados. También se tendrá en cuenta la sanitización de la salida, sobre todo ésta se vaya a utilizar para la construcción de sentencias (por ejemplo, SQL, XML, LDAP, etc.) o para el envío de comandos al sistema operativo.

[RGS05] Autenticación y gestión de contraseñas.

Será necesario requerir autenticación para todos los recursos excepto aquellas específicamente clasificadas como públicas.

Todos los controles de autenticación deben ser efectuados en un sistema confiable (por ejemplo, el servidor).

Siempre que sea posible, establecer y utilizar servicios de autenticación estándares y ampliamente probados.

Utilizar una implementación centralizada para todos los controles de autenticación, incluyendo librerías que llamen a servicios externos de autenticación.

Segregar la lógica de la autenticación del recurso solicitado y utilizar redirección desde y hacia el control centralizado de autenticación.

Todos los errores de los controles de autenticación deben ser controlados y, en caso de que se produzca el fallo, hacerlo de forma segura.

Todas las funciones de la aplicación dedicadas a la administración y gestión de las cuentas de usuario deben ser al menos tan seguras como el mecanismo primario de autenticación.

La aplicación permitirá establecer políticas relativas a asegurar la fortaleza de la contraseña. Por ejemplo, la longitud de la contraseña deberán ser de, al menos, 8 caracteres, conteniendo tanto caracteres alfanuméricos, con mayúsculas y minúsculas, como no alfanuméricos. Se recomienda una longitud de 16 caracteres o el uso de "frases

de contraseña” (*passphrases*) de varias palabras, que incluyan también números y caracteres no alfanuméricos.

Si la aplicación dispone de un almacenamiento de contraseñas, se debe asegurar que únicamente se almacenará el resumen de las mismas, generado a través de funciones resumen unidireccionales, implementadas en un sistema confiable (por ejemplo, el servidor), criptográficamente robustas y que usen un *salt* aleatorio y único para cada contraseña.

El archivo/tabla donde se almacenen sólo podrá ser escrito por la aplicación.

No utilizar algoritmos de hash comunes, tales como MD5 o SHA1, dado que no son criptográficamente robustos o que presentan ataques conocidos. En su defecto, se utilizarán funciones de derivación de clave (*key derivation function*), con las siguientes características:

- i. *Salt* aleatorio de, al menos, 64 bits de longitud (se recomiendan 128 bits).
- ii. Al menos, 1000 iteraciones.

Se deberán validar los datos de autenticación únicamente después de haber completado todos los datos de entrada, especialmente en implementaciones de autenticación secuencial.

Las respuestas a los fallos en la autenticación no deben indicar qué parte de la autenticación fue incorrecta. Por ejemplo, en lugar de “usuario inválido” o “contraseña inválida”, utilizar “usuario y/o contraseña inválidos” en ambos casos. Las repuestas a los errores deben ser idénticas tanto a nivel de lo que se le muestra al usuario como lo que éste pueda visualizar en el código fuente (por ejemplo, en páginas web).

Utilizar siempre autenticación en conexiones a sistemas externos que involucren información o funciones sensibles.

Las credenciales de autenticación para acceder a servicios externos a la aplicación deben estar cifradas y almacenadas en ubicaciones protegidas y en un sistema confiable (por ejemplo, el servidor). El código fuente NO es una ubicación segura.

Las contraseñas se transmitirán exclusivamente a través de conexiones cifradas. En caso de sea necesaria una autenticación sobre HTTP, las credenciales de autenticación serán transmitidas exclusivamente en el cuerpo POST, nunca en la URL.

Utilizar únicamente conexiones cifradas o datos cifrados para el envío de contraseñas que no sean temporales. Las contraseñas temporales (como, por ejemplo, aquellas asociadas con restablecimientos enviados por correo electrónico), pueden ser una excepción.

Las entradas de datos en los campos “contraseña” siempre deben ser ofuscadas u ocultadas en la pantalla del usuario (por ejemplo, utilizando el tipo de entrada “*password*” en los formularios de páginas web).

Proteger las cuentas contra ataques de fuerza bruta mediante la aplicación de técnicas de protección estándar como, por ejemplo:

- Uso de CAPTCHAs.
- Deshabilitar las cuentas tras un número establecido y configurable de intentos fallidos de acceso al sistema. Nota: el tiempo que permanecerá la cuenta deshabilitada deberá ser suficiente como para evitar el ataque por fuerza bruta, pero no tan alto como para permitir un ataque de denegación de servicio.

- Limitando el número de intentos en un periodo de tiempo determinado y configurable.

Los procesos de cambio y reseteo de contraseñas requieren los mismos niveles de control que aquellos asociados a la creación y autenticación de cuentas.

Si se utiliza el correo electrónico en el proceso de reseteo de una contraseña, únicamente se enviará un enlace a una página web dinámica del sistema o contraseñas temporales a direcciones de correo previamente registradas en el sistema. Este proceso debe realizarse siempre antes de las preguntas de seguridad (en caso de que existan).

Las contraseñas y enlaces temporales deben tener un corto periodo de tiempo de validez, además de ser de un solo uso. Se debe forzar el cambio de las contraseñas temporales después de su utilización

En caso de que existan las preguntas de seguridad en la propia aplicación para que el usuario pueda resetear su contraseña en caso de olvido, deberán ser al menos tres, y contemplar un amplio rango de respuestas aleatorias por parte del usuario. No deben ser aceptadas preguntas que pueda establecer el propio usuario o preguntas estándar típicas como “¿Libro favorito?” o “¿Color preferido?”, dado que tienen una alta probabilidad de presentar respuestas comunes.

Los usuarios deben ser notificados cada vez que se produce un reseteo de su contraseña.

Prevenir la reutilización de contraseñas a través del mantenimiento de un histórico.

Las contraseñas deben tener al menos un día de antigüedad antes de poder ser cambiadas, para evitar ataques de reutilización de contraseñas.

Se debe establecer un tiempo de caducidad de las contraseñas, que dependerá de la clasificación de la información a acceder. Por ejemplo, el acceso a información reservada obligará a un cambio de las contraseñas con una periodicidad mayor que el acceso a información confidencial.

Ejemplos: Información "Reservada": 30 días, Información "Confidencial": 40-50 días, Información de "Difusión Limitada": 60-90 días

Se debe establecer el tiempo mínimo permitido entre cada reseteo de contraseñas.

Deshabilitar siempre la funcionalidad de “recordar contraseña” en los campos de tipo “contraseña” de los formularios.

La aplicación debe poder identificar ataques a múltiples cuentas utilizando la misma contraseña, como forma de intentar superar bloqueos estándar de la aplicación cuando los nombres de usuario pueden ser obtenidos o adivinados de alguna forma.

Cambiar todos los usuarios y contraseñas por defecto o deshabilitar las cuentas asociadas.

Será obligatorio reautenticar a los usuarios antes de la puedan realizar operaciones sensibles o críticas.

Siempre que sea posible, utilizar autenticación multifactor para las cuentas más sensibles, con permisos privilegiados o de mayor valor.

Si se utiliza un código de terceros para la autenticación, deberá ser inspeccionado minuciosamente para asegurar que no se encuentre afectado por vulnerabilidades o código malicioso.

[RGS06] Control de la sesión.

Las aplicaciones deberán implementar mecanismos robustos que garanticen el control de la sesión del usuario en la aplicación. De esta forma se evitará que usuarios no autorizados accedan a la información desde inicios de sesiones realizados de forma no controlada o por tiempo indefinido.

A la hora de diseñar la aplicación es preferible intercambiar un único parámetro entre el cliente y el servidor (un identificador de sesión), en lugar de pasar todos los parámetros asociados a la sesión (parámetros de entrada de formularios, rutas de navegación, etc.).

Utilizar los controles del servidor o de un *framework* para la administración de sesiones. La aplicación sólo debe reconocer estos identificadores como válidos.

La creación de identificadores de sesión solo debe ser realizada en un sistema confiable (por ejemplo, el servidor). Se evitará trasladar toda o parte de la lógica de los procesos de autenticación a la parte cliente.

Los controles de administración de sesiones deben utilizar algoritmos que generen identificadores únicos con valores suficientemente aleatorios.

Definir el dominio y ruta para las cookies que contienen identificadores de sesión autenticados con un valor estricto apropiado para la aplicación.

La función de finalización de la sesión (*logout*) debe terminar completamente con la sesión y la conexión asociada, y debe estar disponible en todas las páginas protegidas por autenticación.

Establecer un tiempo de vida de la sesión lo más corto posible (balanceando los riesgos con los requisitos del negocio), incluso cuando la sesión esté activa. Nunca deberá ser superior a varias horas. Llegado al límite fijado, se finalizará la sesión y será necesario volver a autenticarse.

Generar un nuevo identificador de sesión después de cada nueva autenticación.

No permitir inicios de sesión concurrentes con el mismo usuario. Si existe una sesión previa y se inicia una nueva de forma exitosa, la previa deberá finalizarse.

No exponer identificadores de sesión en URLs, mensajes de error, logs en niveles mayores o iguales que INFO, etc. Los identificadores de sesión sólo deben ser ubicados en la cabecera de la cookie HTTP. Por ejemplo, no transmitir identificadores de sesión como parámetros GET.

Proteger la información sobre las sesiones del lado del servidor, implementando los controles de acceso apropiados.

Generar un nuevo identificador de sesión y desactivar el anterior de forma periódica. De esta forma se pueden mitigar algunos escenarios de ataque para el robo de sesiones, donde el identificador se compromete.

Generar un nuevo identificador de sesión si la seguridad cambia de HTTP a HTTPS, como puede suceder durante la autenticación. Dentro de la aplicación es recomendable usar siempre HTTPS en lugar de cambiar entre HTTP y HTTPS.

Es necesaria una gestión complementaria de la sesión para todas las operaciones sensibles realizadas en el lado del servidor como, por ejemplo, la gestión de cuentas de usuario, utilizando identificadores (*tokens*) más robustos (por ejemplo, con mayor requisito de aleatoriedad como garantía de unicidad) o mediante el uso de parámetros. Este método puede ser utilizado para prevenir ataques de *Cross Site Request Forgery* (CSRF). Para operaciones críticas se utilizarán *tokens* o parámetros por petición (*per request*) en lugar de por sesión.

Configurar el atributo “Secure” para las cookies transmitidas sobre una conexión TLS.

Configurar las cookies con el atributo “HttpOnly”, salvo que la aplicación requiera del uso de scripts por parte del cliente para leer o configurar una cookie.

Para facilitar la detección de ataques, se recomienda el uso de identificadores de sesión “*booby trapped*”. Se trata de registrar el uso de identificadores de sesión que nunca son asignados y que permiten detectar si se está realizando un ataque de fuerza bruta contra el identificador de sesión.

[RGS07] Control de acceso.

Para la toma de decisiones de autorización, se utilizarán únicamente objetos confiables del sistema, como por ejemplo, objetos de sesión del servidor.

Utilizar un único componente para el chequeo de autorizaciones para toda la aplicación. Esto incluye librerías que llamen a servicios de autorización externos.

Todos los errores de los controles de acceso deben ser controlados y, en caso de fallo, hacerlo de forma segura.

Por defecto se denegarán todos los accesos en caso de que la aplicación no pueda acceder a la información de la configuración de seguridad.

Requerir controles de autorización en cada solicitud realizada desde el cliente (por ejemplo, AJAX o Flash) y también aquellas creadas por scripts en el servidor (por ejemplo, “*includes*”).

Segregar el código fuente dedicado a la lógica privilegiada.

Restringir el acceso a ficheros u otros recursos únicamente a usuarios autorizados, incluyendo aquellos fuera del control directo de la aplicación. Es obligatorio implementar en la aplicación un modelo de roles, perfiles y autorizaciones.

Restringir sólo a usuarios autorizados el acceso a:

- i. URLs protegidas.
- ii. funciones protegidas
- iii. referencias directas a objetos
- iv. servicios.
- v. información de la aplicación

- vi. usuarios, atributos y políticas de información utilizadas por los controles de acceso.
- vii. a información relevante de la configuración

Se utilizará siempre una arquitectura cliente/servidor de tres niveles: capa de base de datos, capa de aplicación y capa de presentación. Esto permitirá ubicar la capa de presentación en aquellas zonas que se identifiquen necesarias según el origen (confiable o no) de las conexiones del cliente, con el objeto de salvaguardar siempre las capas de aplicación y de base de datos.

Las reglas de control de acceso implementadas en la capa de aplicación y en la capa de presentación deben coincidir siempre.

Si existen datos de estado que deben ser guardados en la parte cliente, será necesario el uso de cifrado robusto y comprobaciones de integridad del lado del servidor para poder evaluar el estado de los datos.

Limitar el número de transacciones que se pueden realizar en un cierto período de tiempo.

Utilizar el “*referer*” de la cabecera HTTP sólo como un chequeo complementario. Nunca debe ser utilizado como chequeo de autorización, ya que es posible modificarlo.

Si se permiten sesiones autenticadas por un largo periodo de tiempo, se deberá revalidar periódicamente la autorización de las entidades autenticadas para asegurar que sus privilegios no han sido modificados. En caso de modificación, finalizar la sesión autenticada y forzar una nueva autenticación.

Se implementará una auditoría básica de cuentas que permita deshabilitar aquellas cuentas en desuso o sin actividad por un periodo de tiempo definido.

La aplicación debe permitir deshabilitar cuentas y terminar sesiones una vez que se finaliza la autorización (por ejemplo, durante el cambio de rol, etc.).

Las cuentas de servicio o las cuentas definidas para crear interfaces de entrada o de salida con otros sistemas externos deben tener el mínimo privilegio.

[RGS08] Gestión de errores y excepciones.

En caso de que la aplicación entre en estado de error o excepción, se deberá capturar dicho estado y salir del mismo de modo estable, liberando los recursos utilizados y sin dar posibilidad de acceso a los mismos.

No difundir información sensible en las respuestas de error, incluyendo detalles del sistema, identificadores de sesión o información de la cuenta, depuración (*debugging*) de memoria, etc.

Se deberán utilizar mensajes de error genéricos y utilizar páginas de error adaptadas, que serán acordados internamente durante la fase de desarrollo y recogidos en la documentación técnica de la aplicación, de tal manera que sólo sean entendibles por los equipos de desarrollo, soporte, operación y explotación.

Durante la fase de diseño y desarrollo se deberán identificar las posibles causas de error de la aplicación.

La lógica para la gestión de errores debe especificar que, en caso de error, los controles de seguridad no permitirán el acceso por defecto.

[RGS09] Gestión de registros (logs).

Todos los controles de registro (log) deberán estar implementados en sistemas confiables. Por tanto, la aplicación deberá poder comunicarse con sistemas externos estándar para el almacenamiento y tratamiento de los logs (por ejemplo, syslog).

La configuración del log para los controles de acceso debe contemplar recoger tanto los casos de éxito como de error.

Toda aplicación deberá tener un mecanismo de configuración de los registros de log que permita especificar el nivel del detalle que contemplarán estos: sólo errores, errores y advertencias, errores, advertencias e información, etc.).

Los registros de logs relativos a auditoría deberán permitir reconstruir por completo una sesión, transacción, etc. de la aplicación

Asegurar que los logs que incluyan información potencialmente peligrosa (como, por ejemplo, comandos del sistema operativo) no serán ejecutados en los interfaces o en el aplicativo de visualización y/o tratamiento de los logs.

Restricción de acceso a los logs: únicamente los usuarios autorizados podrán acceder a los logs, y exclusivamente con permiso de sólo lectura.

Utilizar una rutina centralizada para todas las operaciones de logging.

No guardar información sensible en logs, incluyendo detalles innecesarios del sistema, identificadores de sesión, contraseñas, etc.

Se registrarán en los logs:

- i. todos los errores en la validación de los datos de entrada.
- ii. todos los intentos de autenticación, en particular, los fallidos.
- iii. todos los errores en los controles de acceso.
- iv. todos los eventos de intento de evasión de controles, incluyendo cambios no esperados en el estado de la información.
- v. todos los intentos de conexión con tokens inválidos o expirados.
- vi. todas las excepciones del sistema.
- vii. todas las funciones administrativas, incluyendo los cambios en la configuración de seguridad.
- viii. todos los errores de conexión de TLS.
- ix. todos los errores de los módulos criptográficos.

[RGS10] Protección de los datos.

Proteger todos los almacenamientos temporales (cualquier que sea su naturaleza) de datos sensibles almacenados en el servidor de accesos no autorizados y datos que solamente puedan ser accedidos por usuarios específicos. Para ello, es necesario implementar en la aplicación, al menos:

- a) un modelo de perfiles y autorizaciones
- b) controles de accesos apropiados a los datos sensibles.

Eliminar de forma segura todos los archivos y memoria de trabajo temporal intermedios tan pronto como no sean necesarios.

Cifrar con algoritmos robustos toda la información altamente sensible almacenada, incluida la almacenada en el servidor, como son, por ejemplo, los datos para la verificación de la autenticación. Siempre se han de utilizar algoritmos de cifrado robustos.

Es necesario proteger el código fuente en el servidor, de forma que no pueda ser descargado por el usuario.

No permitir almacenar contraseñas, cadenas de conexión u otra información sensible en texto claro o de forma que no sea criptográficamente segura del lado del cliente. Esto incluye incluirla en formatos inseguros tales como, por ejemplo, MS Viewstate, Adobe Flash, código compilado, etc.

Revisar el código fuente de los sistemas productivos que se accesible por el usuario final para eliminar cualquier comentario que pueda revelar información sensible (usuarios, contraseñas, hostnames, IPs privadas, etc.).

Revisar los sistemas productivos para comprobar que no exponen información o documentación sensible o útil para un potencial atacante (ficheros temporales, de configuración, copias de seguridad, etc.).

Eliminar cualquier aplicación que no sea estrictamente necesaria (extensiones, módulos, etc.).

No incluir información sensible en los parámetros del método HTTP GET.

Deshabilitar las funcionalidades de autocompletar en todos aquellos formularios o campos que contengan o puedan contener información sensible, incluyendo la autenticación.

Deshabilitar el almacenamiento temporal del lado del cliente de páginas que contienen información sensible: por ejemplo, se debe utilizar "Cache-Control: no-store" conjuntamente con el control de cabecera HTTP "Pragma: no-cache", que es menos efectivo, pero mantiene la compatibilidad con HTTP/1.0.

La aplicación debe tener como funcionalidad la de permitir la eliminación de datos clasificados como sensibles cuando ya no son necesarios (por ejemplo: datos de carácter personal, datos financieros, etc.).

Siempre que sea posible, implementar la Política de Contenido Seguro (CSP) según marca el W3C en las cabeceras HTTP.

[RGS11] Seguridad en las comunicaciones.

Es necesario implementar cifrado en las comunicaciones para todas las transmisiones de datos o funciones sensibles, lo que incluye el acceso autenticado. Esto debería incluir TLS (TLS v1.1 o v1.2) para proteger la conexión, que se puede combinar con un cifrado de archivos sensibles en aquellas conexiones entre sistemas que no estén basadas en el protocolo HTTP.

Los certificados TLS deben de ser válidos y contener el nombre de dominio correcto, no deben estar caducados y deberán ser instalados con los certificados intermedios cuando sean necesarios.

Las conexiones TLS que fallen no deben transformarse en una conexión insegura.

Utilizar una única implementación estándar de TLS y configurarla correctamente.

Especificar la codificación de caracteres en todas las conexiones.

Cuando existan vínculos a sitios externos, filtrar los parámetros que contengan información sensible de los *referer* de las cabeceras HTTP.

[RGS12] Configuración de los sistemas.

Asegurar que los servidores, los *frameworks* y los componentes del sistema están ejecutando la última versión aprobada por la organización en el ámbito del proyecto de implantación.

Asegurar que los servidores, los *frameworks* y los componentes del sistema están actualizados con todos los parches y actualizaciones de seguridad liberados por el fabricante para las versiones aprobadas por la organización, validando previamente su impacto en la aplicación.

Deshabilitar los listados de directorio.

Restringir la ejecución del servidor web, los procesos y las cuentas de servicios al mínimo privilegio posible.

Eliminar todas las funcionalidades y archivos que no sean estrictamente necesarios.

Especialmente en los entornos productivos, eliminar cualquier código de test o prueba, y cualquier funcionalidad que no sea necesaria e imprescindible antes de la puesta en producción.

Prevenir revelar la estructura de directorios en el archivo “robots.txt” colocando directorios que estén disponibles para el índice público en un directorio raíz aislado y luego, “Deshabilitar” el directorio raíz en el archivo robots.txt en lugar de “Deshabilitar” cada directorio individual.

Definir cuáles de los métodos HTTP, GET o POST, va a soportar la aplicación, y si deben de ser manejados de forma diferente en las distintas páginas de la aplicación.

Deshabilitar extensiones del método HTTP innecesarias, como las extensiones WebDAV. Si una extensión del método HTTP que soporte gestión de archivos es realmente necesaria, utilice un mecanismo de autenticación robusto y bien comprobado.

Deshabilitar métodos HTTP potencialmente inseguros, como OPTIONS, TRACE, DELETE, PUT, etc.

Si el servidor web manejará HTTP 1.0 y HTTP 1.1, asegurarse de que ambos están configurados de manera similar o asegurarse de entender bien las diferencias que puedan existir (por ejemplo, en el manejo de métodos extendidos de HTTP (tokens)).

Eliminar toda información innecesaria de las cabeceras HTTP de respuesta, sobre todo las referidas al Sistema Operativo, versión del servidor web y *frameworks* de aplicación (*productive banners*). Si es necesaria una herramienta de estadísticas, es recomendable utilizar un sistema externo. Si es necesario que se ejecute internamente, será obligatorio proteger el acceso al mismo.

La configuración de seguridad de la aplicación debe de ser listada en un formato completo y legible para facilitar su auditoría.

Aislar los entornos de desarrollo de los entornos de calidad y éstos de los entornos de producción. Permitir el acceso a los primeros solamente a los grupos de desarrollo, pruebas y formación específicamente autorizados. Los entornos de desarrollo a menudo son configurados de forma menos segura que los entornos de producción y un potencial atacante puede utilizar estas diferencias para descubrir vulnerabilidades y cómo poder explotarlas en los entornos de producción.

[RGS13] Seguridad en la base de datos.

El acceso de la aplicación a la base de datos no se realizará nunca desde la capa cliente, siempre se realizará a través de la capa de aplicación.

La aplicación debe utilizar el mínimo nivel de privilegios cuando acceda a la base de datos. Si es posible, la aplicación deberá conectarse a la base de datos con credenciales diferentes para cada nivel o rol de confianza establecido en la aplicación (por ejemplo: usuarios con capacidad de modificación, usuarios de sólo lectura, invitados, administradores, etc.).

Es obligatorio utilizar credenciales seguras para el acceso de la aplicación a la base de datos.

Las cadenas de conexión a la base de datos no deben de estar incluidas en el código de la aplicación (*hard-coded*) y deben estar en un archivo de configuración separado que debería de estar cifrado siempre que sea posible.

Se priorizará el uso de consultas predefinidas fuertemente parametrizadas, manteniendo la consulta y los datos separados mediante el uso de marcadores de posición. La estructura de la consulta se definirá con los marcadores de posición, la instrucción SQL se enviará a la base de datos y se preparará y, a continuación, la declaración ya preparada se combinará con los valores de los parámetros. Esto evita que la consulta sea alterada, debido a que los valores de los parámetros se combinan con la sentencia ya compilada, no con una cadena SQL.

Será necesario validar las entradas y la codificación de las salidas, asegurándose de gestionar adecuadamente los metacaracteres. Si esto falla, la sentencia no deberá ejecutarse en la base de datos.

En los lenguajes de programación fuertemente tipados, será obligatorio que todas las variables tengan tipo de datos asociados. Para los lenguajes de programación no tipados, débilmente tipados o con tipado dinámico, se tendrán en cuenta las recomendaciones de

seguridad propias del lenguaje de programación específico y relativas a la declaración de variables.

Utilizar procedimientos almacenados para abstraer el acceso a los datos y eliminar los permisos de las tablas en la base de datos.

Se recomienda el uso de pools de conexión para hacer más eficiente el acceso a la BBDD, optimizando recursos, aumentando el rendimiento y eliminando conexiones innecesarias.

Eliminar o cambiar todas las contraseñas de las cuentas administrativas por defecto. Utilizar contraseñas fuertes, frases de varias palabras (*passphrases*) o implementar autenticación de múltiples factores.

Deshabilitar todas las funcionalidades innecesarias de la base de datos (por ejemplo: procedimientos almacenados innecesarios, servicios no utilizados, paquetes de utilidades, etc.). Instale sólo el conjunto mínimo de funcionalidades y opciones estrictamente necesarias para reducir superficie susceptible de ataque.

Eliminar el contenido innecesario incluido por el proveedor (por ejemplo: esquemas de ejemplo).

Deshabilitar todas las cuentas de usuarios que no son necesarias para la operativa del negocio.

[RGS15] Gestión de los ficheros.

Exigir autenticación antes de permitir la transferencia de un archivo al servidor.

Sólo se permitirá transferir al servidor únicamente los tipos de archivo (por ejemplo: pdf, doc, etc.) requeridos por la aplicación para la ejecución de los procesos definidos.

Validar los tipos de archivo transferidos verificando la estructura de los encabezados. La validación del tipo de archivo únicamente por la extensión del mismo no es suficiente.

No guardar los archivos transferidos en el mismo contexto que la aplicación web. Los archivos deben almacenarse en un filesystem o repositorio específico, controlado y aislado.

Evitar o restringir la transferencia de archivos que puedan ser interpretados por el servidor web (por ejemplo: asp, php, js, jsp, cgi, etc.).

Eliminar siempre los permisos de ejecución a los archivos transferidos.

En entornos UNIX o GNU/Linux, será obligatorio implementar una transferencia de archivos segura mediante el uso de discos lógicos y el uso de las rutas (*paths*) correspondientes o mediante la utilización de jaulas *chroot*.

Cuando sea necesario referenciar a un archivo existente en el servidor, será obligatorio, al menos:

- utilizar una lista blanca de nombres y extensiones válidas.
- validar el contenido del parámetro proporcionado contra dicha lista blanca
- si no se encuentran coincidencias, denegar la operación o utilizar la transferencia de un archivo inocuo predefinido.

No utilizar información provista por el usuario en ninguna operación dinámica o para la generación de redirecciones dinámicas. Si por algún motivo justificado se debe proveer la funcionalidad de redirección, ésta debe aceptar únicamente rutas relativas dentro de la URL previamente establecidos a través de una lista blanca.

No incluir en parámetros nombres de directorios o rutas de archivos, en su lugar utilizar índices que internamente se asocien a directorios o rutas predefinidas.

Nunca se enviarán rutas absolutas a la parte cliente.

Asegurarse de que los archivos y recursos de la aplicación sean de sólo lectura.

Es necesario comprobar siempre los archivos transferidos por los clientes en busca de virus y malware.

[RGS16] Gestión de la memoria.

Para la información proveniente del cliente, utilizar siempre controles en la entrada y en la salida de información.

Revisar dos veces que el tamaño de los buffers sean los requeridos y especificados.

Evitar el uso de funciones que permitan definir el número de bytes a copiar (como `strncpy()`), dado que, por ejemplo, si el tamaño del buffer de destino es igual al tamaño del buffer origen, el destino podría quedar sin el NULL-byte necesario del final.

Verifique los límites de los buffers si se llama a las funciones dentro de un bucle y asegúrese de no escribir fuera del espacio reservado (como `printf()`).

Truncar el largo de todas las cadenas de entrada a un tamaño razonable antes de pasarlos a una función de copia o concatenación.

Liberar explícitamente los recursos (por ejemplo: objetos de conexión, manejadores de archivos, etc.), no confíe en el *garbage collector*.

Utilizar *stacks* no ejecutables cuando sea posible (NX bit).

Evitar siempre el uso de funciones con vulnerabilidades conocidas (por ejemplo: `printf()`, `strcat()`, `strcpy()`, etc.).

Liberar correctamente la memoria asignada a la finalización cumplimiento de las funciones y en todos los puntos de salida.

[RGS17] Protección de datos de carácter personal.

Las aplicaciones que traten datos de carácter personal deberán contemplar una serie de controles adicionales obligados por normativa legal, y la aplicación de la legislación de protección de datos. De cara al cumplimiento legal el responsable de la aplicación deberá ponerse en contacto con el área legal correspondiente dentro de la Secretaría General Técnica (SGT), con el objeto de identificar el nivel de seguridad que de acuerdo con la normativa de protección de datos vigente y siempre según la tipología de datos que se

vayan a tratar a través de la aplicación. A tal efecto, el Responsable de la Aplicación deberá facilitar al área legal correspondiente dentro de la Secretaría General Técnica (SGT) el detalle de los datos que se puedan tratar a través de la aplicación, si van a existir campos de texto libre, catalogados, etc., así como las finalidades.

En consonancia con lo anterior, el Responsable de la Aplicación deberá recabar del área legal competente en materia de protección de datos las cláusulas a incluir en los documentos relacionados con el expediente de licitación.

[RGS18] Uso de criptografía.

Todas las funciones criptográficas de la aplicación deben ser implementadas en un sistema confiable (por ejemplo, el servidor).

Será necesario proteger las claves maestras de accesos no autorizados.

En caso de fallo o error, los módulos de criptografía deberán hacerlo de forma segura.

Todos los números aleatorios, nombres aleatorios, GUIDs, y frases aleatorias, deberán generarse utilizando módulos aprobados para su generación, es decir, dichos módulos deben cumplir con Common Criteria EAL 2+, FIPS 140-2 o con su estándar equivalente.

○ Gestión de certificados.

Pueden ser utilizados tanto por usuarios como por procesos o aplicaciones para proporcionar confidencialidad, integridad o no repudio entre las partes intervinientes.

Los certificados digitales deben ser gestionados a través de una política de uso, la cual debe contemplar todo el ciclo de vida del certificado: solicitud, instalación, salvaguarda, validación, transmisión, uso y expiración o revocación.

○ Firmado de aplicaciones.

Dada la gran cantidad existente de código malicioso y el aumento del riesgo de infección de los sistemas a la hora de distribuir e instalar aplicaciones, con objeto de mitigar este riesgo, se debe garantizar el origen y la integridad del software a instalar, de manera que se asegure que no sea posible hacer modificaciones posteriores no autorizadas sobre las aplicaciones ya distribuidas para su despliegue o instalación.

Para ello, se utiliza la firma de aplicaciones, que, básicamente, consiste en utilizar técnicas criptográficas para la realización de un resumen (hash) firmado de fuentes o ficheros objeto de las versiones completas de código. Se deberán utilizar funciones hash criptográficamente robustas (resistentes a colisiones).

[RGS19] Uso de una metodología de desarrollo segura.

Actualmente, el desarrollo de aplicaciones de manera *ad hoc* no es lo suficiente estructurado para producir aplicaciones seguras. Si se pretenden desarrollar aplicaciones consistentes desde el punto de vista de la seguridad, se necesita de una metodología de desarrollo que soporte dicho objetivo e integre la seguridad en todas las fases del ciclo de vida del desarrollo.

Se deberá por tanto adoptar y seguir una Metodología de Desarrollo Seguro para garantizar que los desarrollos para Canal de Isabel II cumplan unos requisitos mínimos de seguridad. La metodología a utilizar ha de incluir mecanismos robustos de aceptación de diseño, testeo y documentación e incluir la introducción de controles de seguridad.

Para ello, es conveniente consensuar, adoptar y usar frameworks de desarrollo basados en las mejores prácticas aceptadas por la industria y que incorporen funciones de seguridad en la validación de los datos (entrada, procesamiento y salida), el acceso a las bases de datos, la gestión de sesiones, el uso de librerías de funciones de seguridad (manejo de credenciales, cifrado, ofuscación de código, depuración de caracteres, etc.), el control de errores, la gestión de logs, etc.

Asimismo, se recomienda utilizar herramientas de calidad de código que se integren con dichos frameworks de desarrollo para complementarlos a través de sus métricas: arquitectura y diseño, código duplicado, código muerto (variables, parámetros o métodos sin usar), complejidad de métodos, reglas de codificación según las convenciones y buenas prácticas del estándar del lenguaje de programación utilizado, con el objeto de asegurar la usabilidad, portabilidad, mantenibilidad, eficacia, confiabilidad, mutabilidad, la capacidad de prueba, el análisis de dependencias, cobertura de código, la generación de test unitarios, el uso razonable de los comentarios, etc.

Es necesario por tanto promover y garantizar la formación del equipo técnico de desarrollo (programadores) en los aspectos de desarrollo seguro y calidad del software.

[RGS20] Auditoría de seguridad del código fuente.

Se llevará a cabo desde una perspectiva de caja blanca (revisión tanto estática como dinámica) como de caja negra (técnicas de provisión de datos incorrectos, inesperados y/o aleatorios en los parámetros de entrada o *fuzzing*).

Caja Blanca.

El objetivo de la revisión estática es encontrar errores durante el proceso de desarrollo y evitar así que se conviertan en fallos públicos (por ejemplo, la no eliminación de comentarios en el código fuente en aplicaciones desarrolladas en código interpretado antes de su puesta en producción).

El objetivo de la revisión dinámica es revisar el comportamiento del código durante su ejecución, identificando, por ejemplo, dependencias (polimorfismo) o falsos negativos, no detectados durante la fase de revisión estática.

Caja Negra.

También se abordará el uso de técnicas de *fuzzing* para auditar el comportamiento de la aplicación desarrollada y para localizar puntos de inestabilidad en el software que puedan ser aprovechados para ejecutar código.

En el caso de que se realicen revisiones de la calidad del código, éstas se realizarán juntamente con la Dirección de Seguridad para identificar y en su caso activar las comprobaciones de seguridad que se incluyan, de serie o vía conectores externos (*plug-in*), en las herramientas utilizadas para la revisión, con el objeto de obtener métricas que permitan completar los requisitos de seguridad existentes o identificar otros adicionales que puedan formar parte del catálogo.

La revisión del código fuente precisa del conocimiento del lenguaje o lenguajes de programación utilizados, así como de los aspectos básicos referentes a la visión del software. Es importante conocer la finalidad del producto, sus requisitos, el tipo de datos que se van a tratar, los interfaces, el perfil de los usuarios que vayan a utilizar la aplicación, etc. La documentación aportada por el programador con respecto al código fuente a revisar es otro factor básico para un correcto proceso de revisión.

La auditoría de seguridad del código fuente tiene también la finalidad de comprobar que las aplicaciones han sido implementadas siguiendo las medidas de seguridad propuestas en este Procedimiento.

Recomendaciones de seguridad generales.

Para la realización de tareas o funciones habituales, reutilizar código probado y verificado, en lugar de crear códigos específicos.

Utilizar las APIs previstas para el acceso a funciones específicas del Sistema Operativo. No se permitirá que la aplicación ejecute comandos directamente en el Sistema Operativo, y menos aún mediante la invocación de una consola de comandos o *shell*.

Se deberán utilizar funciones resumen (*hash*, *checksum*) criptográficamente robustas para verificar la integridad del código interpretado, bibliotecas, ejecutables y archivos de configuración previamente a su utilización.

Utilizar bloqueos (*locks*) para evitar múltiples accesos simultáneos a recursos o mecanismos de sincronización (por ejemplo: semáforos) y así evitar vulnerabilidades de tipo estado de carrera o condiciones de carrera (*race conditions*).

Es necesario proteger de accesos concurrentes inadecuados las variables y recursos compartidos.

Explícitamente será necesario inicializar todas las variables y mecanismos de almacenamiento de información (por ejemplo: buffers), durante su declaración o antes de usarlos por primera vez.

Explícitamente será necesario liberar recursos una vez dejen de ser necesarios.

Las aplicaciones que requieran privilegios especiales deberán elevarlos sólo cuando sea necesario y devolverlos (bajar privilegios) lo antes posible. Los privilegios especiales se mantendrán únicamente cuando sea estrictamente necesario.

Evitar los errores de cálculo comprendiendo la forma en que el lenguaje de programación maneja las operaciones matemáticas y las representaciones numéricas. Será necesario prestar especial atención a las discrepancias en la cantidad de bytes utilizados para la representación, la precisión, diferencias entre valores con y sin signo, truncamiento, conversiones y casting entre tipos de variables, los cálculos “no-numéricos” y cómo el lenguaje maneja los números demasiado grandes o demasiado pequeños para su representación.

No se utilizarán datos provistos por el usuario para ninguna función dinámica.

Bajo ningún concepto se permitirá que los usuarios introduzcan o modifiquen código de la aplicación.

Se revisarán obligatoriamente todas las aplicaciones secundarias, código provisto por terceros y bibliotecas para determinar la necesidad de su utilización y validar su funcionamiento seguro, ya que estos componentes pueden introducir nuevas vulnerabilidades.

Será necesario implementar mecanismos seguros para las actualizaciones:

- Si la aplicación realiza actualizaciones automáticas, utilizar firmas criptográficas para verificar la integridad del código.
- Asegurarse que el cliente que descarga la aplicación verifique dichas firmas.
- Utilizar canales cifrados para las transferencias de código desde el servidor de actualización.

Dentro del proyecto de desarrollo, es necesaria la identificación e integración en la aplicación resultante de mecanismos simples de protección y seguridad, que pasan inadvertidos al usuario final y tienen como objetivo principal el proteger a la aplicación de los usuarios autorizados y, por añadidura, facilitar su uso y conocimiento, así como su aceptación. Por ejemplo, textos, iconos e imágenes auto explicativos, ayudas contextuales, ejemplos gráficos y casos de uso, etc.

3.1.2.- Diseño de los Controles de Seguridad.

Para ayudar al cumplimiento de estos requisitos generales de seguridad en la fase de diseño, se proporcionarán una serie de Instrucciones Técnicas de cara a facilitar el desarrollo de los mecanismos necesarios para el cumplimiento de los requisitos en las diferentes plataformas.

Una vez identificados los controles de seguridad, se contemplarán en el diseño de arquitectura, actualizándose por tanto el documento de arquitectura de la aplicación y obteniéndose un nuevo documento denominado “**Arquitectura de Seguridad de la Aplicación**”. En dicho documento se recogerán los controles de seguridad, indicando dónde se aplican y los mecanismos que se van a utilizar e implementar para cumplir con los requisitos de seguridad establecidos.

3.1.3.Actividades de esta fase.

- Establecimiento de los requisitos de seguridad obtenidos de la caracterización del sistema/aplicación.
- Entrega del documento de **Arquitectura de la Aplicación** a la Dirección de Seguridad para su revisión.
- Identificación de los controles de seguridad.
- Entrega del documento de **Arquitectura de Seguridad de la Aplicación** a la Dirección de Seguridad para su revisión

3.2.- Fase de Construcción.

3.2.1.- Adecuación a los requisitos de seguridad.

Durante la fase de construcción del sistema, se procederá a la adecuación del sistema a los requisitos generales de seguridad recogidos en la fase de diseño, teniendo en cuenta las diferentes plataformas existentes.

3.2.2.- Requisitos de seguridad propios de la fase de construcción.

[RG21] Gestión de entornos.

Se deberá garantizar la separación física de los diferentes entornos empleados en Canal de Isabel II: desarrollo, calidad y producción.

El paso entre entornos se realizará de forma controlada y mediante una adecuada gestión de cambios. Para su aprobación, deberá garantizar que se dispone de un procedimiento de marcha atrás a utilizar en caso de que el cambio produzca resultados no deseados (errores funcionales, interrupción del servicio, subida incompleta, errores reiterados en el/los proceso(s) de subida o durante el/los proceso(s) de actualización, etc.).

Implementar un sistema de control de versiones y cambios para la gestión y registro de los cambios entre los distintos entornos (desarrollo, calidad y producción), tanto para el código fuente como para las versiones de software, la configuración de la aplicación, etc.

Si el sistema realiza tratamiento de datos de carácter personal (de conformidad con el RGPD y la LOPDGDD) y se requiere un volcado de los mismos desde el entorno de producción a otros entornos no productivos, se empleará un mecanismo que garantice la disociación de dichos datos. En caso de que no exista dicho mecanismo, las medidas de seguridad de los entornos no productivos en los que se han volcado los datos serán, al menos, las mismas que las contempladas para el entorno productivo, siempre y cuando dichas medidas no sean superiores a las establecidas en la legislación vigente relativa a protección de datos de carácter personal.

[RG22] Gestión de redes de comunicaciones.

Existirá una separación lógica de las redes de comunicación de los diferentes entornos para contribuir a garantizar la separación de los mismos.

Las redes de comunicaciones serán gestionadas de forma que las reglas habilitadas para las comunicaciones entre los distintos sistemas pasen por un proceso procedimentado de solicitud, valoración, prueba y aprobación.

[RG23] Gestión del código fuente.

El código fuente de las aplicaciones será gestionado mediante una herramienta de gestión de versiones de forma que se garantice el correcto etiquetado, almacenamiento y control de versiones.

Se deberá mantener un registro de cambios o control de versiones con todos los cambios efectuados sobre el software así como un adecuado control de acceso y perfilado de usuarios de la herramienta de gestión de versiones para impedir las modificaciones no autorizadas y garantizar la correcta administración de la herramienta.

[RG24] Gestión de la configuración.

Se llevará a cabo un proceso de gestión de la configuración de la aplicación en el que se desarrollarán, al menos, las siguientes actividades:

- Identificación de los elementos de configuración de la aplicación para cada entorno (ficheros .properties, etc.).
- Control de cambios sobre los elementos de configuración y la línea base.
- Procedimiento de aprobación de solicitudes de cambio.
- Mantenimiento actualizado del registro del estado de los elementos de configuración.

3.2.3.- Actividades de esta fase,

- ✓ Construcción de los controles de seguridad de la aplicación.

3.3.- Fase de Finalización.

3.3.1.- Auditoría de cumplimiento de los requisitos de seguridad.

Una vez construido el sistema, la Dirección de Seguridad realizará una auditoría para verificar el cumplimiento de los requisitos de seguridad. A través de las tablas de medición de los controles, se verificará la correcta implantación de dichos controles identificados en las Instrucciones Técnicas correspondientes a la plataforma, y que respondan a los

requisitos de seguridad planteados en la fase de diseño. Esta auditoría se realizará sobre el entorno candidato a su puesta en producción. En caso de que el entorno candidato sufra alguna modificación antes de su puesta en producción, deberá ser auditado de nuevo.

El resultado de dicha auditoría se reflejará en el “Informe de Auditoría de Seguridad”. En dicho informe se describirán las verificaciones realizadas y el resultado obtenido para cada una de ellas.

3.3.3.- Auditoría de seguridad final.

Una vez que se haya cumplido la planificación propuesta para la resolución de los no cumplimientos identificados como “a resolver” por el dueño de los datos / responsable de la aplicación, se volverá a realizar la auditoría de seguridad completa, donde se comprobará si se han subsanado las deficiencias de seguridad detectadas y que no se han introducido nuevas en el proceso de resolución.

3.3.4.- Revisión de la valoración y clasificación de la aplicación.

Después de la última auditoría de seguridad, independientemente de sus resultados, el Dueño de los Datos / Responsable de la Aplicación podrá revisar la valoración ACIDA de los activos de información que se gestionarán en la aplicación.

Se procederá a una revisión final de la adecuación de los controles identificados en las fases anteriores contra los requisitos impuestos por la valoración ACIDA de los activos.

Posteriormente, se procederá a la clasificación de la propia aplicación.

Para dicha revisión de la valoración ACIDA y para la clasificación de la aplicación será de aplicación el Procedimiento General de Clasificación y Tratamiento Seguro de la Información PGS-001.

3.3.5.- Actividades de esta fase.

- ✓ Diseño del Plan de Auditoría.
- ✓ Ejecución de las pruebas de auditoría.
- ✓ Documentación del resultado de las pruebas de auditoría.
- ✓ Planificación de la resolución de las No Conformidades.
- ✓ Resolución de las No Conformidades
- ✓ Auditoría final.
- ✓ Valoración y clasificación final del sistema.
- ✓ Revisión opcional de valoración final de los activos de información
- ✓ Revisión de la adecuación de los controles identificados en las fases anteriores contra los requisitos impuestos por la valoración ACIDA de los activos.
- ✓ Clasificación de la aplicación.

De todos los requisitos generales de seguridad aquí expuestos se derivarán recomendaciones de seguridad específicas para cada plataforma tecnológica, así como guías y documentos de desarrollo seguro complementarios, que quedarán recogidas en las instrucciones técnicas que correspondan o en documentos o guías de seguridad.

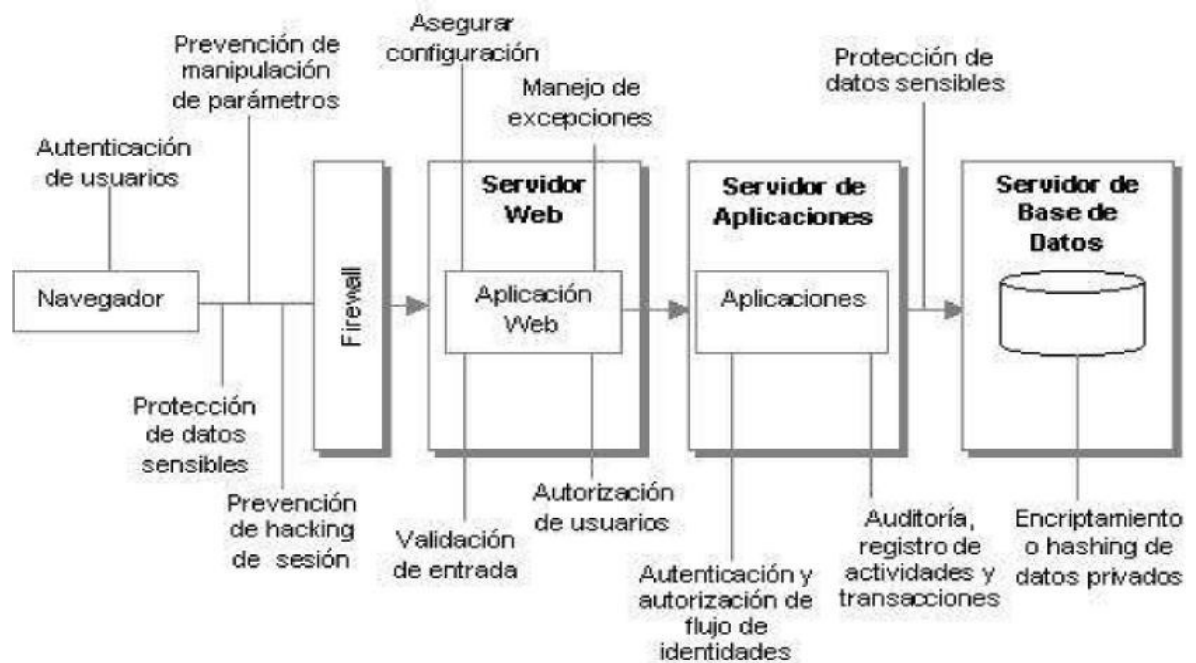
CONSIDERACIONES DE SEGURIDAD PARA EL DISEÑO Y CONSTRUCCIÓN DE APLICACIONES WEB:

1. INTRODUCCION

Las aplicaciones Web, entendiendo por aplicaciones Web todas aquellas que por la naturaleza de su uso requieran acceso desde redes públicas de comunicación, 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.

2. CONSIDERACIONES DE SEGURIDAD PARA EL DISEÑO DE UNA APLICACIÓN.

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.

3. CONSIDERACIONES DE SEGURIDAD Y VULNERABILIDADES ASOCIADAS

Consideración de seguridad	Vulnerabilidades asociadas
	<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
Validación de datos de entrada	<ul style="list-style-type: none"> 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 interfaces de administración, alteración de datos de configuración, acceso no autorizado a cuentas de usuario y perfiles de cuentas de usuarios
Datos sensibles	Acceso a información confidencial. Pérdida de integridad de los datos.
Administración de sesiones	Captura de identificadores de sesión. Tiempo excesivo de expiración de la sesión.
Cifrado	Acceso a datos confidenciales y/o credenciales de cuentas de usuario.
Manipulación de parámetros	Ejecución de comandos, elevación de privilegios, denegación de servicios (DoS y DDoS), etc.
Gestión de excepciones	Denegación de servicios y acceso a información específica de los sistemas base (sistema operativo, servidor web y de aplicaciones, base de datos, etc.).
Auditoría y registro de actividades	Fallos en el registro de pruebas de intrusión, acciones realizadas por el intruso y dificultades para diagnosticar problemas

1. 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. (en adelante, Canal de Isabel II) 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. WASC (Web Application Security Consortium).

Para Código Fuente:

1. OWASP (Open Web Application Security Project).
2. ISSAF (Information System Security Assessment Framework).
3. CVSS v2 (Common Vulnerability Scoring System).

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

Por lo tanto, todo adjudicatario que desarrolle una aplicación Web para Canal de Isabel II 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.

2. 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 la misma.

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.

ANEXO 5. ESPECIFICACIÓN ENTORNOS TECNOLÓGICOS PARA NUEVOS DESARROLLOS.

1. CONTEXTO

Canal de Isabel II, pretende estandarizar la arquitectura de sus aplicaciones, así como los procesos de control de la calidad de software a exigir a los contratistas que realizan desarrollos de sistemas de información. El objetivo de este anexo es describir la infraestructura que dispone Canal de Isabel II así como los procesos, herramientas, librerías, normativa y convenciones que deben seguir los contratistas durante la prestación de sus servicios.

Las siguientes convenciones que se van a describir, se aplicarán solo en el caso de que se haga un desarrollo externo al producto y las tecnologías que se usen permitan aplicar la tecnología y arquitectura propuesta.

2. OBJETIVOS DEL PROYECTO/ÁREA FUNCIONAL

Los objetivos que se pretenden son:

- Dar un marco homogéneo al personal técnico de Canal de Isabel II.
- Facilitar el desarrollo de aplicaciones mediante servicios comunes ya implementados: seguridad, notificaciones, etc.
- Realizar el control de los desarrollos realizados y que cumplen con la calidad requerida.
- Estandarizar procedimientos de trabajo.

3. FASES DEL PROYECTO/ÁREA FUNCIONAL Y ENTREGABLES

La metodología y procedimientos de trabajo deben cumplir con los estándares PMI de Gestión de Proyectos.

Dentro de la primera fase del proyecto se fijará el entorno de desarrollo del proyecto y la integración con el entorno de QA de Canal de Isabel II así como la replicación de repositorios de código, si hubiera que hacerla.

Será responsabilidad de contratista el realizar dichas tareas con la colaboración de los técnicos de Canal de Isabel II.

4. HITOS CLAVE

Integración de entornos de desarrollo, repositorios y entorno QA de Canal de Isabel II o uso por parte del contratista de los que dispone Canal de Isabel II.

Entrega de procesos de integración continua desde las primeras tareas de diseño y arquitectura de las aplicaciones.

5. FACTORES CRÍTICOS DE ÉXITO

Es básico para la consecución del proyecto contar activamente con el apoyo del contratista para dicha integración del entorno de desarrollo, así como la experiencia del contratista en entornos de aseguramiento de la calidad de software basados en procesos de integración continua, calidad de software y gestión de la configuración. Es importante el conocimiento previo del contratista de las tecnologías que utiliza Canal de Isabel II para dichos procesos, las cuales son Open Source en su mayoría.

6. RESTRICCIONES

Entorno de infraestructura Canal de Isabel II

- VMWare
- Cacti
- Nagios

Entorno de desarrollo Canal de Isabel II

- Subversion
- IDE Eclipse o derivativo (STS)
- Maven
- Sun JDK
- .Net Framework

Entorno QA Canal de Isabel II

- Hudson/Jenkins
- Apache Archiva / Nexus
- Sonar

7. DETALLE DE LOS REQUISITOS

Requisitos Generales

[RG001] Decisiones de Diseño.

Se documentarán las decisiones de diseño para cada componente desarrollado y/o utilizado.

[RG002] Flexibilidad, Reutilización y Reuso.

Primará la simplicidad y flexibilidad en el diseño. En general cualquier servicio disponible que cumpla los requisitos será utilizado en lugar de realizar desarrollo a medida. Primará así mismo la extensión del código de los servicios y su contribución a la comunidad, en lugar del desarrollo a medida.

[RG003] Rendimiento

Las aplicaciones deberán tener en cuenta la topología de red Canal de Isabel II debido al diferente ancho de banda de los enlaces.

[RG004] Escalabilidad

Las aplicaciones desarrolladas se diseñarán de forma que sean escalables tanto horizontalmente como verticalmente.

El adjudicatario deberá plantear escenarios de incremento de capacidad de la plataforma, según los parámetros más relevantes del sistema (número de usuarios concurrentes, número de transacciones, volumen de datos: número de documentos, etc), de forma que sirva de base para redimensionar la infraestructura en caso de incremento de dichos parámetros.

[RG005] Dimensionamiento

La aplicación tendrá en cuenta las magnitudes siguientes (incluir las que correspondan)

Las referidas en el apartado 4.10

- N° de operaciones por unidad de tiempo
- N° de expedientes por unidad de tiempo
- N° de documentos

[RG006] Disponibilidad, tolerancia a fallos y balanceo de carga

Las aplicaciones se diseñarán teniendo en cuenta que el periodo de operación es 24x7 y la disponibilidad del servicio debe ser del 99,9%

Las aplicaciones se diseñarán para que sus diferentes componentes soporten balanceo de carga y tolerancia a fallos.

Se debe hacer transparentes los fallos de los componentes de las mismas evitando perder la sesión de usuario.

Se contemplarán diferentes mecanismos de balanceo de carga: pesos, turnos (Round Robin), etc. Los métodos de balanceo de carga tendrán en cuenta las sesiones establecidas del usuario y las consideraciones para hacer un balanceo de carga efectivo (replicación de sesiones de usuario, compartición de sesión, etc).

[RG007] RGPD, LOPD y GDD Y ESQUEMA NACIONAL DE SEGURIDAD

El contratista deberá ejecutar el contrato y los desarrollos solicitados cumpliendo con el principio de privacidad desde el diseño y por defecto, y en cualquier caso, los desarrollos objeto del contrato deberán ofrecer garantías suficientes en cuanto a la aplicación de medidas técnicas y organizativas apropiadas, como el cifrado de los datos de carácter personal, auditoría de registro de actividades y trazabilidad, gestión de perfiles (sin tratamiento de datos de usuario), autenticación, complejidad de contraseña, etc., teniendo en cuenta la tipología de datos que se tratarán, de manera que el tratamiento sea conforme con los requisitos del RGPD y LOPD y GDD, y resto de normativa que pudiera aplicar como pudiera ser el Real Decreto 1112/2018, de 7 de septiembre, sobre accesibilidad de los sitios web y aplicaciones para dispositivos móviles del sector público, garantizando en todo momento la protección de los derechos del interesado. El contratista ofrecerá a Canal de Isabel II un análisis de riesgos de protección de datos con relación a los desarrollos a realizar, indicando las recomendaciones que en su caso considera debe implementarse para que los desarrollos cumplan con el principio de privacidad por desde el diseño y por defecto, así como el principio de responsabilidad proactiva.

Los entornos, sistemas, aplicaciones, etc., de Canal de Isabel II cumplirán los aspectos de RGPD y LOPD y GDD relativos a protección de datos. La prestación de los servicios así como las soluciones tecnológicas desarrolladas deberán ser conformes con lo dispuesto en el Esquema Nacional de Seguridad y Declaraciones o Certificaciones de Conformidad, según lo señalado en la Resolución de 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad o bien cualquiera que pudiera modificar, completa y/o sustituir la anterior.

Requisitos de Infraestructura

[RI001] Virtualización.

Se harán plantillas virtualizadas de los servidores y/o componentes de los que Canal de Isabel II no disponga actualmente. Dichas plantillas deben haber sido construidas siguiendo los pasos de instalación y configuración del componente y deberán mantenerse actualizados tanto la documentación como la plantilla virtualizada. El producto de virtualización que usa Canal de Isabel II está indicado arriba.

[RI002] Tipos de entorno y generación

Se contemplarán al menos 3 tipos de entorno: desarrollo, preproducción y producción. Los entornos estarán en redes lógicas separadas e incluso en el mismo entorno los servidores de datos podrían estar en red lógica diferente según criterio de Canal de Isabel II. Deberán documentarse los servicios expuestos y consumidos por la aplicación.

El entorno de desarrollo puede ser diferente en recursos de los entornos de preproducción y producción. Cuando dichas diferencias influyan en el desarrollo de la aplicación, por ejemplo, en un cluster de aplicación J2EE, deberá indicarse claramente en la documentación.

El adjudicatario deberá determinar e implantar los procedimientos para construir un entorno a partir de otro. Dichos procedimientos se automatizarán.

[RI003] Monitorización

Los componentes de infraestructura se integrarán en los sistemas de monitorización de

Canal de Isabel II. Se indicará para cada servidor y/o componente cómo realizar dicha monitorización, así como los parámetros y rangos de valores operacionales a fin de detectar las posibles incidencias en el funcionamiento de los mismos.

Deberán implementarse todos los monitores necesarios (disponibilidad y rendimiento), para incluir el sistema y sus componentes en la consola de monitorización de Canal de Isabel II.

Se adjuntará un Excel con la información de comunicación entre el cliente y los servidores que formen parte de la solución indicando puertos y protocolos.

IRI004 Middleware de Integración

Se ofertarán las tecnologías para realizar integraciones avanzadas o tratamiento avanzado de señales

IRI005 Disponibilidad de entornos

Los entornos de desarrollo e integración tendrán una disponibilidad limitada conforme a entornos no productivos. Canal de Isabel II se compromete a ofrecer una disponibilidad en estos entornos del 95%, excluyendo aquellas paradas programadas. Las paradas programadas se realizarán en la ventana de 8:00 a 20:00 horas, buscando minimizar el impacto en los equipos de desarrollo, pero nunca fuera de estos horarios al no ser sistemas productivos.

La caída del entorno de desarrollo no será óbice para la interrupción del proceso de desarrollo ni la justificación de retrasos en el mismo.

Requisitos de Arquitectura

IRA001 Arquitectura de aplicación.

Las aplicaciones se construirán en capas: presentación, negocio, persistencia, interfaces, procesos, etc. Existirán capas transversales a toda la aplicación como son la seguridad, monitorización, rendimiento, logs y trazas. No todas las capas tienen que estar representadas en cada una de las aplicaciones.. Los contextos que se usen en la aplicación estarán diferenciados para las capas de seguridad, interfases, persistencia, negocio, etc.

IRA002 Capa de presentación

El GUI de las aplicaciones seguirá el patrón de Diseño MVC o variaciones del mismo. Deberá justificarse la decisión de utilizar cliente pesado y recibir aprobación escrita por parte de Canal de Isabel II.

EL GUI de las aplicaciones será internacionalizable así mismo permitirá previsualización de las impresiones via PDF y previsualización/exportación de datos via Excel.

Canal de Isabel II requerirá al contratista el diseño del mismo con un nivel de Accesibilidad que dé cumplimiento al Real Decreto 1112/2018, de 7 de septiembre, sobre accesibilidad de los sitios web y aplicaciones para dispositivos móviles del sector público.

.

IRA003 Capa de negocio

Los servicios internos que ofrezca la aplicación se codificarán mediante un interfaz y una o varias implementaciones. La codificación de la lógica de negocio se orientará a clases simples (POJOs).

[RA004] Capa de persistencia

La persistencia del modelo de datos las aplicaciones se realizará mediante DAO's , se entiende por DAO un interfaz que contiene los métodos necesarios para realizar las operaciones, como por ejemplo CRUD sobre el modelo de la aplicación. La implementación de dichos DAO's se realizará siguiendo el paradigma ORM u otro. Será posible cambiar la implementación de los DAO's para utilizar diferentes paradigmas de persistencia (Hibernate, JPA, JDBC, Spring Data, etc). Se utilizará un mecanismo de inyección de dependencias para enlazar diferentes implementaciones de los DAO's. Se utilizarán excepciones de acceso a datos que no dependan del mecanismo utilizado.

El acceso a fuentes de datos se hará siempre mediante pool de conexiones configurables. Los pool de conexiones se definirán en el servidor de aplicaciones para aprovechar las capacidades de monitorización y alarmas del mismo. Caso de que la aplicación defina el pool será responsabilidad del contratista la integración con los sistemas de monitorización de Canal de Isabel II, Nagios, Cacti y Dynatrace. Se automatizarán todas las operaciones de manipulación y creación del modelo de las aplicaciones mediante scripts sujetos igualmente a procesos de integración continua.

[RA005] Capa de interfaces

Las aplicaciones deberán poder exponer y consumir servicios mediante diferentes protocolos entre los que destacamos los siguientes: RMI, Mensajería,, Web Services REST y SOAP.

Se implementarán ejemplos en Java y .Net de los servicios que exponga la aplicación.

[RA006] Capa de seguridad

Se recomienda usar Spring Security en aplicaciones Java cuando sea posible, definiéndose en el descriptor el modelo de seguridad de la aplicación.

En aplicaciones no Java se utilizará el Servicio Central de Autenticación de Canal de Isabel II basado en CAS Jasig.

El uso de otro enfoque debe estar aprobado de forma escrita por parte del responsable de Canal de Isabel II.

Se programarán pruebas unitarias de seguridad.

[RA007] Capa de monitorización

Las aplicaciones se integrarán en los sistemas de monitorización de Canal de Isabel II. Se crearán los monitores que Canal de Isabel II estime adecuado y que testeen tanto el correcto funcionamiento de los componentes individuales como el de las funcionalidades de las aplicaciones. Se construirán también monitores funcionales que validarán el correcto funcionamiento de los puntos más críticos de las aplicaciones

Se crearán monitores de ayuda a la hora de realizar tareas de explotación de los sistemas, por ejemplo arranque y parada.

Las aplicaciones y/o sistemas exportaran mediante SNMP y/o JMX las métricas y parámetros de configuración de los mismos, así como los contadores sobre las métricas definidas como escalables.

[RA008] Capa de rendimiento

Las aplicaciones construidas exportarán métricas de rendimiento.

Deberán proveer como mínimo las siguientes métricas:

Consumo de CPU, memoria, red, número de procesos, consumo de acceso a discos, carga, etc

Tiempos de respuesta máximo, mínimo, medio de sus operaciones.

Tamaño actual, máximo y mínimo de las diferentes agrupaciones de recursos: conexiones, hebras, heap, etc

Valor actual, máximo, mínimo y medio de número de sesiones de usuario, lista de usuarios con sesión, número de sesiones por usuario, número de transacciones totales y por usuario del componente, número de errores del componente.

Cuando el servidor de la aplicación no provea estas métricas será responsabilidad de la aplicación proveer estos detalles.

La activación de esta capa debe ser configurable en “caliente”.

[RA009] Capa de logs y trazas

El sistema de logs será parametrizable en cuanto a formato del log, destino del log (fichero, BD, syslog, otros), política de rotación, tamaño, archivado y severidad a mostrar.

Deberá incluir al menos la fecha, y hora del log, usuario, nivel de severidad y mensaje. No se mostrarán contraseñas sin cifrar.

Las aplicaciones permitirán la modificación en caliente (sin reinicio de la aplicación) de los parámetros de configuración de logs y trazas.

Los mensajes de error deberán ser internacionalizables.

El sistema permitirá identificar las transacciones que realiza el usuario a través de todos sus componentes e interfases de las aplicaciones. Se deberá identificar fácilmente cual es el componente que detecta y/o genera el fallo y como proceder para la resolución de cada uno de los mismos.

Se utilizará un Framework reconocido de logs y trazas. Se deberá justificar una implementación propietaria con aceptación de Canal de Isabel II por escrito.

Se utilizarán mecanismos de AOP para habilitar, en cliente, trazas en capas de la aplicación con volcado de parámetros de los métodos.

Requisitos de Integración Continua

[RS001] Integración en entorno de Integración Continua de Canal de Isabel II.

Las aplicaciones a desarrollar se integrarán en el entorno de integración continua de Canal de Isabel II el cual utiliza Maven, Subversion, Hudson/Jenkins, Archiva / Nexus y Sonar.

Procesos repetibles

[RS002] Proceso de construcción de aplicaciones java.

Las aplicaciones java utilizarán Maven para construir los desplegables correspondientes. La sentencia mvn package construirá el conjunto de aplicaciones a entregar. El proceso de construcción tendrá en cuenta las diferentes propiedades de configuración de los diferentes entornos de building.

En general se realizarán un único proyecto maven con los módulos necesarios.

En caso de tener que ampliar funcionalidad de una aplicación existente (Open Source) se utilizará el método Maven war Overlay para personalización y cambios de comportamiento

[RS003] Proceso de generación de entorno de desarrollo (IDE)

Las aplicaciones utilizarán Maven para construir el proyecto que se abrirá desde el IDE. Configurando todas las dependencias de librerías, código fuente, etc

La sentencia mvn eclipse:eclipse creará en proyecto para ser abierto en el IDE eclipse.

[RS004] Proceso de lanzamiento de pruebas unitarias

Las aplicaciones utilizarán Maven para lanzar las pruebas unitarias: funcionalidad, seguridad, etc

La sentencia mvn test realizará el lanzamiento de dichas pruebas.

[RS005] Proceso de lanzamiento de pruebas de integración

Las aplicaciones utilizarán Maven para lanzar las pruebas de integración: funcionalidad, seguridad, etc

La sentencia mvn integration-test realizará el lanzamiento de dichas pruebas.

[RS006] Proceso de release de las aplicaciones

Las aplicaciones utilizarán Maven para realizar un release de las aplicaciones. Este proceso deberá integrarse con el repositorio de código utilizado en Canal de Isabel II.

Requisitos de Calidad software

[RQA001] Estilo de programación y nomenclatura de paquetes

El estilo de programación a utilizar será el estándar de Java, <http://www.oracle.com/technetwork/java/codeconvtoc-136057.html>

Los paquetes Java seguirán la siguiente nomenclatura

es.cyii.<appName>.[<componentName>].[<appLayer>]

donde:

appName es el nombre de la aplicación

componentName es el nombre de un componente o módulo de la aplicación

appLayer es una capa de la aplicación

[RQA002] Cobertura de código

La cobertura de las pruebas unitarias será superior al 50% del código a nivel de proyecto maven.

[RQA003] Calidad de código.

No deberán existir avisos de calidad en la aplicación en el cumplimiento de reglas

No deberán existir violaciones de duplicados en la aplicación

No deberán existir pruebas unitarias no satisfactorias. El tiempo de ejecución de las mismas estará por debajo de 10 minutos

Las métricas que utiliza Canal de Isabel II pueden consultarse en la instancia sonar de Canal de Isabel II

Requisitos de Gobierno

[RGB001] Descripción de servicios.

Se documentarán los servicios expuestos de forma remota por las aplicaciones de acuerdo a la plantilla de Canal de Isabel II.

El contexto de exposición de servicios estará claramente definido en la aplicación.

[RGB002] Documentación de arquitectura física y lógica, de acuerdo al formato establecido por Canal de Isabel II.

Entendemos por arquitectura física de la solución el conjunto de servidores, subredes, elementos de comunicación, elementos de seguridad, elementos de redundancia, interfaces con otros servidores que formen parte de la infraestructura de Canal de Isabel II pero sean necesarios para el funcionamiento de la solución, clientes, protocolos y puertos de comunicación entre los mismos. Todos los elementos físicos anteriores deberán estar identificados de forma única.

Entendemos por arquitectura lógica cada uno de los servicios que se ejecutan cada uno de los elementos de la arquitectura física, protocolos que comunican los servicios anteriores, cada una de las capas que conforman las aplicaciones de la solución y el detalle de componentes y/o librerías de cada una de las capas

[RGB003] Documentación de interfases

Se documentarán todas las interfases del sistema de acuerdo al formato establecido por Canal de Isabel II.

[RGB004] Paso entre entornos

El adjudicatario deberá determinar e implantar los procedimientos de pasos y marcha atrás de las aplicaciones. Dichos procedimientos tendrán una implementación desatendida y planificable. Se aplicarán las políticas de gestión de errores y excepciones a estos procesos.

El adjudicatario deberá determinar e implantar los procedimientos de paso de información (datos) entre entornos. Estos procedimientos tendrán una implementación que deberá ser desatendida y planificable además de respetar la LOPD, por lo que debería existir un procedimiento de disociación de datos según la clasificación de la información establecida por Canal de Isabel II y un procedimiento de reconfiguración del sistema copiado que garantice la integridad tanto de los datos que recibe (el sistema recibe sólo los datos que debe recibir) como los que envía (el sistema envía datos a los sistemas que debe enviar y no a otros).

Se aplicarán las políticas de gestión de errores y excepciones a estos procesos.

El adjudicatario utilizará los tres entornos del sistema conforme a las buenas prácticas. Toda subida a producción deberá haberse probado y validado adecuadamente en el entorno de integración.

[RGB005] Ciclo de vida de los datos

Se definirá el ciclo de vida de los datos, así como los procedimientos para el archivado o borrado de la información en base a tiempo y/o tamaño, establecer los mecanismos necesarios para la consulta y/o recuperación de la información archivada. Todos los procedimientos de Bases de Datos deberán automatizarse.

En el caso de migraciones se definirán procesos repetibles (continuando a partir de determinado paso), desatendidos, automáticos y planificables y diseñados de manera que puedan ser reutilizados para tratamientos masivos de datos.

[RGB006] Externalización de configuración

Todos los parámetros de configuración de las aplicaciones y componentes, fuentes de datos, propiedades de despliegue (dependientes del entorno), etc. serán externos al código de la aplicación.

Las propiedades de configuración podrán leerse de diferentes fuentes (fichero (path y classpath), JNDI, URL, etc).

Canal de Isabel II podrá requerir que los cambios de configuración y parametrización de la aplicación se lleven a cabo a través de un GUI.

Canal de Isabel II podrá requerir que la modificación de los cambios se aplique en caliente sin reinicio de la aplicación.

[RGB007] Política de errores, logs y trazas

El adjudicatario elaborará e implantará una política de gestión de errores, logs y trazas en los aplicativos. La implantación de la política se realizará mediante AOP.

Las aplicaciones y/o sistemas tendrán un catálogo de errores que indique para cada código de error las causas del mismo y las posibles soluciones. Los mensajes de error contendrán la información de despliegue del sistema, por ejemplo, en caso de no poder conectar con un determinado servicio, el mensaje de error contendrá las propiedades de despliegue del mismo (servidor, puerto, etc).

Se registrarán en el log de las aplicaciones y/o sistemas el arranque y parada de las mismas indicando claramente si el arranque y/o parada ha ocurrido satisfactoriamente o no.

En caso errores se indicará claramente el código de error, el catálogo de errores recogerá las causas probables del mismo, así como las acciones a realizar.

Toda excepción capturada se escribirá en el log de la aplicación.

Se registrarán en el log todas las llamadas a sistemas externos (remotos), a nivel informativo al comienzo y final de la llamada. La información a nivel informativo incluirá el resultado de la invocación además de datos usuales en logs. Los parámetros de llamada y resultados obtenidos se escribirán en nivel DEBUG. Todos los errores y las pilas de llamadas de escribirán a nivel ERROR o WARNING según corresponda.

La recarga de la configuración de log y trazas se hará en caliente sin reinicio de la aplicación

[RGB008] Guía de desarrollo

El adjudicatario elaborará una guía de desarrollo que contenga como realizar las ampliaciones funcionales en la aplicación.

[RGB090] Pasos entre entornos

Los procedimientos de despliegue de las aplicaciones serán automáticos, desatendidos y planificables.

CANAL podrá requerir que el proceso anterior sea transaccional. Igualmente CANAL podrá requerir que el paso de datos entre entornos sea igualmente automático, planificable y desatendido además debe existir un procedimiento de disociación de datos según la clasificación de la información establecida por CANAL y un procedimiento de reconfiguración del sistema copiado que garantice la integridad tanto

de los datos que recibe (el sistema recibe sólo los datos que debe recibir) como los que envía (el sistema envía datos a los sistemas que debe enviar y no a otros).

Como fase previa a la entrada en producción, se realizarán las siguientes tareas:

- Definición de entornos, pruebas y procedimientos de producción.
- Pruebas de componentes del sistema.
- Determinación de necesidades especiales para el funcionamiento del sistema.

Requisitos de Pruebas

[RP001] Plan de pruebas

Se diseñará un plan de pruebas para cubrir todas las pruebas que apliquen en el sistema.

Pruebas unitarias

Pruebas de integración

Pruebas de disponibilidad

Pruebas funcionales

Pruebas de rendimiento

Pruebas de aceptación

[RP002] Pruebas unitarias

Las pruebas unitarias se desarrollarán en código y se lanzarán con la herramienta de integración continua.

[RP003] Pruebas de integración

Las pruebas de integración se desarrollarán en código y se lanzarán con la herramienta de integración continua.

[RP004] Pruebas funcionales

Las pruebas funcionales se desarrollarán en código y se lanzarán con la herramienta de integración continua.

[RP005] Pruebas de rendimiento

Las pruebas de rendimiento se realizarán con la herramienta JMeter.

ANEXO 5. CONDICIONES PARA LA CONEXIÓN A LA RED CORPORATIVA DE DATOS Y DE SEGURIDAD DE CANAL DE ISABEL II

El adjudicatario queda obligado a realizar una conexión privada a la Red Corporativa de Datos (en adelante, RCD) de Canal de Isabel II, S.A. para la realización de aquellos trabajos contemplados dentro del alcance del presente contrato que lo requieran. El adjudicatario, por tanto, deberá asignar un recurso técnico especializado en redes de datos y comunicaciones, que se responsabilice, en el ámbito de la prestación de los servicios asociados al contrato de prestación de servicios, de la configuración y mantenimiento de la parte de la infraestructura de comunicaciones entre el adjudicatario y Canal de Isabel II, S.A. que sea responsabilidad del adjudicatario, al objeto de garantizar el cumplimiento de estas condiciones de conexión, la cual se realizará bajo los siguientes condicionantes obligatorios:

1. Conexión única del operador de comunicaciones con la RCD de Canal de Isabel II

El operador de comunicaciones elegido por la empresa colaboradora para la puesta en marcha de la conexión de la misma con Canal de Isabel II, S.A. entregará en un único punto todo el tráfico gestionado de las empresas colaboradoras que conecten a través del mismo con Canal de Isabel II, S.A. Esto es, si el operador ya presta servicio a una empresa colaboradora de Canal de Isabel II, S.A., la nueva conexión deberá utilizar la infraestructura física existente en Canal de Isabel II, S.A. para generar la nueva conexión, sin que sea necesaria la instalación de nuevo equipamiento físico ni la realización de ninguna actividad en las dependencias de Canal de Isabel II, S.A. La utilización de infraestructura común por parte de las empresas colaboradoras no supone la disponibilidad de conexión entre las mismas, siendo el objeto la conexión privada uno a uno de cada una de las empresas colaboradoras con Canal de Isabel II, S.A. En caso de que el operador no preste en la actualidad este servicio a ninguna empresa colaboradora, podrá realizar la conexión a la RCD de Canal de Isabel II, S.A., teniendo en cuenta la casuística expuesta para futuras conexiones de otras posibles empresas. El operador de comunicaciones preservará la privacidad de las comunicaciones con la RCD de Canal de Isabel II, S.A. y en especial entre las diferentes empresas colaboradoras a las que pudiera dar servicio con la misma infraestructura.

En caso de que el contrato sea adjudicado a una Unión Temporal de Empresas (UTE), se presentará una única conexión a Canal de Isabel II, S.A., y serán las empresas que forman la UTE las que deberán coordinarse entre ellas y realizar las acciones que sean necesarias para garantizar que la prestación de los servicios contratados por parte de Canal de Isabel II, S.A. se realice exclusivamente a través de dicha conexión única.

2. Conexión de backup, contingencia o respaldo con la RCD de Canal de Isabel II

Si por parte del área de Canal de Isabel II, S.A. responsable de la empresa colaboradora se identificara que el servicio contratado es crítico, necesitara una conexión de *backup*, contingencia o respaldo, o tuviera unos requisitos de disponibilidad altos (por ejemplo, 24x7), la empresa colaboradora quedaría obligada a provisionar una segunda línea de comunicación con Canal de Isabel II, S.A. a través de otro operador de comunicaciones distinto del seleccionado para la primera línea de comunicación, y en los mismos términos identificados en el punto 1. Conexión única del operador de comunicaciones con la RCD de Canal de Isabel II, S.A., con el objeto de disponer de una línea adicional y poder garantizar así la disponibilidad de las comunicaciones.

3. Direccionamiento IP

La empresa contratista se adecuará a los rangos de direccionamiento IP establecidos por Canal de Isabel II, S.A. Se establecerá por parte de Canal de Isabel II, S.A. un rango IP compatible en el que la empresa contratista se integrará en la RCD de Canal de Isabel II, S.A. Si fuera necesaria la aplicación de traducción de direcciones (NAT) ésta será responsabilidad exclusiva de la empresa contratista, bien con medios propios o bien a través de la capacidad de la línea contratada con el operador de comunicaciones elegido.

4. Monitorización de la conexión

Canal de Isabel II, S.A. se reserva el derecho de monitorizar la línea de comunicaciones solicitada por la empresa contratista. Para ello se debe garantizar el acceso de consulta SNMP a los routers en extremos (no a los routers que pudieran componer la propia red del operador) dedicados a la conexión.

5. Contacto

En caso de duda sobre alguna de las condiciones reflejadas en este documento, pueden dirigir sus consultas o dudas, haciendo referencia a los apartados de este documento, a su responsable o contacto en Canal de Isabel II, S.A. quien se encargará de tramitarlas de forma interna.

A continuación se recogen los requisitos técnicos de seguridad que deberá cumplir toda entidad externa a Canal de Isabel II S.A. (en adelante, Canal de Isabel II) con la que exista un contrato firmado vigente, un convenio o encomienda suscrito por ambas partes firmado y vigente o trabajos acordados, cuya naturaleza y alcance estarán reflejados por escrito y vigentes para referencia y consulta por ambas partes, y que requieran el acceso a Sistemas de Información de Canal de Isabel II para la ejecución de los trabajos reflejados en el contrato, convenio, encomienda o acuerdo (en adelante, los trabajos).

1. Las entidades externas deberán utilizar el acceso concedido a la Red Corporativa de Datos de Canal de Isabel II (en adelante, RCD) y a los sistemas informáticos de Canal de Isabel II, única y exclusivamente para la realización de los trabajos.

2. Las entidades externas deberán adoptar, en aquellos equipos de su propiedad que vayan a ser utilizados para acceder a los recursos proporcionados por Canal de Isabel II, las medidas de índole técnico que establezca Canal de Isabel II para garantizar la seguridad e integridad de la RCD, de los sistemas informáticos y de la información que contienen, propiedad de Canal de Isabel II. Estas medidas incluyen, como mínimo, los siguientes puntos:

- El equipo informático, dispositivo hardware o aplicación propia utilizados para la realización de los trabajos estarán actualizados con todos los parches y actualizaciones, principalmente las críticas y las de seguridad, liberadas por el fabricante o comunicadas de forma particular, tanto del hardware como de los Sistemas Operativos base y las aplicaciones.
- El equipo informático, dispositivo hardware o aplicación propia utilizados para la realización de los trabajos deberán mantenerse actualizados mediante la aplicación programada de los parches y actualizaciones, principalmente las críticas y las de seguridad, proporcionados por el fabricante, tanto del hardware como de los Sistemas Operativos base y las aplicaciones propias, a la mayor brevedad posible, una vez se hayan publicado de forma oficial o hayan sido comunicadas de forma particular.
- Siempre que los Sistemas Operativos base lo permitan, deberán contar con medidas de contención (antivirus, antispyware, antimalware, etc.) instaladas, activas y actualizadas de forma periódica.
- Los equipos destinados a dar servicio para la prestación de los trabajos, deberán estar aislados de la red propia de la entidad externa, contrata o proveedor.
- Se deberá mantener informado al responsable de los trabajos en Canal de Isabel II en todo momento, aportando la adecuada justificación, de cualquier cambio en equipos, hardware y aplicaciones y configuración de los mismos, así como de personal propio o externo que acceda a los recursos proporcionados por Canal de Isabel II para el desempeño del trabajo reflejado en las obligaciones contractuales de los trabajos.

3. La conexión de entidades externas se hará siempre a través de los sistemas de control de acceso de Canal de Isabel II para permitir el acceso exclusivamente a los sistemas de información y comunicación de Canal de Isabel II necesarios, y por los servicios requeridos, para el desarrollo de los trabajos.

4. Todos los accesos a los sistemas de información y comunicación de Canal de Isabel II se realizarán, en la medida de lo posible, de forma segura, evitando siempre protocolos de comunicación manifiestamente inseguros (TELNET, NetBIOS, RDP, FTP, TFTP, etc.).
5. Una vez concedido el acceso a sistemas de información y comunicación de Canal de Isabel II, éste se registrará siempre por el Principio del Menor Privilegio (asignación de los privilegios mínimos necesarios para poder realizar y completar los trabajos).
6. Toda entidad externa cuyo cometido exclusivo sea el desarrollo de aplicaciones o soluciones informáticas para Canal de Isabel II, sólo tendrá acceso a los entornos de desarrollo para la realización de los trabajos. El acceso a los sistemas de integración y producción, de autorizarse explícitamente por el Responsable de la Aplicación en Canal de Isabel II, sólo se realizará con perfiles de consulta y siempre con la supervisión del responsable del proyecto en Canal de Isabel II, y exclusivamente para llevar a cabo las pruebas de calidad estrictamente necesarias, justificadas y derivadas de los trabajos realizados en el entorno de desarrollo.
7. Toda entidad externa cuyo cometido sea la operación de determinados sistemas de información productivos de Canal de Isabel II, sólo tendrán acceso a dichos sistemas con el perfil de operación mínimo necesario para poder realizar con garantía y de forma satisfactoria los trabajos. El perfil de operación no tendrá ninguna autorización ni rol que permita la modificación del sistema.
8. Se restringirá al máximo el acceso remoto a sistemas de información y comunicación de Canal de Isabel II. No se permitirá el acceso remoto ni local a sistemas de información y comunicación con permisos de administrador, salvo que el objeto de los trabajos refleje explícitamente la explotación y administración de dichos sistemas de información y comunicación o que se autorice explícitamente por el Responsable de la Aplicación en Canal de Isabel II.
9. Canal de Isabel II se reserva el derecho de desconexión en caso de detectar cualquier incidente de seguridad imputable a la entidad externa, contrata o proveedor que pueda comprometer la integridad de la RCD y los Sistemas de Información y Comunicación de Canal de Isabel II, así como la confidencialidad, integridad y disponibilidad de la información que contienen.
10. La entidad externa, en caso de que haya evidencias demostrables de que un incidente de seguridad en Canal de Isabel II es imputable a ella, se compromete a elaborar un informe pormenorizado y exhaustivo del incidente en el que hará constar, como mínimo, la siguiente información:
 - Alcance y objetivos del documento.
 - Descripción del incidente.
 - Origen del incidente.
 - Descripción cronológica de los hechos del incidente.
 - Descripción de las acciones preventivas/correctivas llevadas a cabo por la entidad externa, contrata o proveedor.
 - Evaluación de los recursos humanos pertenecientes al equipo de trabajo asignado al contrato, convenio o acuerdo bajo el que se prestan los servicios a Canal de

Isabel II y que han sido necesarios para el análisis y resolución del incidente. Dicho informe, una vez terminado, se remitirá al responsable del contrato, convenio, encomienda o acuerdo en Canal de Isabel II.

11. Canal de Isabel II se reserva el derecho de realizar las auditorías de seguridad que considere oportunas y necesarias, previa comunicación con antelación suficiente a la entidad externa y con el único objeto de garantizar el cumplimiento de los requisitos técnicos aquí dispuestos. Si Canal de Isabel II detecta no conformidades con cualquiera de los puntos aquí reflejados, se concederá a la entidad externa un plazo temporal para subsanar dichas no conformidades. Si éstas persisten una vez agotado dicho plazo temporal, podrán ser causa de resolución del contrato según lo establecido en la Cláusula 9.2 del Anexo I del Pliego de Cláusulas Administrativas Particulares.