Expte. S-06041-2022

Servicio Integral de Ciberseguridad para RTVE (SIC23)

Pliego de especificaciones técnicas

Índice

1 OBJETO

Este pliego define los servicios a contratar para dar continuidad al Servicio Integral de Ciberseguridad de RTVE.

Las funciones de este servicio serán las propias de la ciberseguridad en cuanto a la protección de activos de información digital por medio del tratamiento de amenazas que ponen en riesgo la información y los servicios ofrecidos por RTVE. Para esta protección se utilizan, además de un conjunto de políticas, métodos de gestión de riesgos, medidas, tecnologías y campañas activas de auditorías y concienciación, unos recursos externos especializados en distintos aspectos de ciberseguridad que, bajo la supervisión de responsables de RTVE, resuelvan positivamente cualquier incidente que se produzca.

Estas funciones se desarrollan actualmente dentro de un modelo de gobierno de la ciberseguridad para el que se requiere de servicios especializados para darle continuidad y desarrollo.

La meta de este servicio es conseguir un grado suficiente de industrialización de los controles y servicios de ciberseguridad como para poderlos monitorizar y gestionar dentro de un ciclo de mejora continua con la ayuda de herramientas especializadas.

Este soporte se desplegará mediante recursos profesionales especializados, así como con el despliegue de las herramientas necesarias, tal y como se describirá más adelante.

El servicio abarcará el soporte de ciberseguridad a las distintas áreas técnicas de RTVE:

- Dirección de Sistemas
- Dirección de Operaciones de TVE
- Dirección de Medios de RNE
- Dirección RTVE Digital
- Dirección de Emisiones y Redes

Dada la interrelación con otros servicios de CRTVE, se exige la coordinación estrecha del adjudicatario con otros proveedores para el funcionamiento conjunto con el resto de servicios IT, tales como:

- Comunicaciones corporativas
- Servicio de CAU
- Servicios de Desarrollo de Aplicaciones
- Servicios de Mantenimiento Hw y Sw de distintos fabricantes
- Servicios cloud de distintos proveedores
- Servicio de Gestión de Identidades
- Servicios de Administración de Sistemas
- Servicio de correo y colaboración
- Otros

Esta coordinación se realizará siempre a través de los responsables de cada servicio de RTVE.

CRTVE requiere por tanto un servicio “llave en mano” mediante el cual el adjudicatario proporcione un servicio

integral extremo a extremo y bajo su total responsabilidad en cuanto a su funcionamiento.

En este pliego se definen los requisitos del servicio a contratar, su funcionalidad, las condiciones de prestación del servicio y los parámetros de calidad y garantía del servicio.

El licitador incluirá en su oferta técnica cualquier información adicional relativa a la propuesta de servicio, aunque no se especifique en los pliegos, de forma que permita a CRTVE tener el máximo conocimiento de las características y prestaciones del servicio ofertado, teniendo lo recogido en este pliego la consideración de requerimientos mínimos.

Este proyecto debe permitir alcanzar los objetivos fijados, asegurando la evolución de los servicios incluidos en el pliego, implementando los nuevos requisitos y plataformas, los diseños tecnológicos, los procedimientos necesarios, las herramientas de software utilizadas y los servicios de soporte necesarios.

El licitador establecerá en su propuesta la estructura funcional de los servicios, definiendo de forma clara cuáles son los agentes y sus responsabilidades, de forma que se obtenga una mejora continua en el servicio.

Algunos de los beneficios a obtener son los siguientes:

- Máxima optimización de los servicios objeto del contrato con la consiguiente reducción de costes.
- Puesta al día tecnológica constante de las plataformas asociadas.
- Garantizar los niveles de servicio de RTVE requeridos por los usuarios finales.
- Gestión del cambio eficiente tanto en la puesta en marcha inicial del servicio como en las evoluciones e implantaciones de nuevos servicios o elementos en los entornos IT.

Para RTVE, el modelo de servicio ofertado debe proporcionar la máxima eficiencia en costes, sin que ello afecte la calidad del servicio, siendo prioritario establecer un modelo de mejora continua que permita avanzar hasta alcanzar los máximos niveles de calidad.

Estos trabajos se realizarán de acuerdo a un modelo de nivel de servicio (ANS), que permita, a partir de los indicadores, evaluar y medir de manera eficaz estos niveles y compararlos con los objetivos establecidos.

En el diseño del servicio se tendrán en cuenta las posibles evoluciones futuras que requiera CRTVE permitiendo ofrecer un servicio abierto, flexible y adaptable a las necesidades.

2 SITUACION ACTUAL

2.1 Marco de ciberseguridad actual

RTVE dispone actualmente de un Servicio Integral de Ciberseguridad, mediante el cual se están coordinando las actividades que atienden las necesidades y medidas a implantar en las distintas áreas.

Se ha implementado un modelo de gobierno por el que se van desarrollando los planes de acción y mejora paulatina de la seguridad. Este modelo requiere unos ciclos permanentes de revisión y mejora hasta alcanzar unos grados óptimos de gestión e industrialización de la seguridad digital en RTVE.

A partir de los planes de acción, se van generando nuevos servicios consolidados que requieren su permanente desarrollo, tales como la concienciación y formación en materia de seguridad de la información, las auditorías y test de Intrusión y la gestión de incidentes.

Periódicamente se confronta la realidad de las actividades de las distintas áreas con responsabilidades digitales en RTVE, con un marco general de controles de referencia. A partir de los resultados de esa confrontación se establecen unos objetivos de cumplimiento flexibles y realistas y un plan de Plan de Acción para alcanzarlos.

Estas recomendaciones pueden cubrir los distintos apartados de seguridad de la Información, desde definición de políticas, procesos y procedimientos, hasta medidas técnicas concretas que traten de remediar algún fallo o vulnerabilidad encontrado.

RTVE, en relación con la Ciberseguridad, tiene en la actualidad como autoridades de control de referencia:

- El Centro Criptológico Nacional (CCN)
- El Centro Nacional de Protección de Infraestructuras Críticas y Ciberseguridad (CNPIC)
- Instituto Nacional de Ciberseguridad (INCIBE)
- Oficina de Coordinación de ciberseguridad del Ministerio del Interior (OCC)
- Agencia Española de Protección de Datos (AEPD). Para aquellos incidentes en los que pudiera verse afectada la privacidad y los datos personales.

2.2 Marco normativo

Actualmente RTVE tiene definidas e implantadas diversas normativas y procedimientos relacionados con la ciberseguridad, que incluye, entre otros:

- Marco de controles basado en el Esquema Nacional de Seguridad (cruzado con otras normas ISO 27002, CSA, NIS2 entre otras)
- Política de Control de Usuarios y Accesos
- Norma de Protección de Datos y sus anexos
- Procedimientos de gestión de ciberincidentes
- Procedimiento de gestión de vulnerabilidades
- Guías de Bastionado de Puestos de trabajo y servidores
- Guía de desarrollo seguro
- Marco definición de arquitectura de redes

- Marco de definición de Plataformas tecnológicas
- Comité de Ciberseguridad
- Otros

2.3 Entornos tecnológicos

A título de referencia, se describen los principales entornos de Tecnología de la Información y Comunicaciones (TIC) gestionados por la Dirección Área de Sistemas.

A lo largo del servicio se irán identificando y clasificando los distintos elementos tecnológicos de las demás áreas técnicas que gestionan infraestructuras digitales:

- Sistemas Corporativos
- Medios y Operaciones de TVE
- Medios y Operaciones de RNE
- RTVE Interactivos.
- Emisiones y Redes.

Estas infraestructuras son tanto TI como de Tecnologías Operacionales (OT), núcleo de negocio principal de RTVE (Sistemas de producción audiovisual), y que también serán objeto del alcance de este pliego.

PLATAFORMAS CENTRALES CPD CORPORATIVO

- **Entornos HW:**
  - Servidores centrales IBM pSeries
  - Servidores centrales INTEL x86/64
  - Sistemas de almacenamiento HPE 3PAR
  - Servidores Cloud Azure

- **Entornos Lógicos**
  - Sistemas Operativos (AIX, Suse, Red Hat, Windows Server)
  - Sistemas de Virtualización (VMWare)
  - Servidores Web (WAS, JBOSS, Tomcat)
  - Sistemas Documentales (Filenet, IDOL, DOGMA)
  - Sistemas MAM (Tarsys)
  - Bases de Datos (DB2, ORACLE, SQL-Server, TAMINO, MySQL)

- **Entornos de Administración y Gestión**
  - Clúster de ficheros
  - Sistema de Monitorización ZABBIX
  - Planificador de procesos CONTROL-M
  - Sistema de Backup TSM
  - CMDB: CMDBuild
  - SCCM

- **Aplicaciones**
  - Gestor Documental audiovisual ARCA
  - Sistemas de Producción y Emisión
  - Aplicaciones J2EE
  - Aplicaciones .NET
  - Aplicaciones Intranet
  - Otras aplicaciones y paquetes
  - Aplicaciones en cloud (SaaS)
  - Aplicaciones Móviles (OMNIA)

El volumen de Sistemas Operativos de cada tipo es en el momento actual el siguiente:

COMUNICACIONES

RTVE dispone de una Red Corporativa que alcanza todas sus sedes a nivel nacional. Se dispone de cobertura WiFi en todos los centros.

La Red Corporativa dispone de una conexión a Internet que se presta de manera centralizada para todos los centros, compuesta por 3 accesos totalmente diversificados.

Las principales magnitudes de la red son:

- Sedes con conectividad: 90
- Equipos de comunicaciones: 500
- Puertos LAN: 20.000
- Puntos WiFi: 650
- Velocidad acceso Internet: 4Gb

Asimismo, existe una Red Técnica que también da cobertura a todas las sedes.

FIREWALL

Las distintas Áreas Técnicas de RTVE disponen de seguridad perimetral con Firewall.

El Área de Sistemas dispone de un equipamiento de seguridad para el acceso a Internet y conexión con otras redes de RTVE (Red de Contribución, Red de FFDD, Red de Radio, Redes Técnicas, empresas externas, etc.). Estos equipos realizan las siguientes funciones, entre otras:

- Firewall tanto de navegación como interno
- IPS (intrusion prevention system)

- Filtrado de tráfico a nivel de aplicación
- Antivirus y Sandbox para detección de amenazas avanzadas
- Filtrado de Navegación
- Filtrado de tráfico DNS
- Servidor VPN.
- Balanceador de carga.
- Gestión de ancho de banda.
- Análisis centralizado de logs
- Autenticación transparente de usuarios

PUESTOS DE TRABAJO

En el Área de Sistemas, en el ámbito del puesto de trabajo las plataformas son las siguientes:

- **Equipos ofimáticos y periféricos**
  - PCs de sobremesa y Portátiles: 7.000
  - Impresoras y MPF centralizadas: 600

- **Equipos Móviles**
  - Tabletas: Android, iOS: 200
  - Smartphones: Android, iOS: 5.000 (gestionados por el área de Emisiones y redes)
  - Para la gestión de los dispositivos móviles que acceden a recursos corporativos se encuentra en proceso de despliegue un sistema MDM.

- **Servicios de Colaboración (office365)**
  - Correo electrónico: Office365: 8.000 buzones
  - OneDrive, Teams: 1.000 cuentas aproximadamente

- **Plataforma de Movilidad** (APPs Móviles) OMNIA, basada en el middleware CONVERTIGO, en proceso de despliegue.

CONTROL DE ACCESOS Y SEGURIDAD

Las siguientes herramientas de gestión de seguridad y accesos están desplegadas en RTVE:

- **Gestión de Identidades (OpenIAM), compuesto por:**
  - Single Sign On (S3o): OpenLand
  - Gestión de Usuarios y Accesos Internos (GIDA): OpenIAM
  - Gestión de Usuarios y Accesos Externos Web (MCAW): OpenIAM
  - Portal de Autoservicio de Contraseñas (GAC): OpenIAM
  - Portal de Usuarios y Roles (PUR): Open IAM
  - Portal de accesos Privilegiados (PAP): Open IAM

- **Directorio activo**

  Se utiliza el AD de Microsoft para la autenticación de accesos en base a pertenencia a distintos grupos.

HERRAMIENTA SIEM

Se dispone de un SIEM (sistema de información de seguridad y gestión de eventos) **IBM Qradar** que monitoriza las distintas áreas técnicas de RTVE, en constante evolución e ingesta de eventos, con la incorporación paulatina de distintas fuentes. Esta herramienta se dispone actualmente en modo SaaS proporcionada por parte del proveedor actual del servicio SIC.

Las fuentes de eventos que se encuentran actualmente integradas con el SIEM para recopilación de eventos son las siguientes:

- **Antivirus** (Symantec y Trend Micro): 4 integraciones de distintas Áreas técnicas.
- **XDR** (Trend micro): 1 integración.
- **Firewall** (Fortianalyzer): 3 integraciones de distintas Áreas técnicas.
- **O365**: 1 integración.
- **Protección de correo** (Proofpoint): 1 integración.
- **HIDS** (WAZUH): 2 integraciones de distintas Áreas técnicas.
- **Portmirroring:** 3 integraciones de distintas Áreas técnicas.
- **VPN** (Fortianalyzer): 2 integraciones de distintas Áreas técnicas.

Estas integraciones evolucionan y se incrementan según cambios de tecnología en las Áreas Técnicas y nuevas fuentes de eventos y logs integrables.

Con objeto de realizar una recolección filtrada desde el origen de los LOGS se disponen actualmente de 3 sondas – ***Erismon*** – propiedad de RTVE, que serán puestas a disposición del adjudicatario si las requiere. Cada sonda contiene estos elementos:

- IBM Event Collector (recolector de eventos)
- IBM Flow Collector (recolector de flujos de red)

La recolección citada es filtrada por dos elementos que NO quedarán a disposición del adjudicatario (proporcionadas por el actual proveedor del servicio):

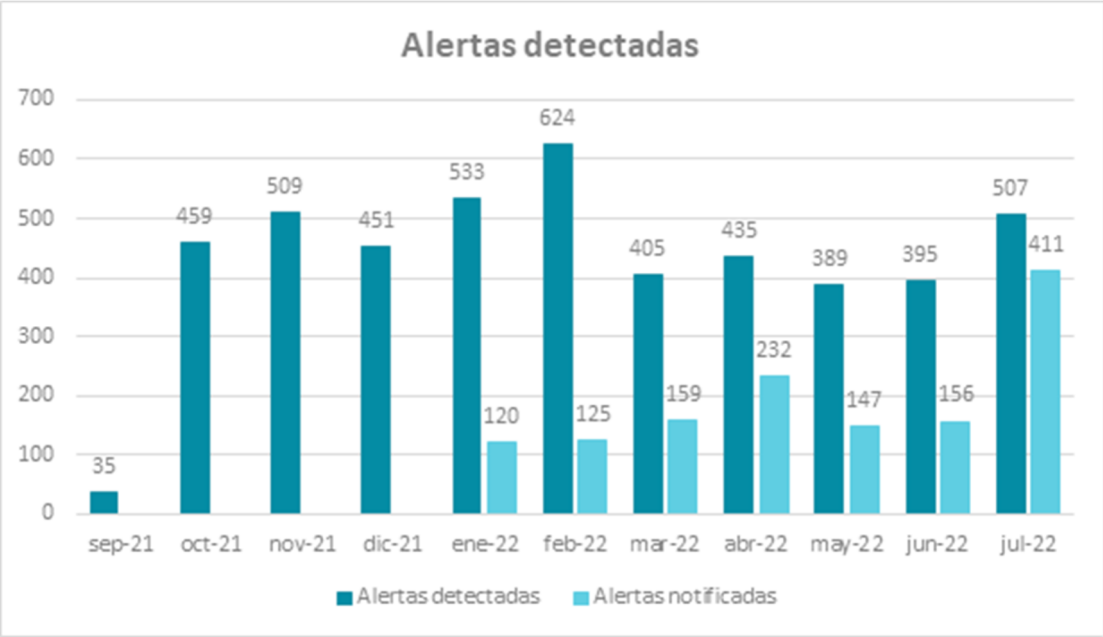
- Wazuh
- ZEEK

A título orientativo, los volúmenes aproximados de alertas gestionados (antes del filtrado) son los siguientes:

- **Eventos por segundo** (EPS): 5.000
- **Flujos de red por minuto** (FPM): 30.000

Estos datos corresponden al volumen final de eventos una vez filtrados por los dos elementos mencionados en el párrafo anterior.

A continuación, se muestran estadísticas de eventos recibidos y gestionados por el SOC (Centro de Operaciones de Seguridad) en los últimos meses:



Dado que se encuentra en proceso la integración de nuevas fuentes, estos datos podrán variar en el momento de inicio del servicio y durante toda la duración del contrato, y se muestran solo a título ilustrativo de la situación actual.

HERRAMIENTA DE GESTION DE ALERTAS

Se encuentra en proceso de despliegue la herramienta de ticketing SERVICE DESK PLUS que permite realizar el seguimiento de las actividades que se determinen necesarias para investigar, mitigar o solucionar eventos/alertas detectados en el SIEM. Esta herramienta la proporciona actualmente en modo SaaS por parte del proveedor actual del servicio SIC.

HERRAMIENTA DE CUADROS DE MANDO

Se dispone de una herramienta basada en PowerBI desde la que se visualiza el estado de los distintos indicadores o KPIs del servicio, tales como:

- Volumen de vulnerabilidades detectadas y resueltas en las distintas áreas técnicas
- Volumen de incidentes
- Cumplimiento de controles de seguridad en las distintas áreas
- Otros indicadores.

El licitador deberá detallar en su propuesta la metodología propuesta para estas tareas, formatos de plantillas y de entregables, etc.

Esta herramienta se encuentra en modo SaaS en el tenant Office365 de RTVE, siendo desarrollada y administrada por el actual adjudicatario del servicio SIC.

2.4 Modelo de servicio actual

Actualmente para la prestación del servicio SIC se dispone de la estructura descrita a continuación.

- **OTS Oficina Técnica de Seguridad**. Equipo fijo que trabaja bajo un modelo de tareas BAU (Business as Usual). Mensualmente se informa de forma pormenorizada de todas las actividades desarrolladas y que posteriormente se facturan en función del volumen de horas acordado para cada tarea.
- **Servicios especializados**. Se utilizan para acometer los trabajos especializados bajo demanda como puedan ser análisis técnicos, Test de intrusión, revisión de arquitecturas, informes específicos relacionados con ciberseguridad, tareas de integración de nuevas fuentes en el SOC, etc., que requieren diversos perfiles altamente especializados.
- **Servicio SOC**, es el que se encarga de la monitorización, mejoras en las reglas del SIEM, generación de informes periódicos detallados por fuentes y áreas técnicas, etc. Las incidencias se comunican a la OTS para que gestione las mismas con los técnicos identificados en cada AT de RTVE.
- **Responsable del Servicio,** disponible, para coordinar y dirigir los trabajos, y para la permanente coordinación con los responsables de RTVE. Seguirá permanente la evolución del contrato entre el Director Técnico de CRTVE y el responsable del Servicio, con reuniones periódicas con el Director Técnico de RTVE y Responsable de Ciberseguridad, al objeto de revisar el grado de cumplimiento de los objetivos, la planificación de actividades y demás aspectos de gestión. Los servicios de Responsable del Servicio NO son facturables de forma específica sino contenidos en el coste total del Servicio SIC.

3 ESPECIFICACIONES TÉCNICAS DEL SERVICIO

3.1 Alcance y enfoque general del servicio

El proyecto tiene por objeto un modelo de servicio que proporcione el soporte técnico y consultivo en la gestión de la Ciberseguridad de RTVE.

Las tareas y actividades que se requiere que realice el adjudicatario se agrupan del siguiente modo:

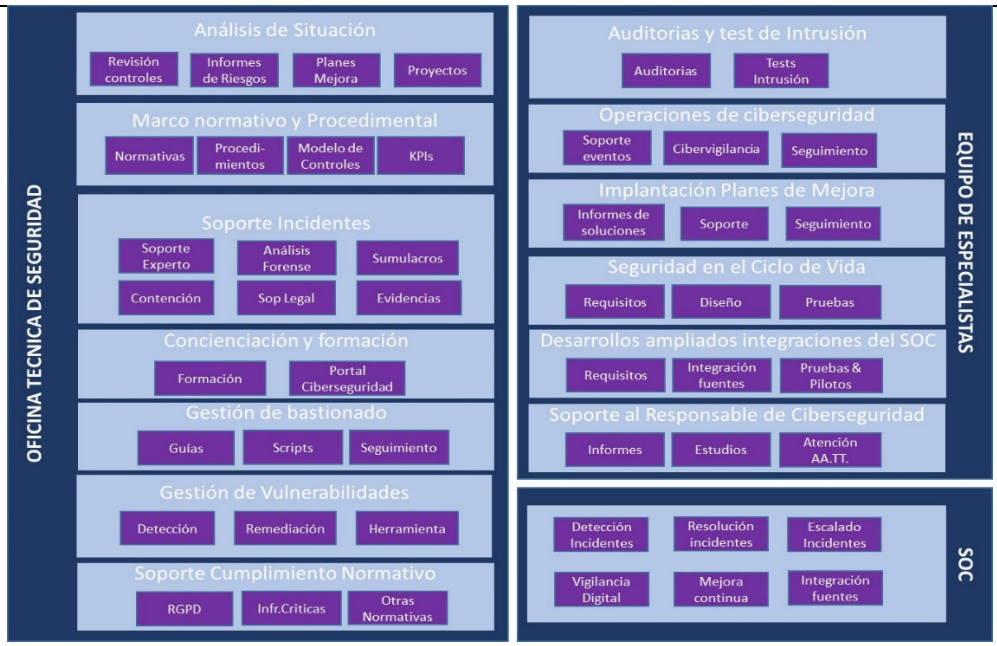
- **Servicio OTS**: es el conjunto de actividades de la línea base del servicio. La dedicación podrá ser variable a lo largo del servicio en función de la demanda, planificación de actividades BAU (Business as Usual). Las principales actividades son las siguientes:
    - Análisis de adecuación ENS y Planes de Mejora
    - Actualización del marco normativo y procedimental
    - Soporte a ciberincidentes
    - Concienciación y formación
    - Gestión de bastionado
    - Gestión de vulnerabilidades
    - Soporte al cumplimiento normativo

- **Servicios especializados:** conjunto de actividades desarrolladas a modo de proyectos con un marco temporal definido. Ejemplo de actividades son las siguientes:
    - Auditorías y Test de intrusión
    - Soporte a eventos
    - Evaluación de herramientas
    - Seguridad en el ciclo de vida de los sistemas
    - Desarrollo y mantenimiento de integraciones del SOC
    - Soporte Avanzado y Análisis Forenses
    - Soporte al Responsable de Seguridad
    -

- **Actividades del SOC:** es el conjunto de actividades de la línea base del servicio del SOC donde se realiza la monitorización de las distintas fuentes de RTVE. Las actividades incluyen, entre otras:
    - Monitorización de alertas a través del SIEM y comunicación de incidentes
    - Mejora de reglas
    - Generación de informe mensual
    - Soporte a Integración de nuevas fuentes

El alcance de los servicios serán todas las áreas con responsabilidad en tecnología digital de la corporación RTVE.

La siguiente figura presenta una visión resumida de todas estas actividades:



3.2 Oficina Técnica Seguridad (OTS)

A continuación, se describen en detalles las actividades requeridas en este apartado.

El licitador detallará en su oferta técnica, en una página como máximo por actividad, la metodología y herramientas propuestas para estas actividades, y el contenido propuesto para los entregables, y cualquier otro entregable que proponga para cada actividad.

3.2.1. Análisis de adecuación ENS y Planes de Mejora

Con esta actividad se pretende dar continuidad al ciclo de análisis de situación que se viene realizando en las distintas áreas, y la definición de los planes de acción correspondientes para la mejora de la seguridad.

De esta tarea irán generándose los planes de acción con los proyectos y recomendaciones a aplicar para cada caso.

El adjudicatario revisará periódicamente la situación de cumplimiento de los controles implantados en las distintas áreas, determinando su grado de implantación y su adecuación para mantener los niveles de ciberseguridad requeridos por CRTVE, **según el marco de controles definido, basado en el ENS.**

De cada ciclo de revisión se generará un informe de situación de riesgos y grado de cumplimiento de los controles, y un plan de acción de mejora, que incluirá recomendaciones priorizadas englobadas en distintos proyectos según los distintos apartados de la Seguridad de la Información y la Ciberseguridad.

Aparte de estos análisis periódicos de cada área tecnológica, cuando sea necesario se podrán requerir análisis de ciber-riesgos de sistemas concretos y la propuesta de planes de acción para su mejora.

El licitador detallará en su propuesta la documentación e información de RTVE que considere necesaria para la ejecución de estos trabajos.

CRTVE pondrá a disposición del adjudicatario toda la información existente que sea requerida, en el formato en el que se disponga, tal como:

- Modelo de controles de seguridad de RTVE (ENS)
- Análisis de Situación Actual, realizados con anterioridad en las distintas áreas
- Planes de Acción y proyectos en curso
- Descripción de los entornos tecnológicos existentes
- Descripción de los sistemas de seguridad existentes
- Cualquier otra información que se requiera

El adjudicatario será responsable de facilitar la coordinación con las distintas áreas afectadas, realizando tareas como:

- Preparación de reuniones con las áreas para conocer su casuística, activos, sistemas, y servicios críticos, explicando la metodología del proceso de toma de datos y aclarando dudas.
- Envío a los diferentes responsables de las plantillas de información a rellenar, y soporte a su cumplimentación.
- Recepción y chequeo de completitud de la información recibida, aclaración de dudas, etc.
- Comprobaciones de la veracidad de la información obtenida, en una muestra lo más representativa posible.
- Introducción de las vulnerabilidades detectadas en la Herramienta de Gestión.

Los entregables de esta tarea serán los siguientes:

- INFORMES DE SITUACIÓN DE LAS DISTINTAS ÁREAS
- PLANES DE MEJORA PROPUESTOS

3.2.2. Actualización del Marco Normativo y procedimental

Esta actividad consistirá en mantener actualizado el marco normativo de RTVE relacionado con la gestión de la ciberseguridad. Esto incluye la revisión y actualización permanente de las distintas normativas y procedimientos internos, tales como:

- Marco de Controles de Seguridad (basado en ENS)
- Procedimientos de gestión de ciberincidentes, vulnerabilidades, monitorización y correlación de eventos.
- Guías de Bastionado
- Marco de definición de Plataformas tecnológicas y redes
- Guías de Desarrollo Seguro
- Otros procedimientos

El adjudicatario proporcionará el soporte para la actualización permanente de este marco de referencia, según los cambios que se produzcan en las normativas y legislaciones de referencia y por cualquier otra necesidad o cambio tecnológico.

La actividad irá orientada a mantener un grado suficiente de industrialización de los procesos y controles de ciberseguridad sobre los activos digitales, los servicios y los datos.

Asimismo, el adjudicatario prestara soporte a la definición de los indicadores y KPIs necesarios con el fin de poder monitorizar la situación de madurez de la ciberseguridad y seguir su evolución.

Nuevos procesos

Asimismo, se incluirá la definición de nuevos procesos, procedimientos, normativas y estrategias de implantación de las mismas.

KPIs de ciberseguridad

El adjudicatario prestara soporte a la definición de los indicadores y KPIs necesarios con el fin de poder monitorizar la situación de madurez de la ciberseguridad y seguir su evolución.

El licitador detallará en un folio como máximo en su oferta técnica sus propuestas y ejemplos de KPIs y Cuadros de Mando que puedan ser de utilidad y aplicables al servicio.

El licitador deberá detallar en su propuesta la metodología propuesta para estas tareas, formatos de plantillas y de entregables, etc.

Los entregables de esta tarea serán los siguientes:

- MODELO CONTROLES ACTUALIZADO (BASADO EN ENS)
- MARCO NORMATIVO ACTUALIZADO
- POLITICAS DE CIBERSEGURIDAD ACTUALIZADAS
- PROCEDIMIENTOS DE CIBERSEGURIDAD ACTUALIZADOS
- PLANES Y ESTRATEGIAS DE DESPLIEGUE
- CUADROS DE MANDO Y KPIs DE CIBERSEGURIDAD

3.2.3. Soporte a ciberincidentes

Este servicio incluye el soporte en el tratamiento de los incidentes de ciberseguridad que se detecten, gestionando con los distintos servicios de soporte de RTVE las alertas recibidas. Las actividades al respecto son las siguientes:

- Determinar la causa raíz del incidente lo antes posible.
- Recomendar las acciones de contención necesarias para minimizar el impacto lo antes posible.
- Interactuar con las áreas de RTVE y servicios de soporte que sean necesarios para el diagnóstico y la resolución.
- Colaborar en la documentación del incidente y lecciones aprendidas.
- Proponer mejoras al procedimiento de gestión de incidentes para mejorar su efectividad.
- Proponer mejoras en las alertas, sistemas de correlación o de sistemas de detección para dar una respuesta cada vez más eficiente a los incidentes.

En caso de que se requiera, se podrá incorporar personal experto de los servicios especializados que sean necesarios según la naturaleza del incidente, para:

- Analizar los eventos de la red, que permitan situar el incidente en el tiempo.
- Aportar herramientas especializadas que sean necesarias en cada escenario.

- Ayudar en la recolección de evidencias, análisis forense y peritaje cuando sea necesario.
- Determinar los orígenes del ataque, los medios utilizados y los objetivos.
- Proporcionar soporte legal si fuera necesario ante un incidente.
- Análisis forenses.

En caso de que el incidente requiera soporte experto del adjudicatario para su resolución o para cualquier consulta relacionada con el mismo, deberán cumplirse los ANS de tiempos de reacción ante incidentes indicados en el apartado ANS.

Las posibles fuentes de incidentes serán:

- Detectados de forma automática por los distintos sistemas de seguridad (Firewall, Antivirus, SIEM, etc.).
- Reportados a través del CAU RTVE (si son detectados por usuarios finales).
- Reportados por los responsables de ciberseguridad de RTVE.
- Reportados por entidades externas como INCIBE, CCN, fabricantes, etc.
- Detectados por el SOC del adjudicatario.
- Otros

Ensayos de respuesta a ciberincidentes

Se realizarán ensayos periódicos para poner a prueba el grado de madurez de RTVE en los procedimientos y en la reacción ante incidentes, para verificar que se encuentran actualizados y que se utilizan adecuadamente:

- Detección
- Clasificación
- Priorización
- Asignación de tareas
- Coordinación entre los participantes y escalados
- Toma de decisiones
- Recolección de evidencias
- Comunicación a las partes requeridas
- Resolución
- Cierre

El adjudicatario proporcionará la metodología y herramientas propuestas para estos ensayos, que implicarán a todos los niveles de RTVE y del propio adjudicatario que sean necesarios en cada supuesto. Cualquier herramienta, escenario o simulación necesaria para estos ensayos será proporcionada por el adjudicatario sin coste adicional.

Los entregables de este apartado serán los siguientes:

- INFORMES DE ACTUACIÓN EN CADA INCIDENTE
- INFORMES MENSUALES DE INCIDENTES
- RESULTADOS DE ENSAYOS DE INCIDENTES

3.2.4. Concienciación y formación

Esta tarea consistirá en la realización de acciones de concienciación en ciberseguridad y seguridad de la información para los empleados y responsables de RTVE a distintos niveles, a lo largo de la prestación del servicio.

Los objetivos del plan de concienciación serán los siguientes:

- Ayudar a los usuarios y a los distintos niveles de dirección, para llevar a cabo un cambio positivo de comportamiento en relación con la adopción de buenos hábitos de seguridad.
- Mantenerles informados de la normativa de ciberseguridad que les aplique.
- Hacerles conscientes de su propia responsabilidad en relación con la ciberseguridad, y cómo reaccionar ante las amenazas.
- Responder a las dudas relacionadas con la ciberseguridad que, desde los distintos ámbitos de la empresa o de sus relaciones, puedan surgir.
- Informarles de los riesgos y amenazas.
- Analizar el grado de conocimiento y sensibilización.
- Contribuir, en definitiva, a minimizar el número y gravedad de incidencias de seguridad experimentadas por el usuario.

El colectivo objeto de las acciones de formación y concienciación es de aproximadamente **6.500 empleados**. Se deberán tener en cuenta:

- Los distintos perfiles a los que se debe dirigir la concienciación
- Las acciones formativas y de concienciación y divulgación más adecuadas a cada colectivo.
- La forma de medir la aceptación y efectividad de las mismas.

La metodología y materiales de formación incluirán las herramientas más adecuadas para cada caso:

- Formación presencial (en caso de necesidad)
- Autoformación interactiva y auto evaluación
- Formación en casos prácticos
- Simulación de ataques (phishing, smishing, etc.)

Dentro de estas actividades, se actualizará periódicamente con nuevos contenidos el Portal de Ciberseguridad de RTVE en Intranet.

Las acciones formativas y de concienciación se realizarán gradualmente, de acuerdo con el plan que proponga el adjudicatario y consensuado con CRTVE, y con la periodicidad que se determine para asegurar su efectividad.

RTVE dispone de una plataforma basada en Moodle, gestionada por el Instituto de RTVE, y que deberá usarse preferentemente para las acciones de formación.

Los materiales se actualizarán periódicamente según la evolución de las necesidades, amenazas y carencias detectadas.

El licitador detallará en un folio como máximo en su oferta técnica la metodología propuesta y modelos y ejemplos de materiales propuestos para estas tareas.

Los entregables de este apartado serán los siguientes:

- PLANES DE FORMACIÓN Y CONCIENCIACIÓN
- CONTENIDOS Y HERRAMIENTAS DE FORMACION Y CONCIENCIACIÓN

3.2.5. Gestión de Bastionado

El objetivo de este servicio es doble. En primer término, es la elaboración, mantenimiento, desarrollo y actualización de guías de bastionado, así como la realización de scripts de revisión para chequear el cumplimiento de la guía en particular.

Las guías a realizar serán de distinta índole y tecnologías, usando como referente las guías existentes de los fabricantes y las guías del CCN, si existieran.

Por otro lado, se debe establecer ciclos de revisión del cumplimiento de las guías de bastionado por cada tecnología, para lo cual el adjudicatario tendrá que determinar con las distintas áreas de RTVE el modelo y alcance de revisiones.

Las actividades necesarias para esta tarea serán, entre otras, las siguientes:

- Realización de guías de bastionado
- Realización de Scripts de verificación
- Gestión de revisiones
- Seguimiento de resolución o justificación de incumplimientos
- Información periódica de situación

Actualmente RTVE no tiene implantada una herramienta de gestión de bastionado. En cualquier caso, el adjudicatario gestionará el ciclo de vida de las vulnerabilidades mediante las herramientas que se determinen con RTVE.

El licitador indicará en su oferta técnica si dentro del servicio incluye alguna herramienta sin coste para RTVE, así como sus funcionalidades. En caso de ser coste, si indicará el coste mensual en la oferta económica para su contratación en posibles ampliaciones si lo requiere RTVE.

Los entregables de este apartado serán los siguientes:

- GUIAS DE BASTIONADO ACTUALIZADAS
- SCRIPTS DE REVISION ACTUALIZADOS
- INFORMES DE REVISION DE BASTIONADO

3.2.6. Gestión de Vulnerabilidades

El objetivo de este servicio consistirá, una vez se vayan implementando las distintas fases del proceso, en la gestión permanente e integral del ciclo de vida de las vulnerabilidades que se vayan identificando en los distintos entornos, según el procedimiento de gestión de vulnerabilidades establecido en RTVE.

Las actividades necesarias para esta tarea serán, entre otras, las siguientes:

- Registro de vulnerabilidades por entornos
- Clasificación de las vulnerabilidades

- Asignación de responsables

- Seguimiento de su resolución
- Información periódica de situación

Actualmente RTVE no tiene implantada una herramienta de gestión de vulnerabilidades. En cualquier caso, el adjudicatario gestionará el ciclo de vida de las vulnerabilidades mediante las herramientas que se determinen con RTVE.

El adjudicatario gestionará con las áreas responsables de los sistemas afectados, la planificación de las acciones necesarias para resolverlas y/o mitigar los riesgos (ej.: implantación de parches, propuesta de acciones alternativas, etc.), teniendo en cuenta la criticidad de cada una.

Asimismo, se implementarán alertas para notificar los posibles incumplimientos en cuanto a políticas de seguridad y verificar la correcta implantación de parches y corrección de otras vulnerabilidades.

Se mantendrá contacto estrecho con los grupos de soporte de RTVE para determinar y tratar posibles amenazas e incidentes recurrentes, en un proceso de evolución y mejora continuo.

El licitador deberá detallar en su oferta técnica la metodología, entregables y herramientas propuestas para estos servicios, e indicará en la misma si dentro del servicio incluye alguna herramienta sin coste para RTVE, así como sus funcionalidades. En caso de tener coste adicional, este se indicará el importe mensual en la oferta económica.

Los entregables de este apartado podrán ser:

- INFORMES PERIODICOS DE VULNERABILIDADES

3.2.7. Soporte al cumplimiento normativo

Este servicio incluye la asesoría y soporte al cumplimiento de las distintas normas aplicables actuales o futuras, tales como:

- Legislación de Protección de Datos (RGPD/LOPD).
- Ley 8/2011 de Infraestructuras críticas.
- Directiva NIS traspuesto al Real Decreto 43/2021 de 26 de enero y NIS2.
- Real Decreto – Ley 12/2018, de seguridad de las redes y sistemas de la información.
- Otras legislaciones o normativas del ámbito de Seguridad de la Información a las que pueda estar sujeta RTVE durante la ejecución del contrato.
- Esquema nacional de Seguridad

En relación con el cumplimiento del RGPD/LOPD, en RTVE a nivel corporativo se lidera la realización de iniciativas desde la Dirección de Protección de Datos, que realiza la generación del marco normativo corporativo, y la identificación de los tratamientos de datos.

Por ello, el servicio de ciberseguridad se orientará a asesorar técnicamente en el cumplimiento de dicho marco normativo, incluyendo tareas de soporte, como:

- Definir o ajustar procedimientos internos para cumplir la normativa.

- Asesorar en la implementación de medidas que se requieran en los sistemas corporativos, tanto detectadas por el propio adjudicatario, como por las auditorias de terceras partes que se realicen.
- Dar soporte a la elaboración de la documentación necesaria.
- Resolución de consultas y dudas sobre la implementación de medidas.
- Elaborar y actualizar los documentos de seguridad relativos a los sistemas corporativos.
- Prestar soporte para atender cualquier solicitud de información por parte de las autoridades de control o unidades internas, o al tratamiento de cualquier solicitud.
- Prestar soporte a la auditoria de contratistas de servicios TIC de RTVE que actúen como encargados de tratamiento de datos.
- Prestar soporte ante cualquier incidente de protección de datos o elaboración de informes que requiera el DPO o cualquier otra área o entidad.
- Otros servicios relacionados que se requieran.

Los entregables de este apartado serán los siguientes:

- INFORMES DE SOPORTE AL CUMPLIMIENTO NORMATIVO

3.3 Servicios especializados

A continuación, se describen las actividades requeridas en este apartado.

El licitador detallará en un folio como máximo en su oferta técnica la metodología y herramientas propuestas cada una de estas actividades, y cualquier otro entregable que proponga para cada actividad.

3.3.1. Auditorías y test de intrusión

Dentro de este servicio se realizarán auditorías periódicas de situación de ciberseguridad en los sistemas críticos de las distintas áreas de RTVE, con objeto de:

- Conocer periódicamente el estado de los mismos.
- Determinar el nivel de protección y las vulnerabilidades y riesgos existentes.
- Determinar el grado de cumplimiento de las normativas y procedimientos y la efectividad de los distintos planes de acción.
- Detectar y notificar los incumplimientos en cuanto a políticas de seguridad.

Como resultado de las mismas, se generará un informe con los resultados, indicando de manera clara las vulnerabilidades detectadas, su severidad, y los posibles riesgos y las acciones de mejora.

Se deberán evaluar las posibles excepciones de los controles implementados por causas justificadas en algún servicio, estableciendo controles alternativos para mitigar el riesgo que pudiera generarse.

Estas auditorías se realizarán a partir de los controles definidos y los resultados del análisis de riesgos de cada área.

Los entornos sobre los que se realizarán estos test serán, entre otros, los siguientes:

- Red de comunicaciones corporativa, redes WiFi, redes técnicas
- Cortafuegos
- Plataformas tecnológicas (servidores, etc.)
- Aplicaciones corporativas
- Sistemas de producción de audio y video
- Plataforma RTVE.ES y otros medios interactivos de RTVE en internet y móviles
- Servicios y aplicaciones móviles
- Puestos de trabajo
- Servicios externos y cloud
- Otros servicios y plataformas de RTVE

En los test de intrusión, se incluirán, entre otros análisis y comprobaciones de vulnerabilidades:

- Ejecución de código remoto
- Gestión de errores y validaciones de datos
- Autenticación y autorización
- Control de sesiones
- Encriptado de datos
- Robo de datos
- Elevación de privilegios
- Otras vulnerabilidades

Durante la ejecución del contrato RTVE definirá la planificación de las auditorias y test de intrusión a realizar por el adjudicatario.

Las pruebas, auditorías técnicas y test se han de planificar y ejecutar garantizando que no afectarán negativamente a los sistemas y servicios en producción. Es responsabilidad del adjudicatario informar del impacto que puedan causar las auditorias, así como de acordar las ventanas de actuación necesarias.

El licitador describirá en su oferta técnica la metodología y herramientas propuestas para estas tareas, y deberá incluir las herramientas que se vayan a utilizar, que serán sin coste adicional para RTVE.

Los entregables de este apartado serán los siguientes:

- PROPUESTAS DE ALCANCE DE AUDITORIAS Y TESTS DE INTRUSION
- INFORMES DE RESULTADOS Y RECOMENDACIONES

3.3.2. Soporte a eventos RTVE

Esta actividad tiene como objetivo el soporte a RTVE en aquellos eventos (por ejemplo, eurovisión, JJOO, etc.) en los que se determine necesario realizar revisiones preventivas de activos y sistemas que se utilicen para cubrir el evento, así como soporte online e incluso guardias durante el evento como soporte a ciberincidentes que puedan ocurrir a lo largo del evento. Inclusive, se puede determinar la necesidad de realizar labores de Cibervigilancia relacionado con el evento.

Esta tarea implicará no solo interlocución con áreas técnicas de RTVE involucradas en el evento sino, inclusive, puede ser necesario interlocución con otros organismos externos a RTVE, como por ejemplo en el caso de eventos internacionales.

Entre las tareas a realizar se pueden destacar:

- Determinación del alcance de activos y sistemas a revisar
- Vigilancia digital necesaria
- Soporte en el evento
- Seguimiento de remediación de las vulnerabilidades identificadas
- Interlocución activa con las Áreas Técnicas

Los entregables de este apartado serán los siguientes:

- INFORMES DEL SOPORTE A EVENTOS

3.3.3. Evaluación de Herramientas

El adjudicatario deberá proporcionar asesoramiento experto sobre las herramientas más adecuadas para mitigar posibles riesgos y vulnerabilidades, como, por ejemplo:

- Sistemas anti-intrusión
- Protección avanzada de puestos de trabajo y servidores
- Herramientas de gestión de vulnerabilidades
- Herramientas de resolución de incidentes
- Herramientas de monitorización y correlación (SIEM)
- Otras herramientas y tecnologías

Este asesoramiento permitirá, entre otros:

- Soporte para definir los requerimientos específicos de RTVE
- Evaluación de herramientas y tecnologías
- Soporte al despliegue de herramientas en caso necesario

Los entregables de este apartado podrán ser:

- INFORMES SOBRE HERRAMIENTAS DE SEGURIDAD

3.3.4. Seguridad en el ciclo de vida de los sistemas

Se evaluarán los diferentes aspectos de seguridad que puedan afectar o que deban tenerse en cuenta en los nuevos sistemas, aplicaciones y cambios relevantes en los mismos, con el fin de prevenir vulnerabilidades en las fases de diseño, desarrollo y despliegue de éstos, incluyendo:

- Requerimientos de seguridad en el diseño.
- Planes de pruebas de seguridad.
- Revisión técnica de seguridad, antes de la puesta en producción.
- Controles de seguridad en el proceso de gestión de cambios.
- Revisión de la seguridad de servicios externos y cloud, y control y gestión del cumplimiento de requisitos de seguridad con proveedores.

Como aspectos destacados de estas revisiones, se ha de garantizar que se cumplan los requerimientos

legales y normativos, las recomendaciones de las auditorías y test de intrusión, así como las buenas prácticas reconocidas y las recomendaciones de los fabricantes.

Los entregables de este apartado podrán ser:

- PLANES DE PRUEBAS DE SEGURIDAD
- INFORMES DE REVISION DE SEGURIDAD
- REQUISITOS DE SEGURIDAD EN NUEVOS SISTEMAS
- MODELO DE GESTIÓN DE SERVICIOS EXTERNOS Y EN LA NUBE

3.3.5. Desarrollo y mantenimiento integraciones del SOC

Dentro de esta actividad, y como complemento a la actividad del SOC, descrita más adelante, se requerirá soporte técnico para realizar nuevas integraciones de fuentes de datos.

En este sentido, el equipo de especialistas deberá de hacer las actividades necesarias, primeramente, para analizar la viabilidad de la integración y posteriormente realizar los desarrollos necesarios para poder alcanzar la integración, incluyendo:

- Interlocución con fabricantes / propietarios de la fuente objeto de integración
- Evaluación de la viabilidad de la integración
- Estimación de costes de desarrollos necesarios
- Desarrollo técnico de integración
- Pruebas técnicas de la integración
- Evolución y mantenimiento de integraciones existentes
- Mantenimiento y actualización de las Sondas ERISMON (en caso de mantener su utilización en el servicio)

Los entregables de este apartado serán los siguientes:

- INFORMES DE EVALUACION DE INTEGRACIONES SOC
- DESARROLLO TECNICO Y MANTENIMIENTO DE INTEGRACIONES

3.3.6. Análisis forense

Cuando se produzca un incidente relevante, si lo requiere RTVE o una autoridad de control, se realizarán actividades de soporte avanzado especializado que puedan requerirse, así como análisis forenses por recursos expertos del adjudicatario.

El adjudicatario deberá disponer de personal altamente especializado en distintas tecnologías que puedan ser requeridos en caso de incidentes.

Para los análisis forenses, el adjudicatario deberá disponer, en el marco de la prestación del servicio, de herramientas como:

- Sandboxes para el análisis automatizado de muestras de código malicioso.
- Entorno para ingeniería inversa de código malicioso.
- Herramientas de análisis de forense de discos.

- Material para la realización de intervenciones para la adquisición de evidencias:

- Kit de material para adquisiciones forense.
- Clonadores de disco.
- Dispositivos "writeblockers" para manipulación segura de evidencias.
- Cámaras fotográficas con localización GPS para registro documental del proceso de adquisición forense.
- Otras herramientas forenses.

El licitador detallará en un folio como máximo en su oferta técnica los medios disponibles, tanto técnicos como humanos para estas tareas según la naturaleza de los incidentes.

Los entregables de este apartado serán los siguientes:

- SERVICIOS DE SOPORTE AVANZADO
- INFORMES FORENSES

3.3.7. Soporte al Responsable de Seguridad

En el ámbito de las funciones y actividades del Responsable de Seguridad de RTVE es necesario el soporte para resolver consultas, realización de informes específicos, búsqueda de información, etc. en el ámbito de la ciberseguridad.

Es de especial relevancia la necesidad de soporte al Responsable de Seguridad para atender las solicitudes que le son requeridas desde organismos/entidades oficiales (CCN, OCC, etc.), donde los plazos de respuesta son establecidos por el propio organismo solicitante y sin poder ser determinado a priori.

En este sentido, deberá realizar las actividades necesarias, para conformar la información solicitada en tiempo y forma, incluyendo:

- Revisión de documentos
- Elaboración de informes ad-hoc
- Respuestas informativas a consultas concretas
- Interlocución con otras áreas técnicas que puedan estar involucradas
- Apoyo en Informes a distintos comités

En caso necesario, se utilizarán también los servicios especializados que fueran necesarios por parte del equipo de especialistas descrito más adelante.

Los entregables de este apartado podrán ser:

- INFORME ESPECIFICOS
- RESPUESTAS INFORMATIVAS DE CONSULTAS

3.4 Servicio de SOC

3.4.1 Características generales

Dentro del modelo de servicio requerido por RTVE, la actividad del Centro de Operaciones de Ciberseguridad (COC) de RTVE se realizará de forma remota desde las instalaciones del adjudicatario.

Para ello el licitador deberá disponer de un Centro de Operaciones de Seguridad (SOC) que reúna las suficientes garantías. El licitador describirá en su oferta técnica, con el mayor detalle posible, las actividades que

proporciona su servicio SOC, la metodología y herramientas utilizadas, formatos de informes, y cualquier otra información que permita conocer las características de dicho servicio.

El licitador describirá cualquier otra tarea o servicio adicionales no especificadas en este pliego que incluya en el servicio sin coste adicional.

En caso de existir servicios del SOC no especificados en este apartado que puedan ofrecerse con coste adicional, se detallaran en su propuesta técnica y se indicará el coste unitario mensual en su oferta económica, para el caso de que RTVE requiera su contratación.

RTVE pondrá a disposición del SOC, el acceso a los entornos y herramientas necesarias de RTVE a través de VPN con el fin de permitir la realización de las tareas encomendadas de forma segura.

El licitador describirá con el mayor detalle posible en su oferta técnica los medios, infraestructura, herramientas y recursos disponibles en el SOC, detallando el número de recursos, cualificación y certificados en cada uno de los aspectos de ciberseguridad requeridos.

A efectos de estimar el volumen de recursos necesarios en el SOC y dimensionar las herramientas necesarias, para dar servicio a RTVE, a continuación, se indica el volumen estimado de alertas a gestionar por el SOC:

- **Eventos por segundo** (EPS): 6.850
- **Flujos de red por minuto** (FPM): 80.000

	SITUACIÓN (con 4 sondas y 100 servidores en Wazuh)		
	EPS actuales Qradar	**EPS sin Arquitectura "proveedor actual" (Wazuh y Zeek)**	**FPM sin Arquitectura "proveedor actual" (Wazuh y Zeek)**
Antivirus (Symantec y Trend Micro): 4 integraciones de distintas Áreas técnicas	65	65	N/A
XDR (Trend micro): 1 integración	5	5	N/A
Firewall (Fortianalizer): 4 integraciones de distintas Áreas técnicas	550	5.500	N/A
Microsoft Office365 – 1 integración	30	30	N/A
Protección de correo (Proofpoint): 1 integración	250	250	N/A
HIDS Wazuh: 4 integraciones de distintas Áreas técnicas (100 Servidores)	0	1.000	N/A
NIDS Zeek: 3 integraciones de distintas Áreas técnicas	N/A	N/A	80.000
TOTAL:	**900**	**6.850**	**80.000**

El número de eventos por segundo corresponde al valor bruto que posteriormente filtra la inteligencia de las sondas del actual proveedor. Si el licitador no utilizara este tipo de solución, deberá gestionar el total de eventos citados con su propia inteligencia.

Actualmente, una vez filtrados los EPS brutos, la cifra que efectivamente gestiona el SIEM Qradar es 900.

Existirá un **margen de variación del +/- 10%** en estos volúmenes, que no supondrá un coste adicional para RTVE. Para el caso de superarse dicho margen, el licitador indicará en su oferta económica el coste mensual por inclusión de eventos adicionales, tanto para la operación del SOC como para la herramienta SIEM propuesta. Igualmente, en caso de que el número de eventos reales sea inferior a dicho margen, se descontará el importe equivalente.

Dada la criticidad de este servicio, y de la información gestionada en el mismo:

- Los recursos dentro del SOC deberán ser estables, bien a través de recursos dedicados en exclusiva o bien compartidos con otros clientes.
- El adjudicatario asegurará que en todo caso se mantiene el conocimiento de los entornos de RTVE cuya supervisión y vigilancia se realice desde este SOC.
- Debe prestarse al 100% por personal propio del adjudicatario, sin subcontrataciones a terceros.
- Deberá encontrarse en España.
- Tendrá un funcionamiento 24x7 para los servicios requeridos.
- Deberá disponer de una herramienta SIEM de correlación de eventos que se deberá integrar con las distintas fuentes de RTVE.
- Los datos que sean alojados en la infraestructura del SOC (herramienta SIEM y otras que se utilicen) deberán encontrarse en la Unión Europea.
- La comunicación con el SOC será siempre en español.

3.4.2 Herramienta SIEM

El servicio SOC deberá incluir la provisión de la herramienta SIEM que proponga el licitador. Deberá detallarse en la oferta técnica con el máximo detalle posible la herramienta propuesta y todas sus funcionalidades.

Según se indica en el apartado “situación actual”, el SIEM actual utilizado en el SOC es *IBM Qradar*, proporcionado por el actual proveedor y configurado con un alto grado de integración con las fuentes de RTVE. El licitador describirá en su oferta técnica el SIEM que propone para el servicio, que deberá proporcionarse en modo SaaS por parte del adjudicatario durante toda la duración del contrato, incluyendo todo lo necesario como:

- Licencias de uso
- Plataforma Hw y SW
- Comunicaciones
- Administración, soporte y operación
- Actualizaciones que sean necesarias
- Otras tareas necesarias para el funcionamiento

El adjudicatario deberá realizar, sin coste para RTVE, todas las tareas de migración de la herramienta SIEM actual a la nueva propuesta que resulten necesarias, tales como:

- Puesta en marcha y configuración del entorno para RTVE

- Integración con todas las fuentes de RTVE, incluyendo los desarrollos necesarios.
- Migración de las reglas de correlación y análisis de eventos actuales
- Migración de datos
- Otras tareas que se requieran

Todas estas tareas se realizarán sin coste para RTVE, tanto en el caso de que se proponga el SIEM del mismo fabricante actual (IBM-QRADAR), que deberá migrar al entorno del adjudicatario, como si se propone un SIEM de un fabricante distinto al actual.

Se valorará que el SIEM propuesto:

- simplifique y cumpla el proceso de transición al nuevo adjudicatario, el mantenimiento de los históricos y pulido de reglas ya realizado y para asegurar el mantenimiento y cumplimiento del servicio actual, así como el proceso de transición en el plazo necesario.
- Se encuentre en el cuadrante Gartner de líderes en los últimos cinco años.
- Que se encuentre en el catálogo CCN-STIC-105 como ENS alto dentro de la familia de Sistemas de Gestión de eventos de Seguridad.

3.4.3 Actividades SOC

Monitorización de fuentes a través del SIEM

Dentro de esta actividad se realizará la correlación de los eventos y se gestionaran las alertas detectadas. El adjudicatario deberá realizar la interlocución con las distintas áreas técnicas de RTVE, para comprobar las alertas, así como mantener y evolucionar las guías de actuación por tipologías de fuentes, así como los interlocutores de las áreas técnicas.

En este sentido, el equipo del SOC se deberá coordinar con la OTS para que las alertas detectadas por el SOC tengan continuidad en el personal de la OTS para hacer las comprobaciones necesarias, incluyendo actividades como:

- Detección y gestión de alertas
- Coordinación con la OTS
- Comunicar los incidentes a través de herramienta de ticketing.
- Mantenimiento de la documentación de las fuentes integradas.
- Comprobación de la conexión / informes de caídas
- Actividades de ciber vigilancia que se soliciten
- Informes mensuales del servicio

Mejora de reglas

El SOC deberá ser capaz de realizar la mejora continua de las reglas de correlación del SIEM de forma que los falsos positivos y, los eventos que llegan al SIEM sean optimizados y se reduzcan las alertas no válidas y falsos positivos.

El SOC deberá realizar cuantas actividades / acciones sean necesarias para evolucionar, mejorar y optimizar las reglas del SIEM.

Generación de informe mensual

El SOC deberá emitir un informe mensual con el detalle del servicio, donde se detallará de forma segmentada las alertas procesadas, las alertas que se han comunicado a RTVE, las alertas que han resultado positivas, los indicadores de disponibilidad, etc.

La segmentación a la que se hace referencia es por tipo de fuente, así como el área técnica de RTVE de la que proviene la alerta.

Se emitirá al menos 1 informe general, sin menoscabo que se determine la necesidad de poner a disposición tantos informes como áreas técnicas integradas (en la actualidad 4 áreas técnicas).

Integración de nuevas fuentes

En el marco de la presentación del servicio del SOC, se entiende que no es un servicio estático, sino más bien dinámico, donde se deberá colaborar en la integración y evolución de integraciones de fuentes que se consideren que se desarrollarán por el equipo de especialistas

Los entregables de este apartado serán los siguientes:

- INFORME DE MENSUAL DEL SERVICIO SOC
- DOCUMENTACION DE LAS INTEGRACIONES DE FUENTES DE DATOS

3.4.4 Herramienta de ticketing

Como se ha comentado, actualmente, el servicio de SOC dispone de la herramienta ***Service Desk Plus***, donde se ha configurado las tareas, actividades, campos y usuarios, de forma que los eventos detectados se comunican a los responsables de las distintas áreas Técnicas de RTVE asignando el ticket a dichos usuarios, para que éstos investiguen, mitiguen o solucionen el evento notificado.

El licitador deberá proponer una herramienta equivalente, siendo aportada por el proveedor saliente toda la exportación necesaria para su migración a la nueva herramienta, así como el histórico de tickets.

Se valorará que la herramienta de ticketing favorezca la migración de un adjudicatario a otro. Por ejemplo: con mínima afección a las labores de sus usuarios, sin pérdida de servicio, sin pérdida de histórico, etc.

La herramienta debe permitir generar el registro y asignación de las solicitudes a los responsables, así como el seguimiento de su evolución, incluyendo:

- Recopilación datos de contacto del usuario final, en su caso
- Priorización a partir Urgencia e Impacto
- Categorización conforme a catálogo de servicios
- Asignación al grupo de resolución
- Monitorización de cambios de estado.
- Notificaciones automáticas vía e-mail.
- Relación con Problemas
- Relación con Cambios.
- Creación de informes y exportación en diferentes formatos.
- Se podrán dar de alta todos los usuarios necesarios (gestores de áreas técnicas, personal de
- ciberseguridad, técnicos de soporte de RTVE y de los distintos servicios técnicos de soporte)

4 EQUIPO PROFESIONAL

4.1 Características generales

El licitador indicará en su oferta técnica con el máximo detalle el equipo de trabajo propuesto para el servicio, que deberá cumplir los mínimos indicados más adelante.

Si bien los licitadores deberán concretar en sus respectivas ofertas el equipo técnico ofrecido que considere idóneo para cubrir las condiciones del presente pliego, **no es objetivo del mismo la contratación de un equipo de personas sino el disponer de un servicio integral ligado al Acuerdo de Nivel de Servicio**.

En concreto, es precisa la dedicación exclusiva (8x5) de:

- un recurso de OTS para valoración de aplicabilidad y cumplimiento de ENS por sistemas.
- Un recurso de OTS para gestión de alertas.
    - Adicionalmente otro recurso de OTS para revisión de cumplimiento.
- Un recurso de "Servicios Especializados" de coordinación técnica de los trabajos de este ámbito.

Deberá justificarse mensualmente esta dedicación exclusiva facturándose lo realmente ejecutado.

Los servicios que son objeto del alcance de este pliego serán realizados de forma remota, pero puntualmente podrán ser realizados in-situ en las dependencias de CRTVE, según lo requiera la naturaleza de la actividad sin coste adicional para RTVE. En caso de requerirse, el adjudicatario deberá asegurar que cualquier miembro del equipo de trabajo estable preste servicio presencial con un preaviso de 24h.

El servicio prestado a RTVE por el adjudicatario deberá quedar garantizado en cualquier circunstancia, independientemente de las posibles eventualidades sobre los recursos asignados a la prestación del servicio, debiendo ser sustituidos o reemplazados dado el caso, por otros recursos que tengan al menos la misma experiencia laboral y conocimientos de modo que la transferencia de conocimiento sea transparente al servicio.

Dada la propia diversidad del servicio y el equipo multidisciplinar necesario, el licitador deberá asegurar toda la flexibilidad precisa para incrementar puntualmente el número de recursos, en caso de que se produzca una necesidad sobrevenida por parte de RTVE, incidente grave, picos de trabajo, de forma permanente o puntual, con dedicación parcial o total, y que no pueda asumirse por el equipo habitual.

Los licitadores deberán aportar los currículos de los recursos personales destinados al servicio según el formato indicado en el Anexo I, con la finalidad de que RTVE pueda evaluarlos.

La inexactitud en el nivel de conocimientos técnicos de los recursos destinados para el equipo inicial, implicará la sustitución inmediata del mismo.

El adjudicatario se compromete a mantener el nivel de conocimientos y cualificación asociados a los recursos requeridos en este pliego, para el perfecto cumplimiento de los objetivos del proyecto durante todo el periodo de ejecución del mismo.

Durante el servicio se irán acordando entre el adjudicatario y CRTVE las tareas a acometer y el esfuerzo aprobado para cada una de ellas.

El idioma de trabajo será el español.

4.2 Volumen de Servicios

La contratación consistirá en servicios profesionales variables según el volumen de actividad requerido, a excepción del SOC que tendrá un coste fijo mensual según los parámetros definidos.

SERVICIO INTEGRAL DE CIBERSEGURIDAD				
Servicios Oficina Técnica de Seguridad (OTS)	Horas/Año			
	Consultor Ciber	Especialista Ciber	Soporte Ciber	Total
Análisis de adecuación ENS y Planes de Mejora	0	1.760	0	1.760
OTS engranaje alertas entre Admins fuentes de logs y SOC	1.760	0	0	1.760
Análisis cíclico de situación y elaboración de Planes de Mejora. Analisis de ciberriesgos.	0	176	0	176
Actualización del Marco Normativo y procedimental	176	0	0	176
Desarrollos ampliados para integraciones del SOC	0	352	0	352
Gestión de vulnerabilidades y bastionado	176	880	0	1.056
Soporte al cumplimiento normativo	176	176	0	352
Concienciación y formación	352	352	0	704
TOTAL OTS	**2.640**	**3.696**	**0**	**6.336**
Servicios de Especialistas bajo demanda	Horas/Año			
	Consultor Ciber	Especialista Ciber	Soporte Ciber	Total
Seguridad en el ciclo de vida	17	53	0	70
Recurso Arquitecto coordinacion servicios especializados	880	0	0	880
Auditorías y test de intrusión	176	528	0	704
Operaciones de ciberseguridad y soporte a eventos RTVE (adicional a SOC)	18	176	0	194
Implantación de Planes de Mejora y Evaluación de herramientas	53	88	35	176
Analisis forenses	176	0	0	176
Desarrollos ampliados para integraciones del SOC	88	53	53	194
Soporte ad hoc al Responsable de Seguridad	352	0	0	352
TOTAL SERVICIO ESPECIALISTAS	**1.760**	**898**	**88**	**2.746**
TOTAL OTS + SERVICIO ESPECIALISTAS	**4.400**	**4.594**	**88**	**9.082**

La distribución de los Servicios y perfiles es orientativa, **pudiendo variar, según las necesidades durante el proyecto, la distribución de horas entre los distintos perfiles**, e incluso crearse nuevos según las necesidades, siempre que no se modifique el importe total.

Por todo ello el adjudicatario deberá garantizar la flexibilidad suficiente para su adecuación a las necesidades, en caso necesario.

Para cada actividad o necesidad, se realizará una valoración del esfuerzo necesario por parte del adjudicatario en base a los servicios profesionales previstos y, salvo que RTVE autorice un cambio de alcance, se ejecutarán consumiendo los esfuerzos previstos.

4.3 Equipo profesional

A continuación, se detallan los perfiles profesionales requeridos para cada servicio y los requisitos mínimos que deberán cumplir.

PERFILES REQUERIDOS						
Servicio	**Cod**	**Perfil**	**Titulación Mínima**	**Certificaciones mínimas**	**Experiencia específica mínima en el perfil requerido**	**CVs a presentar**
Responsable y Coordinador de Servicio	RdS	Consultor Seguridad de la Información (Estrategia)	Superior	Certificación PMP y adicionalmente 5 certificaciones: 3 certificaciones grupo I 1 certificación grupo II 1 certificación grupo III	15 años	1
Consultoría Ciberseguridad	CC.1	Consultor seguridad legal y ciber delitos	Superior (relacionado Derecho o similar)	3 certificaciones: 2 Certificaciones grupo III 1 Certificación grupo II	5 años	1
	CC-2	Consultor Seguridad de la Información (Estrategia y gestión SGSI) Consultor en Análisis de Riesgos Analista especialista en seguridad para la realización e interpretación de cuadro de mandos e informes.	MEDIA	7 certificaciones: 4 certificaciones grupo I 2 certificaciones grupo II 1 certificaciones grupo III	10 años	1
	CC-3	Inteligencia Amenazas Inteligencia Monitorización Incidentes (casos de uso, tunning, correlación SIEM, integración logs de eventos y fuentes de seguridad) Analista de intrusión (Gestor de incidentes, SIEM-UEBA) Inteligencia tunning seguridad perimetral (IPS, FW, NGF, PROXYS, UEBA/IPS/NGFW/EPP, etc.)	MEDIA	4 certificaciones: 1 certificaciones grupo I 1 certificaciones grupo II 2 certificaciones grupo IV	10 años	1
	CC-4	Experto en análisis forense (sin repercusión legal) Experto en seguridad perimetral	MEDIA	3 certificaciones grupo V o VI	6 años	1

PERFILES REQUERIDOS						
Servicio	**Cod**	**Perfil**	**Titulación Mínima**	**Certificaciones mínimas**	**Experiencia específica mínima en el perfil requerido**	**CVs a presentar**
		Experto en test de intrusión y HE				
Especialista Ciberseguridad	EC-1	Experto en formación y concienciación en ciberseguridad Consultor técnico de seguridad Analista especialista en seguridad para la realización e interpretación de cuadro de mandos e informes.	MEDIA	4 certificaciones: 2 certificaciones grupo I 1 certificaciones grupo II 1 certificación grupo III	5 años	1
	EC-2	Experto gestión de vulnerabilidades (herramientas automáticas y actividades complejidad media) Experto en seguridad (sistemas, comunicaciones y redes)	MEDIA	2 certificaciones grupo VI	3 años	1
	EC-3	Analista de intrusión nivel 1-2 (Gestor de incidentes/SIEM-UEBA	MEDIA	1 certificación grupo I o IV	3 años	1
Soporte Ciberseguridad	SP -1	Técnico en gestión de métricas, KPIs, cuadro de mandos e informes	MEDIA	1 certificaciones grupo IV	3 años	1
	SP - 2	Técnico Gestión de vulnerabilidades	MEDIA	1 certificaciones grupo V	3 años	1
	SP - 3	Técnico de Monitorización y Gestión de incidentes de seguridad (nivel 1 SOC)	MEDIA	1 certificaciones grupo VI	3 años	1

A continuación, se define el Cuadro de certificaciones a presentar agrupados según se indica a continuación:

GRUPO I	GRUPO II	GRUPO III	GRUPO IV	GRUPO V	GRUPO VI
CISM (ISACA) Lead Auditor ISO 27001 o CISA (ISACA) Lead Auditor ISO 22031 Lead Implementer ISO 27001	ITIL Foundation (mínimo v3) ITIL v4 Managing Professional Cobit 5 Foundation ISO 2000 auditor ISO 2000 Consultant	DPD Certificado (bajo el esquema de la AEPD) CDPSE (ISACA) CDPP (Isms Forum)	IBM Certified Associate Security QRadar IBM Certified Deployment Professional Security Qradar SIEM IBM Certified Associate Administrator - Security QRadar SIEM	CEH (eCOUNCIL) CHFI (eCOUNCIL) OSCP Comptia CCNA	Microsoft 365 Certified: Security Administrator Associate NSE 1 Network Security Associate (Fortinet) NSE 2 Network Security Associate

Lead Implementer ISO 22301 CRISC o ISO31000 Risk Manager Cybersecurity Fundamentals Certificate (CSX)	Manager Prince 2 PMP		V7.2.8 IBM Certified Associate Analyst - IBM QRadar SIEM		(Fortinet) NSE 3 Network Security Associate (Fortinet)

Se deberá presentar un CV distinto por cada perfil solicitado, es decir, **un total de 11 CVs**. En la valoración técnica no se tendrán en consideración CVs adicionales a los solicitados.

La empresa adjudicataria prestará el servicio con recursos que cumplan con los requisitos exigidos en este pliego, adoptando las medidas necesarias para que esto se cumpla a lo largo de todo el contrato

Nota:

- Se considera Titulación Superior: Ingeniería superior, Licenciatura, Grado + Master.
- Se considera Titulación Media: Ingeniería Técnica, FP2, Grado.

Los licitadores incluirán en sus propuestas documentación que acredite la formación exigida.

El licitador rellenará la tabla resumen de recursos propuestos mostrada a continuación, para facilitar la valoración. Dicha tabla será revisada por RTVE, prevaleciendo la valoración que realice RTVE a la vista de los CV presentados y la documentación acreditativa en caso de que se solicite.

PERFILES REQUERIDOS						
Servicio	**Cod**	**Perfil**	**Titulación**	**Certificaciones**	**Experiencia específica**	**Iniciales**
Responsable y Coordinador de Servicio	RdS	Consultor Seguridad de la Información (Estrategia)				
Consultoría Ciberseguridad	CC.1	Consultor seguridad legal y ciber delitos				
	CC-2	Consultor Seguridad de la Información (Estrategia y gestión SGSI)				

PERFILES REQUERIDOS						
Servicio	**Cod**	**Perfil**	**Titulación**	**Certificaciones**	**Experiencia específica**	**Iniciales**
		Consultor en Análisis de Riesgos Analista especialista en seguridad para la realización e interpretación de cuadro de mandos e informes.				
	CC-3	Inteligencia Amenazas Inteligencia Monitorización Incidentes (casos de uso, tunning, correlación SIEM, integración logs de eventos y fuentes de seguridad) Analista de intrusión nivel 2 y 3 (Gestor de incidentes, SIEM-UEBA) Inteligencia tunning seguridad perimetral (IPS, FW, NGF, PROXYS, UEBA/IPS/NGFW/EPP, etc.)				
	CC-4	Experto en análisis forense (sin repercusión legal) Experto en test de intrusión y HE				
Especialista Ciberseguridad	EC-1	Experto en formación y concienciación en ciberseguridad Consultor técnico de seguridad				

PERFILES REQUERIDOS						
Servicio	**Cod**	**Perfil**	**Titulación**	**Certificaciones**	**Experiencia específica**	**Iniciales**
		Analista especialista en seguridad para la realización e interpretación de cuadro de mandos e informes.				
	EC-2	Experto gestión de vulnerabilidades (herramientas automáticas y actividades complejidad media) Experto en seguridad (sistemas, comunicaciones y redes)				
	EC-3	Analista de intrusión nivel 1-2 (Gestor de incidentes/SIEM-UEBA				
Soporte Ciberseguridad	SP -1	Técnico en gestión de métricas, KPIs, cuadro de mandos e informes				
	SP - 2	Técnico Gestión de vulnerabilidades				
	SP - 3	Técnico de Monitorización y Gestión de incidentes de seguridad (nivel 1 SOC)				

4.4 Dirección y Coordinación del Servicio

El adjudicatario gestionará todo el servicio, bajo la supervisión de CRTVE y por medio de la estructura de gestión y dirección que considere necesaria, que deberá detallar en su propuesta técnica.

Deberá designar un **responsable y Coordinador de Servicio (RdS)** para toda la duración del contrato**,** que será el coordinador de todos los trabajos y será el único interlocutor válido entre los responsables de RTVE y los recursos personales integrantes del servicio a todos los efectos.

Realizará el seguimiento de todos los servicios, y tareas tales como:

- Dirección de los trabajos y servicios del adjudicatario.
- Coordinación del equipo de profesionales.

- Coordinación de actividades in-situ y remotas.
- Planificación, ejecución y priorización de las tareas.
- Aseguramiento de la disponibilidad de los recursos.
- Supervisión de la calidad en los trabajos y entregas de documentación.
- Supervisión de cumplimiento de ANS.
- Escalado de incidentes.
- Seguimiento de las incidencias hasta su cierre.
- Propuestas de mejora del servicio.
- Disponibilidad para la coordinación de cualquier incidencia crítica en caso necesario.
- Elaboración de informes de seguimiento del servicio.
- Gestión de Riesgos.
- Elaboración de actas de reunión.
- Participar en las reuniones de seguimiento.
- Coordinación con los responsables de los distintos departamentos de RTVE.
- Asegurar el cumplimiento de los procedimientos de trabajo.
- Control de la documentación.
- Otros.

Dado que lo que se requiere es un servicio llave en mano, el licitador indicará en su propuesta el equipo propuesto para la dirección y seguimiento del servicio y la dedicación de los mismos. Los recursos dedicados a estas tareas deberán tener la adecuada cualificación y experiencia, acordes a las características y criticidad del servicio, para garantizar su correcto funcionamiento.

En todo momento, en horario 8x5 habrá, un Responsable del Servicio disponible, para coordinar y dirigir los trabajos, y para la permanente coordinación con los responsables de RTVE.

Asimismo, siempre habrá un responsable localizable 24x7 para el escalado de cualquier incidencia crítica que requiera atención inmediata.

RTVE podrá solicitar la sustitución de cualquier miembro del equipo de gestión en caso de que, de forma justificada, no se considere adecuado.

El responsable y Coordinador de Servicio (RdS) y cualquier otro dedicado por el adjudicatario a estas tareas no supondrá coste alguno para RTVE ni consumirá horas de servicios variables descritos anteriormente.

4.5 Horario del servicio y servicios 24x7

El horario normal del servicio será fijado durante la fase de transición.

El horario del servicio SOC será siempre 24x7.

En todo caso, el horario de trabajo podrá modificarse a solicitud de RTVE, y se adaptará siempre para garantizar que se cumplen las necesidades del servicio teniendo en cuenta cualquier situación, evento especial, intervención programada o incidencia que requiera servicio presencial o remoto en cualquier horario, incluyendo noches, fines de semana y festivos. Los recursos empleados en estos trabajos tendrán el mismo coste que los servicios prestados en el horario habitual de servicio.

Para ello, el adjudicatario dispondrá en todo momento de los **recursos de guardia necesarios localizables 24x7** para resolver cualquier incidencia crítica en el servicio, para en todo momento cumplir los ANS indicados en este pliego, para lo cual el adjudicatario deberá disponer de un **teléfono de guardia** para el escalado de las incidencias críticas.

De igual forma deberán existir procedimientos para realizar consultas telefónicas en horario 8x5 a aquellos técnicos especialistas que no tengan una presencia habitual en las instalaciones de RTVE.

Los trabajos solicitados en horario 24x7 se **realizarán con las mismas tarifas acordadas para el servicio regular. Estos trabajos fuera del horario habitual no superarán el 5% del total de servicios profesionales a realizar (sin incluir el servicio SOC). En caso de superarse dicho volumen, las horas adicionales en 24x7 se computarán como 1,5 veces sobre las horas de servicio en horario normal.**

4.6 Constitución y Modificación del equipo de trabajo

El adjudicatario, una vez formalizado el contrato, deberá incorporar, en un plazo máximo de **15 días laborables**, **todos los recursos previstos para la fase de transición,** para prestar los servicios a CRTVE.

Si, por circunstancias no previstas, hubiera que sustituir a un recurso del equipo durante el tiempo de vigencia del contrato, el sustituto deberá ser previamente aprobado por CRTVE, asumiendo el adjudicatario el tiempo de solapamiento de un mínimo de **15 días laborales**, entre el recurso saliente y el entrante, requerido para la adquisición del conocimiento del nuevo miembro del equipo. El recurso sustituto deberá cumplir los conocimientos y certificaciones requeridas. RTVE se reserva durante ese plazo el derecho de aceptar o rechazar al nuevo recurso.

CRTVE podrá requerir la disminución o aumento de los recursos asignados a algunas actividades, en función de las necesidades surgidas en cada momento. Esta alteración del equipo será notificada con la suficiente antelación al adjudicatario.

Se considerará rotación a cualquier sustitución de los recursos, ya sea por causas imputables al adjudicatario, o bien a petición expresa y justificada por parte de CRTVE y, en ningún caso, **podrá superar el 20% anual.**

En caso de requerirse algún recurso para cualquier necesidad sobrevenida, el adjudicatario deberá garantizar la puesta a disposición en un plazo máximo de **10 días** naturales, bien sea de forma presencial, bien de forma remota.

Cambios Requeridos por RTVE

Será potestad de RTVE, si existen razones justificadas que así lo aconsejen, solicitar el cambio de los recursos asignados al servicio por otros de características similares, mediante aviso de quince días de antelación a la empresa adjudicataria.

La empresa adjudicataria se compromete a facilitar la incorporación del nuevo recurso en un plazo máximo de 15 días, siendo en todo caso, a costa del adjudicatario el tiempo de solapamiento, entre el recurso saliente y el entrante, requerido para la adquisición del conocimiento del nuevo miembro del equipo.

Cambios requeridos por el adjudicatario

Si durante la ejecución del contrato la empresa adjudicataria solicitase la sustitución de alguno de los

recursos que realiza el servicio, este hecho deberá ser comunicado a RTVE con dos semanas de antelación, exponiendo los motivos de dicha decisión, garantizando la idoneidad del nuevo recurso para la ejecución del proyecto.

RTVE deberá aprobar la sustitución, siendo en todo caso, a costa del adjudicatario el tiempo de solapamiento, entre el recurso saliente y el entrante.

5 ASPECTOS GENERALES DEL SERVICIO

5.1 Plan de transición y fases del servicio

5.1.1 Transición de Entrada del Servicio

El adjudicatario desarrollará un Plan de Transición detallado a lo largo de las dos primeras semanas tras la formalización del contrato, en el que se identifique el plan de trabajo para el arranque de los distintos servicios de acuerdo con RTVE.

En dicho plan se detallarán todas las actividades que se deben llevar a cabo, las fechas de inicio y fin de cada actividad, la distribución de responsabilidades de las partes, criterios aplicables de aceptabilidad, recursos específicos que debe proveer CRTVE y cualquier otro detalle pertinente. Este plan ha de ser aprobado por CRTVE previo a su ejecución.

Se definirán y dotarán junto con los responsables de CRTVE las necesidades de conectividad desde los locales de CRTVE y los del SOC del adjudicatario. En particular, la conectividad necesaria hacia el SIEM del adjudicatario desde las actuales fuentes de eventos y logs de seguridad de RTVE, descritos en el presente documento.

Tal como se indica en el apartado correspondiente, el adjudicatario realizará:

- La puesta en marcha y configuración de la herramienta SIEM propuesta.
- La integración con las fuentes de alertas de RTVE
- La migración de reglas y resto de datos necesarios
- La migración de la herramienta de ticketing y gestión del cambio para la implantación de la nueva herramienta.
- Traspaso de conocimiento sobre las infraestructuras y servicios de RTVE
- Traspaso de conocimiento del Marco de Seguridad, procedimientos de ciberseguridad, etc.
- Traspaso del conocimiento de todas las líneas de Servicio actuales necesario para continuarlos.

CRTVE pondrá a disposición del adjudicatario toda la documentación requerida, que se identificará y analizará por éste para actualizarla o generarla si no existiera.

Una vez finalizado el periodo de transición, el adjudicatario deberá garantizar que se hayan incorporado todos los recursos previstos en su propuesta.

Durante el período de transición, no se aplicarán penalizaciones relativas al ANS.

El adjudicatario tiene obligación de documentar todas las actividades del proceso de transición y entregar esa documentación a CRTVE cuando termine el proceso.

La duración máxima del periodo de transición será de **2 meses** a partir de la fecha de inicio del contrato**.**

Los trabajos realizados por el adjudicatario durante el periodo de transición serán asumidos íntegramente por éste, hasta que finalice la transferencia de los servicios desde el proveedor saliente y el adjudicatario inicie el servicio de forma regular realizando las tareas encomendadas.

Los licitadores detallarán en su propuesta la metodología y la planificación propuesta, y los recursos aportados para realizar la transición asegurando el correcto traspaso de conocimientos entre los equipos

y garantice la continuidad del servicio minimizando los riesgos y asegurando el cumplimiento del plazo máximo.

5.1.2 Servicio Regular

Una vez concluida la fase de transición se iniciará la fase de Servicio Regular, para gestionar y mantener operativo el servicio:

- Servicios de la OTS, de forma regular según necesidades
- Servicios de Especialistas, cuando se requieran
- Servicio del SOC

5.1.3 Transición de salida

En el momento de finalización del contrato, el adjudicatario estará obligado a devolver el control del servicio a RTVE.

Con anticipación suficiente al inicio de la fase de devolución del servicio, como minino **dos meses**, se hará una evaluación y planificación de todas estas actividades.

El adjudicatario deberá realizar el proceso de reversión, asegurando que se mantiene el servicio regular a CRTVE durante el traspaso del control de servicios, y deberá colaborar activamente con CRTVE y el futuro proveedor durante este proceso para facilitar la transición de los servicios sin causar perjuicios, asegurando en todo momento la disponibilidad de los recursos que CRTVE requiera en esta fase.

En particular, el adjudicatario saliente deberá dar soporte proactivo al adjudicatario entrante para asegurar la conectividad y correcta configuración necesaria hacia el SIEM del adjudicatario entrante desde las fuentes de eventos y logs de seguridad de RTVE, descritos en el presente documento y que puedan evolucionar en la prestación del servicio durante la fase de servicio regular.

El adjudicatario deberá prestar a CRTVE servicios de asistencia de transición y colaborará con el nuevo proveedor en la necesaria transferencia de conocimiento. El personal de CRTVE colaborará con el adjudicatario, durante el período de servicios de reversión. Durante la ejecución de los trabajos objeto del contrato, el adjudicatario se compromete, en todo momento, a facilitar a las personas designadas por CRTVE a tales efectos, la información y documentación que éstas soliciten para disponer de un pleno conocimiento de las circunstancias en que se desarrollan los trabajos, así como de los eventuales problemas que puedan plantearse y de las tecnologías, métodos y herramientas utilizados para resolverlos. Se pretende, en definitiva, que este contrato contemple una transferencia tecnológica apropiada.

Durante esta fase el adjudicatario estará obligado a actualizar toda la documentación existente generada durante el servicio.

5.2 Acuerdos de Nivel de Servicio

Los servicios se realizarán, siempre que sea posible, de acuerdo a un modelo de nivel de servicio (ANS) que permita, a partir de indicadores definidos, evaluar y medir de manera eficaz estos niveles y compararlos con los objetivos establecidos para los distintos tipos de desarrollos a considerar.

A todas y cada una de las incidencias y peticiones se les asignará un nivel de prioridad que permitirá realizar

un seguimiento y evaluar de manera objetiva el nivel de servicio.

Los indicadores que conforman el acuerdo de nivel de servicio (ANS) se recogen en este apartado, pudiendo ser completados y ampliados por el licitador, conforme a su planteamiento y metodología para asumir los compromisos de servicio.

Los Niveles de Servicio se podrán revisar por acuerdo de las partes para adaptarlos a las circunstancias de evolución en el tiempo.

No serán de aplicación los ANS en los periodos de transición de entrada y salida.

Tampoco se aplicarán los ANS cuando los problemas que causen la desviación sean ajenos al adjudicatario por la no aplicación por parte de CRTVE de recomendaciones dadas por el adjudicatario o por cambios en los procesos o procedimientos establecidos.

En ningún caso afectará al nivel de servicio la no disponibilidad de recursos por parte del adjudicatario, así como la incorporación de nuevos recursos por sustitución de los originales.

El adjudicatario emitirá con periodicidad mensual los informes de seguimiento que se determinen en el periodo de transición. En los informes se deberán analizar las causas del incumplimiento si lo hubiera, indicando las acciones adoptadas para corregirlo.

5.2.1 Indicadores

A efectos del ANS, se tendrán en cuenta las siguientes definiciones:

- **Horario de Cobertura:** La franja horaria de servicio de cara al cumplimiento de ANS será **24x7**
- **Tiempo de respuesta**: Tiempo que transcurre desde que se comunica la incidencia adjudicatario, hasta que un técnico inicia los trabajos de su resolución y/o escalado.
- **Nivel de Criticidad**: Se establecen los siguientes niveles de criticidad según el impacto del incidente

Nivel	Descripción
1 – Bajo	• No afecta a servicios/datos relacionados con el negocio o estos son de **criticidad baja**. • Afecta a **menos de 25 equipos**, y sin datos especialmente sensibles. • No se aprecia riesgo de propagación del incidente. • No afecta a datos personales. • No hay daños reputacionales. • Las actividades de resolución precisadas son internas en RTVE y poco costosas.

2 – Medio	• Afecta a sistemas/datos de **criticidad media** para el negocio • Afecta **entre 25 y 500** equipos o a equipos con **datos sensibles**. • Hay **riesgo de propagación** del incidente. • Afecta a **datos personales**. • Hay **riesgo de daños reputacionales**, con eco mediático moderado. • Las actividades de resolución precisadas requieren de actividades de **complejidad media**.
3 – Alto	• Afecta a sistemas/datos de **criticidad alta** para el negocio. • Afecta a más de **500 equipos** o a equipos con datos muy sensibles. • Hay **daños reputacionales relevantes**, con eco mediático (amplia cobertura en los medios de comunicación) y/o afectando a la reputación de terceros • Las actividades de resolución precisadas requieren de actividades **muy costosas**.

Se considera **"Tiempo de respuesta**" al que transcurre desde que se conoce la incidencia, hasta que se inician las actividades de diagnóstico y resolución. Dicho tiempo se medirá a partir del momento en que RTVE comunica directamente el incidente al adjudicatario o bien el propio adjudicatario detecta el incidente (lo que antes ocurra):

ACUERDOS DE NIVEL DE SERVICIO CIBERSEGURIDAD	
Descripción	**Objetivo**
Tiempo medio respuesta incidente/petición criticidad Alta (24x7)	<1h
Tiempo de respuesta incidente/petición de criticidad Media (24x7)	< 3h
Tiempo de respuesta incidente/petición de criticidad Baja (12x5)	< 8h
Calidad de entregas de documentación - Porcentaje de entregas sin errores	90,00%
Cumplimiento de plazo en tareas asignadas - Porcentaje de tareas entregadas en plazo	90,00%

En la siguiente tabla se muestra un ejemplo ilustrativo del seguimiento de cumplimiento de los ANS a presentar por el adjudicatario mensualmente:

Descripción	Objetivo	Valor	NC
Tiempo medio respuesta incidente/petición de criticidad Alta (24x7)	<1h	0,9h	OK
Tiempo de respuesta incidente/petición de criticidad Media (24x7)	< 3h	3,5h	**KO**
Tiempo de respuesta incidente/petición de criticidad Baja (12x5)	< 8h	7h	OK
Calidad de entregas de documentación - Porcentaje de entregas sin errores	90,00%	18h%	OK
Cumplimiento de plazo en tareas asignadas - Porcentaje de tareas entregadas en plazo	90,00%	100,00 %	OK

5.3 Entregables y gestión de la documentación

En los distintos apartados se han detallado los entregables requeridos para cada tarea.

Toda la documentación generada y entregables detallados en los distintos apartados del pliego será revisada por los responsables de servicio de RTVE y también podrá ser revisada por la Oficina de Gestión de Proyectos de RTVE, que determinará si la calidad de la documentación entregada es suficiente según los requerimientos de RTVE.

Los formatos de los entregables serán acordados con RTVE en la fase de transición, pudiendo el adjudicatario proponer los que considere más adecuados.

En caso de detectarse defectos en la documentación, el adjudicatario deberá realizar las correcciones oportunas y realizar una nueva entrega sin coste alguno para la CRTVE.

5.4 Modelo de seguimiento del servicio

5.4.1 Seguimiento y Control del Servicio

La gestión del servicio deberá incluir el control y seguimiento de avance de las distintas tareas, así como el seguimiento de acuerdos de nivel de servicio, informes de seguimiento, interlocución con los responsables del servicio de CRTVE, gestión de la disponibilidad del servicio y la gestión del servicio con orientación a la mejora continua.

El licitador detallará en un folio como máximo en su oferta la metodología y herramientas de control del servicio, que faciliten la gestión y la evaluación de la calidad del mismo.

Para el seguimiento y control del servicio CRTVE designará un Director Técnico del Proyecto cuyas funciones en relación con el objeto del presente contrato serán las siguientes:

- Establecimiento de Comités de Dirección y Seguimiento del contrato.
- Seguimiento permanente de la evolución del contrato entre el Director Técnico de CRTVE y el responsable del Servicio, con reuniones periódicas al objeto de revisar el grado de cumplimiento de los objetivos, la planificación de actividades y demás aspectos de gestión.

El adjudicatario establecerá un plan de gestión de riesgos del servicio que se mantendrá actualizado a lo largo de la duración del contrato, e incluirá:

- Identificación de riesgos y clasificación de los mismos
- Propuesta de medidas de mitigación

Como norma general, de forma periódica y para controlar la buena gestión de los servicios se considera necesario establecer, siempre de común acuerdo entre CRTVE y el adjudicatario:

- Reuniones periódicas de planificación y seguimiento.
- Informes periódicos de nivel de servicio y tendencias

Asimismo, se fijarán los mecanismos de control y coordinación necesarios con otros proyectos de CRTVE.

5.4.2 Roles y responsabilidades

Con el objetivo de fijar en líneas generales las responsabilidades del adjudicatario y de CRTVE, a continuación, se describen una serie de tareas y el responsable de ejecutarlas. En todo caso CRTVE podrá modificarlas de acuerdo con el adjudicatario para adaptarse a las necesidades puntuales del servicio.

El siguiente cuadro resume las principales responsabilidades en torno al servicio:

Tareas	**Responsable** (Principal en primer lugar)	**Comentarios**
Identificar nuevas necesidades	CRTVE	
Priorizar actividades relevantes	CRTVE	
Propuesta de mejoras de procesos de Seguridad	Adjudicatario	CRTVE, supervisa esta actividad
Aprobación de procedimientos	CRTVE	
Definición de políticas	CRTVE	Con la colaboración del adjudicatario
Supervisión de las tareas del adjudicatario y control de ANS	CRTVE	
Estrategia de evolución de servicios	CRTVE	Con la del

		colaboración adjudicatario
Autorización de acceso y utilización de recursos	CRTVE	
Priorizar actividades	CRTVE	
Realizar la planificación y calendarios, desglosando las actividades en hitos.	Adjudicatario	CRTVE, supervisa esta actividad
Definir los recursos asignados a cada tarea.	Adjudicatario	CRTVE, supervisa esta actividad
Revisión y aceptación de productos, servicios y entregables	CRTVE	
Seguimiento de las actividades: Detalle de avance, Revisión de la planificación, Riesgos y posibles desviaciones.	Adjudicatario	CRTVE, supervisa esta actividad
Cumplimentación de los datos en las herramientas de control de incidencias y peticiones y de gestión del servicio	Adjudicatario	CRTVE, supervisa esta actividad
Realizar los informes periódicos del nivel de servicio.	Adjudicatario	
Proponer, definir e implantar estándares y procedimientos que mejoren la gestión del servicio.	Adjudicatario	CRTVE, supervisa esta actividad
Aprobación de modificaciones o aceptación de nuevos estándares y procedimientos.	CRTVE	
Documentar la resolución de cada incidente.	Adjudicatario	
Realizar las entregas de nuevas versiones de los distintos documentos siguiendo la metodología propuesta.	Adjudicatario	
Proponer herramientas de gestión del servicio	Adjudicatario	
Apoyo a los usuarios en la resolución de incidencias y peticiones.	RTVE/Adjudicatario	CRTVE determinará que peticiones e incidentes son atendidas directamente por el adjudicatario.

Registro de las peticiones e incidencias de usuario en las herramientas de CRTVE.	CRTVE	
Priorización de las peticiones e incidencias.	CRTVE	
Recepción y Análisis de Incidencias.	Adjudicatario	Supervisado por CRTVE
Comunicaciones con el usuario de estado de la incidencia.	CRTVE/Adjudicatario	A determinar según el caso
Cierre de la incidencia o petición.	CRTVE	
Actualizar la información sobre la incidencia o petición en la herramienta de CRTVE según su tratamiento	Adjudicatario	
Asistencia in-situ o remota 24x7 según el caso para incidentes críticos	Adjudicatario	

5.5 Transferencia tecnológica y de Conocimiento y Formación

Durante la ejecución de los trabajos objeto del contrato, el adjudicatario se compromete, en todo momento, a facilitar a las personas designadas por RTVE a tales efectos, la información y documentación que éstas soliciten para disponer en todo momento, de un pleno conocimiento de las circunstancias en que se desarrollan los trabajos, así como de los eventuales problemas que puedan plantearse, y de las tecnologías, métodos y herramientas utilizados para resolverlos. Se pretende, en definitiva, que este contrato contemple una transferencia tecnológica apropiada.

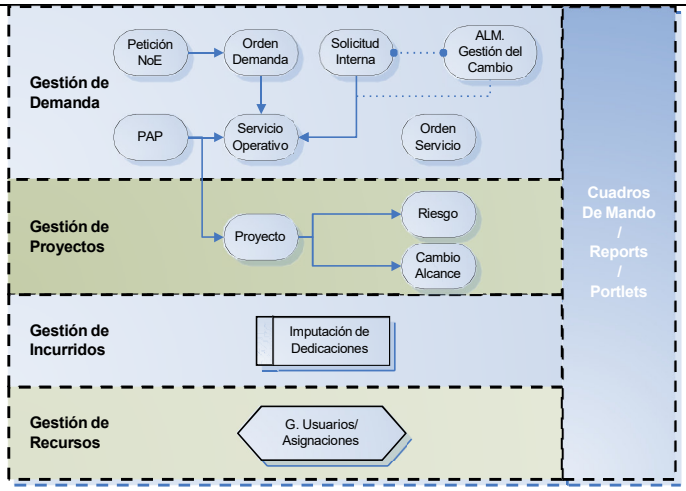
Se podrán solicitar acciones de formación en cualquiera de los aspectos y tecnologías de ciberseguridad para el personal de RTVE sobre las tecnologías y servicios objeto del contrato con cargo a los Servicios Variables contratados, en cualquier momento si fuese necesario para completar la transferencia de conocimiento.

5.6 Herramienta de Gestión SIGO

SIGO es la herramienta de Gobierno TI utilizada en la Dirección de Sistemas de CRTVE y cuya utilización es obligatoria para el adjudicatario.

Se trata de un sistema de gestión integrado orientado a la gestión de la demanda y la gestión de la cartera de proyectos.

El sistema proporciona la cobertura para los procesos de gestión y gobierno corporativo de TI facilitando al área de Sistemas la gestión y automatización de sus procesos de acuerdo con los flujos de trabajo y reglas previamente definidas para cada uno de sus módulos:



El módulo de **Gestión de la Demanda** en SIGO centraliza la demanda estratégica ejecutada a través de los procesos de Tramitación y Apertura de Proyectos y la demanda operativa relacionada con los procesos de gestión de peticiones, orientado a satisfacer los nuevos requerimientos (técnicos, funcionales, etc.) solicitados por las unidades de negocio de CRTVE, y la propia demanda interna para realizar actividades encaminadas a la gestión de activos clave de TI.

La demanda operativa en SIGO tiene como objetivo la gestión de las distintas peticiones no estandarizadas, tales como mantenimientos correctivos, evolutivos, asignación de tareas a los proveedores, etc., estableciendo una normalización y estandarización de las tareas a realizar aplicando diferentes flujos de gestión en función de la tipología de peticiones. Estos flujos de gestión están definidos por una secuencia ordenada de actividades, los roles que las desempeñan y los niveles de Gestión y aprobación establecidos para cada uno de ellos.

Las peticiones, una vez validadas por la Dirección de Sistemas, se enviarán al adjudicatario correspondiente para su realización, a través de la propia herramienta SIGO.

El soporte a los procesos de **Gestión de Cambios** dentro de la Dirección de Sistemas Información y Gestión se realiza utilizando la solución implementada en SIGO, la cual proporciona las herramientas necesarias para cumplir con el estándar Información Technology Infrastructure Library (ITIL).

El objetivo del proceso de Gestión de Cambios es garantizar que los cambios producidos en la infraestructura de TI son registrados, evaluados, autorizados, priorizados, planificados, probados, implementados, documentados y revisados de forma controlada. Un Gestor de Cambios se encarga de la supervisión del cambio a lo largo del ciclo de vida, coordinando las diversas organizaciones o departamentos involucrados.

Todos los flujos de peticiones soportan la gestión de los niveles de servicio sobre la demanda, configurándose los indicadores en función de los ANS definidos con los proveedores y calculándose el grado de cumplimiento mensual de forma automática.

Para los servicios externos basados en los servicios variables, SIGO facilita la gestión del tiempo de los recursos de un proveedor. Los recursos pueden imputar el tiempo dedicado a nivel de proyecto o de tarea,

en peticiones específicas o actividades genéricas, y sincronizarse el tiempo imputado con el tiempo asignado a cada concepto, y será la base para la facturación de los servicios.

6 INCUMPLIMIENTOS GRAVES DEL SERVICIO

Dada la criticidad e importancia de los servicios objeto de este pliego por su impacto en la disponibilidad de los sistemas críticos para los usuarios de CRTVE, el adjudicatario deberá asegurar el estricto cumplimiento del mismo sin deficiencias que puedan afectar al servicio prestado.

Se considerarán incumplimientos graves las siguientes situaciones:

- **Fallos graves** en el servicio que causen graves deficiencias en el funcionamiento de un servicio crítico imputables a los servicios prestados por el adjudicatario en este contrato, tales como:
  - **Indisponibilidad** prolongada por más de **4 horas** de un servicio crítico por causas imputables al adjudicatario.
  - **Fallos graves en funcionalidad** de un servicio por causa del adjudicatario.
  - **Pérdida de Información** no recuperable por causa del adjudicatario.
  - **Perdida grave de rendimiento** de un servicio durante más de 4 horas por causa del adjudicatario.
  - Otros fallos graves.

    No se imputarán al adjudicatario los fallos en los sistemas derivados de posibles incidentes de seguridad, sino los derivados directamente de su propia actividad, en el caso de que se produzcan por cualquier intervención del adjudicatario durante sus servicios.
- **Incumplimiento del plazo** acordado para una tarea de relevancia en más de **15 días naturales**.
- La **no incorporación** al inicio de cualquier recurso concreto y comprometido en la propuesta del adjudicatario.
- **Incumplimiento del período de preaviso** de sustitución de un recurso (15 días) por parte del adjudicatario.
- **Incumplimiento del plazo de solapamiento** mínimo de 15 días laborables en caso de baja de un recurso.
- Incumplimiento por parte del adjudicatario del **plazo de incorporación puntual** de recursos solicitados por CRTVE.
- Incumplimiento del **índice máximo de rotación anual**, en el mes en el que se produzca, y por cada vez que suceda superando dicho límite.
- **Ausencia temporal de prestación** de alguno de los servicios durante más de **5 días** naturales imputable al adjudicatario, por cualquier causa ajena a CRTVE, sin proporcionar un recurso sustituto.
- **Falta de colaboración** en el cumplimiento de los objetivos de la **transición de salida**, a criterio de CRTVE).
- Incumplimiento de la **entrega de informes mensuales** de seguimiento de ANS.

Cualquier incumplimiento grave de los anteriormente descritas supondrá una **penalización según lo indicado en el Anexo II del pliego de condiciones generales.**

7 ESTRUCTURA DE LAS OFERTAS TECNICAS

La siguientes es la estructura de la oferta de Servicios con indicación del número de páginas por apartado. La oferta total no deberá exceder setenta páginas en tamaño mínimo de letras de once, en tipo Arial o similar.

1. INTRODUCCION (1 página)
2. RESUMEN EJECUTIVO (3 página)
3. DESCRIPCIÓN DE LOS SERVICIOS
   - 3.1 SERVICIOS OTS (máximo 15 páginas)
     - Catálogo de actividades de servicio a disposición de RTVE
     - Gestión de la capacidad y demanda
   - 3.2 SERVICIOS ESPECIALIZADOS (máximo 15 páginas)
     - Catálogo de actividades de servicio a disposición de RTVE
     - Gestión de la capacidad y demanda
   - 3.3 CENTRO DE OPERACIONES DE SEGURIDAD (SOC) (máximo 15 páginas))
     - Metodología y procesos internos
     - Medios tecnológicos y herramientas
     - Flexibilidad para picos de trabajo no previstos
     - Coordinación entre el equipo de personal in situ y remoto
     - Gestión de la capacidad y demanda
4. EQUIPO PROFESIONAL (máximo 10 páginas)
   - 4.1 CARACTERÍSTICAS GENERALES
   - 4.2 VOLUMEN DE SERVICIOS
   - 4.3 SERVICIOS DEL EQUIPO PROFESIONAL
   - 4.4 DIRECCIÓN Y COORDINACIÓN DEL SERVICIO
   - 4.5 CONSTITUCIÓN Y MODIFICACIÓN DEL EQUIPO PROFESIONAL
   - 4.6 SERVICIOS REMOTOS Y SOPORTE 24X7
   - 4.7 LUGAR DE REALIZACIÓN DEL SERVICIO
5. ASPECTOS GENERALES DEL SERVICIO (máximo 10 páginas)
   - 5.1 PLAN DE TRANSICIÓN Y FASES DEL SERVICIO
   - 5.2 ACUERDOS DE NIVEL DE SERVICIO
   - 5.3 ENTREGABLES Y GESTIÓN DE LA DOCUMENTACIÓN
   - 5.4 MODELO DE SEGUIMIENTO DEL SERVICIO

5.5 TRANSFERENCIA TECNOLÓGICA Y DE CONOCIMIENTO Y FORMACIÓN

6. SUBCONTRATACIONES (máximo 1 página)
7. ANEXOS

8 ANEXO FORMATO DE CV'S

TODOS LOS CV SE PRESENTARÁN EN CASTELLANO, EN CASO CONTRARIO NO SERÁN EVALUADOS

CUESTIONARIO DE PERSONAL (CV)

Datos particulares (1 hoja por recurso aplicable al objeto del contrato)

Categoría ofertada y Perfil:	
Iniciales:	
Empresa de pertenencia:	

Antigüedad en empresa (antigüedad en categoría y experiencia en Seguridad de la Información)

Empresa	Categoría	Fecha alta	Fecha baja	Meses	Actividad en Seguridad de la Información

Formación técnica/seguridad

(solo se tendrá en cuenta si se aportan los diplomas y certificados)

	Entorno del Servicio de Ciberseguridad	Otros entornos

Curso	Horas	Empresa	F-inicio	Horas	Empresa	F-inicio

Certificaciones TIC

Certificación	Descripción larga	Fecha Expedición

Certificaciones Seguridad

Certificación	Descripción larga	Fecha Expedición

Titulación académica TIC / Seguridad

(solo se tendrá en cuenta si se aportan los títulos)

Título académico	Centro	Años	Fecha Expedición

Años: Duración oficial

Datos relativos a los proyectos (para experiencia en proyectos de seguridad y ciberseguridad)

Clave	Nombre	F-inicio	F-fin	Entidad usuaria	Características
P1					
P2					
..					
..					
Pn					

Características: breve descripción de las características del proyecto/servicio

Experiencia en los entornos tecnológicos/seguridad

Clave	Categoría	Meses	ET1	ET2	.....	.....	.....	.....
P1								
P2								
P3								
P4								
P5								

Categoría: La ejercida en el proyecto

ET: Marcar con X las tecnologías que intervienen relacionadas con los servicios objeto del pliego.

Los ETs deben ser sustituidos por las tecnologías respectivamente de las que se desee contrastar la experiencia del personal.