

**Pliego de Prescripciones Técnicas para la  
Contratación de Servicios de Centro de  
Operaciones de Seguridad (SOC) y Oficina  
Técnica de Seguridad (OTS) para Canal de  
Isabel II Gestión, S.A.**

**(PROYECTO SOCOTS) 104/2015**

Madrid, noviembre de 2015

Empresa	Proyecto	Fecha
Canal de Isabel II Gestión, S.A.	Centro de Operaciones de Seguridad (SOC) y Oficina Técnica de Seguridad (OTS)	11/2015
Elaborado por:	Documento	Versión
Coordinación de Seguridad Informática.	Pliego de Cláusulas Técnicas Particulares	V0.17
Área de Planificación, Control y Seguridad		

## Índice

<b>1. INTRODUCCIÓN .....</b>	<b>5</b>
<b>2. OBJETIVOS DEL PROYECTO .....</b>	<b>6</b>
<b>3. ALCANCE .....</b>	<b>8</b>
3.1. Alcance de la Seguridad Proactiva. ....	9
3.2. Alcance de la Seguridad Preventiva. ....	12
3.3. Alcance de la Seguridad Reactiva. ....	13
3.3.1. Objeto del Servicio de Monitorización de la Seguridad.....	14
3.3.2. Descripción del Servicio de Monitorización de la Seguridad.....	14
3.4. Gestión del Cambio.....	20
3.4.1. Documentación.....	21
3.4.2. Previo al Inicio de los Trabajos objetos del contrato. ....	22
3.4.3. En el ámbito de la Organización, Seguimiento y Control de los trabajos asociados al servicio.....	22
<b>4. ENTORNO TECNOLÓGICO .....</b>	<b>25</b>
<b>5. ACUERDO DE NIVEL DE SERVICIO .....</b>	<b>26</b>
5.1 Medida de los parámetros del ANS.....	26
5.2 Proceso de Revisión del nivel de cumplimiento del ANS.....	26
5.2 Cálculo de Penalizaciones en Parámetros.....	29
5.3 Aplicación del ANS a lo largo del Contrato.....	31
5.4 Terminación del contrato por incumplimiento del ANS.....	32
<b>6. MODELO DE GESTIÓN .....</b>	<b>33</b>
6.1. Gestión de Servicios. ....	33
6.2. Gestión del ANS.....	34
6.3. Gestión de la Relación.....	35
6.3.1. Modelo de Referencia.....	35
6.3.1.1 Comité de Dirección.....	36
6.3.1.2 Comité de Seguimiento y Control. ....	37

Empresa	Proyecto	Fecha
Canal de Isabel II Gestión, S.A.	Centro de Operaciones de Seguridad (SOC) y Oficina Técnica de Seguridad (OTS)	11/2015
Elaborado por:	Documento	Versión
Coordinación de Seguridad Informática.	Pliego de Cláusulas Técnicas Particulares	V0.17
Área de Planificación, Control y Seguridad		

6.3.1.3 Comité Operacional.....	38
6.4. Gestión del Contrato.....	39
<b>7. EJECUCIÓN DE LOS TRABAJOS ASOCIADOS AL SERVICIO.....</b>	<b>41</b>
7.1. Plazos de ejecución.....	41
7.2. Metodología de Gestión de Proyectos.....	41
7.3. Fase 1.- Implantación, configuración y puesta en marcha del Servicio de Monitorización de la Seguridad (trabajos enmarcados en el ámbito de la Seguridad Reactiva).....	44
7.4. Fase 2.- Monitorización y Gestión de la Seguridad (trabajos enmarcados en el ámbito de la Seguridad Reactiva).....	45
7.5. Fase 3.- Asistencia Técnica al Comité Técnico de Seguridad (trabajos enmarcados en los ámbitos de la Seguridad Proactiva y Preventiva). ....	46
7.6. Fase 4.- Devolución de los servicios.....	47
7.7. Metodología para la Gestión de Riesgos.....	49
7.8. Metodologías para los Análisis de Seguridad y Vulnerabilidades.....	50
7.9. Metodología para la Gestión de la Seguridad de la Información.....	50
7.10. Equipo de trabajo.....	51
7.11. Organización, Seguimiento y Control de los trabajos asociados al servicio.....	53
7.11.1. Ámbitos de Seguridad Proactiva y Seguridad Preventiva.....	53
7.11.2. Ámbito de Seguridad Reactiva.....	58
7.12. Formación y transferencia de conocimiento.....	60
7.13. Lugar de realización de los trabajos asociados al servicio.....	61
<b>8. CONDICIONES DE ACEPTACIÓN, GARANTÍA Y MANTENIMIENTO.....</b>	<b>63</b>
<b>9. ESTRUCTURA DE LAS OFERTAS.....</b>	<b>64</b>
<b>ANEXO 1. CUESTIONARIO PERSONAL.....</b>	<b>66</b>
<b>ANEXO 2. REFERENCIAS.....</b>	<b>68</b>
<b>ANEXO 3. TABLAS DE ACUERDO DE NIVEL DE SERVICIO (ANS). ....</b>	<b>69</b>
<b>ANEXO 4. TIPOS DE DISPOSITIVOS Y VOLUMEN DE GB/DÍA EN ORIGEN.....</b>	<b>83</b>
<b>ANEXO 5. CONDICIONES DE ACCESO A LA RED CORPORATIVA DE DATOS DE CANAL GESTIÓN. ....</b>	<b>84</b>

Empresa	Proyecto	Fecha
Canal de Isabel II Gestión, S.A.	Centro de Operaciones de Seguridad (SOC) y Oficina Técnica de Seguridad (OTS)	11/2015
Elaborado por:	Documento	Versión
Coordinación de Seguridad Informática.	Pliego de Cláusulas Técnicas Particulares	V0.17
Área de Planificación, Control y Seguridad		

**ANEXO 6. REQUISITOS DE SEGURIDAD. ....87**

Empresa	Proyecto	Fecha
Canal de Isabel II Gestión, S.A.	Centro de Operaciones de Seguridad (SOC) y Oficina Técnica de Seguridad (OTS)	11/2015
Elaborado por:	Documento	Versión
Coordinación de Seguridad Informática.	Pliego de Cláusulas Técnicas Particulares	V0.17
Área de Planificación, Control y Seguridad		

## 1. INTRODUCCIÓN.

Canal de Isabel II Gestión, S.A. (en adelante, Canal Gestión) consciente de la importancia de la seguridad de la información emprendió un proceso para su gestión integral, que se inició con el desarrollo del Plan Director de Seguridad (proyecto PERSEO) basado en la norma internacional UNE-ISO/IEC 27001 y en las buenas prácticas de la seguridad de la información comúnmente aceptadas, y que dio como resultado una Política de Seguridad de la Información y Continuidad de Negocio, como pilar fundamental en el desarrollo de dicho Plan Director de Seguridad, y la definición de un claro objetivo: la reducción de los riesgos en seguridad identificados en el análisis de cumplimiento de la norma ISO/IEC 27002.

Para la consecución de este objetivo de reducción del riesgo existente, se identificó un Plan de Acción, detallado en distintas iniciativas en materia de seguridad de la información. Para gestionar dichas iniciativas de manera conjunta, se puso en marcha un comité con funciones específicas en materia de seguridad: el Comité de Coordinación de la Seguridad de la Información (CCSI).

La creciente complejidad y criticidad de la gestión de la seguridad de la información y de los sistemas de información de Canal Gestión que la gestionan y que permiten sostener su actividad, hace necesario disponer de un Centro de Operaciones de Seguridad (SOC) y una Oficina Técnica de Seguridad (OTS) que aporte conocimientos y recursos especializados para responder con garantías a los requisitos que, cada vez más, se plantean, consolidando las iniciativas ya implantadas y permitiendo continuar en el camino tanto de minimizar los riesgos identificados como afrontar los nuevos que se detecten, al tiempo que se garantiza el cumplimiento legal vigente, y con el alineamiento con las directrices corporativas, la normativa internacional adoptada y con las mejores prácticas comúnmente aceptadas en el ámbito de la seguridad de la información.

Empresa	Proyecto	Fecha
Canal de Isabel II Gestión, S.A.	Centro de Operaciones de Seguridad (SOC) y Oficina Técnica de Seguridad (OTS)	11/2015
Elaborado por:	Documento	Versión
Coordinación de Seguridad Informática.	Pliego de Cláusulas Técnicas Particulares	V0.17
Área de Planificación, Control y Seguridad		

## 2. OBJETIVOS DEL PROYECTO.

El objetivo del proyecto es la contratación de un Servicio de Operación de la Seguridad (en adelante, SOC) y un Servicio de Oficina Técnica de Seguridad (en adelante, OTS) que tendrá como misión la estrecha colaboración con el Comité Técnico de Seguridad (integrado dentro del CCSI, proporcionándole asesoramiento y apoyo), para ayudarle en la gestión de los riesgos relacionados con el desarrollo, mantenimiento y utilización de los sistemas informáticos e infraestructuras tecnológicas corporativas de Canal Gestión, teniendo en cuenta los requisitos de negocio y garantizando la integridad, disponibilidad y confidencialidad de la información corporativa y de los sistemas de información que la albergan y gestionan, así como la garantía en el cumplimiento de los requisitos legales que sean de aplicación y del desarrollo y consolidación tanto de la Política de Seguridad de la Información y Continuidad de Negocio como de toda la normativa interna que emana de ella, a través de su definición, implantación y verificación de su cumplimiento.

Por lo tanto, es necesario disponer de una empresa especialista en Seguridad de la Información y en Seguridad Gestionada, que posea un SOC certificado y un equipo de personas especializadas y con capacidad suficiente para afrontar tanto los dominios que componen la seguridad de la información como el amplio abanico de las tareas de seguridad de la información que los forman, tanto a nivel operativo y jurídico como técnico, por lo que deberá tener una visión global que permita la prestación de un servicio integral de seguridad de la información a Canal Gestión.

Empresa	Proyecto	Fecha
Canal de Isabel II Gestión, S.A.	Centro de Operaciones de Seguridad (SOC) y Oficina Técnica de Seguridad (OTS)	11/2015
Elaborado por:	Documento	Versión
Coordinación de Seguridad Informática.	Pliego de Cláusulas Técnicas Particulares	V0.17
Área de Planificación, Control y Seguridad		

Para garantizar esta visión global a través de la supervisión continua de la seguridad que proporciona un SOC y una OTS, se han de considerar tres focos de actuación:

1. **Seguridad Proactiva**, que tendrá como objetivo la implantación y mejora continua del proceso de gestión de la seguridad alineado con las buenas prácticas internacionales de seguridad y la legislación aplicable.
2. **Seguridad Preventiva**, que tendrá como objetivo incorporar los mecanismos necesarios de vigilancia que permitan anticipar la posible ocurrencia de incidentes de seguridad, aplicando para ello las medidas correctoras más adecuadas.
3. **Seguridad Reactiva**, que tendrá como objetivos, entre otros, la mejora del control y del nivel de seguridad de los sistemas informáticos corporativos, la mejora en los plazos de detección, evaluación y respuesta a los posibles incidentes de seguridad que se produzcan, disminuir el riesgo ante las amenazas actuales (*phishing*, fraude, virus y malware en general, denegación de servicio, intrusión, robo o filtración de información, pérdida de datos, etc.), el acceso a mejores mecanismos y herramientas de seguridad, la monitorización de la seguridad a través de la integración de los eventos de los distintos sistemas de seguridad, así como disponer de un equipo especializado para la actuación ante posibles incidentes de seguridad.

Empresa	Proyecto	Fecha
Canal de Isabel II Gestión, S.A.	Centro de Operaciones de Seguridad (SOC) y Oficina Técnica de Seguridad (OTS)	11/2015
Elaborado por:	Documento	Versión
Coordinación de Seguridad Informática.	Pliego de Cláusulas Técnicas Particulares	V0.17
Área de Planificación, Control y Seguridad		

### 3. ALCANCE.

El trabajo a desarrollar al amparo de presente Pliego Técnico será el soporte al Comité de Coordinación de la Seguridad de la Información, siempre a través del Comité Técnico de Seguridad, a través de un SOC y una OTS, en las tareas en las que se consideren necesarias y en el marco del cumplimiento de las funciones y responsabilidades de dicho Comité Técnico y de la Coordinación de Seguridad Informática.

Durante la realización del proyecto se tendrán en cuenta, al menos, los siguientes referentes normativos:

- Familia de Normas ISO 27000:2013 de buenas prácticas y gestión de seguridad de la información.
- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.
- R.D. 1720/2007 de desarrollo de la LOPD.
- Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la Sociedad de la Información.
- Ley 8/2011 de Protección de Infraestructuras Críticas (LPIC).
- R.D. 704/2011 que aprueba el Reglamento de Protección de Infraestructuras Críticas.
- Resolución del 15 de Noviembre de 2011 de la Secretaría de Estado Seguridad (contenidos mínimos de los Planes de Seguridad del Operador (PSO) y de los Planes de Protección Específicos (PPE)).



Empresa	Proyecto	Fecha
Canal de Isabel II Gestión, S.A.	Centro de Operaciones de Seguridad (SOC) y Oficina Técnica de Seguridad (OTS)	11/2015
Elaborado por:	Documento	Versión
Coordinación de Seguridad Informática.	Pliego de Cláusulas Técnicas Particulares	V0.17
Área de Planificación, Control y Seguridad		

### 3.1. Alcance de la Seguridad Proactiva.

Tendrá como objetivo la implantación y mejora continua de un proceso de gestión de la seguridad alineado con las buenas prácticas internacionales de seguridad, la legislación aplicable y la normativa interna de Canal Gestión. Los servicios que se consideran son, al menos:

- o Sistema de gestión de la seguridad conforme a UNE-ISO/IEC 27001:2013 y UNE-ISO/IEC 27002:2013.
- o Adecuación legal a la LOPD, RLOPD, Ley 11/07 LAECSP, LISI, así como otras normas o legislaciones a nivel autonómico, nacional o internacional de seguridad que sean de aplicación o de relevancia.
- o Adecuación a la Ley 8/11 Protección Infraestructuras Críticas.
- o Apoyo experto a la evolución del actual Marco Normativo de la seguridad de la información en, al menos:
  - Revisión, propuesta y actualización de la Política de Seguridad de la Información y Continuidad de Negocio.
  - Propuesta y creación de políticas y procedimientos generales de seguridad, y su desarrollo asociado a través de las guías, manuales, normas de uso, buenas prácticas, normativas e instrucciones técnicas necesarias.
- o Integración de la Oficina Técnica de Seguridad en todos aquellos proyectos que requieran de asesoría en materia de Seguridad Informática, para la identificación, definición y propuesta de requisitos de seguridad en el desarrollo y/o implantación, tanto de nuevos sistemas de información como en la evolución de los existentes (correctivos, evolutivos y perfectivos).
- o Definición de requerimientos de seguridad a incluir en los pliegos de contratación según las normas y los requisitos legales existentes que sean de aplicación, así como las políticas, normas y procedimientos aprobados por Canal Gestión o que se consideren necesarios.

Empresa	Proyecto	Fecha
Canal de Isabel II Gestión, S.A.	Centro de Operaciones de Seguridad (SOC) y Oficina Técnica de Seguridad (OTS)	11/2015
Elaborado por:	Documento	Versión
Coordinación de Seguridad Informática.	Pliego de Cláusulas Técnicas Particulares	V0.17
Área de Planificación, Control y Seguridad		

- Apoyo a la formación y concienciación continua en materia de seguridad, abordando, al menos, las siguientes tareas:
  - Apoyo a la acciones de concienciación:
    - ✓ Selección, redacción y composición de los contenidos.
    - ✓ Propuestas de difusión por medios electrónicos (email, intranet corporativa, etc.).
    - ✓ Propuestas de marketing asociado a la divulgación.
  - Elaboración de planes de formación en materias de seguridad.
  - Sesiones puntuales de formación (presenciales y/o por medios virtuales) orientadas a la formación y concienciación en aspectos específicos de la seguridad (por ejemplo, ingeniería social, seguridad informática para personal no técnico, seguridad en el ciclo de vida del desarrollo software, bastionado de sistemas, gestión efectiva de incidentes de seguridad, etc.).
- Mantenimiento del mapa de riesgos corporativos a través de la identificación, actualización y valoración de activos de información, identificación de vulnerabilidades, amenazas y salvaguardas, valoración de los riesgos y revisión/definición de los planes de acción para su mitigación.
- Apoyo a la continuidad de negocio en, al menos, la revisión y propuesta de actualización de:
  - Análisis de Impacto en el Negocio (BIA).
  - La estrategia de continuidad de negocio.
  - Los planes de recuperación ante desastres y de las pruebas de los mismos, así como la revisión de los resultados obtenidos en las pruebas de continuidad, prestando especial atención a las deficiencias observadas que permitan identificar oportunidades y aspectos de mejora.
  - Desarrollo, diseño y ejecución de test de controles sobre los sistemas corporativos de gestión y control de la información financiera (SCIIF).

Empresa	Proyecto	Fecha
Canal de Isabel II Gestión, S.A.	Centro de Operaciones de Seguridad (SOC) y Oficina Técnica de Seguridad (OTS)	11/2015
Elaborado por:	Documento	Versión
Coordinación de Seguridad Informática.	Pliego de Cláusulas Técnicas Particulares	V0.17
Área de Planificación, Control y Seguridad		

o Trabajos y asistencias de consultoría y asesoramiento continuo en todo lo relativo a seguridad de la información, incluyendo la evaluación de tecnologías a través de pruebas de concepto, y prestando especial atención en aquellos aspectos en los que se observen deficiencias. Las áreas de actuación a considerar en este alcance serán, al menos:

- Gestión y de identidades y control de acceso a los sistemas de información.
- Gestión de certificados digitales y firma electrónica.
- Gestión de vulnerabilidades
- Sistemas de Detección/Prevención de Intrusos (IDS/IPS).
- Control de acceso a la red (NAC).
- Seguridad perimetral, filtrado de red y firewalls de aplicaciones web (WAF).
- Gestión de *logs* y correlación de eventos.
- Seguridad en los sistemas de información:
  - ✓ Definición de arquitecturas seguras.
  - ✓ Seguridad en las aplicaciones y servicios (configuraciones seguras).
  - ✓ Seguridad en los procesos
  - ✓ Seguridad en los protocolos de comunicación y en las comunicaciones.
- Seguridad en dispositivos móviles.
- Seguridad en los distintos servicios prestados en la nube (*SaaS, IaaS, PaaS, VDI, etc.*).
- Seguridad en el puesto de trabajo (*end-point*).
- Virus, Troyanos, Gusanos y Malware en general:
  - ✓ Situación actual, tendencias y propuestas de medidas de protección.
  - ✓ Propuesta de procedimiento a seguir en caso de incidente, incluyendo provisión del equipo o grupo de primera intervención.
- Detección, prevención, análisis (tácticas y técnicas) y respuesta ante Amenazas Avanzadas Persistentes (*APTs*).
- Análisis del entorno actual de cumplimiento con respecto a los requerimientos de seguridad recogidos en el estándar de seguridad PCI-DSS vigente en el momento de la ejecución del análisis, pero teniendo también en cuenta la última versión publicada por el PCI-SSC, su fecha de entrada en vigor y los plazos existentes.
- Definición de criterios de acreditación de sistemas.

Empresa	Proyecto	Fecha
Canal de Isabel II Gestión, S.A.	Centro de Operaciones de Seguridad (SOC) y Oficina Técnica de Seguridad (OTS)	11/2015
Elaborado por:	Documento	Versión
Coordinación de Seguridad Informática.	Pliego de Cláusulas Técnicas Particulares	V0.17
Área de Planificación, Control y Seguridad		

### 3.2. Alcance de la Seguridad Preventiva.

Tiene como objetivo incorporar los mecanismos necesarios de vigilancia que permitan anticipar la posible ocurrencia de incidentes de seguridad, aplicando para ello las medidas correctoras más adecuadas. Las áreas de actuación a considerar en este alcance serán, al menos:

- o Ciberinteligencia:
  - ✓ Vigilancia digital: búsqueda en Internet de información relacionada con Canal Gestión, su marca, imagen y servicios, con el objeto de detectar posibles fugas de información, campañas contra su seguridad y/o imagen, fraude, *phishing*, etc. Los ámbitos de búsqueda incluyen, al menos, foros, blogs, redes sociales y redes profesionales, bases de datos de ofertas y demandas de empleo, sitios corporativos de terceros y *sites* personales, metadatos, webs externas a Canal Gestión, canales y foros *underground*, redes alternativas, redes P2P, criptodivisas (Bitcoin, Litecoin, etc.), etc.
  - ✓ Ciberinvestigación para el análisis de datos relevantes.
  - ✓ *Cyber Threat Intelligence*.
- o Enumeración de los diferentes recursos expuestos hacia Internet y que, por tanto, están en riesgo al ser susceptibles de recibir ataques relacionados con su plataforma tecnológica, aplicaciones, arquitectura, implantación y/o desarrollo.
- o Análisis de visibilidad (pasiva y activa), enumeración, identificación y revisión de los dispositivos inalámbricos dentro del área de radiofrecuencia WiFi en las ubicaciones físicas que determine Canal Gestión.
- o Revisión del diseño de los actuales escenarios de uso WiFi y de la evolución prevista de los mismos.
- o Verificación de la eficacia de las medidas de seguridad establecidas a través de los distintos sistemas de seguridad implantados.
- o Análisis del nivel de exposición y riesgo de los sistemas de información que soportan las distintas aplicaciones y servicios existentes.
- o Análisis en profundidad de los mecanismos que gestionan las sesiones de usuario en aplicativos y servicios web, incluyendo la autenticación y autorización de los mismos.
- o Identificación y verificación de las vulnerabilidades y amenazas asociadas a los sistemas de información, aplicaciones y servicios existentes, y análisis de los actuales mecanismos de seguridad desplegados para el control de dichas vulnerabilidades y amenazas.
- o Propuesta de una metodología de desarrollo seguro, así como el desarrollo del marco normativo necesario y relacionado con las distintas tecnologías de programación utilizadas en Canal Gestión (al menos, HTML, XML, Java, .NET y ABAP).
- o Análisis de código fuente (estático y dinámico), tanto en la parte cliente como en la parte servidora.

Empresa	Proyecto	Fecha
Canal de Isabel II Gestión, S.A.	Centro de Operaciones de Seguridad (SOC) y Oficina Técnica de Seguridad (OTS)	11/2015
Elaborado por:	Documento	Versión
Coordinación de Seguridad Informática.	Pliego de Cláusulas Técnicas Particulares	V0.17
Área de Planificación, Control y Seguridad		

- o Buenas prácticas, recomendaciones y propuestas de mejora, securización, bastionado y *hardening* de sistemas, aplicaciones y servicios en base a las arquitecturas y escenarios actuales y previstos, y los distintos problemas detectados. Priorización por esfuerzo (temporal y económico) y beneficios obtenidos (*quickwins*).
- o Soporte al seguimiento y control de las medidas correctoras y planes de acción identificados en los resultados de auditorías de seguridad realizadas por terceros.

### 3.3. Alcance de la Seguridad Reactiva.

El SOC es un centro especializado donde se gestiona la seguridad de la información de una organización a través de la monitorización en tiempo real de su estado.

Tiene como objetivos, entre otros, la mejora del control y del nivel de seguridad de los sistemas informáticos corporativos, la mejora en los plazos de detección, evaluación y respuesta a los posibles incidentes de seguridad que se produzcan, disminuir el riesgo ante las amenazas actuales (malware en general, denegación de servicio, intrusión, robo o filtración de información, pérdida de datos, etc.), el acceso a mejores mecanismos y herramientas de seguridad, integración de los eventos de los distintos sistemas de seguridad, así como disponer de un equipo especializado en seguridad para la actuación ante posibles incidentes.

Las actividades que se consideran dentro de este alcance y que serán llevadas a cabo por el SOC son:

- o Servicio de Monitorización de la Seguridad.
- o Gestión de Incidentes de Seguridad.
- o Servicio de Respuesta ante Incidentes. El licitador deberá proporcionar en su oferta un equipo o Grupo de Intervención Rápida (GIR) para la actuación ante incidentes de seguridad relevantes que se desplace a las instalaciones de Canal Gestión bajo petición. Se proporcionará al menos una bolsa de 375 horas, contempladas dentro del Alcance Máximo del contrato y recogido en el Pliego de Cláusulas Administrativas Particulares como "S3.2 Servicio de Respuesta ante incidentes".
- o Análisis de Malware.
- o Investigación Forense, donde se dotará de plena garantía al proceso de peritaje, recolección, almacenamiento y cadena de custodia de las evidencias obtenidas para, llegado el caso, permitir su presentación, aceptación y validez plena en entornos legales y jurídicos.
- o Uso de Indicadores de Compromiso en la Respuesta a Incidentes de Seguridad y en la Investigación Forense.

Empresa	Proyecto	Fecha
Canal de Isabel II Gestión, S.A.	Centro de Operaciones de Seguridad (SOC) y Oficina Técnica de Seguridad (OTS)	11/2015
Elaborado por:	Documento	Versión
Coordinación de Seguridad Informática.	Pliego de Cláusulas Técnicas Particulares	V0.17
Área de Planificación, Control y Seguridad		

### 3.3.1. Objeto del Servicio de Monitorización de la Seguridad.

El objetivo principal que se persigue es la contratación por parte de Canal Gestión de un servicio de Monitorización de la Seguridad a través de una plataforma de Gestión de Información y Monitorización de Eventos de Seguridad albergada en el SOC del adjudicatario. Dicha plataforma será provisionada, instalada, configurada, optimizada, operada y gestionada por el SOC, recogerá y centralizará los registros y *logs* que contengan información y eventos de seguridad, normalizará, categorizará, agregará, correlacionará y almacenará dichos eventos con un periodo de retención inicial de 365 días, detectando incidentes de seguridad y generando alertas que permitan gestionar los incidentes detectados con la ayuda de una herramienta de toma proactiva de decisiones, y proporcionará una única consola web accesible que permita a Canal Gestión consultar y generar informes y cuadros de mando a partir de las políticas y métricas de riesgo definidas.

### 3.3.2. Descripción del Servicio de Monitorización de la Seguridad.

El licitador deberá proponer y detallar en su oferta el servicio de Monitorización de la Seguridad a Canal Gestión que se prestará desde su SOC a través de dicha plataforma de Gestión de Información y Monitorización de Eventos de Seguridad, que **deberá** contar, al menos, con dos herramientas para la prestación de dicho servicio de Monitorización de la Seguridad:

1. Una solución proactiva de base de datos de conocimiento para la toma de decisiones.
2. Una solución SIEM (*Security Information and Event Management*) integral.

La solución proactiva de base de datos de conocimiento para la toma de decisiones incluirá todos los elementos necesarios para la prestación con garantía del servicio de Monitorización de Seguridad objeto del contrato y **deberá**, al menos, ser compatible con las soluciones SIEM líderes de mercados sin ser estrictamente dependiente de la solución SIEM ofertada por el licitador, prever la posibilidad de almacenar y crear un histórico de las incidencias de seguridad detectadas por la solución SIEM ofertada por el licitador y un registro de las acciones y pasos realizados para solucionar dichas incidencias, así como de la solución final aplicada, actualizando con todo ello, y en tiempo real, la base de datos de conocimiento. Para cada incidencia, debe proponer todas las soluciones posibles disponibles, que podrán ser gestionables. Cada solución propuesta debe estar asociadas a una

Empresa	Proyecto	Fecha
Canal de Isabel II Gestión, S.A.	Centro de Operaciones de Seguridad (SOC) y Oficina Técnica de Seguridad (OTS)	11/2015
Elaborado por:	Documento	Versión
Coordinación de Seguridad Informática.	Pliego de Cláusulas Técnicas Particulares	V0.17
Área de Planificación, Control y Seguridad		

puntuación de *scoring* que ayude a elegir la mejor solución y debe tener una guía asociada, gestionable y estructurada en pasos a ejecutar, debe permitir pedir una nueva solución en caso de que se compruebe que la solución aplicada no es efectiva, y debe disponer de un cuadro de mando personalizable que permita mostrar relaciones estadísticas, al menos, sobre las incidencias recibidas y para las cuales no hay una solución definida en su base de datos y las incidencias detectadas por la solución SIEM ofertada por el licitador.

La solución SIEM integral deberá estar recogida en el grupo de soluciones líderes en el último *Magic Quadrant for Security Information and Event Management* publicado por *Gartner*, e incluirá todos los elementos necesarios para la prestación con garantía del servicio de Monitorización de la Seguridad objeto del contrato, el cual, **deberá** cumplir con todos los condicionantes y requisitos descritos a continuación:

- El servicio deberá proporcionar un análisis de los eventos en tiempo casi real.
- El servicio deberá poder generar alertas basadas en anomalías observadas y cambios en el comportamiento de los flujos de red y en los eventos de seguridad como poder añadir anomalías definidas por Canal Gestión.
- El servicio deberá poder correlacionar y analizar información compleja procedente de diferentes fuentes y sistemas (entornos heterogéneos).
- El servicio deberá proporcionar una recopilación de los eventos sin agentes, siempre que sea posible.
- El servicio deberá proporcionar alertas en base a políticas establecidas (por ejemplo, tráfico de mensajería instantánea no permitido, almacenamiento en la nube no permitido, uso de protocolos no autorizados, equipos con IPs de direccionamientos segmentados/aislados, etc.) y aplicaciones potencialmente peligrosas (*file sharing*, *P2P (Peer to Peer)*, *proxies*, etc.).
- El servicio deberá poder transmitir alertas a través de múltiples protocolos y mecanismos hacia otras soluciones de *ticketing*.
- El servicio deberá poder correlacionar información procedente de fuentes de datos de seguridad de terceros que deben ser actualizadas automáticamente (por ejemplo, geolocalización y detección de fraude por IP, *botnets*, redes *zombie*, redes hostiles conocidas, URLs maliciosas, etc.).

Empresa	Proyecto	Fecha
Canal de Isabel II Gestión, S.A.	Centro de Operaciones de Seguridad (SOC) y Oficina Técnica de Seguridad (OTS)	11/2015
Elaborado por:	Documento	Versión
Coordinación de Seguridad Informática.	Pliego de Cláusulas Técnicas Particulares	V0.17
Área de Planificación, Control y Seguridad		

- El servicio deberá poder establecer sinergias con otros servicios y herramientas de seguridad propias (al menos dos, en distintos continentes y husos horarios) y de terceros (por ejemplo: *feeds* de inteligencia, plataformas de *Cyber Threat Intelligence*, etc.).
- El servicio deberá poder correlacionar resultados proporcionados por herramientas de escaneos de vulnerabilidades de terceros.
- El servicio deberá monitorizar y alertar cuando se produzca una interrupción en la recopilación de registros de una fuente o dispositivo supervisado (por ejemplo, si no se obtienen registros de un determinado servidor en un número de minutos configurado, se debe generar una alerta).
- El servicio deberá ser capaz de descubrir y clasificar activos de forma automática por su tipología (por ejemplo, servidores de correo, servidores de bases de datos, etc.) para minimizar los falsos positivos asociados a una clasificación de activos poco adecuada.
- El servicio deberá mantener una base de datos de todos los activos descubiertos en la red y que dicha base de datos tenga capacidades de búsqueda e incluya información relevante sobre dichos activos como atributos de los mismos, información que podrá ser adquirida tanto de forma automática (por ejemplo, atributos del sistema, atributos de red, vulnerabilidades que les afectan y estado de las mismas, etc.) como establecida de forma manual (por ejemplo, dueño del activo, valoración, clasificación, ubicación, tipo, etc.).
- El servicio deberá soportar y mantener un histórico de la actividad de la autenticación de usuarios en función de cada activo, que permita la generación de informes de auditoría y trazabilidad.
- El servicio deberá ser compatible con los tipos de dispositivos, tipologías y productos, así como soportar el volumen de GB/día **en origen** indicado por cada tipo de dispositivo en el ANEXO 4 - "Tipos de dispositivos y volumen de GB/día en origen" del presente Pliego.
- El servicio deberá correlacionar una secuencia esperada fallida (por ejemplo, que a un servicio parado no le siga el reinicio del servicio en un tiempo configurado).
- El servicio deberá permitir la correlación de valores añadidos en el tiempo (por ejemplo, enviar una alerta cuando una IP origen envía más de un volumen de datos configurado a un solo servicio publicado en una IP destino en una ventana de tiempo configurada).
- El servicio deberá proveer información relacionada con los perfiles de tráfico en términos de número de bytes, frecuencia de paquetes, número de activos en comunicación por aplicación, puertos, protocolos, amenazas u otros posibles puntos de monitorización en la red.



Empresa	Proyecto	Fecha
Canal de Isabel II Gestión, S.A.	Centro de Operaciones de Seguridad (SOC) y Oficina Técnica de Seguridad (OTS)	11/2015
Elaborado por:	Documento	Versión
Coordinación de Seguridad Informática.	Pliego de Cláusulas Técnicas Particulares	V0.17
Área de Planificación, Control y Seguridad		

- El servicio deberá soportar la identificación de aplicaciones más allá del puerto y el protocolo utilizados, identificando aplicaciones que utilizan puertos y protocolos distintos a los conocidos (estándar) y aplicaciones que se tunelizan a sí mismas en otros puertos y protocolos (por ejemplo, si una aplicación de mensajería instantánea tuneliza sus mensajes en protocolo HTTP, debe detectarse la aplicación de mensajería instantánea, no el protocolo HTTP).
- El servicio deberá ser capaz de detectar eventos relacionados con amenazas de tipo "0-day".
- El servicio deberá ser capaz de demostrar proactividad para la alerta temprana y la defensa contra malware y amenazas externas en general.
- El servicio deberá ser capaz de auto-aprender dinámicamente de los patrones de comportamiento analizados (tanto eventos como actividad de red) y alertar sobre actividad anómala que pudiera significar un incidente de seguridad.
- El servicio deberá ser capaz de detectar ataques de tipo DoS (*Denial of Service*) y DDoS (*Distributed Denial of Service*).
- El servicio deberá ser capaz de detectar y mostrar el tráfico relacionado con una amenaza específica observada en la red.
- El servicio deberá soportar la creación de perfiles de tráfico asociados con el diseño lógico de la red, tanto a nivel de dirección IP individual como de rango de redes (por ejemplo, subred/CIDR).
- El servicio deberá ser capaz de perfilar comunicaciones procedentes de o dirigidas hacia Internet por regiones geográficas y en tiempo real.
- El servicio deberá crear perfiles claramente independientes y diferenciados del tráfico local y del tráfico con origen o destino a Internet.
- El servicio deberá permitir la creación personalizada de perfiles de tráfico utilizando cualquiera información relacionada con flujos de red, *logs*, fuentes de *logs* y eventos, o perfiles de tráfico ya existentes.
- El servicio deberá soportar la creación de perfiles de tráfico basados en direcciones IP, grupos de direcciones IP, parejas de direcciones IP origen/destino, etc.
- El servicio deberá identificar claramente el tráfico generado en entornos virtuales.
- El servicio deberá permitir el acceso a los detalles de los eventos de seguridad y de los flujos de red almacenados, al menos, durante 12 meses.

Empresa	Proyecto	Fecha
Canal de Isabel II Gestión, S.A.	Centro de Operaciones de Seguridad (SOC) y Oficina Técnica de Seguridad (OTS)	11/2015
Elaborado por:	Documento	Versión
Coordinación de Seguridad Informática.	Pliego de Cláusulas Técnicas Particulares	V0.17
Área de Planificación, Control y Seguridad		

- El servicio será responsable del análisis y asesoramiento continuo para la mejora de la madurez de la plataforma que presta el servicio de Monitorización de la Seguridad, proponiendo para ello un ciclo de mejora continua para la incorporación de nuevas fuentes, desarrollo de casos de uso, reglas de correlación y detección, objetos estándar y "ad hoc", filtros, informes estándar y custom, alertas, listas, elementos de la base de datos de conocimiento con incidencias y las actuaciones realizadas para su resolución, etc., con el objeto de aprovechar al máximo la plataforma que presta de dicho servicio.
- El servicio deberá proveer un modelo de inteligencia basada en casos de uso.
- El servicio describirá e implantará una metodología para la gestión del ciclo de vida del modelo de inteligencia desplegado, estableciendo para ello un *roadmap* estratégico para la mejora de dicho modelo de inteligencia, que tenga en cuenta, al menos, pero no limitado a, los siguientes aspectos:
  - Casos de uso a medida y personalizados.
  - Categorización de los casos de uso.
  - Optimización de las reglas de correlación y detección.
  - Definición, configuración y aplicación de *parsers*.
  - Alerta temprana contra malware y amenazas en general.
  - Etc.
- El servicio deberá realizar la gestión, análisis y presentación de informes relativos a la prestación del servicio, proporcionar plantillas para la fácil creación y entrega de informes tanto de operación como de negocio (al menos, existirán plantillas estándar para la confección de informes de autenticación, identidad, actividad del usuario, cumplimiento (PCI-DSS, SoX, etc.), marcos y normas de control (NIST, COBIT, ISO, etc.), crear informes personalizados, proporcionar informes históricos, de vulnerabilidades e informes sobre activos y todos los elementos disponibles, gestión de la configuración y de los cambios, informes específicos del dispositivo (*switches*, *routers*, *firewalls*, etc.) y fuentes de *logs* (aplicación, sistema operativo, bases de datos, etc.), informes de la red corporativa de datos (uso y gestión), informes de seguridad y actividad de las aplicaciones, así como permitir programar la ejecución y distribución de dichos informes.
- El servicio deberá tener la capacidad de ofrecer múltiples cuadros de mando que se puedan personalizar para satisfacer las necesidades específicas de Canal Gestión en cuestión de indicadores de seguridad, como pueden ser, entre otros, y sin limitarse a: gestión de amenazas, gestión de cumplimiento, incidentes de seguridad, estadísticas de los dispositivos y fuentes de

Empresa	Proyecto	Fecha
Canal de Isabel II Gestión, S.A.	Centro de Operaciones de Seguridad (SOC) y Oficina Técnica de Seguridad (OTS)	11/2015
Elaborado por:	Documento	Versión
Coordinación de Seguridad Informática.	Pliego de Cláusulas Técnicas Particulares	V0.17
Área de Planificación, Control y Seguridad		

datos supervisadas, Top 10 (amenazas, atacantes, etc.), vistas generales de las redes, servicios y aplicaciones, estado y uso de los activos gestionados, vistas generales de alto nivel de información resumida de datos de incidentes de seguridad, actividad de la red, detalle de eventos y *logs*, etc.

El adjudicatario deberá proveer toda la infraestructura, dispositivos y licencias de software necesarias, y realizar las tareas relacionadas con la instalación, configuración, mantenimiento y garantía de soporte de los respectivos fabricantes de todo el hardware y de todo el software asociado a la prestación del servicio de Monitorización de la Seguridad durante toda la duración del contrato. Todo cambio, sustitución o adquisición que resulten necesarios será responsabilidad del adjudicatario, quien deberá realizar todas las tareas oportunas para garantizar el funcionamiento completo e integral de la plataforma de Gestión de Información y Monitorización de Eventos de Seguridad requerida para la adecuada y completa prestación del servicio de Monitorización de la Seguridad contratado, sin que esto suponga ningún coste añadido para Canal Gestión, sin pérdida de la continuidad del servicio que se presta y sin perjuicio de los plazos establecidos en el Apartado 5.1 del presente Pliego.

El licitador deberá describir en su oferta cómo el servicio de Monitorización de la Seguridad cumple con los requisitos y condicionantes anteriormente expuestos, aportando toda aquella información útil que sea necesaria para permitir a Canal Gestión valorar si el servicio de Monitorización de la Seguridad propuesto cumple o no con dichos requisitos y condicionantes.

**Las ofertas cuya propuesta de servicio de Monitorización de la Seguridad no cumplan con alguno de los condicionantes y requisitos anteriormente expuestos no serán tenidas en cuenta.**

Empresa	Proyecto	Fecha
Canal de Isabel II Gestión, S.A.	Centro de Operaciones de Seguridad (SOC) y Oficina Técnica de Seguridad (OTS)	11/2015
Elaborado por:	Documento	Versión
Coordinación de Seguridad Informática.	Pliego de Cláusulas Técnicas Particulares	V0.17
Área de Planificación, Control y Seguridad		

### 3.4. Gestión del Cambio.

Dadas las implicaciones que conlleva la puesta en marcha en Canal Gestión de servicios de SOC y de una Oficina Técnica de Seguridad, afectando 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 Gestión en la forma que se estime más adecuada, con el objetivo de que Canal Gestión esté debidamente informado sobre la iniciativa en general, y en particular de los cambios que deberán ser realizados en su operativa diaria.

Empresa	Proyecto	Fecha
Canal de Isabel II Gestión, S.A.	Centro de Operaciones de Seguridad (SOC) y Oficina Técnica de Seguridad (OTS)	11/2015
Elaborado por:	Documento	Versión
Coordinación de Seguridad Informática.	Pliego de Cláusulas Técnicas Particulares	V0.17
Área de Planificación, Control y Seguridad		

### 3.4.1. 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** del presente Pliego, y conjuntamente con sus respectivos alcances identificados en el Apartado **3. ALCANCE** del presente Pliego.

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 Gestión.

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 Gestión (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 Gestión, S.A.	Centro de Operaciones de Seguridad (SOC) y Oficina Técnica de Seguridad (OTS)	11/2015
Elaborado por:	Documento	Versión
Coordinación de Seguridad Informática.	Pliego de Cláusulas Técnicas Particulares	V0.17
Área de Planificación, Control y Seguridad		

### 3.4.2. 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. EJECUCIÓN DE LOS TRABAJOS ASOCIADOS AL SERVICIO incluido en este mismo pliego.

### 3.4.3. En el ámbito de la Organización, Seguimiento y Control de los trabajos asociados al servicio.

Informes periódicos de seguimiento de la prestación del servicio. 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 solicitados por Canal Gestión e identificados en los alcances identificados dentro de los ámbitos de Seguridad Proactiva y Seguridad Preventiva:

- Documento de requisitos.
- Propuesta de Ejecución Valorada: documento que contendrá la planificación y previsión de esfuerzos para la realización de las tareas determinadas 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:

- 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.

Empresa	Proyecto	Fecha
Canal de Isabel II Gestión, S.A.	Centro de Operaciones de Seguridad (SOC) y Oficina Técnica de Seguridad (OTS)	11/2015
Elaborado por:	Documento	Versión
Coordinación de Seguridad Informática.	Pliego de Cláusulas Técnicas Particulares	V0.17
Área de Planificación, Control y Seguridad		

- 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).
  - Entregables.
  - Coste de los trabajos.
- 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 Gestión. En este caso, Canal Gestión deberá aprobar la documentación recibida en cuanto a calidad y completitud. En caso de no ser aprobado, Canal Gestión 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 Gestión da la aprobación.
  - Documentos de diseño técnico/funcional, para aquellos trabajos que precisen de la realización de un diseño previo. Canal Gestión deberá aprobar estos entregables en cuanto a calidad y completitud.
  - Documentos acordados en la realización de los trabajos encomendados. Canal Gestión 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 Gestión da la aprobación. El tiempo de aprobación de Canal Gestión 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 Gestión, S.A.	Centro de Operaciones de Seguridad (SOC) y Oficina Técnica de Seguridad (OTS)	11/2015
Elaborado por:	Documento	Versión
Coordinación de Seguridad Informática.	Pliego de Cláusulas Técnicas Particulares	V0.17
Área de Planificación, Control y Seguridad		

El adjudicatario asumirá el sistema de gestión, nomenclatura e identidad visual corporativa de la documentación de Canal Gestión, según la Guía de Referencia de Gestión de Proyectos de Canal Gestión 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](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 Gestión.

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 Gestión, S.A.	Centro de Operaciones de Seguridad (SOC) y Oficina Técnica de Seguridad (OTS)	11/2015
Elaborado por:	Documento	Versión
Coordinación de Seguridad Informática.	Pliego de Cláusulas Técnicas Particulares	V0.17
Área de Planificación, Control y Seguridad		

## 4. ENTORNO TECNOLÓGICO

Los sistemas informáticos corporativos que dan servicio a la actividad diaria de la organización se encuentran centralizados en dos CPDs (Centros de Proceso de Datos) sitos en la Comunidad de Madrid.

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

- Estaciones de trabajo con sistema operativo Windows 7 o superior.
- Estaciones cliente con navegador web basado en Google Chrome at Work e Internet Explorer.
- Controladores de dominio basados en Windows, con un único dominio Windows corporativo.
- Bases de datos Oracle, ADABAS e Interbase-BDE.
- Servidores basados en Windows, Linux y z/OS.
- ERP basado en tecnología SAP.
- Backup basado en tecnología Commvault.
- Almacenamiento SAN y NAS.
- Virtualización basada en tecnología VMware.
- Electrónica de red del fabricante Cisco.
- Monitorización basada en tecnología ForeScout, WhatsUp, Dynatrace y Nagios.

Empresa	Proyecto	Fecha
Canal de Isabel II Gestión, S.A.	Centro de Operaciones de Seguridad (SOC) y Oficina Técnica de Seguridad (OTS)	11/2015
Elaborado por:	Documento	Versión
Coordinación de Seguridad Informática.	Pliego de Cláusulas Técnicas Particulares	V0.17
Área de Planificación, Control y Seguridad		

## 5. ACUERDO DE NIVEL DE SERVICIO.

Se adjunta a este pliego el ANEXO 3 – “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 mensualmente, 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 Gestión.

### 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.

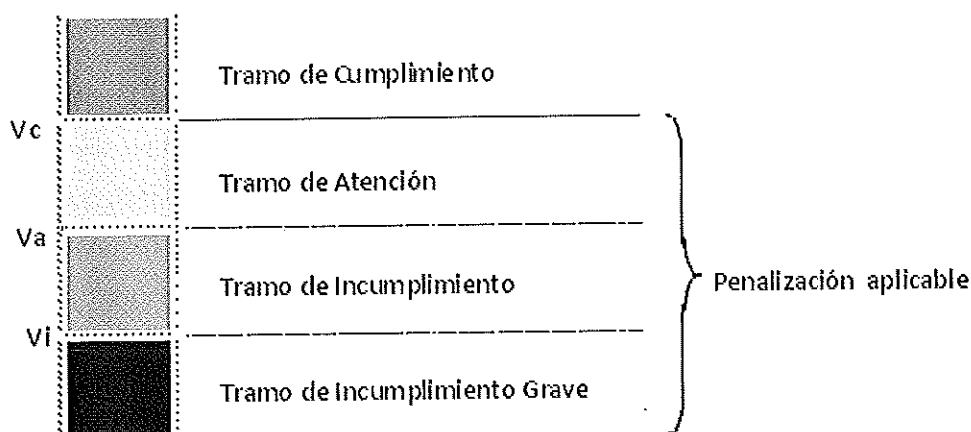
Tal como ya se ha dicho, el Anexo IV recoge el Acuerdo de Nivel de Servicio (ANS) que el adjudicatario se compromete a cumplir para cada parámetro que lo integra.

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 Gestión, S.A.	Centro de Operaciones de Seguridad (SOC) y Oficina Técnica de Seguridad (OTS)	11/2015
Elaborado por:	Documento	Versión
Coordinación de Seguridad Informática.	Pliego de Cláusulas Técnicas Particulares	V0.17
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 Gestión 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.

Empresa	Proyecto	Fecha
Canal de Isabel II Gestión, S.A.	Centro de Operaciones de Seguridad (SOC) y Oficina Técnica de Seguridad (OTS)	11/2015
Elaborado por:	Documento	Versión
Coordinación de Seguridad Informática.	Pliego de Cláusulas Técnicas Particulares	V0.17
Área de Planificación, Control y Seguridad		

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 3 – “Tabla de Acuerdo Nivel de Servicio (ANS)”. Este valor, como se explica más adelante, forma parte de la fórmula para el cálculo de la penalización. Canal Gestión 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 anuales, que deberá notificar e informar convenientemente al adjudicatario con una antelación mínima de dos (2) meses.

El adjudicatario podrá solicitar a Canal Gestión 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 de los parámetros GSE03 a GSE05, siempre que la complejidad de los trabajos a realizar así lo requiera. Canal Gestión se reserva el derecho a aceptar la solicitud del adjudicatario en base a la urgencia que el trabajo tenga para Canal Gestión.

Empresa	Proyecto	Fecha
Canal de Isabel II Gestión, S.A.	Centro de Operaciones de Seguridad (SOC) y Oficina Técnica de Seguridad (OTS)	11/2015
Elaborado por:	Documento	Versión
Coordinación de Seguridad Informática.	Pliego de Cláusulas Técnicas Particulares	V0.17
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 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 Gestión, S.A.	Centro de Operaciones de Seguridad (SOC) y Oficina Técnica de Seguridad (OTS)	11/2015
Elaborado por:	Documento	Versión
Coordinación de Seguridad Informática.	Pliego de Cláusulas Técnicas Particulares	V0.17
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 Gestión 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 Gestión 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 Gestión, un Plan de Acciones Correctivas ("PAC") para todos los incumplimientos de los Parámetros de control del ANS.

Empresa		Proyecto	Fecha
Canal de Isabel II Gestión, S.A.		Centro de Operaciones de Seguridad (SOC) y Oficina Técnica de Seguridad (OTS)	11/2015
Elaborado por:		Documento	Versión
Coordinación de Seguridad Informática.		Pliego de Cláusulas Técnicas Particulares	V0.17
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) trimestre desde su inclusión en el ANS durante el que no se aplicarán penalizaciones.

Empresa	Proyecto	Fecha
Canal de Isabel II Gestión, S.A.	Centro de Operaciones de Seguridad (SOC) y Oficina Técnica de Seguridad (OTS)	11/2015
Elaborado por:	Documento	Versión
Coordinación de Seguridad Informática.	Pliego de Cláusulas Técnicas Particulares	V0.17
Área de Planificación, Control y Seguridad		

## 5.4 Terminación del contrato por incumplimiento del ANS.

Canal Gestión 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 12 meses.
- Si durante tres (3) periodos consecutivos o cuatro (4) periodos alternos en el periodo de los últimos 24 meses, el importe total de la Penalización aplicable supera el 10% 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.

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 Gestión considere que le han sido causados por el adjudicatario con dichos incumplimientos.

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.

Una vez Canal Gestión comunique al adjudicatario la necesidad de terminación del contrato, éste deberá continuar los trabajos hasta que Canal Gestión 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 Gestión, S.A.	Centro de Operaciones de Seguridad (SOC) y Oficina Técnica de Seguridad (OTS)	11/2015
Elaborado por:	Documento	Versión
Coordinación de Seguridad Informática.	Pliego de Cláusulas Técnicas Particulares	V0.17
Área de Planificación, Control y Seguridad		

## 6. MODELO DE GESTIÓN

Canal Gestión 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 Gestión. 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 Gestión.

### 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 Gestión.

El objetivo que persigue Canal Gestión 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 Gestión, si Canal Gestión así lo requiriera, un Manual de Procedimientos conteniendo todos los procesos de Gestión que utilizará, debiendo

Empresa	Proyecto	Fecha
Canal de Isabel II Gestión, S.A.	Centro de Operaciones de Seguridad (SOC) y Oficina Técnica de Seguridad (OTS)	11/2015
Elaborado por:	Documento	Versión
Coordinación de Seguridad Informática.	Pliego de Cláusulas Técnicas Particulares	V0.17
Área de Planificación, Control y Seguridad		

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

Canal Gestión 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 Gestión 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 Gestión, S.A.	Centro de Operaciones de Seguridad (SOC) y Oficina Técnica de Seguridad (OTS)	11/2015
Elaborado por:	Documento	Versión
Coordinación de Seguridad Informática.	Pliego de Cláusulas Técnicas Particulares	V0.17
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 Gestión.
- Asegurar que la relación definida incluye de forma proactiva la innovación TIC y que esta se traduce en beneficios para el Canal Gestión.

En el siguiente apartado se describe el Modelo de Relación (Modelo de Referencia) requerido habitualmente por Canal Gestión. No obstante, Canal Gestión, 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 Gestión 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 Gestión, S.A.	Centro de Operaciones de Seguridad (SOC) y Oficina Técnica de Seguridad (OTS)	11/2015
Elaborado por:	Documento	Versión
Coordinación de Seguridad Informática.	Pliego de Cláusulas Técnicas Particulares	V0.17
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 Gestión 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.
- Revisar el seguimiento de los incidentes de seguridad ocurridos durante la prestación del servicio y la evolución de los planes de acción acordados para su gestión.
- 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.
- En general, discutir cualquier incidencia o problema surgido durante la ejecución del Servicio

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 Gestión, S.A.	Centro de Operaciones de Seguridad (SOC) y Oficina Técnica de Seguridad (OTS)	11/2015
Elaborado por:	Documento	Versión
Coordinación de Seguridad Informática.	Pliego de Cláusulas Técnicas Particulares	V0.17
Área de Planificación, Control y Seguridad		

### 6.3.1.2 Comité de Seguimiento y Control.

En un nivel de gestión táctico, Canal Gestión y el Adjudicatario, ambos, asignarán 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.

Empresa	Proyecto	Fecha
Canal de Isabel II Gestión, S.A.	Centro de Operaciones de Seguridad (SOC) y Oficina Técnica de Seguridad (OTS)	11/2015
Elaborado por:	Documento	Versión
Coordinación de Seguridad Informática.	Pliego de Cláusulas Técnicas Particulares	V0.17
Área de Planificación, Control y Seguridad		

- Seguimiento de los informes de análisis de los incidentes de seguridad ocurridos durante la prestación del servicio y la definición de los planes de actuación identificados.
- Servir como punto único de contacto entre las organizaciones de Canal Gestión y del Adjudicatario para todos los asuntos relacionados nivel de gestión táctico del Servicio.
- 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 Gestión 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.

Empresa	Proyecto	Fecha
Canal de Isabel II Gestión, S.A.	Centro de Operaciones de Seguridad (SOC) y Oficina Técnica de Seguridad (OTS)	11/2015
Elaborado por:	Documento	Versión
Coordinación de Seguridad Informática.	Pliego de Cláusulas Técnicas Particulares	V0.17
Área de Planificación, Control y Seguridad		

- 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.
- Realizar los informes de análisis de los incidentes de seguridad ocurridos durante la prestación del servicio y recoger en ellos los planes de actuación identificados para su resolución y verificación de la misma, además de implantación de los controles detectivos, correctivos, preventivos y/o compensatorios que sean de aplicación según la naturaleza del incidente.
- Servir como interlocutor entre las organizaciones de Canal Gestión 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 Gestión 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 Gestión, o cambios en el entorno de negocio de Canal Gestión. 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.

Empresa	Proyecto	Fecha
Canal de Isabel II Gestión, S.A.	Centro de Operaciones de Seguridad (SOC) y Oficina Técnica de Seguridad (OTS)	11/2015
Elaborado por:	Documento	Versión
Coordinación de Seguridad Informática.	Pliego de Cláusulas Técnicas Particulares	V0.17
Área de Planificación, Control y Seguridad		

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:

- 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 Gestión que impactan en el ámbito, volúmenes o la forma de entrega de los servicios.
- Posibles auditorías de la prestación del servicio realizadas por terceros independientes elegidos por Canal Gestión, con el objeto de garantizar que la prestación del servicio contratado se realiza con todas las garantías de seguridad y confidencialidad exigidas en este Contrato.
- 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 Gestión, S.A.	Centro de Operaciones de Seguridad (SOC) y Oficina Técnica de Seguridad (OTS)	11/2015
Elaborado por:	Documento	Versión
Coordinación de Seguridad Informática.	Pliego de Cláusulas Técnicas Particulares	V0.17
Área de Planificación, Control y Seguridad		

## 7. EJECUCIÓN DE LOS TRABAJOS ASOCIADOS AL SERVICIO.

### 7.1. Plazos de ejecución.

El plazo de ejecución se encuentra recogido 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 Gestión supondrá la exclusión del licitante del presente procedimiento.**

Empresa	Proyecto	Fecha
Canal de Isabel II Gestión, S.A.	Centro de Operaciones de Seguridad (SOC) y Oficina Técnica de Seguridad (OTS)	11/2015
Elaborado por:	Documento	Versión
Coordinación de Seguridad Informática.	Pliego de Cláusulas Técnicas Particulares	V0.17
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. No Aplica.

Empresa	Proyecto	Fecha
Canal de Isabel II Gestión, S.A.	Centro de Operaciones de Seguridad (SOC) y Oficina Técnica de Seguridad (OTS)	11/2015
Elaborado por:	Documento	Versión
Coordinación de Seguridad Informática.	Pliego de Cláusulas Técnicas Particulares	V0.17
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 Gestión. Deberá, por tanto, ser aprobado por Canal Gestión antes del inicio de los trabajos.

El adjudicatario asumirá el sistema de gestión y nomenclatura de la documentación de Canal Gestión 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 Gestión.

A continuación se describen con mayor detalle los aspectos a tener en cuenta en cada una de las fases.

Empresa	Proyecto	Fecha
Canal de Isabel II Gestión, S.A.	Centro de Operaciones de Seguridad (SOC) y Oficina Técnica de Seguridad (OTS)	11/2015
Elaborado por:	Documento	Versión
Coordinación de Seguridad Informática.	Pliego de Cláusulas Técnicas Particulares	V0.17
Área de Planificación, Control y Seguridad		

### 7.3. Fase 1.- Implantación, configuración y puesta en marcha del Servicio de Monitorización de la Seguridad (trabajos enmarcados en el ámbito de la Seguridad Reactiva).

En esta fase, que se extenderá durante el periodo indicado en el en el **Apartado 2 del Anexo I del PCAP**, se realizarán las siguientes tareas con la duración máxima indicada:

- |         |  |
|---------|--|
| Tarea 1 | <p>Instalación de la solución SIEM propuesta y configuración inicial de los componentes.</p> <p>Duración: 20 días laborables.</p>  |
| Tarea 2 | <p>Integración de las fuentes de datos identificadas en el ANEXO 4 - "Tipos de dispositivos y volumen de GB/día en origen" del presente Pliego.</p> <p>Duración: 40 días laborables.</p> |
| Tarea 3 | <p>Activación de los contenidos estándar de la solución SIEM propuesta (reglas de contenidos, alertas e informes).</p> <p>Duración: 5 días laborables.</p>                               |
| Tarea 4 | <p><i>Fine tuning</i> de todos los contenidos estándar (adecuación de reglas, alertas e informes, eliminación de falsos positivos, etc.).</p> <p>Duración: 10 días laborables.</p>       |
| Tarea 5 | <p>Instalación de la solución proactiva para la toma de decisiones.</p> <p>Duración: 5 días laborables.</p>  |
| Tarea 6 | <p>Configuración de la solución proactiva para la toma de decisiones para su correcta integración con la solución SIEM propuesta.</p> <p>Duración: 2 días laborables.</p>                |

Empresa	Proyecto	Fecha
Canal de Isabel II Gestión, S.A.	Centro de Operaciones de Seguridad (SOC) y Oficina Técnica de Seguridad (OTS)	11/2015
Elaborado por:	Documento	Versión
Coordinación de Seguridad Informática.	Pliego de Cláusulas Técnicas Particulares	V0.17
Área de Planificación, Control y Seguridad		

Durante esta fase también se definirán todos los procedimientos de organización y actuación de todos los actores involucrados en la prestación de los servicios de monitorización, del equipo o grupo de primera intervención y de la solución proactiva para la toma de decisiones.

#### **7.4. Fase 2.- Monitorización y Gestión de la Seguridad (trabajos enmarcados en el ámbito de la Seguridad Reactiva).**

Esta fase se iniciará una vez finalice la Fase 1 y tendrá la duración total indicada en el ***Apartado 2 del Anexo I del PCAP.***

Además de las tareas propias derivadas de la monitorización y gestión de la seguridad, durante esta fase se llevarán a cabo también, y conjuntamente con Canal Gestión, las tareas necesarias de creación de modelo de inteligencia basado en casos de uso que será independiente de la tecnología y del operador responsable de aplicarlo, con el objeto de que dicho modelo de inteligencia pueda ser aplicado sobre otras plataformas y operadores que presten y operen un servicio de Monitorización de la Seguridad. Durante la prestación del servicio se generarán un máximo de **dos (2) casos de uso a medida y personalizados al mes**, y con una duración máxima de 10 días laborables para la definición, configuración y puesta en marcha de cada caso de uso.

Se define caso de uso como el conjunto de aquellos contenidos (reglas de correlación y detección, objetos estándar y “*ad hoc*”, filtros, informes estándar y *custom*, alertas, listas, elementos de la base de datos de conocimiento con incidencias y las actuaciones realizadas para su resolución, etc.) que permitan a Canal Gestión obtener una prestación eficiente del servicio a través de información de interés para los requisitos de seguridad del negocio, obtenida a partir de los *logs* procesados por el servicio de Monitorización de la Seguridad.

Durante toda esta fase se documentará con todo detalle cada caso de uso creado así como toda aquella información adicional necesaria, con el objeto de permitir a Canal Gestión la nueva puesta en marcha del servicio de forma efectiva.

Empresa		Proyecto	Fecha
Canal de Isabel II Gestión, S.A.		Centro de Operaciones de Seguridad (SOC) y Oficina Técnica de Seguridad (OTS)	11/2015
Elaborado por:		Documento	Versión
Coordinación de Seguridad Informática.		Pliego de Cláusulas Técnicas Particulares	V0.17
Área de Planificación, Control y Seguridad			

El modelo de inteligencia creado quedará como propiedad intelectual de Canal Gestión.

Los licitantes deberán aportar en el PGGPAT todos los aspectos relativos a la gestión de los trabajos.

La mayoría de las actividades se realizarán en las instalaciones del Adjudicatario, a excepción de aquéllas que requieran interacción con el personal de Canal Gestión o sean acordadas entre las partes.

Los parámetros del ANS revisados y acordados en la primera fase relativos a la monitorización e intervención ante incidentes de seguridad entrarán en funcionamiento, incluido el esquema de penalizaciones, aplicándose al mismo una cuantía del 100%.

La descripción del detalle de los procedimientos de gestión que el licitante aplique para la realización de esta fase se incluirá en el Plan de Comunicación del PGGPAT.

### **7.5. Fase 3.- Asistencia Técnica al Comité Técnico de Seguridad (trabajos enmarcados en los ámbitos de la Seguridad Proactiva y Preventiva).**

Esta fase se iniciará de manera simultánea a la Fase 1 y tendrá la duración indicada en el ***Apartado 2 del Anexo I del PCAP.***

Los licitantes deberán aportar en el PGGPAT todos los aspectos relativos a la gestión de los trabajos.

La mayoría de las actividades se realizarán en las instalaciones del Adjudicatario, a excepción de aquéllas que requieran interacción con el personal de Canal Gestión o sean acordadas entre las partes.

Los parámetros del ANS acordados referentes a estos trabajos entrarán en funcionamiento desde el primer momento, incluido el esquema de penalizaciones, aplicándose al mismo una cuantía del 100%.

Empresa	Proyecto	Fecha
Canal de Isabel II Gestión, S.A.	Centro de Operaciones de Seguridad (SOC) y Oficina Técnica de Seguridad (OTS)	11/2015
Elaborado por:	Documento	Versión
Coordinación de Seguridad Informática.	Pliego de Cláusulas Técnicas Particulares	V0.17
Área de Planificación, Control y Seguridad		

La descripción del detalle de los procedimientos de gestión que el licitante aplique para la realización de esta fase se incluirá en el Plan de Comunicación del PGGPAT.

#### 7.6. Fase 4.- Devolución de los servicios.

Esta fase se deberá realizar cuando se determine la finalización del servicio ya sea por cumplimiento del plazo inicial establecido para el contrato, o por la cancelación del servicio solicitada por Canal Gestión con base en el incumplimiento reiterado del ANS.

Durante esta fase, adicionalmente a la devolución del servicio, la ejecución de los servicios seguirá siendo responsabilidad del Adjudicatario, aplicándose las mismas condiciones que las descritas en la fase de Soporte.

Durante esta fase el Adjudicatario debe comprometer los recursos y ejecutar las actividades necesarias para devolver el servicio a Canal Gestión o a quien éste designe. En concreto, la empresa adjudicataria debe actualizar toda la documentación generada durante la Fase 2 y exportar todos los objetos *“ad hoc”* (casos de uso, reglas asociadas e independientes existentes, *dashboard*, informes, filtros, *custom reports*, base de datos de conocimiento con incidencias y las actuaciones realizadas para su resolución, etc.) creados para la prestación eficiente del servicio contratado y de toda aquella información adicional necesaria para permitir a Canal Gestión la puesta en marcha efectiva del servicio. Una vez finalizado el Contrato, la empresa adjudicataria tiene que garantizar el almacenamiento de los eventos recibidos durante un año más. Durante este periodo no se recibirán nuevos eventos pero sí se garantizará el acceso de Canal de Isabel II Gestión, S.A. al histórico de eventos para actividades en línea con la funcionalidad de gestión de *logs (log management)*, como, por ejemplo: realización de informes, búsquedas, identificación forense, etc.

El Adjudicatario deberá ejecutar el Plan de Devolución del servicio en coordinación con el nuevo Plan de Transición que aporte Canal Gestión.

Empresa	Proyecto	Fecha
Canal de Isabel II Gestión, S.A.	Centro de Operaciones de Seguridad (SOC) y Oficina Técnica de Seguridad (OTS)	11/2015
Elaborado por:	Documento	Versión
Coordinación de Seguridad Informática.	Pliego de Cláusulas Técnicas Particulares	V0.17
Área de Planificación, Control y Seguridad		

El Plan de Devolución debe ser gestionado a lo largo del proyecto por el Adjudicatario, por lo que en los procesos de gestión de cambios que se implanten, deberán controlar que los cambios que afectan a este Plan son actualizados en el mismo. El Plan de Devolución, deberá incluir el conjunto de actividades necesarias para la correcta devolución del Servicio por parte del Adjudicatario, cuando se produzca la terminación de la relación contractual. Por lo tanto, se deberán incluir en los diferentes planes del PGGPAT todos los aspectos relativos a esta fase:

- Aspectos generales del Plan.
- Planificación detallada, con detalle de los hitos, el calendario de ejecución, responsables, interdependencias.
- Recursos, roles y responsabilidades de Canal Gestión y del Adjudicatario durante la ejecución del Plan.
- Descripción de cómo se hará la transferencia del servicio, incluyendo la transferencia de conocimiento.
- Análisis de Riesgos de la Transferencia de los Servicios.

El Adjudicatario debe comprometerse a ejecutar el Plan de Devolución, si así se le solicita por Canal Gestión, y a **disponer de recursos con conocimiento del entorno particular de Canal Gestión durante tres (3) meses tras la devolución del Servicio.**



Empresa	Proyecto	Fecha
Canal de Isabel II Gestión, S.A.	Centro de Operaciones de Seguridad (SOC) y Oficina Técnica de Seguridad (OTS)	11/2015
Elaborado por:	Documento	Versión
Coordinación de Seguridad Informática.	Pliego de Cláusulas Técnicas Particulares	V0.17
Área de Planificación, Control y Seguridad		

## 7.7. 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 Gestión 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 tendrá en cuenta la adecuación al marco de trabajo de mejores prácticas reflejado en la norma ISO/IEC 27005:2011: "Guía para la gestión del riesgo de la seguridad de la información" y, complementando a todo lo anterior, 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 vigente y aplicable al ámbito de la presente contratación.

Empresa	Proyecto	Fecha
Canal de Isabel II Gestión, S.A.	Centro de Operaciones de Seguridad (SOC) y Oficina Técnica de Seguridad (OTS)	11/2015
Elaborado por:	Documento	Versión
Coordinación de Seguridad Informática.	Pliego de Cláusulas Técnicas Particulares	V0.17
Área de Planificación, Control y Seguridad		

## 7.8. Metodologías para 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 para su posterior uso durante toda la ejecución del servicio).

## 7.9. 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 y toda otra normativa existente y aplicable en materia de seguridad de la información en el ámbito de políticas y gestión de la seguridad de la información que complemente a las normas expuestas anteriormente, como pueden ser COBIT 5 e ITIL v3.

Empresa	Proyecto	Fecha
Canal de Isabel II Gestión, S.A.	Centro de Operaciones de Seguridad (SOC) y Oficina Técnica de Seguridad (OTS)	11/2015
Elaborado por:	Documento	Versión
Coordinación de Seguridad Informática.	Pliego de Cláusulas Técnicas Particulares	V0.17
Área de Planificación, Control y Seguridad		

## 7.10. 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 Gestión del equipo de proyecto, el adjudicatario presentará a Canal Gestión los certificados técnicos y laborales requeridos en el Apartado 5 del ANEXO I del PCAP.

Empresa	Proyecto	Fecha
Canal de Isabel II Gestión, S.A.	Centro de Operaciones de Seguridad (SOC) y Oficina Técnica de Seguridad (OTS)	11/2015
Elaborado por:	Documento	Versión
Coordinación de Seguridad Informática.	Pliego de Cláusulas Técnicas Particulares	V0.17
Área de Planificación, Control y Seguridad		

Canal Gestión 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 de Canal Gestión. 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 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 Gestión 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 Gestión, S.A.	Centro de Operaciones de Seguridad (SOC) y Oficina Técnica de Seguridad (OTS)	11/2015
Elaborado por:	Documento	Versión
Coordinación de Seguridad Informática.	Pliego de Cláusulas Técnicas Particulares	V0.17
Área de Planificación, Control y Seguridad		

## 7.11. Organización, Seguimiento y Control de los trabajos asociados al servicio.

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.

### 7.11.1. Ámbitos de Seguridad Proactiva y Seguridad Preventiva.

En los alcances identificados dentro de los ámbitos de Seguridad Proactiva y Seguridad Preventiva, para cada uno de los trabajos y/o asistencias que Canal Gestión demande o solicite al adjudicatario, éste 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 Gestión en un plazo igual o inferior al determinado en el ANS desde que le sea requerido formalmente.
2. Entregará a Canal Gestión 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 Gestión.
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 Gestión.

Empresa	Proyecto	Fecha
Canal de Isabel II Gestión, S.A.	Centro de Operaciones de Seguridad (SOC) y Oficina Técnica de Seguridad (OTS)	11/2015
Elaborado por:	Documento	Versión
Coordinación de Seguridad Informática.	Pliego de Cláusulas Técnicas Particulares	V0.17
Área de Planificación, Control y Seguridad		

### Fase de Elaboración de la Propuesta de Ejecución Valorada<sup>1</sup> (PEV)

1. Basado en el documento de requisitos, el adjudicatario deberá realizar un estudio de las tareas a realizar y una planificación de los recursos y del esfuerzo necesarios para la realización de los trabajos.
2. El adjudicatario generará una planificación del proyecto detallando el alcance, las tareas y la planificación de las mismas, los recursos y los entregables, y valorará económicamente el importe de los trabajos a realizar según la planificación realizada y de acuerdo a los recursos necesarios, incluyendo los trabajos realizados en la fase previa de Análisis de Requisitos.
3. El adjudicatario deberá realizar la entrega de la Propuesta de Ejecución en un plazo igual o inferior al determinado en el ANS desde que Canal Gestión finalice el análisis de requisitos, es decir, desde la aceptación por parte de Canal Gestión del documento de requisitos.
4. Si la propuesta presentada por el adjudicatario no satisface las necesidades de Canal Gestión, el trabajo o asistencia en cuestión quedará cancelado. No obstante, el adjudicatario, a petición de Canal Gestión, podrá presentar nuevas propuestas ajustándose a los requisitos fijados por Canal Gestión. La valoración económica contenida en esta propuesta de ejecución tendrá un carácter cerrado, y por tanto si hubiera retrasos en la ejecución de los trabajos, la propuesta no se verá modificada. La única forma de modificar la propuesta es a través de la correspondiente gestión de cambio aceptada por Canal Gestión. Si por las diferentes circunstancias descritas hasta el momento el proyecto no fuera a ser finalmente realizado por el adjudicatario el proyecto se considerará cerrado a todos los efectos incluidos los relacionados con el cálculo del cumplimiento del ANS.
5. En caso de ser rechazada definitivamente la propuesta de ejecución valorada, los trabajos realizados por el adjudicatario para la elaboración de la propuesta de ejecución no serán facturables.

<sup>1</sup> Se utiliza el concepto "propuesta de ejecución valorada" en lugar de "oferta" para distinguirlo de la "oferta" de servicios para optar a la adjudicación del contrato.

Empresa	Proyecto	Fecha
Canal de Isabel II Gestión, S.A.	Centro de Operaciones de Seguridad (SOC) y Oficina Técnica de Seguridad (OTS)	11/2015
Elaborado por:	Documento	Versión
Coordinación de Seguridad Informática.	Pliego de Cláusulas Técnicas Particulares	V0.17
Área de Planificación, Control y Seguridad		

### Fase de Realización de los Trabajos

Para aquellas propuestas de ejecución valoradas que Canal Gestión apruebe:

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 Gestión, salvo que Canal Gestión 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 Gestión del Plan de Gestión del Proyecto. En ambos casos, Canal Gestión 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.
2. Si, debido a la envergadura o criticidad de los trabajos o asistencias, Canal Gestión 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 Gestión 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 Gestión. 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.

Empresa	Proyecto	Fecha
Canal de Isabel II Gestión, S.A.	Centro de Operaciones de Seguridad (SOC) y Oficina Técnica de Seguridad (OTS)	11/2015
Elaborado por:	Documento	Versión
Coordinación de Seguridad Informática.	Pliego de Cláusulas Técnicas Particulares	V0.17
Área de Planificación, Control y Seguridad		

- (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 Gestión, 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 Gestión 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 Gestión, 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 Gestión 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 Gestión. En caso de no ser aprobados por Canal Gestión, debido a errores o falta de adecuación a los requisitos, Canal Gestión 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 Gestión de los resultados previstos del proyecto, dichos resultados no cumplen con los requisitos y el alcance previsto, Canal Gestión quedará liberado del compromiso de pago de dicho proyecto.
  5. El adjudicatario realizará las labores de cierre del proyecto y análisis de lecciones aprendidas.



Empresa	Proyecto	Fecha
Canal de Isabel II Gestión, S.A.	Centro de Operaciones de Seguridad (SOC) y Oficina Técnica de Seguridad (OTS)	11/2015
Elaborado por:	Documento	Versión
Coordinación de Seguridad Informática.	Pliego de Cláusulas Técnicas Particulares	V0.17
Área de Planificación, Control y Seguridad		

### 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 de Canal Gestión.

### 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 Gestión.

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 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 Gestión, 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 Gestión, S.A.	Centro de Operaciones de Seguridad (SOC) y Oficina Técnica de Seguridad (OTS)	11/2015
Elaborado por:	Documento	Versión
Coordinación de Seguridad Informática.	Pliego de Cláusulas Técnicas Particulares	V0.17
Área de Planificación, Control y Seguridad		

### 7.11.2. **Ámbito de Seguridad Reactiva.**

Para los alcances identificados dentro del ámbito de Seguridad Reactiva y la puesta en marcha del servicio contratado, el licitador deberá incluir en su oferta todas las tareas necesarias para poder ofrecer dicho servicio con total garantía. Al menos, deberá reflejar y describir con detalle las siguientes tareas:

1. Despliegue de las comunicaciones (ver "Condiciones de Acceso a la Red Corporativa de Datos de Canal Gestión" en el ANEXO 5 del presente Pliego), teniendo en cuenta los Requisitos de Seguridad recogidos en el ANEXO 6 del presente Pliego.
2. Proceso detallado de integración de los dispositivos contemplados con la solución SIEM ofrecida, especificando fases e hitos.
3. Gestión de alertas e incidentes.
4. Definición de procedimientos.

Se deberá detallar en la oferta la planificación y tiempos asociados a la puesta en marcha, dando prioridad al Punto 1 "Despliegue de las comunicaciones".

El horario de prestación del servicio en este ámbito será de 24 x 7. Los festivos nacionales, fines de semana y nocturnos (19:00 a 8:00 horas), se considerarán como horario 24 x 7. No obstante, una vez puesto en marcha el servicio, y conociendo con mayor detalles las características del servicio, se podrá considerar categorizar en un nivel más alto algún servicio en concreto para poder ajustar los compromisos de ANS a los requerimientos de Canal Gestión.

Empresa	Proyecto	Fecha
Canal de Isabel II Gestión, S.A.	Centro de Operaciones de Seguridad (SOC) y Oficina Técnica de Seguridad (OTS)	11/2015
Elaborado por:	Documento	Versión
Coordinación de Seguridad Informática.	Pliego de Cláusulas Técnicas Particulares	V0.17
Área de Planificación, Control y Seguridad		

Para la atención a este servicio, el adjudicatario deberá contar, al menos, con los siguientes roles para poder interactuar con Canal Gestión:

➤ **Service Desk 24x7.**

Punto único de contacto para la gestión de incidencias, peticiones y solicitudes.

➤ **Equipo o Grupo de Primera Intervención (GIR) disponible bajo solicitud.**

Las funciones a realizar por este rol serán las de identificación y valoración de los incidentes que, desde Canal Gestión se considere que requieran de su actuación, así como la emisión documentada de propuestas de solución (si existe) y/o las medidas de control o controles detectivos, correctivos, preventivos y/o compensatorios que se identifiquen como necesarios.

➤ **Gestor del Servicio.**

Las funciones a realizar serán:

- Seguimiento y supervisión del servicio.
- Presentación de informes, entregables acordados y resultados.

Esta figura podrá desplazarse a las oficinas de Canal Gestión cuando sea requerido. Además si las circunstancias lo requirieran, existirá la posibilidad de que Canal Gestión pueda comunicarse directamente con el equipo de soporte especializado según el procedimiento definido conjuntamente por el adjudicatario y Canal Gestión.

Empresa	Proyecto	Fecha
Canal de Isabel II Gestión, S.A.	Centro de Operaciones de Seguridad (SOC) y Oficina Técnica de Seguridad (OTS)	11/2015
Elaborado por:	Documento	Versión
Coordinación de Seguridad Informática.	Pliego de Cláusulas Técnicas Particulares	V0.17
Área de Planificación, Control y Seguridad		

## 7.12. 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 Gestión 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 Gestión, 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 Gestión, S.A.	Centro de Operaciones de Seguridad (SOC) y Oficina Técnica de Seguridad (OTS)	11/2015
Elaborado por:	Documento	Versión
Coordinación de Seguridad Informática.	Pliego de Cláusulas Técnicas Particulares	V0.17
Área de Planificación, Control y Seguridad		

### 7.13. 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 las dependencias de Canal Gestión.

En el caso que los trabajos se realicen en las instalaciones del adjudicatario, los costes derivados de las posibles conexiones necesarias con Canal Gestión 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 Gestión.

El licitador deberá tener su SOC y todas las oficinas que destinen a la prestación de los servicios objeto de este contrato ubicados a una distancia de las Oficinas Centrales de Canal Gestión tal que permita garantizar:

- El desplazamiento de los técnicos del Equipo o Grupo de Primera Intervención (GIR) en caso de incidentes de seguridad en un tiempo no superior a 3 horas, para dar cumplimiento al ANS mínimo en la gestión de incidencias asociadas a la actividad de Servicio de Respuesta ante Incidentes recogido en el ANEXO 3 de este Pliego.
- El cumplimiento del ANEXO 5 de este Pliego.

Empresa	Proyecto	Fecha
Canal de Isabel II Gestión, S.A.	Centro de Operaciones de Seguridad (SOC) y Oficina Técnica de Seguridad (OTS)	11/2015
Elaborado por:	Documento	Versión
Coordinación de Seguridad Informática.	Pliego de Cláusulas Técnicas Particulares	V0.17
Área de Planificación, Control y Seguridad		

Para la gestión del proyecto el adjudicatario utilizará la herramienta Clarity PPM implantada en Canal Gestión.

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 Gestión, así como adaptarse a los cambios futuros que Canal Gestión 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 Gestión.

Empresa	Proyecto	Fecha
Canal de Isabel II Gestión, S.A.	Centro de Operaciones de Seguridad (SOC) y Oficina Técnica de Seguridad (OTS)	11/2015
Elaborado por:	Documento	Versión
Coordinación de Seguridad Informática.	Pliego de Cláusulas Técnicas Particulares	V0.17
Área de Planificación, Control y Seguridad		

## 8. CONDICIONES DE ACEPTACIÓN, GARANTÍA Y MANTENIMIENTO.

El adjudicatario comunicará por escrito a Canal Gestión 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 Gestión 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 Gestión realice modificaciones por su cuenta, incluyendo implantaciones de nuevas funcionalidades.

Empresa	Proyecto	Fecha
Canal de Isabel II Gestión, S.A.	Centro de Operaciones de Seguridad (SOC) y Oficina Técnica de Seguridad (OTS)	11/2015
Elaborado por:	Documento	Versión
Coordinación de Seguridad Informática.	Pliego de Cláusulas Técnicas Particulares	V0.17
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. **No se valorarán las ofertas que no se ajusten a la estructura indicada.**

La estructura de la oferta se encuentra detalla en el **Apartado 6 del ANEXO I del PCAP.**



Empresa

Canal de Isabel II Gestión, S.A.

Proyecto

Centro de Operaciones de Seguridad (SOC) y  
Oficina Técnica de Seguridad (OTS)

Fecha

11/2015

Elaborado por:

Documento

Versión

Coordinación  
Informática.

de

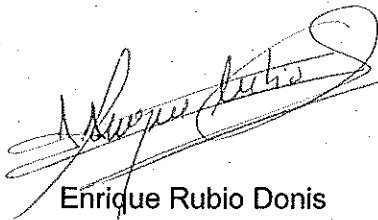
Seguridad

Pliego de Cláusulas Técnicas Particulares

V0.17

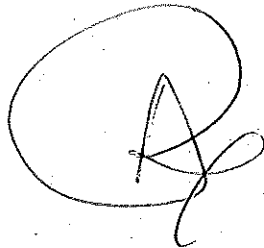
Área de Planificación, Control y  
Seguridad

Noviembre de 2015



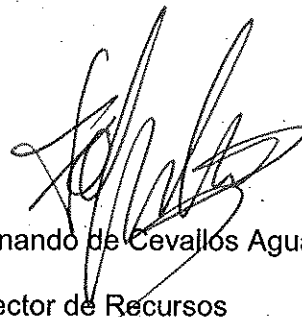
Enrique Rubio Donis

Fdo. Jefe de Área de Planificación, Control y Seguridad



Ángel Rodríguez García

Subdirector de Sistemas Informáticos



Fernando de Cevallos Aguarón

Director de Recursos

Empresa Proyecto Fecha  
Canal de Isabel II Gestión, S.A. Centro de Operaciones de Seguridad (SOC) y 11/2015  
Oficina Técnica de Seguridad (OTS)

Elaborado por: Documento Versión  
Coordinación de Seguridad Pliego de Cláusulas Técnicas Particulares V0.17  
Informática.

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 T.I.

Empresa	Categoría	F-alta	F-baja	Meses	Actividad Informática

Formación Académica.

Título Académico	Centro	Años	F-expedición

Formación en Tecnologías de la Información y/o Consultoría.

Curso	Impartido por	Horas	Fecha inicio

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

Certificaciones exigidas

Módulo/Tecnología	Fecha de Certificación	Nivel de Certificación

Empresa	Proyecto	Fecha
Canal de Isabel II Gestión, S.A.	Centro de Operaciones de Seguridad (SOC) y Oficina Técnica de Seguridad (OTS)	11/2015
Elaborado por:	Documento	Versión
Coordinación de Seguridad Informática.	Pliego de Cláusulas Técnicas Particulares	V0.17
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 Gestión, S.A.	Centro de Operaciones de Seguridad (SOC) y Oficina Técnica de Seguridad (OTS)	11/2015
Elaborado por:	Documento	Versión
Coordinación de Seguridad Informática.	Pliego de Cláusulas Técnicas Particulares	V0.17
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?

En caso de contestar "Sí" en la columna "¿Certificado de buena ejecución?", se deberá proporcionar copia de éste para su verificación por parte de Canal Gestión.

Empresa	Proyecto	Fecha
Canal de Isabel II Gestión, S.A.	Centro de Operaciones de Seguridad (SOC) y Oficina Técnica de Seguridad (OTS)	11/2015
Elaborado por	Documento	Versión
Coordinación de Seguridad Informática	Pliego de Prescripciones Técnicas Particulares	V0.17
Área de Planificación, Control y Seguridad		

## ANEXO 3. TABLAS DE ACUERDO DE NIVEL DE SERVICIO (ANS).

### Calidad del Servicio

Código	Parámetro	Descripción	Cálculo	KPI	Peso	Vc	Va	Vi
CLS01	Calidad y eficacia de la planificación de las Propuestas de Ejecución Valorada (PEV) realizadas por el adjudicatario	Entrega de los resultados de los trabajos conformes a los requerimientos aprobados, en un plazo inferior o igual al incluido en la PEV correspondiente. Se considerará entregado cuando Canal Gestión apruebe la entrega en cantidad y calidad. El tiempo de aprobación de Canal Gestión 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	Índice de desviación total (o índice de Programación Ganada IPG). Se calculará a la finalización y cierre de los trabajos tomando como referencia la fecha de entrega de los resultados sobre la fecha prevista:  IPG = días hábiles totales previstos de los trabajos finalizados en el periodo de medición / días hábiles totales reales de los trabajos finalizados en el periodo de medición	S	14	0,9	0,8	0,7

Empresa

Canal de Isabel II Gestión, S.A.  
Elaborado por

Proyecto

Centro de Operaciones de Seguridad (SOC) y Oficina Técnica de Seguridad (OTS)  
Documento

Fecha

11/2015

Versión

V0.17

Coordinación de Seguridad Informática  
Área de Planificación, Control y Seguridad

Pliego de Prescripciones Técnicas Particulares

<b>CLS02</b>	Calidad y completitud de los análisis previos de la necesidad	Este parámetro mide la calidad y completitud de los documentos de requisitos. Una <b>merma significativa</b> en estos aspectos provocará la devolución por parte de Canal Gestión del documento al adjudicatario para su revisión y reformulación.	Documentos devueltos por Canal Gestión 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.	S	9	0/0%	1/10%	2/20%
<b>CLS03</b>	Calidad y completitud de las Propuestas de Ejecución Valorada (PEV)	Este parámetro mide la calidad y completitud de las Propuestas de Ejecución Valorada (PEV). Una <b>merma significativa</b> en estos aspectos provocará la devolución por parte de Canal Gestión del documento al adjudicatario para su revisión y reformulación.	Propuestas devueltas por Canal Gestión en su primera entrega del conjunto 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.	S	6	0/0%	1/10%	2/20%
<b>CLS04</b>	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 <b>merma significativa</b> en estos aspectos provocará la devolución por parte de Canal Gestión del documento al adjudicatario para su revisión y reformulación.	PGP devueltos por Canal Gestión 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.	S	9	0/0%	1/10%	2/20%

Empresa

Proyecto

Fecha

Canal de Isabel II Gestión, S.A.

Centro de Operaciones de Seguridad (SOC) y Oficina Técnica de Seguridad (OTS)

11/2015

Elaborado por

Documento

Versión

Coordinación de Seguridad Informática

Pliego de Prescripciones Técnicas Particulares

V0.17

Área de Planificación, Control y Seguridad

<b>CLS05</b>	Calidad y completitud de los diseños técnicos/funcionales	Este parámetro mide la calidad y completitud de los diseños técnicos/funcionales. Una <b>merma significativa</b> en estos aspectos provocará la devolución por parte de Canal Gestión del documento al adjudicatario para su revisión y reformulación.	Diseños devueltos por Canal Gestión 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.	<b>9</b>	<b>0/0%</b>	<b>1/10%</b>	<b>2/20%</b>
<b>CLS06</b>	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 Gestión.	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).	<b>6</b>	<b>0%</b>	<b>10%</b>	<b>20%</b>
<b>CLS07</b>	Eficacia en la realización de las Propuestas de Ejecución Valoradas (PEV)	Este parámetro mide la desviación, respecto del plazo máximo, en la realización de las Propuestas de Ejecución Valoradas (PEV) descritas la Fase de Elaboración de la Propuesta de Ejecución Valorada. Dicho plazo máximo se establece en siete (7) días hábiles desde la aprobación del documento de requerimientos correspondiente.	Porcentaje de desviación total. Porcentaje de días hábiles totales de retraso del conjunto de los documentos correspondientes a los trabajos cerrados en el periodo de medición del parámetro, sobre el total de días hábiles previstos (Número trabajos *7).	<b>5</b>	<b>0%</b>	<b>10%</b>	<b>20%</b>

Empresa

Canal de Isabel II Gestión, S.A.

Elaborado por

Coordinación de Seguridad Informática

Área de Planificación, Control y Seguridad

Proyecto

Centro de Operaciones de Seguridad (SOC) y Oficina Técnica de Seguridad (OTS)

Documento

Pliego de Prescripciones Técnicas Particulares

Fecha

11/2015

Versión

V0.17

<b>CLS08</b>	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 período de medición del parámetro, sobre el total de días hábiles previstos (Número PGP *15).	S	5	0%	10%	20%
<b>CLS09</b>	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 período de medición del parámetro, sobre el total de días hábiles previstos (Número trabajos *5).	S	6	0%	10%	20%



Empresa	Proyecto	Fecha
Canal de Isabel II Gestión, S.A.	Centro de Operaciones de Seguridad (SOC) y Oficina Técnica de Seguridad (OTS)	11/2015
Elaborado por	Documento	Versión
Coordinación de Seguridad Informática	Pliego de Prescripciones Técnicas Particulares	V0.17
Área de Planificación, Control y Seguridad		

Código	Parámetro	Descripción	Cálculo	Peso	KPI	Vc	Va	Vi
CLS10	Eficacia en los tiempos de identificación y propuesta de solución (si existe) de incidencias y solicitudes asociadas al desarrollo de la actividad asociada al Servicio S3.1 - Monitorización de la Seguridad y Gestión de Eventos (Servicio S3.- Seguridad Reactiva).	Información facilitada según la tipología identificada para la identificación y propuesta de solución (si existe) de incidencias y solicitudes críticas, altas, medias y bajas	Total de horas de retraso en la identificación y propuesta de solución (si existe) de incidencias y solicitudes respecto a los plazos indicados en la tabla de nivel de acuerdo de servicio mínimo en la gestión de incidencias y solicitudes asociadas al Servicio S3.1 - Monitorización de la Seguridad y Gestión de Eventos (Servicio S3.- Seguridad Reactiva).	6	S	0	2	3
				6	S	0	3	4
				4	S	0	4	5
				3	S	0	6	7
				6	S	0	2	3
				5	S	0	3	4
				4	S	0	4	5
				3	S	0	6	7

<b>Empresa</b>	<b>Proyecto</b>	<b>Fecha</b>
Canal de Isabel II Gestión, S.A.	Centro de Operaciones de Seguridad (SOC) y Oficina Técnica de Seguridad (OTS)	11/2015
Elaborado por	Documento	Versión
Coordinación de Seguridad Informática	Pliego de Prescripciones Técnicas Particulares	V0.17
Área de Planificación, Control y Seguridad		

Código	Parámetro	Descripción	Cálculo	Peso	KPI	Vc	Va	Vi
CLS11	Eficacia en los tiempos de respuesta del grupo de intervención rápida en la actividad contemplada como S.3.2 - Servicio de Respuesta ante Incidentes (Servicio S3.- Seguridad Reactiva).	Información facilitada según la tipología identificada para la identificación de incidencias críticas, altas, medias y bajas, y propuesta de solución (si existe).	Total de horas de retraso, incluyendo desplazamiento a las oficinas de Canal Gestión si fuera necesario, en la identificación de incidencias y propuesta de solución (si existe) respecto a los plazos indicados en la tabla de nivel de acuerdo de servicio mínimo en la gestión de incidencias asociadas a la actividad del Servicio de Respuesta ante Incidentes.	6	s	0	1	2
				6	s	0	2	3
				4	s	0	3	4
				3	s	0	6	7

Empresa

Proyecto

Fecha

Canal de Isabel II Gestión, S.A.

Centro de Operaciones de Seguridad (SOC) y Oficina Técnica de Seguridad (OTS)

11/2015

Elaborado por

Documento

Versión

Coordinación de Seguridad Informática

Pliego de Prescripciones Técnicas Particulares

V0.17

Área de Planificación, Control y Seguridad

Código	Parámetro	Descripción	Cálculo	Peso	KPI	Vc	Va	Vi
CLS12	Eficacia en los plazos de ejecución de las tareas identificadas en la Fase 1 de implantación, configuración y puesta en servicio de la solución SIEM propuesta y de la solución proactiva para la toma de decisiones, asociada a la actividad contemplada de Monitorización de la Seguridad y Gestión de Eventos (Servicio S3.- Seguridad Reactiva).	Información facilitada según las tareas identificadas y su duración establecida.	Total de días de retraso en la realización de las tareas identificadas en la Fase 1 de implantación, configuración y puesta en servicio de la solución SIEM propuesta y de la solución proactiva para la toma de decisiones, respecto a los plazos indicados en la tabla de nivel de acuerdo de servicio en la realización de las tareas identificadas en dicha Fase 1.	8	S	0	1	2
				9	S	0	1	2
				8	S	0	1	2
				9	S	0	1	2
				8	S	0	1	2
				9	S	0	1	2

**Empresa**

Canal de Isabel II Gestión, S.A.  
Elaborado por

**Proyecto**

Centro de Operaciones de Seguridad (SOC) y Oficina Técnica de Seguridad (OTS)  
Documento

**Fecha**

11/2015

**Versión**

V0.17

**Coordinación de Seguridad Informática**

Área de Planificación, Control y Seguridad

**Pliego de Prescripciones Técnicas Particulares**

Código	Parámetro	Descripción	Cálculo	Peso	KPI	Vc	Va	Vi
CLS13	Eficacia en los plazos de ejecución de las tareas identificadas en la Fase 2 del Servicio S3.1 - Monitorización de la Seguridad y Gestión de Eventos (Servicio S3.- Seguridad Reactiva).	Información facilitada según las tareas identificadas y su duración establecida.	Total de días de retraso en la realización de la tarea identificada en la Fase 2 del Servicio S3.1 - Monitorización de la Seguridad y Gestión de Eventos (Servicio S3.- Seguridad Reactiva), respecto a los plazos indicados en la tabla de nivel de acuerdo de servicio en la realización de las tareas identificadas en dicha Fase 2.	10	s	0	1	2

Empresa

Canal de Isabel II Gestión, S.A.

Elaborado por

Coordinación de Seguridad Informática

Área de Planificación, Control y Seguridad

Proyecto

Centro de Operaciones de Seguridad (SOC) y Oficina Técnica de Seguridad (OTS)

Documento

Pliego de Prescripciones Técnicas Particulares

Fecha

11/2015

Versión

V0.17

## Gestión ANS

Código	Parámetro	Descripción	Cálculo	Peso	KPI	Vc	Va	Vi
ANS01	Modo de prestación del servicio	El servicio de SOC se prestará en modo 24x7	Días de no prestación del servicio. Se considerará que un día no se ha prestado servicio si el servicio no ha estado disponible durante 5 horas o más.	7,00	s	0	1	2
ANS02	Disponibilidad del servicio	El servicio de SOC tendrá una disponibilidad media del 99%	Informes corporativos de la disponibilidad del servicio de SOC (como evidencia de garantía de continuidad del Servicio de SOC) donde se recoja que la disponibilidad del mismo supera el 99%	8,00	s	0	-1%	-2%
ANS03	Fiabilidad de la información	Fiabilidad de la información facilitada	Errores detectados en los informes de ANS periódicos, para el período medido	5,64	s	0	1	2
ANS04	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	2,66	s	0	2	4

Empresa	Proyecto	Fecha
Canal de Isabel II Gestión, S.A.	Centro de Operaciones de Seguridad (SOC) y Oficina Técnica de Seguridad (OTS)	11/2015
Elaborado por	Documento	Versión
Coordinación de Seguridad Informática	Pleigo de Prescripciones Técnicas Particulares	V0.17
Área de Planificación, Control y Seguridad		

## TABLA DE ACUERDO DE NIVEL DE SERVICIO (ANS) EN LA EJECUCIÓN DE LAS TAREAS IDENTIFICADAS EN LA FASE DE IMPLANTACIÓN, CONFIGURACIÓN Y PUESTA EN SERVICIO DE LA SOLUCIÓN SIEM PROPUESTA Y DE LA SOLUCIÓN PROACTIVA PARA LA TOMA DE DECISIONES.

Tareas	Plazo máximo (en días laborables)
Tarea 1: Instalación de la solución SIEM propuesta y configuración inicial de los componentes.	20 días
Tarea 2: Integración de las fuentes de datos identificadas en el ANEXO 4 - "Tipos de dispositivos y volumen de GB/día en origen"	40 días
Tarea 3: Activación de los contenidos estándar de la solución SIEM propuesta (reglas de contenidos, alertas e informes).	5 días
Tarea 4: <i>Fine tuning</i> de todos los contenidos estándar.	10 días
Tarea 5: Instalación de la solución proactiva para la toma de decisiones.	5 días
Tarea 6: Configuración de la solución proactiva para la toma de decisiones para su correcta integración con la solución SIEM propuesta.	2 días

Empresa

Canal de Isabel II Gestión, S.A.

Elaborado por

Coordinación de Seguridad Informática

Área de Planificación, Control y Seguridad

Proyecto

Centro de Operaciones de Seguridad (SOC) y Oficina Técnica de Seguridad (OTS)

Documento

Pliego de Prescripciones Técnicas Particulares

Fecha

11/2015

Versión

V0.17

## TABLA DE ACUERDO DE NIVEL DE SERVICIO (ANS) MÍNIMO EN LA GESTIÓN DE INCIDENCIAS Y SOLICITUDES ASOCIADAS A LA ACTIVIDAD DE MONITORIZACIÓN DE LA SEGURIDAD.

Tipo de Evento	Tiempo de Identificación y propuesta de resolución (si existe)	Horario de Soporte
Incidencia Crítica	2 horas	24x7
Incidencia Alta	4 horas	24x7
Incidencia Media	10 horas	10x5
Incidencia Baja	20 horas	10x5
Solicitud Crítica	3 horas	24x7
Solicitud Alta	4 horas	24x7
Solicitud Media	10 horas	10x5
Solicitud Baja	20 horas	10x5

Empresa	Proyecto	Fecha
Canal de Isabel II Gestión, S.A.	Centro de Operaciones de Seguridad (SOC) y Oficina Técnica de Seguridad (OTS)	11/2015
Elaborado por	Documento	Versión
Coordinación de Seguridad Informática	Pliego de Prescripciones Técnicas Particulares	V0.17
Área de Planificación, Control y Seguridad		

## TABLA DE ACUERDO DE NIVEL DE SERVICIO (ANS) EN LA EJECUCIÓN DE LAS TAREAS IDENTIFICADAS EN LA FASE DE MONITORIZACIÓN Y GESTIÓN DE LA SEGURIDAD.

Tareas	Plazo máximo (en días laborables)
Configuración y puesta en marcha de cada caso de uso a medida y personalizado (máximo, 2 al mes, durante toda la prestación del servicio).	10 días



Empresa	Proyecto	Fecha
Canal de Isabel II Gestión, S.A.	Centro de Operaciones de Seguridad (SOC) y Oficina Técnica de Seguridad (OTS)	11/2015
Elaborado por	Documento	Versión
Coordinación de Seguridad Informática	Pliego de Prescripciones Técnicas Particulares	V0.17
Área de Planificación, Control y Seguridad		

## TABLA DE ACUERDO DE NIVEL DE SERVICIO (ANS) MÍNIMO EN LA GESTIÓN DE INCIDENCIAS ASOCIADAS A LA ACTIVIDAD DE SERVICIO DE RESPUESTA ANTE INCIDENTES.

Tipo de Evento	Tiempo de respuesta, incluyendo desplazamiento	Horario de Soporte
Incidencia Crítica	2,5 horas	24x7
Incidencia Alta	3,5 horas	24x7
Incidencia Media	5 horas	10x5
Incidencia Baja	15 horas	10x5

**Empresa**

Canal de Isabel II Gestión, S.A.

**Elaborado por**

Coordinación de Seguridad Informática

Área de Planificación, Control y Seguridad

**Proyecto**

Centro de Operaciones de Seguridad (SOC) y Oficina Técnica de Seguridad (OTS)

**Documento**

Pliego de Prescripciones Técnicas Particulares

**Fecha**

11/2015

**Versión**

V0.17

## Gestión del Servicio

Código	Parámetro	Descripción	Cálculo	Peso	KPI	Vc	Va	Vi	Código
GSE01	Solvencia del Equipo	Este parámetro mide la solvencia del equipo para la prestación del servicio contratado, a través del número de personas como personal propio del adjudicatario y dedicadas a la prestación de su Servicio de SOC con capacidades técnicas demostrables.	Al menos, 10 personas dedicadas a la prestación del Servicio de SOC y certificadas oficialmente en soluciones SIEM que aparezcan como Leaders en el último cuadrante Gartner publicado.	10	S	0	3	4	>4
GSE02	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	9,37	s	1	2	3	>3
GSE03	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 desde la fecha de la baja de la persona para realizar la sustitución.	Número total de semanas de retraso en el conjunto de las sustituciones realizadas en el período de medición	15	s	0	1	2	>2
GSE04	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	s	1	2	3	>3

(1)

Canal Gestión 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 Gestión, S.A.	Centro de Operaciones de Seguridad (SOC) y Oficina Técnica de Seguridad (OTS)	11/2015
Elaborado por:	Documento	Versión
Coordinación de Seguridad Informática.	Pliego de Prescripciones Técnicas Particulares	V0.17
Área de Planificación, Control y Seguridad		

## ANEXO 4. TIPOS DE DISPOSITIVOS Y VOLUMEN DE GB/DÍA EN ORIGEN.

Esta información tiene **carácter confidencial**, para obtenerla deberán solicitarla formalmente al Área de Planificación, Control y Seguridad de Canal de Isabel II Gestión, S.A. mediante el envío de un correo electrónico a la dirección: [proteccion.informatica@canalgestion.es](mailto:proteccion.informatica@canalgestion.es) de conformidad con lo establecido en el apartado 10.14 "Información y aclaraciones" del Anexo I del Pliego de Cláusulas Administrativas Particulares.

Empresa	Proyecto	Fecha
Canal de Isabel II Gestión, S.A.	Centro de Operaciones de Seguridad (SOC) y Oficina Técnica de Seguridad (OTS)	11/2015
Elaborado por:	Documento	Versión
Coordinación de Seguridad Informática.	Pliego de Prescripciones Técnicas Particulares	V0.17
Área de Planificación, Control y Seguridad		

## **ANEXO 5. CONDICIONES DE ACCESO A LA RED CORPORATIVA DE DATOS DE CANAL GESTIÓN.**

El adjudicatario queda obligado a realizar una conexión privada a la Red Corporativa de Datos (en adelante, RCD) de Canal Gestión 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 comunicación, que se responsabilice, en el ámbito de la prestación de los servicios asociados al contrato, de la configuración y mantenimiento de la parte de la infraestructura de comunicaciones entre el adjudicatario y Canal Gestión que sea responsabilidad del adjudicatario, al objeto de garantizar el cumplimiento de este Anexo 5.

Dicha conexión se realizará bajo los siguientes condicionantes obligatorios:

### **1. Conexión única del operador de comunicaciones con la RCD de Canal Gestión.**

El operador de comunicaciones elegido por la empresa colaboradora para la puesta en marcha de la conexión de la misma con el Canal Gestión entregará en un único punto todo el tráfico gestionado de las empresas colaboradoras que conecten a través del mismo con Canal Gestión. Esto es, si el operador ya presta servicio a una empresa colaboradora de Canal Gestión, la nueva conexión deberá utilizar la infraestructura física existente en Canal Gestión 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 Gestión. La utilización de infraestructura común por parte de las empresas colaboradoras no supone la disponibilidad de conexión entre las mismas, siendo el objeto la conexión privada uno a uno de cada una de las empresas colaboradoras con Canal Gestión. En caso de que el operador no preste en la actualidad este servicio a ninguna empresa colaboradora, podrá realizar la

Empresa	Proyecto	Fecha
Canal de Isabel II Gestión, S.A.	Centro de Operaciones de Seguridad (SOC) y Oficina Técnica de Seguridad (OTS)	11/2015
Elaborado por:	Documento	Versión
Coordinación de Seguridad Informática.	Pliego de Prescripciones Técnicas Particulares	V0.17
Área de Planificación, Control y Seguridad		

conexión a la RCD de Canal Gestión, 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 Gestión 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 Gestión, 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 Gestión se realice exclusivamente a través de dicha conexión única.

## 2. Conexión redundante, de *backup*, contingencia o respaldo con la RCD de Canal Gestión.

El adjudicatario queda obligado a provisionar una segunda línea de comunicación con Canal Gestión 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 Gestión, con el objeto de disponer de una línea adicional y poder garantizar así la disponibilidad de las comunicaciones y la continuidad de los servicios contratados.

Empresa	Proyecto	Fecha
Canal de Isabel II Gestión, S.A.	Centro de Operaciones de Seguridad (SOC) y Oficina Técnica de Seguridad (OTS)	11/2015
Elaborado por:	Documento	Versión
Coordinación de Seguridad Informática.	Pliego de Prescripciones Técnicas Particulares	V0.17
Área de Planificación, Control y Seguridad		

### 3. Direccionamiento IP.

El adjudicatario se adecuará a los rangos de direccionamiento IP establecidos por Canal Gestión. Se establecerá por parte de Canal Gestión un rango IP compatible en el adjudicatario se integrará en la RCD de Canal Gestión. Si fuera necesaria la aplicación de traducción de direcciones (NAT) ésta será responsabilidad exclusiva del adjudicatario, 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 Gestión se reserva el derecho de monitorizar la línea de comunicaciones solicitada por el adjudicatario. 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 10.14. "Información y aclaraciones" del PCAP.

Empresa	Proyecto	Fecha
Canal de Isabel II Gestión, S.A.	Centro de Operaciones de Seguridad (SOC) y Oficina Técnica de Seguridad (OTS)	11/2015
Elaborado por:	Documento	Versión
Coordinación de Seguridad Informática.	Pliego de Prescripciones Técnicas Particulares	V0.17
Área de Planificación, Control y Seguridad		

## ANEXO 6. 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 Gestión.

1. El adjudicatario deberá utilizar el acceso concedido a la RCD y a los sistemas informáticos de Canal Gestión, 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 Gestión las medidas de índole técnico que establezca Canal Gestión 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, antispyware, etc.) instaladas, activas y actualizadas.
- Los equipos destinados a dar servicio al contrato, convenio o acuerdo mantenido con Canal Gestión deberán estar aislados de la red propia del adjudicatario.

Empresa	Proyecto	Fecha
Canal de Isabel II Gestión, S.A.	Centro de Operaciones de Seguridad (SOC) y Oficina Técnica de Seguridad (OTS)	11/2015
Elaborado por:	Documento	Versión
Coordinación de Seguridad Informática.	Pliego de Prescripciones Técnicas Particulares	V0.17
Área de Planificación, Control y Seguridad		

- Se deberá mantener informado en todo momento al responsable del contrato en Canal Gestión de cualquier cambio en equipos, configuración de los mismos y personal propio o externo que acceda a los recursos proporcionados por Canal Gestión para el desempeño de los trabajos y la prestación de los servicios recogidos en el contrato, aportando la adecuada justificación.
3. Canal Gestión 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 Gestión, 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 Gestión 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.
    - 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 Gestión y que han sido necesarios para el análisis y resolución del incidente.



Empresa	Proyecto	Fecha
Canal de Isabel II Gestión, S.A.	Centro de Operaciones de Seguridad (SOC) y Oficina Técnica de Seguridad (OTS)	11/2015
Elaborado por:	Documento	Versión
Coordinación de Seguridad Informática.	Pliego de Prescripciones Técnicas Particulares	V0.17
Área de Planificación, Control y Seguridad		

Dicho informe, una vez terminado, se remitirá al responsable del contrato en Canal Gestión.

5. Canal Gestión 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 Gestión detecta no conformidades con cualquiera de los puntos aquí reflejados, se concederá a la entidad externa, contrata o adjudicatario un plazo para subsanar dichas no conformidades. Si éstas persisten una vez agotado el plazo, podrán ser causa de resolución del contrato según lo establecido en la Cláusula 23ª de las Condiciones Generales de Contratación de Canal Gestión.
6. 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 10.14. "Información y aclaraciones" del PCAP.