PLIEGO DE PRESCRIPCIONES TÉCNICAS PARA EL CONTRATO DE LOS SERVICIOS DE MANTENIMIENTO DE APLICACIONES (SOPORTE A USUARIOS, CORRECTIVO Y EVOLUTIVO) DE LAS PLATAFORMAS SAP CORPORATIVAS DE CANAL DE ISABEL II Y EMPRESAS PARTICIPADAS

CONTRATO Nº 40/2020

Madrid, 6 de mayo de 2020

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A.	Servicios de mantenimiento de aplicaciones (soporte a usuarios, correctivo y evolutivo) de las plataformas SAP corporativas de Canal de Isabel II y empresas participadas	06/05/2020
Elaborado por	**Documento**	**Versión**
Área de Aplicaciones Informáticas	Pliego de Prescripciones Técnicas	V1.0

Índice

1. INTRODUCCIÓN

1.1. Contexto y antecedentes

Canal de Isabel II S.A., en adelante Canal de Isabel II en el presente documento, dispone en la actualidad de diferentes aplicaciones SAP corporativas que dan soporte a sus procesos dentro de su quehacer diario. Es por esto por lo que se demanda un servicio de mantenimiento de aplicaciones que, gestionado mediante acuerdos de niveles de servicio, permita asegurar el soporte, el correcto funcionamiento y la evolución de dichas aplicaciones.

1.2. Ámbito del contrato

Adicionalmente a Canal de Isabel II, S.A., y dentro del ámbito de la presente licitación, se encuentran encuadradas las siguientes entidades y empresas:

- Ente público Canal de Isabel II.
- Hispanagua, S.A.U.
- Canal de Comunicaciones Unidas, S.A.U.
- Canal Gestión Lanzarote, S.A.U.

1.3. Objetivos del servicio

El objeto del presente concurso es la contratación de los "**Servicios de Mantenimiento de Aplicaciones (soporte a usuarios, mantenimiento correctivo y evolutivo) de las plataformas SAP Corporativas de Canal de Isabel II y empresas participadas"** durante un periodo de cuatro años.

Canal de Isabel II desea establecer/definir el mantenimiento de las aplicaciones SAP corporativas mediante un modelo de servicio gestionado por un Adjudicatario. Los objetivos de este modelo de servicio son los siguientes:

- Un servicio de soporte que satisfaga las exigencias de servicio que las áreas de Canal de Isabel II demandan de sus aplicaciones corporativas, asegurando su satisfacción.
- Disponer de un equipo de trabajo suficientemente dimensionado y con la experiencia y perfiles adecuados para hacer frente al servicio con garantía.
- Definir un modelo de gestión de servicio que permita medir y controlar el nivel de servicio ofertado mediante Acuerdos de Nivel de Servicio (ANS) y detectar y corregir desviaciones rápidamente.

- Garantizar la evolución adecuada de los sistemas en consonancia con los cambios en los procesos empresariales y/o normativos.
- Identificar áreas de mejora y adaptaciones en las aplicaciones actuales que permitan disponer de entornos más estables, más fáciles de mantener y con mayor funcionalidad.
- Reducir los costes de mantenimiento mediante el aprovechamiento de perfiles comunes.
- Garantizar una gestión eficiente del conocimiento de las aplicaciones, tanto dentro del equipo del Adjudicatario como dentro del equipo de Canal de Isabel II. Para ellos será objetivo primordial documentar y mantener actualizada la documentación de dichas aplicaciones.
- 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.

Para el cumplimiento de estos objetivos el Adjudicatario debe ofrecer los siguientes servicios cuyo alcance se detalla en el apartado 2 de este documento:

- **Soporte**
- **Soporte extendido**
- **Mantenimiento Correctivo**
- **Gestión de problemas**
- **Mantenimiento Evolutivo**
- **Mantenimiento Preventivo**
- **Mantenimiento Adaptativo**
- **Gestión del servicio**

Para poder disponer de un servicio global satisfactorio, se han detectado los siguientes factores críticos de éxito:

- Adecuada adquisición del conocimiento durante la transición del servicio.
- Realizar una adecuada gestión del conocimiento del sistema, minimizando el tiempo de transición y asegurando la correcta gestión del conocimiento 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 y/o normativos.
- Polivalencia del equipo para poder trabajar con diferentes demandas de servicios.
- Seleccionar un Adjudicatario con capacidad humana y técnica suficiente en las diferentes plataformas tecnológicas objeto del servicio.
- Definir un modelo de relación y gestión adecuado para hacer frente a un servicio de mantenimiento de gran envergadura.
- Definir los procedimientos de trabajo adecuados con el equipo de Administración TI.

2. ALCANCE DEL SERVICIO LICITADO

2.1. Descripción de los servicios solicitados

El trabajo consistirá en la prestación de los siguientes servicios de mantenimiento de aplicaciones:

- Soporte
- Soporte extendido
- Mantenimiento Correctivo
- Gestión de problemas
- Mantenimiento Evolutivo
- Mantenimiento Preventivo
- Mantenimiento Adaptativo
- Gestión del servicio

Para llevar a cabo todos los servicios anteriores, se establecerá una Bolsa de Puntos Tarea sobre la que se imputarán todos los trabajos realizados por parte del Adjudicatario, pudiéndose dedicar dicha bolsa a cualquiera de los servicios anteriores indistintamente.

Se ha incluido dentro del Anexo 5 del presente documento la siguiente información particular:

Anexo 5

1. **Objeto:** objeto del documento
2. **Alcance Funcional:** descripción de las funcionalidades soportadas en la plataforma y previsión de proyectos a acometer sobre la misma.
3. **Alcance Técnico:** plataforma tecnológica sobre la que funciona las aplicaciones a mantener por parte del Adjudicatario.
4. **Volumetría del servicio:** de cara al dimensionamiento de las ofertas por parte de los licitantes, se facilitan volumetrías de los servicios de mantenimiento de aplicaciones que prestan actualmente servicio sobre las plataformas requeridas.
5. **Puntos Tarea:** cuadro de puntos tarea para las actividades a realizar sobre la plataforma.
6. **Acuerdos de Niveles de Servicio**
7. **Soporte Extendido y Horario**

Además de los sistemas y aplicativos descritos en el Anexo 5, dentro del alcance del contrato se **incluyen los nuevos aplicativos que se desarrollen o pongan en producción, tanto por el Adjudicatario como por Canal de Isabel II o terceros contratados por Canal de Isabel II, mientras el contrato se encuentre en vigor**, manteniéndose las condiciones de servicio para el conjunto de aplicativos sobre la plataforma tecnológica mantenida por el Adjudicatario.

En los casos en los que el nuevo aplicativo se haya desarrollado o puesto en producción por Canal de Isabel II o por terceros en su nombre, se establecerá una transición entre Canal de Isabel II o dicho tercero y el Adjudicatario para que el Adjudicatario se encuentre en condiciones de mantenerlo. Los trabajos a realizar por parte del Adjudicatario se encuadrarán dentro de los servicios de soporte o proyecto y serán con cargo a la bolsa de puntos tarea.

De igual manera, queda dentro del alcance del contrato, la evolución y/o migraciones de los sistemas citados para la adaptación a las nuevas versiones de las herramientas englobadas en la plataforma tecnológica objeto del contrato.

El Adjudicatario se compromete a utilizar los procedimientos, procesos y sistemas de reporte y control de incidencias y solicitudes implantados en Canal de Isabel II, así como adaptarse a los cambios futuros que Canal de Isabel II pueda implantar en estos procedimientos y sistemas.

El Adjudicatario utilizará sus propias licencias de uso de las herramientas de desarrollo, gestión, soporte y gestión de incidencias necesarias para la ejecución de los trabajos objeto de este pliego, tanto para las herramientas por él mismo designadas como para las herramientas necesarias existentes en Canal de Isabel II. Como herramienta de soporte y gestión de solicitudes e incidencias se utilizará CA Service Desk.

Los equipos personales (PC’s) para llevar a cabo los trabajos requeridos por parte del equipo de trabajo serán proporcionados y mantenidos por el propio Adjudicatario, así como aquellas licencias necesarias para su correcto funcionamiento.

Canal de Isabel II facilitará los entornos de desarrollo, calidad y producción. Los traspasos entre entornos se realizarán de acuerdo a los procedimientos dados por Canal de Isabel II. El código fuente del entorno de desarrollo deberá ser proporcionado por el Adjudicatario según procedimiento indicado por Canal de Isabel II.

El código fuente del entorno de desarrollo deberá ser proporcionado por el Adjudicatario según procedimiento indicado por Canal de Isabel II, el cual puede incluir control de versiones y entornos de integración continua.

2.1.1. Soporte

Soporte a usuarios:

El equipo de mantenimiento deberá ofrecer soporte telefónico a las consultas planteadas sobre el sistema por parte de los usuarios, resolviendo consultas sobre funcionalidad operativa, así como proporcionando soporte en la notificación de incidencias o gestión de solicitudes.

El equipo de soporte al usuario recabará de éste la información suficiente para poder identificar la posible anomalía.

Dentro de este apartado se incluirá el soporte relacionado con procesos de especial criticidad que necesiten de la atención de los consultores expertos, realizándose un seguimiento detallado para ayudar en la resolución del problema.

El horario de atención a usuarios será el descrito en el Apartado 7 – Soporte Extendido y Horario dentro del Anexo 5 de Información Particular de SAP.

El Adjudicatario proporcionará un número de teléfono convenientemente dimensionado para proporcionar este soporte.

El escenario estimado de consultas/mes para el contrato será el descrito en el Apartado 4 – Volumetría del Servicio dentro del Anexo 5 de Información Particular de SAP.

Este servicio estará sujeto al cumplimiento de los Acuerdos Nivel de Servicio del Canal de Isabel II.

Las consultas telefónicas que por su complejidad requieran de más de **8 horas** de trabajo deberán gestionarse como peticiones de servicio.

Para la realización de estos trabajos se dispone de una bolsa de Puntos Tarea (ver Apartado 5 – Puntos Tarea del Anexo 5 de Información Particular de SAP) sobre la que se imputarán mensualmente los puntos tarea asociados a los soportes realizados.

Peticiones de servicio:

Se definen peticiones de servicio aquellas solicitudes cuyos trabajos asociados no implican un cambio en la aplicación existente, tales como los siguientes:

- Parametrizaciones de la aplicación
- Creación de roles o usuarios
- Generación de informes
- Extracciones de información
- Consultas a soporte de fabricante
- Estimación gruesa de evolutivos

El soporte también incluirá la realización y monitorización de procesos de carácter periódico en los sistemas, los cuales serán gestionados como peticiones de servicio.

Este servicio estará sujeto al cumplimiento de los *Acuerdos Nivel de Servicio* de Canal de Isabel II.

Los trabajos asociados a Peticiones de Servicio tendrán una garantía de **60** días laborables desde su puesta en producción o su entrega aceptada por Canal de Isabel II. Las incidencias surgidas durante esos días y que sean imputables a una realización errónea o incompleta de la petición por el Adjudicatario deberán ser corregidas por éste sin cargo a CanaI de Isabel II. A estas incidencias se les aplicarán los niveles de servicio asociados a incidencias, pero no se imputarán con cargo a la bolsa de puntos tarea.

Para la realización de estos trabajos se dispone de una bolsa de Puntos Tarea (ver Apartado 5 – Puntos Tarea del Anexo 5 de Información Particular de SAP) sobre la que se imputarán mensualmente los puntos tarea asociados a las peticiones de servicio realizadas.

El escenario estimado de peticiones de servicio/mes para el contrato será el descrito en el Apartado 4 – Volumetría del Servicio dentro del Anexo 5 de Información Particular de SAP.

En caso necesario se demandará un soporte presencial por lo que el Adjudicatario debe disponer de oficinas en la Comunidad de Madrid para ofrecer dicho soporte. Las actividades típicas que pueden requerir soporte presencial son:

- Soporte a pruebas
- Formación sobre funcionalidades de la herramienta
- Soporte a procesos críticos
- Reuniones de coordinación con otros equipos
- Reuniones con usuarios

2.1.2. Mantenimiento Correctivo

Las funciones del servicio de mantenimiento correctivo tienen como objetivo resolver el funcionamiento incorrecto de la aplicación sin que se alteren las especificaciones funcionales.

Son actividades que modifican una aplicación y su documentación para aplicar soluciones permanentes o soluciones alternativas temporales (*workarounds*) para corregir, eliminar, resolver o minimizar el impacto de los defectos conocidos (problemas o incidencias). Las soluciones alternativas temporales pueden inicialmente ser empleadas para prevenir incidencias adicionales, pero el resultado final del soporte correctivo es una solución permanente. Estas modificaciones no están hechas con el propósito de cambiar la

funcionalidad, pero pueden incluir la recuperación de funcionalidades de los usuarios, sólo para garantizar el cumplimiento con los requisitos base.

Incluirá las actividades relacionadas con la resolución de errores funcionales, técnicos y de datos de la aplicación.

El equipo de soporte para el mantenimiento correctivo atenderá a las incidencias que se reciban por parte de los usuarios de Canal de Isabel II según los plazos de escalado, respuesta y resolución recogidos en la Tabla de Criticidad de Incidencias reflejada en el Apartado 6 – Acuerdos de Niveles de Servicio dentro del Anexo 5.

La criticidad de las incidencias será determinada por Canal de Isabel II. Los cambios en la categorización de las mismas se coordinarán entre Canal de Isabel II y el responsable del servicio.

Cuando la anomalía urgente requiera una intervención en las instalaciones de Canal de Isabel II el tiempo de atención y desplazamiento no podrá exceder las 2 horas, por lo que el licitador deberá disponer de personal técnico y de una oficina de atención o soporte técnico a 2 horas de las Oficinas Centrales de Madrid a fin de cumplir el requerimiento de atención de anomalías urgentes, de conformidad con lo indicado en el apartado 5.1 del Anexo I del Pliego de Cláusulas Administrativas Particulares.

El Adjudicatario deberá hacer frente a las incidencias existentes en el momento de transición del servicio, aunque no se aplicarán las penalizaciones en caso de incumplimiento excepto las que correspondan a las indicadas en los ANS propios de esta fase. Será responsabilidad del Adjudicatario actual durante la fase de transición (devolución del servicio) el cumplimiento de los ANS establecidos en el contrato actual. En el caso de resultar ser el Adjudicatario el mismo que el Adjudicatario actual deberá cumplir los ANS establecidos en el contrato anterior durante la fase de transición (adaptación) al nuevo servicio.

Una incidencia se considera resuelta sólo cuando la entrega ha sido aceptada y la solución ha sido implantada en productivo.

Para el cómputo del tiempo de resolución de las incidencias de cara a medir los ANS, el Adjudicatario podrá proponer justificaciones a las causas de suspensión quedando a único criterio del Canal de Isabel II su aceptación.

A efectos de cómputos de contabilización de incidencias, aquellas incidencias asociadas a cambios erróneos implementados por el Adjudicatario y detectados durante los **60** días laborables siguientes a su puesta en producción, se considerarán cubiertos por la garantía de los trabajos y, por tanto, no se imputarán los trabajos de resolución con cargo a la bolsa de puntos tarea y se tendrán en cuenta dichas resoluciones a efectos de cálculo de cumplimiento de los ANS.

El Adjudicatario se compromete a utilizar los procedimientos y sistemas de reporte y control de incidencias implantados en Canal de Isabel II, así como adaptarse a los cambios futuros que Canal de Isabel II pueda implantar en estos procedimientos y sistemas. El Adjudicatario deberá aportar sus propias licencias de estos productos para el uso por su equipo de

trabajo. Actualmente se utiliza como herramienta de soporte y gestión de solicitudes e incidencias CA Service Desk.

Para la realización de estos trabajos se dispone de una bolsa de Puntos Tarea (ver Apartado 5 – Puntos Tarea del Anexo 5) sobre la que se imputarán mensualmente los puntos tarea asociados a las incidencias solucionadas.

El escenario estimado de incidencias/mes para el contrato será el descrito en el Apartado 4 – Volumetría del Servicio dentro del Anexo 5.

2.1.3. Gestión de Problemas

Se entiende por problema la causa desconocida de una o más incidencias, en la que resulta fundamental el descubrimiento de una solución definitiva que resuelva la causa raíz del problema y la aparición de nuevas incidencias, así como soluciones temporales durante la identificación y resolución del problema.

Un problema, por definición, es una incidencia recurrente, es decir, que se ha repetido varias veces. Aunque se puedan haber proporcionado soluciones a los “síntomas”, el hecho de que se repita de forma recurrente la incidencia demuestra que el problema sigue sin resolverse.

Una incidencia podrá ser considerada como problema a partir de la tercera repetición de la incidencia en el plazo de 1 mes y se procederá al registro de un problema. También se considera problema una incidencia o casuística sobre la que se desconozca la causa y se encuentra justificado realizar una investigación adicional para controlar el riesgo, el coste y la planificación.

En este tipo de gestión resulta básica la colaboración entre varios servicios y proveedores para la identificación real del problema y conseguir su resolución.

La respuesta a un problema debe de contener, al menos,

- Las acciones que se van a seguir para la resolución del problema
- Plan de acción detallado con fechas de finalización de cada una de las acciones

Aunque actualmente no está operativo en Canal de Isabel II el proceso de Gestión de Problemas, podrá activarse a lo largo del contrato. El tratamiento que se le dará a dicha Gestión de Problemas será mediante la solicitud por parte de Canal de Isabel II de peticiones de servicio.

Actualmente Canal de Isabel II no dispone de volumetrías asociadas al proceso de Gestión de Problemas.

2.1.4. Mantenimiento Evolutivo

Para cada solicitud de mantenimiento evolutivo el Adjudicatario deberá analizar y presupuestar la misma en puntos tarea. Las actividades de gestión asociadas a la solicitud deberán estar incluidas en dicho presupuesto.

Esta presupuestación deberá realizarse cumpliendo con los plazos marcados en los ANS según la naturaleza del trabajo. Canal de Isabel II revisará el presupuesto en puntos tarea y solicitará toda la información aclaratoria que precise. A partir del análisis y presupuesto realizados, Canal de Isabel II determinará si aprueba el presupuesto, en cuyo caso se planificarán y ejecutarán estas solicitudes, siempre supeditándose a la criticidad de las actividades del mantenimiento correctivo.

El Adjudicatario deberá desarrollar y probar las solicitudes en el entorno de desarrollo, y realizar pruebas finales en el entorno de integración. Canal de Isabel II podrá delegar la gestión de las solicitudes/transportes a producción en el Adjudicatario.

En el caso de sufrir modificaciones funcionales durante el desarrollo de una solicitud de mantenimiento evolutivo, deberá volverse a presupuestar por el Adjudicatario y aceptar por Canal de Isabel II teniendo en cuenta las modificaciones en las que se incurra.

En el caso de que Canal de Isabel II detecte la imposibilidad de poder llevar a cabo una presupuestación en puntos tarea de los trabajos debido a la casi total incertidumbre de estos, se llevarán a cabo los trabajos mediante un paquete de solicitudes con un tamaño fijo de Puntos Tarea, de tal manera que se vayan consumiendo según se vayan realizando los trabajos. Si finalmente dicho paquete se consume en su totalidad, podrá nuevamente ampliarse si así lo decide Canal de Isabel II a su único criterio.

Concluidas las pruebas el Adjudicatario notificará a Canal de Isabel II la finalización del desarrollo y entregará la documentación específica de la funcionalidad (tanto técnica como funcional), así como la documentación existente actualizada. Canal de Isabel II revisará la documentación y realizará las pruebas de aceptación.

Una solicitud de mantenimiento evolutivo se considerará resuelta sólo cuando la entrega haya sido aceptada y la solicitud haya sido implantada en productivo.

Se facturará en base a los trabajos certificados por Canal de Isabel II para las mismas, pudiéndose dar casos en los que no se facture por la totalidad del presupuesto de la solicitud. En aquellas solicitudes en las que surja la necesidad de ampliarlas, el Adjudicatario deberá pasar una nueva presupuestación para su posterior aprobación por parte de Canal de Isabel II, no pudiendo acometer los nuevos trabajos sin contar con dicha aprobación.

Para que una entrega se considere finalizada y facturable, debe superar los criterios de aceptación de Canal de Isabel II en todos sus aspectos:

- Análisis y Diseño
  - Matriz trazabilidad de requisitos -> paquetes de trabajo
  - Estimación de costes
  - Piloto de pantallas de usuario
- Documentación: se realizará sobre la herramienta corporativa indicada por Canal de Isabel II
  - Requisitos y análisis

    - Actas, informes, presentaciones
- Pruebas
    - Unitarias: pruebas de los desarrollos (Unit testing)
    - Validación de usuario: pruebas funcionales entornos de Calidad
- Entrega
    - El código fuente debe quedar recogido en el repositorio de software que Canal de Isabel II indique
- Calidad
    - Funcionales: se cumplen todos los requisitos
    - Técnicas: El código fuente pasará por la herramienta de análisis de código que Canal de Isabel II disponga
- Seguridad
    - Análisis de impacto
    - Cumplimiento requerimientos Seguridad (ver Anexo 3 del presente documento)
    - Auditorías (ver Anexo 3 del presente documento)
- Privacidad
    - Cumplimiento requerimientos accesibilidad
- Puesta en Producción
    - Si el entregable lleva funcionalidad asociada deberá cumplir como hito final la puesta en producción de la misma

Los cambios asociados a solicitudes de Mantenimiento Evolutivo tendrán una garantía de **6 MESES** desde su puesta en producción. Las incidencias surgidas durante esos días y que sean imputables a una realización errónea o incompleta de los cambios por el Adjudicatario deberán ser corregidas por éste sin cargo a Canal de Isabel II. A estas incidencias se les aplicarán los niveles de servicio asociados a incidencias de cara al cumplimiento de los ANS y **NO** se imputarán los trabajos de resolución, llevados a cabo por el contratista, con cargo a la bolsa de puntos tarea.

Este servicio estará sujeto al cumplimiento de los *Acuerdos Nivel de Servicio* de Canal de Isabel II.

El Adjudicatario se compromete a utilizar los procedimientos y sistemas de reporte y control de solicitudes de mejora implantadas en Canal de Isabel II, así como adaptarse a los cambios futuros que Canal de Isabel II pueda implantar en estos procedimientos y sistemas. El Adjudicatario deberá aportar sus propias licencias de estos productos para el uso por su equipo de trabajo. Como herramienta de soporte y gestión de solicitudes e incidencias se utilizará CA Service Desk.

Para la realización de estos trabajos de mantenimiento evolutivo se dispone de una bolsa de Puntos Tarea (ver Apartado 5 – Puntos Tarea del Anexo 5) sobre la que se imputarán mensualmente los puntos tarea asociados a las solicitudes de mantenimiento evolutivo realizadas.

El escenario estimado de evolutivos/mes para el contrato será el descrito en el Apartado 4 – Volumetría del Servicio dentro del Anexo 5 de Información Particular.

2.1.5. Mantenimiento Preventivo

Se considera mantenimiento preventivo a aquellas actuaciones encaminadas a mejorar el rendimiento de la aplicación o a evitar posibles incidencias. Son actividades que examinan las aplicaciones y los procesos con el fin de crear cambios para el mejorar el rendimiento y planificación de capacidad. También se realizan las actividades requeridas por los cambios derivadas de modificar una aplicación y su documentación, para mejorar el funcionamiento de la aplicación, su rendimiento o mantenimiento, o para evitar problemas futuros. Las modificaciones no son hechas con el propósito de cambiar funcionalidades.

El tratamiento será muy similar al descrito en el apartado de Mantenimiento Evolutivo con la diferencia de que, en este caso, las solicitudes pueden originarse tanto desde el personal técnico de mantenimiento o explotación de los sistemas de información de Canal de Isabel II, como incluso, por el propio Adjudicatario, como resultado del análisis de incidencias.

Las actuaciones de Mantenimiento Preventivo tendrán el mismo tratamiento que las solicitudes de evolutivo a efectos de los niveles de servicio y del consumo de Puntos Tarea.

2.1.6. Mantenimiento Adaptativo

Se considera mantenimiento adaptativo a aquellas modificaciones de un sistema de software o de un componente, después de su puesta en funcionamiento, para adaptarlo a cambios del entorno, como por ejemplo migraciones de versiones, máquinas físicas o cambios en sistemas con los que interactúe. Son actividades, alienadas con los procedimientos de Canal de Isabel II, para modificar una aplicación y su documentación, derivadas de cambios en el entorno técnico en lo cual la aplicación opera. Las modificaciones no son hechas con el propósito de cambiar de funcionalidades

Dentro de este apartado se incluirá el soporte relacionado con procesos de especial criticidad que necesiten del soporte del equipo de mantenimiento, como por ejemplo procesos masivos para regularizaciones de datos (cambios organizativos, migraciones de datos entre versiones de aplicaciones, etc.)

También dentro de este apartado se incluirá la adaptación de aplicaciones sujetas al contrato de mantenimiento a estándares o tecnologías, como por ejemplo cambiar el interfaz cliente de una aplicación por un interfaz web.

Aquellas actuaciones que se consideren mantenimiento adaptativo se planificarán como solicitudes a incluir en la bolsa de servicios del Mantenimiento Evolutivo.

Las actuaciones de Mantenimiento Adaptativo tendrán el mismo tratamiento que las solicitudes de evolutivo a efectos de los niveles de servicio y del consumo de Puntos Tarea.

En el Apartado 2 – Alcance Funcional dentro del Anexo 5, se indican algunos cambios tecnológicos previstos. Dichos cambios tecnológicos son a título informativo, no teniendo la obligación en ningún momento Canal de Isabel II de solicitar al Adjudicatario que los lleve a cabo.

2.1.7. Gestión del servicio

Todas las actividades asociadas al soporte, mantenimiento correctivo, gestión de problemas, mantenimiento evolutivo, preventivo y adaptativo deberán valorarse en puntos tarea tal y como se indica en el Apartado 5 – Puntos Tarea del Anexo 5 y se imputarán con cargo a la bolsa de Puntos Tarea del contrato.

Todas las actividades de Gestión del servicio deberán valorarse en puntos tarea en base al Apartado 5 – Puntos Tarea del Anexo 5 y se imputarán una vez realizadas con cargo a la bolsa de Puntos Tarea del contrato.

Con carácter mensual el Adjudicatario elaborará un informe a partir de los datos recogidos por la herramienta de gestión de Canal de Isabel II con las imputaciones realizadas a la bolsa de Puntos Tarea del contrato junto con la valoración realizada para su aprobación posterior por parte de Canal de Isabel II en base al informe de seguimiento mensual del servicio.

2.1.8. Gestión de Quejas y Reclamaciones

El Adjudicatario del contrato será responsable de los servicios prestados y por tanto deberá dar respuesta a las reclamaciones o quejas que se tengan del servicio.

Las quejas y reclamaciones deberán gestionarse conforme al siguiente procedimiento:

- El Responsable del Servicio de Canal de Isabel II o los responsables en los que delegue registrará las reclamaciones y quejas que les transmitan para su seguimiento.
- El Responsable del Servicio (o los responsables) transmitirán por correo electrónico la reclamación al Coordinador del Servicio del Adjudicatario.
- El Adjudicatario tendrá 2 días laborables para gestionar la reclamación o queja, dando respuesta o solución a la misma e informando al Jefe de Proyecto de Canal de Isabel II.
- Si pasados 2 días desde la reclamación no se ha tenido solución o respuesta satisfactoria, el responsable del servicio de Canal de Isabel II escalará la reclamación al Director de Servicio del Adjudicatario, con copia al Director del Servicio de Canal de Isabel II. El Director del Servicio tendrá 2 días laborables para gestionar la reclamación o queja, dando respuesta o solución a la misma e informando al Jefe de Proyecto y Director del Servicio de Canal de Isabel II.
- Si pasados 2 días laborables no se ha solucionado adecuadamente la reclamación o queja, Canal de Isabel II podrá optar por dar solución a la queja o reclamación por sus propios medios o medios de terceros. En este caso se imputarán los costes de la solución al Adjudicatario como penalización, lo cual incluirá:
    - Los costes del personal de Canal de Isabel II a una tarifa de 50 euros/hora
    - Los costes directos en los que haya incurrido Canal de Isabel II con otros proveedores para solucionar la reclamación

Todas aquellas quejas y reclamaciones que, aun habiéndose atendido, hayan derivado en:

- Indisponibilidades de sistemas
- Trabajos adicionales por el personal de Canal de Isabel II para realizar servicios dentro del alcance del contrato del Adjudicatario (cambios mal implementados que haya habido que corregir urgentemente o hayan supuesto pérdida de trabajo ya realizado)

tendrán la categorización de mala operativa y se contabilizarán mensualmente, aplicándose el nivel de servicio definido en las tablas de acuerdos de servicios.

2.1.9. Alcance Funcional y Técnico

El alcance funcional y el técnico necesarios para la prestación de los servicios requeridos aparece descrito en los Apartados 2 – Alcance Funcional y 3 – Alcance Técnico del Anexo 5.

2.1.9.1 Responsabilidad en actividades técnicas

A continuación, se detalla cada uno de los grupos de actividad:

Grupo de actividad	Ejecución de actividades
Mantenimiento Correctivo	
Definir planes relacionados con el mantenimiento correctivo	Adjudicatario
Proporcionar un punto único de contacto para la resolución de incidencias (2º nivel)	Adjudicatario
Iniciar incidencias adicionales para soporte correctivo	Adjudicatario
Realizar el mantenimiento correctivo con la prioridad asignada por Canal de Isabel II	Adjudicatario
Actualizar el nivel de prioridad y el estado de la incidencia cuando haya información adicional	Adjudicatario
Definir soluciones temporales para la resolución de incidencias	Adjudicatario
Mantener el repositorio de soluciones	Adjudicatario
Registrar las resoluciones relacionadas con funcionalidades anormales y errores de producción en las herramientas apropiadas de Canal de Isabel II	Adjudicatario
Apoyar para restablecer archivos o en otras medidas correctivas para reparar archivos de datos	Adjudicatario

Grupo de actividad	Ejecución de actividades
Identificar la necesidad de una recuperación de base de datos y comunicarla al administrador de base de datos	Adjudicatario
Proporcionar instrucciones de instalación y scripts de instalación	Adjudicatario
Determinar la causa raíz de problemas	Adjudicatario
Definir soluciones permanentes para la resolución de incidencias	Adjudicatario
Apoyo durante las actividades de recuperación de desastres	Adjudicatario
Mantenimiento Adaptativo	
Definir planes relacionados con el mantenimiento adaptativo	Adjudicatario
Analizar el impacto en las aplicaciones de cambios en la infraestructura incluyendo aspectos de Seguridad y Privacidad	Adjudicatario
Proponer cambios en las aplicaciones derivadas de cambios en la infraestructura	Adjudicatario
Planificar y aprobar cambios en las aplicaciones derivadas de cambios en la infraestructura	Canal de Isabel II
Desarrollo de cambios en las aplicaciones derivadas de cambios en la infraestructura	Adjudicatario
Implantar cambios en las aplicaciones derivadas de cambios en la infraestructura	Adjudicatario
Actualizar la documentación (de usuario, explotación, administración y monitorización) y versiones tras un cambio adaptativo	Adjudicatario
Mantener el repositorio de soluciones	Adjudicatario
Mantenimiento Preventivo	
Definir planes relacionados con el mantenimiento preventivo	Adjudicatario
Realización de pruebas de rendimiento	Adjudicatario
Monitorización de aplicaciones	Adjudicatario
Proponer mejoras (de hardware o software) necesarios para mantener y optimizar el rendimiento de las aplicaciones incluyendo aspectos de Seguridad y Privacidad	Adjudicatario
Planificar y aprobar cambios debido a mejoras propuestas	Canal de Isabel II
Desarrollar e implantar mejoras	Adjudicatario
Definición y realización de pruebas de recuperación ante desastres	Adjudicatario

Grupo de actividad	Ejecución de actividades
Actualizar la documentación (de usuario, explotación, administración y monitorización) y versiones tras un cambio preventivo	Adjudicatario
Mantener el repositorio de soluciones	Adjudicatario
Resolución de peticiones de servicio	
Proporcionar un punto único de contacto para la resolución de peticiones de servicio (2º nivel)	Adjudicatario
Realizar la petición de servicio con la prioridad asignada por Canal de Isabel II	Adjudicatario
Actualizar el nivel de prioridad y el estado de la petición de servicio cuando haya información adicional	Adjudicatario
Actualizar la documentación (de usuario, explotación, administración y monitorización) tras una petición de servicio	Adjudicatario
Mantener el repositorio de soluciones	Adjudicatario
Análisis de evolutivos medios	
Analizar evolutivos incluyendo un estudio de viabilidad, cronograma, esfuerzo (jornadas-hombre) y análisis de impacto incluyendo aspectos de Seguridad y Privacidad	Adjudicatario

Seguidamente se detalla cada uno de dichos grupos de actividad:

Grupo de actividad	Ejecución de actividades
Análisis de requisitos del negocio	
Relación con las unidades de negocio	Canal de Isabel II
Identificación de oportunidades o necesidades	Canal de Isabel II

Grupo de actividad	Ejecución de actividades
Definición de necesidades a un nivel de detalle suficiente para el diseño incluyendo aspectos de Seguridad y Privacidad.	Canal de Isabel II
Diseño y análisis funcional	
Comprender los objetivos, requisitos y el proceso de negocio actual incluyendo aspectos de Seguridad y Privacidad	Canal de Isabel II y Adjudicatario
Toma de requisitos adicionales incluyendo aspectos de Seguridad y Privacidad.	Canal de Isabel II y Adjudicatario
Diseño funcional de alto nivel y detallado incluyendo aspectos de Seguridad y Privacidad	Adjudicatario
Aprobación del diseño funcional	Canal de Isabel II
Planificación	
Planificación de evolutivos	Canal de Isabel II y Adjudicatario
Seguimiento y actualización de la planificación de evolutivos	Canal de Isabel II y Adjudicatario
Diseño y análisis técnico	
Análisis del diseño funcional incluyendo aspectos de Seguridad y Privacidad	Adjudicatario
Diseño técnico de la solución incluyendo aspectos de Seguridad y Privacidad	Adjudicatario
Preparar una descripción del entorno técnico para las aplicaciones, del servidor/host y de la estación de trabajo necesaria para soportar la aplicación desarrollada, de los entornos de pruebas y de producción y de los niveles de servicio asociados, en consonancia con la infraestructura de Canal de Isabel II y sus procesos	Adjudicatario
Realizar o actualizar la documentación (de usuario, explotación, administración y monitorización)	Adjudicatario
Aprobación del diseño técnico y de la descripción del entorno de producción incluyendo aspectos de Seguridad y Privacidad	Canal de Isabel II
Desarrollo	

Grupo de actividad	Ejecución de actividades
Crear, preparar, organizar, programar y documentar los desarrollos en las aplicaciones según el diseño funciona y diseño técnico	Adjudicatario
Realizar o actualizar la documentación (de usuario, explotación, administración y monitorización)	Adjudicatario
Aprobación del desarrollo	Canal de Isabel II
Pruebas Técnica (unitarias y de sistema)	
Realizar pruebas unitarias para comprobar que las unidades individuales de código fuente están funcionando correctamente. Una unidad es la parte más pequeña comprobable de una aplicación	Adjudicatario
Almacenar las pruebas unitarias en un repositorio de pruebas unitarias separado para permitir la reutilización	Adjudicatario
Realizar pruebas sobre un sistema completo para evaluar su rendimiento: pruebas de carga, pruebas de volumen, pruebas de estrés y pruebas de regresión	Adjudicatario
Documentación de las pruebas técnicas	Adjudicatario
Realizar o actualizar la documentación (de usuario, explotación, administración y monitorización)	Adjudicatario
Aprobación de las pruebas técnicas	Canal de Isabel II
Pruebas funcionales y de integración	
Revisar la descripción del entorno técnico definida en la fase de diseño y análisis técnico	Adjudicatario
Asegurar que el equipo que suministra los servicios de línea base tiene las habilidades necesarias para mantener la aplicación	Adjudicatario
Revisar los resultados de cada fase del proceso de desarrollo (cualquier deficiencia debe ser documentada y tratada antes de la aceptación formal de la solicitud de mantenimiento)	Adjudicatario
Asegurar que las deficiencias detectadas durante las pruebas unitarias y pruebas de sistema han sido tratadas	Adjudicatario
Elaboración y actualización de la documentación final y de los scripts de despliegue	Adjudicatario
Aprobación para el despliegue en el entorno de integración	Canal de Isabel II
Despliegue en el entorno de pruebas de integración	Canal de Isabel II
Realizar pruebas funcionales y de integración de la aplicación en los sistemas de Canal de Isabel II	Adjudicatario

Grupo de actividad	Ejecución de actividades
Documentación de las pruebas de integración	Adjudicatario
Realizar o actualizar la documentación (de usuario, explotación, administración y monitorización)	Adjudicatario
Aprobación para las pruebas de usuario	Canal de Isabel II
Pruebas de aceptación de usuarios	
Realizar pruebas para obtener la confirmación por el cliente, a través de ensayo o examen, que la modificación o adición cumple con los requisitos acordados mutuamente	Canal de Isabel II
Despliegue en el entorno de producción	Canal de Isabel II
Auditorias de Seguridad y Privacidad	
Realizar auditorías de Seguridad y Privacidad para detección de requisitos de Seguridad y Privacidad incumplidos.	Canal de Isabel II
Subsanación de incumplimientos de requisitos de Seguridad y Privacidad incumplidos.	Adjudicatario

2.1.9.2 Responsabilidades en actividades funcionales

Canal de Isabel II mantiene el gobierno de todos los procesos, lo que significa que establece las directrices y objetivos para la ejecución de los procesos y define los mecanismos de monitorización para asegurar el cumplimiento de tales directrices y objetivos. La ejecución de las actividades será responsabilidad de Canal de Isabel II o del Adjudicatario. La tabla siguiente muestra las responsabilidades sobre el gobierno y ejecución de cada proceso.

Proceso	Gobierno del proceso	Ejecución de actividades
Planificación Estratégica	Canal de Isabel II	Canal de Isabel II y Adjudicatario
Gestión de Clientes	Canal de Isabel II	Canal de Isabel II
Planificación de Servicios (Demanda y Catálogo de Servicios)	Canal de Isabel II	Canal de Isabel II
Gestión de la Seguridad	Canal de Isabel II	Canal de Isabel II y Adjudicatario

Proceso	Gobierno del proceso	Ejecución de actividades
Gestión de la Continuidad	Canal de Isabel II	Canal de Isabel II
Gestión de la Disponibilidad	Canal de Isabel II	Canal de Isabel II y Adjudicatario
Gestión de la Capacidad	Canal de Isabel II	Canal de Isabel II y Adjudicatario
Gestión Financiera	Canal de Isabel II	Canal de Isabel II
Desarrollo y Pruebas de Servicio	Canal de Isabel II	Canal de Isabel II y Adjudicatario
Paso a Producción	Canal de Isabel II	Canal de Isabel II y Adjudicatario
Gestión de Operaciones	Canal de Isabel II	Canal de Isabel II y Adjudicatario
Gestión de Problemas	Canal de Isabel II	Canal de Isabel II y Adjudicatario
Gestión de Incidencias	Canal de Isabel II	Canal de Isabel II y Adjudicatario
Gestión de Peticiones	Canal de Isabel II	Canal de Isabel II y Adjudicatario
Gestión del Conocimiento	Canal de Isabel II	Canal de Isabel II y Adjudicatario
Gestión de Niveles de Servicio	Canal de Isabel II	Canal de Isabel II y Adjudicatario
Gestión de Cambios	Canal de Isabel II	Canal de Isabel II y Adjudicatario
Gestión de la Configuración	Canal de Isabel II	Adjudicatario

Seguidamente mostramos el detalle de la responsabilidad de las actividades para los procesos cuya ejecución es completamente por parte del Adjudicatario o de manera compartida por el Adjudicatario y Canal de Isabel II.

La descripción de responsabilidades se realiza mediante una matriz de RACI, donde:

- R: significa responsable de ejecutar la actividad (*Responsible*). Es el ejecutor de la actividad. Si para una actividad hay más de una “R” significa que los roles implicados ejecutan esa actividad de manera consensuada.
- A: significa responsable final (*Accountable*). Es el responsable último de la actividad, aquel al que se debe rendir cuentas sobre el cumplimiento de la actividad. Canal de Isabel II, al tener el gobierno de todos los procesos es dicho responsable

último para todas las actividades, por lo que en esta matriz no se especifica dicha responsabilidad.

- I: significa informado del resultado de la actividad.
- C: significa que el rol debe ser consultado para que se ejecute la actividad.

Proceso	Actividad	Canal de Isabel II	Adjudicatario
PLANIFICACIÓN ESTRATÉGICA	Recopilación y propuesta de necesidades de negocio	R	I
	Recopilación y propuesta de necesidades en sistemas	I	R
	Definición de objetivos de Sistemas de Información	R*	I
	Definición del Plan de Estratégico	R*	I
	Comunicación del Plan Estratégico	R*	I
	Seguimiento del Plan Estratégico	R*	I
GESTIÓN DE LA DISPONIBILIDAD	Definición del Plan de Disponibilidad	R*	
	Diseño de la recuperación de servicios	R*	
	Realizar pruebas de disponibilidad	R*	I
	Mantener el Plan de Disponibilidad	R*	
	Monitorizar la disponibilidad	R*	I
	Realizar informes de disponibilidad	R*	
GESTIÓN DE LA CAPACIDAD	Definición del Plan de Capacidad	R*	I
	Mantener el Plan de Capacidad	R*	
	Realizar pruebas de capacidad	R*	
	Realizar informes de capacidad	R*	
	Analizar tendencias de capacidad	R*	
GESTIÓN DE PROBLEMAS	Definir, construir, probar e implantar soluciones temporales (*workarounds*)	I	R
	Mantener base de datos de errores conocidos	I	R
	Detección de problemas	I	R
	Registro de problemas	I	R
	Investigación y diagnóstico de problemas	I	R
	Registro de error conocido	I	R
	Soporte y comunicación de errores conocidos	I	R

Proceso	Actividad	Canal de Isabel II	Adjudicatario
	Cierre de problemas	R	I
	Revisión de problemas mayores	I	R
	Producir informes de gestión	I	R
GESTIÓN DE INCIDENCIAS	Definir procedimiento de clasificación, priorización y escalado	R	C/I
	Registro de incidencia	R	I
	Resolución en Nivel 1 por Service Desk de Canal de Isabel II (*)	R	I
	Escalado a Nivel 2 Service Desk Canal de Isabel II (*)	R	I
	Resolución en Nivel 2 por Service Desk de Canal de Isabel II (*)	I	R
	Escalado a Nivel 3 por Service Desk de Canal de Isabel II (*)	I	R
	Resolución en Nivel 3	I	R
	Monitorizar el progreso de la incidencia	I	R
	Cerrar incidencia	R	I
	Producir informes de gestión	I	R
	(*) Sólo aplica para el caso en el que Canal de Isabel II disponga de un servicio de Service Desk para la resolución de incidencias de Nivel 1 y/o Nivel 2. En ese caso, el adjudicatario será responsable del Nivel 3 de resolución. En caso de no disponer de Service Desk, la resolución será siempre responsabilidad del adjudicatario, tal como aparece en la línea “Resolución en Nivel 3” anterior.		
GESTIÓN DE PETICIONES	Definir procedimiento de clasificación, priorización y escalado	R	C/I
	Crear lista de peticiones de servicio	R	I
	Registro de peticiones	R	I
	Revisar, aprobar y priorizar peticiones	R	I
	Ejecutar petición (instalar, añadir, cambiar, quitar)	I	R
	Monitorizar el progreso de la petición	I	R
	Cierre de la petición	R	I
	Producir informes de gestión	I	R

Proceso	Actividad	Canal de Isabel II	Adjudicatario
GESTIÓN DE CONOCIMIENTO	Definir el conocimiento para ser capturado	R	R
	Construir y mantener bases de datos de conocimiento	I	R
	Transferir conocimiento	I	R
GESTIÓN DE NIVELES DE SERVICIO	Definir ANS	R	C/I
	Definir requisitos para nuevos servicios	R	C
	Revisar ANS	R	C
	Monitorizar el rendimiento de los servicios respecto a los ANS	I	R
	Medir la satisfacción del cliente	R	I
	Producir informes de cumplimiento de ANS	I	R
	Definir plan de mejora del servicio	C/I	R
GESTIÓN DE CAMBIOS	Definición de procedimiento de gestión de cambios	R	I
	Crear RFC	R	I
	Registro de RFC	I	R
	Evaluación del cambio (análisis de esfuerzo e impacto)	C/I	R
	Organizar CAB	R	C
	Autorización del cambio (CAB)	R	I
	Coordinar la implementación del cambio	R	C
	Revisar y cerrar el cambio	R	I
	Producir informes de gestión	I	R
GESTIÓN DE LA CONFIGURACIÓN	Verificación y auditoría	R	C
	Registro de elementos de configuración	I	R
	Mantenimiento de elementos de configuración	R	
	Control de elementos de configuración	R	I
	Producir informes de gestión y estado de la CMDB	R	

* Las actividades en las que Canal de Isabel II aparece como responsable no son de obligado cumplimiento, siendo por lo tanto su realización un derecho y no una obligación.

2.1.9.3 Gestión del conocimiento

Si bien el Adjudicatario es responsable ciertas actividades, e incluso de procesos completos, dentro del servicio, Canal de Isabel II desea disponer de una gestión del conocimiento que le permita gobernar la actividad del Adjudicatario y garantizar un traspaso sin pérdida de servicio. El licitador habrá de identificar de forma expresa en el Plan de Gestión de la Comunicación del Plan de Proyecto las acciones concretas que va a realizar para dicha gestión del conocimiento, en particular:

- Roles y responsabilidades del Adjudicatario y de Canal de Isabel II implicados en la gestión del conocimiento (matriz de comunicación).
- Repositorios para la gestión del conocimiento y su acceso por Canal de Isabel II.
- Tipo de información y métodos de aprobación para el manejo de la información.

2.2. Perfiles requeridos

El licitador habrá de identificar de forma expresa en el Plan de Gestión de Recursos del Plan de Proyecto el equipo ofertado responsable de los trabajos relacionados con la fase de pleno servicio.

El licitador deberá proporcionar las características de los equipos de trabajo debidamente detallados, especialmente el personal clave definido en este apartado, incluyendo para cada uno:

- 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 servicio por cada categoría profesional.
- Declaración expresa del cumplimiento de los requisitos técnicos y laborales exigidos en el apartado 5 del anexo I del PCAP.

Para acreditar la solvencia deberá presentarse lo indicado en el apartado 5.2 del PCAP.

El Adjudicatario deberá asegurar la disponibilidad de un recurso técnico especializado en redes de datos y comunicación, que se responsabilice, en el ámbito de la prestación del servicio asociado al proyecto, de la configuración y mantenimiento de la parte de la infraestructura de comunicaciones entre el Adjudicatario y Canal de Isabel II que sea responsabilidad del Adjudicatario. Dicho técnico será el responsable por parte del Adjudicatario de participar en la resolución de incidencias en las comunicaciones que requieran de actuación o revisión conjunta entre el Adjudicatario y Canal de Isabel II, SA. En caso de que el contrato sea adjudicado a una UTE, se definirá igualmente y a nivel de proyecto, un único interlocutor en este ámbito.

Los perfiles técnicos requeridos deberán incluirse como solvencia técnica en el apartado 5 del Anexo I del PCAP. Así mismo, deberá incluirse en dicho apartado la necesidad de

disponer, para su presentación en el momento de la constitución del equipo, de certificación para cada componente de pertenencia a la plantilla del Adjudicatario o empresas subcontratadas indicadas en la oferta.

El Adjudicatario deberá haber constituido el equipo de trabajo al inicio de los trabajos. En caso contrario el Adjudicatario incurrirá en la penalización correspondiente como queda reflejado en el apartado 9 del Anexo I del PCAP.

Para la conformidad definitiva por parte de Canal de Isabel II de los equipos del servicio, el Adjudicatario presentará a Canal de Isabel II los certificados técnicos y laborales requeridos en el apartado 5 del Anexo I del PCAP.

Canal de Isabel II considera un factor clave para el éxito del servicio la permanencia de ciertos roles para la ejecución de algunas tareas, denominadas personal clave, que tendrán las siguientes funciones:

- Toda comunicación formal se realizará a través de dichas personas clave. Estas personas clave serán necesarias al nivel apropiado para consensuar los acuerdos respecto, pero no limitado, a solicitudes de cambio, niveles de servicio, penalizaciones.
- El Adjudicatario asegurará que cada componente del personal clave es asignado para la entrega de los servicios establecidos en este contrato durante un período de al menos un año y medio. Durante este periodo Canal de Isabel II y el Adjudicatario deberán adoptar todas las medidas razonables para asegurar los servicios del personal clave.
- En caso de producirse cambios en el personal clave, éstos deberán ser acordados previamente con Canal de Isabel II.
- En el supuesto de que un componente del personal clave no pueda estar disponible por causa imprevista, el Adjudicatario deberá disponer de una persona alternativa en un plazo de 5 días con plenas competencias para entregar el servicio.

Se considera personal clave del Adjudicatario los roles caracterizados como tales en el Subapartado 5.1 B) del Anexo I del PCAP.

Además, si bien entiende que la gestión de su personal es responsabilidad del Adjudicatario, se desea mantener un nivel de rotación de personal limitado, con el fin de ayudar a evitar riesgos en la entrega de los servicios.

La composición de los equipos de trabajo no podrá ser modificada sin el consentimiento expreso de Canal de Isabel II. Cualquier modificación en los equipos de trabajo suscitada por el Adjudicatario requerirá las siguientes condiciones:

- Justificación escrita, detallada y suficiente, explicando el motivo que suscita el cambio con un plazo mínimo de quince (15) días de preaviso.
- Presentación de sustitutos con un perfil de cualificación técnica y experiencia igual o superior al de la persona que se pretende sustituir, junto con las certificaciones técnica y laboral exigidas para la prestación de los servicios incluidos en este contrato.

- Verificación por parte de Canal de Isabel II del cumplimiento de los requisitos de cualificación técnica y experiencia exigidos en este contrato y, en caso positivo, aceptación de los sustitutos.
- El Adjudicatario dispone de un plazo máximo de quince (15) días para sustituir el recurso desde la fecha de la baja del mismo en el equipo, transcurrido el cual el Adjudicatario incurrirá en la penalización correspondiente indicada en el apartado 9 del Anexo I del PCAP.

El Adjudicatario deberá facilitar en su propuesta los Currículos de las personas que asignará para las posiciones de dirección y coordinación de este servicio y del personal clave definido, y currículos genéricos que definan los perfiles del personal técnico que formará los equipos de trabajo.

Los datos se detallarán en el formulario adjunto como Anexo 1 del presente documento. Se debe incluir una tabla con la distribución de perfiles asignados.

Se requiere que el licitador indique en la oferta, en su caso, la parte del contrato que tengan previsto subcontratar, señalando su importe, y el nombre o el perfil empresarial, definido por referencia a los criterios de selección cualitativa establecidos en el apartado 5 del Anexo I del PCAP, de los subcontratistas a los que vaya a encomendar su realización, esta exigencia deberá incluirse expresamente en el apartado 10.3 del anexo I del PCAP. En este caso, los subcontratos que no se ajusten a lo indicado en la oferta, por celebrarse con empresarios distintos de los indicados nominativamente en la misma o por referirse a partes de la prestación diferentes a las señaladas en ella, no podrán celebrarse hasta que transcurran veinte días desde que se hubiese cursado la notificación y aportación de las justificaciones correspondientes, siempre que el Canal de Isabel II no hubiese notificado dentro de ese plazo su oposición a los mismos.

Este régimen será igualmente aplicable si los subcontratistas hubiesen sido identificados en la oferta mediante la descripción de su perfil profesional (ver cláusula 25 del PCAP).

Ante cualquier cambio del equipo, el solapamiento de recursos para la transferencia del conocimiento no generará coste alguno para Canal de Isabel II.

2.3. Administración, Ubicación y Horario

2.3.1. Administración

Las labores de configuración de equipos y administración de sistemas en los entornos de desarrollo, calidad y producción de Canal de Isabel II serán realizados por personal del Área de Infraestructura Tecnológica que podrá solicitar soporte del Adjudicatario que documentará adecuadamente todas las tareas de administración necesarias.

El Adjudicatario deberá cumplir todos los procedimientos de trabajo fijados por Canal de Isabel II para la adecuada coordinación de las labores de desarrollo, mantenimiento funcional y administración de los sistemas y participará de forma activa en la mejora de los procedimientos definidos.

2.3.2. Ubicación física de los recursos

De manera general, las tareas a realizar en el marco del proyecto para la consecución de los objetivos se realizarán en las dependencias de la empresa adjudicataria, excepto aquellos trabajos que, por su naturaleza, requieran ser ejecutados en las dependencias de Canal de Isabel II.

En el caso que los trabajos se realicen en las instalaciones del Adjudicatario, los costes derivados de las posibles conexiones necesarias con Canal de Isabel II serán por cuenta del Adjudicatario.

El Adjudicatario utilizará sus propios equipos y servidores y sus propias licencias de uso de las herramientas de desarrollo necesarias para la ejecución de los trabajos objeto de este pliego. También usará sus propias licencias de las herramientas de gestión de servicio que se utilicen. Actualmente en Canal de Isabel II está implementada una solución basada en la herramienta CA Service Desk.

Canal de Isabel II podrá solicitar al Adjudicatario la realización de determinados trabajos puntuales de forma presencial.

Al tener que prestarse obligatoriamente el servicio se prestará de forma remota, el Adjudicatario ubicará sus grupos de trabajo en instalaciones propias dotadas de las infraestructuras de comunicaciones, elementos de seguridad lógica y física, espacios habilitados para los recursos humanos y recursos según las normativas vigentes.

La ubicación física de los recursos humanos deberá ser una sala cerrada, con acceso restringido mediante tarjeta identificadora u otro medio similar y deberá contar con los medios técnicos necesarios para la prestación del servicio a cuenta del Adjudicatario (ordenadores, central telefónica, equipos de videoconferencia, etc.

El Adjudicatario proporcionará un número de teléfono convenientemente dimensionado para proporcionar soporte telefónico.

En caso necesario se demandará un soporte presencial por lo que el Adjudicatario debe garantizar su disponibilidad presencial para ofrecer dicho soporte. Las actividades típicas que pueden requerir soporte presencial son:

- Soporte a pruebas
- Formación sobre funcionalidades de la herramienta
- Reuniones de coordinación con otros equipos
- Reuniones con usuarios finales

En el caso de que no se encuentre activo el servicio de soporte extendido, Canal de Isabel II incluye en el alcance de este contrato la posibilidad de realizar hasta 4 intervenciones anuales por sistema para la realización de trabajos excepcionales fuera del horario habitual (fines de semana, prolongación de la jornada laboral más allá de las 22:00h, festivos, etc.).

El uso de estas jornadas se realizará a solicitud de Canal de Isabel II para trabajos que por su naturaleza deban realizarse fuera de horario y con cargo a la bolsa de puntos tarea:

- Aplicación y Validación de parches
- Procesos masivos (cargas y/o extracciones)
- Fallos críticos en procesos críticos de Canal de Isabel II producidos fuera de horario o más allá de los niveles de servicio pactados

2.3.3. Horario

El horario para la prestación de los servicios asociados aparece descrito en el Apartado 7 – Soporte Extendido y Horario dentro del Anexo 5. Dicho horario se rige en base al calendario de festivos autonómicos de la Comunidad de Madrid. Todas las fiestas locales de todos los municipios de la Comunidad de Madrid deberán estar cubiertas por el servicio.

2.4. Acuerdos de nivel de servicio

Se entiende por Acuerdos Nivel de Servicio (ANS), los parámetros que serán necesario cumplir para considerar que el Adjudicatario cumple con sus compromisos. El Adjudicatario puede proponer valores diferentes o parámetros adicionales, justificando convenientemente su inclusión y con un detalle similar al menos al que se marcan los aquí descritos. Canal de Isabel II, a su único criterio, podrá considerar o no los cambios sugeridos por el Adjudicatario.

Para la medición de los niveles de servicio se establecen los indicadores de objetivo que se indican en este apartado. Adicionalmente se establecen otros indicadores (indicadores de rendimiento) para realizar un seguimiento de la actividad.

El Adjudicatario deberá satisfacer los niveles de servicio establecidos según los indicadores de objetivo. Si al finalizar un periodo de monitorización no se ha cumplido un indicador el Adjudicatario deberá establecer medidas correctoras.

El Adjudicatario proporcionará mensualmente un informe a Canal de Isabel II para verificar el cumplimiento del Adjudicatario con los niveles de servicio establecidos a través de los indicadores de objetivo. Este informe podrá ser publicado en panel electrónico propiedad del Adjudicatario. El Adjudicatario, en este caso, dará acceso a este panel a Canal de Isabel II mediante usuario y contraseña.

El Adjudicatario utilizará las herramientas de Canal de Isabel II disponibles en cada momento, pudiéndose complementar con sistemas auxiliares o toma de datos específicos según sea necesario.

Canal de Isabel II podrá adoptar, a su único criterio, las herramientas que el Adjudicatario proponga implantar para facilitar esta monitorización activa, en el supuesto de que Canal

de Isabel II no pueda medir el cumplimiento de ANS por sus propios medios. La funcionalidad y alcance de tales herramientas deberán ser detallados en su propuesta (incluyendo ejemplos ilustrativos) en el Plan de Gestión del Alcance del Plan de Proyecto.

Canal de Isabel II podrá en todo momento auditar la información facilitada por el Adjudicatario, así como las fuentes de datos.

En caso de fallo en la provisión de los Servicios de acuerdo con los niveles de servicio acordados, el Adjudicatario incurrirá en una penalización, que tiene como objetivo una compensación económica que refleje que ha entregado los Servicios con un nivel de servicio inferior al comprometido, como se explica en el apartado 9 del anexo I del PCA.

Se establecerán varios Tramos de Control para la medida del cumplimiento de los compromisos de calidad. Cada Tramo viene definido por un valor contra el que comparar el valor obtenido por el Adjudicatario, tal como se muestra en la siguiente figura:

	Tramo de cumplimiento (V_C)	
	Tramo de atención (V_a)	Penalidad aplicable
	Tramo de incumplimiento (V_i)	
	Tramo de incumplimiento grave	

Si el valor medido es igual o mayor al definido en el Tramo de Cumplimiento (Vc), se considerará que el Adjudicatario ha entregado el servicio conforme a los compromisos contractuales. Por debajo de dicho valor, se considerará que el Adjudicatario ha incumplido con los objetivos requeridos, por lo que Canal de Isabel II podrá aplicar la penalización correspondiente al Tramo de Control en el que se situé el valor obtenido. Si el valor medido es igual o inferior al definido en el Tramo de incumplimiento (Vi) se considerará que el Adjudicatario ha incurrido en Incumplimiento Grave.

Con el fin de diferenciar la criticidad de los Parámetros del ANS, y focalizar la atención sobre aquellos aspectos críticos del Servicio, cada uno de ellos tendrá definido un Peso o prioridad, que se fija en el presente pliego por Canal de Isabel II. Este valor, como se explica más adelante, forma parte de la fórmula de cálculo de la penalización. Canal de Isabel II podrá variar estas prioridades a lo largo del Servicio, a su único criterio, con la única limitación de un máximo de 2 cambios anuales, que deberá notificar e informar convenientemente al Adjudicatario con una antelación mínima de dos meses.

En el Apartado 6 – Acuerdos de Nivel de Servicio dentro del Anexo 5, se indican los ANS de este servicio.

Las penalizaciones por incumplimiento en parámetros generales, se calculará conforme a la siguiente fórmula:

$$\mathbf{R_{pc} = [0{,}35 * F_T] * F_t * (P_{pc} / P_T)}$$

Donde:

R_{pc}, Penalización aplicable por el incumplimiento del Parámetro

F_T, Facturación total, por todos los conceptos, correspondiente al periodo medido

F_t, Factor Corrector del Tramo en el que se produce el incumplimiento. Los valores iniciales definidos para cada Tramo son los siguientes:

Atención = 0,75

Incumplimiento = 1

Incumplimiento Grave = 1,5

En caso de reiteración en el incumplimiento de un Parámetro en dos meses consecutivos, el segundo mes se aplica el valor del **F_t** correspondiente al tramo inmediatamente superior al que correspondería

P_{pc}, Peso definido para el Parámetro de Control

P_T, Suma de todos los Pesos de los Parámetros de Control que definen el ANS del Servicio

La penalización, será la suma de las penalizaciones correspondientes a los incumplimientos de los parámetros. En el caso de que el cálculo anterior suponga un valor mayor que el 35% del total facturado por todos los conceptos en el periodo medido, se aplicará esta última cantidad.

Independientemente de las Penalizaciones que sean de aplicación, el Adjudicatario deberá elaborar e implementar sin coste adicional para Canal de Isabel II, un **Plan de Acciones Correctivas** (“PAC”) para todos los incumplimientos de los Parámetros de control del ANS.

2.5. Entregables

El adjudicatario documentará los trabajos realizados, y actualizará la documentación existente, tanto técnica como de usuario, como consecuencia de estos. Esta documentación deberá ser aceptada por Canal de Isabel II.

Toda la documentación entregada deberá ser aprobada por Canal de Isabel II para su aceptación en cuanto a calidad y completitud. En caso de no ser aprobado, Canal de Isabel II devolverá el documento presentado al adjudicatario para su revisión y subsanación. Este proceso se repetirá tantas veces como sea necesario. La fecha definitiva de entrega del documento a efectos de cumplimiento del ANS será la de la entrega en la que Canal de Isabel II da la aprobación.

La documentación generada durante la ejecución del contrato es de propiedad exclusiva de Canal de Isabel II sin que el adjudicatario pueda conservarla, ni obtener copia de esta o facilitarla a terceros sin la expresa autorización de Canal de Isabel II.

Toda la documentación se entregará en español y en formato electrónico. El adjudicatario deberá suministrar Canal de Isabel II las nuevas versiones de la documentación que se vayan produciendo.

Adicionalmente, el Adjudicatario deberá presentar a lo largo del periodo de este los siguientes documentos:

2.5.1. Documentación

2.5.1.1 Previo al inicio de los trabajos

RD101. El Adjudicatario deberá presentar para su aprobación antes del inicio de los trabajos un Plan de Gestión de Proyecto según los requisitos establecidos en el apartado “Alcance del Servicio Licitado” incluido en este mismo pliego.

2.5.1.2 Durante la fase de Pleno Servicio del **proyecto**

RD102. Plan de Gestión del servicio. En este caso, Canal de Isabel II deberá aprobar la documentación recibida en cuanto a calidad y completitud. En caso de no ser aprobado, Canal de Isabel II devolverá el PGP al Adjudicatario para su revisión y subsanación. Este proceso se repetirá tantas veces como sea necesario. La fecha definitiva de entrega del PGP a efectos de cumplimiento del ANS será la de la entrega en la que Canal de Isabel II da la aprobación.

RD103. Informes periódicos de seguimiento del servicio y cumplimiento de ANS. Estos informes se realizarán, con carácter general, trimestralmente, si bien Canal de Isabel II los podrá solicitar puntualmente con menor frecuencia.

RD104. Plan de Devolución del Servicio. Este documento se mantendrá actualizado a lo largo de la vida del contrato.

2.6. Otros requisitos

RO101. Canal de Isabel II se reserva el derecho de contratar un tercero como asesor independiente para la revisión de los ANS, si procede. El objetivo de esta asesoría será verificar la entrega de los servicios y la adecuación de los ANS a cambios en la organización e infraestructura de Canal de Isabel II, o bien originados por posibilidades brindadas por nuevas tecnologías. Canal de

Isabel II se compromete a que la empresa tercera no sea un competidor directo del Adjudicatario.

2.7. Gestión del conocimiento

Si bien el Adjudicatario es responsable de ciertas actividades, e incluso de procesos completos, dentro del proyecto, Canal de Isabel II desea disponer de una gestión del conocimiento que le permita gobernar la actividad del Adjudicatario y garantizar un traspaso sin pérdida de servicio. El licitador habrá de identificar de forma expresa en el Plan de Gestión de la Comunicación del Plan de Proyecto las acciones concretas que va a realizar para dicha gestión del conocimiento, en particular:

- Roles y responsabilidades del Adjudicatario y de Canal de Isabel II implicados en la gestión del conocimiento (matriz de comunicación).
- Repositorios para la gestión del conocimiento y su acceso por Canal de Isabel II.
- Tipo de información y métodos de aprobación para el manejo de la información.

2.8. Ejecución de Pruebas y Control de Calidad

De cara a agilizar el servicio y asegurar la calidad del mismo, Canal de Isabel II se reserva el derecho a contratar los servicios de Ejecución de Pruebas y Control de Calidad de los servicios entregados mediante un tercero, actuando dicho tercero en ese caso en representación de Canal de Isabel II.

Asimismo, Canal de Isabel II podrá utilizar herramientas para el Control de la Calidad y la Seguridad del Software entregado. La utilización de dichas herramientas podrá permitir a Canal de Isabel II rechazar entregas de trabajos que no cumplan con los mínimos requisitos de calidad y seguridad establecidos por Canal de Isabel II.

2.9. 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 siguientes consideraciones de conectividad y seguridad incluidas dentro del Anexo 5 del presente documento.

3. 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.

3.1. 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.

3.2. Gestión de la Relación

Para la gestión de la relación se tendrán presentes los siguientes principios que se consideran clave para el éxito de este proyecto:

- Asegurar que se dispone de la necesaria flexibilidad para responder a los cada vez más rápido cambios en el entorno de negocio de Canal de Isabel II
- Asegurar que la relación definida incluye de forma proactiva la innovación TIC y que esta se traduce en beneficios para Canal de Isabel II.

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

3.2.1. 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.

3.2.2. 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**	▪ 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.	▪ Director ejecutivo (capacitado para asegurar el nivel de decisión y compromiso que requieren las decisiones estratégicas) (*)	▪ Gestor Estratégico (capacitado para asegurar el nivel de decisión y compromiso que requieren las decisiones estratégicas)

(*) Rol que preside el Comité

3.2.3. Comité de Seguimiento y control

Frecuencia	Comité	Responsabilidades	Asistentes	
			Canal de Isabel II	Adjudicatario
Mensual	**Seguimiento y control**	▪ Asegurar que se consiguen los niveles de calidad acordados y, que en el caso de deficiencias no	▪ Director / Jefe de Proyecto (*)	▪ Responsable del Servicio/ Proyecto

Frecuencia	Comité	Responsabilidades	Asistentes	
			Canal de Isabel II	Adjudicatario
(o a petición de cualquiera de las partes)		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 Adjudicatario para todos los asuntos relacionados nivel de gestión táctico del Servicio ▪ Controlar que la facturación se está realizando conforme a los		

Frecuencia	Comité	Responsabilidades	Asistentes	
			Canal de Isabel II	Adjudicatario
		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

3.2.4. Comité Operacional

Frecuencia	Comité	Responsabilidades	Asistentes	
			Canal de Isabel II	Adjudicatario
Semanal/ A petición de cualquiera de las partes	**Operativo**	▪ 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	▪ Jefe de Proyecto / Responsable Operativo (*)	▪ Jefe de Proyecto / Responsable Operativo

Frecuencia	Comité	Responsabilidades	Asistentes	
			Canal de Isabel II	Adjudicatario
		▪ 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

3.3. 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. Para ello debe completar adecuadamente el **apartado 3.1.1.4 Verificación y Control del Alcance del Plan de Gestión del Alcance, dentro del Plan de Gestión del Proyecto**. 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

3.4. 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 cumplimento 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.

3.5. 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.

4. FASES DEL CONTRATO

El licitador presentará un plan general de desarrollo e implantación donde se indiquen los principales hitos con tareas y entregables por cada una de las distintas fases del proyecto.

Al comienzo del proyecto el Adjudicatario presentará un plan detallado para la prestación de los servicios en sus diferentes fases, que serán las siguientes:

- Pleno Servicio.
- Devolución.

4.1. Fase de Pleno Servicio

El servicio se seguirá prestando con responsabilidad del Adjudicatario, tal como se hacía en la fase anterior.

Se incorporarán de mutuo acuerdo las adaptaciones al modelo que se consideren oportunas en virtud de las lecciones aprendidas en los meses de rodaje previos. La mayoría de las actividades se realizarán en las instalaciones del Adjudicatario, a excepción de aquéllas que requieran interacción con el personal de Canal de Isabel II o sean acordadas entre las partes.

Los ANS revisados y acordados en la fase de transición entrarán en pleno funcionamiento, incluido el esquema de penalizaciones aplicándose una cuantía del 100%.

4.2. 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.

4.2.1. Principios clave

El objetivo del Plan de Devolución es permitir la finalización del contrato y la transferencia de todos los servicios a Canal de Isabel II y a un nuevo Adjudicatario de dichos servicios

El Adjudicatario deberá, en un plazo de seis (6) meses a partir del comienzo de la fase de Pleno Servicio, producir un borrador del Plan de Devolución, que estará basado en los principios establecidos en este documento.

El Plan de Devolución detallará los tipos de procesos y actividades que el Adjudicatario

prestará para la finalización ordenada, con la mínima alteración material para el negocio de Canal de Isabel II, de los servicios del Adjudicatario a Canal de Isabel II o cualquier Adjudicatario sustituto en caso de cualquier finalización o vencimiento de este contrato por cualquier motivo.

En un plazo de 30 días a partir del envío del borrador del Plan de Devolución, las partes deberán reunirse y realizar todos los esfuerzos para acordar definitivamente el contenido y forma del Plan de Devolución definitivo.

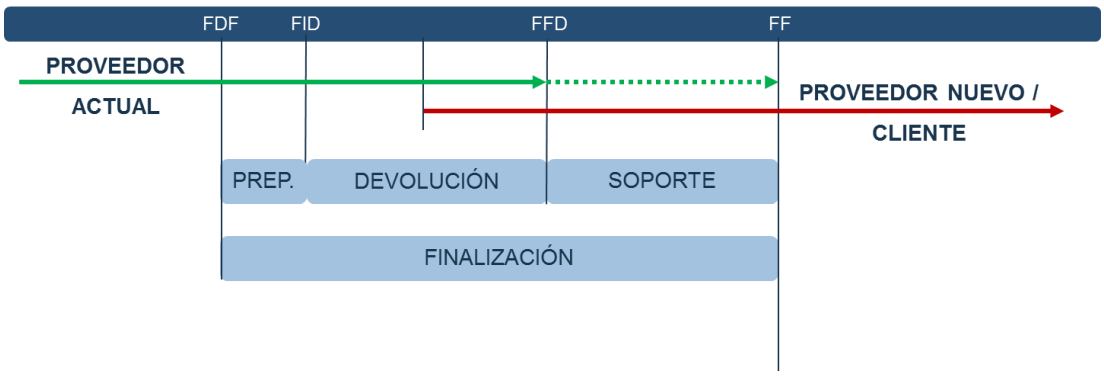
El Plan de Devolución deberá cubrir las siguientes cuestiones con detalle:

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 soporte
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.

4.2.2. 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.

4.2.3. 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, software y licencias, bases de datos y datos, documentación, ajustes de instalaciones, contratos y acuerdos de terceros, así como personal, en uso para la prestación de los servicios, que se transferirán a petición de Canal de Isabel II durante la finalización y antes de la Fecha de Inicio de la Devolución. 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:

- 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 licenciatarios 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 licenciatarios 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 conocimientos. El Adjudicatario dedicará tiempo y recursos razonables durante la transición de finalización a garantizar la adecuada transferencia de conocimiento. La transferencia de conocimiento deberá incluir (sin limitación):
  - La transferencia de todo el conocimiento relacionado con la provisión de los servicios a Canal de Isabel II o a un Adjudicatario sustituto.
  - La transferencia de todos los errores conocidos y soluciones provisionales relacionados con la provisión de los servicios a Canal de Isabel II o a un Adjudicatario sustituto.
  - La base de conocimientos necesaria para el centro de atención al usuario.
  - Las respuestas a todas las preguntas razonables, formuladas por Canal de Isabel II o el Adjudicatario sustituto, hasta la Fecha de Devolución.

4.2.4. 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.

4.2.5. 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	▪ 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	▪ Gestor Estratégico (*) ▪ Responsable de la Finalización	▪ 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	▪ 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.	▪ Responsable de la Finalización (*) ▪ Gestor Operativo	▪ 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.

4.2.6. 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.

4.2.7. 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.

4.2.8. 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.

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 Devolución 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 Devolución.

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.

4.2.9. 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.

5. 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**.

6. 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.

Madrid, 6 de mayo de 2020

Firma: Rafael Egido Blández
COORDINADOR DE APLICACIONES

Firma: Alberto Villacián Fernández
JEFE ÁREA APLICACIONES INFORMÁTICAS

Firma: Ángel Rodríguez García
SUBDIRECTOR SISTEMAS INFORMÁTICOS

Firma: Pablo Galán González
DIRECTOR RECURSOS

El presente documento ha sido por el procedimiento establecido al efecto en la fecha indicada en el mismo

ANEXO 1. CUESTIONARIO PERSONAL

Cuestionario por persona del equipo propuesto.

Apellidos, Nombre - identificador	
Categoría ofertada	

Antigüedad en la empresa, antigüedad en la categoría y experiencia en T.I.

Empresa	Categoría	F-alta	F-baja	Meses	Actividad Informática

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

Proyecto	Empresa	Categoría	F-inicio	F-fin	Descripción funciones realizadas

Tal y como se explica en el apartado 5 del anexo 1 del PCAP, además de los CV es preciso completar la **matriz** siguiente, especificando las áreas de conocimiento que cada persona cubre, certificaciones obligatorias con las que cuenta y años de experiencia en implantaciones o servicios de mantenimiento de productos SAP.

Persona Propuesta	Área conocimiento cubierta	Certificaciones obligatorias	Experiencia exigida en esta área de conocimiento	Experiencia acreditada por el Miembro del Equipo en esta área de conocimiento

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

Los siguientes documentos y plantillas de apoyo para la correcta elaboración del Plan de Proyecto:

Los siguientes documentos y plantillas de apoyo para la correcta elaboración del Plan de Proyecto:

- ODP-G-Guía de Referencia- Guía de referencia para la aplicación de la Metodología.
- ODP-G-Plan de Gestión del Proyecto varias fases

Este documento será la plantilla que el licitador deberá utilizar para presentar el Plan de Proyecto en su oferta y 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.

Los capítulos son los siguientes:

- 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 transición o transferencia, estabilización, desarrollo o 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.

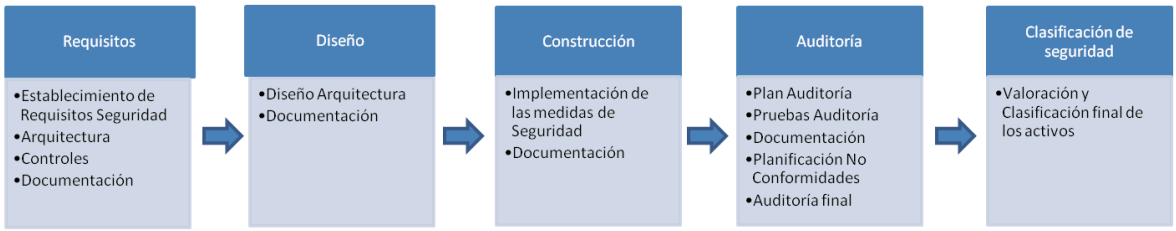
Es la protección de la información y de los sistemas de información contra el acceso no autorizado y/o la modificación de la información, ya sea en su almacenamiento, procesamiento o tránsito, y en su disponibilidad a los usuarios autorizados.

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.
Acrónimo 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 División de Protección Informática 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
- Proporcionar una estrategia sólida para evitar posibles vulnerabilidades y brechas de seguridad.

- 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 contemplara 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 riego, 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 División de Protección Informática 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 permitirán 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 División de Protección Informática para su revisión.
- Identificación de los controles de seguridad.
- Entrega del documento de **Arquitectura de Seguridad de la Aplicación** a la División de Protección Informática 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 (afectados por la LOPD y el Reglamento que la desarrolla) 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 División de Protección Informática 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.

3.3.2.- Seguimiento de los no cumplimientos.

En el caso de que se haya detectado no cumplimientos, se deberá informar al dueño de los datos / responsable de la aplicación, exponiendo los riesgos de seguridad asociados. El dueño de los datos / responsable de la aplicación decidirá qué no cumplimientos se resuelven, priorizando su resolución en una planificación con las áreas responsables y con la División de Protección Informática, y cuáles no, aceptando entonces y de forma explícita su riesgo asociado.

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.

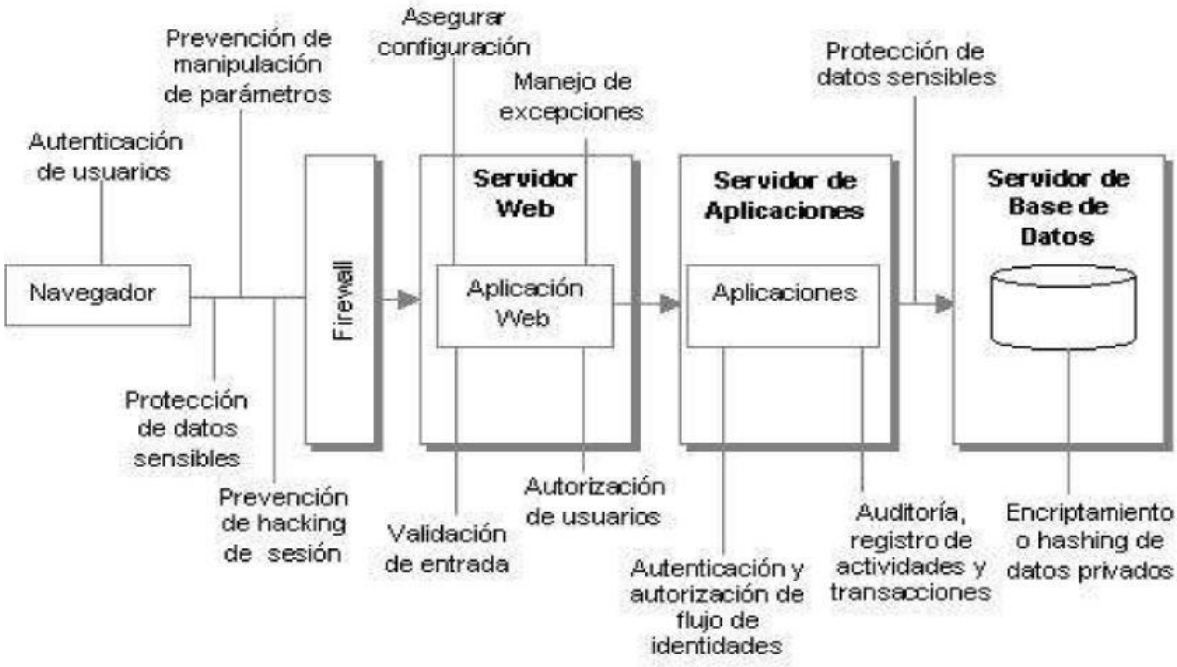
CONSIDERACIONES DE SEGURIDAD PARA EL DISEÑO Y CONSTRUCCIÓN DE APLICACIONES WEB:

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

Validación de datos de entrada	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: a) las longitudes de las cadenas de entrada b) los datos de entrada provenientes de variables de entorno del sistema c) los campos obligatorios d) el uso de valores por defecto o establecidos (listas que contenga sólo las entradas permitidas) en lugar entradas que se puedan realizar libremente por el usuario e) la comprobación de parámetros vacíos *f)* la comprobación del formato de los datos de entrada para aceptar sólo los formatos aceptados y evitar la inserción de cadenas de texto especialmente diseñadas/manipuladas o maliciosas en *query strings* (uso de *mime-types, content-type, magic numbers,* etc*.)* *g)* la comprobación del *file size* 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 *HTTP Request Smuggling, heap overflow (use-after-free, double free, derefe-* *rence after free)**,** off-by-one, format string, integer overflows/underflows, memory leaks, buffer overflow*, etc.
Control de procesamiento interno	Condiciones de carrera (*race conditions*).
Autenticación	Suplantación de identidad, *password cracking*, 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, altera-ción 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 4. 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 Gestión, 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 regirá 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.

ANEXO 5 INFORMACIÓN PARTICULAR SAP.

Ver anexo: “40_2020 Anexo 5 Información Particular SAP.pdf”