

16 - 10 - 17

ENTRADA

Pliego de Prescripciones Técnicas para la
Contratación de Servicios de Consultoría y
Asistencia Técnica para la realización de un
Plan Director de Seguridad de la Tecnología
Operacional.

(PROYECTO PDSOT) 264/2017

Madrid, septiembre de 2017

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A.	Plan Director de Seguridad de la Tecnología Operacional.	09/2017
Elaborado por:	Documento	Versión
Coordinación de Seguridad Informática	Pliego de Prescripciones Técnicas Particulares	V0.8
Área de Planificación, Control y Seguridad		

Índice

1. INTRODUCCIÓN.....	4
2. OBJETIVOS DEL PROYECTO.....	7
3. ALCANCE.....	8
3.1. Alcance Funcional.....	9
3.1.1. Fase 0: Divulgación y concienciación.....	10
3.1.2. Fase 1: Organización y Planificación.....	11
3.1.3. Fase 2: Estudio de los servicios y procesos, identificación de los flujos de información y estudio del entorno y de los sistemas.....	13
3.1.4. Fase 3: Evaluación de Riesgos y Análisis Técnicos de Seguridad.....	17
3.1.5. Fase 4: Tratamiento de Riesgos de Seguridad.....	24
3.1.6. Fase 5: Plan Director de Seguridad de la Tecnología Operacional.....	28
3.2. Alcance Técnico.....	31
3.2.1. Requisitos técnicos de las tecnologías propuestas para la inspección de redes ICS/SCADA.....	35
3.3. Gestión del Cambio.....	39
3.3.1. Documentación.....	40
3.3.2. Previo al Inicio de los Trabajos objetos del contrato.....	41
3.3.3. En el ámbito de la Organización, Seguimiento y Control de los trabajos.....	41
4. ENTORNO TECNOLÓGICO.....	44
5. ACUERDO DE NIVEL DE SERVICIO.....	45
5.1 Medida de los parámetros del ANS.....	45
5.2 Proceso de Revisión del nivel de cumplimiento del ANS.....	45
5.2 Cálculo de Penalizaciones en Parámetros.....	48
5.3 Aplicación del ANS a lo largo del Contrato.....	50
5.4 Terminación del contrato por incumplimiento del ANS.....	51
6. MODELO DE GESTIÓN.....	52
6.1. Gestión de Servicios.....	52
6.2. Gestión del ANS.....	53

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A.	Plan Director de Seguridad de la Tecnología Operacional.	09/2017
Elaborado por:	Documento	Versión
Coordinación de Seguridad Informática	Pliego de Prescripciones Técnicas Particulares	V0.8
Área de Planificación, Control y Seguridad		

6.3. Gestión de la Relación	54
6.3.1. Modelo de Referencia.....	54
6.3.1.1 Comité de Dirección.....	55
6.3.1.2 Comité de Seguimiento y Control.	56
6.3.1.3 Comité Operacional.	57
6.4. Gestión del Contrato.	58
7. EJECUCIÓN DE LOS TRABAJOS ASOCIADOS AL SERVICIO.....	60
7.1. Plazos de ejecución.	60
7.2. Metodología de Gestión de Proyectos.	60
7.3. Metodología para la Gestión de Riesgos.	63
7.4. Metodologías de los Análisis de Seguridad y Vulnerabilidades.	64
7.5. Metodología para la gestión de la seguridad de la información.	64
7.6. Equipo de trabajo.	66
7.7. Organización, Seguimiento y Control de los trabajos asociados al Servicio S2.....	68
7.8. Formación y transferencia de conocimiento.	73
7.9. Lugar de realización de los trabajos asociados al servicio.....	74
8. CONDICIONES DE ACEPTACIÓN, GARANTÍA Y MANTENIMIENTO.....	75
9. ESTRUCTURA DE LAS OFERTAS.....	76
ANEXO 1. CUESTIONARIO PERSONAL.....	77
ANEXO 2. REFERENCIAS.....	79
ANEXO 3. TABLA ACUERDO DE NIVEL DE SERVICIO (ANS).	80
ANEXO 4. CONDICIONES DE ACCESO A LA RED CORPORATIVA DE DATOS DE CANAL DE ISABEL II.	85
ANEXO 5. REQUISITOS DE SEGURIDAD.	88
ANEXO 6. ENTORNO TECNOLÓGICO DE CANAL GESTION.....	91
ANEXO 7. INSTALACIONES FÍSICAS DE CANAL DE ISABEL II.....	92

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A.	Plan Director de Seguridad de la Tecnología Operacional.	09/2017
Elaborado por:	Documento	Versión
Coordinación de Seguridad Informática.	Pliego de Prescripciones Técnicas Particulares	V0.8
Área de Planificación, Control y Seguridad		

1. INTRODUCCIÓN.

Tradicionalmente los sistemas relativos a la Tecnologías de la Información (TI) y los relativos a la Tecnología Operacional (OT), que incluyen tanto los Sistemas de Supervisión, Control y Adquisición de Datos (SCADA) como otros sistemas de control y automatización industrial (ICS), han estado aislados debido a su diferente naturaleza, objetivos, ciclo de vida extenso, campo de acción y elevados requisitos de integridad y disponibilidad de la información que manejan, existiendo un flujo de información limitado exclusivamente al propio sistema y a sus usuarios. Sin embargo, la necesidad de gestionar eficientemente la producción ha favorecido la aparición de un flujo vertical y permanente de información desde los elementos finales de la cadena productiva (instalaciones industriales de producción) hacia los órganos de dirección de la organización (en el entorno corporativo), y viceversa. De esta forma se obtiene una valiosa información, prácticamente en tiempo real y, principalmente, como soporte a la toma de decisiones.

Esta necesidad conlleva que en los entornos productivos se adopten cada vez en mayor medida técnicas y herramientas propias de los entornos TI corporativos (equipos informáticos, redes Ethernet, etc.), lo que comporta, como contrapartida, que los sistemas OT queden expuestos a los riesgos y vulnerabilidades propios del ámbito de la TI. Asimismo, las prácticas habituales llevadas a cabo por personal técnico en el mantenimiento y operación de los sistemas ICS/SCADA no suelen tener en cuenta principios básicos y esenciales de ciberseguridad.

Es en este contexto donde se pone de manifiesto la necesidad de adoptar políticas, procedimientos y medidas que garanticen, en la medida de lo posible, la confidencialidad, integridad y disponibilidad de ambos sistemas y de la información que manejan (cualquiera que sea su soporte físico), siendo ineludible abordar este objetivo desde un punto de vista integral que contemple la mejora continua, como resultado de una revisión permanente del modelo de seguridad adoptado.

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A.	Plan Director de Seguridad de la Tecnología Operacional.	09/2017
Elaborado por:	Documento	Versión
Coordinación de Seguridad Informática	Piiego de Prescripciones Técnicas Particulares	V0.8
Área de Planificación, Control y Seguridad		

Otra de las principales motivaciones para llevar a cabo este Plan Director de Seguridad de la Tecnología Operacional es la necesidad de adecuación a la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la Protección de las Infraestructuras Críticas (LPIC) y el Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de Protección de las Infraestructuras Críticas que desarrolla dicha Ley, y al Esquema Nacional de Seguridad Industrial (ENSI) como marco común de cumplimiento de la norma establecida por medio del desarrollo de actuaciones en materia de seguridad industrial y de un tratamiento de problemáticas comunes a través de un marco homogéneo:

- **Política General:** La política del ENSI establece la situación contextual que promueve la necesidad de su creación y del apoyo normativo que lo sustenta, señalando los principios que se persiguen, así como los objetivos y beneficios que supone la implantación de dicho esquema en el ámbito industrial, identificando a los actores y partes interesadas que están llamados a participar en el ENSI para mejorar de manera integral la seguridad en la industria.
- **Metodología de Análisis de Riesgos Ligero de Seguridad Integral (ARLI-SI):** Esta metodología permite identificar, analizar, evaluar y tratar oportunamente aquellos riesgos que afectan a infraestructuras con sistemas de control industrial; y, al mismo tiempo, obtener resultados comparables y reproducibles, proporcionando un modelo sencillo y práctico de análisis de riesgos integral en sistemas de control industrial. Por su parte, la metodología de Análisis de Riesgos Ligero de Ciberseguridad Industrial (ARLI-CIB), permite un acercamiento específico y también ligero, al análisis de riesgos de ciberseguridad en sistemas de control industrial. ARLI-CIB proporciona una herramienta para facilitar la aplicación, por parte de los operadores de sistemas de control industrial, de la metodología del análisis de riesgos de ciberseguridad.

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A.	Plan Director de Seguridad de la Tecnología Operacional.	09/2017
Elaborado por:	Documento	Versión
Coordinación de Seguridad Informática.	Pliego de Prescripciones Técnicas Particulares	V0.8
Área de Planificación, Control y Seguridad		

- **Indicadores para la Mejora de la Ciberresiliencia (IMC):** El modelo de indicadores para la mejora de la capacidad de ciberresiliencia (IMC) de las organizaciones ante distintos ataques, amenazas o incidentes que puedan sufrir, está basado en un modelo que permite medir el estado de la ciberresiliencia en las metas objetivo definidas (anticipar, resistir, recuperar y evolucionar), permitiendo a la organización medir la resiliencia de las funciones críticas de la prestación de sus servicios esenciales.
- **Modelo de Construcción de Capacidades en Ciberseguridad de la Cadena de Valor (C4V):** C4V proporciona una serie de controles basándose en un modelo de madurez de diferentes niveles que permita tanto la evaluación interna o a la cadena de valor como establecer niveles mínimos aceptables en función de los resultados obtenidos durante el análisis de riesgos.

Por todo ello, Canal de Isabel II Gestión S.A. (en adelante, Canal de Isabel II) se plantea la contratación de servicios profesionales para la elaboración de dicho Plan Director de Seguridad de la Tecnología Operacional.

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A.	Plan Director de Seguridad de la Tecnología Operacional.	09/2017
Elaborado por:	Documento	Versión
Coordinación de Seguridad Informática.	Pliego de Prescripciones Técnicas Particulares	V0.8
Área de Planificación, Control y Seguridad		

2. OBJETIVOS DEL PROYECTO.

El objeto del proyecto es la contratación de servicios de consultoría y asistencia técnica para la elaboración del Plan Director de Seguridad de la Tecnología Operacional de Canal de Isabel II, que abarque tanto las infraestructuras físicas, lógicas y de comunicaciones, como las medidas concernientes a las políticas de seguridad, administrativas, organizativas y de cumplimiento legal y normativo aplicable.

Se trata de un proyecto llave en mano que ha de contemplar todos los requisitos que Canal de Isabel II debe cumplir en materia de seguridad de la información relativa a las redes de operación y telecontrol (y a las telecomunicaciones en lo concerniente a infraestructura crítica de soporte a las dos primeras), realizando para ello las siguientes tareas fundamentales:

- Análisis y diagnóstico de la situación actual.
- Análisis de vulnerabilidades.
- Análisis de riesgos.
- Planificación de las medidas a adoptar a corto, medio y largo plazo (Planes de Acción) que garanticen continuidad, integridad y disponibilidad a las redes de operación, telecontrol y telecomunicaciones (esta última, en el alcance delimitado exclusivamente como infraestructura técnica crítica de soporte a todos los recursos y operaciones OT).
- Se proporcionará una bolsa de 320 horas para el apoyo en el desarrollo de los Planes de Acción derivados de los resultados obtenidos en el Análisis de Riesgos realizado, así como de cualquier otra tarea relacionada con la implantación de los mismos. Esta bolsa de horas está contemplada dentro del Alcance Máximo del contrato y recogida en el Pliego de Cláusulas Administrativas Particulares como "Servicio S2 - Apoyo al Desarrollo de los Planes de Acción".

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A.	Plan Director de Seguridad de la Tecnología Operacional.	09/2017
Elaborado por:	Documento	Versión
Coordinación de Seguridad Informática.	Pliego de Prescripciones Técnicas Particulares	V0.8
Área de Planificación, Control y Seguridad		

3. ALCANCE.

El objetivo principal de este proyecto es la identificación, valoración y clasificación de todos los activos informáticos de las redes de Tecnología Operacional (OT) a través de una evaluación objetiva de los mismos basada tanto en entrevistas con los respectivos responsables como en la identificación de aquellos activos necesarios para la correcta identificación de los servicios que se prestan, de los procesos que se ejecutan y sus dependencias, y poder por tanto identificar aquellos aspectos que garanticen su correcto funcionamiento.

Por tanto, los servicios objeto del presente pliego son:

Servicio S1: Consultoría y Asistencia Técnica para la realización de un Plan Director de Seguridad de la Tecnología Operacional, donde se realizarán las revisiones integrales de seguridad (aspectos organizativos, seguridad física, seguridad lógica (IT+OT), seguridad de la información en cualquiera de sus ámbitos (seguridad personal, seguridad ambiental, autoprotección y prevención de riesgos laborales, etc.) de las instalaciones físicas recogidas en el ANEXO 7 de este pliego, entre las que se encuentran todas aquellas identificadas oficialmente por el CNPIC como Infraestructura Crítica.

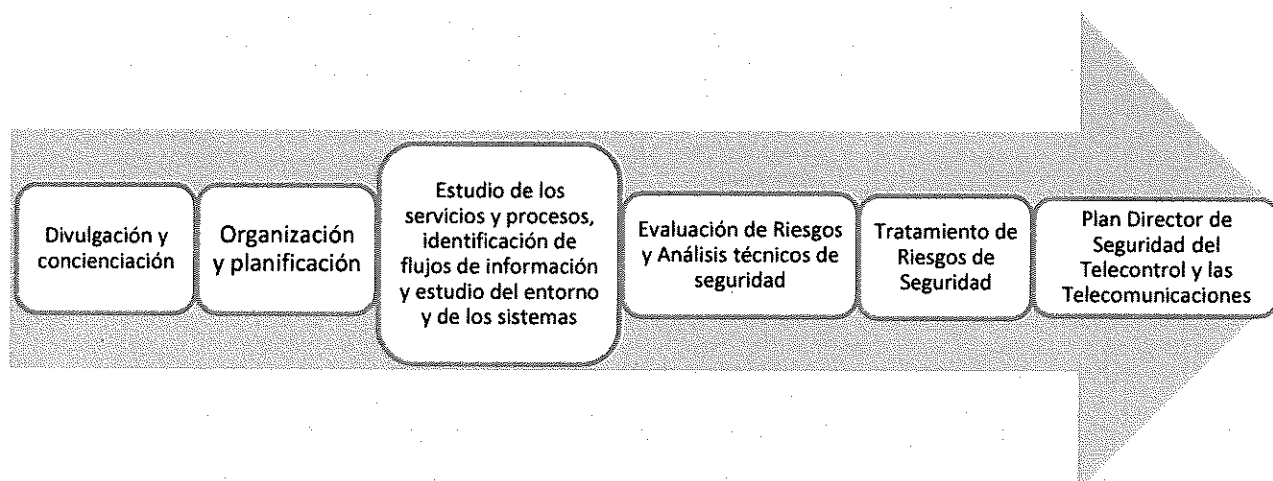
Servicio S2: Servicios de apoyo al Desarrollo de los Planes de Acción derivados de los resultados obtenidos en el Análisis de Riesgos realizado, así como de cualquier otra tarea relacionada con la implantación de los mismos, entre las que se encuentran, al menos:

- Seguimiento de la implantación de las medidas a adoptar en las distintas Infraestructuras, resultantes de los Planes de Acción a Corto Plazo resultantes.
- Revisión de los trabajos realizados en los Planes de Acción a Corto Plazo resultantes.
- Actualización de los documentos susceptibles de sufrir cambios tras la realización en las infraestructuras de las dos tareas anteriores.
- Elaboración del cuadro de mando de indicadores de ciberresiliencia del ENSI.

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A.	Plan Director de Seguridad de la Tecnología Operacional.	09/2017
Elaborado por:	Documento	Versión
Coordinación de Seguridad Informática.	Pliego de Prescripciones Técnicas Particulares	V0.8
Área de Planificación, Control y Seguridad		

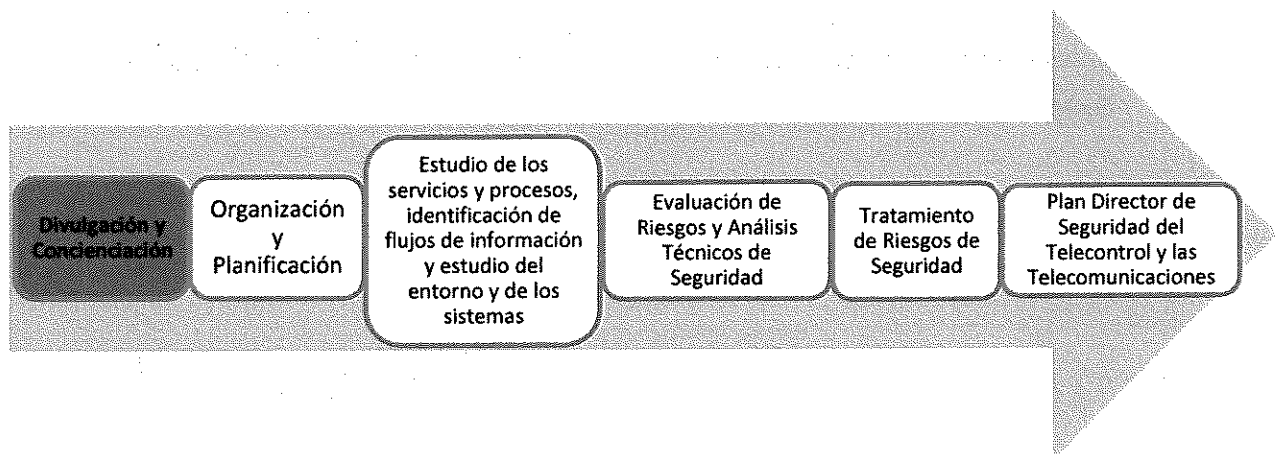
3.1. Alcance Funcional.

En este apartado se indican y describen las fases identificadas para la realización del Plan Director de Seguridad de la Tecnología Operacional:



Empresa	Proyecto	Fecha
Canal de Isabel II, S.A.	Plan Director de Seguridad de la Tecnología Operacional.	09/2017
Elaborado por:	Documento	Versión
Coordinación de Seguridad Informática.	Pliego de Prescripciones Técnicas Particulares	V0.8
Área de Planificación, Control y Seguridad		

3.1.1. Fase 0: Divulgación y concienciación.



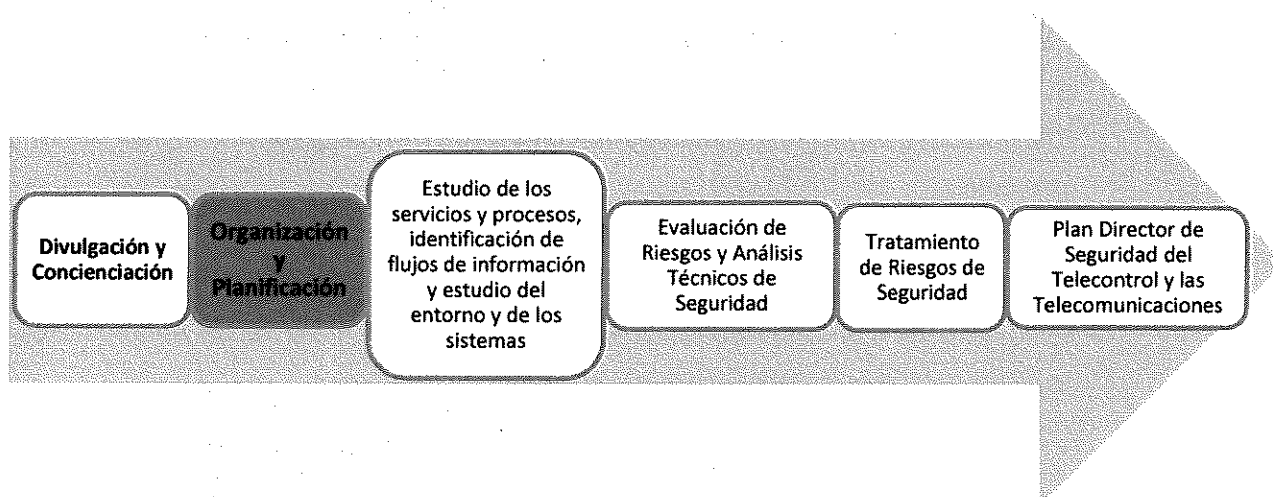
La fase de Divulgación y Concienciación sentará las bases para la realización del proyecto, y constará de una sesión orientada al Comité de Dirección de Canal de Isabel II, exponiendo la justificación, los objetivos y los alcances del proyecto.

La correcta definición del alcance del Plan Director de Seguridad de la Tecnología Operacional es fundamental a la hora de cumplir los objetivos identificados y establecidos. Resulta por tanto indispensable una plena colaboración por parte de los responsables de las subdirecciones y áreas responsables de Canal de Isabel II para la correcta y completa identificación de activos, procesos y servicios, a través de la existencia de un apoyo explícito y visible al proyecto por parte del Comité de Dirección.

Una vez realizada dicha sesión, el Comité de Dirección de Canal de Isabel II patrocinará explícitamente el proyecto y, sólo entonces, se dará inicio al mismo.

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A.	Plan Director de Seguridad de la Tecnología Operacional.	09/2017
Elaborado por:	Documento	Versión
Coordinación de Seguridad Informática.	Pliego de Prescripciones Técnicas Particulares	V0.8
Área de Planificación, Control y Seguridad		

3.1.2. Fase 1: Organización y Planificación.



Una vez patrocinado el proyecto explícitamente por el Comité de Dirección, la Fase de Organización y Planificación dará inicio efectivo a la realización del proyecto.

Objetivos principales de esta fase:

- Establecer las bases de trabajo para el desarrollo del proyecto dentro de los plazos definidos y a través de una planificación detallada del proyecto, con el fin de garantizar su cumplimiento a través de las especificaciones y de los requerimientos incluidos en la propuesta del adjudicatario.
- Realizar una identificación correcta y completa por parte de Canal de Isabel II de todos los procesos y servicios considerados críticos e importantes por Canal de Isabel II para la correcta prestación de los servicios esenciales a la población.

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A.	Plan Director de Seguridad de la Tecnología Operacional.	09/2017
Elaborado por:	Documento	Versión
Coordinación de Seguridad Informática.	Pliego de Prescripciones Técnicas Particulares	V0.8
Área de Planificación, Control y Seguridad		

Trabajos a realizar:

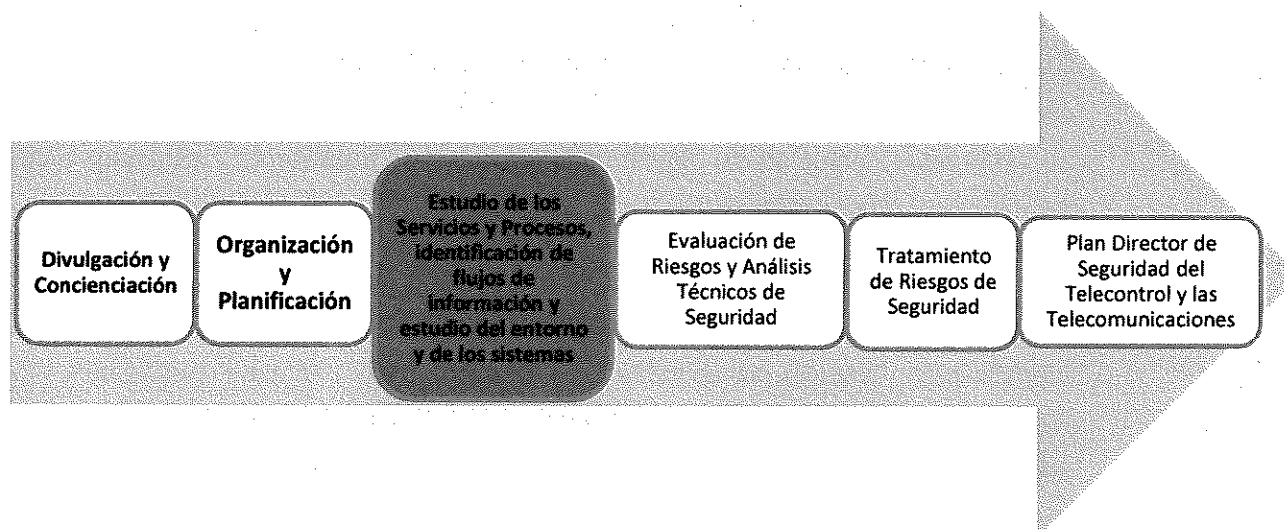
- Planificación de la reunión de presentación y toma de contacto, en la que se explicará el Plan de Trabajo inicial y se coordinará la ejecución de los trabajos.
- Identificación de los interlocutores y colaboradores que deberán formar parte del proyecto.
- Planificación de entrevistas iniciales. Se presentará un calendario y una agenda de entrevistas con los distintos responsables con el fin de desarrollar el proyecto.
- Obtención de una visión detallada del alcance del Plan Director de Seguridad de la Tecnología Operacional que incluirá, al menos:
 - La identificación de todos los procesos y servicios considerados críticos e importantes por Canal de Isabel II y que, a través de su adecuado funcionamiento, permiten la correcta prestación a la población de los servicios esenciales de abastecimiento (servicio esencial identificado por la LPIC), saneamiento y reutilización de agua.
 - Personal implicado.
 - Relaciones entre las distintas áreas de Canal de Isabel II.
- Solicitud de información y documentación específica en materia de seguridad que dé soporte a la gestión de la seguridad.
- Determinación del alcance final del Plan Director de Seguridad de la Tecnología Operacional en función de los objetivos identificados, su infraestructura de gestión, sus ubicaciones, los procesos y servicios identificados y a evaluar, activos de información que hayan sido identificados y evaluados previamente, e infraestructura y tecnología asociada.
- Presentación del Plan Operativo del Proyecto para la aprobación del mismo.

Entregable:

- Plan Operativo del Proyecto.

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A.	Plan Director de Seguridad de la Tecnología Operacional.	09/2017
Elaborado por:	Documento	Versión
Coordinación de Seguridad Informática.	Pliego de Prescripciones Técnicas Particulares	V0.8
Área de Planificación, Control y Seguridad		

3.1.3. Fase 2: Estudio de los servicios y procesos, identificación de los flujos de información y estudio del entorno y de los sistemas.



Objetivos:

- Durante esta fase se procederá:
 - Al estudio pormenorizado de los servicios y procesos identificados en la Fase 1, para su evaluación dentro del Plan Director de Seguridad de la Tecnología Operacional
 - A realizar una primera identificación de todos los activos de información que soportan dichos servicios y procesos identificados en la Fase 1, activos de información que serán tomados como base para el desarrollo de la siguiente fase (Fase 3: Evaluación de Riesgos y Análisis Técnicos de Seguridad).
 - Identificar los procesos de captación y recogida de información, acceso, tratamiento e intercambio de información, tanto internamente como en el envío hacia terceros.
 - Al estudio pormenorizado del entorno y de los sistemas.
 - A la identificación e inventario de otros recursos OT.

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A.	Plan Director de Seguridad de la Tecnología Operacional.	09/2017
Elaborado por:	Documento	Versión
Coordinación de Seguridad Informática.	Pliego de Prescripciones Técnicas Particulares	V0.8
Área de Planificación, Control y Seguridad		

Trabajos a realizar:

- Identificación de las relaciones que impliquen un intercambio de información.
- Conocimiento y estudio de los procedimientos y medidas de seguridad, tanto técnicas como organizativas, actualmente implantadas, incluyendo la evaluación de los controles de seguridad actualmente implantados para el tratamiento, almacenamiento, distribución y destrucción de la información.
- Estudiar los diferentes entornos de las redes de Telecontrol y Telecomunicaciones.
- Identificación y estudio pormenorizado de los servicios y procesos identificados en la Fase 1. En este punto se prestará especial atención, al menos, a los siguientes aspectos, que serán tenidos en cuenta en la Fase 3 (Evaluación de Riesgos y Análisis Técnicos de Seguridad):
 - Ventanas programadas de no disponibilidad de los servicios y procesos.
 - Medidas de tiempo de interrupción de los servicios y procesos permitidas por Canal de Isabel II.
 - Responsables de la monitorización de los servicios y procesos.
 - Posibilidades, probabilidades y consecuencias de la interrupción de los servicios y procesos.
 - Procedimientos existentes para mantener actualizado el inventario de servicios y procesos.
- Identificación de todos los activos de información, aplicaciones, otros servicios y funciones que soportan dichos servicios y procesos.

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A.	Plan Director de Seguridad de la Tecnología Operacional.	09/2017
Elaborado por:	Documento	Versión
Coordinación de Seguridad Informática.	Pliego de Prescripciones Técnicas Particulares	V0.8
Área de Planificación, Control y Seguridad		

- Identificación de relaciones con otros servicios dentro de Canal de Isabel II y/o con entidades externas (empresas del Grupo Canal, contratas, Administraciones, etc.) que impliquen un acceso a la información y/o intercambio de la misma (cualquiera que sea su categoría).
- Identificación de aquellos recursos OT que son necesarios para que la prestación de los servicios y procesos identificados en la Fase 1 puedan llevarse a cabo con garantías y de manera adecuada, evidenciando aquellos que sean críticos.
- Realización de un estudio de la arquitectura hardware, software y de red, entendiendo los diferentes entornos de la plataforma tecnológica actual y los elementos que la componen y dan soporte a la misma.
- Analizar otros recursos OT existentes (como puedan ser servicios internos y/o externos), suministros, centros de procesamiento de datos, personal propio y externo, etc.), con el fin de identificar aquéllos que son necesarios para prestar servicio a los servicios y procesos identificados en la Fase 1, evidenciando aquellos que sean críticos.
- Analizar detalladamente las interdependencias entre los servicios y procesos identificados en la Fase 1, y las interrelaciones entre los diferentes entornos de la plataforma tecnológica actual y los elementos que la componen y dan soporte a la misma, todo ello conforme a la norma ISO 22301:2012.
- Asociar los diferentes recursos OT identificados con dichas medidas de seguridad implantadas.

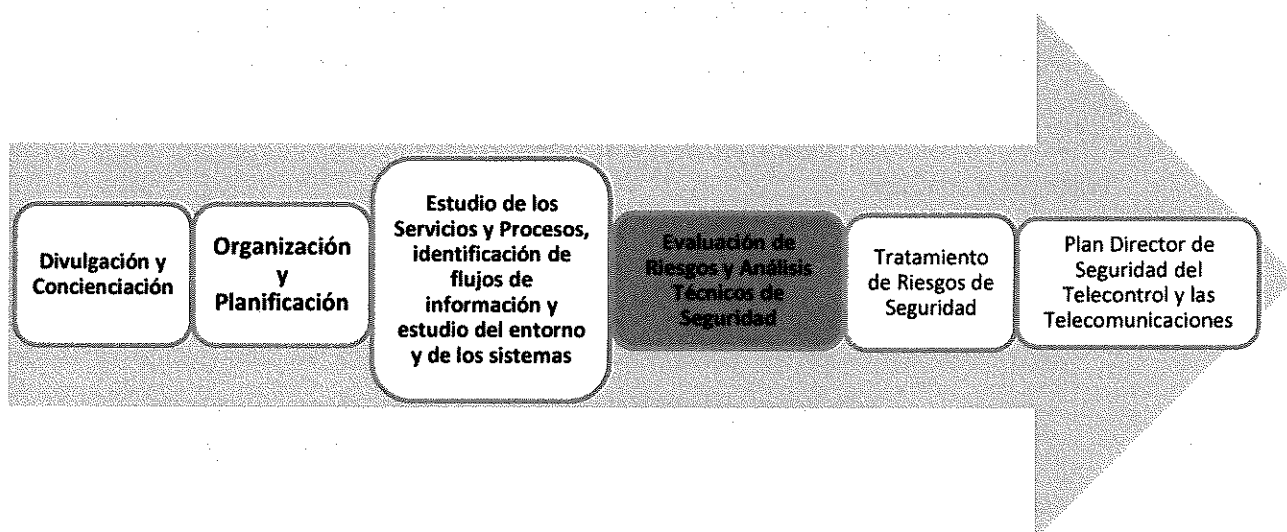
Empresa	Proyecto	Fecha
Canal de Isabel II, S.A.	Plan Director de Seguridad de la Tecnología Operacional.	09/2017
Elaborado por:	Documento	Versión
Coordinación de Seguridad Informática.	Pliego de Prescripciones Técnicas Particulares	V0.8
Área de Planificación, Control y Seguridad		

Entregables:

- Relación documentada de los diferentes servicios y procesos identificados en la Fase 1, y de los entornos de las redes de Telecontrol y Telecomunicaciones, incluyendo las plataformas tecnológicas actuales.
- Relación documentada de los diferentes recursos OT identificados que dan soporte a los servicios y procesos identificados en la Fase 1.
- Asociación de los diferentes recursos OT identificados con las medidas de seguridad identificadas y actualmente implantadas.

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A.	Plan Director de Seguridad de la Tecnología Operacional.	09/2017
Elaborado por:	Documento	Versión
Coordinación de Seguridad Informática.	Pliego de Prescripciones Técnicas Particulares	V0.8
Área de Planificación, Control y Seguridad		

3.1.4. Fase 3: Evaluación de Riesgos y Análisis Técnicos de Seguridad.



Objetivos:

Durante esta fase se procederá:

- A la revisión completa y a la valoración de los activos identificados en la Fase 2. Para poder evaluar correctamente el riesgo, se deben identificar correcta, clara y completamente todos los activos y todas sus características.
- A la identificación de las amenazas a las que están expuestas los activos identificados y validar su aplicabilidad en el Análisis de Riesgos definido por el ENSI.
- A la identificación de vulnerabilidades de los activos identificados desarrollando un inventario de vulnerabilidades y debilidades que podrían ser explotadas por las fuentes potenciales de amenazas. En este punto, se realizarán distintos análisis técnicos para detectar las vulnerabilidades y debilidades que pueden afectar a los activos identificados. Las vulnerabilidades detectadas serán revisadas manualmente para evitar falsos positivos e incluidas en los informes indicando su criticidad.

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A.	Plan Director de Seguridad de la Tecnología Operacional.	09/2017
Elaborado por:	Documento	Versión
Coordinación de Seguridad Informática.	Pliego de Prescripciones Técnicas Particulares	V0.8
Área de Planificación, Control y Seguridad		

- A la evaluación del impacto. El objetivo es estimar el impacto en los activos identificados en caso de que amenazas identificadas efectivamente exploten vulnerabilidades detectadas.

Trabajos a realizar:

- Identificar, describir y documentar correcta, clara y completamente todos los activos, detallando claramente todas sus características, límites y los distintos componentes que los forman, así como las relaciones entre los distintos activos. Los resultados tendrán un carácter de aplicación transversal hacia todos los servicios y procesos identificados en la Fase 1, y se utilizará MAGERIT v.3 como metodología de análisis y gestión de riesgos y PILAR como herramienta de soporte y apoyo en este trabajo.

En esta fase, la información a recopilar sobre los activos de información identificados será, al menos:

- Propietario/Dueño.
- Naturaleza del activo.
- Función del activo.
- Marcos legales, normativos y o regulatorios que afecten al activo y que pudieran ser de obligado cumplimiento.
- Hardware relacionado.
- Software relacionado.
- Entorno físico y lógico (ecosistema) del activo.
- Identificar todas las relaciones de afectación y dependencia de los activos con información (datos), sistemas de información, aplicaciones, funciones, servicios y procesos.
- Identificar las relaciones de afectación y dependencia entre los activos, al menos:
 - Diagramas de flujo de tráfico.

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A.	Plan Director de Seguridad de la Tecnología Operacional.	09/2017
Elaborado por:	Documento	Versión
Coordinación de Seguridad Informática.	Pliego de Prescripciones Técnicas Particulares	V0.8
Área de Planificación, Control y Seguridad		

- Inventario de protocolos, mensajes y valores existentes.
- Ventanas de ejecución/no ejecución.
- Rangos de funcionamiento (temperaturas, alimentación, etc.)
- Valoración del activo en 5 dimensiones:
 - Accesibilidad.
 - Confidencialidad.
 - Integridad.
 - Disponibilidad.
 - Auditoría.
- Identificar los orígenes y posibles amenazas de los activos inventariados en el punto anterior, considerándose también fuentes de información interna en base a entrevistas y sesiones de *brainstorming* con el personal identificado en la Fase 1 (interlocutores, colaboradores y personal implicado).
- Validar la existencia de la amenaza en el catálogo definido por el ARLI y ARLI-CIB del ENSI.
- Analizar y documentar los efectos de las amenazas sobre cada uno de esos activos, tomando también en consideración posibles motivaciones para cometer fraudes y/o delitos (incentivos, presiones, oportunidades, etc.).
- Identificar las vulnerabilidades asociadas a los activos, teniendo en cuenta que las vulnerabilidades pueden ser de distinta naturaleza:
 - Vulnerabilidades técnicas (presentes en el software, hardware o en cualquier otro componente técnico del activo).
 - Vulnerabilidades no técnicas (físicas, administrativas, procedimentales, ambientales, etc.).
- Las vulnerabilidades se entenderán extensibles a todos los ámbitos de aplicación:
 - Seguridad lógica.
 - Seguridad física asociada al activo.

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A.	Plan Director de Seguridad de la Tecnología Operacional.	09/2017
Elaborado por:	Documento	Versión
Coordinación de Seguridad Informática.	Pliego de Prescripciones Técnicas Particulares	V0.8
Área de Planificación, Control y Seguridad		

- Establecer la relación entre las vulnerabilidades asociadas a los activos y las amenazas mediante la creación de pares Amenaza \leftrightarrow Vulnerabilidad.
- Se evaluará la madurez de los procesos asociados a los recursos OT identificados en la Fase 2, con el objeto de conocer el grado de incumplimiento con los controles y mejores prácticas que se describen a continuación:
 - **Controles organizativos y de gestión:**
 - Política inadecuada de seguridad para los recursos OT.
 - Inexistencia de una normativa interna de diseño de las arquitecturas de los distintos recursos OT.
 - Inexistencia de un plan de formación y concienciación del personal en seguridad de los recursos OT.
 - Guías de implantación de recursos OT deficientes o inexistentes.
 - Falta de mecanismos administrativos para obligar al cumplimiento de las políticas y normativas de seguridad de los recursos OT.
 - Auditorías de seguridad técnicas relativas a recursos OT inexistentes, escasas, poco frecuentes, incompletas o inadecuadas.
 - Falta de procedimientos de control en la modificación de hardware, firmware, software y documentación técnica de los recursos OT.
 - Ausencia de procedimientos y operaciones relacionadas con la continuidad del negocio.
 - **Controles técnicos de seguridad:**
 - Falta de mantenimiento a nivel de parcheo en los recursos OT identificados.
 - Uso de configuraciones por defecto del fabricante.
 - Inexistencia de copias de seguridad, o gestión deficiente de las mismas, de las configuraciones de los recursos OT identificados, prestando especial atención a aquellos que se hayan evidenciado como críticos.

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A.	Plan Director de Seguridad de la Tecnología Operacional.	09/2017
Elaborado por:	Documento	Versión
Coordinación de Seguridad Informática.	Pliego de Prescripciones Técnicas Particulares	V0.8
Área de Planificación, Control y Seguridad		

- Gestión inapropiada en dispositivos portátiles y extraíbles de la información identificada en la Fase 2, así como otra información propiedad de Canal de Isabel II clasificada como reservadas y/o confidencial, y aquella que se hayan evidenciado como crítica.
- Ausencia de una adecuada política de contraseñas.
- Sistemas de control de accesos lógicos y físicos ineficientes.
- Accesos remotos y físicos no apropiados.
- Pruebas inadecuadas de los cambios.
- Existencia de activos relevantes indocumentados.
- Falta de redundancia en de los recursos OT identificados que se hayan evidenciado como críticos.
- Capacidades de seguridad disponibles en equipamiento y recursos OT identificados y que no estén activadas por defecto.
- Uso no seguro de protocolos intrínsecamente inseguros (por ejemplo, OPC-DA, Modbus/TCP, etc.).
- Existencia de servicios y/o funcionalidades activadas de forma innecesaria en equipamiento y recursos OT identificados, prestando especial atención a aquellos que se hayan evidenciado como críticos.
- Inexistencia de o ineficiencia en los sistemas de monitorización de seguridad: sistemas IDS/IPS, gestión de eventos/logs.
- Inexistencia de o ineficiencia en los sistemas cortafuegos: reglas laxas, configuraciones inadecuadas, etc.
- Falta de detección y gestión de incidentes de seguridad.
- Falta de mecanismos de protección eficientes contra el malware en general.
- Arquitectura de red de Telecontrol y Telecomunicaciones insegura.
- Perímetros de red de Telecontrol y Telecomunicaciones indefinidos.
- Ausencia de control de flujos de las comunicaciones en la red de Telecontrol y Telecomunicaciones

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A.	Plan Director de Seguridad de la Tecnología Operacional.	09/2017
Elaborado por:	Documento	Versión
Coordinación de Seguridad Informática.	Pliego de Prescripciones Técnicas Particulares	V0.8
Área de Planificación, Control y Seguridad		

- Electrónica de red y *end-points* mal asegurados (no bastionados).
- Puertos físicos desprotegidos.
- Identificar a los propietarios/dueños de los activos y al personal implicado, identificando entre ellos a los usuarios claves para recabar de ellos toda la información relevante que permita poder evaluar correcta y completamente el impacto.
- La evaluación del impacto ha de tener en cuenta el impacto de la vulnerabilidad. Se tendrán en cuenta, al menos, los siguientes aspectos:
 - Impacto negativo a la reputación y a la imagen de la compañía.
 - Pérdida económica cuantificable.
 - Pérdida de beneficios cuantificable.
 - Coste de reposición.
 - Duración temporal de la no-disponibilidad (horas, días, etc.)
 - Personas y/o información (datos), sistemas de información, aplicaciones, funciones, servicios y procesos afectados
 - Estimación, en porcentaje representativo, de las pérdidas producidas en cada activo.
 - Se deben contemplar de manera expresa las amenazas de baja probabilidad y alto impacto.

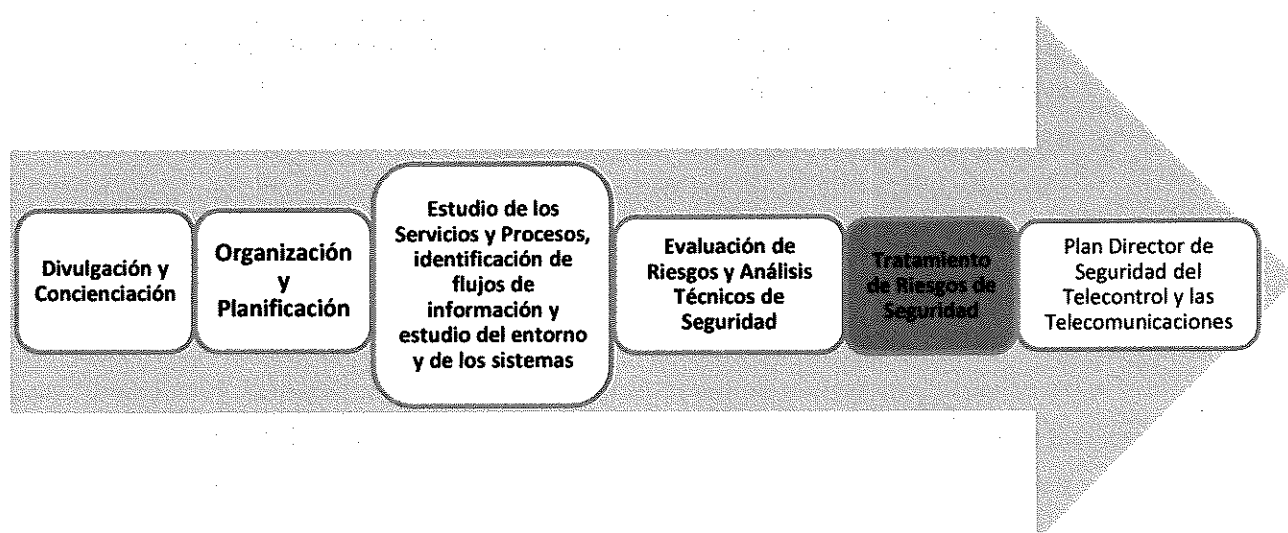
Empresa	Proyecto	Fecha
Canal de Isabel II, S.A.	Plan Director de Seguridad de la Tecnología Operacional.	09/2017
Elaborado por:	Documento	Versión
Coordinación de Seguridad Informática.	Pliego de Prescripciones Técnicas Particulares	V0.8
Área de Planificación, Control y Seguridad		

Entregables

- Documento con la identificación, descripción y valoración de todos los activos que soportan todos los servicios y procesos identificados en la Fase 1.
- Informe con la identificación de vulnerabilidades y debilidades asociadas a los activos, y encontradas a través de los distintos controles técnicos realizados, cuya existencia podría determinar la materialización de una amenaza.
- Identificación de amenazas para cada activo. La información relativa a activos y amenazas se incorporará a la herramienta PILAR (fichero .mgr).
- Asociación e inventario de pares Amenazas \leftrightarrow Vulnerabilidades, teniendo en cuenta la existencia de las amenazas identificadas en el catálogo definido por el ARLI y ARLI-CIB del ENSI.
- Evaluación del impacto para cada par Amenazas \leftrightarrow Vulnerabilidades.

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A.	Plan Director de Seguridad de la Tecnología Operacional.	09/2017
Elaborado por:	Documento	Versión
Coordinación de Seguridad Informática.	Pliego de Prescripciones Técnicas Particulares	V0.8
Área de Planificación, Control y Seguridad		

3.1.5. Fase 4: Tratamiento de Riesgos de Seguridad.



Objetivos

Los objetivos de esta fase son:

- Conocer la situación actual de la seguridad de los recursos OT identificados en la Fase 2, además de identificar y seleccionar los objetivos de control y los controles específicos que deberían ser implantados por Canal de Isabel II para mejorar la gestión de la seguridad de la información de los recursos OT.
- Identificar los controles que han sido implantados por Canal de Isabel II para minimizar o eliminar la probabilidad de las amenazas a las que se encuentran expuestos los activos de información identificados en la Fase 2, o reducir su impacto en caso de ocurrencia de las mismas.
- Dependiendo de las situaciones, los controles implementados pueden reducir el nivel de riesgo, pero no eliminarlo completamente. El riesgo que permanece (riesgo residual) ha de ser identificado y evaluado, para que Canal de Isabel II pueda decidir si se reduce/controla, se elimina, transfiere o se acepta dicho riesgo residual.

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A.	Plan Director de Seguridad de la Tecnología Operacional.	09/2017
Elaborado por:	Documento	Versión
Coordinación de Seguridad Informática.	Pliego de Prescripciones Técnicas Particulares	V0.8
Área de Planificación, Control y Seguridad		

Trabajos a realizar

- Análisis del grado de cumplimiento de los controles establecidos en las Normas de referencia ISO/IEC 27002:2013, la Ley de Protección de Infraestructuras Críticas (LPIC), el Esquema Nacional de Seguridad Industrial (ENSI) y en las buenas prácticas NIST SP-800-82 e ISA/IEC 62443. En esta revisión, se evaluará la madurez de los controles implantados.
- Valoración del estado de seguridad que se basará en los indicadores proporcionados por el "Modelo de Construcción de Capacidades de Ciberseguridad de la Cadena de Valor (C4V)" del ENSI. En el modelo C4V se definen 6 valores de niveles de indicadores de madurez:
 - Inexistente (nivel 0).
 - Inicial / ad-hoc (nivel 1).
 - Repetible pero intuitivo (nivel 2).
 - Definido (nivel 3).
 - Gestionado y medible (nivel 4).
 - Optimizado (nivel 5).
- Seleccionar los controles adecuados que deben ser implantados para garantizar una correcta gestión de la seguridad. Los controles y medidas de seguridad que serán considerados para la realización del Análisis de Riesgos serán los establecidos por:
 - La Norma ISO/IEC 27002:2013, "Código de Buenas Prácticas para la Gestión de la Seguridad de la Información".
 - La Ley PIC 8/2011.
 - El Modelo de Construcción de Capacidades de Ciberseguridad de la Cadena de Valor (C4V) del ENSI.

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A.	Plan Director de Seguridad de la Tecnología Operacional.	09/2017
Elaborado por:	Documento	Versión
Coordinación de Seguridad Informática.	Pliego de Prescripciones Técnicas Particulares	V0.8
Área de Planificación, Control y Seguridad		

- El Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, TÍTULO VIII. "De las medidas de seguridad en el tratamiento de datos de carácter personal".
- La ISA/IEC 62443 en el ámbito de los sistemas ICS.
- Las áreas que serán objeto de análisis serán, inicialmente, las siguientes:
 - 01. Programa de Gestión de Seguridad de la información [ISMP].
 - 02. Operación de Sistemas [SO].
 - 03. Seguridad del Personal [PS].
 - 04. Seguridad de la Instalación [FS].
 - 05. Procesamiento para Terceros [TPP].
 - 06. Resiliencia [RE].
 - 07. Cumplimiento [CO].
 - 08. Protección contra Códigos Maliciosos [MCP].
 - 09. Controles de Red [NC].
 - 10. Monitorización [MO].
 - 11. Control de Acceso [AC].
 - 12. Desarrollo Seguro [SD].
 - 13. Gestión de Incidentes [IH].
 - 14. Criptografía [CR].
- Sobre cada activo:
 - Analizar de qué forma los controles identificados pueden mitigar el riesgo.
 - Estimar el riesgo residual para cada par Amenaza \leftrightarrow Vulnerabilidad.
- Agrupación de los riesgos para identificar las áreas de mayor riesgo y las que necesitan, por tanto, mayor protección.
- Acordar y documentar el nivel de riesgo aceptable.

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A.	Plan Director de Seguridad de la Tecnología Operacional.	09/2017
Elaborado por:	Documento	Versión
Coordinación de Seguridad Informática.	Pliego de Prescripciones Técnicas Particulares	V0.8
Área de Planificación, Control y Seguridad		

- Determinación documentada de la estrategia de gestión de riesgos:
 - Reducción/Control.
 - Eliminación.
 - Transferencia.
 - Asunción.
- Selección de los controles que deberán ser implantados por Canal de Isabel II para reducir el riesgo al nivel de riesgo aceptable acordado.

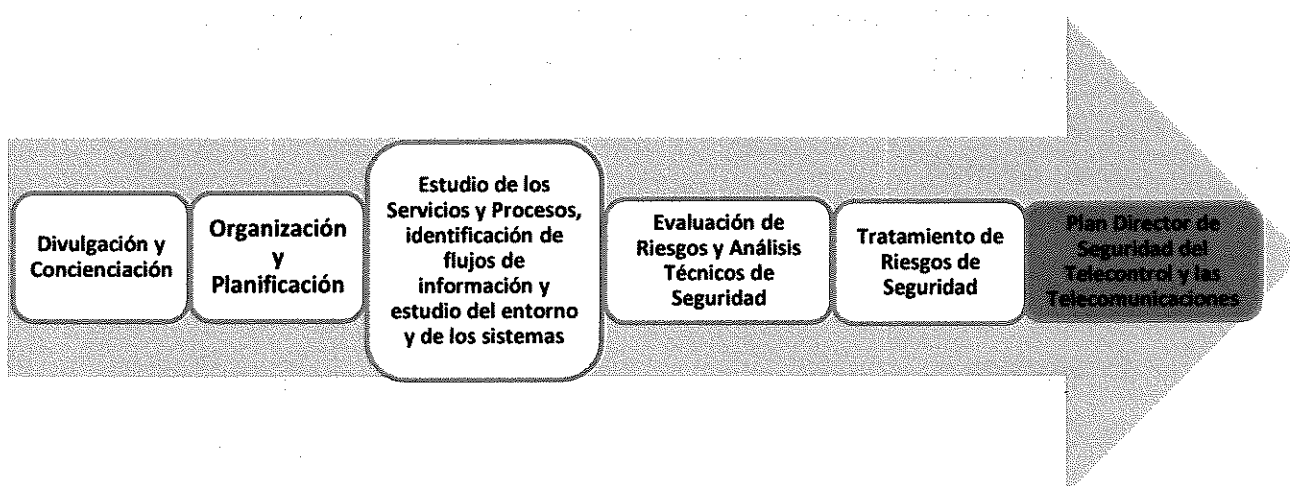
Entregables

Análisis de situación del modelo de seguridad actual que incluirá, al menos, información sobre los siguientes aspectos:

- Diagnóstico del nivel de posicionamiento.
- Mapa de Riesgos de Seguridad en sentido amplio.
- Análisis de los flujos de trabajo del negocio desde la perspectiva del tratamiento de la información identificada en la Fase 2, así como otra información propiedad de Canal de Isabel II clasificada como reservadas y/o confidencial, y aquella que se hayan evidenciado como crítica en la Fase 3, comparándolo con las mejores prácticas organizativas y la legislación aplicable en el sector Agua.
- Análisis GAP de controles implantados frente a controles identificados como necesarios y no existentes.
- Selección de objetivos de control y controles específicos que es necesario implantar según las normas ISO/IEC 27002:2013, ISA/IEC 62443, ENSI y Ley PIC 8/2011.
- Evaluación de Riesgos conforme a los resultados de ARLI-CIB del ENSI.
- Resultado del Análisis de Riesgos realizado a través de la herramienta PILAR (archivo .mgr)
- Propuesta de mejoras en la arquitectura de red en materia de seguridad de la información y operaciones.

Empresa		Proyecto	Fecha
Canal de Isabel II, S.A.		Plan Director de Seguridad de la Tecnología Operacional.	09/2017
Elaborado por:		Documento	Versión
Coordinación de Seguridad Informática.		Pliego de Prescripciones Técnicas Particulares	V0.8
Área de Planificación, Control y Seguridad			

3.1.6. Fase 5: Plan Director de Seguridad de la Tecnología Operacional.



Objetivos

Los objetivos de esta fase son:

- Documentación del Plan Director de Seguridad de la Tecnología Operacional especificando los proyectos que se deben acometer para garantizar una correcta gestión de la seguridad y minimizar los riesgos identificados en las fases anteriores.
- Confección de un Plan Estratégico como propuesta global que incluya todas y cada una de las opciones y recomendaciones, con los requisitos técnicos detallados elemento a elemento, que podrían incluirse en dicho Plan Estratégico. Se recogerá un número definido de opciones que contendrán agrupaciones lógicas de los recursos OT (por ejemplo, tres opciones: nivel básico de seguridad, nivel medio de seguridad y nivel de seguridad y protección avanzada), identificación de *quick-wins*, plazo estimado de implantación de la opción (corto, medio y largo plazo) y estimación presupuestaria. El objetivo es facilitar la toma de decisiones a Canal de Isabel II.
- Los componentes de este Plan Estratégico tendrán en cuenta, al menos, los siguientes elementos:
 - Plan Director de Seguridad de la Tecnología Operacional.
 - Definición de estrategias de seguridad.

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A.	Plan Director de Seguridad de la Tecnología Operacional.	09/2017
Elaborado por:	Documento	Versión
Coordinación de Seguridad Informática.	Pliego de Prescripciones Técnicas Particulares	V0.8
Área de Planificación, Control y Seguridad		

Trabajos a realizar

- Definición del Plan Director de Seguridad de la Tecnología Operacional, en el que se detallen los proyectos y medidas de seguridad que deberían ser implantados por Canal de Isabel II para garantizar una correcta gestión de la seguridad.
- Establecimiento de las medidas a adoptar, prioridades de implantación, fechas, costes y recursos necesarios para la implantación de cada uno de los controles seleccionados, la consiguiente reducción cuantificada de los riesgos identificados en fases anteriores y la estimación del porcentaje de beneficio económico derivado de dicha reducción del riesgo.
- Priorización de las acciones y medidas a adoptar. Se tendrán en cuenta, al menos y entre otros, los siguientes factores:
 - Criticidad.
 - Complejidad.
 - *Quick-Wins*
 - Interrelación y dependencia con otros proyectos.
 - Exigencias legales y normativas.
 - Presupuesto.
- Agrupación de distintos controles en proyectos temáticos que simplifiquen su gestión.
- Planificación de la implantación de los controles seleccionados.
- Establecimiento de dependencias entre proyectos para planificar su ejecución en el orden adecuado.

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A.	Plan Director de Seguridad de la Tecnología Operacional.	09/2017
Elaborado por:	Documento	Versión
Coordinación de Seguridad Informática.	Pliego de Prescripciones Técnicas Particulares	V0.8
Área de Planificación, Control y Seguridad		

Entregables

- Plan Director de Seguridad de la Tecnología Operacional, en el que se detallen los proyectos y medidas de seguridad que deberían ser implantados por Canal de Isabel II para garantizar una correcta gestión de la seguridad. Este Plan Director incluirá, al menos:
 - Plan de proyectos/acciones a corto/medio/largo plazo que incluyan en cada proyecto/acción, una exposición del mismo, trabajos a realizar y los beneficios que se pretenden obtener mediante su ejecución.
 - Priorización de los proyectos/acciones en cuanto a criticidad, identificando dependencias.
 - Evaluación en coste, duración y esfuerzo en cada proyecto/acción.
 - Identificando *Quick-Wins*
- Resumen Ejecutivo del Proyecto en forma de presentación, detallando los principales resultados obtenidos en el marco del proyecto.

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A.	Plan Director de Seguridad de la Tecnología Operacional.	09/2017
Elaborado por:	Documento	Versión
Coordinación de Seguridad Informática.	Pliego de Prescripciones Técnicas Particulares	V0.8
Área de Planificación, Control y Seguridad		

3.2. Alcance Técnico.

Objetivos

El objetivo es realizar un análisis desde el punto de vista técnico, pero también desde el punto de vista organizativo y de gestión. Se tendrán por tanto como referencias, al menos, la guía de buenas prácticas ISO/IEC 27002:2013, las buenas prácticas especificadas dentro de los documentos NIST SP 800-82, ISA/IEC 62443-2 (Políticas y Procedimientos) e ISA/IEC 62443-3 (Requisitos del Sistema), el Esquema Nacional de Seguridad Industrial (ENSI) y sus instrumentos asociados, las guías de seguridad SCADA del CCN que sean de aplicación para los objetivos de este proyecto, y durante todo el desarrollo del proyecto se automatizarán las tareas de análisis del estado de la seguridad, de los centros de control y alarmas, el inventariado y reconocimiento de activos, flujos de comunicación, protocolos, tipos de mensajes, los campos de los mensajes y valores de dichos campos identificados por Canal de Isabel II como normales, con el objeto de generar el patrón de comportamiento normal de las redes OT (*ICS Network Behavioral BluePrint - Baseline*) y garantizar el control y la calidad del tráfico.

El licitador, por tanto, deberá proponer y utilizar, y demostrar experiencia en el uso de, tecnologías nativas de inspección pasiva y análisis de sistemas de control industrial (ICS/SCADA) pero que también sean capaces de reconocer los protocolos más comunes de redes IT, así como de productos para el análisis de archivos de configuración de equipamiento de red (*switches, routers, etc.*).

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A.	Plan Director de Seguridad de la Tecnología Operacional.	09/2017
Elaborado por:	Documento	Versión
Coordinación de Seguridad Informática.	Pliego de Prescripciones Técnicas Particulares	V0.8
Área de Planificación, Control y Seguridad		

Trabajos a realizar

Los trabajos a realizar estarán enfocados en la identificación, caracterización y valoración de vulnerabilidades a múltiples niveles, teniendo como referencia las mejores prácticas y/o controles definidos en las normas, estándares y guías de buenas prácticas antes mencionadas.

- Un análisis a nivel de controles de seguridad organizativos y de gestión que, al menos, incluirá aspectos como:
 - Revisión de la política de seguridad.
 - Análisis de la organización de la seguridad.
 - Revisión de la adecuación y cumplimiento de la normativa y legislación vigente y aplicable.
 - Gestión de proveedores en la adquisición, desarrollo y mantenimiento de recursos OT.
 - Gestión del cambio en recursos OT y en las infraestructuras de comunicación.
 - Seguridad física y ambiental.
 - Seguridad en los recursos humanos.
 - Evaluación y gestión de incidentes de seguridad.
 - Continuidad de la operación.
- Un análisis a nivel de controles técnicos de seguridad que, al menos, abarcaría aspectos como:
 - Revisión de la arquitectura del SCADA y la interconexión con distintos sistemas.
 - Evaluación de los flujos de tráfico desde el punto de vista de ciberseguridad.
 - Revisión del control de accesos físicos y lógicos.
 - Revisión del sistema de monitorización de seguridad.
 - Análisis técnico de alto nivel de las vulnerabilidades en plataformas tanto software como hardware.
 - Aspectos técnicos de la identificación, evaluación y gestión de incidentes de seguridad.
 - Aspectos técnicos de la continuidad de la operación.

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A.	Plan Director de Seguridad de la Tecnología Operacional.	09/2017
Elaborado por:	Documento	Versión
Coordinación de Seguridad Informática.	Pliego de Prescripciones Técnicas Particulares	V0.8
Área de Planificación, Control y Seguridad		

En el análisis de los sistemas ICS/SCADA, es fundamental el análisis del tráfico de red, que se realizará de forma **pasiva**. La información se recogerá a partir de capturas de tráfico de red en puntos que se identifiquen como relevantes a partir de reuniones con el personal identificado en la Fase 1 (interlocutores, colaboradores y personal implicado) teniendo como documentos de trabajo, al menos, las arquitecturas y mapas de red disponibles.

- Se validarán entonces, al menos, aspectos como:

- Seguridad perimetral.

A nivel de seguridad perimetral se determinarán, inventariarán y auditarán los puntos de acceso a las redes ICS/SCADA para determinar el nivel de protección perimetral. Si las redes ICS/SCADA están conectadas con otras redes, se determinará el nivel de protección (control de acceso y filtrado de tráfico vía firewall u otros dispositivos de control de acceso).

- Seguridad a nivel 2.

Desde el punto de vista de la seguridad a nivel 2, se verificará si las redes ICS/SCADA está separadas o no de otras redes, determinando si la separación es física o lógica. Si la separación es a nivel 2 (utilizando VLANs), se auditará la seguridad de red a ese nivel, comprobando la seguridad a nivel 2 de todos los elementos de red (*switches*) que gestionen las VLANs identificadas para la detección e identificación de vulnerabilidades.

- Seguridad a nivel 3.

Desde el punto de vista de la seguridad a nivel 3, si existe separación lógica, se comprobará que no existen rutas que permitan comunicar (enrutar) con las redes ICS/SCADA de forma no prevista. Este análisis se realizará a través de la conexión directa a las redes ICS/SCADA objeto del análisis o, en su defecto, y para minimizar un posible impacto sobre el entorno productivo, mediante el análisis de las configuraciones

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A.	Plan Director de Seguridad de la Tecnología Operacional.	09/2017
Elaborado por:	Documento	Versión
Coordinación de Seguridad Informática.	Pliego de Prescripciones Técnicas Particulares	V0.8
Área de Planificación, Control y Seguridad		

de los elementos de red implicados (*switches*, *routers*). En caso de que existan firewalls u otros sistemas de control de acceso, se comprobará que no existen rutas de acceso a las redes ICS/SCADA que no pasen a través de dichos elementos de control de acceso.

- Identificación de protocolos de comunicación.

En lo que respecta a la identificación de los protocolos de comunicación, se determinará, mediante capturas y análisis del tráfico, qué protocolos de comunicación están operando en las redes ICS/SCADA, si son protocolos estándar o propietarios, si son serie o utilizan medios conmutados, los protocolos en los que se encapsulan, los puertos TCP y UDP que precisan para establecer las comunicaciones, etc.

- Uso de criptografía y robustez de la misma en los protocolos.

Se determinará, mediante capturas y análisis del tráfico, si los protocolos identificados utilizan o no métodos criptográficos, tanto para la autenticación como para la integridad de mensajes o el cifrado del tráfico, y la robustez de dichos métodos criptográficos. Para los protocolos estándar identificados, se comprobará si aporta o no una capa de cifrado y de autenticación de mensajes. Para los protocolos propietarios identificados, será necesario realizar ingeniería inversa del mismo para determinar su idoneidad en este aspecto.

- Accesos de los usuarios a los sistemas ICS/SCADA y protecciones de los mismos.

Se determinará si los usuarios autorizados acceden desde conexiones directas en las propias redes ICS/SCADA o mediante accesos remotos externos. En este caso, se realizará una auditoría de dichos accesos remotos. Además, se determinará si existen o no VLANs o segmentos de administración delimitados.

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A.	Plan Director de Seguridad de la Tecnología Operacional.	09/2017
Elaborado por:	Documento	Versión
Coordinación de Seguridad Informática.	Pliogo de Prescripciones Técnicas Particulares	V0.8
Área de Planificación, Control y Seguridad		

3.2.1. Requisitos técnicos de las tecnologías propuestas para la inspección de redes ICS/SCADA.

Las tecnologías propuestas para el análisis **pasivo** del tráfico de las redes ICS/SCADA **deberán cumplir con todos los requisitos** descritos a continuación:

RT01 Deberán, de forma automatizada, analizar los ficheros de captura y ser capaces de identificar, al menos, aspectos como equipamiento existente, tanto IP y como no IP (electrónica de red), sesiones TCP/IP, puertos TCP y UDP abiertos para cada dispositivo, credenciales de autenticación y ficheros enviados/recibidos, así como ser capaces de identificar, analizar y realizar la disección profunda de, al menos, los siguientes protocolos de control industrial:

1. MMS
2. OPC-DA
3. Modbus/TCP
4. S7 (Siemens)
5. DNP3
6. IEC 101/104
7. ICCP TASE.2
8. IEC 61850
9. IEEE C37.118 (Synchrophasor)
10. CSLib (ABB)
11. DMS (ABB)
12. S7 (Siemens)

RT02 Deberán ser capaces de construir una topología lógica (vista lógica) de las redes ICS/SCADA a partir de las capturas pasivas realizadas del tráfico de red.

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A.	Plan Director de Seguridad de la Tecnología Operacional.	09/2017
Elaborado por:	Documento	Versión
Coordinación de Seguridad Informática	Pliego de Prescripciones Técnicas Particulares	V0.8
Área de Planificación, Control y Seguridad		

RT03 Dispondrán de un centro de mando con control de acceso del usuario en base a roles y que dispondrá, al menos, de una interfaz de usuario basada en web, un amplio conjunto de filtros de alerta y analíticas visuales predefinidas, un motor de *workflow* configurable para el procesamiento de alertas y envío a distintos sistemas vía interface (por ejemplo, concentradores de logs, plataformas SIEM, etc.) mediante reglas definidas por el usuario, un motor de tareas configurable para la programación de tareas (envío de informes, optimización de la base de datos interna, etc.) y una serie de sensores de monitorización y detección que pueden ser usados para inspeccionar diferentes segmentos de red.

RT04 Tendrán en su *roadmap* la inclusión del reconocimiento y análisis (conexión y/o disección/inspección profunda) de otros protocolos estándar, tanto industriales como no industriales.

RT05 Dispondrán de, al menos, cuatro tipos de motores:

1. Motor de detección de posibles ataques, intrusiones y anomalías, que no requerirá de tiempo de aprendizaje y será capaz de detectar desde el inicio, al menos, ataques conocidos, ataques dirigidos, ataques tipo *0-day*, *portmapping* y *Man-in-the-Middle (MitM)*, anomalías del protocolo ARP, paquetes malformados o no conformes a la definición y a las especificaciones técnicas del protocolo en cuestión que indiquen posibles problemas de implementación del *stack* TCP por parte del fabricante, uso indebido de componentes, dispositivos y protocolos, posibles errores y/o malas configuraciones o la inyección y generación sintética de paquetes que puedan ser debidos a malos usos o posibles ataques o intrusiones. Dicho motor deberá ser capaz de agregar eventos frecuentes para optimizar la gestión de eventos, avisos y alarmas.

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A.	Plan Director de Seguridad de la Tecnología Operacional.	09/2017
Elaborado por:	Documento	Versión
Coordinación de Seguridad Informática.	Pliego de Prescripciones Técnicas Particulares	V0.8
Área de Planificación, Control y Seguridad		

2. Motor de perfilado de comunicaciones en redes ICS/SCADA, para inspección de patrones de comunicación: flujos, protocolos y tipos de mensajes, así como dispositivos conectados a las redes ICS/SCADA, con qué otros dispositivos se comunican, a través de qué interfaces, con qué protocolos, cómo y cuándo.
3. Motor de inspección profunda de comportamiento de cada protocolo industrial utilizado, para inspección detallada de tipos de mensajes, campos y longitud de los mensajes y valor o distribución de los valores de los campos, contra los identificados y definidos por Canal de Isabel II como normales.
4. Motor basado en scripts que permita, al menos:
 - a) Realizar un control y una correlación operacional sobre los eventos producidos en las redes ICS/SCADA.
 - b) Disponer de una inteligencia operacional sobre las redes ICS/SCADA.
 - c) Permitir la optimización (*tunning*) de la configuración y la personalización (*customizing*) del patrón de comportamiento de la red de control.
 - d) Responder a eventos.

RT06 Podrán añadir soporte para cualquier protocolo de control de industrial no estándar en un tiempo máximo de tres (3) meses naturales, previo estudio de la complejidad del mismo, número de mensajes, etc.

RT07 Serán capaces de reconocer protocolos de red IT, al menos los siguientes a nivel de conexión e inspección profunda:

1. SMB/CIFS
2. RPC/DCOM

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A.	Plan Director de Seguridad de la Tecnología Operacional.	09/2017
Elaborado por:	Documento	Versión
Coordinación de Seguridad Informática.	Pliego de Prescripciones Técnicas Particulares	V0.8
Área de Planificación, Control y Seguridad		

Y, al menos, los siguientes, a nivel de conexión:

3. PVSS
4. LDAP
5. NetBIOS
6. HTTP
7. FTP
8. SSH
9. SSL
10. SMTP
11. IMAP
12. POP3
13. VNC
14. RFB
15. RTSP
16. AFP

RT08 Serán conformes, al menos, con los siguientes estándares y guías de seguridad industrial: ISA/IEC 62443, NERC CIP (*Critical Infrastructure Protection*) y NIST Cybersecurity Framework.

Para todos los requisitos anteriormente expuestos y descritos, el licitador ha de describir en detalle cómo las tecnologías propuestas por él para el análisis **pasivo** de tráfico de redes ICS/SCADA cumplen con cada uno de los requisitos indicados, aportando cualquier información adicional **útil y relevante** que permita a Canal de Isabel II valorar si cada requisito se cumple o no conforme a lo especificado en su descripción.

Las ofertas cuya propuesta de tecnologías para el análisis pasivo de tráfico de redes ICS/SCADA no cumpla con alguno de los requisitos anteriormente expuestos y descritos, no serán tenidas en cuenta.

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A.	Plan Director de Seguridad de la Tecnología Operacional.	09/2017
Elaborado por:	Documento	Versión
Coordinación de Seguridad Informática.	Pliego de Prescripciones Técnicas Particulares	V0.8
Área de Planificación, Control y Seguridad		

3.3. Gestión del Cambio.

Dadas las implicaciones que conlleva la realización de un Plan Director de Seguridad del Telecontrol de las Telecomunicaciones, que afecta directamente a distintas áreas y a sus procesos existentes, es imprescindible que a lo largo de la ejecución de todo el proyecto se gestione el cambio que esto supone.

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

- Identificación del personal clave que deba participar de manera activa en el proyecto, tanto por su implicación directa en el mismo como por sus conocimientos. Dicho personal recibirá la formación necesaria en función de los roles que deban asumir, y estará contemplada en el Plan de Formación.
- Difusión del proyecto dentro de Canal de Isabel II en la forma que se estime más adecuada, con el objetivo de que Canal de Isabel II esté debidamente informado sobre la iniciativa en general, queden perfectamente recogidos la justificación, objetivos y alcances del proyecto, y permita su patrocinio de forma expresa y explícita por el Comité de Dirección de Canal de Isabel II.

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A.	Plan Director de Seguridad de la Tecnología Operacional.	09/2017
Elaborado por:	Documento	Versión
Coordinación de Seguridad Informática.	Pliego de Prescripciones Técnicas Particulares	V0.8
Área de Planificación, Control y Seguridad		

3.3.1. Documentación.

Se definirán todos los entregables que se consideren de interés dentro de los tres focos de actuación identificados en el apartado **2. OBJETIVOS DEL PROYECTO**, y conjuntamente con sus respectivos alcances identificados en el apartado **3. ALCANCE**.

Toda la documentación se entregará en soporte electrónico, preferiblemente en formato PDF y Microsoft Office (con compatibilidad para Microsoft Office 2007).

Con carácter general, se usará UML, con las extensiones BPMn, para la modelización de procesos, clases, modelos de datos y diseños en general.

Por lo que respecta a la documentación a entregar será necesario seguir las siguientes directrices:

- El adjudicatario establecerá un sistema de gestión de la documentación. Los documentos, tanto de apoyo como los generados por el propio trabajo, han de tener una identificación única en nombre y número de revisión. Deben mantenerse todas las versiones de la documentación entregada, contemplando el control de los cambios.
- Toda la documentación e información desarrollada en el ámbito de la realización de los trabajos será guardada durante todo el transcurso de los trabajos y a disposición del personal de Canal de Isabel II.

La gestión y documentación de los proyectos que se derivaran de la ejecución de este contrato se ajustarán a la metodología de Gestión de Proyectos de Canal de Isabel II (basada en PMI) y a lo que al respecto determine la Oficina de Gestión de Proyectos dependiente del Área de Planificación, Control y Seguridad.

Como consecuencia de las tareas identificadas en el alcance de este contrato, el adjudicatario deberá presentar a lo largo del periodo del mismo los siguientes documentos:

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A.	Plan Director de Seguridad de la Tecnología Operacional.	09/2017
Elaborado por:	Documento	Versión
Coordinación de Seguridad Informática.	Pliego de Prescripciones Técnicas Particulares	V0.8
Área de Planificación, Control y Seguridad		

3.3.2. Previo al Inicio de los Trabajos objetos del contrato.

El adjudicatario deberá presentar para su aprobación antes del inicio de los trabajos objeto de este contrato un Plan General de Gestión de Proyecto según los requisitos establecidos en el apartado 6 MODELO DE GESTIÓN incluido en este mismo pliego.

3.3.3. En el ámbito de la Organización, Seguimiento y Control de los trabajos.

Informes periódicos de seguimiento de la prestación de los servicios S1 y S2. Estos informes se realizarán, con carácter general, mensualmente.

Documento con el Plan de Acciones Correctivas ("PAC") para los incumplimientos de los parámetros de control del ANS.

Para los trabajos y/o asistencias solicitadas por Canal de Isabel II e identificados dentro del servicio S2:

- Documento de requisitos.
- Propuesta de Ejecución Valorada: documento que contendrá la planificación y previsión de esfuerzos para la realización de las tareas identificadas en el documento de requisitos. Este documento, será la referencia para el seguimiento del ANS en cuanto a calidad y eficacia de la planificación.

Este documento contendrá al menos:

- Identificación del alcance.
- Fecha prevista de entrega del Plan de Gestión del Proyecto (si lo hubiera).
- Fecha prevista de inicio de cada una de las fases del proyecto.
- Fecha prevista de fin del proyecto y de cada una de sus fases.
- Recursos necesarios para la realización de los trabajos (perfiles y horas previstas).
- Relación de entregables.
- Coste de los trabajos.

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A.	Plan Director de Seguridad de la Tecnología Operacional.	09/2017
Elaborado por:	Documento	Versión
Coordinación de Seguridad Informática.	Pliego de Prescripciones Técnicas Particulares	V0.8
Área de Planificación, Control y Seguridad		

- Plan de Gestión de Proyecto para aquellos casos en que la entidad o criticidad de los trabajos y/o asistencias así lo justifique, y siempre a petición de Canal de Isabel II. 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.
- Documentos de diseño técnico/funcional, para aquellos trabajos que precisen de la realización de un diseño previo. Canal de Isabel II deberá aprobar estos entregables en cuanto a calidad y completitud.
- Documentos acordados en la realización de los trabajos encomendados. Canal de Isabel II deberá aprobar estos entregables en cuanto a calidad y completitud, en función del alcance determinado en el propio PGP si lo hubiera y del documento de requerimientos. La fecha definitiva de los entregables del proyecto a efectos de cumplimiento del ANS será la de la entrega en la que Canal de Isabel II da la aprobación. El tiempo de aprobación de Canal de Isabel II no se tendrá en cuenta para el cómputo del retraso, aunque sí se tendrá en cuenta el tiempo que el adjudicatario utilice para la subsanación de las inconformidades. Si en los documentos de gestión de cambios aprobados que se realicen a lo largo de los proyectos, se recoge de manera expresa que éstos modifican la nueva fecha prevista de entrega a efectos de la penalización por incumplimiento del plazo previsto, esta nueva fecha se utilizará como nueva referencia para el cálculo del ANS.

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A.	Plan Director de Seguridad de la Tecnología Operacional.	09/2017
Elaborado por:	Documento	Versión
Coordinación de Seguridad Informática.	Pliego de Prescripciones Técnicas Particulares	V0.8
Área de Planificación, Control y Seguridad		

El adjudicatario asumirá el sistema de gestión, nomenclatura e identidad visual corporativa de la documentación de Canal de Isabel II, según la Guía de Referencia de Gestión de Proyectos de Canal de Isabel II y que puede ser descargada, junto con las plantillas necesarias, desde el enlace siguiente:

http://www.canalgestion.es/es/galeria_ficheros/concursos/Metodologia_Gestion_de_Proyectos_Proyecto_y_Servicio.zip

Todos los productos resultantes del trabajo serán propiedad y quedarán en posesión de Canal de Isabel II.

En este apartado de documentación se incluye también toda la documentación relativa a la prevención de riesgos laborales.

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A.	Plan Director de Seguridad de la Tecnología Operacional.	09/2017
Elaborado por:	Documento	Versión
Coordinación de Seguridad Informática.	Pliego de Prescripciones Técnicas Particulares	V0.8
Área de Planificación, Control y Seguridad		

4. ENTORNO TECNOLÓGICO OPERACIONAL.

La información de detalle sobre el entorno tecnológico operacional de Canal de Isabel II se engloban dentro del alcance del contrato y se consideran confidenciales por razones de seguridad. Los licitadores podrán solicitar a Canal de Isabel II dicha información bajo el siguiente procedimiento:

- La empresa licitadora que vaya a presentarse al pliego y requiera la información, la solicitará a Canal de Isabel II por medio del procedimiento establecido en el Apartado 10.13. "Información y aclaraciones" del ANEXO I del PCAP.
- Canal de Isabel II enviará el Acuerdo de Confidencialidad por correo electrónico.
- La empresa licitadora que desea la información adicional devolverá el Acuerdo de Confidencialidad firmado digitalmente con un certificado reconocido y en vigor de representación de la empresa.
- Canal de Isabel II suministrará la información solicitada debidamente protegida para garantizar que sólo la o las personas autorizadas por la empresa licitadora puedan acceder a dicha información. Además, Canal de Isabel II proporcionará el procedimiento de acceso a dicha información protegida. Una vez realizada la adjudicación del Contrato y a la firma del mismo, Canal de Isabel II cancelará el acceso a dicha información.

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A.	Plan Director de Seguridad de la Tecnología Operacional.	09/2017
Elaborado por:	Documento	Versión
Coordinación de Seguridad Informática	Pleigo de Prescripciones Técnicas Particulares	V0.8
Área de Planificación, Control y Seguridad		

5. ACUERDO DE NIVEL DE SERVICIO.

Se adjunta a este pliego el ANEXO 4 - Tabla de Acuerdo Nivel de Servicio (ANS), con los parámetros que serán necesarios cumplir. El licitante deberá aceptar expresamente este ANS para que su oferta sea considerada.

El ANS y el procedimiento para su gestión tendrán carácter contractual.

5.1 Medida de los parámetros del ANS.

Cada parámetro del ANS acordado será medido trimestralmente, salvo que expresamente se establezca otro periodo de medición. El adjudicatario entregará un informe para dicho periodo que permita determinar si ha conseguido los niveles de servicio acordados. 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.

5.2 Proceso de Revisión del nivel de cumplimiento del ANS.

Trimestralmente se revisarán conjuntamente los informes de cumplimiento previamente enviados por el adjudicatario, para establecer y acordar el cumplimiento de los compromisos por parte del mismo. Dichos informes contendrán un anexo con los eventos que se hayan desviado significativamente de los comprometidos y hayan producido desvíos importantes en la media.

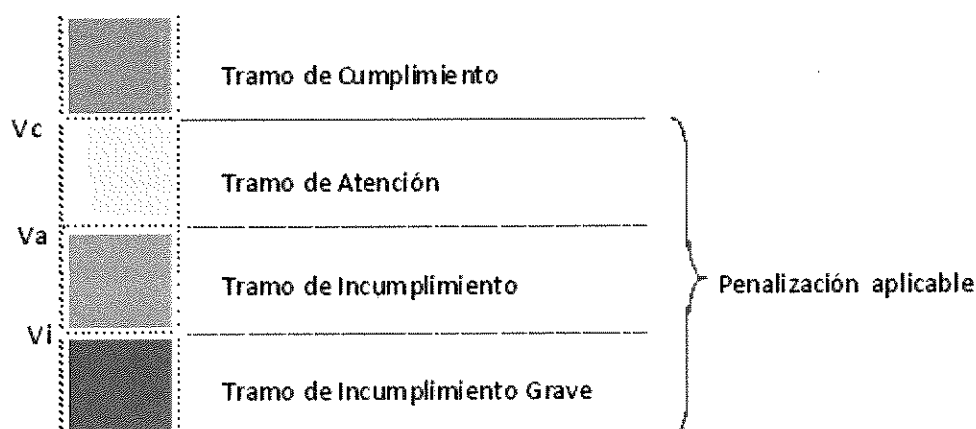
Tal como ya se ha dicho, el Anexo IV recoge el Acuerdo de Nivel de Servicio (ANS) que el adjudicatario se compromete a cumplir para cada parámetro que lo integra.

En caso de fallo en la provisión de los Servicios de acuerdo a los requerimientos de calidad acordados, el adjudicatario incurrirá en una penalización, que tiene como objetivo una

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A.	Plan Director de Seguridad de la Tecnología Operacional.	09/2017
Elaborado por:	Documento	Versión
Coordinación de Seguridad Informática.	Pliego de Prescripciones Técnicas Particulares	V0.8
Área de Planificación, Control y Seguridad		

compensación económica que refleje que ha entregado los servicios contratados con un nivel de calidad inferior al comprometido.

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:



Si el valor medido es igual o mejor al definido en el Tramo de Cumplimiento (V_c), 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 su compromiso, por lo que Canal de Isabel II aplicará la penalización correspondiente al Tramo de Control en el que se situó el valor obtenido.

Si el valor medido es igual o inferior al definido en el Tramo de Incumplimiento (V_i) se considerará que el Proveedor 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. El valor inicial para este peso está recogido en el propio Anexo 4. Este valor, como se explica

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A.	Plan Director de Seguridad de la Tecnología Operacional.	09/2017
Elaborado por:	Documento	Versión
Coordinación de Seguridad Informática.	Piiego de Prescripciones Técnicas Particulares	V0.8
Área de Planificación, Control y Seguridad		

más adelante, forma parte de la fórmula para el cálculo de la penalización. Canal de Isabel II podrá revisar estos Pesos o Prioridades a lo largo del servicio, a su único criterio, con la única limitación de un máximo de dos (2) cambios durante la prestación del servicio, que deberá notificar e informar convenientemente al adjudicatario con una antelación mínima de un (1) mes natural.

El adjudicatario podrá solicitar a Canal de Isabel II para un trabajo particular ampliar algunos de los plazos de tiempo recogidos en su oferta en su propuesta de Acuerdo de Nivel de Servicio, especialmente los valores N2 a N4 del parámetro GSE03, siempre que la complejidad de los trabajos a realizar así lo requiera. Canal de Isabel II se reserva el derecho a aceptar la solicitud del adjudicatario en base a la urgencia que el trabajo tenga para Canal de Isabel II.

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A.	Plan Director de Seguridad de la Tecnología Operacional.	09/2017
Elaborado por:	Documento	Versión
Coordinación de Seguridad Informática	Pliego de Prescripciones Técnicas Particulares	V0.8
Área de Planificación, Control y Seguridad		

5.2 Cálculo de Penalizaciones en Parámetros.

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

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

Donde:

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

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

F_C, 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 (2) 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 en el periodo de medición.

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A.	Plan Director de Seguridad de la Tecnología Operacional.	09/2017
Elaborado por:	Documento	Versión
Coordinación de Seguridad Informática.	Pliego de Prescripciones Técnicas Particulares	V0.8
Área de Planificación, Control y Seguridad		

Las penalizaciones se calcularán siempre a la finalización o cancelación de los trabajos, es decir, que en cada uno de los periodos medido se tendrán en cuenta los proyectos cerrados (trabajos finalizados y aprobados) en ese periodo y se calcularán para éstos las penalizaciones sobre los parámetros incumplidos, independientemente de la fecha de cada incumplimiento.

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.

Canal de Isabel II se reserva, no obstante, el derecho a no aplicar, a su único criterio, la penalización correspondiente a algún parámetro determinado.

El desacuerdo en cuanto a la penalización no suspende la aplicación de las penalizaciones, que si fuera necesario serían regularizadas en procesos de facturación posteriores.

Canal de Isabel II devolverá al adjudicatario cualquier factura que no se ajuste a la penalización de aplicación.

La penalización no supone en ningún caso que Canal renuncie a la exigencia de los daños directos o indirectos que considere ha sufrido como consecuencia de los incumplimientos del adjudicatario.

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.

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A.	Plan Director de Seguridad de la Tecnología Operacional.	09/2017
Elaborado por:	Documento	Versión
Coordinación de Seguridad Informática.	Pliego de Prescripciones Técnicas Particulares	V0.8
Área de Planificación, Control y Seguridad		

5.3 Aplicación del ANS a lo largo del Contrato.

Cuando sea necesario incluir en ANS un nuevo parámetro computable para el cálculo de penalizaciones, se establece un periodo de un (1) mes desde su inclusión en el ANS durante el que no se aplicarán penalizaciones.

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A.	Plan Director de Seguridad de la Tecnología Operacional.	09/2017
Elaborado por:	Documento	Versión
Coordinación de Seguridad Informática.	Pliego de Prescripciones Técnicas Particulares	V0.8
Área de Planificación, Control y Seguridad		

5.4 Terminación del contrato por incumplimiento del ANS.

Canal de Isabel II podrá **cancelar el contrato** por incumplimiento reiterado del ANS, sin coste adicional para el mismo, en los siguientes casos:

- Si el adjudicatario incurre en la Penalización Máxima establecida para el mismo, durante dos (2) periodos consecutivos o tres (3) periodos alternos en el periodo de los últimos tres (3) meses.
- Si durante tres (3) periodos consecutivos o cinco (5) periodos alternos en el periodo de los últimos tres (3) meses, el importe total de la Penalización aplicable supera el 20% del total de la factura por todos los servicios incluidos en el contrato de soporte.
- A los incidentes de seguridad achacables al adjudicatario se les aplicará la penalización descritas en el PCAP. No obstante a dicha penalización, si se producen tres (3) incidentes de seguridad en un periodo de tres (3) meses consecutivos, o un total de seis (6) incidentes de seguridad durante el periodo de prestación del servicio, supondrá la resolución del contrato en los términos recogidos en el PCAP.

Los incidentes de seguridad achacables al adjudicatario se calificarán como graves, y se aplicarán las penalizaciones descritas en el Apartado 9 del ANEXO I del PCAP, siendo motivo de terminación del Contrato conforme a las condiciones reflejadas en dicho Apartado 9 del ANEXO I del PCAP.

La terminación del Contrato, conforme a las condiciones anteriores, no supone renuncia a la aplicación de las penalizaciones correspondientes, ni a la reclamación de otros daños que Canal de Isabel II considere que le han sido causados por el adjudicatario con dichos incumplimientos.

Una vez Canal de Isabel II comunique al adjudicatario la necesidad de terminación del contrato, éste deberá continuar los trabajos hasta que Canal de Isabel II disponga de un nuevo adjudicatario de los servicios, momento en que se aplicará el plan de devolución propuesto.

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A.	Plan Director de Seguridad de la Tecnología Operacional.	09/2017
Elaborado por:	Documento	Versión
Coordinación de Seguridad Informática.	Pliego de Prescripciones Técnicas Particulares	V0.8
Área de Planificación, Control y Seguridad		

6. MODELO DE GESTIÓN

Canal de Isabel II considera que, para el éxito de este proyecto, es imprescindible un Modelo de Gestión con los Proveedores 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. En el PGGPAT, el proveedor deberá describir con detalle suficiente la organización de sus equipos de trabajo. Esta descripción debe incluir el detalle de los procedimientos que utilizará durante la vigencia del contrato para la gestión y supervisión de los servicios y de los equipos de trabajo implicados en la prestación de los servicios.

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

6.1. 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.

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.

El Proveedor deberá incluir en el Plan de Comunicación del PGGPAT la descripción del entorno de gestión de servicios que propone utilizar.

El Adjudicatario deberá hacer entrega a Canal de Isabel II, si Canal de Isabel II así lo requiriera, un Manual de Procedimientos conteniendo todos los procesos de Gestión que utilizará,

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A.	Plan Director de Seguridad de la Tecnología Operacional.	09/2017
Elaborado por:	Documento	Versión
Coordinación de Seguridad Informática	Piiego de Prescripciones Técnicas Particulares	V0.8
Área de Planificación, Control y Seguridad		

debiendo detallar la participación requerida de personal de Canal de Isabel II en cada uno de ellos. Este manual deberá ser revisado y aprobado por Canal de Isabel II.

Canal de Isabel II se reserva el derecho de, por sí mismo o por un tercero y en cualquier momento, auditar la forma en que el Adjudicatario está entregando sus servicios, controlando que éstos se ejecutan conforme a las definiciones y que asignan los recursos necesarios para su desarrollo.

6.2. Gestión del ANS.

El Proveedor debe describir en detalle el procedimiento y herramientas que propone utilizar para la gestión del Acuerdo de Nivel de Servicio. El Proveedor debe facilitar información detallada sobre:

- El proceso de seguimiento del nivel de servicio y el tratamiento de desviaciones
- Los informes periódicos que propone facilitar para la monitorización del servicio
- El procedimiento de aplicación de penalizaciones
- El proceso para gestionar las modificaciones o adiciones en los parámetros, valores y condicionantes que componen el ANS.

Sin perjuicio de que se establezca en el futuro como medida del ANS la que se obtenga a través de la herramienta de monitorización que utilice Canal de Isabel II para la gestión y control de este servicio, será responsabilidad del Adjudicatario la medición del ANS y de las penalizaciones exigidas en este pliego.

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A.	Plan Director de Seguridad de la Tecnología Operacional.	09/2017
Elaborado por:	Documento	Versión
Coordinación de Seguridad Informática.	Pliego de Prescripciones Técnicas Particulares	V0.8
Área de Planificación, Control y Seguridad		

6.3. Gestión de la Relación.

El Adjudicatario debe describir en el Plan de Gestión de la Comunicación del PGGPAT un Modelo de Relación “end-to-end” así como la estrategia y planificación para su implantación, paralelamente con el Modelo de Gestión de Servicios. En la definición y diseño de este Modelo el Adjudicatario debe tener presente 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 rápidos cambios del 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 el Canal de Isabel II.

En el siguiente apartado se describe el Modelo de Relación (Modelo de Referencia) requerido habitualmente por Canal de Isabel II. No obstante, Canal de Isabel II, conocedor de que el volumen de los trabajos a realizar no precisa de un modelo tan específico, permitirá que los licitantes, basándose en las principales directrices de este modelo, describan en el Plan de Comunicación del PGGPAT un modelo propio de relación entre Canal de Isabel II y el Proveedor.

6.3.1. Modelo de Referencia.

El Modelo de referencia 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.

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A.	Plan Director de Seguridad de la Tecnología Operacional.	09/2017
Elaborado por:	Documento	Versión
Coordinación de Seguridad Informática.	Pliego de Prescripciones Técnicas Particulares	V0.8
Área de Planificación, Control y Seguridad		

6.3.1.1 Comité de Dirección.

En el nivel de gestión estratégica se establece el Comité de Dirección, en el que participa Canal de Isabel II y el Adjudicatario asignando cada uno un Director Ejecutivo, capaces de asegurar el nivel de decisión y compromiso que requieren las disposiciones estratégicas requeridas a este nivel del modelo.

Entre otras, son responsabilidad del Comité de Dirección:

- Aprobar los cambios al Acuerdo de Nivel de Servicio 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
- En general, 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.

El Comité de Dirección se reunirá semestralmente o con la frecuencia que razonablemente se considere necesaria o dentro de los 10 días laborables siguientes a una petición por escrito de cualquiera de las partes.

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A.	Plan Director de Seguridad de la Tecnología Operacional.	09/2017
Elaborado por:	Documento	Versión
Coordinación de Seguridad Informática.	Pliego de Prescripciones Técnicas Particulares	V0.8
Área de Planificación, Control y Seguridad		

6.3.1.2 Comité de Seguimiento y Control.

En un nivel de gestión táctico, tanto Canal de Isabel II como el Adjudicatario asignarán ambos un Jefe de Proyecto para establecer el Comité de Seguimiento y Control, encargado de dirigir, monitorizar y controlar de la ejecución de todos los servicios.

Serán responsabilidades de este Comité, sin limitación:

- Asegurar que se consiguen los niveles de calidad acordados y que, en el caso de deficiencias no resueltas a nivel operativo, se desarrollen e implementen planes de resolución de problemas.
- Monitorizar el estado de los servicios.
- Revisar, actualizar y controlar el cumplimiento de la planificación.
- Coordinar los grupos y personas asignados a la entrega del Servicio.
- Discutir nuevos requerimientos o cambios. Revisar y aprobar las Peticiones de Cambio.
- En el caso de que el cambio requiera de cambios en el Contrato, deberán 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.

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A.	Plan Director de Seguridad de la Tecnología Operacional.	09/2017
Elaborado por:	Documento	Versión
Coordinación de Seguridad Informática.	Pliego de Prescripciones Técnicas Particulares	V0.8
Área de Planificación, Control y Seguridad		

- Controlar que la facturación se está realizando conforme a los acuerdos y resolver cualquier problema relacionado con el precio o los pagos.
- Revisar y facilitar al Comité de Dirección cualquier información que le sea solicitada.

El Comité de Seguimiento y Control se reunirá al menos mensualmente o con la frecuencia que razonablemente se considere necesaria o después de un (1) día laborable tras una petición de cualquiera de los Jefes de Proyecto.

6.3.1.3 Comité Operacional.

En un nivel de gestión operativo, Canal de Isabel II y el Adjudicatario trabajarán en plena coordinación para la consecución de los objetivos de los servicios objeto del contrato. Se nombrará a un Jefe de Proyecto/Responsable Operativo de cada una de las partes, cuyas responsabilidades se detallan a continuación:

- Revisar la lista de 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.

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A.	Plan Director de Seguridad de la Tecnología Operacional.	09/2017
Elaborado por:	Documento	Versión
Coordinación de Seguridad Informática.	Pliego de Prescripciones Técnicas Particulares	V0.8
Área de Planificación, Control y Seguridad		

- 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.

Se establecerán las reuniones de trabajo que se consideren necesarias a petición de cualquiera de las partes.

6.4. 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.

En un contrato susceptible de ser de larga duración como el que se recoge en este pliego, se producen cambios en el entorno gestionado y en el de negocio que provocan la necesidad de variar el ámbito y alcance inicialmente definidos para los Servicios.

El Adjudicatario debe incluir en el Plan de Gestión del Alcance para esta fase una descripción de los procedimientos, métodos y herramientas que propone implantar para la gestión del ámbito y alcance, que englobamos dentro del concepto de Gestión de Contrato. El Adjudicatario debe incluir el Modelo de Gestión de Contrato que propone para conseguir estos objetivos. El Adjudicatario deberá proponer concretamente un Procedimiento de Gestión de Cambios al Contrato capaz de gestionar:

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A.	Plan Director de Seguridad de la Tecnología Operacional.	09/2017
Elaborado por:	Documento	Versión
Coordinación de Seguridad Informática.	Piiego de Prescripciones Técnicas Particulares	V0.8
Área de Planificación, Control y Seguridad		

- 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 el 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.

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A.	Plan Director de Seguridad de la Tecnología Operacional.	09/2017
Elaborado por:	Documento	Versión
Coordinación de Seguridad Informática.	Pliego de Prescripciones Técnicas Particulares	V0.8
Área de Planificación, Control y Seguridad		

7. EJECUCIÓN DE LOS TRABAJOS ASOCIADOS AL SERVICIO.

7.1. Plazos de ejecución.

Los plazos de ejecución se encuentran recogidos en el **Apartado 2 del ANEXO I del PCAP**.

7.2. Metodología de Gestión de Proyectos.

Los licitantes incluirán en su oferta un Plan General de Gestión del Proyecto y de la Asistencia Técnica (PGGPAT) donde se indiquen los principales aspectos a considerar durante la gestión de los trabajos objeto del contrato por cada una de las distintas fases que lo componen.

El Área de Planificación, Control y Seguridad, a través de su Oficina de Proyectos, pone a disposición de los licitantes los siguientes documentos de apoyo para la correcta elaboración del PGGPAT:

- ODP-G-Guía de Referencia- Guía de referencia para la aplicación de la Metodología.

Este documento servirá de referencia para la elaboración del PGGPAT. En él se encuentran todas las plantillas que puedan ser necesarias para ello.

- ODP-G-Plan de Gestión del Proyecto Varias Fases Documento Único (PGGPAT).

Este documento será la plantilla que el licitante deberá utilizar para presentar el PGGPAT en su oferta y contiene todos los capítulos necesarios para describir los objetivos, alcance, y modelo y para el adecuado seguimiento y control del proyecto. **La no presentación del plan en la plantilla suministrada por Canal de Isabel II supondrá la exclusión del licitante del presente procedimiento.**

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A.	Plan Director de Seguridad de la Tecnología Operacional.	09/2017
Elaborado por:	Documento	Versión
Coordinación de Seguridad Informática	Pliego de Prescripciones Técnicas Particulares	V0.8
Área de Planificación, Control y Seguridad		

Los capítulos son los siguientes:

- **Introducción al Plan de Gestión del Proyecto.**
 - **Ámbito de aplicación.**
 - **Propósito del PGP.**
 - **Alcance del PGP.**
 - **Preparación del PGP.**
 - **Aprobación del PGP.**
 - **Actualización del PGP.**
 - **Periodicidad del control y revisión del PGP.**
- **Introducción al Proyecto (Descripción general del Proyecto y Servicios).**
 - **Descripción general.**
 - **Descripción del Alcance.**
 - **Descripción detallada del modelo/metodología propuestos y sus componentes.**
 - **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 el ANS que el licitante 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.** El Adjudicatario deberá asignar un peso a los paquetes de trabajo del Servicio S1 que servirán para el cálculo del Valor Ganado.

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A.	Plan Director de Seguridad de la Tecnología Operacional.	09/2017
Elaborado por:	Documento	Versión
Coordinación de Seguridad Informática.	Pliego de Prescripciones Técnicas Particulares	V0.8
Área de Planificación, Control y Seguridad		

- 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 Asistencia Técnica). En ésta se incluirán los modelos de Gestión del ANS, del Servicio, de la Relación y del Contrato que el licitante propone según las directrices contenidas en los sucesivos apartados de este pliego.
- Plan de Gestión de la Calidad.
- Cierre del Proyecto.

El PGGPAT 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.

El adjudicatario asumirá el sistema de gestión y nomenclatura de la documentación de Canal de Isabel II según la Guía de Referencia para la aplicación de la Metodología.

Deben mantenerse todas las versiones de la documentación entregada, contemplando las fechas de creación y modificación y el control de los cambios.

Todos los productos resultantes del trabajo quedarán en posesión de Canal de Isabel II.

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A.	Plan Director de Seguridad de la Tecnología Operacional.	09/2017
Elaborado por:	Documento	Versión
Coordinación de Seguridad Informática	Pliego de Prescripciones Técnicas Particulares	V0.8
Área de Planificación, Control y Seguridad		

7.3. Metodología para la Gestión de Riesgos.

La metodología a emplear en este punto será MAGERIT – versión 3. “Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información del Ministerio de Administraciones Públicas”, y la herramienta EAR para aplicar esta metodología será PILAR, en su última versión disponible en el CCN-CNI. Canal de Isabel II proporcionará su licencia para el uso de dicha herramienta.

MAGERIT se complementará con los Criterios de Seguridad, Normalización y Conservación de las aplicaciones (Criterios SNC) para la identificación y selección de funciones y mecanismos de salvaguarda.

También se tendrán en cuenta, al menos:

- La metodología de Análisis de Riesgos Ligero de Seguridad Industrial (ARLI-SI) del Esquema Nacional de Seguridad Industrial (ENSI) y, en particular, su metodología de Análisis de Riesgos Ligero de Ciberseguridad Industrial (ARLI-CIB).
- La adecuación al marco de trabajo de las mejores prácticas recogidas en la norma ISO/IEC 27005:2011: “Guía para la gestión del riesgo de la seguridad de la información”.
- El estándar de seguridad ANSI/AWWA J100-10 “*RAMCAP Standard for Risk and Resilience Management of Water and Wastewater Systems*”.
- La guía NIST SP 800-82 Rev.2 (“*Guide to Industrial Control Systems (ICS) Security*”).
- Todas las guías CCN-STIC-480A-H del Centro Criptológico Nacional que sean de aplicación.

Dado que el listado anterior no pretende ser exhaustivo, complementándolo se tendrá en cuenta toda otra normativa existente y aplicable en materia de seguridad de la información en el ámbito de análisis y gestión de riesgos, así como toda normativa legal aplicable al ámbito de la presente contratación.

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A.	Plan Director de Seguridad de la Tecnología Operacional.	09/2017
Elaborado por:	Documento	Versión
Coordinación de Seguridad Informática.	Pliego de Prescripciones Técnicas Particulares	V0.8
Área de Planificación, Control y Seguridad		

7.4. Metodologías de los Análisis de Seguridad y Vulnerabilidades.

Los análisis de seguridad y vulnerabilidades se realizarán como referencia metodologías de trabajo, *frameworks* y procedimientos generales de seguridad reconocidos internacionalmente como puedan ser OSSTMM, OWASP, WASC, ISSAF, PTES, etc., o bien propios, pero que mapeen sus contenidos a dichas referencias para la realización de diferentes pruebas y tests de aplicabilidad en los alcances que se recogen en el apartado 3. ALCANCE.

En las distintas pruebas y test se realizarán comprobaciones manuales y/o automáticas con el objetivo de confirmar, mediante evidencias, la existencia o no de las vulnerabilidades detectadas, eliminando así la posible existencia de falsos positivos. La valoración objetiva de las vulnerabilidades identificadas y verificadas se realizará utilizando la metodología *Common Vulnerability Scoring System Version 2 (CVSSv2)* o *Version 3 (CVSSv3)*. El adjudicatario justificará adecuadamente la elección de una u otra, reflejándose también la identificación de las vulnerabilidades identificadas según *Common Weakness Enumeration (CWE)*.

7.5. Metodología para la gestión de la seguridad de la información.

La metodología a emplear en este punto seguirá el estándar UNE-ISO/IEC 27001:2014. También se utilizará la norma UNE-ISO/IEC 27002:2014, guía de buenas prácticas, que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información, como desarrollo del Anexo A de la norma UNE-ISO/IEC 27001:2014.

También se tendrán en cuenta, al menos, las siguientes guías, normas y buenas prácticas de seguridad reconocidas nacional e internacionalmente en el ámbito de la protección de redes y sistemas de control industrial:

- “Process Control System Security Guidance for the Water Sector” (American Water Works Association - AWWA).

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A.	Plan Director de Seguridad de la Tecnología Operacional.	09/2017
Elaborado por:	Documento	Versión
Coordinación de Seguridad Informática.	Pliego de Prescripciones Técnicas Particulares	V0.8
Área de Planificación, Control y Seguridad		

- *ANSI/AWWA G430-09: Security Practices for Operations and Management.*
- *NIST SP 800-82 Rev.2 ("Guide to Industrial Control Systems (ICS) Security").*
- *ISA-99: Security Guidelines for Industrial Automation and Control Systems.*
- *ISA/IEC 62443: Industrial Automation and Control Systems (IACS) Security.*
- *El Esquema Nacional de Seguridad Industrial (ENSI).*
- **CCN-STIC-480 Seguridad en sistemas SCADA.**
 - CCN-STIC-480A SCADA - Guía de buenas prácticas.
 - CCN-STIC-480B SCADA - Comprender el riesgo del negocio.
 - CCN-STIC-480C SCADA - Implementar una arquitectura segura.
 - CCN-STIC-480D SCADA - Establecer capacidades de respuesta.
 - CCN-STIC-480E SCADA - Mejorar la concienciación y las habilidades.
 - CCN-STIC-480F SCADA - Gestionar el riesgo de terceros.
 - CCN-STIC-480G SCADA - Afrontar proyectos.
 - CCN-STIC-480H SCADA - Establecer una dirección permanente
- *Agence nationale de la sécurité des systèmes d'information (ANSSI): Profils de Protection Pour Les Systèmes Industriels.*

Dado que el listado anterior no pretende ser exhaustivo, complementándolo se tendrá en cuenta toda otra normativa existente y aplicable en materia de seguridad de la información en el ámbito de análisis y gestión de riesgos, así como toda normativa legal aplicable al ámbito de la presente contratación.

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A.	Plan Director de Seguridad de la Tecnología Operacional.	09/2017
Elaborado por:	Documento	Versión
Coordinación de Seguridad Informática.	Pliego de Prescripciones Técnicas Particulares	V0.8
Área de Planificación, Control y Seguridad		

7.6. Equipo de trabajo.

El licitador habrá de identificar de forma expresa en el Plan de Recursos del PGGPAT los equipos ofertados.

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

- Descripción de las categorías profesionales necesarias, incluyendo las tareas y actividades a realizar por cada una, así como las responsabilidades a asumir.
- Número de personas dedicadas al proyecto por cada categoría profesional.
- Perfil profesional asociado a cada puesto de trabajo.
- Dedicación, en jornadas, de cada uno de los perfiles.
- Declaración expresa del cumplimiento de los requisitos técnicos y laborales exigidos en el Apartado 5 del ANEXO I del PCAP.

Los datos se detallarán en el formulario adjunto al presente pliego como ANEXO 1. Además, se debe incluir una tabla con la distribución de perfiles asignados.

El adjudicatario deberá constituir el equipo de trabajo ofertado en el plazo máximo de 15 días desde la fecha de firma del Acta de Inicio. En caso contrario el adjudicatario incurrirá en la penalidad correspondiente como queda reflejado en el Apartado 9 del ANEXO I del PCAP.

Para la conformidad definitiva por parte de Canal de Isabel II del equipo de proyecto, el adjudicatario presentará a Canal de Isabel II los certificados técnicos y laborales requeridos en el Apartado 5 del ANEXO I del PCAP.

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A.	Plan Director de Seguridad de la Tecnología Operacional.	09/2017
Elaborado por:	Documento	Versión
Coordinación de Seguridad Informática.	Pliego de Prescripciones Técnicas Particulares	V0.8
Área de Planificación, Control y Seguridad		

Canal de Isabel II considera un factor clave para el éxito del proyecto la permanencia de ciertas personas en el equipo del proyecto para la ejecución de determinadas tareas. Además, si bien entiende que la gestión de su personal es responsabilidad del Adjudicatario, desea mantener un nivel de rotación de personal limitado, con el fin de ayudar a evitar riesgos en la entrega de los servicios. En el ANS se han incluido parámetros concentrados en medir estos requisitos referidos al personal.

La composición de los equipos de trabajo no podrá ser modificada sin el consentimiento expreso del Canal de Isabel II. Cualquier modificación en los equipos de trabajo suscitada por el Adjudicatario requerirá de 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 los 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 al incumplimiento del parámetro correspondiente del ANS.

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A.	Plan Director de Seguridad de la Tecnología Operacional.	09/2017
Elaborado por:	Documento	Versión
Coordinación de Seguridad Informática.	Pliego de Prescripciones Técnicas Particulares	V0.8
Área de Planificación, Control y Seguridad		

7.7. Organización, Seguimiento y Control de los trabajos asociados al Servicio S2.

En el PGGPAT, a través del Plan de Comunicación, se establecerá el modelo para la prestación, organización, seguimiento y control de los trabajos asociados al servicio contratado.

El adjudicatario deberá acometer las siguientes acciones, especificadas por fases:

Fase de Análisis de Requisitos

1. El Jefe de Proyecto coordinador del contrato por parte del adjudicatario deberá designar un consultor y/o analista de su equipo de trabajo para que inicie el análisis de requisitos y del contexto de las necesidades planteadas por Canal de Isabel II en un plazo igual o inferior al determinado en el ANS desde que le sea requerido formalmente.
2. Entregará a Canal de Isabel II un documento de requisitos en un plazo igual o inferior al determinado en el ANS desde el inicio del análisis de requisitos. El documento de requerimientos habrá de ser aprobado por Canal de Isabel II.
3. Los trabajos realizados por el adjudicatario para la elaboración del documento de requisitos no serán facturables salvo que su propuesta de ejecución sea aceptada definitivamente por Canal de Isabel II.

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A.	Plan Director de Seguridad de la Tecnología Operacional.	09/2017
Elaborado por:	Documento	Versión
Coordinación de Seguridad Informática	Pliego de Prescripciones Técnicas Particulares	V0.8
Área de Planificación, Control y Seguridad		

Fase de Ejecución Valorada.

El adjudicatario deberá elaborar un documento que será la propuesta de ejecución valorada, y contendrá la planificación y previsión de esfuerzos para la realización de las tareas identificadas en el documento de requisitos. Este documento será la referencia para el seguimiento del ANS en cuanto a calidad y eficacia de la planificación.

Este documento contendrá, al menos:

- Identificación del alcance.
- Fecha prevista de entrega del Plan de Gestión del Proyecto (si lo hubiera).
- Fecha prevista de inicio de cada una de las fases del proyecto.
- Fecha prevista de fin del proyecto y de cada una de sus fases.
- Recursos necesarios para la realización de los trabajos (perfiles y horas previstas).
- Relación de entregables.
- Coste de los trabajos.

Fase de Realización de los Trabajos.

1. El adjudicatario deberá constituir el equipo de trabajo e iniciar la ejecución de los trabajos en un plazo igual o inferior al determinado en el ANS desde el momento de aceptación de la propuesta de ejecución valorada por parte de Canal de Isabel II, salvo que Canal de Isabel II considere que es necesario realizar un Plan de Gestión del Proyecto, en cuyo caso, el plazo determinado en el ANS comenzará a contar desde el momento de la aceptación por parte de Canal de Isabel II del Plan de Gestión del Proyecto. En ambos casos, Canal de Isabel II puede determinar a su único criterio una fecha alternativa (siempre posterior) a la que se obtenga de aplicar el plazo descrito en el ANS. En este caso, superar esta fecha sin que se hubieran iniciado los trabajos tendrá la consideración de que el plazo determinado en el ANS ha sido incumplido.

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A.	Plan Director de Seguridad de la Tecnología Operacional.	09/2017
Elaborado por:	Documento	Versión
Coordinación de Seguridad Informática.	Pliego de Prescripciones Técnicas Particulares	V0.8
Área de Planificación, Control y Seguridad		

2. Si, debido a la envergadura o criticidad de los trabajos o asistencias, Canal de Isabel II considerara que éstos tienen la entidad suficiente para ser gestionados como un proyecto, el adjudicatario deberá proponer un Plan de Gestión del Proyecto conforme a la metodología y procedimientos de trabajo desarrollados por Canal de Isabel II según el estándar PMI de Gestión de Proyectos y acorde con la envergadura del mismo. Para ello se realizarán las entrevistas que se consideren necesarias. Este Plan de Gestión del Proyecto ha de ser aprobado por Canal de Isabel II. El Plan deberá contemplar los siguientes planes subsidiarios:
 - (i) Plan de Gestión del Alcance. Se detallarán los diferentes paquetes de trabajo que conformen el alcance el proyecto, incluyendo, en su caso, planes de formación y de gestión del cambio.
 - (ii) Plan Gestión del Tiempo/Cronograma.
 - (iii) Plan de Gestión de Costes. Una vez aprobada la Propuesta de Ejecución Valorada, cada proyecto se comportará en cuanto a costes como un proyecto cerrado. Para realizar el seguimiento del mismo habrá que estimar el coste de cada uno de los paquetes de trabajo.
 - (iv) Plan de Gestión de Riesgos/Contingencias.
 - (v) Plan de Gestión de Recursos. En este plan se tendrán en cuenta los diferentes equipos de trabajo que puedan participar en los diferentes paquetes de trabajo del proyecto.
 - (vi) Plan de Gestión de la Comunicación.
 - (vii) Plan de Gestión de la Calidad.
3. Si, de la necesidad planteada por Canal de Isabel II, se derivara la necesidad de presentar un diseño previo para su aprobación, el adjudicatario deberá realizar un documento de diseño técnico y funcional que habrá de ser aceptado formalmente por Canal de Isabel II antes del inicio de los trabajos. El diseño de la solución incluirá la documentación necesaria para su implementación. Si el diseño no cumple las expectativas de Canal de Isabel II, podrá solicitar su modificación o dar por finalizado el trabajo sin incurrir en otros costes que los estimados en la propuesta para el diseño.
4. El adjudicatario realizará los trabajos necesarios, comunicará su finalización a Canal de Isabel II por los medios acordados por ambas partes y realizará la entrega de todos los productos y documentación generados en los trabajos para su validación por Canal de

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A.	Plan Director de Seguridad de la Tecnología Operacional.	09/2017
Elaborado por:	Documento	Versión
Coordinación de Seguridad Informática.	Pliego de Prescripciones Técnicas Particulares	V0.8
Área de Planificación, Control y Seguridad		

Isabel II. En caso de no ser aprobados por Canal de Isabel II, debido a errores o falta de adecuación a los requisitos, Canal de Isabel II lo hará constar al adjudicatario para su revisión y subsanación sin cargo adicional. Este proceso se repetirá hasta un máximo de tres (3) veces, es decir, si la cuarta vez que el adjudicatario hace entrega a Canal de Isabel II de los resultados previstos del proyecto, dichos resultados no cumplen con los requisitos y el alcance previsto, Canal de Isabel II quedará liberado del compromiso de pago de dicho proyecto.

5. El adjudicatario realizará las labores de cierre del proyecto y análisis de lecciones aprendidas.

Fase de Plan de Pruebas

1. Para aquellos trabajos o asistencias que así lo requieran, el adjudicatario deberá desarrollar y ejecutar un Plan de Pruebas destinado a garantizar la calidad de los trabajos desarrollados.
2. El adjudicatario deberá realizar la correcta ejecución del plan de pruebas, como paso previo para la aceptación de los trabajos o asistencias por parte del Canal de Isabel II.

Fase de Soporte a la Puesta en Producción

1. Para aquellos trabajos que, por su naturaleza, así lo requieran o que proporcionen soluciones técnicas que hayan de ser desplegadas en entornos productivos, el adjudicatario deberá proveer soporte a su despliegue para garantizar su correcta puesta en marcha.

El horario de prestación del servicio en estos dos ámbitos será de 10 x 5, ajustándose a las necesidades de horario requeridas por Canal de Isabel II.

Para aquellos trabajos enmarcados en este servicio cuya ejecución obligue a la realización de tareas fuera del horario laboral que, para el objeto de este concurso, se establece en la franja

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A.	Plan Director de Seguridad de la Tecnología Operacional.	09/2017
Elaborado por:	Documento	Versión
Coordinación de Seguridad Informática.	Pliego de Prescripciones Técnicas Particulares	V0.8
Área de Planificación, Control y Seguridad		

horaria comprendida entre las 8:00 y las 18:00 horas de lunes a viernes rigiéndose el calendario de festivos autonómicos de la Comunidad de Madrid, Canal de Isabel II, siempre que el proveedor demuestre suficientemente dichos trabajos, aplicará a las tarifas establecidas en la oferta los siguientes incrementos:

- Trabajos realizados de lunes a viernes fuera del horario laboral: 25%
- Trabajos realizados en sábados o festivos:..... 50%

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A.	Plan Director de Seguridad de la Tecnología Operacional.	09/2017
Elaborado por:	Documento	Versión
Coordinación de Seguridad Informática.	Pliego de Prescripciones Técnicas Particulares	V0.8
Área de Planificación, Control y Seguridad		

7.8. Formación y transferencia de conocimiento.

Los licitantes incluirán en su oferta una propuesta de Plan de Formación con identificación y especificación de los contenidos y la planificación de las acciones formativas que considere necesarias. La formación y su documentación figurarán como entregables del proyecto y, por lo tanto, deberán figurar en el Plan de Alcance como un paquete más de trabajo, dado que el adjudicatario impartirá la formación identificada y suministrará el material formativo que sea necesario. El objetivo es garantizar que el personal de Canal de Isabel II implicado en el proyecto cuente con los conocimientos adecuados.

Adicionalmente al Plan de Formación identificado, durante la ejecución de los trabajos objeto del contrato, el adjudicatario se compromete a facilitar en todo momento a las personas designadas a tales efectos por Canal de Isabel II, la información y documentación que se solicite para disponer de un pleno conocimiento de las circunstancias en que se desarrollan los trabajos, los problemas detectados, los que puedan plantearse y que puedan surgir en una evolución futura, así como de las tecnologías, métodos y herramientas (incluyendo configuraciones de las mismas) disponibles y utilizadas para identificarlos, verificarlos y resolverlos.

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A.	Plan Director de Seguridad de la Tecnología Operacional.	09/2017
Elaborado por:	Documento	Versión
Coordinación de Seguridad Informática.	Pliego de Prescripciones Técnicas Particulares	V0.8
Área de Planificación, Control y Seguridad		

7.9. Lugar de realización de los trabajos asociados al servicio.

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 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 propias licencias de uso de las herramientas necesarias para la ejecución de los trabajos objeto de este pliego, salvo aquellas identificadas expresamente como que serán proporcionadas por Canal de Isabel II.
- Para la gestión del proyecto el adjudicatario utilizará la herramienta CA Clarity PPM implantada en Canal de Isabel II.

En caso de que sea necesario, y así se determine, el adjudicatario:

- se compromete a utilizar los procedimientos y sistemas de reporte 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.
- utilizará sus propias licencias de uso de las herramientas de desarrollo, 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 el Canal de Isabel II.

Empresa	Proyecto	Fecha
Canal de Isabel II Gestión, S.A.	Plan Director de Seguridad de la Tecnología Operacional.	09/2017
Elaborado por:	Documento	Versión
Coordinación de Seguridad Informática.	Pliego de Prescripciones Técnicas Particulares	V0.8
Área de Planificación, Control y Seguridad		

8. CONDICIONES DE ACEPTACIÓN, GARANTÍA Y MANTENIMIENTO.

El adjudicatario comunicará por escrito a Canal de Isabel II la entrega de los trabajos objeto 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 **12 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. Esta garantía no será aplicable a aquellas partes a las que, en dicho periodo, Canal de Isabel II realice modificaciones por su cuenta, incluyendo implantaciones de nuevas funcionalidades.

Empresa	Proyecto	Fecha
Canal de Isabel II Gestión, S.A.	Plan Director de Seguridad de la Tecnología Operacional.	09/2017
Elaborado por:	Documento	Versión
Coordinación de Seguridad Informática.	Pliego de Prescripciones Técnicas Particulares	V0.8
Área de Planificación, Control y Seguridad		

9. 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 en formato electrónico de la oferta. En caso de discrepancia prevalecerá la copia en papel.

La estructura de la oferta se encuentra detallada en el **Apartado 6 del ANEXO I del PCAP** por lo que **no se valorarán las ofertas que no se ajusten a la estructura indicada.**

Septiembre de 2017

P.A.

Enrique Rubio Donis

Jefe del Área de Planificación, Control y Seguridad

Ángel Rodríguez García

Subdirector de Sistemas Informáticos



Pablo Galán González

Director de Recursos

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A.	Plan Director de Seguridad de la Tecnología Operacional.	09/2017
Elaborado por:	Documento	Versión
Coordinación de Seguridad Informática.	Pliego de Prescripciones Técnicas Particulares	V0.8
Área de Planificación, Control y Seguridad		

ANEXO 1. CUESTIONARIO PERSONAL

Cuestionario por persona del equipo propuesto.

Identificador del recurso	
Categoría ofertada	

Antigüedad en la empresa, antigüedad en la categoría y experiencia en trabajos similares a los del objeto de este contrato.

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 Tecnologías Operacionales.

Curso	Impartido por	Horas	Fecha inicio

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

Certificaciones exigidas

Módulo/Tecnología	Fecha de Certificación	Nivel de Certificación

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A.	Plan Director de Seguridad de la Tecnología Operacional.	09/2017
Elaborado por:	Documento	Versión
Coordinación de Seguridad Informática.	Pliego de Prescripciones Técnicas Particulares	V0.8
Área de Planificación, Control y Seguridad		

Experiencia Profesional

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

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A.	Plan Director de Seguridad de la Tecnología Operacional.	09/2017
Elaborado por:	Documento	Versión
Coordinación de Seguridad Informática.	Piiego de Prescripciones Técnicas Particulares	V0.8
Área de Planificación, Control y Seguridad		

ANEXO 2. REFERENCIAS

Se relacionarán únicamente los proyectos con características similares al objeto de este contrato, que estén activos o que hayan finalizado en fecha posterior a enero de 2015.

Nombre Empresa	Fecha inicio	Fecha fin	Nº recursos % Dedicación	Jornadas contratadas o importe	Funcionalidad implantada	¿Certificado de buena ejecución?

Para la columna "¿Certificado de buena ejecución?":

- En caso de contestar "Sí" en dicha columna, se deberá proporcionar copia de éste para su verificación por parte de Canal de Isabel II.
- En caso de que contestar "No" en dicha columna, de deberá proporcionar declaración responsable y persona(s) de contacto en la empresa destinataria del proyecto reflejado, para su verificación por parte de Canal de Isabel II.

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A.	Plan Director de Seguridad de la Tecnología Operacional	09/2017
Elaborado por	Documento	Versión
Coordinación de Seguridad Informática	Pliego de Prescripciones Técnicas Particulares	V0.8
Área de Planificación, Control y Seguridad		

ANEXO 3. TABLA ACUERDO DE NIVEL DE SERVICIO (ANS).

Calidad del Servicio

Código	Parámetro	Descripción	Cálculo	KPI	Peso	Vc	Va	Vi
CLS02	Calidad y completitud de los análisis previos de la necesidad	Este parámetro mide la calidad y completitud de los documentos de requisitos. Una merma significativa en estos aspectos provocará la devolución por parte de Canal de Isabel II del documento al adjudicatario para su revisión y reformulación.	Documentos devueltos por Canal de Isabel II en su primera entrega del conjunto de los trabajos cerrados en el periodo de medición del parámetro: si el número de trabajos es igual o inferior a 10 en el periodo de medición, los valores de los tramos de control corresponderán a las unidades absolutas, en caso contrario corresponderán al porcentaje de documentos devueltos sobre el total de documentos.	\$	9	0/0%	1/10%	2/20%
CLS04	Calidad y completitud de los Planes de Gestión de Proyectos (PGP)	Este parámetro mide la calidad y completitud de los Planes de Gestión de Proyectos (PGP). Una merma significativa en estos aspectos provocará la devolución por parte de Canal de Isabel II del documento al adjudicatario para su revisión y reformulación.	PGP devueltos por Canal de Isabel II en su primera entrega de los trabajos cerrados en el periodo de medición del parámetro: si el número de documentos es igual o inferior a 10 en el periodo de medición, los valores de los tramos de control corresponderán a las unidades absolutas, en caso contrario corresponderán al porcentaje de documentos devueltos sobre el total de documentos.	\$	9	0/0%	1/10%	2/20%

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A.	Plan Director de Seguridad de la Tecnología Operacional	09/2017
Elaborado por	Documento	Versión
Coordinación de Seguridad Informática	Pliego de Prescripciones Técnicas Particulares	V0.8
Área de Planificación, Control y Seguridad		

CLS05	Calidad y completitud de los diseños técnicos/funcionales	Este parámetro mide la calidad y completitud de los diseños técnicos/funcionales. Una merma significativa en estos aspectos provocará la devolución por parte de Canal de Isabel II del documento al adjudicatario para su revisión y reformulación.	Diseños devueltos por Canal de Isabel II en su primera entrega en el periodo de medición del parámetro: si el número de documentos es igual o inferior a 10 en el periodo de medición, los valores de los tramos de control corresponderán a las unidades absolutas, en caso contrario corresponderán al porcentaje de documentos devueltos sobre el total de documentos.	\$	9	0/0%	1/10%	2/20%
CLS06	Eficacia en el inicio de los trabajos de la Fase de Análisis de Requisitos	Este parámetro mide la desviación, respecto del plazo máximo, en el inicio de la Fase de Análisis de Requisitos. Dicho plazo máximo se establece en cinco (5) días hábiles desde la fecha de la solicitud expresa por parte de Canal de Isabel II.	Porcentaje de desviación total. Porcentaje de días hábiles totales de retraso en el inicio del conjunto de trabajos cerrados en el periodo de medición del parámetro, sobre el total de días hábiles previstos (Número trabajos *5).	\$	6	0%	10%	20%
CLS08	Eficacia en la realización de los Planes de Gestión de Proyecto (PGP)	Este parámetro mide la desviación, respecto del plazo máximo, en la realización de los Planes de Gestión de Proyecto (PGP) descritos en la Fase de Realización de los Trabajos. Dicho plazo máximo se establece en quince (15) días hábiles desde la aprobación de la Propuestas de Ejecución Valoradas (PEV) correspondiente.	Porcentaje de desviación total. Porcentaje de días hábiles totales de retraso del conjunto de los Planes de Gestión de Proyecto (PGP) correspondientes a los proyectos cerrados en el periodo de medición del parámetro, sobre el total de días hábiles previstos (Número PGP *15).	\$	5	0%	10%	20%

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A.	Plan Director de Seguridad de la Tecnología Operacional	09/2017
Elaborado por	Documento	Versión
Coordinación de Seguridad Informática	Pliego de Prescripciones Técnicas Particulares	V0.8
Área de Planificación, Control y Seguridad		

CLS09	Eficacia en el inicio de los trabajos	Este parámetro mide la desviación, respecto del plazo máximo, en el inicio de los trabajos descritos en la Fase de Realización de los Trabajos. Dicho plazo máximo se establece en cinco (5) días hábiles desde la aceptación del Planes de Gestión de Proyectos (PGP), o si éste no hubiera sido necesario, desde la aprobación de la Propuestas de Ejecución Valoradas (PEV). Si hubiera una fecha pactada de inicio, este plazo se considerará incumplido en el momento en el que esta fecha de inicio fuera superada sin que se hubieran iniciado los trabajos.	Porcentaje de desviación total. Porcentaje de días hábiles totales de retraso del conjunto de los trabajos correspondientes a los proyectos cerrados en el periodo de medición del parámetro, sobre el total de días hábiles previstos (Número trabajos *5).	s	6	0%	10%	20%
CLS10	Rendimiento de Tiempo (SPI)	Rendimiento del dinero planificado en base al cumplimiento del Valor Planificado.	Índice de Rendimiento de Tiempos = Valor Ganado (EV) / Valor Planificado (PV)	10	s	0%	5%	10%

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A.	Plan Director de Seguridad de la Tecnología Operacional	09/2017
Elaborado por	Documento	Versión
Coordinación de Seguridad Informática	Pliego de Prescripciones Técnicas Particulares	V0.8
Área de Planificación, Control y Seguridad		

Gestión ANS

Código	Parámetro	Descripción	Cálculo	Peso	KPI	Vc	Va	Vi
ANS01	Fiabilidad de la información	Fiabilidad de la información facilitada.	Errores detectados en los informes de ANS periódicos, para el período medido.	6,64	s	0	1	2
ANS02	Retrasos en el informe del ANS	Información facilitada según los plazos acordados.	Total de días de retraso en la entrega de los informes de ANS respecto a los plazos acordados.	3,66	s	0	5	10

Empresa	Proyecto	Fecha
Canal de Isabel III, S.A.	Plan Director de Seguridad de la Tecnología Operacional	09/2017
Elaborado por	Documento	Versión
Coordinación de Seguridad Informática Área de Planificación, Control y Seguridad	Pliego de Prescripciones Técnicas Particulares	V0.8

Gestión del Servicio

Código	Parámetro	Descripción	Cálculo	Peso	KPI	Vc	Va	Vi	Código
GSE01	Estabilidad del Equipo	La cantidad de cambios en los recursos asignados a la gestión del servicio (jefe de proyecto) y a la realización de los trabajos.	Número de cambios al año.	9,50	\$	1	2	3	>3
GSE02	Mantenimiento de la capacidad del equipo	Este parámetro mide la estabilidad en la capacidad del equipo, es decir, la agilidad con que el adjudicatario realiza los cambios de personas a requerimiento del propio adjudicatario. Se establece un plazo máximo de 2 semanas naturales desde la fecha de la baja de la persona para realizar la sustitución.	Número total de semanas naturales de retraso en el conjunto de las sustituciones realizadas en el periodo de medición.	15	\$	0	1	2	>2
GSE03	Modelo de Relación (1)	Cumplimiento del modelo de relación definido y acordado.	Incidencias (reuniones no celebradas, o sin la asistencia requerida o sin acta).	3,11	\$	1	2	3	>3

(1)

Canal de Isabel II y el Proveedor definirán el Modelo de Relación, cuyo cumplimiento será medido con la aplicación de este parámetro

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A.	Adecuación a la Ley de Infraestructuras Críticas	09/2017
Elaborado por:	Documento	Versión
Coordinación de Seguridad Informática	Pliego de Prescripciones Técnicas Particulares	V0.8
Área de Planificación, Control y Seguridad		

ANEXO 4. CONDICIONES DE ACCESO A LA RED CORPORATIVA DE DATOS 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 Gestión, S.A. (en adelante, Canal de Isabel II) 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 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 el Canal de Isabel II entregará en un único punto todo el tráfico gestionado de las empresas colaboradoras que conecten a través del mismo con Canal de Isabel II. Esto es, si el operador ya presta servicio a una empresa colaboradora de Canal de Isabel II, la nueva conexión deberá utilizar la infraestructura física existente en Canal de Isabel II 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. 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

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A.	Adecuación a la Ley de Infraestructuras Críticas	09/2017
Elaborado por:	Documento	Versión
Coordinación de Seguridad Informática	Pliego de Prescripciones Técnicas Particulares	V0.8
Área de Planificación, Control y Seguridad		

empresas colaboradoras con Canal de Isabel II. 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, 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 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, 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 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 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 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, con el objeto de disponer de una línea adicional y poder garantizar así la disponibilidad de las comunicaciones.

3. Direccionamiento IP.

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A.	Adecuación a la Ley de Infraestructuras Críticas	09/2017
Elaborado por:	Documento	Versión
Coordinación de Seguridad Informática.	Pliego de Prescripciones Técnicas Particulares	V0.8
Área de Planificación, Control y Seguridad		

La empresa contratista se adecuará a los rangos de direccionamiento IP establecidos por Canal de Isabel II. Se establecerá por parte de Canal de Isabel II un rango IP compatible en el que la empresa contratista se integrará en la RCD de Canal de Isabel II. 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 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 ANEXO, a la dirección de correo electrónico recogida en el Apartado 10.13. "Información y aclaraciones" del PCAP.

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A.	Adecuación a la Ley de Infraestructuras Críticas	09/2017
Elaborado por:	Documento	Versión
Coordinación de Seguridad Informática.	Pliego de Prescripciones Técnicas Particulares	V0.8
Área de Planificación, Control y Seguridad		

ANEXO 5. REQUISITOS DE SEGURIDAD.

El adjudicatario deberá cumplir durante todo el plazo de ejecución del contrato con los siguientes requisitos de seguridad en el acceso a los sistemas de información de Canal de Isabel II.

1. El adjudicatario deberá utilizar el acceso concedido a la RCD y a los sistemas informáticos de Canal de Isabel II, única y exclusivamente para el desempeño de los trabajos identificados y la prestación de los servicios contratados.
2. El adjudicatario deberá adoptar en aquellos equipos de su propiedad que vayan a 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 y de los sistemas informáticos, así como de la información que contienen y a la que tienen acceso.

Estas medidas incluyen, como mínimo, los siguientes puntos:

- El equipo informático o dispositivo hardware estará actualizado con todos los parches y actualizaciones críticas y de seguridad liberadas por el fabricante, tanto del hardware como del sistema operativo.
- El equipo informático o dispositivo hardware deberá mantenerse actualizado mediante la aplicación de los parches y actualizaciones críticas y de seguridad proporcionados por el fabricante, tanto del hardware como del sistema operativo, a la mayor brevedad posible una vez se hayan publicado de forma oficial dichos parches y actualizaciones.
- Siempre que el sistema operativo lo permita, deberá contar con medidas de contención (antivirus, antispymware, etc.) instaladas, activas y actualizadas.

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A.	Adecuación a la Ley de Infraestructuras Críticas	09/2017
Elaborado por:	Documento	Versión
Coordinación de Seguridad Informática	Pliego de Prescripciones Técnicas Particulares	V0.8
Área de Planificación, Control y Seguridad		

- Los equipos destinados a dar servicio al contrato, convenio o acuerdo mantenido con Canal de Isabel II deberán estar aislados de la red propia del adjudicatario.
 - Se deberá mantener informado en todo momento al responsable del contrato en Canal de Isabel II de cualquier cambio en equipos, configuración de los mismos y personal propio o externo que acceda a los recursos proporcionados por Canal de Isabel II para el desempeño de los trabajos y la prestación de los servicios recogidos en el contrato, aportando la adecuada justificación.
3. Canal de Isabel II se reserva el derecho de desconexión en caso de detectar cualquier incidente de seguridad imputable al adjudicatario que pueda comprometer la integridad de la RCD, de los sistemas informáticos y de comunicación de Canal de Isabel II, así como la confidencialidad, integridad y disponibilidad de la información que contienen y/o gestionan.
4. El adjudicatario, en caso de que haya evidencias demostrables de que un incidente de seguridad en Canal de Isabel II es achacable a él, 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 adjudicatario.

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A.	Adecuación a la Ley de Infraestructuras Críticas	09/2017
Elaborado por:	Documento	Versión
Coordinación de Seguridad Informática.	Pliego de Prescripciones Técnicas Particulares	V0.8
Área de Planificación, Control y Seguridad		

- 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 a la mayor brevedad posible al responsable del contrato en Canal de Isabel II.

- Canal de Isabel II se reserva el derecho de realizar las auditorías de seguridad que considere oportunas y necesarias, previa comunicación previa al adjudicatario, para 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 al adjudicatario un plazo razonable para subsanar dichas no conformidades. Si éstas persisten una vez agotado el plazo, podrán ser causa de resolución del contrato según lo establecido en el PCAP.
- En caso de duda sobre alguno de los requisitos de seguridad recogidos en este documento, pueden dirigir sus consultas o dudas, haciendo referencia a los apartados de este ANEXO, a la dirección de correo electrónico recogida en el Apartado 10.13. "Información y aclaraciones" del PCAP.

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A.	Adecuación a la Ley de Infraestructuras Críticas	09/2017
Elaborado por:	Documento	Versión
Coordinación de Seguridad Informática.	Pliego de Prescripciones Técnicas Particulares	V0.8
Área de Planificación, Control y Seguridad		

ANEXO 6. ENTORNO TECNOLÓGICO OPERACIONAL DE CANAL DE ISABEL II.

Las tecnologías asociadas a los recursos ICS/SCADA son:

- Siemens
- Rockwell
- Infoplus21

Canal de Isabel II dispone de dos tipo de PLCs de creación propia (ICAROS y TESEOS) que utilizan comunicación UDP.

Empresa	Proyecto	Fecha
Canal de Isabel II, S.A.	Adecuación a la Ley de Infraestructuras Críticas	09/2017
Elaborado por:	Documento	Versión
Coordinación de Seguridad Informática	Pliego de Prescripciones Técnicas Particulares	V0.8
Área de Planificación, Control y Seguridad		

ANEXO 7. INSTALACIONES FÍSICAS DE CANAL DE ISABEL II.

Relación de instalaciones físicas de Canal de Isabel II incluidas en el alcance del proyecto. Entre ellas, se encuentran las seis (6) catalogadas por el CNPIC como Infraestructura Crítica:

- ETAP de Colmenar
- ETAP de Valmayor
- ETAP de Majadahonda
- Presa de El Atazar
- Presa de Valmayor
- Canal de El Atazar
- Depósito Elevado de El Goloso
- Depósito de Agua Regenerada de Arroyo del Soto
- EBAR de Villaviciosa de Odón
- EDAR de Arroyo de la Vega
- EDAR La China
- Depuradora de Arroyo del Soto
- Tanque de tormenta de Arroyo del Fresno
- Elevadora Arganda II